CITRIX

AppDNA 1906

Contents

AppDNA 1906

June 17, 2019

AppDNA is the application migration component of Citrix Virtual Apps and Desktops Premium edition (formerly XenApp and XenDesktop Platinum edition). AppDNA enables enterprises to discover, automate, model, and manage applications for application migration, virtualization, and streamlined application management.

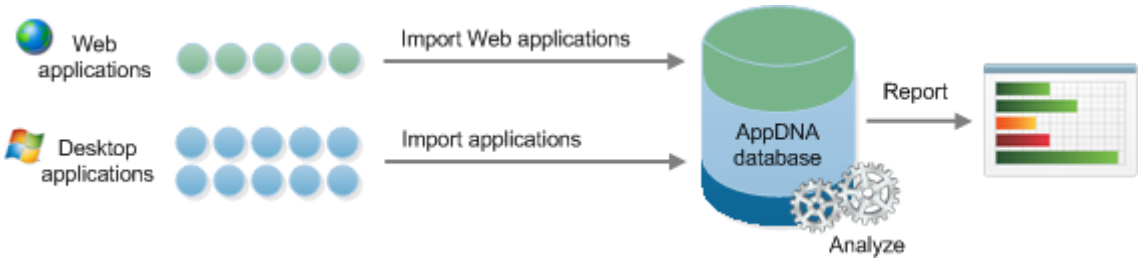
For example, AppDNA helps accelerate application migrations to Windows 10 and Windows Server 2016 by predicting potential issues and showing a clear path to application compatibility on the new operating system.

You can download and install AppDNA from https://www.citrix.com/downloads/appdna/.

For enhancements and new features in this release, see What's New.

Import, analyze, and report

AppDNA performs automated analysis of the compatibility of applications with a variety of platforms. Each supported platform is represented by a separate report that contains a set of algorithms that validate the suitability and performance of applications in a specific target environment.



Import - Applications are the raw material for AppDNA - so before you begin, you need to import them. When you do this, AppDNA interrogates each application's files, registry entries, and API usage to expose the application's "DNA". AppDNA then loads this into a SQL Server database. You can import desktop and Web applications of any type - whether internally developed or supplied by an independent software vendor (ISV).

Learn more: Import applications

Analyze - When you start the analysis process, you select the reports that correspond to the platforms against which you want to test your applications. AppDNA combines all of the information it has about the application portfolio and runs the report algorithms against the application DNA and produces and stores the reporting data.

Learn more: Analyze applications

Report - After the import and analysis processes have completed, you can view the reporting results. AppDNA presents the results of the analysis in a set of report views that provide the information that you need to plan, fix, and test your application portfolio.

Learn more: Report views

What's new

May 5, 2020

AppDNA 1906

AppDNA 1906 does not include any new features. For information about bug fixes, see Fixed issues.

IIS configuration for AD Integrated Login

Changes are required to the way IIS is configured if you are using AD Integrated login. For more information, see Integrated Login.

New product and component version numbers

In this release, the AppDNA version number is displayed in the user interface and documentation in the same numeric format as Citrix Virtual App and Desktops (1906). The file version continues to use the 7.x format (7.21). For a full description of this format, see New product names and version numbers.

Fixed issues

June 17, 2019

- 10 GB file on OS image causes incomplete OS snapshot. [APPDNA-1770]
- Exception when importing App-V files using AppDNA 7.16 client. [APPDNA-1789]
- Algorithm OSV_001 does not correctly check the service pack level on some OS Snapshots. [APPDNA-1794]
- Quoted paths for install capture are not handled correctly. [APPDNA-1795]

- Some internal errors cause User group info collection to be incomplete. [APPDNA-1796]

Known issues

June 17, 2019

The following warning applies to any workaround that suggests changing a registry entry.

> **Warning:**
>
> Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

- When the IIS Web server is set up to require Windows Authentication, clicking the **Download** button for the OS Snapshot Manager results in an "Unauthorised" message.

  To workaround this issue, either 1) manually copy the MSI from the AppDNA Webserver (C:\Program Files\Citrix\AppDNA\Server\Download\snapshotmanager.exe), or 2) temporarily allow Anonymous Authentication in the Internet Information Services (IIS) Manager. [AppDNA-1797]

- AppDNA reports assess the suitability of XenApp and XenDesktop, and Citrix Virtual Apps and Desktops, as deployment mechanisms for your applications. However, reporting modules, solutions and algorithm remediation texts refer only to XenApp and XenDesktop. Similarly, various references throughout the user interface and product documentation do not refer to Citrix Virtual Apps and Desktops.

- During App-V solution configuration, when using the Fix option to fix the VM, the installation gets stuck at installing App-V Sequencer step for Windows 10 build 1703 with the configured built-in sequencer. To work around this issue, cancel the "Go to Microsoft website" action and warning. The VM configuration can then finish successfully. [APPDNA-1685]

- The AppDNA web server processes depend on .NET 4.5.1 as a minimum version. If the web server has .NET 4.6 or later installed, the AppDNA IIS process can stop working unexpectedly. This issue produces unhandled exceptions and failed import or analysis tasks. Error messages are likely to contain a statement that refers to w3wp.exe. For example, "DotNet Framework exception Error w3wp.exe [4520]".

  To resolve the issue, install the Microsoft update for your server environment:

  https://support.microsoft.com/en-us/kb/3088955 (Windows Server 2012 and Windows 8)
  https://support.microsoft.com/en-us/kb/3088956 (Windows Server 2012 R2 and Windows 8.1)

https://support.microsoft.com/en-us/kb/3088957 (older Windows versions) [# APPDNA- 1475]

- The App-V Solution cannot use Windows 10 AU (Version 1607 and 1703) or Windows Server 2016 platforms to create App-V packages. [APPDNA-1636]
- The error message, "DirectedSpider.exe is not a valid Win32 application", is displayed when launching the Directed Spider on Windows XP SP3.

  To work around the issue, use an older version of AppDNA (AppDNA 7.9 or earlier). [APPDNA-1371]
- When the client side parts of the import process take an unusually long time to complete, cancelation requests may not be responded to in a timely manner.

  To work around this issue, close AppDNA. This will stop the import. [AppDNA-432]

Deprecation

June 17, 2019

The announcements in this article are intended to give you advanced notice of platforms, Citrix products, and features which are being phased out so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when they are withdrawn. This list is subject to change in subsequent releases and might not include every deprecated feature or functionality.

The following platforms, Citrix products, and features are deprecated. This does not mean that they are removed immediately. Deprecated items will be removed in a Current Release following the next Long Term Service Release (LTSR). Alternatives for deprecated items are suggested where possible.

For details about product lifecycle support, see the Product Lifecycle Support Policy article.

Item	Announced in	Removed in
Support for AppDNA server and client on: Microsoft Windows Server 2012; Microsoft Windows Server 2008 R2 SP1; Microsoft Windows 10 RTM; Microsoft Windows 10 1511; Microsoft Windows 8.1; Microsoft Windows 7 SP1	7.16	7.18

Item	Announced in	Removed in
Support for Install Capture platforms and Install Capture supported hypervisors: Microsoft Hyper-V Server 2012; Microsoft Hyper-V Server 2008 R2; Microsoft Windows 8.1 Hyper-V Client;Microsoft Windows 8 Hyper-V Client; Microsoft Windows 10 RTM; Microsoft Windows 10 1511; Microsoft Windows 8.1; Microsoft Windows 8; Microsoft Windows 7 SP1*; VMware Workstation (all versions);* supported on Install Capture platform only	7.16	7.18
Microsoft SQL Server 2008 R3 (all SPs)	7.16	7.18
AD Data Collector tool support on: Microsoft Windows Server 2012; Microsoft Windows Server 2008 R2 SP1; Microsoft Windows 10 RTM; Microsoft Windows 10 1511; Microsoft Windows 8.1; Microsoft Windows 7 SP1	7.16	7.18
AppDNA VM tools support on: Microsoft Windows 8.1	7.16	7.18
AppDisks support	7.15	
AppDNA standalone licensing	7.14	7.16
Upgrades from 7.6.2990.2378 and 7.5.26.239473	7.14	7.16
App-V 4.6 support and analysis	7.14	7.16

Item	Announced in	Removed in
AD Data Collector tool support for SCCM 2003 or SCCM 2007	7.14	7.16
Support on Microsoft Windows Vista or Microsoft Windows 8.0 for: AppDNA VM tools; Directed Spider tool; AD Data Collector tool	7.14	7.14

System requirements

June 17, 2019

This article lists the supported systems and prerequisites for the AppDNA server and client. Read the Prepare to install article before installing AppDNA.

Quick links to topic sections:

- Hardware requirements
- Supported operating systems
- AppDNA server requirements
- AppDNA client requirements
- Citrix License Server requirement
- Report requirements
- Requirements for optional features

Hardware requirements

For a complete installation (server and client)

For small proof-of-concept deployments: A Windows laptop with at least 4 GB of RAM is usually sufficient.

For production deployments

- Server-class physical or virtual machine with at least 12 GB of RAM

Additional memory might be required for the Interoperability solution if you choose to analyze a large number of applications. The amount of additional memory is dependent on the number of applications and size of the application DNA. In testing, a portfolio of 2,500 applications required 12GB RAM for optimum performance during interoperability analysis.

- To support up to 200 applications:
  - Dual core 2Ghz processor
  - One hard drive with at least 80GB free disk space
- To support over 200 applications:
  - 2 x dual core 2Ghz processor
  - 150GB+ free disk space
  - The database (.mdf file) should be installed on a separate high performance (10K/15K) physical hard disk from the operating system and when possible the database log file (.ldf) should be moved to a separate physical hard disk.

For a client only installation

- Pentium 4 or better processor
- At least 2GB memory with 1GB free memory (running under typical conditions)
  - If using VMware Workstation for Install Capture: At least 3GB memory with 2GB free memory
- At least 5GB free disk space
  - For Install Capture: Up to at least 80GB free on one hard drive

Screen resolution

A screen resolution of 1024 x 768 or higher is recommended. At a screen resolution lower than 1024 x 768, you may not be able to see some controls (for example, Import Applications > Import).

Supported operating systems

The AppDNA server and client are supported on the following OS platforms (64-bit only):

- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2

The AppDNA client is supported on the following desktop platforms (64-bit only):

- Microsoft Windows 10

AppDNA server requirements

> **Important**
>
> The AppDNA server must be installed on a dedicated machine.

Microsoft .NET Framework. The following versions are required:

- .NET Framework 4.5.1 or higher, up to and including .NET Framework 4.7.
- .NET 3.5 SP1 is required on any machine running client software that is attempting to import applications.

Microsoft SQL Server. The following versions are supported:

- SQL Server 2016
- SQL Server 2016 Express Edition (built-in 10GB database size limit)
- SQL Server 2014
- SQL Server 2014 Express Edition (built-in 10GB database size limit)
- SQL Server 2012 SP2
- SQL Server 2012 SP2 Express Edition (built-in 10GB database size limit)
- SQL Server 2008 R2 SP3

Microsoft Internet Information Services (IIS)

AppDNA supports the versions of IIS that are compatible with the version of Windows in use. By default, IIS is not enabled when Windows is installed.

The name of the machine on which you install the AppDNA server must conform to the IIS requirements for domain names: It must consist only of Latin characters a through z, A through Z, digits 0 through 9, or the hyphen character (-). The name must not start or end with a hyphen and must not contain an underscore (_) character.

AppDNA requires the following IIS and ASP .NET features.

Web Management Tools

- IIS Management Compatibility
  - IIS Metabase and IIS 7 Configuration Compatibility
- IIS Management Console
- IIS Management Scripts and Tools
- IIS Management Service
- IIS Application Initialization
- IIS IP Security
- IIS URL Authorization

- World Wide Web Services

World Wide Web Services

- Application Development Features
  - .NET Extensibility
  - ASP
  - ASP .NET (not Windows Server 2012)
  - ASP .NET 4.5.1 or higher, up to and including ASP .NET 4.7
  - ISAPI Extensions
  - ISAPI Filters
  - Server-Side Includes
- Common HTTP Features
  - Default Document
  - Directory Browsing
  - HTTP Errors
  - HTTP Redirection
  - Static Content
- Health and Diagnostics
  - HTTP Logging
  - Request Monitor
- Performance Features
  - Dynamic Content Compression
  - Static Content Compression
- Security
  - Basic Authentication
  - Request Filtering
  - Windows Authentication

Internet Explorer 11, 10, 9, 8, 7, 6 or Microsoft Edge (AppDNA 7.6.5 and later)

You can use Internet Explorer versions 6-10, but Microsoft supports (and Citrix recommends using) version 11.

To view reports and the Help system on the server machine, enable JavaScript and unencrypted forms.

> **Note**
>
> Internet Explorer Enhanced Security Configuration is enabled by default on the supported versions of Windows Server. Because Enhanced Security Configuration disables JavaScript, which

> is required to view reports and the Help system, you can either disable Enhanced Security Configuration on those systems or use the AppDNA client on a remote machine to view reports and Help.

AppDNA client requirements

Microsoft .NET Framework. The following versions are required.

- .NET Framework 4.5.1 or higher, up to and including .NET Framework 4.7.
- .NET 3.5 SP1 is required on any machine running client software that is attempting to import applications.

Internet Explorer 11, 10, 9, 8, 7, 6 or Microsoft Edge (AppDNA 7.6.5 and later)

You can use Internet Explorer versions 6-10, but Microsoft supports (and Citrix recommends using) version 11.

To view reports, enable JavaScript and unencrypted forms.

Citrix License Server requirement

For XenApp or XenDesktop Platinum licenses only: The minimum supported Citrix License Server version is 11.10.

Report requirements

- Report generation requires Microsoft Office.
- Reports exported as a Word document require Microsoft Word 2007 or higher for viewing.
- Reports exported as a PDF document require Adobe Reader for viewing.

Requirements for optional features

August 1, 2018

The following optional AppDNA features require additional software:

AppDNA web client

The AppDNA web client requires Internet Explorer 8 or later with JavaScript and unencrypted forms enabled in Internet Explorer.

You can use Internet Explorer versions 8-10, but Microsoft supports (and Citrix recommends using) version 11.

Install Capture

You use Install Capture to import desktop applications for which an MSI, SFT, or App-V file is not available. Install Capture installs the application within a virtual machine and creates an MSI file that is then imported into the AppDNA software. This requires the use of a virtual machine based on one of the following desktop virtualization technologies:

- Citrix XenServer 7, 6.5 SP1, 6.5, 6.2 or 6.1
- Microsoft Hyper-V Server 2016, 2012 R2
- VMware vSphere 6 update 2, 6 update 1 or 5.5

The capture process can create App-V sequences instead of (or as well as) MSI files for importing into the AppDNA software. This requires additional software, called the App-V Sequencer, which is not provided with the AppDNA software. For more information, see Install Capture.

Supported Install Capture platforms:

- Windows 10
- Windows 7 SP1
- Windows XP
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2008 R2

Organization reports

Use Organization reports to gain insight into applications managed through Microsoft Active Directory and System Center Configuration Manager, such as whether those applications are ready to be rolled out on a new platform. This supplementary feature requires access to Active Directory and Configuration Manager data.

Active Directory requirements

The AppDNA software can integrate data from Active Directory installed on the following Windows server versions:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2008 SP2
- Windows Server 2003

Data extraction from Active Directory requires a user account that:

- Belongs to the “Authenticated Users” group in the Active Directory domain or to a more privileged group
- Has at least these permissions:
  - List Contents
  - Read All Properties
  - Read Permissions

  For information about Active Directory administrative groups and accounts, see Securing Active Directory Administrative Groups and Accounts.

Configuration Manager requirements

The AppDNA software can integrate data from the following versions of Microsoft System Center Configuration Manager:

- System Center 2016 Configuration Manager
- System Center 2012 Configuration Manager R2
- System Center 2012 Configuration Manager SP1
- System Center 2012 Configuration Manager

The AppDNA connector to Configuration Manager uses the WMI interface, which uses port 135.

Data extraction from Configuration Manager requires a user account that:

- Is assigned a Configuration Manager security role that has the following permissions:
  - Application = Read
  - Collection = Read
  - Package = Read
  - Site = Read

  A Configuration Manager might add those permissions to the built-in Remote Tools Operator security role or create a copy of that role and assign the permissions.
- Has these WMI permissions: Enable Account, Remote Enable

For information about configuring these permissions, see Authorize WMI users and set permissions.

Patch Impact Analysis solution

In the Patch Impact Analysis solution, you can choose to manually import patches or to use Windows Server Update Services (WSUS).

To use WSUS in the Patch Impact Analysis solution, the WSUS SDK must be installed on the client.

Discover applications

The Discover feature requires connectivity to the Lakeside Software SysTrack database.

Get started

June 17, 2019

Current AppDNA users upgrading to this version of AppDNA

This group of Get started topics is for experienced AppDNA users upgrading to this latest version:

- Quick start guide
- What's new in AppDNA
- Add custom information to applications
- Prepare for a XenApp or XenDesktop 7.x upgrade
- Prepare for a move to XenApp or XenDesktop 7.x

New AppDNA users

This group of Get started topics is for new AppDNA users:

- Quick start guide
- Import, analyze, and report
- Prepare for a XenApp or XenDesktop 7.x upgrade
- Prepare for a move to XenApp or XenDesktop 7.x

Quick start guide

August 3, 2018

Citrix AppDNA application migration software enables enterprises to confidently discover, automate, model, and manage applications for faster application migration, easier application virtualization, and streamlined application management.

These quick start steps summarize first-time installation and upgrades.

Step 1. Deploy prerequisites

Before you install AppDNA, deploy the prerequisite components. The following items are required unless otherwise indicated.

- Microsoft SQL Server (32-bit, 64-bit, or Express)

  If you do not have an installation, you can download and install Microsoft SQL Server Express for free for a proof-of-concept or trial of AppDNA.

  Microsoft .NET Framework

- AppDNA requires these versions:
  - Download .NET Framework 4.5.1
  - Download .NET Framework 3.5 SP1
- IIS (required on the AppDNA server only)

  For more information about IIS requirements and installation, refer to System requirements or Installing IIS 8.5 on Windows Server 2012 R2.
- XenServer, Hyper-V, VMware Workstation, or VMware vSphere (required only for Install Capture)

Step 2. Download and install AppDNA

Download the installer, Citrix AppDNA.msi, and run it in a VM.

The installer handles first time and upgrade installations for all licensing types. For trial licenses, the installer creates a database that will work with Microsoft SQL Server Express.

Step 3 - Configure AppDNA

After the installation completes, the Configure AppDNA Environment wizard starts.

1. When prompted to enter database details, specify the SQL Server name, database name, and the administrator user name and password.
2. When choosing how to configure a service account, the appropriate option for most cases is Use the built-in IIS application pool identity.
3. When prompted for license information: If you already have a copy of AppDNA, your license will continue to work for this release.
4. After the Configure AppDNA Environment wizard finishes successfully, open the Windows Start screen or menu, choose AppDNA, and then log on.

   The default administrator account user name is “administrator” and the default password is “apps3cur3”.
5. If you are using a trial license, make sure that the OS images finish loading before you continue.

   When the import completes, AppDNA displays the results.

   You have now completed the installation.
6. To start importing a few applications:
   a) From the AppDNA side bar, choose Import & Analyze and then click Applications.
   b) After you import one or more applications, click Analyze, then view the resulting reports.

      The run time for the import and analyze steps will vary from a few minutes up to a few hours depending on how many applications you choose and the speed of your computer.

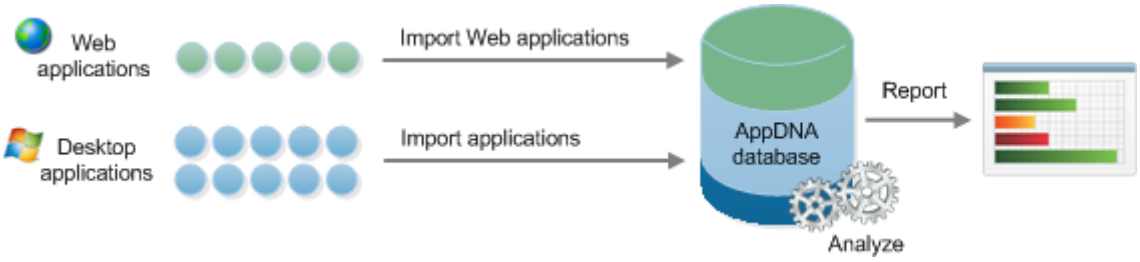
Import, analyze, and report

May 8, 2019

AppDNA performs automated analysis of the compatibility of applications with a variety of platforms. Each supported platform is represented by a separate report that contains a set of algorithms that validate the suitability and performance of applications in a specific target environment.

AppDNA process overview

The AppDNA approach is simple: Import - analyze - report.



Import - Applications are the raw material for AppDNA - so before you begin, you need to import them. When you do this, AppDNA interrogates each application's files, registry entries, and API usage to expose the application's "DNA". AppDNA then loads this into a SQL Server database. You can import desktop and Web applications of any type - whether internally developed or supplied by an independent software vendor (ISV).

Learn more: Import applications

Analyze - When you start the analysis process, you select the reports that correspond to the platforms against which you want to test your applications. AppDNA combines all of the information it has about the application portfolio and runs the report algorithms against the application DNA and produces and stores the reporting data.

Learn more: Analyze applications

Report - After the import and analysis processes have completed, you can view the reporting results. AppDNA presents the results of the analysis in a set of report views that provide the information that you need to plan, fix, and test your application portfolio. AppDNA provides the same set of report views for each report, including the following:

- The EstateView provides a consolidated overview of the state of the entire application portfolio for the target technology. This view does not provide any application-specific information and is particularly useful when you are evaluating AppDNA, because it does not rely on individual application licensing. The Effort Calculator is based on the EstateView and is also useful when you are evaluating AppDNA. You can use it to estimate the time, cost, and effort associated with migrating a portfolio of applications to a new platform.
- The Application Issues and Application Actions views provide high-level management overviews about the state of individual applications.
- The Remediation Issues and Remediation Actions views provide detailed information for the remediation team about how to fix individual applications.

Learn more: Report views

Add custom information to applications

August 1, 2018

You can record information about applications that is specific to your organization in AppDNA application attributes. An application attribute can contain information such as asset ID, cost center, application status, or owner.

The following attributes are already created:

- **AppID.** An AppID is a unique identifier for an application such as an asset ID. AppID is configured to appear on all reports.

  AppIDs, tracked by many organizations, might be an asset tag number or other tracking number held in a corporate purchasing system or other application. You are responsible for obtaining AppIDs from your corporate system: You can handle that manually, through scripts that you write, or by working with Citrix Consulting to integrate AppDNA with your corporate system. If you do not assign a value to AppIDs, AppDNA assigns them, starting at 1, based on the order in which the applications are imported into AppDNA.

- **Analyzed Date.** The date that an application was analyzed is configured to appear on remediation reports.

To add custom information to applications you:

- **Create an unlimited number of application attributes.** For example, to track application status you might create an attribute named App Status and define a list of values for it: Imported, Analyzed, In test, Failed test, Passed Test, In Production.

  When creating an attribute, use the AppDNA management console to:

  - Choose from a variety of data types: Text field, number, list, yes/no choice, date, or RAG indicator.
  - Define how an attribute is to be reported. You specify whether the attribute will have different or the same values for each report; you choose which reports are to include the attribute.
    Note: Depending on your screen resolution, you might be able to show a limited number of application attributes on the Overview and Assessment reports.

- **Set the value of application attributes.** If you track application information in other IT systems, you can set attribute values by importing a CSV file or by using the AppDNA SDK . You can also set values by directly editing them in the AppDNA management console.

- **View application attribute information.** The reports that include application attributes will contain a column for each attribute.

To create an application attribute

You must use the AppDNA management console to create application attributes.

Note: Users with the administrator role can manage (add, delete, edit) application attribute definitions. All users can change attribute values.

1. From the AppDNA menus, choose Configure > Attributes.

   The Application attributes screen appears.

2. Click New.

3. In the Attribute definition page:

   a) Specify a Name for the attribute.

      This is the label that will identify the attribute on reports.

   b) Specify whether the attribute value will differ per report or should be reported globally.

      Your selection determines which reports can include the attribute. If you select the Per-report attribute check box, the attribute cannot appear on the Application List screen or the Overview Summary report, which include only the data that applies globally to the application.

      - To report different values for an attribute on the various reports, select the Per-report attribute check box.

      For example, suppose that you are creating an attribute, Tested, to indicate whether the application is tested. If the value for Tested might differ for the various operating systems, select the check box.

      - To report the same value for an attribute on the various reports, leave the Per-report attribute check box cleared.

      For example, suppose that you are creating an attribute for cost center. In your organization, the same cost center applies for a particular application, regardless of the operating system. In this case, you would not select the check box.

      After you create an attribute, you cannot change its Per-report attribute setting.

   c) Choose a Data type from the list.

      The data type restricts the attribute value to a particular input format.

      If you choose
      List, the Select or create list page appears.

      - To use a list that is already defined, select Use existing list and then choose the list name from the menu.

- To create a list, select Create new list, specify a New list name, and then type the list items in the Current items in list box.

  To reorder a list or change its members, see To edit a list, later in this section.

After you create an attribute, you cannot change its Data type setting.

d) Click Next.

4. In the Display options page, specify where you want the attribute to appear.

   - **Screen: Application List.** Attributes with the same values for all reports, including AppID, appear on the Application List screen by default (unless Per-report attribute is selected).
   - **Report: Overview Summary.** Attributes, including AppID, appear on the Overview Summary report by default (unless Per-report attribute is selected).
   - **Reports: Application Issues and Application Actions.** To include the attribute on these reports, select the check box.
   - **Reports: Remediation Issues and Remediation Actions.** Attributes, including AppID, appear on these application reports by default, regardless of the Per-report attribute option selected.

   Consider the space requirements of additional columns when determining which attributes to show in a report.

5. Click Finish.

   The attribute appears in the selected locations.

6. After you complete the changes, click Save.

To import attribute values

Note: Users with the administrator role can import application attribute values.

To set the value of application attributes for multiple applications at a time, you can import the values from a comma-separated values (.csv) file or the AppDNA SDK .

If you import applications from a file, as described in Import from List, you can import the attributes at the same time or subsequently. Before you import attribute values, you must create the application attributes. Creating an attribute automatically adds it to the template import file.

Be sure to re-import your template import file after adding, editing, or deleting attributes.

If you use other methods from the AppDNA management console to import applications, you can import the attributes after the applications are available in AppDNA.

To change attribute values

Note: Users with the administrator or user role can view or change application attribute values.

1. When viewing the Application List screen:
   a) In the Application List screen, select the check box for the applications you want to change and then click Properties.
   The properties page appears.
   b) To set the value of an attribute, select the check box for the attribute, enter its value, and then click OK.
2. When viewing an Application Remediation report:
   a) In the Application Remediation report screen, click Properties.
   The properties page appears.
   b) To set the value of an attribute, select the check box for the attribute, enter its value, and then click OK.

To rename or delete an application attribute

Note: Users with the administrator role can rename and delete application attributes.

1. From the AppDNA menus, choose Manage > Application Attributes.

   The Application Attributes Settings appear.

2. Select the attribute and then click Edit or Delete.
3. After you complete the changes, click Save.

Application attributes forms

Group application attributes into logical containers (forms) which are then available in the properties of an application.

To create a new application attribute form, select **Configure** > **Application Attributes Forms**.

For more information, see Application attributes forms.

Prepare for a XenApp or XenDesktop 7.x upgrade

August 7, 2018

When planning how to deliver desktops and applications after an upgrade to XenApp or XenDesktop 7.x, use the XenApp and XenDesktop 7.x Upgrade solution to get the information you need. The solution provides information such as:

- The delivery method available for your applications, either server hosted or desktop hosted.

  Server hosted refers to applications and desktops that reside on a Server OS machine, either physical or virtual. These deployments provide users access to applications from StoreFront, their Start menu, or a URL you provide to them. Applications are delivered virtually and display seamlessly in high definition on user devices.

  Desktop hosted refers to applications and desktops that reside on a virtual Desktop OS machine. These deployments support applications that run on older operating systems and architectures, while providing users with applications that display seamlessly in high-definition.

- The applications that require remediation to work with XenApp or XenDesktop 7.x in your target deployment.
- The applications that will not work with XenApp or XenDesktop 7.x in your target deployment.

Note: For information about upgrading to XenApp or XenDesktop 7.x, refer to the Upgrade topics in the XenApp and XenDesktop 7.x documentation in eDocs.

To configure a XenApp and XenDesktop 7.x Upgrade solution

Before you start, gather the following information.

- For your current XenApp or XenDesktop deployment:
  - The version of XenApp or XenDesktop that you are upgrading
  - The operating system family on which it is installed
  - Whether App-V is used
- The applications you want to deliver
- For your target XenApp or XenDesktop deployment:
  - Whether it will use App-V
    XenDesktop 7.x supports App-V as the preferred technology to stream applications to user devices. It does not support XenApp application streaming.
  - The desktop operating systems to use (if delivering virtual desktops)
    AppDNA provides a default image for the Windows desktop operating systems. You can import custom images, as described in Operating system images.

1. In the AppDNA side bar, click Solutions and then click Add solution.
2. In the Solutions Templates page, select XenApp and XenDesktop 7.x Upgrade and then click Next.

The solution wizard opens.

3. Identify the solution: In the Solution name page, type a Solution name and Description, to be used in the solution report.
4. Specify your current environment:
   a) In the Platform name page, type a Platform name to identify the platform of your current XenDesktop deployment.

      Including the main characteristics of your platform in the name, such as “Windows 2008 64-bit”, will help you distinguish this platform later in the list of available platforms.

   b) Provide an optional Description of the platform.
   c) Choose your platform parameters.
5. Choose applications: In the Applications page, select the applications you want to include in the upgrade.
6. To review or edit the target platform, click XenDesktop 7.x Upgrade target and then click Edit.

   Important: The default target, Windows Server 2012, 64-bit, is the recommended best practice. Other than changing the App-V selection, we recommend that you not change the other target settings unless necessary.

   On the Desktop deployment page, change the settings as needed:

   - By default, if AppDNA detects major issues with server OS hosting, it uses desktop OS hosting for the operating systems that are selected. To prevent any desktop hosting, clear the Host applications on desktop check box.
   - To remove a particular desktop operating system from the analysis, clear the check box for it.
   - To choose a different image for a desktop operating system, choose it from the menu.

     The menu lists the default image provided with AppDNA and any custom operating system images that you import, as described in Operating system images.
7. To complete the solution:
   a) After you finish defining the current and target platforms, click Build.
   b) On the Progress page, click Analyze. When the analysis completes, choose report to view and then click Finish.

   To view the reports at any time: In the AppDNA side bar, click Solutions and then click the name of the solution.

To interpret a XenDesktop Upgrade Report

A XenDesktop Upgrade Report lists the applications you selected, sorted under the following categories:

- **Applications that can run.** No action is required for these applications to run in a XenApp or XenDesktop 7.x environment on the target platform. The deployment method for these applications is server hosted.
- **Applications that require remediation to run.** These applications can run in a XenApp or XenDesktop 7.x environment on your chosen target platform if you perform remediation. Click the Remediation link in the report for details.
- **Applications that must be deployed using desktop hosting (pooled or dedicated).** These applications can run in a XenApp or XenDesktop 7.x environment on your chosen target platform if you deploy them using pooled or dedicated desktops.
- **Applications that cannot be deployed with XenDesktop 7.x.** These applications cannot be deployed using Server OS or Desktop OS machines without redevelopment. Click the Reason link for details.

For more information about Server OS and Desktop OS machines, refer to Plan for hosting desktops and applications in the XenApp and XenDesktop 7.x documentation in eDocs.

To add an existing platform to a solution

1. In the AppDNA side bar, click Solutions.
2. In the Solutions pane, click the solution category and then click Edit across from the solution name.
3. Click the icon above Existing platforms and then complete the wizard.

   The report reflects the platform you just added.

To build a report for a different platform

1. In the AppDNA side bar, click Solutions.
2. In the Solutions pane, click the solution category and then click Edit across from the solution name.
3. Click Next, click a platform, and then click Build.

Prepare for a move to XenApp or XenDesktop 7.x

August 7, 2018

When planning how to deliver desktops and applications after moving to a XenApp or XenDesktop environment from other systems, use the XenApp and XenDesktop 7.x Adoption solution to get the information you need. The solution provides information such as:

- The delivery method available for your applications, either server hosted or desktop hosted.

  Server hosted refers to applications and desktops that reside on a Server OS machine, either physical or virtual. These deployments provide users access to applications from StoreFront, their Start menu, or a URL you provide to them. Applications are delivered virtually and display seamlessly in high definition on user devices.

  Desktop hosted refers to applications and desktops that reside on a virtual Desktop OS machine. These deployments support applications that run on older operating systems and architectures, while providing users with applications that display seamlessly in high-definition.

- The applications that require remediation to work with XenApp or XenDesktop 7.x in your target deployment.
- The applications that will not work with XenApp or XenDesktop 7.x in your target deployment.

To configure a XenApp and XenDesktop 7.x Adoption solution

Before you start, gather the following information.

- For your current environment:
  - The operating system family
  - Whether App-V is used
- The applications you want to deliver
- For your target XenApp or XenDesktop deployment:
  - Whether it will use App-V
    XenApp and XenDesktop 7.x supports App-V as the preferred technology to stream applications to user devices. It does not support XenApp application streaming.
  - The desktop operating systems to use (if delivering virtual desktops)
    AppDNA provides a default image for the Windows desktop operating systems. You can import custom images, as described in Operating system images.

1. In the AppDNA side bar, click Solutions and then click Add solution.
2. In the Solutions Templates page, select XenApp and XenDesktop 7.x Adoption and then click Next.

The solution wizard opens.

3. Identify the solution: In the Solution name page, type a Solution name and Description, to be used in the solution report.
4. Specify your current environment:
   a) In the Platform name page, type a Platform name to identify the platform of your current environment.

      Including the main characteristics of your platform in the name, such as “Windows 8.1 32-bit”, will help you distinguish this platform later in the list of available platforms.

   b) Provide an optional Description of the platform.
   c) Choose your platform parameters.
5. Choose applications: In the Applications page, select the applications you want to deliver after moving to XenDesktop.

   Your existing platform appears in the Solutions platforms page.
6. To review or edit the target platform, click XenDesktop 7.x Adoption target and then click Edit.

   On the Desktop adoption page, change the settings as needed:

   - By default, if AppDNA detects major issues with server OS hosting, it uses desktop OS hosting for the operating systems that are selected. To prevent any desktop hosting, clear the Host applications on desktop check box.
   - To remove a particular desktop operating system from the analysis, clear the check box for it.
   - To choose a different image for a desktop operating system, choose it from the menu.

     The menu lists the default image provided with AppDNA and any custom operating system images that you import, as described in Operating system images.
7. To complete the solution:
   a) After you finish defining the current and target platforms, click Build.
   b) On the Progress page, click Analyze. When the analysis completes, choose report to view and then click Finish.

   To view the reports at any time: In the AppDNA side bar, click Solutions and then click the name of the solution.

To interpret a XenDesktop Adoption Report

A XenDesktop Adoption Report lists the applications you selected, sorted under the following categories:

- **Applications that can run.** No action is required for these applications to run in a XenApp or XenDesktop 7.x environment on the target platform. The deployment method for these applications is server hosted.
- **Applications that require remediation to run.** These applications can run in a XenApp or XenDesktop 7.x environment on your chosen target platform if you perform remediation. Click the Remediation link in the report for details.
- **Applications that must be deployed using desktop hosting (pooled or dedicated).** These applications can run in a XenApp or XenDesktop 7.x environment on your chosen target platform if you deploy them using pooled or dedicated desktops.
- **Applications that cannot be deployed with XenDesktop 7.x.** These applications cannot be deployed using Server OS or Desktop OS machines without redevelopment. Click the Reason link for details.

To add an existing platform to a solution

1. In the AppDNA side bar, click Solutions.
2. In the Solutions pane, click the solution category and then click Edit across from the solution name.
3. Click the plus icon above Existing platforms and then complete the wizard.

   The report reflects the platform you just added.

To build a report for a different platform

1. In the AppDNA side bar, click Solutions.
2. In the Solutions pane, click the solution category and then click Edit across from the solution name.
3. Click Next, click a platform, and then click Build.

Install

June 17, 2019

To create a new AppDNA environment:

1. Plan your server needs according to the type of deployment (proof-of-concept or production) and determine the SQL Server architecture needed for your data.
2. Prepare your environment for installation.

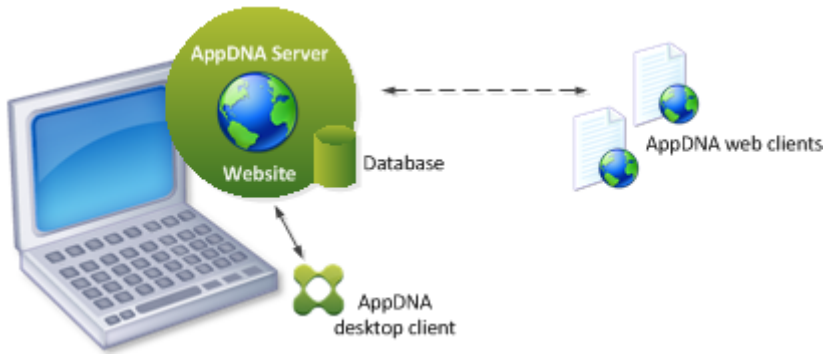
3. Install AppDNA and then configure the server installation and the client installations.
4. To ensure that AppDNA runs as efficiently as possible, optimize related components such as SQL Server and IIS.
5. Test the performance of your configuration.

Important: If you are upgrading AppDNA from a previous release, see Upgrade to AppDNA.

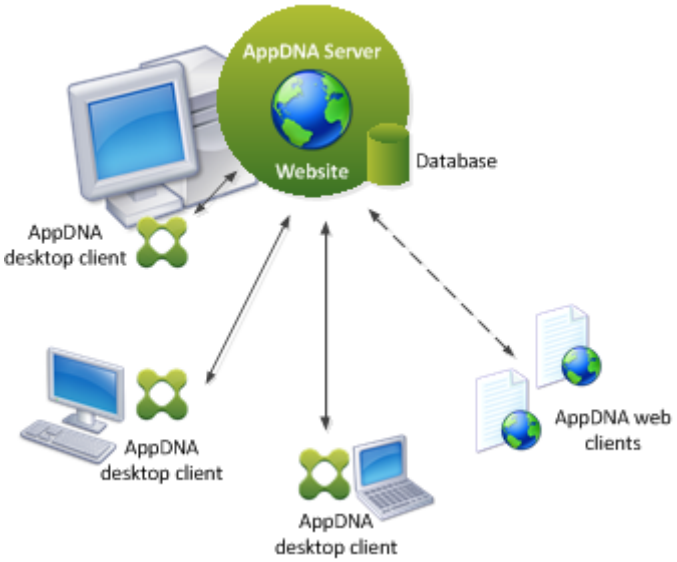
Plan

August 1, 2018

The AppDNA server, desktop client, and database install on the same machine. For a small proof-of-concept deployment, that is all you need.

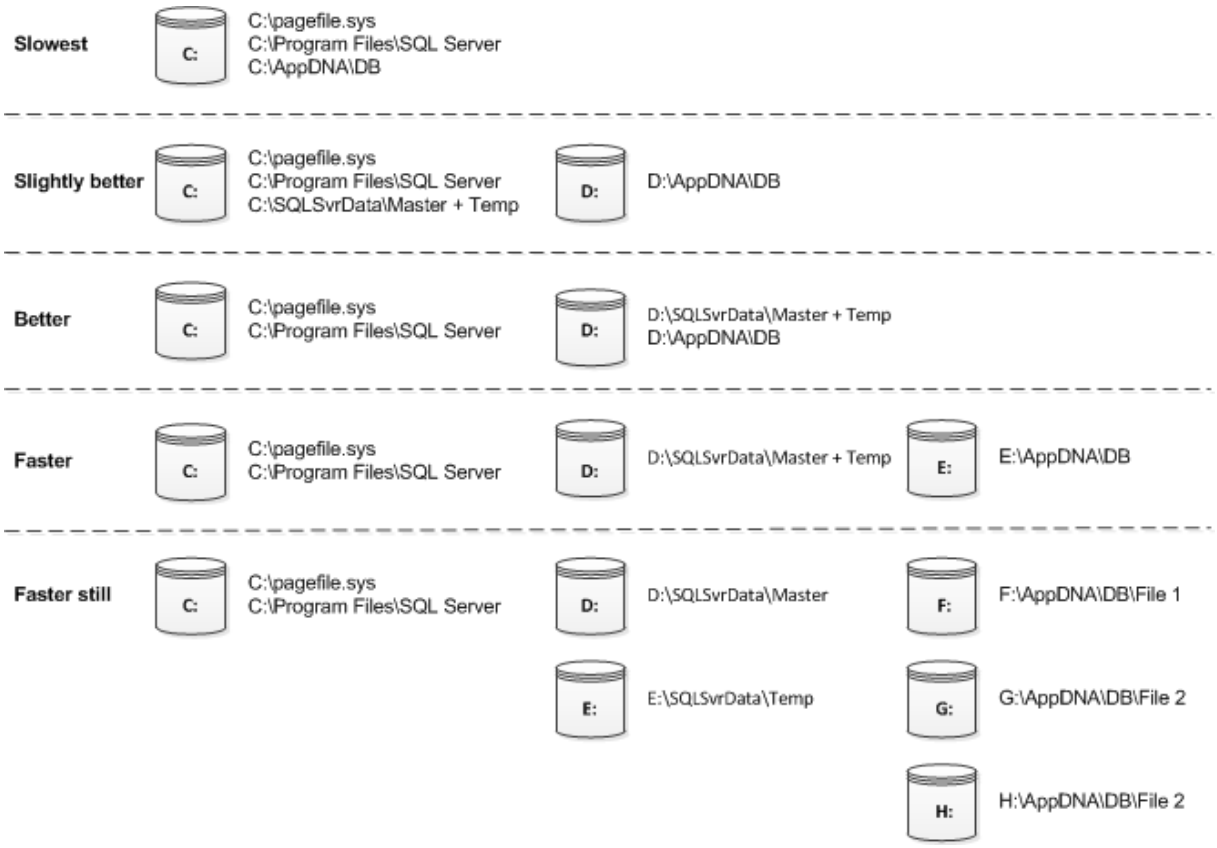


For a production deployment involving multiple users, you must also install the AppDNA desktop client on user desktops.



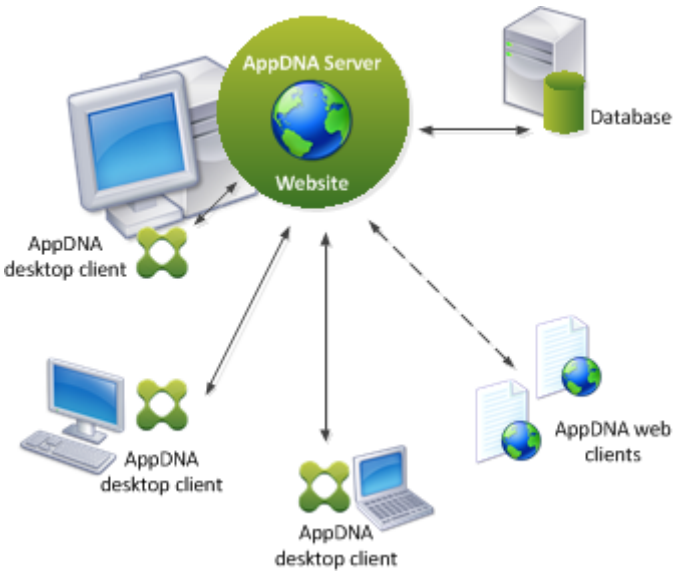
AppDNA database

AppDNA uses Microsoft SQL Server to store and manipulate the application and OS image DNA. As the size of the portfolio of applications grows, so do the demands on SQL Server. Consider the SQL Server architecture that will handle your data. The following diagram shows how various architectures for the SQL Server correspond to AppDNA performance.



For more information about optimizing SQL, refer to Optimize SQL Server.

You can optionally install the AppDNA database on a dedicated SQL Server machine instead of on the machine with the AppDNA server. If the SQL Server machine is outside of your local network, ensure that there is excellent connectivity between the machines so that the communication between them does not impact AppDNA performance.



AppDNA installation on a virtual machine

For non-evaluation versions only, you can install AppDNA on a virtual machine. However, if you plan to use Install Capture with VMware Workstation, be aware that VMware Workstation requires AppDNA to be installed on the virtual machine's host machine. This is not possible when AppDNA is itself installed on a virtual machine. If you must install AppDNA on a virtual machine, you can work around this limitation by using the AppDNA Self-Provisioning feature for Install Capture tasks.

If you plan to use Install Capture with a virtualization technology that provides full remote control (such as Citrix XenServer, VMware vSphere, and Microsoft Hyper-V), you can install AppDNA on a virtual machine.

Prepare to install

August 3, 2018

Before you install AppDNA, prepare your environment as follows.

Description

- Check Known issues for installation issues you might encounter.

Decide where you will install the components and then prepare the machines and operating systems.

- Review the deployment scenarios in [Technical overview].

- Review System requirements for supported operating systems versions for AppDNA and its components.
- Be sure that each operating system has the latest updates.

Prepare to install the AppDNA database:

- Verify that the SQL Server instance and database are configured for Latin1_General_CI_AS collation.
- Determine which user account you will use to install the AppDNA database. The account must have the sysadmin server role.
- Determine which user account the AppDNA web site will use to connect to the database. The account must have the bulkadmin server role and the db_owner database role.
  - For a production deployment, Citrix recommends that this is a generic service account with a password that never expires. Otherwise, you must update the AppDNA web site each time the password changes. For a proof-of-concept deployment, you can typically use the currently logged in user account.
  - If you use Windows authentication, this user account must have administrator privileges on the machine on which the AppDNA server is running. If that is not possible, relax the permissions on the AppDNA web site folder to give read-write permissions to the user account. By default, the AppDNA web site folder is C:\Program Files[(x86)]\Citrix\AppDNA\Server.
- Determine the location of the database files. The Configure AppDNA Environment wizard creates new databases in the default database file location set in SQL Server. To store the database files in a different location, change the default location in SQL Server before you run the wizard. For more information, refer to View or Change the Default Locations for Data and Log Files.
- Note: In some localized environments (for example, Chinese and Japanese), a new user cannot be created because the user name may contain special characters which are not recognized by the database.

Make sure that these ports are opened.

Port	Protocol	For connections to:
53	TCP/UDP	DNS
80/443	HTTP/HTTPS	AppDNA web site from the AppDNA server or clients
135	DCOM	Optional components (Active Directory, System Center Configuration Manager, a Hyper-V host, or virtual machines)
445	TCP/UDP	Network shares

Port	Protocol	For connections to:
1433, 1746, 1748, 1750	TCP	SQL server
7279, 27000	TCP	Citrix License server
8079	TCP	AppDNA licensing service; configurable
8199	HTTP	IIS; configurable
54593	TCP	Remote Admin agent; configurable

Tip: For complete port information, see CTX101810.

Verify that group policies meet these requirements:

- Group policies must not restrict Unencrypted Form Data or Active Scripting.
- Group policies must not restrict software installation or configuration of IIS.
- Enable the AppDNA web site URLs to be placed in Trusted Sites.
- For AppDNA clients only: Do not use an authenticating proxy for http(s) traffic between the client and the server URLs. You can use a proxy bypass/exception to meet this requirement.

Install AppDNA

August 1, 2018

The installer, Citrix AppDNA.msi, handles first time and upgrade installations for all licensing types. For trial licenses, the installer creates a database that will work with Microsoft SQL Server Express.

Important: If you are upgrading, do not uninstall AppDNA before installing. For more information about upgrading, refer to
Upgrade to AppDNA.

1. Start the AppDNA installer and follow the on-screen instructions.
2. On the Installation Type page, select one of the following options:
    - **Client only.** This installs the AppDNA client only. This is an installation of the AppDNA application, which connects to an AppDNA web site and database that are located on another machine (sometimes the database is on a different machine from the AppDNA web site). At the end of the installation, you will use the Configure AppDNA Environment wizard to configure the client connection to the AppDNA web site and database.

- **Complete (server + client).** This installs the AppDNA server and client on the same machine. At the end of the installation, you will use the Configure AppDNA Environment wizard to create or upgrade the SQL Server database and configure the AppDNA web site. The database can be installed and configured on the local machine or on a machine located on the network.

3. If you are prompted to install missing pre-requisites: Click Cancel to exit the installer, install the pre-requisites listed in System requirements, restart the AppDNA installer, and continue.
4. When the installation completes, the Installation Wizard Completed page opens.
   - To configure AppDNA now, click Finish. The Configure AppDNA Environment wizard starts.
   - To configure AppDNA later, clear the Launch the Configuration Wizard check box and then click Finish. You can launch the Configure AppDNA Environment wizard later from the Windows Start screen or menu (Programs > Citrix AppDNA > Management Tools > Configure AppDNA).

You must complete the steps in the Configure AppDNA Environment wizard before you can use AppDNA. The wizard varies according to the type of installation or upgrade:

If you are	See
Installing a complete installation	Configure a server installation
Installing or upgrading a client installation	Configure a client installation
Upgrading a complete or server installation	Upgrade a database

Install AppDNA on a virtual machine

For production deployments only, you can install AppDNA on a virtual machine. Trial mode installation is not supported on virtual machines.

If you plan to use Install Capture with VMware Workstation, be aware that VMware Workstation requires AppDNA to be installed on the virtual machine's host machine. This is not possible when AppDNA is itself installed on a virtual machine. If you must install AppDNA on a virtual machine, you can work around this limitation by using the AppDNA Self-Provisioning feature for Install Capture tasks.

If you plan to use Install Capture with a virtualization technology that provides full remote control (such as Citrix XenServer, VMware vSphere, and Microsoft Hyper-V), you can install AppDNA on a virtual machine.

Configure a client installation

August 1, 2018

Use the Configure AppDNA Environment wizard to configure an AppDNA client installation. By default, the wizard opens automatically when the AppDNA installation completes.

1. If the Configure AppDNA Environment wizard is not already open, from the Windows Start screen or menu, choose Programs > Citrix AppDNA > Management Tools > Configure AppDNA.
2. Enter the URL of the AppDNA web site. For example, http://server:8199/AppDNA, where server is the name of the AppDNA server machine, 8199 is the port number, and AppDNA is the name of the AppDNA web site.
3. Click Next to move to the System check page. See System Check issues if any of the checks fail.
4. Click Configure to start the configuration of the AppDNA client.

Configure a server installation

August 1, 2018

Use the Configure AppDNA Environment wizard to configure a new AppDNA installation for a trial or production system. This includes creating a new SQL Server database.

Important: If you already have an AppDNA installation, stop AppDNA clients before running the configuration wizard. That will reset IIS, which terminates import and analysis sessions on running AppDNA clients connected to a web server that hosts the AppDNA web site and database.

By default, the wizard opens automatically when the AppDNA installation completes.

1. If the Configure AppDNA Environment wizard is not open: From the Windows Start screen or menu choose Programs > Citrix AppDNA > Management Tools > Configure AppDNA.
2. Select Configure new installation, click Next and on the Database creation page specify the details as follows:
    - **Server name -** Enter this as Machine\Instance, where Machine is the name of the machine that hosts the SQL Server installation and Instance is the SQL Server instance if a named instance is in use. If a named instance is not in use, omit the backslash (\).
    - **Database name -** Defaults to AppDNADB. If the database administrator has created an empty database for you to use, enter its name here. Otherwise enter a name that does not already exist within the SQL Server instance.

- **Database authentication -** Enter the credentials for connecting to SQL Server when creating the database. The user account must have the sysadmin server role, regardless which authentication method you use.
  - **Windows authentication -** This type of authentication uses the logged on Windows user account when connecting to the database. The user account must have a password.
  - **SQL Server authentication -** This type of authentication uses a SQL Server user account. Selecting this option activates the User name and Password prompts. Enter the user name and password of the account.

3. Click Next and then, in the AppDNA web site credentials step, specify the credentials that the AppDNA web site is to use when connecting to the database after it is created. The options are:

   - **Use the built-in IIS application pool identity**
   - **Use these credentials -** Specify the credentials to be used. For a production system, Citrix recommends an AppDNA-specific service account that has a password that does not expire (not the account used to create the database).

   See Web site credentials for more information.

4. Click Next and then, in the License database step, activate your license or choose to run AppDNA in trial mode for up to 30 days:

   - **Run in trial mode** - Select this option to run AppDNA in trial mode for up to 30 days. This provides no limit to the number of applications that you can import and for which you can view the EstateView and Effort Calculator reports views. However, you can only view the results in the other report views for up to five applications.
   - **Activate a XenDesktop or XenApp Platinum license** - Select this option to activate AppDNA using a XenDesktop or XenApp Platinum license.
     - **Platinum license server machine** - Enter the host name or IP address of the machine on which the XenDesktop or XenApp License Server is installed.
     - **Port** - Enter the license server port. By default, this is 27000. However, sometimes a different port is used. If in doubt, contact your XenDesktop or XenApp administrator.

5. Click Next. In the **CEIP** step, Yes is selected by default.

   - Yes - opts in to the Citrix Customer Experience Improvement Program (CEIP), which gathers anonymous configuration and usage data from AppDNA and automatically sends the data to Citrix.
   - No - you can join later from **Edit** > **Settings** > **CEIP**.

6. Click Next and then, in the **Firewall** step, review the automatic exceptions to Windows Firewall. Uncheck if you do not want to add these exceptions.

7. Click Next to move to the System check step.

See System Check issues if any of the checks fail.

8. Click Configure to start the configuration of AppDNA and the creation of the database.

   This takes some time.

   The configuration wizard also performs an IIS reset. This will make any other web sites hosted by IIS on this server unavailable for a brief interval.

   After the process completes, a summary page opens.

You are now ready to start using AppDNA: From the Windows Start screen or menu, choose Programs > Citrix AppDNA > AppDNA. The default administrator account is:

- Username: administrator
- Password: apps3cur3

Important: Citrix recommends that you change the password the first time you log on.

The first time you log on, the Configure Modules Wizard starts.

Optimize AppDNA

August 3, 2018

This section explains steps that you can take to ensure that AppDNA runs as effectively as possible. Citrix recommends that you perform all of these optimizations for a production system, particularly if you have a large portfolio of applications.

Optimize SQL Server

To improve the performance of SQL Server, first increase the amount of RAM on the server. Additional RAM compensates for slow hard disks.

Maximum server memory and minimum memory per query

By default, SQL Server consumes available memory. This can have a negative impact on other processes running at the same time as the memory-intensive AppDNA import and analysis tasks.

Citrix recommends that you define an upper limit for the amount of memory SQL Server has access to, allowing around 3-5 GB of RAM for the operating system. SQL Server also has a defined amount of memory it allocates for queries. Citrix recommends that you increase this value to allow SQL Server to use more RAM for complex queries so that they run faster.

1. Open SQL Server Management Studio.
2. Right-click the SQL Server instance and choose Properties.
3. In the Server Properties dialog box, click Memory.
4. Set Maximum server memory (in MB) to an appropriate value for your environment.
5. Set Minimum memory per query (in KB) to 2048.

Maximum degree of parallelism

To reduce the likelihood of deadlocks on the database during analysis, set the maximum degree of parallelism to 1 on the SQL Server instance.

1. Open SQL Server Management Studio.
2. Right-click the SQL Server instance and choose Properties.
3. In the Server Properties dialog box, click Advanced.
4. On the Advanced page, set Max Degree of Parallelism to 1.

Windows swap file management

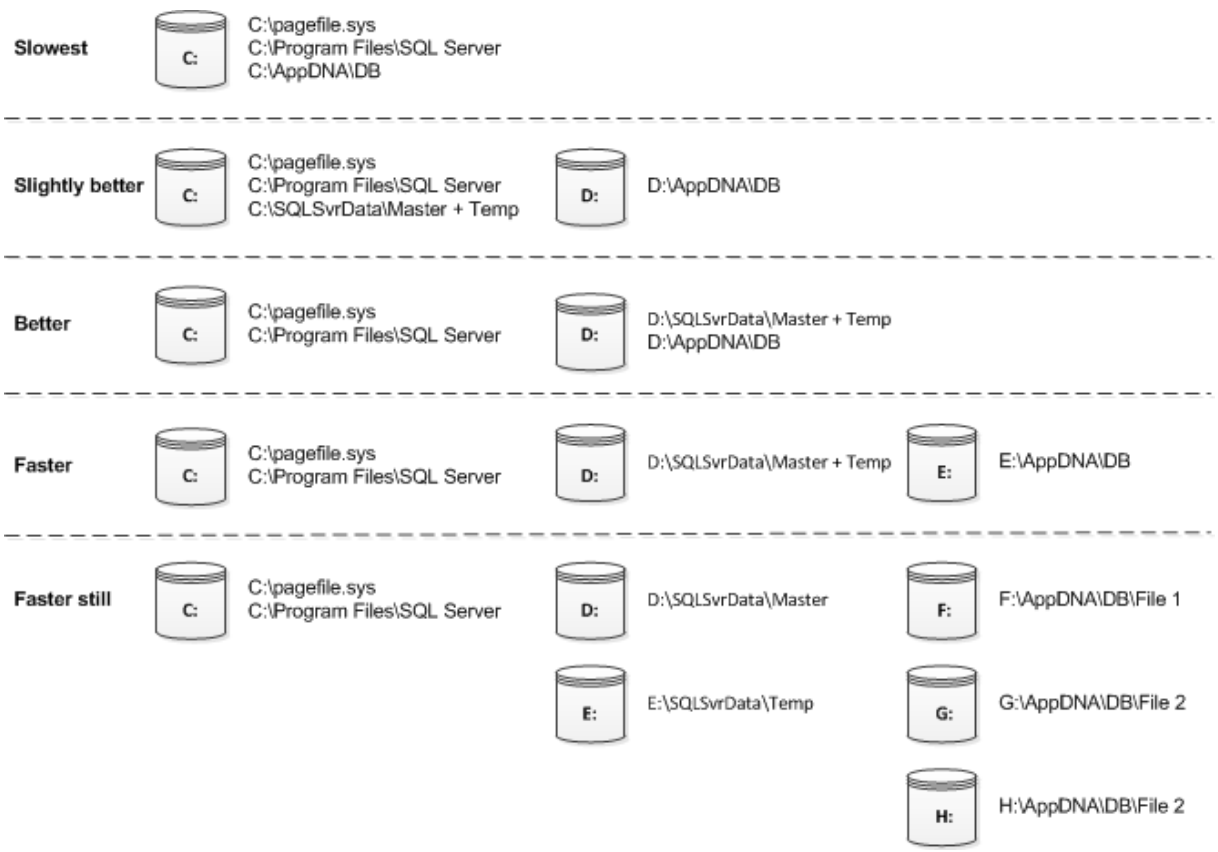
By default, Windows is configured to manage the paging file. Citrix recommends that you retain that default setting. Verify or change the setting as follows.

1. In Windows, go to View advanced system settings.
2. In the System Properties dialog box, click the Advanced tab.
3. Under Performance, click Settings.
4. In the Performance Options dialog box, click the Advanced tab.
5. Under Virtual Memory, click Change.
6. In the Virtual Memory dialog box, select the Automatically manage paging file size check box for all drives option or select System managed for each drive.

Hard disk optimizations

- Have as many files as possible in the file groups that make up the database.
- Put the collection of files on separate physical drives that are not system drives.
- Use smaller, faster hard disks in preference to larger, slow disks.
- If possible, move the master and temp database files to separate dedicated physical disks.
- Ensure there is at least 30GB available on the disk on which the tempdb database is located.

The following diagram shows how various architectures for the SQL Server correspond to AppDNA performance.



Essentially, the more disk heads over which SQL Server can split the work, the faster it performs.

Allowing SQL Server to use RAW partitions also optimizes the use of the available heads in the disk. However, doing this gives exclusive control of the disk to SQL Server and makes it unusable for normal usage in Windows and may lead to loss of any existing data on the drive.

AppDNA database recovery model

AppDNA performs a large number of SQL queries in its analysis of an application portfolio. With larger databases, this can consume a significant amount of hard disk space if all transactions are logged in a “full” recovery model because the SQL log file continues to grow until the database is backed up.

Important: To avoid disk space issues if you use a “full” recovery model, set up a SQL Server maintenance schedule to take regular backups of the AppDNA database.

Citrix recommends that you use the “simple” recovery model for the tempdb and AppDNA databases for a significantly reduced database size during processing and analysis.

1. Open SQL Server Management Studio.
2. Expand Databases > System Databases.
3. Right-click the database and choose Properties.
4. In the Properties dialog box, click Options.

5. From Recovery Model, choose Simple.

For more information, see Recovery Models (SQL Server).

Full-text indexing

AppDNA does not use the full-text indexing function of SQL Server. In some versions of SQL Server you can disable it on the AppDNA database to improve performance.

1. Open SQL Server Management Studio.
2. Right-click the AppDNA database and choose Properties.
3. In the Database Properties dialog box, click Files.
4. On the Files page, clear the Use full-text indexing check box.

Optimize IIS

Although the AppDNA installer and the Configure AppDNA Environment wizard attempt to optimize IIS, sometimes that is not possible or the settings are subsequently changed. Citrix recommends that you optimize IIS as described in this section.

Maximum allowed content length

A maximum allowed content length setting that is too low can prevent the import of larger applications and operating system images. To increase the limit:

1. Close AppDNA and all AppDNA clients.
2. Open Internet Information Services (IIS) Manager.
3. Expand the tree under IIS and click the AppDNA site.
4. In the center pane, double-click Request Filtering.
5. Under Actions, click Edit Feature Settings.
6. In the Edit Request Filtering Settings dialog box, set Maximum allowed content length to 2147483648 and then click OK.
7. Reset IIS: In the tree, click the AppDNA site and then click Restart.

IIS timeouts and recycle settings

By default, IIS is configured with time-out values that are generally too low for use with AppDNA. In particular, the Recycle settings can result in AppDNA tasks terminating before they complete because they have run for too long. This problem occurs particularly for larger application portfolios. To configure the settings:

1. Open Internet Information Services (IIS) Manager.
2. Expand the tree and click Application Pools.
3. In the Application Pools list, click AppDNAAppPool.
4. Under Actions, click Advanced Settings.
5. In the Advanced Settings dialog box, set the following options and then click OK.

Option	Setting
Managed Pipeline Mode	Classic
Idle Time-out (Minutes)	0
Ping Enabled	False
Regular Time Interval (Minutes)	0

6. With the AppDNAAppPool still selected, click Recycling under Actions.
7. Clear the Regular time intervals (in minutes) check box and then click Next and Finish.
8. Reset IIS: In the tree, click the AppDNA site and then click Restart.

Optimize anti-virus settings

On-access anti-virus scanning adversely affects the performance of AppDNA, SQL Server, and IIS. Citrix recommends that you exclude the following folders from on-access anti-virus scanning to ensure that AppDNA runs as efficiently as possible.

- AppDNA program and data folders
- Application installation package folders (if local)
- IIS Web site folders
- SQL Server database folders
- Temporary locations
- Windows\WoWx64

Optimize application imports

To import applications into AppDNA you use application installation packages. The many variables that affect import performance include application size, external files, network bandwidth, and physical network connectivity and capability.

To ensure that importing applications into AppDNA is carried out in the quickest and most efficient way, Citrix recommends that you store application installation files local to the AppDNA import client. Ideally they should be on a separate physical disk from the AppDNA and temporary databases.

Although you can import application installation files over the local area network, that can cause delays in the import process and might result in failed imports or import warnings.

Test performance

August 1, 2018

Citrix recommends that you test the performance of your configuration before you perform any large-scale imports and analysis.

Configure the Performance Monitor

1. Open the Windows Performance Monitor and then expand Data Collector Sets.
2. Right-click User Defined and then choose New > Data Collector Set.
3. Complete the Create New Data Collector Set wizard:
   - Enter a name such as AppDNA Performance.
   - Select Create from a template.
   - Select the template System Performance.

   The new data collector set name appears in the Performance Monitor window.
4. Right-click the new data collector set, choose Properties, click the Stop Condition tab, and clear the Overall Duration check box.

Test AppDNA import and analysis

1. From the AppDNA side bar, choose Import & Analyze > Applications.
2. In the Import Applications screen, add and select a few applications (up to five, including at least one large and complex application).
3. In the Windows Performance Monitor, right-click the AppDNA Performance data collector set and choose Start.
4. In the AppDNA Import Applications screen, click Import.
5. After the applications are imported, click Analyze if the analysis does not automatically start.
6. After the applications are analyzed, open the Windows Performance Monitor and stop the AppDNA Performance data collector set.

7. In Performance Monitor, review the AppDNA Performance report:
    - If Current Disk Queue Length Maximum is more than 2, consider moving the AppDNA database to a separate disk. For more information, see Optimize SQL Server.
    - If Processor Utilization is more than 70-80%, Citrix recommends that you upgrade the processor.

Install using the command line

August 3, 2018

You can optionally run the AppDNA installer from a command prompt. This article describes the syntax.

Syntax

The items enclosed in brackets ([ ]) are optional. When including these options, omit the brackets.

```
msiexec /i "package"/qn [INSTALLDIR="installdir"] [SERVER="serverdir"] [
SETUP="type"]
```

Note: Installing AppDNA from a command prompt requires administrative privileges.

Options

- package
  Required. The name and location of the MSI installer.
- /qn
  Signifies a silent installation.
- installdir
  Optional. The installation folder location, which defaults to Program Files\Citrix\AppDNA.
- serverdir
  Optional. The installation folder for the server components. Defaults to installdir\Server.
- type
  Optional. The installation type, either Complete (the default) or Client.

Examples

Perform a complete install silently using the default options:


```
msiexec /i "C:\Users\fishan\Downloads\Citrix AppDNA.msi"/qn
```

Perform a client install silently using the default options:

```
msiexec /i "C:\Users\fishan\Downloads\Citrix AppDNA.msi"/qn SETUP="Client"
```

Upgrade

June 17, 2019

> **Important**
>
> AppDNA includes all major OS images and loads them when you install or upgrade. As a result, it can take up to a few hours, particularly on less optimal hardware, to install AppDNA in a configuration with a remote SQL server or to upgrade AppDNA. An installation with the database on the same machine as the web server will be as fast as it was previously.

Prepare for an upgrade

From AppDNA 7.13, the AppDNA server and client are installed as 64-bit processes and are supported on 64-bit versions of Windows OS platforms. If the installer detects a 32-bit version of Windows, it does not proceed. This move to 64-bit does not affect AppDNA tools (Install Capture, Self Provisioning Client, Virtual Machine Configuration, Web Application Capture, Remote Admin, and Snapshot Manager). You can continue to install these tools on supported 32-bit or 64-bit OS platforms.

The following steps show you how to prepare for an upgrade if you are moving the AppDNA server from a 32-bit to a 64-bit machine.

1. Prepare the 64-bit machine that AppDNA will be migrated to.
2. From **Start** > **Configure AppDNA** > **Licensing**, export the license from the AppDNA 7.12 (or earlier version between 7.6.5 and 7.12) on the 32-bit machine. For steps on how to export the license token, see Transfer.
3. Back up the AppDNA database.
4. Restore the AppDNA database to the new SQL Server.
5. Install AppDNA 7.12 (or the version previously installed) on the new 64-bit machine.
6. From **Start** > **Configure AppDNA** > **Licensing**, import the license back into the database on the 64-bit machine. For steps on how to import the license token, see Transfer.
7. From **Start** > **Configure AppDNA** > **Reconfigure database**, select Add existing database to add the database to AppDNA.
8. Upgrade the new installation to the latest version of AppDNA (64-bit). For steps on upgrading, see the next section.

> **Note**
>
> An upgrade may consume 30 GB or more of SQL Transaction Log space. This can vary depending on the upgrade path and SQL server versions. Ensure that the disk configured to store the SQL log files has at least 50 GB of free space. In addition we recommend backing up and truncating the transaction log before and after the upgrade.
> Please allow 2-3 hours for the upgrade to complete.

Upgrade from AppDNA 7.6.5 and later

1. Run the installer as described in Install AppDNA.
2. Use the Configure AppDNA Environment wizard to upgrade each database as described in Upgrade a database.

   If you were already using a XenApp or XenDesktop Platinum license with AppDNA, the upgrade makes all AppDNA features available to you.

   Note: When you upgrade to AppDNA, a one-time manual license reactivation is required if your Subscription Advantage date has expired.
3. Upgrade the AppDNA tools as described in Upgrade AppDNA tools.
4. Upgrade any remote AppDNA clients: Run the installer as described in Install AppDNA.
5. If you have forward path scripts with references to the following operating systems or features, remove the references or delete the scripts: Windows XP, Windows Vista, Windows Server 2003 SP3, Windows Server 2008 SP2, and XenApp Streamed.

Those report modules are deprecated.

Upgrade from AppDNA 6.3 and earlier

You can also upgrade directly to AppDNA from AppTitude 5.1, AppDNA 6.0, AppDNA 6.1, AppDNA 6.1 SP1, AppDNA 6.2, and AppDNA 6.3. Do not uninstall the previous version before installing AppDNA 7.6. The installer will automatically delete any unnecessary old files while preserving your settings and configuration options.

Before you upgrade

Before you upgrade, review the following information.

- **System requirements**

  Make sure that your environment meets the System requirements.

- **Disk space requirements**

  In AppDNA 6.0 and later, the results of the analysis of the application DNA are stored in the database in a format optimized for report generation. When you upgrade from AppTitude 5.1, the size of your database will increase by approximately 15% so ensure that you have sufficient disk space available before you upgrade.

  Default OS images are installed in the database for all relevant versions of Windows. This requires significant additional disk space (2 - 3GB) if you are upgrading from AppDNA 6.0 or earlier and previously chose to install only a subset of the available OS images.

- **Families and suites**

  The upgrade to AppDNA 7.6 removes existing families and suites and flattens the application list to its original form. Please contact Citrix support before upgrading AppDNA if the removal of families and suites will cause issues

- **Time needed to upgrade**

  Upgrading a database from AppTitude 5.1 can take a long time, particularly if you have a large application portfolio. On a recommended software and hardware configuration, the upgrade time is expected to be approximately one hour per 500 applications if all reports are enabled. Upgrading from AppDNA 6.0 or later is not expected to take as long.

The results of an upgrade include the following.

- **External data handling when upgrading from AppDNA 6.1 SP1 (6.1.610)**

  AppDNA 6.1 SP1 (6.1.610) included a technical preview of the Windows 8 and Windows Server 2012 support. External data for those platforms was not included as part of the technical preview. An upgrade to AppDNA 7.6 does not apply the external data for Windows 8 and Windows Server 2012 to previously generated analysis results. You must re-analyze the applications to update the reports with the external data.

- **Installation location**

  By default, the AppDNA files are installed into Program Files\Citrix\AppDNA.

- **Web site name**

  If you upgrade from AppDNA 6.0 or earlier, the upgrade process renames the AppTitude web site to AppDNA, preserving the configuration files and moving them to the new location.

- **Licensing**

  The licensing system integrates with the Citrix licensing system. All new AppDNA licenses are issued through http://www.citrix.com. However, if you are upgrading from AppDNA 6.0 or earlier, valid old licenses are upgraded automatically to the new licensing scheme when you upgrade your database.

Important: If your AppDNA licensing service is located on a separate machine from the AppDNA Web server, you need to upgrade it
before you upgrade the AppDNA database. To do this, download Citrix AppDNA License Server.msi and run it on the machine that hosts the AppDNA licensing service.

To upgrade a single-machine or server installation

This procedure applies to upgrades from AppDNA 6.3 and earlier.

1. Upgrade the server on which you plan to install AppDNA if it does not meet the System requirements.
2. Run the installer as described in Install AppDNA.
3. Use the Configure AppDNA Environment wizard to upgrade each database as described in Upgrade a database.
4. Upgrade the AppDNA tools as described in Upgrade AppDNA tools.
5. If there are any remote AppDNA clients, upgrade each one as described next.

After the upgrade, we recommend that you re-analyze applications to take advantage of the data provided by new and improved algorithms.

To upgrade a client installation

This procedure applies to upgrades from AppDNA 6.3 and earlier.

1. Upgrade the client on which you plan to install AppDNA if it does not meet the System requirements.
2. Run the installer as described in Install AppDNA.
3. Configure the client to connect with the server as described in Configure a client installation.
4. Upgrade the AppDNA tools as described in Upgrade AppDNA tools.

After the upgrade, we recommend that you re-analyze applications to take advantage of the data provided by new and improved algorithms.

Upgrade a database

August 1, 2018

Note: If you have multiple databases, perform these configuration steps for each database.

1. Upgrade your database software if it does not meet the System requirements.

2. Stop AppDNA clients before running the configuration wizard.

   When necessary, an upgrade performs an IIS reset. An IIS reset terminates import and analysis sessions on running AppDNA clients connected to a web server that hosts both the AppDNA web site and database.

3. If the Configure AppDNA Environment wizard is not already open, from the Windows Start menu, choose Citrix AppDNA > Management Tools > Configure AppDNA.
4. Select Upgrade installation.
5. On the Choose Database page, select the database you want to upgrade, optionally select Backup, and then click Next.

   To validate the license, AppDNA checks both the expiration date of the Platinum license and the Subscription Advantage maintenance contract. If the Subscription Advantage date has expired, the AppDNA Configuration wizard contacts the Citrix License server originally used to activate AppDNA and refreshes the license.

6. Click Next to start the system check. If a system check fails, refer to System Check issues.
7. Click Upgrade to start the database upgrade. This takes some time.

Upgrade AppDNA tools

August 1, 2018

When you upgrade AppDNA, you also need to upgrade any tools that you use: Install Capture, Self-Provisioning, and Web Application Capture.

When you install AppDNA, the following installers are provided:

- Citrix AppDNA Self-Provisioning Client.msi
- Citrix AppDNA VM Configuration.msi
- Citrix AppDNA Web Application Capture.msi

By default they are installed to the following folder.

Platform	Location of installers
32-bit	C:\Program Files\Citrix\AppDNA\Tools
64-bit	C:\Program Files (x86)\Citrix\AppDNA\Tools

Install Capture

If you use Install Capture, create a new virtual machine snapshot that has the new version of the Citrix AppDNA VM Configuration MSI installed within it and update your virtual machine configurations accordingly. To do this:

1. Log on to the virtual machine.
2. Start the Windows Task Manager.
3. In the Windows Task Manager, click Remote Admin on the Applications tab, and then click End Task.
4. Uninstall the current version of the Citrix AppDNA VM Configuration tools using Control Panel > Programs and Features.
5. Install the new version of the Citrix AppDNA VM Configuration.msi.
6. Take a new snapshot of the virtual machine.
7. Run the Virtual Machine Configuration Wizard to update your virtual machine configuration to use the new snapshot.

For information about configuring the virtual machine for Install Capture, see Install Capture.

Self-Provisioning

If you use Self-Provisioning, install the new versions of the Citrix AppDNA Self-Provisioning Client and Citrix AppDNA VM Configuration MSIs on the Self-Provisioning client machine. Uninstall the previous version of the tools before installing the new ones. For more information, see Install the Self-Provisioning client.

Web Application Capture

If you use the stand-alone Web Application Capture tools, uninstall them and then install the new version of the Citrix AppDNA Web Application Capture MSI. For more information about these tools, see Installing the Stand-alone Web Capture Tools.

Import

June 17, 2019

AppDNA identifies an application as a web or desktop application by the way that it is imported into AppDNA. Applications that are imported through the Import Web Applications screen are considered to be web applications. All other applications are considered desktop applications.

Desktop applications

Import Windows desktop applications using their installation packages. These can be .msi or any other type of installation package. Alternatively, they can be App-V (.sft or .appv) packages. After you locate the application installation packages, go to the Import Applications screen to import them.

Import desktop applications using any of these methods:

- **Direct import.** Use to import applications for which you have a Windows Installer (.msi) or App-V (.sft or .appv) package. This is the quickest way to get the application DNA into the database.
- **Install Capture.** Use to import applications for which you do not have a Windows installer (.msi) or App-V (.sft or .appv) package. Install Capture uses a virtual machine to capture the details of the application's installation and configuration into an MSI which is then imported.
- **Self-Provisioning.** Use to manage Self-Provisioning, which provides an alternative mechanism for capturing desktop applications for import into AppDNA. The capture takes place on a separate machine from AppDNA. This can be any type of machine (virtual, physical, or VDI). Self-Provisioning can be used to delegate the responsibility for capturing and packaging applications to end users.

Managed applications. If you use Active Directory or Microsoft System Center Configuration Manager (Configuration Manager) to deploy applications, you can import applications using the deployed installations. First you load the Active Directory and Configuration Manager data into the AppDNA database. The Active Directory and Configuration Manager data includes organizational units, groups, collections, users, computers, and the installation operations for applications that have been deployed.

After the Active Directory and Configuration Manager data is in the AppDNA database, the Managed Applications screen lists all applications deployed through Active Directory and Configuration Manager. You can select the ones you want to import and AppDNA transfers them to the Import Applications screen where you can import them into AppDNA in the normal way.

When you work with Active Directory and Configuration Manager data in this way, AppDNA creates organization reports. These provide summaries of the status of the managed applications that have been deployed to users and computers in the groups and organizational units that are defined in Active Directory or Configuration Manager.

For more information, see Integrate data from Active Directory and Configuration Manager.

Discovery and rationalization. To find out which Windows applications are used across your enterprise, use the Discover Applications screen. This integrates with, and relies upon, Lakeside SysTrack, which audits and tracks actual application use within the enterprise. The Discover Applications screen pulls in the application auditing information from the SysTrack database and lists the applications that are in use across your organization. This can help you rationalize the applications and decide which you want to migrate to a new platform, for example. You can then import those applications

into AppDNA.

For more information, see Discover Applications.

Web applications

You can import web applications into AppDNA by using two different approaches or a combination of both.

1. Use the AppDNA directed spider to crawl over the run-time HTML pages and capture them for import into AppDNA.
2. Import the web application's source files.
3. Combine the output from the directed spider with the web application's source files.

Both approaches can be done from within AppDNA or by using the stand-alone AppDNA Web Application Capture tools.

For more information, see Import web applications.

Direct Import

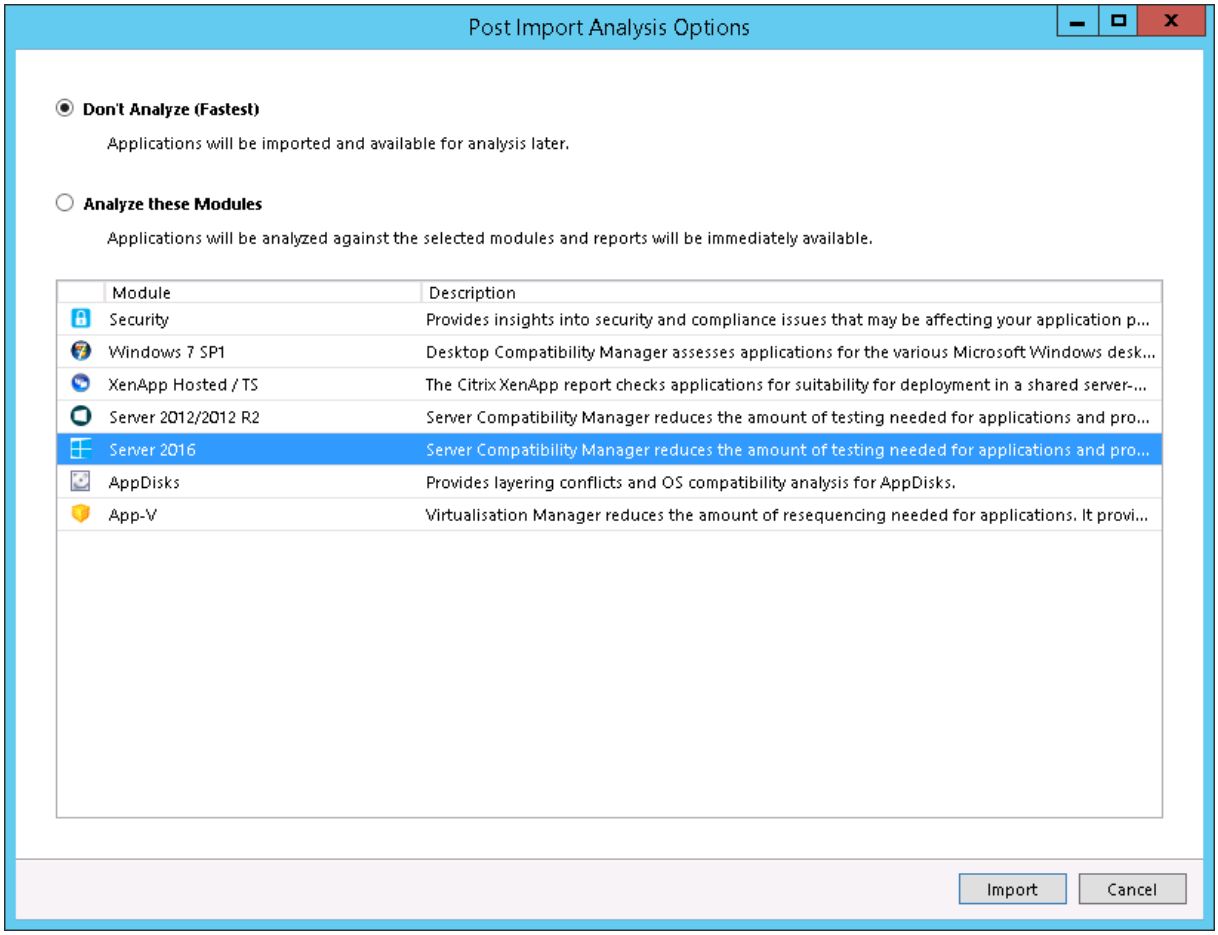
August 1, 2018

You can directly import desktop applications for which an .msi, .appv, or .sft file is available.

If you have both a standard Windows installer (.msi) file and an App-V (.sft or .appv) package file, it is better to import the .msi. This is because the App-V package is prepared for the virtual environment and therefore does not include all of the application DNA for a native Windows environment. For example, it might omit information about drivers and registry settings. Therefore Citrix recommends that you import the .msi file if one is available.

To import applications:

1. From the AppDNA side bar, choose **Import** > **Applications**.
2. Click the **Direct Import** tab.
3. Specify the .msi, .appv, or .sft files to import, click **Browse**, **Search**, or **Import from list**.
4. Select the applications to import.
5. Click **Import**.
6. In the dialog, select **Don't Analyze** > **Import**.



You can add new imports at the same time as other application imports are in progress. **Note**: The **Import** button is available when the cursor highlights any application import which is not in progress. If your selection includes multiple applications where some import processes are in progress and others complete, then the Import button is disabled until all processing has completed.

Track the progress of the import in:

- **Progress** column.
- **Log** icon to the right of the application progress message.
- **View Server Queue** link in the lower right-hand corner.

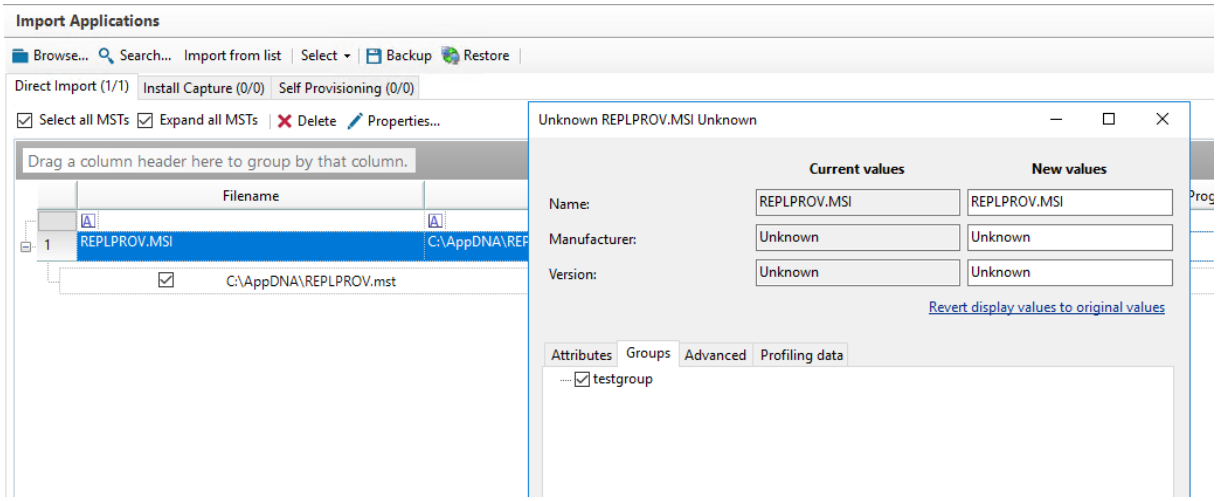
To cancel an import, click the **Cancel** button. If the import is canceled during client-side processing, the Canceled status displays once the MSI extraction is complete.

Apply MST files during import

You can use .mst files with .msi files to transform or manipulate the installation package.

If an .mst file is available in the same location as the .msi file, you can choose to apply it during the import. To apply for all applications for which an .mst file is available, select the Select All MSTs check

box.



Alternatively, you can select .mst files for specific applications. To select .mst files for specific applications, click the + to the left of the application and select the .mst file to apply.

Add applications to a group during import

1. In the Import Applications screen, select the applications to add to the group.
2. Open the application properties.
3. From the Groups tab, select one or more groups.

Alternatively, you can click in the Group column to select a group for an individual application.

Re-imported applications

When a desktop application is first imported into AppDNA, its fingerprint is stored. The fingerprint is a combination of the application product name, manufacturer name, version number, and the number of files and registry entries it has. If the application is imported into AppDNA again, by default the application is considered the same if the fingerprint is the same or has not changed by more than 10%. If you modify an application as part of the remediation process and then re-import it, it is considered the same application. Similarly, AppDNA considers new versions of an application to be the same application.

You can, however, change this behavior so that the application is always considered different even if there is no change in the fingerprint. To do this, select the Finger print override check box in Import and Analyze Settings. However, this action has licensing implications because AppDNA licensing controls the number of applications for which you can view reports.

If you re-import an application from the same location, AppDNA shows the text in the Path column in bold to indicate that the application was previously imported from the same location.

Install Capture

August 1, 2018

You can use Install Capture to import desktop applications for which an .msi, .sft, or .appv file is not available. Install Capture installs the application within a virtual machine and creates an .msi file that is then imported into AppDNA.

Generally the .msi that is created simply captures the application's DNA for import into AppDNA and is not suitable for actually installing the application. However, if you have the additional software requirements, the capture process can create App-V sequences or XenApp profiles as well as .msi files for importing into AppDNA.

Import applications by using Install Capture

1. From the AppDNA side bar, choose Import & Analyze > Applications.
2. Click the Install Capture tab.
3. On the Install Capture tab, select the .exe or other installation files that you want to import. Important: When selecting applications to import using Install Capture, you **must** use a UNC path. For example, \\MyServer\MyApplications\MyApplication.exe. The path you specify must be accessible from the virtual machine, otherwise the import will fail.
4. In the list of applications, select the applications that you want to import.
5. Select the VM configuration you want to use.
6. If applicable, choose a group for the applications.
7. Click Import on the right side of the toolbar to start capturing the application DNA for loading into the AppDNA database.

By default, AppDNA now runs through a series of checks of the virtual machine configuration. If any of the checks fail, refer to Troubleshoot.

If the checks are successful, AppDNA displays a progress bar and opens the virtual machine where the Install Capture processing takes place.

If you are using a vSphere or Hyper-V virtual machine, AppDNA opens the virtual machine in a Remote Desktop Connection window. If a warning window opens, select the Don't ask me again for connections to this computer check box, and then click Connect. If a Windows Security dialog box opens, enter the user name and password for the virtual machine. This should be a domain user account. Then select the Remember my credentials check box, and click OK.

For general information about the Install Capture processing, see "Install Capture processing," next.

Important: If the installation requires the computer to be restarted, make sure that you choose the I will restart my computer later (or equivalent) option. The Install Capture will fail if you restart the

virtual machine during the Install Capture process.

Install Capture processing

After you click Import on the Install Capture tab and the virtual machine configuration checks complete, the AppDNA Virtual Machine Remote Controls window opens.

- If you selected the Automatic check box, the before snapshot is automatically performed on the operating system.
- If you chose manual mode (that is, you cleared the Automatic check box), you need to select the actions to run manually and then click the Perform button. Select the actions in the order in which they are displayed in the drop-down list.

The processing that takes place is controlled by the execution profile. When the Snapshot execution profile is in use, the "before snapshot" is the first action that is run on the virtual machine. After the "before snapshot" has completed, the installation runs. If a manual installation is required, install and configure the application as required.

Important: If the installation requires the computer to be restarted, make sure that you choose the I will restart my computer later (or equivalent) option. The Install Capture will fail if you restart the virtual machine during the Install Capture process.

After the installation of the application finishes, the "after snapshot" begins (again assuming the Snapshot execution profile is in use). When this completes, AppDNA begins loading the MSI that was created. When the import finishes, the AppDNA Virtual Machine Remote Controls window closes and the progress on the Install Capture tab becomes "Loading Completed Successfully".

> **Note**
>
> In the Application List, the Manufacturer and Name and columns may display as Unknown (and the Version as 0.0.0) if AppDNA is unable to get this information from the application. This can cause an issue when reimporting apps with Install Capture. If the manufacturer, name and version were not captured, a different app of a similar size can overwrite the existing app. The workaround is to enable the Finger print override setting (**Edit** > **Settings** > **Import and Analyze**). This will force a new instance of the app to be imported. For more information on Finger print override, see Import and analyze settings.

Options

August 1, 2018

This topic documents the toolbar on the Install Capture tab in the Import Applications screen and the other options that you can apply to applications during the Install Capture process. You use Install Capture to import applications for which an .msi, .appv, or .sft file is not available.

Install Capture tab toolbar

The toolbar on the Install Capture tab in the Import Applications screen provides the following options:

Use Auto Click. Select this check box if you want to use auto-clicker in the capture of the selected applications. (This applies only if the selected execution profile supports auto-clicker.) Clear this check box if you do not want to use auto-clicker for the selected applications. See Auto-Clicker for more information.

Note: If the
Use Auto Click check box is disabled and you are wondering why, the answer depends on whether there are any applications in the list. When the list is empty, the check box is disabled if the default execution profile does not support auto-clicker or it does not contain the
UseAutoClick replaceable. Once there are some applications in the list, the check box is disabled for an individual application when the execution profile selected for that application does not support auto-clicker or it does not contain the
UseAutoClick replaceable. There's more on execution profiles below.

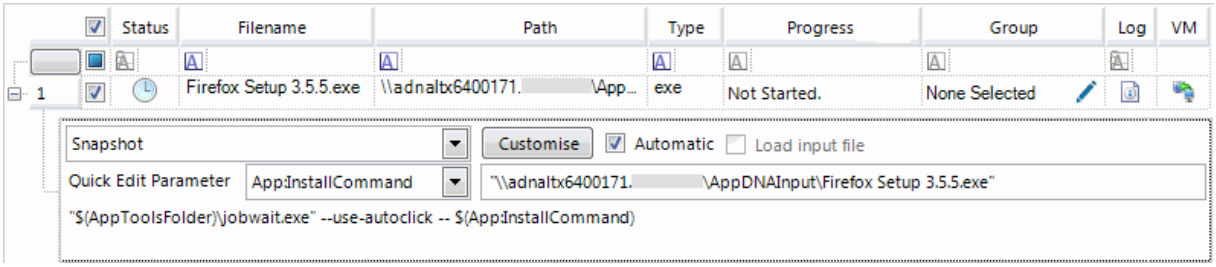
Extract embedded MSIs. Some non-MSI installers contain embedded .msi files. Select this button to extract them. AppDNA then lists the extracted .msi file(s) with the application.

VM Configuration (drop-down box). Select the virtual machine configuration to use. This drop-down box lists the virtual machine configurations that have been set up in Install Capture Settings.

Configuration. Click to open Install Capture Settings.

Per-application options

You can set the following options separately for each application on the Install Capture tab in the Import Applications screen. If the options are not visible, click the + to the left of the application name to open the application's options panel.



Execution profile (first drop-down box) – This controls the tasks and resources that are run on the virtual machine during the capture process. When you select an execution profile from the list, AppDNA creates a copy of it for the current application. This copy has an asterisk (*) appended to the name. This means that you can customize the execution profile for this application only (see Customize below). To revert the changes back to the default, select the corresponding base execution profile (without an asterisk) from this drop-down list. This creates a fresh copy of the execution profile for the current application.

When you first install AppDNA, the default execution profile is called Snapshot. This has three main steps as follows:

1. **Before snapshot**. Performs an analysis of the virtual machine's state, including its complete file system and registry entries.
2. **Launch command.** Runs the application's non-MSI installer.
3. **After snapshot.** Performs a second analysis of the virtual machine's state, including its complete file system and registry entries.

The difference between the state of the virtual machine in the before and after snapshots represents the changes made by installing the application. The capture process uses this information to generate an .msi file for importing into AppDNA and then resets the state of the virtual machine back to how it was before the installation.

Other execution profiles are available and you can set a different execution profile as the default. (For a list of the execution profiles that come with AppDNA and how to activate them, see Execution profiles.)

Customize. Click to open the Edit Execution Profile dialog box, where you can edit the execution profile specifically for the current application. For example, you can set replaceables (placeholders) and edit options. If you subsequently want to revert to the default settings, simply select the original execution profile (without the asterisk) in the drop-down list.

Automatic. By default this check box is selected and the capture process is automated and, provided it is successful, does not require user interaction other than for the selection of manual install options if necessary. Clear this check box if the application has pre-requisites that need to be installed. Install Capture then runs in manual mode and you can control each step.

Load input file. This check box controls whether an .msi file extracted from the non-MSI installer or the .msi created by Install Capture is imported. Select this check box to load an .msi extracted from the installer. However, it is generally safer to use the generated .msi, because some installers contain more than one .msi file but only one can be loaded into AppDNA.

Quick Edit Parameters. This consists of a drop-down list and a text box. The values in the drop-down list are replaceables (placeholders) used in the execution profile. AppDNA automatically provides values for these replaceables and you do not normally need to edit them. However, sometimes you may want to add a switch to the install command so that the installation runs silently, for example. Any

values entered for a replaceable in this box will override the corresponding value stored for that replaceable in the execution profile or virtual machine configuration.

The replaceables in the drop-down list depend on the execution profile, but typically include:

- App:InstallCommand. The command that launches the application installation. When the application is managed through Active Directory or ConfigMgr, the value in the text box is derived from Active Directory or ConfigMgr. Otherwise, AppDNA creates a command of the form msiexec /i “input_file” for .msi files and “input_file” for other installation file types. You can specify any other command line options that the installer accepts. For example, you might want to add a silent switch, and for .msi files, you might want to specify transforms or logging options.
- App:InstallDriveLetter. Only relevant when importing an application managed through Active Directory or ConfigMgr, this represents the mapped drive letter used to map the \\server\share portion of the installation directory to a drive letter.
- App:InstallWrkDir. Only relevant when importing an application managed through Active Directory or ConfigMgr, this represents the working directory used by the installation command.
- UseAutoClick. Set this to –use-autoclick if you want to run the capture with auto-clicker on. (This requires the execution profile to support auto-clicker.) Set this to an empty string if you want to turn auto-clicker off. See Auto-Clicker for more information. Any changes you make to this value will be lost if you change the execution profile in the drop-down box above.

Auto-Clicker

August 2, 2018

Overview

Auto-clicker is an optional feature of Install Capture and Forward Path task scripts that call the Install Capture process. Auto-clicker improves the automation of the Install Capture process by automatically clicking through the steps of a manual installation wherever possible, accepting the default options. This means that you can leave a batch of captures running unattended, even for installers that do not provide a silent switch option.

Sometimes auto-clicker is not able to click through all of the installation steps. For example, if the installer requires you to enter information, such as a license code. When this happens, auto-clicker waits for the information to be entered manually. If no-one enters the information (because, for example, it is part of a batch of captures left to run overnight), Install Capture waits for a configurable time-out period, and then abandons the capture and proceeds to the next capture (if there is one). The Install Capture tab in the Import Applications screen will show the import status as “failed”. You then need to run the capture again without the auto-clicker option.

Auto-clicker automatically takes a screen shot of each installation step that it clicks through and adds them to an HTML page that shows the time at which each one was captured. You can find this in the capture output location. This provides you with a record of the installation and of each option that was chosen.

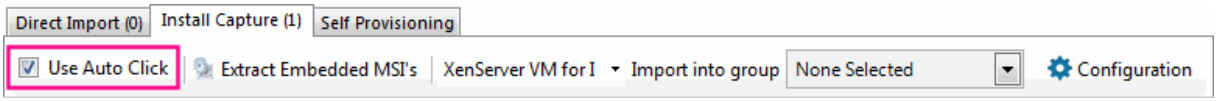
Note: Auto-clicker is off by default in Self-Provisioning, because Self-Provisioning is primarily aimed at expert users performing the installation manually. However, if required, the administrator can enable auto-clicker by enabling the UseAutoClick replaceable in the Quick Edit Parameter box as described below.

Limitations

- On Windows 7 (32-bit) as a VM, auto-clicker does not work for ManageEngine_NetFlowAnalyzer_9600.exe.
- On Windows 7 (32-bit) as a VM, auto-clicker does not work for soapUI-Pro-x32-4.5.1.exe or soapUI-Pro-x64-4.5.1.exe.
- On Windows 7 (32-bit) as a VM, auto-clicker does not work for aimp_3.10.1074.exe or wlsetup-web.exe.
- On Windows 7 (64-bit) as a VM, auto-clicker does not work for Atmn-Anywhere-Server-setup660.exe.

Enable auto-clicker

The steps that run during Install Capture are defined by execution profiles. For auto-clicker to work, execution profiles must support auto-clicker and have a replaceable called UseAutoClick. Provided this is true for the execution profile you are using, you can turn auto-clicker on and off for the currently selected applications in the Import Applications screen. Simply select the Use Auto Click check box on the toolbar on the Install Capture tab.



For information about configuring the replaceable, for example, to control auto-clicker in a Forward Path task script, see “Configuring the auto-clicker replaceable” below.

Important: If you have recently upgraded, be sure to also upgrade the AppDNA VM Configuration tools on the virtual machine, as explained in Upgrade AppDNA tools. Auto-clicker will not work with earlier versions of these tools.

Execution profile support for auto-clicker

The following table lists the execution profiles that come with AppDNA and indicates whether they support auto-clicker and are automatically updated when you upgrade AppDNA.

Execution profile	Supports auto-clicker
Snapshot	Yes
App-V 5.1 Sequencer	Yes
App-V 5.0 Sequencer	Yes

For instructions on importing and activating an execution profile, see “To activate an execution profile” in Execution profiles.

Note: If you have customized execution profiles, customized versions won’t be upgraded. The built-in versions of the execution profiles will be upgraded. You may want to consider refreshing your customized profiles.

Configure the time-out period

As mentioned earlier, sometimes auto-clicker cannot click through all of the installation steps. For example, because the installation requires you to enter information, such as a license code. When this happens, Install Capture waits for the information or option to be entered manually. If no-one enters the information, Install Capture waits for a configurable time-out period, and then abandons the capture and proceeds to the next capture (if there is one).

The time-out period is controlled by the “Abort Installation” Timeout option on the virtual machine configuration. By default, this time-out period is set to 40 minutes, because it also controls the time that Install Capture waits for the installation to finish and some large applications take a considerable amount of time to install. You can reduce this time-out period. However, be aware that this may cause the capture of some large applications to fail.

You change the “Abort Installation” Timeout value in the Virtual Machine Configuration Dialog Box.

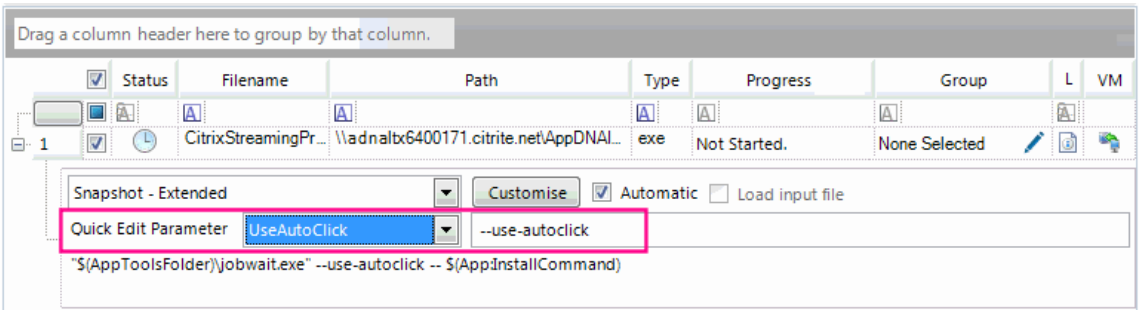
Configure the auto-clicker replaceable

The UseAutoClick execution profile replaceable controls whether auto-clicker is on by default for that execution profile:

- To turn auto-clicker on by default, set the UseAutoClick replaceable to a value of –use-autoclick.
- To turn auto-clicker off by default, set the UseAutoClick replaceable to an empty string (“”).

There are a number of places where you can set the replaceable, as follows:

1. In the Quick Edit Parameter box under the application on the Install Capture or Self-Provisioning tab in the Import Applications screen. For the selected application, this overrides all other options and changes the replaceable. (This is the only way to enable auto-clicker for Self-Provisioning.)



2. On the Replaceables tab in the Edit an execution profile.
3. On the Replaceables tab in the Virtual Machine Configuration Dialog Box.

If more than one of these apply, the highest in the list always take precedence. For example, if you have set the replaceable in the Quick Edit Parameter box, this always takes precedence.

Considerations when running an unattended batch

One of the advantages of auto-clicker is that it enables you to leave a batch of captures running unattended, for example, overnight. Be aware that any problem with the virtual machine configuration can cause the batch to fail. For example, if the virtual machine is identified by its IP address, the batch will fail if the IP address is allocated dynamically and it changes part way through the batch. Similarly the batch will fail if the virtual machine is not configured for automatic logon. Citrix therefore recommends that when you set up the virtual machine, you follow the best practice advice documented in Set up a virtual machine.

As explained in more detail in the “Limitations” section that follows, auto-clicker is not expected to be successful for every single application. You therefore need to check the status of every capture in the batch after it has finished. You can check the status on the Install Capture tab in the Import Applications screen or in the Forward Path Task Sequencing screen, depending on how you ran the batch. You can also view the screenshots that record the steps that auto-clicker clicked through. These are stored in the capture’s output directory. To view them in sequence with the time at which each one was taken, open output.htm in your browser.

Make a careful note of the captures that failed and if the failure was due to the limitations of auto-clicker, run them again manually (without the auto-clicker).

Note: To ensure that the screenshots are available if the capture fails, you need to choose the option

to copy rather than stream the results in the
Capture Output Location step when you create the virtual machine configuration.

Limitations

There are many different types of installers, which use a variety of different technologies. Citrix has tested auto-clicker with a wide range of installers. This section explains auto-clicker's known limitations.

- **Non-default options.** As mentioned earlier, auto-clicker accepts the installer's default options. If you want auto-clicker to select other options, you must provide an install command that specifies a silent switch and parameters that select the other options that you require.

  You can modify the default install command using the App:InstallCommand option in the Quick Edit Parameter box described earlier.

- **User input is required.** Some installers require you to enter something (such as a license code) or to explicitly select an option. When auto-clicker encounters a scenario of this type, it waits for someone to enter the information or perform the required interaction. If no-one does this within the specified time-out period, the capture will fail. You then need to run the capture again manually attending to any required user input.

- **Installer triggers a machine restart.** Some installers require the machine to be restarted after the installation has completed. These installers often provide an option to restart the machine automatically. When you are running the installation manually, you are advised not to use this option, because restarting the capture machine before the capture has completed will make the capture fail.

  Auto-clicker therefore attempts to ensure that it does not accept an option to restart the machine. Occasionally auto-clicker may fail in this and the restart attempt will commence. Remote Admin will then block the restart and Windows will display a message explaining this. Windows will then wait for the user to respond to the message. As the installation has finished, auto-clicker is unable to respond and unless someone intervenes, eventually the time-out period will be reached and the capture will fail. You then need to run the capture again manually and decline the option to restart the machine.

- **Language support.** In this release, auto-clicker has been tested with English language installers only and it is not expected to work with installers in other languages.

Self-Provisioning

August 1, 2018

Self-Provisioning provides an alternative mechanism for capturing desktop applications for import into AppDNA and for packaging applications for App-V or XenApp, for example. The capture and packaging take place on a separate machine from AppDNA. This is called the Self-Provisioning client machine and can be any type of machine (virtual, physical, or VDI).

Self-Provisioning allows the capture process to be driven by an application expert who does not have access to AppDNA itself. The AppDNA administrator prepares and publishes control information that enables the application expert to perform the installation at a convenient time independently of AppDNA.

Self-Provisioning can be used with all types of desktop application installation packages (MSI and non-MSI) and App-V (.sft and .appv) packages.

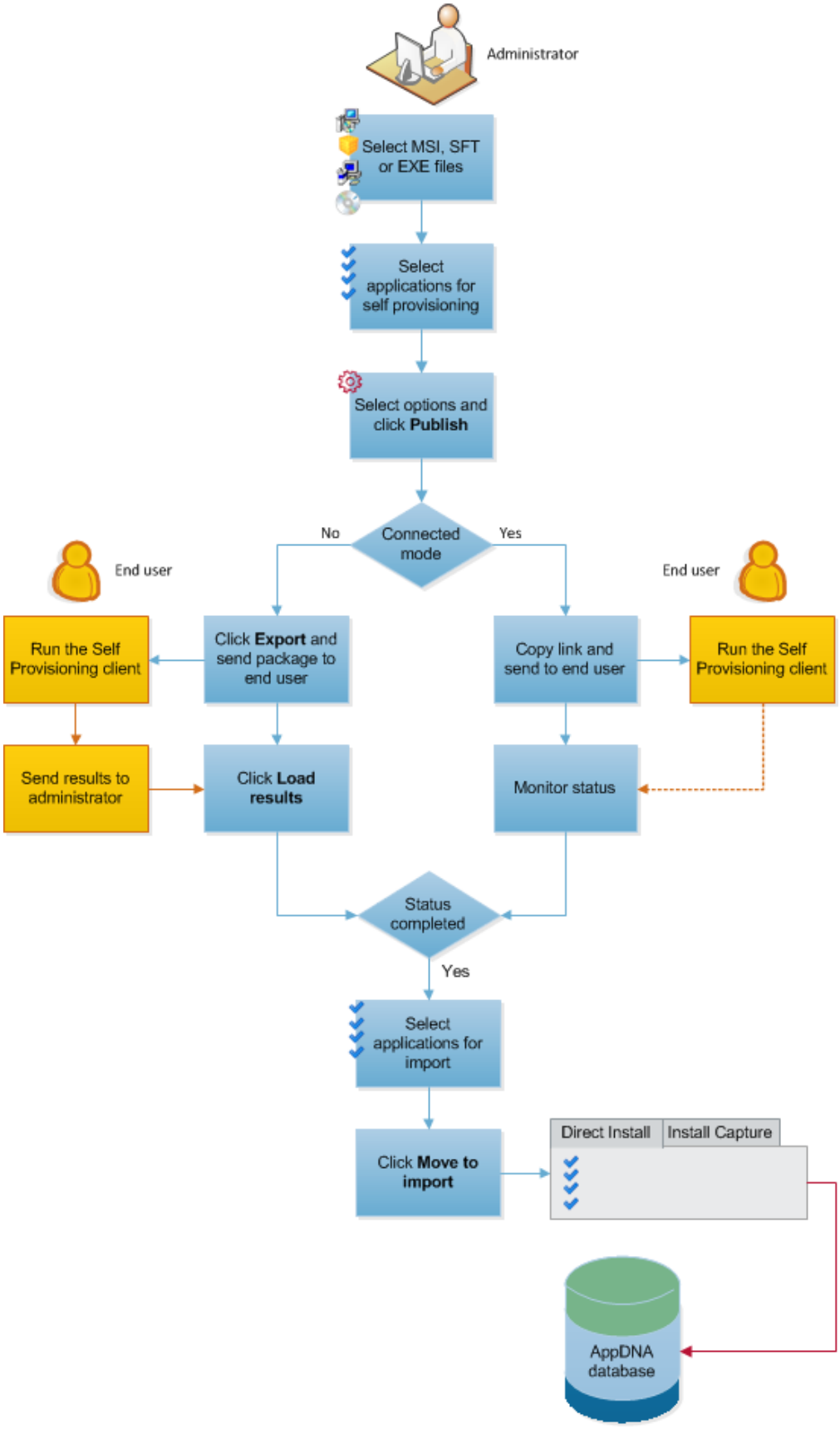
The Self-Provisioning client uses a similar approach to Install Capture and is controlled by execution profiles. The execution profiles that are available for Self-Provisioning mirror those available for Install Capture. By default, the Snapshot execution profile is used. This takes a snapshot of the Self-Provisioning machine, installs the application, and then takes another snapshot of the machine. The difference between the state of the machine in the before and after snapshots represents the changes made by installing the application. The Self-Provisioning client uses this information to generate an MSI file for importing into AppDNA.

Self-Provisioning differs from Install Capture in that it does not reset the machine back to its original state. Therefore Citrix recommends that each capture is run on a clean machine. It is up to the administrator to decide how to handle this, whether by setting up a dedicated physical machine or by using a virtualization technology, such as VDI, which makes it easy to reset the state of the machine.

Self-Provisioning can be used in two modes:

- **Connected.** In this mode, the AppDNA and Self-Provisioning clients are both able to access a network file share.
- **Disconnected.** In this mode, the Self-Provisioning client and the AppDNA client are on different networks and do not both have access to the same network file share. In this mode AppDNA wraps the client instruction files and execution profile into a package that the administrator passes to the end user by FTP, for example. The end user in turn passes the output of the Self-Provisioning client to the administrator by FTP, for example.

The following diagram provides an overview of the Self-Provisioning process.



Note: A client instruction file is a control file used by the Self-Provisioning client to perform the capture or packaging task. Client instruction files are not human-readable instructions intended for end users.

Administer

August 1, 2018

Use the Self-Provisioning tab in the Import Applications screen to administer and manage the Self-Provisioning process. The procedure differs depending on whether you are using the connected or disconnected mode.

To open the Self-Provisioning tab: From the AppDNA side bar, choose Import & Analyze > Applications and then click the Self-Provisioning tab.

Important: Before you start using Self-Provisioning, you must configure the output path in the Self-Provisioning settings. This defines where the Self-Provisioning instructions are stored. When working in connected mode, this also defines the location where the Self-Provisioning client stores the output. Click
Configuration on the Self-Provisioning tab's toolbar to open the Self-Provisioning settings.

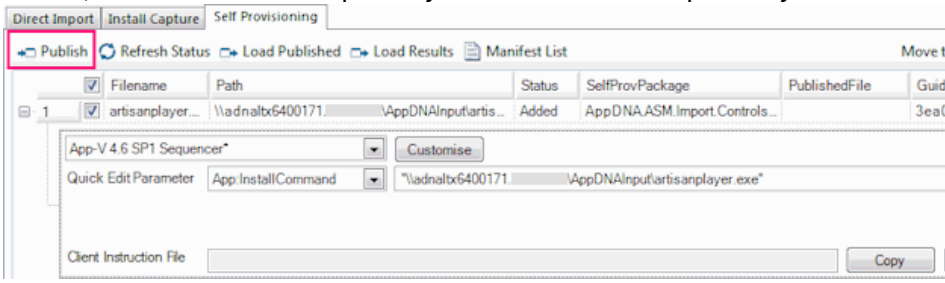
Prepare application for Self-Provisioning

1. Select the installation file(s) that you want to capture. Specify the location of the files using a UNC path, such as \\192.168.50.20\Source\win32-setup.exe. When using the Self-Provisioning client in connected mode, the specified location must also be accessible to the machine that hosts the Self-Provisioning client.

   Click Browse to select individual files, click Search to recursively search a directory structure for files, or use the Import from List option.

   After you select the files, AppDNA lists them.

2. For each application, click the + to the left of the Filename column to show the application options. In the first drop-down list box, select the execution profile you want to use and optionally enter Quick Edit Parameters.

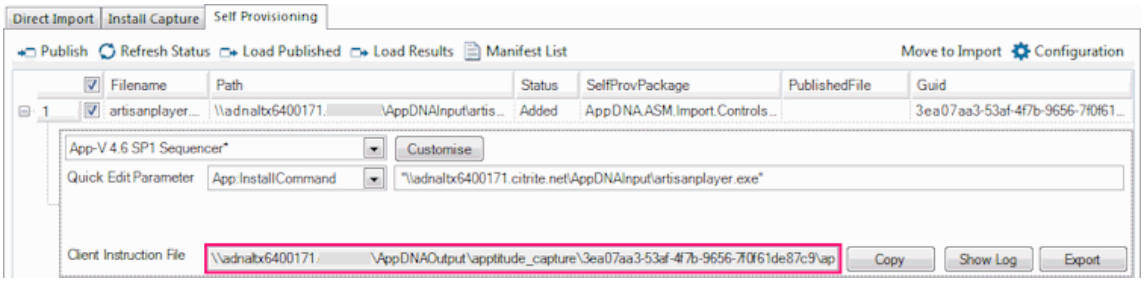


3. Select the application(s) you want to include and then click Publish.

   AppDNA presents a warning that this will overwrite the existing status of the selected applications.

4. Click Yes to continue.

   AppDNA then updates the screen with the details of the client instruction file for each selected application.



5. If you are using connected mode, send the client instruction file to the user who will perform the Self-Provisioning:

   a) To the right of the client instruction file, click Copy to copy the name and location of the file to the clipboard.
   b) Send the copied information to the user who will perform the Self-Provisioning. The user must paste the name and location of the client instruction file into the Self-Provisioning client.

6. If you are using disconnected mode, click Export (to the right of the client instruction file) to create a package to send to the end user who will run the Self-Provisioning client. This opens the Export Self-Provisioning Package dialog box:

   - **Input file from client perspective.** Specify the name and location of the application's installation package, relative to the Self-Provisioning client machine.
   - **Folder where the capture results are to be stored.** Specify the default location where the Self-Provisioning client will write the output of the application capture. The end user can specify a different location during the application capture. Make sure you specify this relative to the Self-Provisioning client machine.
   - **Exported package path.** Specify the name and location of the package that is to be sent to the end user who will run the Self-Provisioning client.

   You now need to send the package and the installation file(s) to the user who will perform the Self-Provisioning in the stand-alone Self-Provisioning client.

Monitor status

To see the status of connected operations in the Self-Provisioning client:

1. On the toolbar, click Refresh status. When you are working in connected mode, this updates the Status column with the results of the operation in the Self-Provisioning client.
2. If the Status changes to Completed, you can import the application into AppDNA. See “Import Completed Applications” below for step-by-step instructions.
3. If the operation failed, click the + to the left of the File name column to show the application options. Then click Show Log to see the processing log.

Load results into AppDNA when using disconnected mode

When you are working in disconnected mode, the Self-Provisioning client creates an output file with a name of the form installer.exe.appcapture_pkg.result, where installer.exe is the name of the installation file.

1. The end user sends the results file to you, for example, by FTP.
2. Save the results file in a suitable location.
3. If necessary, launch AppDNA.
4. From the side bar, choose Import & Analyze > Applications.
5. Click the Self-Provisioning tab.
6. On the Self-Provisioning tab toolbar, click Load Results.
7. In the Search for applications, specify the location of the output files and click Search.

   This changes the status from Published to Completed for the applications for which output files were found.
8. You can now import applications that have a Completed status into AppDNA as described next.

Import completed applications

1. Select the applications that you want to import into AppDNA (these need to have a Completed status).
2. Click Move to Import. This moves the application to the Direct Import tab and removes it from the Self-Provisioning tab. You can import the application into AppDNA on the Direct Import tab in the normal way.

Self-Provisioning toolbar

August 1, 2018

You use the Self-Provisioning tab in the Import Applications screen to administer and manage the Self-Provisioning process. The procedure is different depending on which mode you are using, connected or disconnected.

To open the Self-Provisioning tab:

1. From the AppDNA side bar, choose Import & Analyze > Applications.
2. Click the Self-Provisioning tab.

The toolbar on the Self-Provisioning tab in the Import Applications screen provides the following options:

Publish. Create Self-Provisioning client instruction files (called appcapture.desc) for the selected applications. These are used by the Self-Provisioning client to capture the application for import into AppDNA.

Refresh status. Refresh the status of the applications on the screen. This automatically updates the screen with the results from Self-Provisioning captures that were run in connected mode.

Load published. Load applications that have been previously published. Specify the search options and click Search. AppDNA then searches for matching applications for which there are published instruction files and lists them on the Self-Provisioning tab. Note that AppDNA lists the applications regardless of their status and whether they have already been imported into AppDNA.

Load results. When you are working in disconnected mode, use this button to refresh the status of the applications with the results sent by the end user. Specify the location of the Self-Provisioning output files sent by the end user, and then click Search.

Manifest list. Create a text file in CSV format containing a list of all published client instruction files and their corresponding applications. You can use the list to generate emails to expert users, for example.

Move to Import. Move selected applications that have a Completed status to the Direct Import tab for import into AppDNA in the normal way. This removes these applications from the Self-Provisioning tab.

Configuration. Open the Self-Provisioning page in the Settings dialog. See Self-Provisioning settings for more information.

Self-Provisioning client

August 1, 2018

To capture an application for import into AppDNA, use the Self-Provisioning client. The Self-Provisioning client runs on a separate machine from the machine on which AppDNA is installed. It can be installed on any type of machine (virtual, physical, or VDI).

The Self-Provisioning client can run in two modes:

- **Connected.** In this mode, the Self-Provisioning client can access the location where AppDNA stored the client instruction file. If you are working in this mode, the administrator will have sent you a link to the client instruction file that looks something like this:

  ```
  \\server name\share\25d00eda-8203-4472-9ebf-0fb25107485a\
     appcapture.desc
  ```

  Where server name\share is the first part of the path to the instruction file.

- **Disconnected.** In this mode, the Self-Provisioning client cannot access the location where AppDNA stored the client instruction file. If you are working in this mode, the administrator will have sent you (perhaps by FTP) a package file that has a name like this:

  ```
  installation file name.appcapture_pkg
  ```

  Where installation file name is the name of an application installer that is also provided.

Install the Self-Provisioning client

August 1, 2018

You can install the AppDNA Self-Provisioning client on any type of machine (virtual, physical, or VDI).

Supported operating systems

- Microsoft Windows 10
- Microsoft Windows 7 SP1 (32-bit and 64-bit editions)
- Microsoft Windows XP SP3 (32-bit)
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows Server 2008 SP2 (32-bit and 64-bit editions)
- Microsoft Windows Server 2003 SP2 (32-bit and 64-bit editions)

When capturing Windows applications for testing Windows compatibility, the operating system (OS) on the Self-Provisioning client machine should match the OS on which the applications are currently running. For example, if you are preparing for a migration from Windows 7 to Windows 10, the OS should be based on Windows 7. However, when using Self-Provisioning to create App-V sequences or XenApp packages, the OS should normally match the target OS.

Pre-requisites

- Microsoft .NET Framework 4.5.1
- Installers provided with AppDNA:
  - Citrix AppDNA Self-Provisioning Client.msi
  - Citrix AppDNA VM Configuration.msi

  The 32-bit installers are in C:\Program Files\Citrix\AppDNA\Tools. The 64-bit installers are in C:\Program Files (x86)\Citrix\AppDNA\Tools.

Note: Some execution profiles require additional software to be installed on the Self-Provisioning client machine. For example, to create App-V sequences, the App-V sequencer must be installed. Similarly, to create XenApp profiles, the XenApp profiler must be installed. This additional software is provided separately from AppDNA.

Install the Self-Provisioning client

Install the two MSIs listed above on the Self-Provisioning client machine. Accept the default settings.

Upgrade the Self-Provisioning client

When you upgrade AppDNA to a new version, also upgrade the Self-Provisioning client machine with the new versions of the AppDNA tools.

1. Start the Windows Task Manager.
2. In the Windows Task Manager, click Remote Admin on the Applications tab, and then click End Task.
3. Use Control Panel > Programs and Features to uninstall the current version of the Self-Provisioning client and VM configuration tools.
4. Install the new versions of the tools.

Monitor Self-Provisioning

August 1, 2018

When you are using the Self-Provisioning client to capture an application, you can view a log of the processing at any time. To expand the Progress and Logs display, click the green arrow on the right side of the window. To close the log, click the green arrow above the log.

Error: The directory name is invalid

When this error occurs in the first step, it generally means that the Self-Provisioning client cannot find one of the AppDNA VM Configuration tools.

An AppDNA administrator must set the AppToolsFolder replaceable to point at the correct folder, using the Replaceables tab in Self-Provisioning settings. Then, the administrator must re-publish or re-export the application, as described in Administer Self-Provisioning.

Capture an application

August 1, 2018

This topic describes how to use the Self-Provisioning client to capture an application.

1. To start the Self-Provisioning client: From the Windows Start screen or menu, choose Citrix AppDNA > AppCapture.
2. Enter or browse to the file provided by the administrator. The file might be named appcapture.desc or it may be a package with the file extension appcapture_pkg.
3. To start the application capture process, click the green arrow.

   The Before Snapshot step opens a command window and displays progress messages.
4. Optionally, edit the install command. Then, click the green arrow to start the installation.
5. Typically you now need to manually install and configure the application.
6. Depending on how the capture has been configured (specifically which execution profile is in use), a screen capture utility called ScrnCap might start. It will appear in the bottom right corner of the screen. The utility takes a screen shot of all of the installation and configuration windows that you click. To add a comment to explain an installation or configuration step, click the Snap button.

If the installation requires the computer to be restarted, choose the I will restart my computer later (or equivalent) option. The capture might not succeed if you restart the machine during the capture process.

When the installation finishes, the wizard generates the MSI file for importing into AppDNA and might prompt you to specify an output file location.

Output

The application capture output varies depending on the execution profile used. Typically it includes:

- The generated MSI file
- External source files
- Log files

  For information about viewing the progress log, see Monitor Self-Provisioning.
- Screenshots of the installation and configuration if ScrnCap is used

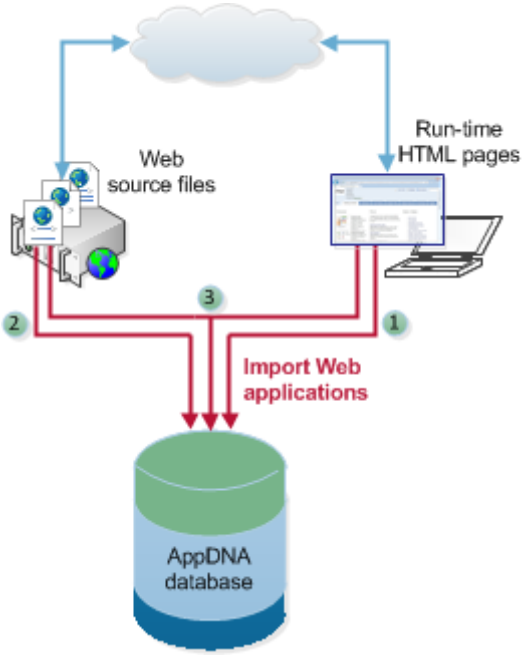
Where the output is stored depends on the name of the file:

- If the file is named appcapture.desc, the Self-Provisioning client stores the output in the same location as this file.
- If the file was a package with the file extension appcapture_pkg, the Self-Provisioning client creates an output file in the location you specified in the last step. This output file has a name of the form installer.exe.appcapture_pkg.result, where installer.exe is the name of the installation file. You must provide the output file to the AppDNA administrator for import into AppDNA.

Web applications

August 1, 2018

To test your web applications for Citrix Secure Web, Internet Explorer, or Firefox compatibility, you first must import them into AppDNA.



You can import web applications by using two different approaches or a combination of both:

1. Use the AppDNA Directed Spider to crawl over the runtime HTML pages and capture them into an MSI for import into AppDNA.
2. Capture the web source files into an MSI file for import into AppDNA.
3. Use a combination of both of these approaches.

You can perform all of these functions within AppDNA on the Import Web Applications screen. Alternatively you can use the stand-alone web application capture tools to perform these functions and then import the generated MSI into AppDNA.

To open the Import Web Applications screen:

- From the AppDNA side bar, choose Import & Analyze > Web Applications.

The Import Web Applications has two tabs:

- Web Capture Import. Use this tab to capture a web application into an MSI and import it in one operation. You can capture the web application's runtime HTML files or the source files, or both for the most comprehensive analysis. When you capture runtime HTML pages, AppDNA opens the AppDNA directed spider.
- Web Direct Import. Use this tab to import web applications that have been captured into an MSI file by using the stand-alone web application capture tools. AppDNA comes with two stand-alone web application capture tools. These can be run on machines that do not have AppDNA installed.

Note: Spider is a generic term for a program that crawls over web pages, following links, and creating copies of all of the pages visited.

Web Capture Import

August 1, 2018

You use the Web Capture Import tab in the Import Web Applications screen to capture web applications into an MSI and import that MSI into AppDNA in one operation.

> **Note**
>
> It is not possible to import a web application by adding a URL (runtime HTML pages). To work around this issue:
>
> 1. Download the version of the .NET Framework Version 2.0 Software Development Kit (SDK).
>   64-bit - https://www.microsoft.com/en-us/download/details.aspx?id=15354
>   32-bit - https://www.microsoft.com/en-us/download/details.aspx?id=19988
> 2. Launch the setup and install the Tools and Debugger feature.

To capture web applications:

1. From the AppDNA side bar, choose Import & Analyze > Web Applications.
2. Click the Web Capture Import tab.
3. To change import options, click Configuration to open the Web import settings.
4. On the toolbar, click Add.
5. In the Select Web Application dialog box, enter the details:
   - Name. The name to be used for the web application within AppDNA.
   - URL. To capture the web application by using the AppDNA directed spider to crawl over the runtime HTML pages, specify the URL of the web application by typing or pasting its URL into the text box.
   - Source folder. To capture the web application's source files, specify their location. For the most comprehensive analysis, specify both a URL and a source folder.
6. Click OK.

   A list of web applications appears.
7. To add more web applications, repeat the previous three steps.
8. To run the spider in manual mode, select the Use Manual Browser Navigation check box. To run the spider in automatic mode, clear the check box.
   - **Manual mode.** This option enables you to walk through the web application manually, following the links that are relevant. Use this for web applications that make significant use of JavaScript and related technologies (such as AJAX) to modify pages after they are

loaded or if there is a complex single sign-on (SSO) scenario. You can optionally switch to automatic mode after capturing the SSO and AJAX pages, for example.

- **Automatic mode.** This option (the default) uses the spider to walk through the web application, stopping only when it encounters an input form or dialog box, depending on the configuration options.

9. In the list, select the web applications that you want to import.
10. On the right-side of the toolbar, click Import.

If you included a web application's URL, AppDNA opens the AppDNA directed spider and an Internet Explorer browser window. See Web Capture Processing for more information.

After you click Import, a message in the Import Web Applications screen shows the progress of the import. To view a log of the import process, click the Log icon to the right of the progress message. This shows the log information in a pop-up window.

Some special characters (such as ":" and "/" cannot be displayed on the Application list page.

Note: For web applications, AppDNA does not use the fingerprint mechanism that it uses for Windows applications. AppDNA treats each web application as a separate application, even if the same application has been imported previously.

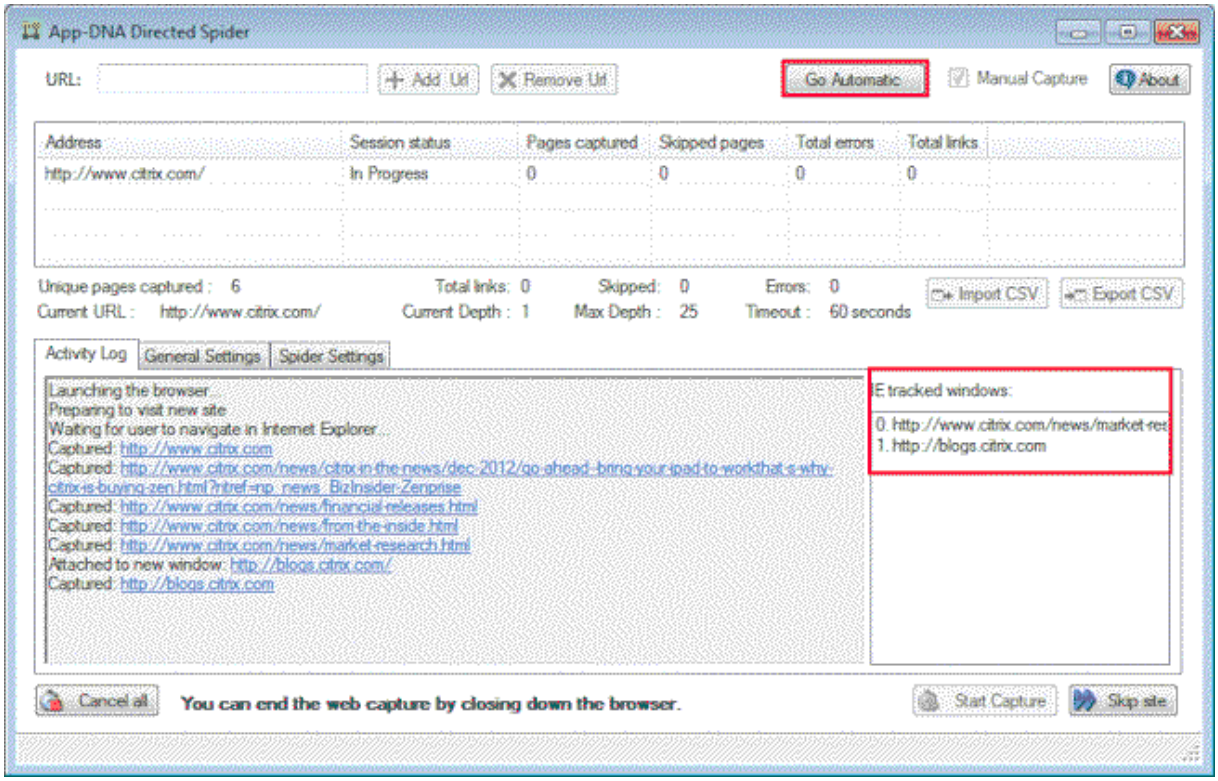
Analysis and reporting

If you have a retail license, AppDNA begins analyzing applications immediately after they are imported, by default. For trial installations, you must run an analysis manually, by default.

Processing

August 1, 2018

This topic provides information about working with the AppDNA directed spider to capture web applications. This topic assumes that you have already started the directed spider as explained in Web Capture Import or Capture Web Application using the Stand-alone Spider.



The AppDNA directed spider opens the specified URL in an Internet Explorer (IE) browser window. What happens next depends on whether you are using manual or automatic mode.

When the spider has finished one web application, it moves on to the next one, if there is another one in the list.

Manual mode

In manual mode, you need to manually walk through the web application and visit every page that you want to capture. If you have selected the option to capture duplicate pages, the spider automatically captures the page again if it changes more than the configurable threshold (provided the specified number of captures has not been exceeded).

You can optionally right-click links and choose Open in new tab. The spider then opens the link in a new window. The spider gives each window that it is tracking a unique index number and lists all of the active windows on the right side of the spider window. To force the capture of a page, right-click the window in this list and choose Capture Page.

Optionally, click Go Automatic in the spider window to switch to automatic mode. The spider then closes the second and any subsequent windows and uses the first window (which has an index of 0) to continue in automatic mode.

When you have finished, close the browser window(s). This ends the capture of the web application.

Automatic mode

In automatic mode, the spider automatically crawls over the web application's pages following the links according to the configuration options chosen.

If you selected the Form User Interaction setting, the spider opens the Form Encountered dialog box when it detects a form on a webpage. When possible the spider then highlights the input boxes in yellow. However, sometimes this is not possible, for example, because the input boxes are customized using a gradient.

The spider then waits for 20 seconds for you to click one of the buttons:

- **Continue**. Click this to close the dialog box and continue with the web capture process.
- **Ignore**. Click this if you want to skip the input fields on this page and the same input fields on every other page in the web application. This is useful when, for example, there is a search form on every page and you want the spider to ignore it. If you want to skip the input fields on this page only, click Continue.
- **Ignore all**. Click this if you want to skip the form on this page and all forms on every subsequent page that the spider encounters in the web application.
- **Wait**. Click this if you want to fill in and submit the form. The spider then waits until you click Continue.

If you do not respond within 20 seconds, the spider skips the form and continues.

Web Direct Import

August 1, 2018

You use the Web Direct Import tab in the Import Web Applications Screen to import MSIs generated by using the stand-alone web capture tools.

To import web applications captured using the stand-alone web capture tools:

1. Launch AppDNA.
2. From the AppDNA side bar, choose Import & Analyze > Web Applications.
3. In the Import Web Applications screen, click the Web Direct Import tab.
4. Select the MSI files that you want to import.

   Click Browse on the toolbar to select individual files; click Search to recursively search a directory structure for files; or click Import List.

   After you have selected the files, AppDNA lists them on the screen.

5. Select the web applications you want to import.
6. On the toolbar, click Import to start loading the web application DNA into the AppDNA database.

After you click Import, a message shows the progress of the import. To view a log of the import process, click the Log icon to the right of the progress message. This shows the log information in a pop-up window.

Important: Although it is possible to import web application MSIs in the Import Applications screen, do not do this, because then AppDNA considers the web application to be a desktop application. Similarly, do not import desktop applications in the Import Web Applications screen.

Import web applications

August 7, 2018

This topic provides information about the Import Web Applications screen's toolbar.

Toolbar

Add. (Only available on the Web Capture Import tab.) Use to open the Select Web Application dialog box, where you can specify the URL of the web application's runtime HTML files, the location of the source files, or both.

URLs. (Only available on the Web Capture Import tab.) Use to select the URL of a web application from a bookmark.

Browse. (Only available on the Web Direct Import tab.) Use to select an individual web application that has been captured into an MSI file using the stand-alone web application capture tools.

Search. (Only available on the Web Direct Import tab.) Use to recursively search down a directory structure for web applications that have been captured into MSI files using the stand-alone web application capture tools. This opens the Search for Applications dialog box.

Select. Provides options to select failed imports, imports with warnings, or successful imports.

Import List. (Only available on the Web Direct Import tab.) Import a predefined list of web applications that have been captured into MSI files using the stand-alone web application capture tools. This opens the Import an Application List dialog box.

Delete. Remove selected applications from the list of applications.

Cancel. Cancel the process that is currently running.

Import. Click to import the selected web applications.

Analyze. Click to analyze the data after it has been imported. Alternatively, you can use the Application List screen to analyze the applications later.

Configuration. Click to set options in Web import settings.

Select Web Application dialog box

You use the Select Web Application dialog box to specify the name of the web application, and the URL of its runtime HTML files, or the location of its source files, or both. To open this dialog box, click Add on the toolbar in the Import Web Applications screen.

Name. The name to be used for the web application within AppDNA.

URL. If you want to capture the web application by using the spider to crawl over the runtime HTML pages, specify its URL here.

Source folder. If you want to capture the web application's source files, specify the location of the folder in which they are located.

Note: You must specify a URL or a source folder. However, you can specify both for the most comprehensive analysis.

Web import settings

August 1, 2018

The Settings dialog box contains general AppDNA options. To open this dialog box, choose Edit > Settings from the menus.

Use the Web Import page of the Settings dialog box to customize the import of web applications through the Import web applications screen.

After making changes in this dialog, click Save to preserve your changes.

Note: With one or two exceptions, the Web Import settings correspond to the settings available on the General Settings and Spider Settings tabs in the stand-alone spider.

Direct Import tab

These options relate to the Web Direct Import tab in the Import Web Applications screen.

Simultaneous Imports (1-20). This controls the number of imports that take place simultaneously. The optimum value is dependent on your hardware configuration. If you increase the value of this

setting and then find that imports fail with a “deadlock” error, decrease it. The default and generally recommended setting is 3.

Preserve Log Files. Select this check box to save log files. This can sometimes be useful for diagnostic purposes. Clear this check box if you do not want to save log files, for example, to save disk space.

Web Spider tab

These options relate to the Web Capture Import tab in the Import Web Applications screen.

Browser timeout. The length of time in seconds that you want the spider to wait for a page to load before ignoring it and moving on to the next page (when running the spider in automatic mode). When you run the spider in manual mode, this setting is used for the first page only. The default is 15 seconds.

Site traversal depth. Specify the link depth that you want the spider to follow. For example, if you specify a depth of 1, the spider starts on the site’s index page and looks to see how many links it contains and visits each of those links. If one of those links contains further links, the spider visits them if the depth is set to a depth of 2 or more. The default is 25.

Automatically close dialog boxes and popups. Select this check box if you want the spider to automatically close dialog boxes that it encounters when running in automatic mode. This is useful, for example, if you want to leave the import running unattended. Clear this check box if you want the spider to wait for you to close dialog boxes manually.

Restrict web app to its virtual directory. Select this check box if you want the spider to ignore any links outside of the web application’s virtual directory (for example, http://myserver/myWebApp). This is useful when there are multiple web applications on the same server and each one is accessed by a different part of the URL. Clear this check box if you want the spider to follow links outside of the virtual directory.

Include sub-domains. Select this check box if you want the spider to follow links to sub-domains of the main domain (for example, http://staging.dev.myserver/myWebApp). Make sure you select this check box if the web application redirects to a sub-domain of the main domain. Clear this check box if you want the spider to ignore links to sub-domains.

Form User Interaction. Select this check box if you want the spider (when running in automatic mode) to stop on every page that has a form and prompt you to fill it in. This is particularly useful when the web application has pages that require the user to login. When this option is selected and the spider detects a form on a webpage, it opens a dialog box and highlights the form input boxes in yellow. For more information, see Web Capture Processing.

Allow Proxy Authentication Prompt. Select this check box if your LAN is configured to use a proxy server and you have selected the Automatically close dialog boxes check box. This means that the spider waits for you to fill in your login information in the authentication dialog box. Clear this check box if your LAN is not configured to use a proxy server.

Allow capture duplicates. This setting affects the spider when running in manual mode only. Select this check box if you want the spider to capture the same page more than once if the page changes. This is useful when capturing web applications that make use of JavaScript and related technologies (such as AJAX) to modify pages after they are loaded. After you select this check box, configure the option with the following:

- **Duplicates count for URL**. Enter the maximum number of times you want the spider to capture a page.
- **Duplicates diff ratio**. Enter the percentage by which the page must change in order for it to be captured again.

Capture results output directory. Specifies the location of the captured results. This is where you can find the generated MSI files and the captured webpages. You normally only need to use these files when you use the stand-alone web application capture tools.

Allowed external domains. A list of external domains that you want the spider to follow links to.

Domain. Specify the web application domain here and click Add to add it to the list of allowed external domains. If the web application redirects to a different domain, enter that domain here. Similarly if an external authentication server that is in a different domain is used, enter that domain here.

Stand-alone Tools

August 1, 2018

AppDNA comes with two stand-alone web application capture tools. These can be run on machines that do not have AppDNA installed.

- **Stand-alone web application capture tool**. This is a stand-alone version of the AppDNA directed spider. This has the same configuration options as the built-in version but has an additional option to generate an MSI. (When you run the capture from inside AppDNA, an MSI is always generated and automatically imported.)
- **Stand-Alone web application source to MSI converter**. This can generate an MSI file from a set of source files. You can use this to generate an MSI from a web application's source files. Because this tool can be run independently of AppDNA, you can send it to the web application administrators and ask them to run it on the web server, for example. Afterwards they simply send you the MSI files and you import them into AppDNA on the Web Direct Import tab in the Import Web Applications screen. This means that you do not need to request permissions to access the web application source files on the server.

If you are using the stand-alone tools and want to combine the output of the spider with the web application's source files, run the spider without selecting the option to create an MSI and then run the MSI Generator over the combined set of files (the output from the spider and the source files).

Install

August 1, 2018

Supported operating systems

- Microsoft Windows 10
- Microsoft Windows 8.1 (32-bit and 64-bit editions)
- Microsoft Windows 8 (32-bit and 64-bit editions)
- Microsoft Windows 7 SP1 (32-bit and 64-bit editions)
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows Server 2008 SP2 (32-bit and 64-bit editions)
- Microsoft Windows XP SP3 (32-bit)
- Microsoft Windows XP SP2 (64-bit)
- Microsoft Windows Vista SP2 (32-bit and 64-bit editions)

Pre-requisite

- Microsoft .NET Framework 3.5 SP1

Additional requirement

- Internet Explorer 11, 10, 9, 8, 7, 6 or Microsoft Edge

Installer

To install the AppDNA stand-alone web capture tools, you need the installer (called Citrix AppDNA Web Application Capture.msi). The installer is available from http://support.citrix.com/article/CTX139494.

To install the AppDNA stand-alone web capture tools:

1. In Windows Explorer, double-click the installer (Citrix AppDNA Web Application Capture.msi) to launch the installation.
2. On the Welcome page, click Next.
3. On the License Agreement page, click I accept the terms in the license agreement, and then click Next.

4. On the Destination Folder page, select an installation folder or accept the default location, and then click Next.
5. On the Ready to Install the Program page, click Install to start the installation.
6. When the installation has completed, click Finish.

Spider

August 1, 2018

You can use the stand-alone directed spider independently of AppDNA to capture your web applications' runtime HTML pages so that you can import them into AppDNA.

To start the stand-alone directed spider:

- From the Windows Start menu, choose Citrix AppDNA > Web Application Capture.

Note: If this option is not available, check that you have installed the stand-alone web capture tools. See
Installing the Stand-alone Web Capture Tools for more information.

Overview

You enter the URLs of the web applications that you want to capture at the top of the screen. Below the list of URLs, there are three tabs. The first provides a log of the spider's activity and you use the other two tabs to enter settings and options. These are documented under separate headings below.

The options on the main part of the screen are as follows:

URL. Specify the web application's URL here and then click Add URL to add it to the list. This must be a valid URL and one to which it is possible to navigate from the computer on which you are running the stand-alone tool. You can add multiple URLs. This is useful, for example, if you want to run a series of web captures.

Remove URL. Removes a URL from the list. Select the URL to be removed before you click this button.

Go automatic. When you are using the Manual capture option, you can use this button to change to automatic mode. The spider then follows links automatically and stops only when it encounters an input form or dialog box, depending on the settings chosen.

Manual capture. Select this check box if you want to use manual mode. In this mode you manually walk through the web application, following the links that are relevant. Use manual mode for web applications that make significant use of JavaScript and related technologies (such as AJAX) to modify pages after they are loaded or if there is a complex single sign-on (SSO) scenario. You can optionally

switch to automatic mode after capturing the SSO and AJAX pages, for example. Clear this check box (the default) if you want the spider to run in automatic mode, stopping only when it encounters an input form or dialog box, depending on the configuration options chosen.

Import CSV. Import a CSV file that lists the URLs that need to be captured.

Export CSV. Export a CSV file listing the URLs that have been captured.

Start capture. Click to begin capturing the list of URLs from the top.

Cancel all. Click to stop the spider.

Skip site. Click to skip the current web site.

General Settings tab

The General Settings tab provides options that control the directed spider's behavior.

Generate MSI. Select this check box if you want to generate an MSI for import into AppDNA. Typically you do this when you are capturing a web application by using the spider only. Clear this check box if you want to combine the captured pages with source files for more comprehensive analysis. You then need to combine the output of the spider with the web application's source files and run the Stand-Alone Web Application Source to MSI Converter over the combined files.

Capture results output directory. Set where you want the output files to be stored. This is where you can find the generated MSI files and the captured webpages.

Site traversal depth. Specify the link depth that you want the spider to follow. For example, if you specify a depth of 1, the spider starts on the site's index page and looks to see how many links it contains and visits each of those links. If one of those links contains further links, the spider visits them if the depth is set to a depth of 2 or more. The default is 25.

Form user interaction. Select this check box if you want the spider (when running in automatic mode) to stop on every page that has a form and prompt you to fill it in. This is particularly useful when the web application has pages that require the user to login. When this option is selected and the spider detects a form on a webpage, it opens a dialog box and highlights the form input boxes in yellow. See Web Capture Processing for more information.

Browser timeout (sec). Specify the length of time in seconds that you want the spider to wait for a page to load before ignoring it and moving on to the next page (when running the spider in automatic mode). When you run the spider in manual mode, this setting is used for the first page only. The default is 15 seconds.

Delay timeout start by (sec). Specify an additional timeout period in seconds for use on older versions of Internet Explorer to cause a delay before the Browser timeout (entered above) starts. This is necessary because older versions of Internet Explorer, particularly when running on older versions of Windows can take some time to move to the next URL. The default value is 1 second.

Delay between capturing (msec). Select this check box if you want the spider to wait for a specified period between the capture of each page. This is useful if your enterprise's firewall would otherwise block the spider from running in automatic mode. This setting is not used when you run the spider in manual mode. Enter the wait period in milliseconds.

Spider Settings tab

The Spider Settings tab provides further options that control the directed spider.

URL inclusions. By default, the AppDNA spider does not follow links to external domains. However, you can create a list of external domains to which you want the spider to follow links.

Domain. Specify the external domain here and click Add to add it to the list of allowed external domains. If the web application redirects to a different domain, enter that domain here. Similarly if an external authentication server that is in a different domain is used, enter that domain here.

Include sub-domains. Select this check box if you want the spider to follow links to sub-domains of the web application's main domain (for example, http://staging.dev.myserver/myWebApp). Make sure you select this check box if the web application redirects to a sub-domain of the main domain. Clear this check box if you want the spider to ignore links to sub-domains.

Restrict web app to its virtual directory. Select this check box if you want the spider to ignore any links outside of the web application's virtual directory (for example, http://myserver/myWebApp). This is useful when there are multiple web applications on the same server and each one is accessed by a different part of the URL. Clear this check box if you want the spider to follow links outside of the virtual directory.

Automatically close dialog boxes and popups. Select this check box if you want the spider to automatically close dialog boxes that it encounters when running in automatic mode. This is useful, for example, if you want to leave the import running unattended. However, note that the spider is unable to close JavaScript-initiated pop-ups. Clear this check box if you want the spider to wait for you to close dialog boxes manually.

Allow Proxy Authentication Prompt. Select this check box if your LAN is configured to use a proxy server and you have selected the Automatically close dialog boxes and popups check box. This means that the spider waits for you to fill in your login information in the authentication dialog box. Clear this check box if your LAN is not configured to use a proxy server.

Duplicates. This setting affects the spider when running in manual mode only. Select this check box if you want the spider to capture the same page more than once if the page changes. This is useful when capturing web applications that make use of JavaScript and related technologies (such as AJAX) to modify pages after they are loaded. After you select this check box, configure the option with the following:

- **Maximum number of duplicates for URL**. Enter the maximum number of times you want the spider to capture a page.
- **Page content difference value to capture**. Enter the percentage by which the page must change in order for it to be captured again.

Capture Web Application

August 1, 2018

1. From the Windows Start menu, choose Citrix AppDNA > Web Application Capture.
2. Use the General Settings tab and the Spider Settings tab to set the options that you want to use. See Stand-Alone Directed Spider for more information.
3. Type or paste the URL of the web application you want to capture into the URL box.
4. Click Add URL to add the URL to the list of URLs to be captured.
5. Repeat steps 3 and 4 if you want to capture multiple web applications.
6. Select the Manual Capture check box if you want to run the spider in manual mode. Clear the check box if you want to run the spider in automatic mode:
    - **Manual mode**. Use this option if you want to walk through the web application manually, following the links that are relevant. Use this mode for web applications that make significant use of JavaScript and related technologies (such as AJAX) to modify pages after they are loaded or if there is a complex single sign-on (SSO) scenario. You can optionally switch to automatic mode after capturing the SSO and AJAX pages, for example.
    - **Automatic mode**. Use this option (the default) if you want the spider to walk through the web application automatically, stopping only when it encounters an input form or dialog box, depending on the configuration options chosen.
7. Click Start Capture. The AppDNA Directed Spider then opens the first URL in the list in an Internet Explorer browser window. For information about the processing that takes place, see Web Capture Processing.
8. When all of the captures have completed, click the X in the top right corner to close the window.

Output

The output is located in the folder that is specified on the General Settings tab in the stand-alone spider window. The output for each application is stored in a separate folder, whose name is derived from the URL, and the date and time stamp.

If you chose not to generate an MSI, the web application's folder contains a Rendered subfolder, which contains all of the captured data. You can use the Stand-alone MSI Converter tool to convert this into an MSI for import into AppDNA.

If an MSI was generated, it is stored in the output folder. You can import this MSI directly into AppDNA on the Web Direct Import tab in the Import Web Applications screen. See Web Direct Import for more information.

Note: When you run the AppDNA Directed Spider from within AppDNA, an MSI file is always generated and imported into AppDNA automatically.

MSI Converter

August 3, 2018

You use the stand-alone Web Application Source to MSI Converter tool to generate an MSI file from a set of web application sources files. Because this tool can be run independently of AppDNA, you can send it to the web application administrators and ask them to run it on the web server, for example. Afterwards they simply send you the MSI files and you import them into AppDNA on the Web Direct Import tab in the Import Web Applications Screen.

This means that you do not need to request permissions to access the web application source files on the server.

Note: The standalone MSI Converter tool is also available to generate an MSI file from any application with source files on your file system. The tool is suitable for applications that are installable using xcopy or for applications with missing source media. Although the MSI Converter tool does not capture additional components in other folders or special registry keys, it does provide a starting place for analysis.

To start the stand-alone MSI Converter tool:

- From the Windows Start menu, choose Citrix AppDNA > Web Application Source to MSI Converter.

  If this option is not available, you must install the stand-alone web capture tools as described in Installing the Stand-alone Web Capture Tools.

About the tool

The main part of the web Application Source to MSI Converter window lists the folders that contain the web application source files that you want to capture into an MSI file for import into AppDNA.

You can double-click in the Product Name, Product Version, and Manufacturer Name columns to edit the details. This is useful because these details are used to identify the web application when you import it into AppDNA (although you can change these details within AppDNA).

The space below the list of folders displays a log of the processing. Click Refresh to update this part of the screen with the latest details.

Toolbar options:

Select. Click to select a folder that contains the files that you want to convert into an MSI for import into AppDNA. This adds the folder to the list.

Search for folders. Opens the Search for Folders dialog box. You can use this to enter sophisticated folder search options. The options are:

- **Path**. Specify a folder that contains subfolders that contain the source files from which you want to generate an MSI for import into AppDNA.
- **Pattern**. If you want to restrict the search to one or more specific folders, enter the name here. You can use an asterisk (*) as a wildcard.
- **Recurse**. Select this check box to specify that you want to search for folders within the folders that are direct children of the folder specified in the Path box. Clear this check box to search only one level down from the folder specified in the Path box.
- **Details mapping**. This controls how the initial values in the Product Name, Product Version, and Manufacturer Name columns are derived. You can edit these values later by double-clicking in the columns.

Option	Description
<No mapping>	Use the default values. Product Name is Unknown Product, Product Version is 1.0.0.0 and Manufacturer Name is Unknown Manufacturer.
…\Product	Base the Product Name on the name of the last folder in the path and use the default values for the Version and Manufacturer Name.
…\Manufacturer\Product\Version	Base the Manufacturer Name, Product Name and Version on the names of the last three folders in the tree, respectively.
…\Manufacturer\Product	Base the Manufacturer Name and Product Name on the names of the last two folders in the tree, respectively, and use the default value for the Version.
…\Product\Version	Base the Product Name and Version on the names of the last two folders in the tree, respectively, and use the default value for the Manufacturer Name.

Import list. Opens the Import List dialog box, where you can specify a CSV file that contains a list of folders to import. The options are:

- **Path**. The name and path of the CSV file that contains the list of folders to import. This can optionally also specify the product name, version and manufacturer in the following format:

```
Directory,ProductName,Version,Manufacturer  c:\test,TestApp
   ,1.0.0.0,TestCompany
```

- **Override CSV details using path regex**. This controls how the initial values in the Product Name, Product Version and Manufacturer Name columns are derived. You can edit these values later by double-clicking in the columns.

  You can select a predefined option from the drop-down list. The available options are as described for the Search for Folders dialog box, except that the <No mapping> option derives the values from the CSV file. Alternatively you can enter your own regular expression.

  Note: Regular expressions are a widely used text pattern matching language. There are many resources on the World Wide Web for learning about the syntax. For example, http://msdn.microsoft.com/en-us/library/az24scfc.aspx.

Configure. Opens the Configuration dialog box where you enter the locations of the generated MSI files and log files and processing options.

- **Generated MSI location**. Specify where you want the MSI output files stored. This is where you can find the generated MSI files after running the tool.
- **Log file location**. Specify where you want the log files stored.
- **Heat options (blank = default)**. Heat is a tool that the MSI generator uses internally to generate the MSI. You can use this box to enter configuration options. Click the ? to get a summary of the various options and their syntax. This is an advanced feature. Leave this box blank for the default options. For more information, see http://wix.sourceforge.net/manual-wix3/heat.htm.

Start. Start converting the selected folders.

Cancel. Cancel the conversion of the selected folders.

Select all. Select all folders in the list.

Invert. Select the folders that are not currently selected and deselect the ones that are selected.

Remove. Remove selected folders.

Generate MSI

August 1, 2018

This topic provides step-by-step instructions for using the Stand-Alone Web Application Source to MSI Converter to generate an MSI from one or more folders containing web application source files.

Note: If you want to create an MSI that combines the output of the Stand-Alone Directed Spider with the web application source files, you need to combine the two types of files in one folder before following these steps.

1. From the Windows Start menu, choose Citrix AppDNA > Web Application Source to MSI Converter.
2. If necessary, click Configure on the toolbar to set the options you want to use.

   For information about these options and the options in the next step, see Stand-alone MSI Converter tool.
3. Click Select, Search for Folders or Import List, to select the folders that contain the web application source files that you want to convert.

   This lists the selected folder(s) in the window.
4. Select the folder(s) for which you want to create an MSI.
5. Click Start to start the processing.

The MSI Generator shows whether the processing is successful in the Status column. Completed means that the processing finished successfully. If the processing is not successful, click the Refresh button to view the log. This provides information that you can use to attempt to understand the cause of the problem.

Output

The output from the Stand-Alone Web Application Source to MSI Converter is located in the folder that is specified in the Configuration dialog box. The output for each application is stored in a separate folder, whose name is derived from the folder name and the date and time stamp.

You import the MSIs into AppDNA on the Web Direct Import tab in the Import Web Applications Screen. See Web Direct Import for more information.

Limitations

August 1, 2018

Limitations of the AppDNA directed spider

The AppDNA directed spider can be run in two modes: automatic and manual. In automatic mode, the AppDNA Directed Spider captures the run-time HTML pages at the point at which they are fully loaded or when the period defined in the Browser timeout setting is reached (whichever is earlier). In automatic mode, the AppDNA directed spider does not capture any modifications that are made to the page after this point.

Automatic mode is therefore not suitable for capturing web applications that rely on JavaScript and related technologies, such as AJAX, to modify pages after they are loaded. For example, some web applications use JavaScript after the page has loaded to fetch results from a database and display them on the page. In automatic mode, the spider does not capture this, because it happens after the page is loaded.

Citrix therefore recommends that you use manual mode for capturing web applications that make significant use of JavaScript and related technologies (such as AJAX) to modify pages after they are loaded. For best results, select the Capture duplicates setting, which allows the same page to be captured more than once when using manual mode and the page has changed by more than a specified threshold.

In addition, the AppDNA directed spider does not close JavaScript-initiated pop-ups, regardless whether the Automatically close dialogs option is selected.

See Web import settings for information about the settings.

File path limit of 260 characters

There is a limit of 260 characters to the length of the fully-qualified file path when generating an MSI. This affects imports on the Web Capture Import tab in the Import Web Applications Screen as well as the stand-alone Web Application Source to MSI Converter.

For example, suppose you want to import some web application source files and the fully-qualified file path to one or more of the source files has more than 260 characters. The import will fail. You can resolve the issue by moving or copying the files to a different location that has a shorter path or by using a mapped drive to shorten the path.

Supported web source file types

AppDNA can import the following web source file types:

.ahtm, .ahtml, .alx, .api, .aqf, .as, .ascx, .ashx, .asmx, .asp, .aspx, .asr, .atom, .axd, .cdf, .cfc, .cfm, .cfml, .cgi, .chl, .chtm, .chtml, .cls, .config, .css, .css1, .dbm,
.dhtml, .dtd, .dwp, .dwt, .ent, .epx, .fhtml, .fl, .ht, .hta, .htc, .htd, .htm

.html, .htmls, .ie3, .ihtm,.ihtml, .inc, .iqy, .jhtm, .jhtml, .js, .jsb, .jsc, .jsf, .json, .jsp, .jsp, .jspx, .jst, .mht, .mhtm, .mhtml, .msie, .mspx, .php, .php4, .php5, .phps, .phtm, .phtml, .pl, .pm, .py, .sdl, .sht, .shtm, .shtml, .sitemap, .ssi, .stm, .stml, .svc, .swf, .swf2, .swfl, .thtml, .ttml, .uri, .url, .vb, .vbs, .webloc, .wsdl, .xht, .xhtm, .xhtml, .xml, .xsc, .xsd, .xsd, .xsl, .xslt

Import Applications Toolbar

August 1, 2018

This topic provides information about the toolbar in the Import Applications screen. You use this screen to import desktop applications into AppDNA.

To open the Import Applications screen:

- From the side bar, choose Import & Analyze > Applications.

Main toolbar

 **Browse**. Use to select individual installation files. If you are on the Direct Import tab and you select a file that is not an .msi, .sft, or .appv, AppDNA automatically adds it to the Install Capture tab. Similarly if you are on the Install Capture tab and select an .msi, .sft, or .appv file, AppDNA automatically adds it to the Direct Import tab.

 **Search**. Use to recursively search down a directory structure for installation files of various types. You can optionally choose to also search for .mst transformation files and to specify the group you want the applications to be added to. When you use this button on the Direct Import or Install Capture tabs, AppDNA automatically adds .msi, .sft, and .appv files to the Direct Import tab and other file types to the Install Capture tab. See Search for applications for more information.

Import from List. Select a .csv file that defines a list of applications to be imported. See Import from List for more information.

Select. Provides options to select failed imports, imports with warnings, or successful imports.

 **Backup**. Back up the lists of applications on the Direct Import and Install Capture tabs so that you can revert back to them later.

 **Restore**. Restore the lists of applications that were backed up previously.

 **Delete**. Remove selected applications from the current tab.

 Cancel. Cancel the process that is currently running.

Import. Click to import the selected applications into AppDNA. This imports any applications that are selected on both the Direct Import tab and the Install Capture tab. If any applications are selected on the Install Capture tab, by default AppDNA runs through a series of checks of the virtual machine configuration. If necessary, you can turn off these checks in Install Capture Settings.

Analyze. Click to analyze the data after it has been imported. Alternatively, you can analyze the applications later. See Analyze applications for more information.

Direct Import toolbar

The Direct Import toolbar provides the following options:

Select All MSTs. Select this check box if you want to automatically apply .mst files to the .msi files during the import. The .mst and .msi files must be stored in the same location. The .mst files are used to transform or manipulate .msi files.

Expand All MSTs. When you select an .msi file for import and there are .mst files in the same directory, AppDNA puts a + to the left of the application's name. When you click the +, AppDNA shows the associated .mst files so that you can select them individually. Select this option to automatically show all .mst files without needing to click the +.

Configuration. Click to open the Import and analyze settings.

Import from List

August 1, 2018

You can use a comma-separated values (.csv) file to define a list of applications to import into AppDNA. The file must have the following columns:

- **Filename.** The name and path of the file to be imported. For Install Capture and Self-Provisioning, this must be expressed as a UNC path.
- **Silent switch**. Use this column to specify a silent switch using the /s notation.
- **Execution profile**. For Install Capture and Self-Provisioning, specify the execution profile to be used.
- **Group**. Use this column to specify the group that the application is to be imported into. If the group is nested, use the RootGroup\ChildGroup\ChildGroup notation to specify the group.
- **AppID**. Use this column to specify the application ID.
- **Application attributes**. When you create an application attribute, AppDNA adds it to the template import file. Use these columns to provide the attribute data.

- Imported dates must be in international date format (YYYY-MM-DD). Microsoft Excel defaults to the date format for the current locale, so be sure to check the format of date columns and change them if needed.
- An imported list value is ignored if it does not match a list item defined for the attribute.
- For a list type of RAG, the accepted values are Red, Amber, and Green. These values are not case-sensitive.

Tip: You can download a template import file from the
Import an Application List dialog box. To open this dialog box, click
Import from List on the toolbar in the
Import Applications screen.

Non-English characters

If the file includes any characters that are not standard printable ASCII characters, the file must be saved with UTF-8 encoding.

Example

In the following example .csv file, the first row defines the columns, including the application attribute AppID. The second row specifies an .msi file to import into the General application group. The third row specifies an .exe file to import using a silent switch and the Snapshot execution profile into the General application group.

```
Filename,Silent Switch,Execution Profile,Group,AppID
\\machine01\25appTest\Dreamweaver_MX_6.0_P1.1.msi,,,General
\\machine171\AppDNAInput\burn4free_setup.exe,/s,Snapshot,General
```

Import the applications specified in the file

1. On the toolbar in the Import Applications screen, click Import from List.
2. Specify the file.
3. If you are importing application attributes, verify the Ignore attribute errors setting.

   Errors are incorrect data, missing data, or columns that cannot be matched. Choose whether to ignore errors for this import.
4. Click Import. If you are on the Self-Provisioning tab, AppDNA lists all types of files found on the Self-Provisioning tab. If you are on the Direct Import or Install Capture tab, AppDNA lists .msi, .sft, and .appv files on the Direct Import tab, and all other file types on the Install Capture tab.

5. Select the applications in the normal way and then click Import on the toolbar.

Note: You can also import web applications using an import list in the Import Web Applications screen.

Search for applications

August 1, 2018

You use the Search for Applications dialog box to search a directory structure for applications to import into AppDNA. AppDNA finds any files in the specified location that match the criteria you enter and then lists them on the appropriate tab in the Import Applications screen.

If you are on the Self-Provisioning tab when you open this dialog box, AppDNA lists all types of files found on the Self-Provisioning tab. If you are on the Direct Import or Install Capture tab when you open this dialog box, AppDNA lists .msi, .sft, and .appv files on the Direct Import tab and all other file types on the Install Capture tab.

To open the Search for Applications dialog box: On the toolbar in the Import Applications screen, click Search.

Folder to search. Specify the folder you want to search. Click Browse to navigate to the folder.

Recursive. Select this check box to specify that you want AppDNA to search the subfolders of the folder specified above.

File name - wildcard *. Use this text box to specify a full or partial file name to search for. You can use an asterisk (*) as a wildcard character. For example, ABC* matches files whose names start with “ABC” and are followed by no or any number of other characters; *ABC* matches files that have “ABC” anywhere in their file name. The search is case-insensitive. The default value is *, which matches all file names.

MSI. Select this check box if you want to find .msi packages.

NON-MSI - Select this check box if you want to find other types of installation package. Use the drop-down list to specify the types of installation files you want to find. These can be .exe, .sft, .appv, or .bat files, or any combination of these types.

Options. Click for additional options. These are organized on two tabs:

- **Import options**. This tab provides options to apply to the applications:
  - **Search for associated MSI transforms (.MST files)**. Select this check box if you want to search for .mst files. The .mst files are enumerated in reverse chronological order.
- **Batch import**. This tab provides options to select applications for import in batches. This is useful if the folder (and if relevant its subfolders) contain a very large number of applications.

- **Import in batches**. Select this check box to select applications in batches.
- **Applications in a batch**. Specify the number of applications in a batch here. You can then use this dialog box to select the applications for import one batch at a time. Increment the Batch number by one each time, until all of the applications have been imported.
- **Batch number**. When importing applications in batches, specify the batch number you want to select for import here.

Settings

August 1, 2018

The Settings dialog box contains general AppDNA options. The settings are grouped into pages. Use the side bar on the left side to move between pages. Click the Save button to preserve your changes.

Click the Help button in the top right corner to open Help specific to the page you are on.

To open the Settings dialog box:

- From the menus, choose Edit > Settings.

AppDNA settings

- Reporting
- Discovery
- Active Directory
- ConfigMgr
- Files
- Import and Analyze
- Web Import
- Self-Provisioning
- Install Capture
- Login
- OS Image Configuration
- Sites
- CEIP

File settings

August 1, 2018

The Settings dialog box contains general AppDNA options. To open this dialog box, choose Edit > Settings from the menus.

The options on the Files page of the Settings dialog box are:

Log File Location. Set where you want log files to be stored.

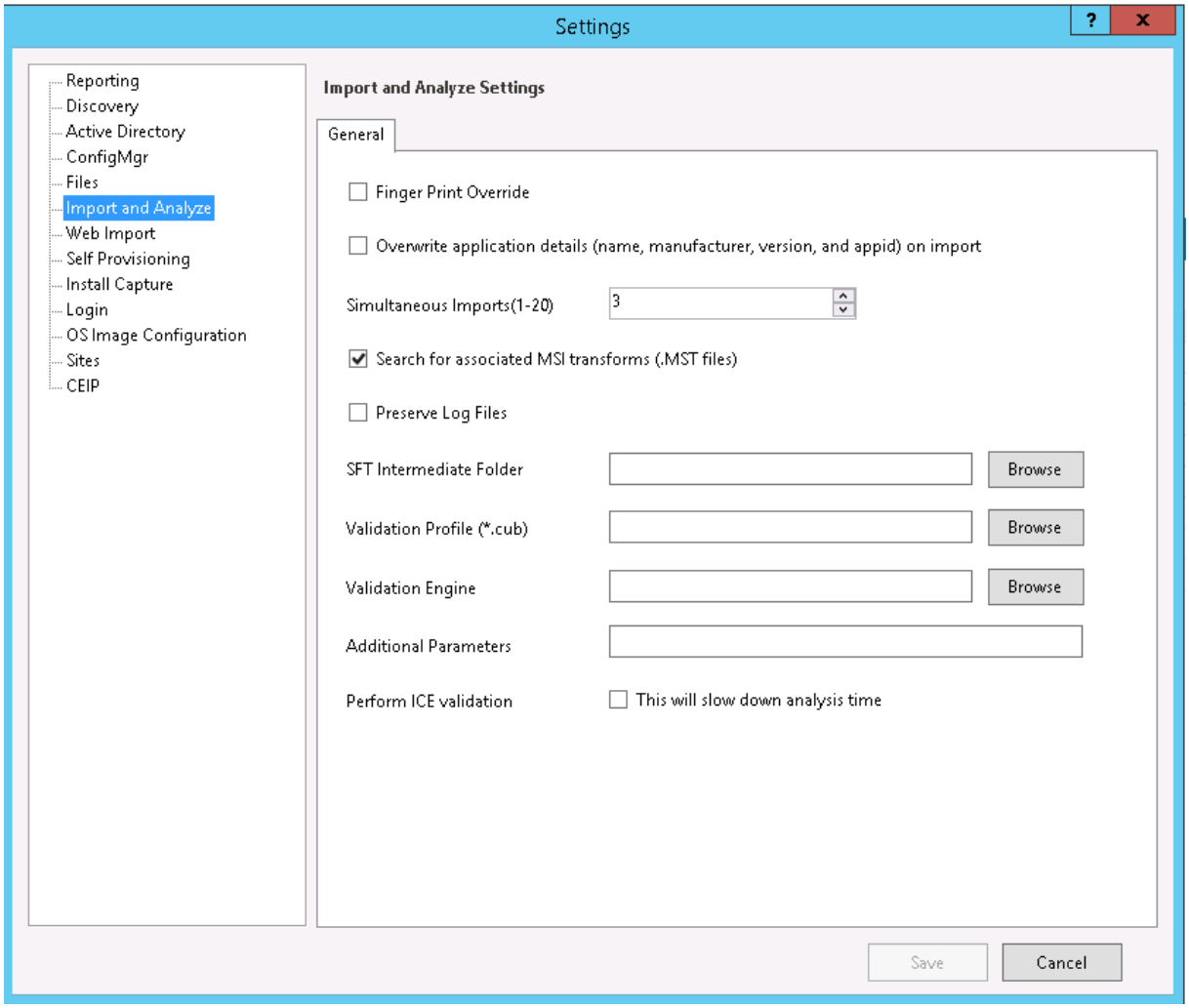
Temporary File Location. Set where you want temporary files to be stored.

Click Save to preserve your changes.

Import and analyze settings

August 1, 2018

Use the Import and Analyze page of the Settings dialog box to customize the imports performed from the Direct Import tab of the Import Applications screen. To open the Settings dialog box, choose Edit > Settings.



Options:

Finger print override. Select this check box if you want AppDNA to consider each re-import of a desktop application to be a separate application. Clear this check box if you want a desktop application to be considered the same application on re-import if its fingerprint has not changed by more than 10%. This is the default behavior and means that if you modify a desktop application as part of the remediation process and then re-import it, it is generally considered to be the same application.

Overwrite application details (name, manufacturer, version, and appid) on import. Choose this option if you want to overwrite manual changes you have made to the application name, manufacturer, version or AppID when you reimport an application.

Simultaneous imports (1-20). This controls the number of imports that take place simultaneously on the client. The optimum value is dependent on your hardware configuration. The default setting is 3.

Search for associated MSI transforms (.MST files). Automatically applies MST files to the MSI files during the import. MST and MSI files must be stored in the same location on your file system.

Preserve log files. Select this check box to save log files. This can sometimes be useful for diagnostic purposes. Clear this check box if you do not want to save log files - for example, to save disk space.

SFT intermediate folder. When AppDNA imports .sft or .appv files, it unpacks them into an intermediate folder. To keep the extracted files, set the location of the intermediate folder here. If you do not specify a location, a temporary folder is used and it is cleared after each .sft and .appv import.

When AppDNA unpacks .sft and .appv files, it preserves their internal directory structure. This can sometimes lead to the maximum number of characters that Windows allows in a file path being exceeded, which will cause the import to fail. You can reduce the chance of this happening by setting the shortest possible file path here.

Validation profile (*.cub). To perform ICE validation of MSI files during import, specify the location of the CUB files here. CUB files store the ICE validation rules.

Validation engine. To perform ICE validation of MSI files during import, specify the location of the package validation tool such as Msival2.exe.

Additional parameters. Specify any command line parameters for the ICE validation engine here. See http://msdn.microsoft.com/en-us/library/windows/desktop/aa370504(v=vs.85).aspx for information about the Msival2.exe parameters.

Perform ICE validation. Select this check box to perform Internal Consistency Evaluator (ICE) validation during the import process to detect potential problems with MSI files.

Install Capture settings

August 1, 2018

The Settings dialog box contains general AppDNA options. To open the Settings dialog box, choose Edit > Settings from the menus.

After making changes in this dialog box, click Save to preserve your changes.

Virtual Machines tab

Use the Virtual Machines tab on the Install Capture page in the Settings dialog box to view, add, edit, and delete virtual machine configurations for use with Install Capture and Forward Path tasks. Each configuration has a unique name, which appears in the Select VM Configuration drop-down box on the Install Capture tab in the Import Applications screen. You can create multiple configurations to meet different requirements.

The toolbar on the Virtual Machines tab provides the following options:

- **New.** Add a new virtual machine configuration. This opens the Virtual Machine Configuration Wizard.
- **Edit**. Opens the Virtual Machine Configuration wizard where you can make any necessary modifications to the selected configuration. This is the recommended way to edit a virtual machine configuration. Select the configuration in the list before you click this button.
- **Advanced**. Opens the Virtual Machine Configuration dialog box to view or edit the settings of an existing configuration. Select the configuration in the list before you click this button. See Virtual Machine Configuration Dialog Box for more information.
- **Delete**. Deletes the selected configuration.
- **Set as default.** If you have multiple virtual machine configurations, use this button to set one as the default. This is then selected by default in the drop-down list on the Install Capture tab in the Import Applications screen.

Note: Virtual machine configurations are stored on a per user basis. This means that this dialog box and the drop-down on the Install Capture tab in the Import Applications screen list only the virtual machine configurations that were created with the AppDNA user account that you are currently logged on as.

Execution Profiles tab

Execution profiles control the tasks and resources that are run on the virtual machine during the Install Capture process. Advanced users can create and edit execution profiles by using the Execution Profiles tab.

The Execution Profiles tab provides the following options:

- **New**. Add a new execution profile. This opens the Edit an execution profile.
- **Edit**. Open the Edit Execution Profile dialog box, where you can make any necessary modifications to the selected execution profile.
- **Delete**. Delete the selected execution profile.
- **Set as Default**. Set the selected execution profile as the default execution profile. This means that it is selected by default, for example, in the execution profile drop-down box on the Install Capture tab in the Import Applications screen.
- **Import**. Import an execution profile from an XML file. This can be an XML file that you saved earlier or an XML file provided by Citrix.
- **Export**. Export an execution profile to an XML file. Citrix recommends that you use this feature to create a backup of an execution profile before changing it.

Settings tab

The Settings tab in Install Capture Settings has one setting:

Skip virtual machine system check. Select this check box if you do not want AppDNA to check the virtual machine configuration when you click Import in the Import Applications screen when importing applications through the Install Capture tab. Clear this check box to enable the checks.

Self-Provisioning settings

August 1, 2018

The Settings dialog box contains general AppDNA options. To open the Settings dialog box, choose Edit > Settings from the menus.

Use the Self-Provisioning page of the Settings dialog to configure Self-Provisioning and customize how the stand-alone Self-Provisioning client appears to your users. For example, you can add welcome, completion, and error texts, and also your company logo.

After making changes in this dialog, click Save to preserve your changes.

General Tab

Output Path. Replace the default value (\\<server>\<share>\appdna_capture) with the path to the location where you want the output to be stored. This defines where the Self-Provisioning client instruction files are stored. When working in connected mode, it also defines the location where the Self-Provisioning client stores the output.

Logo. Add your company logo so that it is displayed when a user runs the stand-alone Self-Provisioning tool.

Execution Profiles Tab

Execution profiles control the tasks and resources that are run on the Self-Provisioning client machine. The Execution Profiles tab lists the execution profiles that already exist. Each execution profile has a unique name, which is used to identify it, for example, in the execution profile drop-down box on the Self-Provisioning tab in the Import Applications screen.

The Execution Profiles tab provides the following buttons:

New. Add a new execution profile. This opens the Edit an execution profile.

Edit. Edit the selected execution profile. This opens the Edit an execution profile where you can make any necessary modifications to the selected execution profile.

Delete. Delete the selected execution profile.

Set as Default. Set the selected execution profile as the default execution profile. This means that it is selected by default in the execution profile drop-down box on the Self-Provisioning tab in the Import Applications screen.

Import. Import an execution profile from an XML file. This can be an XML file that you saved earlier or an XML file provided by Citrix.

Export. Export an execution profile to an XML file. It is recommended that you use this feature to create a backup of an execution profile before changing it.

Replaceables Tab

Use the Replaceables tab in Self-Provisioning Settings to define replaceable values for use in the execution profiles used in the Self-Provisioning tool. However, the replaceable values you define here are overridden if values are explicitly defined for those replaceables in the execution profile itself or in the Quick Edit Parameter box in the Import Applications screen.

Replaceables are placeholders that are replaced by a value provided at run time. The syntax for including a replaceable in the execution profile is: $(replaceable_name), where replaceable_name is the name of the replaceable.

The AppToolsFolder replaceable is used to specify the location of the tools installed on the Self-Provisioning client machine by the Citrix AppDNA VM Configuration MSI. By default, these are installed to C:\Program Files\Citrix\AppDNA\VM Configuration (or C:\Program Files (x86)\Citrix\AppDNA\VM Configuration on 64-bit machines). The default value for the AppToolsFolder replaceable uses the %APPDNAVMCONFIG% environment variable. This stores the actual installed location of the tools. It is created by the AppDNA VM Configuration MSI when the tools are installed.

To define a replaceable value for Self-Provisioning:

- If the replaceable whose value you want to change is in the list, select it and click Edit. This opens the Edit Text dialog box, in which you can enter or paste the new value.
- If the replaceable whose value you want to define does not appear in the list, click New. This opens the Edit Replaceable dialog box, in which you can enter the new replaceable and its value.

The following list shows replaceables that are used internally. AppDNA automatically sets the values of these replaceables and you do not need to do this manually.

- App:InstallCommand
- App:InstallDriveLetter
- App:InstallWrkDir
- App:Manufacturer (Only used in Forward Path task scripts.)
- App:Name (Only used in Forward Path task scripts.)
- App:Version (Only used in Forward Path task scripts.)

- Capture:ImportInputFile
- Capture:InputFile
- Capture:Mode
- Capture:OutputFile
- Capture:OutputDirectory

Note: These replaceables have a colon (:) in their name. This indicates that this is an internal replaceable defined by Citrix. If you create your own replaceables, make sure that they do not include a colon in the name. This will ensure that the name will not conflict with an internal replaceable provided by Citrix in the future. The part of the name before the colon provides an indication of how the replaceable is used. For example, App indicates that the replaceable provides information about the application that is being processed and Capture indicates that it relates to the current capture state.

Text Tab

Use the Text tab to define text to be displayed to the user of the stand-alone Self-Provisioning tool.

Error Text. This is displayed when an error occurs.

Completion Text. This is displayed to users when they finish an application capture.

Welcome Text. This is displayed to users when they start the tool.

Advanced Tab

Restore Defaults. This restores all of the Self-Provisioning settings to their default values. For example, it deletes any replaceables that have been created and removes any changes to the default execution profile.

Click Save to preserve your changes.

CEIP

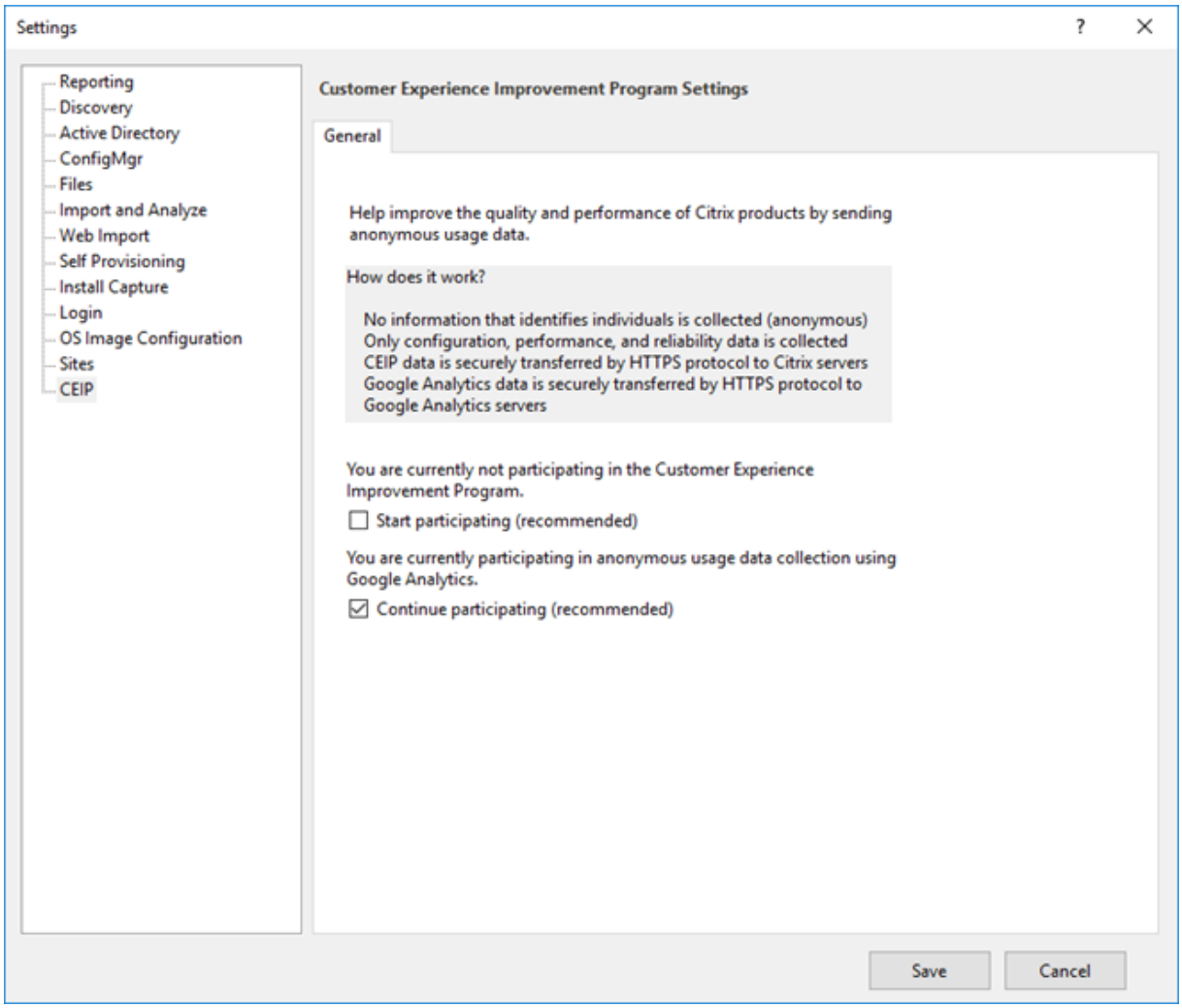
August 1, 2018

The Citrix Customer Experience Improvement Program (CEIP) gathers anonymous configuration and usage data from AppDNA and automatically sends the data to Citrix. For more information on CEIP, see About the Citrix Customer Improvement Program (CEIP) on citrix.com and Citrix Insight Services in the XenApp and XenDesktop documentation.

Citrix also gathers anonymous usage data on AppDNA using Google Analytics. The data is sent to the Google Analytics server via HTTPS. Analytics collection complies with the Citrix Privacy Policy.

Citrix CEIP and Google Analytics data helps Citrix improve the quality, reliability, and performance of AppDNA. Participation is voluntary.

Citrix CEIP and Google Analytics are enabled by default when you install or upgrade AppDNA. To change your participation, go to **Edit** > **Settings** > **CEIP**.



CEIP data collected from AppDNA

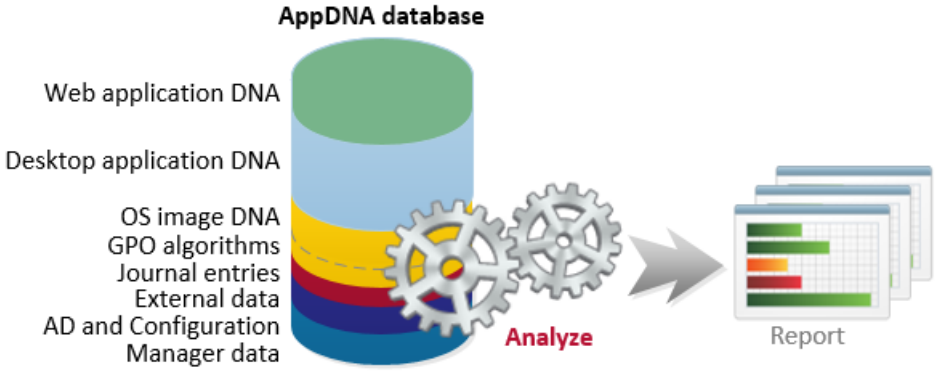
The following table gives examples of the type of anonymous information collected. The data does not contain any details that identify you as a customer.

Application Counts	A count of each of the different types of application present in AppDNA. For example, InstallCapture, SelfProvisioning, Web App, App-V, MSI.
Client OS	A string identifying the OS version on which the AppDNA client is running.
Server OS	A string identifying the OS version on which the AppDNA web site is running.
SQL Server Version	A string identifying the SQL Server version hosting the AppDNA Database.
Custom OS image count	A counter specifying how many OS snapshots are present in addition to the default snapshots supplied.
Account types	A count the number of each type of user or account used to access the database. For example, AD linked, Standard, User, Administrator, Custom.
Feature usage	List of strings denoting which features have been accessed.
Report usage	List of strings denoting which reports have been accessed.
Solutions	List of strings denoting which solution templates have been used to create solutions.
AppDNA version	The version number of AppDNA being used.

Analyze

June 17, 2019

Application analysis is a dedicated SQL Server database process that combines all of the information AppDNA has about the application, analyzes it against each selected target technology, and generates the report data.



Typically you only need to analyze applications once. However, you may need to re-analyze applications if you customize reports or import additional operating system (OS) images. Similarly if you decide to assess your applications for another technology, you will need to analyze the applications for the relevant report.

For desktop applications, you analyze applications after import. You can also choose which modules to analyze.. Alternatively, import the applications without analysis.

For web applications, Analysis can be run after the import has finished.

To select the applications to analyze:

- From the side bar, choose Import & Analyze > Analyze to open the Analyze applications screen. Then select the applications that you want to analyze.
- In the Import Applications or Import Web Applications screen, select the applications you want to analyze after they have loaded successfully.
- In the Application List screen, select the applications that you want to analyze.
- In the Manage Groups screen, select the groups and/or applications that you want to analyze.

To start the analysis: Click Analyze on the toolbar and choose the reports and licensing option to use in the analysis. The upper part of the screen shows the progress through the algorithms in each report. The lower part of the screen shows a detailed log.

To view a report: Select it and click Finish. Alternatively, you can view reports later, from either the Application List or the Reports: Applications section of the side bar.

Which Reports?

August 1, 2018

Reports control the analysis that is performed on the selected applications. Reports are grouped into modules, each of which is a collection of reports for a particular context. For example, the Desktop Compatibility module contains the Windows 7 and Windows 8 reports. Each report is made up of a

suite of algorithms that relate to a target technology against which the application DNA is evaluated. The algorithms validate the suitability, interoperability, conflicts, and performance of applications in the target environment. Each algorithm identifies applications that potentially have a specific issue on the target platform. Applications that are identified as having this issue are said to trigger the algorithm.

Which reports are available as options to select when you analyze your applications depend on your license, which reports are active, and whether you select desktop applications, web applications, or a mixture of both:

- If you select only desktop applications, the web application compatibility reports are not shown.
- If you select only web applications, the desktop application compatibility reports are not shown.
- If you select a mixture of desktop and web applications, all of the active reports are shown.
- All of the active custom reports are shown regardless whether you select desktop or web applications.

The Firefox, Internet Explorer, and Citrix Secure Web reports only analyze web applications and ignore any desktop applications in the selection. All of the other reports (with the exception of any custom reports) only analyze desktop applications and ignore any web applications. Custom reports analyze both desktop and web applications. You therefore need to make sure that you select appropriate applications before selecting custom reports for analysis. Citrix recommends that you indicate in the name of custom reports whether they are for web or desktop applications.

AppDNA identifies an application as a web or desktop application by the way that it is imported into AppDNA. Applications that are imported through the Import Web Applications screen are considered to be web applications. All other applications are considered desktop applications.

Standard AppDNA reports

August 3, 2018

Reports control the analysis that is performed on the selected applications. Each report is made up of a suite of algorithms that relate to a target technology against which the application DNA is evaluated. The algorithms validate the suitability, interoperability, conflicts, and performance of applications in the target environment. Each algorithm identifies applications that potentially have a specific issue on the target platform. Applications that are identified as having this issue are said to trigger the algorithm.

This section provides an overview to the standard AppDNA reports. You can also define your own reports by creating custom reports.

Windows 10

Description	Tests desktop applications for compatibility with editions of Windows 10 for the x86 and x64 architectures. In order to reduce the number of false positives in Windows 10 migration reports, algorithms trigger only when the specific legacy and target OSs introduce the break. For example, algorithms that trigger between Windows XP and Windows 7 because a component was removed in Windows 7 will also trigger between XP and 10 but do not trigger when analyzing between Windows 7 and 10. The assumption is that if your application is already working on Windows 7, it is not a real issue.
Restrictions	AppDNA does not support the import or testing of Windows Store apps, nor compatibility testing for Windows RT. The Windows 10 report tests the compatibility of traditional Windows desktop applications, such as applications that are based on the Windows API (Win32 API).
OS images	Analyzes against the legacy and target OS images

Windows 8/8.1

Description	Tests desktop applications for compatibility with editions of Windows 8/8.1 for the x86 and x86-64 architectures.

Restrictions	Windows 8 introduced a new application run-time environment called the Windows Runtime (WinRT). Applications written for this environment are called Windows Store apps and they work on x86-64 editions of Windows 8/8.1 and editions of Windows 8/8.1 (such as Windows RT) that run on tablets and other devices that are based on ARM chips. AppDNA does not support the import or testing of Windows Store apps, nor compatibility testing for Windows RT. The Windows 8/8.1 report tests the compatibility of traditional Windows desktop applications, such as applications that are based on the Windows API (Win32 API).
OS images	Analyzes against the legacy and target OS images

Windows 7 SP1

Description	Tests desktop applications for compatibility with Windows 7 SP1.
OS image	Analyzes against the legacy and target OS images

Windows Server 2016

Description	Tests desktop applications for compatibility with Windows Server 2016.
Restrictions	The Windows Server 2016 report tests the compatibility of traditional Windows desktop applications, such as applications that are based on the Windows API (Win32 API). This report does not test the compatibility of Windows Store apps.
OS image	Analyzes against the legacy and target OS images

Windows Server 2012/2012 R2

Description	Tests desktop applications for compatibility with Windows Server 2012/2012 R2.
Restrictions	The Windows Server 2012/2012 R2 report tests the compatibility of traditional Windows desktop applications, such as applications that are based on the Windows API (Win32 API). This report does not test the compatibility of Windows Store apps.
OS image	Analyzes against the legacy and target OS images

Windows Server 2008 R2 SP1

Description	Tests desktop applications for compatibility with Windows Server 2008 R2 SP1.
OS image	Analyzes against the legacy and target OS images

App-V

Description	Tests desktop applications for suitability with Microsoft Application Virtualization (App-V) 4.5, 4.6 SP1, or 5.0.
OS image	Does not analyze against an OS image

XenApp Hosted

Description	Tests desktop applications for suitability for deployment in a shared server-hosted environment, such as through XenApp 6and later, XenDesktop 7, or Remote Desktop Services (formerly known as Terminal Services). An application deployed in this way is presented to the user as if it were running on the user's device, but all user actions, such as keystrokes and mouse actions, are relayed back to the application hosted on the server. Potentially many users can use each application simultaneously. This poses a particular set of challenges. Important: When you are moving to a XenDesktop environment from another system, we recommend that you use the XenDesktop Adoption solution instead of the XenApp Hosted report. The XenDesktop Adoption solution provides a more complete picture of application compatibility with XenDesktop based on your current environment. The XenApp Hosted report only indicates if an application that already runs on a server platform will work with XenApp.
OS image	Does not analyze against an OS image

Internet Explorer

Description	Tests web applications for compatibility with 32-bit or 64-bit versions of Internet Explorer 7.0, 8.0, 9.0, 10.0, and 11.
Restrictions	The Internet Explorer 11 and 10 algorithms test compatibility with the desktop browser only and not the Windows Store app style UI that is optimized for touch devices.
OS image	Analyzes against the target OS image

Firefox

Description	Tests web applications for compatibility with all versions of Firefox from Firefox 5 to Firefox 9. Unlike the IE report, you do not need to configure the Firefox report with a specific version. This is because Firefox is a standards-based browser and as such variations between versions tend to be minor.
OS image	Analyzes against the target OS image

Licensing options

August 1, 2018

If you have an evaluation or trial license, when you start an analysis you can choose whether you want AppDNA to automatically apply licenses to applications or whether you want do this yourself manually later. Applying a license to an application enables you to see that application's report views. Before that, these report views are unavailable or locked for the application. Applying a license to an application is therefore called unlocking the application.

If you have purchased a full license, AppDNA always unlocks the applications automatically up to your license limit and the licensing options do not appear in the Analysis screen.

When you are evaluating AppDNA, you typically import more applications than you have licenses for, and then use the EstateView and Effort Calculator to get an overview of the state of your application portfolio. (These provide a consolidated view of the state of all of the applications that have been analyzed for that report, regardless whether the applications are unlocked or not.) Typically you then unlock a few applications to get an understanding of the richness of the detailed information that AppDNA can provide about individual applications.

If you have an evaluation license, the Analysis screen provides the following licensing options:

- **Auto-unlock now**. Select this option if you want AppDNA to automatically unlock the applications during the analysis process. AppDNA then unlocks the applications in the order in which they were imported – up to the license limit.
- **I will unlock the applications later**. Select this option if you want to unlock the applications yourself later - for example, if you want to carefully choose which applications to unlock. You do this in the Apply Licenses screen.

Note: After your license limit is reached, AppDNA does not unlock any more applications automatically during analysis, regardless whether you have an evaluation or full license or which option you select here. However, you can manually unlock a few more applications (up to 10% of your total limit) in the Apply Licenses screen. This additional allowance is called the license reserve.

Operating systems

August 1, 2018

Some AppDNA algorithms analyze application DNA against one or more operating system (OS) images. Those algorithms:

- Test applications for dependencies on features that are provided by the OS.

  When relevant, these algorithms interrogate the OS image DNA that has been loaded into the AppDNA database. For example, the Internet Explorer report checks the registry entries in the Windows OS image to see whether relevant ActiveX components are registered.

- Analyze application DNA against an image from the OS family you are migrating from and the one you are migrating to.

  The analysis shows the effects of changes when applications are migrated between platforms. AppDNA provides a set of default OS images for each relevant OS family. You can also import your own custom OS images.

Best practices

- Import into AppDNA the actual OS images that you deployed on the legacy platform and plan to deploy on the target platform. See Operating system images for more information.
- For each OS family, set your main OS image as the default OS image for that family. See OS image settings for more information.
- Verify that the default legacy OS is what you intend. For Windows XP and Windows Server 2003, the default image is 32-bit. For Windows 8.1, Windows 7, Windows Server 2012, and Windows Server 2008, the default image is 64-bit. To change the default, go to Edit > Settings > OS Image Configuration.

OS image-dependent algorithms

Algorithms that test applications for dependencies on features provided by the OS are referred to as OS image-dependent algorithms. These algorithms check a variety of OS image information, including:

- APIs
- Certificate store
- File management system for each fixed drive partition
- Group Policy Objects (GPOs)
  Note: Incompatibility with enabled GPOs is one of the main reasons why an application might fail after it is moved to a different OS build. AppDNA GPO check include policies that prevent access to 16-bit applications, prevent Control Panel applets from running, restrict internet communication, restrict or disable Windows installer, and prevent IIS installation.
- Registry information
- Some permissions compatibility settings

Most of the OS image-dependent algorithms simply check the OS images in the target OS family. When you analyze your applications for a report that contains an OS image-dependent algorithm, AppDNA checks the information in every OS image in the relevant OS family that has been imported into AppDNA.

The algorithm results might differ for each OS image. Therefore when you view the results in one of the report views, the algorithm results and the application's overall RAG status may change depending on which OS image you select.

OS image delta algorithms

When you import an OS image into AppDNA, you specify whether it is a legacy or target OS image and its relationships with the other OS images that have been loaded into AppDNA. For example, suppose you are working on a migration from Windows 7 to Windows 10 and your organization has standard laptop images for Windows 7 and Windows 10. When you import them into AppDNA, you would define:

- The Windows 7 laptop image as the legacy image for the Windows 10 laptop image
- The Windows 10 laptop image as the target image for the Windows 7 laptop image

AppDNA then calculates and stores information about APIs, features, GPOs, and other settings that are in the legacy image but not in the target image. This is referred to as the OS image delta.

The OS image delta algorithms detect applications that rely on features in the OS image delta and are likely to fail on the target platform. When you analyze your applications for a report that contains an OS image delta algorithm, AppDNA checks the OS image delta for every pair of relevant OS images (Windows 7 and Windows 10 in the example) that have been configured as legacy and target OS images for each other. Therefore when you view the results in one of the report views, the results may change depending on which legacy and target OS images you select. Typically you would set up your main (base or "gold") OS image for an OS family as the default OS image for that OS family.

Some of the OS image delta algorithms also check the application portfolio for applications that supply the missing features. The algorithm portfolio in this context is all of the applications that have

been imported into AppDNA when the analysis is run. For example, suppose Windows 7 supplies a particular DLL that Windows 10 does not supply by default. This means that applications that rely on that DLL will not work by default on Windows 10. However, sometimes the DLL might be installed automatically with another application.

Typically the OS image delta algorithms come in pairs:

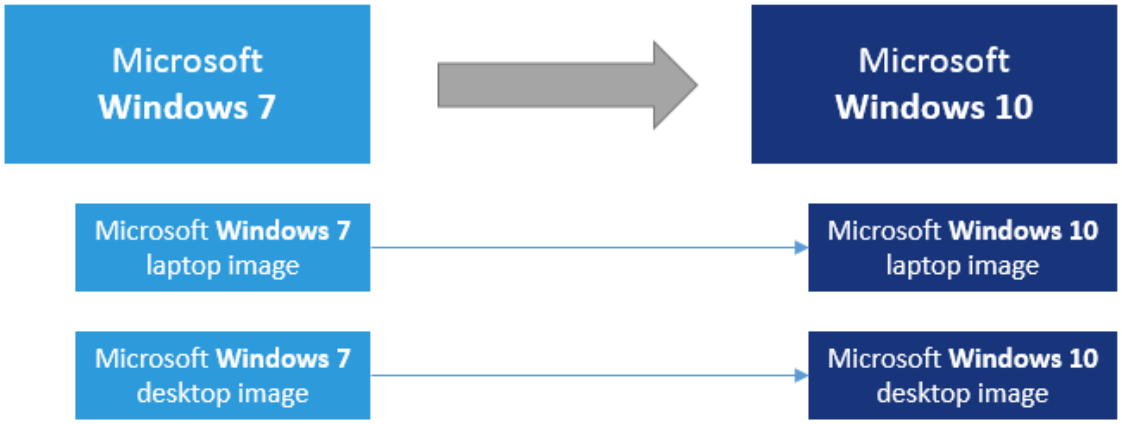
- One identifies applications that rely on features that were provided by the legacy OS image but that are not provided by the target OS image or any of the other applications in the portfolio.
- The other identifies applications that rely on features in the OS image delta that are provided by one or more of the other applications in the portfolio. The remediation report views show which features are required and which applications provide them.

Because the results for both algorithms in the pair depend on which other applications have been imported, the results may change if you re-analyze your applications after you have imported more applications.

Custom image imports

By importing your own images, AppDNA can base its analysis on the images you actually use in your environment rather than the default images. You can optionally import more than one image for each OS family. This is useful when your organization has two (or more) corporate builds of the OS: one for laptops and one for desktops, for example.

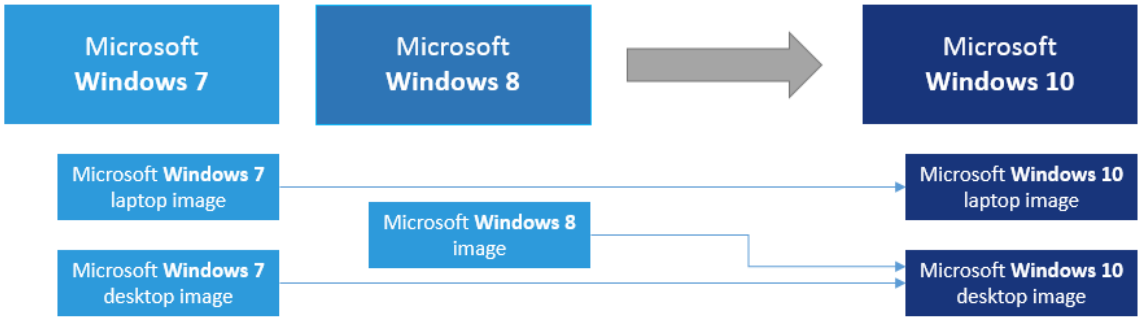
After you import one of your own OS images, you specify its relationships with the other images that have been imported. For example, suppose you are working on a migration from Windows 7 to Windows 10 and your organization has standard laptop and desktop images for both of those OSs. You would import the four images and configure them to define the Windows 7 laptop image as the legacy image for the Windows 10 laptop image, and the Windows 7 desktop image as the legacy image for the Windows 10 desktop image. The following diagram represents these relationships.



Then when you analyze your applications for the Windows 10 report, AppDNA compares the changes between the Windows 7 and Windows 10 laptop images and between the Windows 7 and Windows 10 desktop images. To view the reports, you choose whether you want to view the report for the laptop images or the desktop images.

You also define the default OS image or pair of OS images for each report that performs OS image analysis. You do this in OS Image Configuration Settings.

You can define more than one legacy OS. Specify legacy operating systems in the Configure Modules Wizard.



Application dependencies

August 7, 2018

Whether you use XenApp, XenDesktop, or another method to deploy applications to users, knowing what is required to correctly deliver an application is essential for a successful rollout. AppDNA report algorithms analyze whether the applications, application frameworks, and files required by an application are present. The standard Application Remediation Report includes any missing dependencies and the Application Issues Report compiles all dependent application RAGs.

Suppose that for a suite of financial applications, App1 calls App2, which requires Microsoft Foundation Classes (MFC) and calls App3. AppDNA analyzes those application dependencies and allows you to create dependencies manually or based on suggested dependencies that AppDNA derives by matching missing files or API calls to the runtimes that provide them. The built-in application dependency map includes common libraries and frameworks such as the Visual Studio C++ and Visual Basic run time libraries, as well as applications such as web browsers, SQL Server, and web service connections. If you are aware of other application dependencies, perhaps from information provided by System Center Configuration Manager, you can use the AppDNA SDK to manage those relationships.

View dependencies

1. In the Application List, click an application to select it and then right-click it and choose Properties.
2. Click the Dependencies tab and then click the View Dependencies icon. The icon toggles between a list of applications that require or are required by the selected application(s).

Use a suggested dependency

1. In the Application List, click an application to select it and then right-click it and choose Properties.
2. Click the Dependencies tab and then click Suggestions.
3. Select an item and then click Link Applications.

Define a dependency

1. In the Application List, click an application to select it and then right-click it and choose Properties.
2. Click the Dependencies tab and then click New.

   The Applications tab and the System Frameworks tab list items that are in the AppDNA database.
3. To specify a dependency on an application or a system framework, select the corresponding tab, select an item, and then click OK.

Queue processor

August 1, 2018

The AppDNA queue processor manages a processing queue on the AppDNA server. This reduces the likelihood of deadlocks and resource contention when there are multiple, simultaneous import and analysis processes.

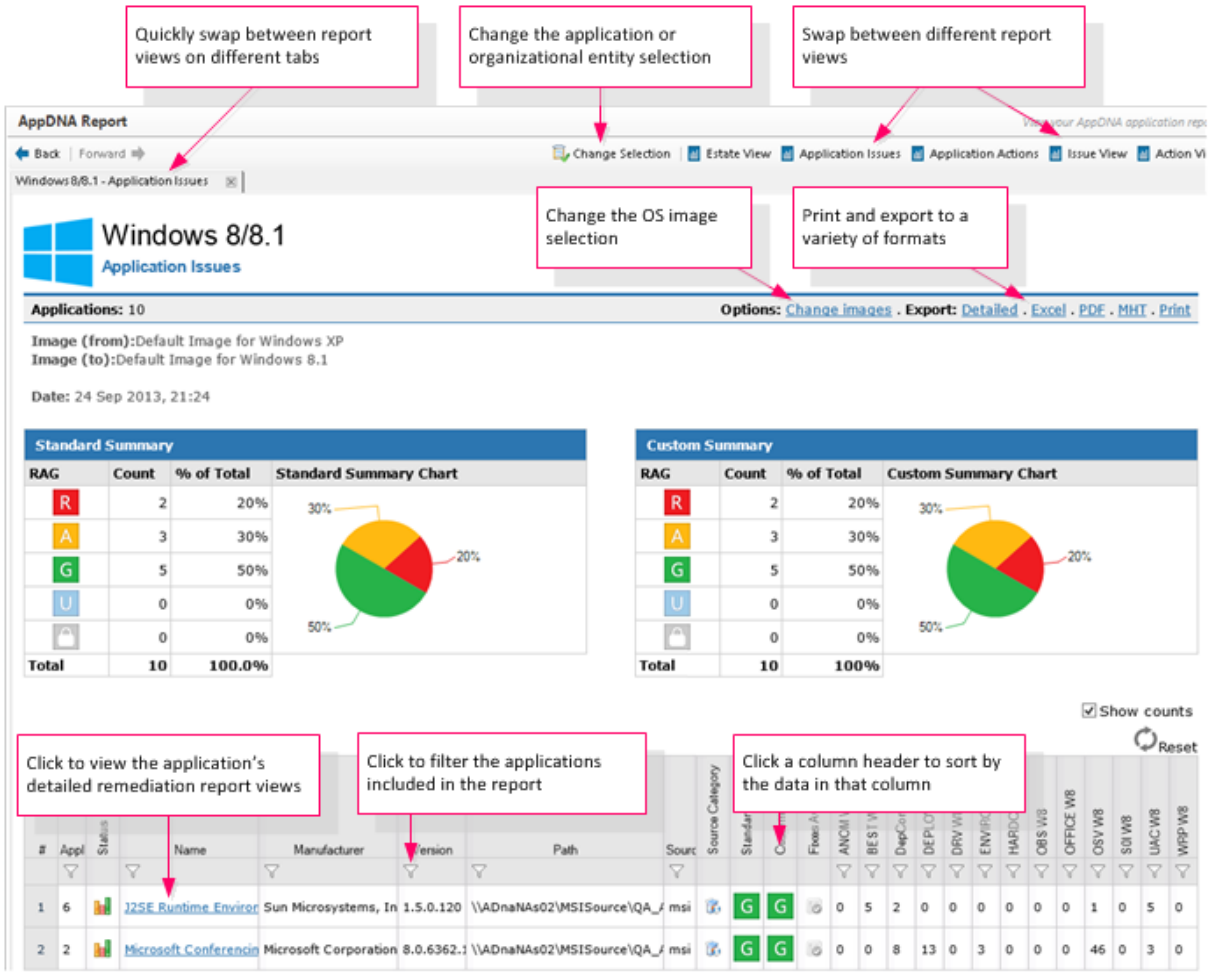
> **Note**
>
> If the Queue Processor has been turned off, depending on the user account under which the AppDNAAppPool is running, the server may not have the permissions to detect and notify the client.
>
> If your application import or analysis is not starting, check the status of the Queue Processor

> (lower right-hand corner of the Import Applications page) and the status of the Citrix AppDNA Service. Restart the Citrix AppDNA Service manually if neccesary.

Report views

June 17, 2019

Analysis results are presented in report views, such as the Overview Summary, Application Issues, and Issue View. The annotations in the following sample report describe the tasks you can perform while viewing a report.



Overview Summary

The Overview Summary is a dashboard that provides a high-level view of the state of your application portfolio. For each of the selected applications, it shows the overall RAG (red, amber, green) status for

each of the active reports. Click the RAG icons to go to the Remediation report views for an application. These give the full details of the remediation required along with an MST fix where applicable. For the lower-level Remediation report views, see Remediate application issues.

For information about the RAG icons, see Understanding RAG Icons.

Application Issues

Application Issues provides a summary of the issues found in the selected applications. Pie charts summarize the standard and custom RAG status of the items included in the report.

A list of the applications shows for each application the standard and custom RAG status and whether AppDNA provides an automatic fix. The Source and Source Category columns indicate the installation type and the Status column indicates whether the application analysis for this report is up to date.

Depending on whether you select the Show counts check box, this report view also shows the number of times the application triggered an algorithm in each of the algorithm groups in the report. An application can trigger an algorithm multiple times because multiple components within the application can each trigger the same algorithm. The application name is a link that takes you to the Remediation report views.

Application Actions

In the Application Actions, a pie chart summarizes the RAG status of the selected applications before and after the remediation actions.

A list of the selected applications shows for each application the before and after action RAGs and indicators of the application complexity and action effort. The action effort is categorized as easy, medium, hard, or no remediation is required. The action effort is associated with the remediation actions and can be customized, as described in Configure algorithms.

Using the information in Application Actions, you can quickly see which applications are ready for user acceptance testing (UAT), because these applications have green before and after action RAGs. Applications that are probably not suitable for migration have a red after action RAG, and those that require some remediation work before migration have an amber or red before action RAG and a green or amber after action RAG. When remediation is required, the application complexity and the action effort provide a rough indication of the amount of work involved.

Depending on whether you select the Show counts check box, this report view also shows the number of issues that require remediation, broken down by the various remediation action types. The application name is a link that takes you to the Remediation report views.

Issue View

Issue View provides a breakdown of the number of applications that triggered each algorithm within the report. It includes a pie chart summary of the standard, custom, and after action RAG status of the applications included in the report. AppDNA does not show the custom RAG pie chart if the custom RAGs are the same as the standard RAGs for all of the report's algorithms.

A bar chart shows the number of applications that have triggered one or more algorithms in each algorithm group.

A list of the algorithms includes the standard, custom, and after action RAGs, whether a fix is available, and the number of applications that are affected. You can expand each algorithm to show a list of the affected applications and an explanation of both the algorithm and its remediation actions. The application name is a link that takes you to the Remediation report views.

Action View

The Action View provides a breakdown of the prevalence of the actions required to remediate the applications in your portfolio. It includes a pie chart summary of the standard, custom, and after action RAG status of the applications included in the report. AppDNA does not show the custom RAG pie chart if the custom RAGs are the same as the standard RAGs for all of the report's algorithms.

A bar chart shows the number of applications that require each type of remediation.

The view includes a list of the remediation action types and subtypes (also known as actions and action details), the after action RAG, and the number of applications that require this type of remediation. You can expand each individual action and action detail combination to show a list of the associated applications. The application name is a link that takes you to the Remediation report views.

Estate View

The Estate View, available for trial licenses only, provides a high-level overview of the consolidated status of the entire application portfolio for a target technology. This report is useful when you are evaluating AppDNA, because it does not rely on individual application licenses.

The Estate View includes a pie chart summary of the standard, custom, and after action RAG status of the applications in the portfolio. AppDNA does not show the custom RAG pie chart if the custom RAGs are the same as the standard RAGs for all of the report's algorithms.

A bar chart shows the number of applications that have triggered one or more algorithms in each algorithm group.

A list of the algorithms includes the standard and custom RAGs, whether AppDNA provides an automatic fix, and the number of applications that are affected. You can expand each algorithm to show an explanation of both the algorithm and its remediation actions.

View the reports

1. From the AppDNA side bar, click Reports: Applications.
2. In the Application List screen, select the applications you want to include in the report.
3. Do one of the following:

- On the toolbar in the Application List, select the report you want to view in the drop-down list and click View Report.
- From the AppDNA side bar, choose Reports: Applications > Module > Report > Report view, where Module, Report and Report view identify the report view that you want to see.

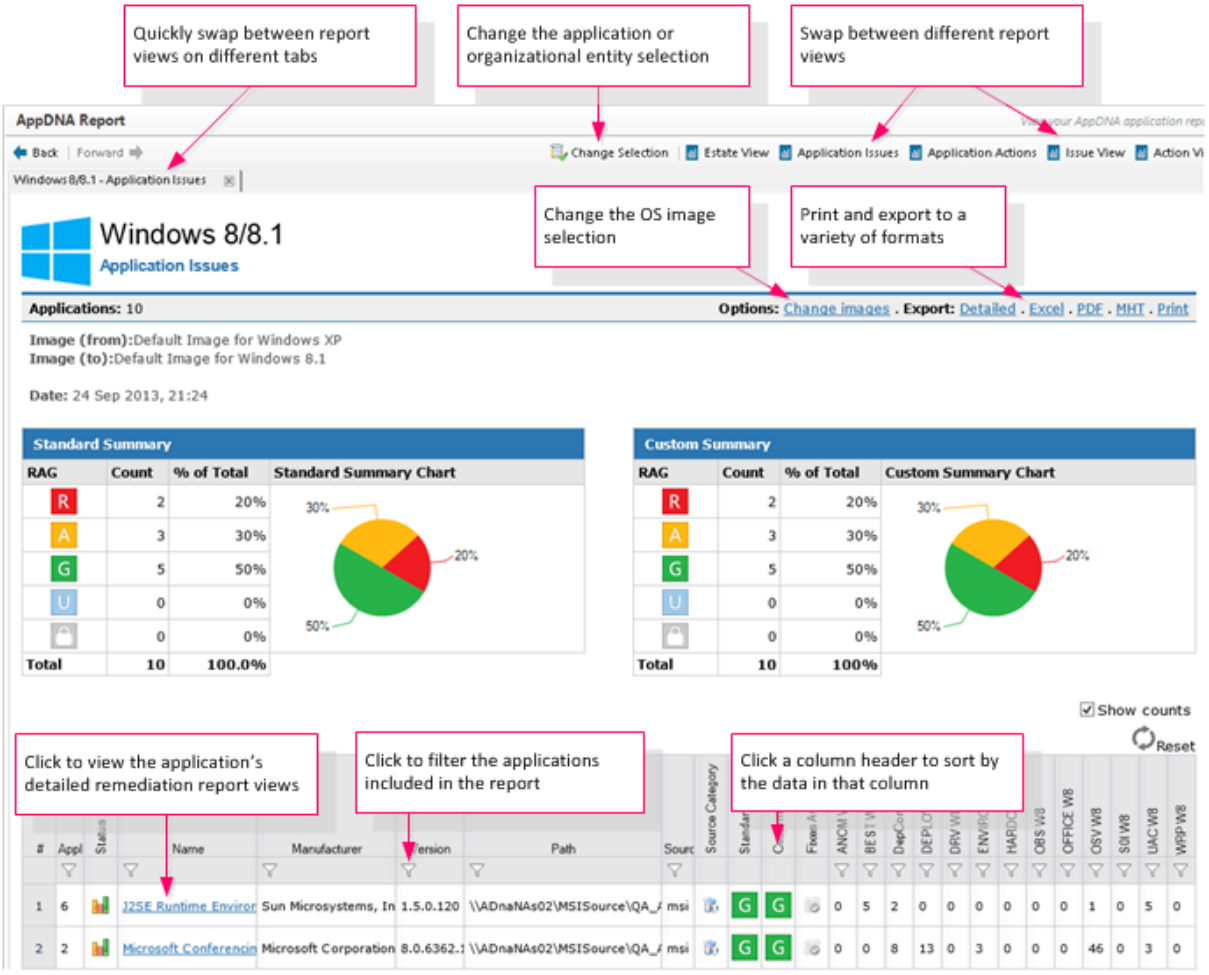
After you have opened a report view, you can use the links in the top right corner of the screen to move to a different report view for the same report.

You can view reports in multiple tabs within AppDNA. This makes it easy to switch between different reports and report views quickly. You can also open a report in a browser window.

- To open a report view in a new tab: On the side bar, right-click the report view you want to view, and from the shortcut menu, choose Open in New Tab.
- To open a report view in a browser window: On the side bar, right-click the report view you want to view, and from the shortcut menu, choose Open in New Window.

Features

August 7, 2018



Note: The
Estate View link, available for evaluation and trial installations only, provides a summary for all relevant applications in the portfolio, regardless of which applications are selected.

Use the options on the main toolbar to swap between different report views.

Open the Remediation report views by drilling down through the application name in one of the other report views, such as the Application Issues view.

Use the Change images link on the Export toolbar to change the OS images that are selected. The link does not appear for reports for which OS images are not relevant. To define the default OS images for reports, use the OS image settings.

Use the Export links to print the report or export it to a variety of formats. The formats that are available depend on the report view type. The options include MHT (a single-file Web page, which you can view in a browser and is easy to send to colleagues), HTML (a single Web page with a separate folder that contains the associated images and other files), Word, Excel, and PDF (Application Issues view only). Use the Report Export Wizard to perform bulk exports.

Click a column header to sort by the data in that column. Click the header again to swap between

ascending and descending order. Drag the vertical bars between the column headings to resize the columns. Click Reset to revert to the default sort order and column sizes.

Use the Show counts check box on the Application Issues and Application Actions report views to show and hide additional columns that show the number of times the application has triggered an algorithm in each algorithm group and the number of applications that require each type of remediation action, respectively.

Click a filter icon (immediately below a column header) to filter by the data in that column. For example, suppose you want to see only Adobe applications in the Application Actions report view. To do this, click the filter icon under the Manufacturer column header, select Contains from the drop-down list, and enter Adobe in the text box. Similarly if you want to restrict the results to applications that need redevelopment, you could create a "greater than zero" filter on the REDEV column. (To see this column, you need to select the Show counts check box.)

You can view application report views in a browser window. To do this: on the side bar, right-click the report view you want to view and from the shortcut menu, choose Open in New Window.

Which applications are included?

The applications included in the application report views are based on the applications you selected previously - for example, in the Application List or Import Applications screens, or the groups you selected in the Manage Groups screen. You can change the selected applications in the Application List screen or by clicking Change Selection on the Report Viewer toolbar.

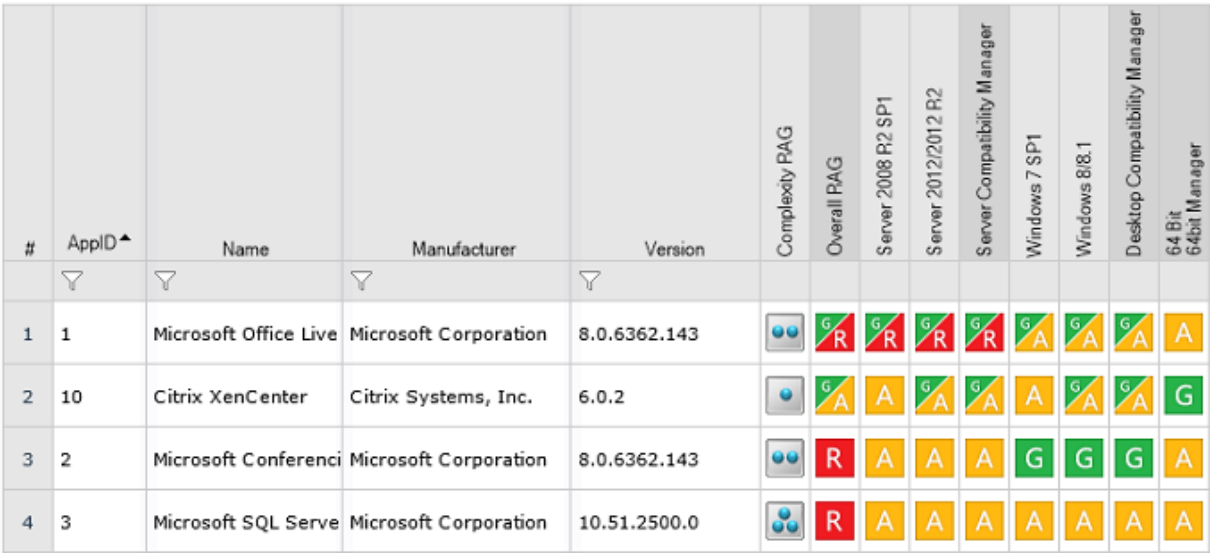
The top of relevant report views show the number of applications selected. If any groups were selected, their names are also shown. An asterisk (*) next to a group name means that the group has changed since the selection was made (for example, some more applications have been added to it).

Note: The above does not apply to the
Organization reports, which show the status of applications that are managed through Active Directory or System Center Configuration Manager.

Understanding RAG Icons

August 2, 2018

AppDNA uses red, amber, and green icons (referred to as RAGs) to indicate application compatibility status. For example, here is a snippet from the Overview Summary report view, which lists applications and shows RAG icons to provide an indication of the overall compatibility status for each of the active reports.



#	AppID	Name	Manufacturer	Version	Complexity RAG	Overall RAG	Server 2008 R2 SP1	Server 2012/2012 R2	Server Compatibility Manager	Windows 7 SP1	Windows 8/8.1	Desktop Compatibility Manager	64 Bit 64bit Manager
1	1	Microsoft Office Live	Microsoft Corporation	8.0.6362.143		R	R	R	R	A	A	A	A
2	10	Citrix XenCenter	Citrix Systems, Inc.	6.0.2		A	A	A	A	A	A	A	G
3	2	Microsoft Conferenci	Microsoft Corporation	8.0.6362.143		R	A	A	A	G	G	G	A
4	3	Microsoft SQL Serve	Microsoft Corporation	10.51.2500.0		R	A	A	A	A	A	A	A

This topic provides a summary of the various RAG icons and their meanings, and the different types of RAGs. It also provides information about how the RAG icons are translated into text in some of the exports and the ToolTips that appear when you move the mouse over a RAG icon in the Application Issues report view, for example.

RAG icons

AppDNA analysis indicates that the application is likely to work on the target platform as it is and is ready for user acceptance testing (UAT).

AppDNA analysis indicates that the application may fail or have impaired functionality, although remediation is possible.

AppDNA analysis indicates that the application is likely or certain to fail and the application may need redevelopment.

The lower right side of the icon shows the AppDNA RAG status and the overlay on the upper left side provides an alternative compatibility status that is derived from outside of AppDNA from an external data source. The image shown here is a standard amber RAG with a green overlay. This means that although the AppDNA analysis suggests that the application may have issues on the target technology, the external data source indicates that the application is compatible - perhaps because it will be shimmed automatically at run time. All other combinations of AppDNA RAG status and external data status are possible (for example, a red overlay on a green RAG, an amber overlay on a green RAG, and a red overlay on a red RAG).

 The compatibility status has been manually set to green through the AppDNA journal - for example, because testing indicates that the application works on the target technology.

 The compatibility status has been manually set to amber through the AppDNA journal - for example, because testing indicates that the application has issues on the target platform.

 The compatibility status has been manually set to red through the AppDNA journal - for example, because testing indicates that the application is incompatible with the target platform.

The status is unknown because not enough data is available - typically because the application has not been analyzed for the report. Desktop applications have this status for the web application reports and web applications have this status for the Windows application reports.

The application is unlicensed (locked) for the report. For information about unlocking applications, see Apply Licenses.

RAG types

For each report, an application has three possible RAG statuses, as shown in the following table.

RAG Type	Description
Standard	This shows the application's overall compatibility status for a particular report and is based on the algorithms built into the report. The highest RAG status of all of the algorithms that the application has triggered becomes the overall RAG status of the application for that report. The RAG icon may be modified by external data or journal entries as described above.
Custom	By default, this is the same as the standard RAG but you can customize it to meet the needs of your enterprise (for example, you can raise an amber status to red or lower it to green). Like the standard RAG, the custom RAG icon can also be modified by external data and journal entries as explained above.

RAG Type	Description
After action	Shows the expected status after the remediation actions have been implemented. For example, if the standard RAG is amber but remediation options are available, the after action RAG is typically green. However, if the standard RAG is red and the only remediation option is to redevelop the application, the after action RAG is also red to indicate that complex development and/or replacement is required.

Complexity RAGs

Some of the application report views also show the application's complexity "RAG". This provides an indication of the complexity of the application. The complexity is based on the number of files and registry entries the application has. You can set thresholds for the three complexity levels in Reporting settings.

 A relatively simple application.

 An application of medium complexity.

 A complex application.

Tooltips

When you move your mouse over a RAG icon in the Application Issues and Application Actions report views, a ToolTip provides a text version of the RAG icon. The same texts are used to represent the RAG icons in some of the report exports. When a RAG icon has been modified by an external data entry, the status from the external data is shown in brackets, like this:

```
Red (Green external)
```

When a manual journal entry or an external data entry applies, it is shown at the beginning of the text (because it overwrites the AppDNA RAG). The RAG provided by AppDNA follows in brackets. For example:

```
Green journal (Amber RAG)
```

```
Green external (Amber RAG)
```


Application reports

August 7, 2018

This topic summarizes the top-level application report views.

For the lower-level Remediation report views, see Remediate application issues.

Overview Summary

The Overview Summary report view is a dashboard that provides a high-level view of the state of your application portfolio. For each of the selected applications, it shows the overall RAG (red, amber, green) status for each of the active reports. You can click the RAG icons to go to the Remediation report views for that application. These give the full details of the remediation required along with an MST fix where applicable.

For information about the RAG icons, see Understanding RAG Icons.

EstateView

The EstateView, available for evaluation and trial installations only, provides a high-level overview of the consolidated status of the entire application portfolio for a target technology. This report is useful when you are evaluating AppDNA, because it does not rely on individual application licenses.

The EstateView starts with a pie chart summary of the standard, custom, and after action RAG status of the applications in the portfolio. (AppDNA does not show the custom RAG pie chart if the custom RAGs are the same as the standard RAGs for all of the report's algorithms.)

Below the pie charts there is a bar chart that shows the number of applications that have triggered one or more algorithms in each algorithm group. The number of applications is shown as a count and a percentage of the application portfolio. The bar chart is followed by a list of the algorithms. This shows the algorithm ID, name, and algorithm group, along with the standard and custom RAGs, whether AppDNA provides an automatic fix, and the number of applications that are affected. You can expand each algorithm to show an explanation of both the algorithm and its remediation actions.

Application Issues

The Application Issues report view provides a summary of the issues found in the selected applications. The view starts with pie chart summaries of the standard and custom RAG status of the items included in the report.

The pie charts are followed by a list of the applications included in the report. For each application, the report shows the standard and custom RAG status, and whether AppDNA provides an automatic fix. The Source and Source Category columns indicate the installation type, and the Status column shows an icon indicating whether the application's analysis for this report is up to date.

Depending on whether you select the Show counts check box, this report view also shows the number of times the application triggered an algorithm in each of the algorithm groups in the report. (An application can trigger an algorithm multiple times – because multiple components within the application can each trigger the same algorithm.)

The application name is a link that takes you to the detailed Remediation report views for the application. Below the list of applications there is a list of algorithm groups and a legend that explains the icons.

Application Actions

The Application Actions report view starts with a pie chart summary of the RAG status of the selected applications before and after the remediation actions.

The pie charts are followed by a list of the selected applications. For each item, the report shows the before and after action RAGs, and indicators of the application complexity and action effort. The action effort is categorized as easy, medium, hard, or no remediation is required. The action effort is associated with the remediation actions and can be customized in the Algorithm Groups screen. See Configure algorithms for more information.

Using this information, you can quickly see which applications are ready for user acceptance testing (UAT), because these applications have green before and after action RAGs. Applications that are probably not suitable for migration have a red after action RAG, and those that require some remediation work before migration have an amber or red before action RAG and a green or amber after action RAG. When remediation is required, the application complexity and the action effort provide a rough indication of the amount of work involved.

Depending on whether you select the Show counts check box, this report view also shows the number of issues that require remediation, broken down by the various remediation action types.

The application name is a link that takes you to the Remediation report views.

Issue View

The Issue View provides a breakdown of the number of applications that triggered each algorithm within the report. This view starts with a pie chart summary of the standard, custom, and after action RAG status of the applications included in the report. (AppDNA does not show the custom RAG pie chart if the custom RAGs are the same as the standard RAGs for all of the report's algorithms.) Below

the pie charts there is a bar chart that shows the number of applications that have triggered one or more algorithms in each algorithm group. The number of applications is shown as a count and a percentage of the portfolio (which here means the applications included in the report).

The bar chart is followed by a list of the algorithms. This shows the algorithm ID, name, and algorithm group, along with the standard, custom, and after action RAGs, whether a fix is available, and the number of applications that are affected. The number of applications is shown as both a count and a percentage of the applications included in the report.

You can expand each algorithm to show a list of the affected applications, and an explanation of both the algorithm and its remediation actions. The application name is a link that takes you to the Remediation report views.

Action View

The Action View provides a breakdown of the prevalence of the actions required to remediate the applications in your portfolio. This view starts with a pie chart summary of the standard, custom, and after action RAG status of the applications included in the report. (AppDNA does not show the custom RAG pie chart if the custom RAGs are the same as the standard RAGs for all of the report's algorithms.) Below the pie charts there is a bar chart that shows the number of applications that require each type of remediation. The number of applications is shown as a count and a percentage of the portfolio (which here means the applications included in the report).

The bar chart is followed by a list of the remediation action types and subtypes (also known as actions and action details) along with the after action RAG and the number of applications that require this type of remediation. The number of applications is shown as both a count and a percentage of the applications included in the report.

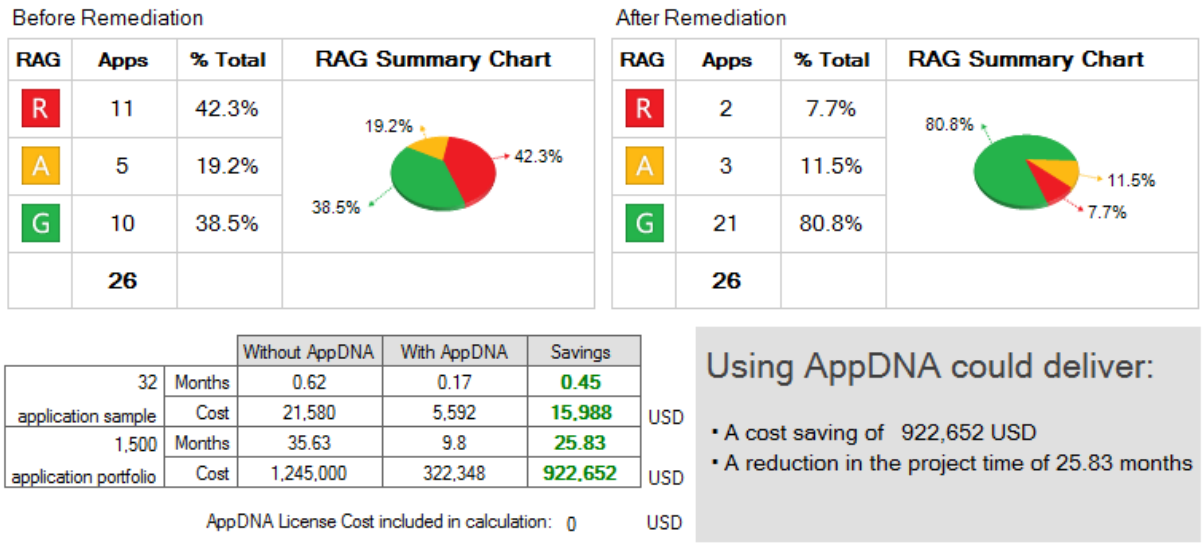
You can expand each individual action and action detail combination to show a list of the associated applications. The application name is a link that takes you to the Remediation report views.

Effort Calculator

August 3, 2018

Use the AppDNA Effort Calculator to estimate the time, cost, and effort associated with migrating a portfolio to a new platform – for example, that it will take five people six months and cost $500,000. Effort Calculator uses a number of variables that define, for example, the cost of a tester per day, the number of working hours in the day, and the time to test an application of a given complexity. You can configure the variables to reflect the specifics of your organization. AppDNA produces a detailed

breakdown of the cost and how much time it will take to remediate the applications as well as the potential savings that AppDNA can provide.



To open the Effort Calculator, from the side bar choose Reports: Applications > Effort Calculator.

Using Effort Calculator involves the following steps:

1. Select the report
2. Configure variables and view the results
3. Export the results

1. Select the report

The first step in using Effort Calculator is to select the report that represents the project for which you want to calculate the effort. For example, if you want to calculate the effort for a Windows 7 migration project, select the Windows 7 report. AppDNA lists the available reports on the left side of the screen.

When you select a report, the right side of the screen provides a summary that shows the overall status of the currently selected applications that have been analyzed for that report.

To change the applications that are selected, click Change Selection on the right side of the toolbar. In the Application List, select the applications you want to include and then click Select to apply them.

Note:

Effort Calculator ignores any applications that have not been analyzed or that are stale (need re-analyzing). This can sometimes lead to an apparent discrepancy between the number of applications that you select and the number of applications that are shown. For example, if you select 10 applications but only 8 of them have been analyzed for the selected report, Effort Calculator will show the total number of applications as 8.

- If you select a group and any of the applications in the group are unanalyzed or stale, the name of the group is shown with an asterisk (*) beside it.

Click Next to move to the next step.

2. Configure variables and view the results

The main Effort Calculator screen provides a summary that gives an estimate of the effort required to remediate the applications in the portfolio for which there are known remediations while highlighting applications that require further testing or need to be treated as exceptions. Applications are considered exceptions if remediation is not possible. This means that the application may need to be redeveloped or decommissioned.

The summary includes two pie charts:

- **Before remediation.** The pie chart on the left side shows the current status of the applications.
- **After remediation.** The pie chart on the right side shows the expected status of the applications after the remediation steps have been completed. For example, if the current status of an application is amber but remediation options are available, the after remediation RAG is typically green, which indicates that the application is ready for UAT. However, if the standard RAG is red and the only remediation option is to redevelop the application, the after remediation RAG is also red to indicate that complex development and/or replacement is required. Effort Calculator considers these applications exceptions, because they fall outside of the scope of issues that can be resolved relatively easily. An amber after remediation RAG indicates that the application requires more testing than an application that has a green after action RAG.

Below the summary there are four tabs.

- **Variables.** Provides a variety of variables that are used in the calculation. You can configure to suit the needs of your enterprise. The following table provides information about some of the less obvious variables.

Variable	Description
Number of applications in the full portfolio	Defaults to the number of applications already imported. You can increase this to reflect the size of your actual application portfolio. AppDNA then extrapolates the effort to migrate the entire portfolio, based on the sample results.
Currency	See http://www.xe.com/iso4217.php for a list of international currency codes.

Variable	Description
Smoke testing time	The time in hours to perform an initial install and run test, commonly known as a smoke test. This is not usually an in-depth test. **Default Value:** 8 - Average time to complete the initial test phase with no dependencies on external parties or processes. **Alternative A:** 24 - When enterprise-specific processes are to be taken into account. For example, when the smoke test includes part of the application certification process and so there are time allotments for application owner expertise for installation, documentation, and initial testing. **Alternative B:** 4 - Light smoke-test process with automated installation and an execution script to test functionality at a very high level only.
Applications that are expected to have issues	The number of applications that are expected to have issues as a percentage of the portfolio. The default value is derived from a variety of market sources, from analysts to technical engagement feedback. The value can vary based on enterprise-specific processes and application readiness.

Variable	Description
Applications that are expected to be exceptions	The percentage of applications that cannot be remediated, or where a decision has been made not to remediate. This variable can change dramatically based on the application portfolio's age. An older portfolio typically has a greater percentage of incompatible applications. **Default Value:** 10% - Based on empirical application rationalization data, organizations 'end of life' anywhere between 10% and 30%, depending on enterprise initiatives. Application incompatibility is often a key driver in the retirement decision. If variables such as the portfolio age are unknown, the default value should be used. **Alternative A:** 35% - Enterprise-specific mandates around application lifecycle management can stipulate an aggressive application retirement initiative tied to desktop migrations and refreshes. **Alternative B:** 5% - Enterprise-specific mandates can also be driven around ensuring that all applications are migrated, regardless of the mixtures of platforms necessary to support them.

Variable	Description
Time to identify the cause of a failure and resolve it	A per-application estimate of how long in hours it generally takes to identify a failure and fix it when AppDNA is not in use. **Default Value:** 24 - Average time associated with a typical manual process around application testing and remediation with no external dependencies. Single point of testing and remediation. **Alternative:** 60 - Average time when additional enterprise-specific processes are to be taken into account - such as application owner expertise for installation, in-depth application-to-application testing, application-to-OS image testing from baseline to gold images, with all permutations in between.
Staging time	The average number of hours to install an application in the target environment and ensure it is running.
Size of remediation team	This depends on the size of the application portfolio. Typically, there is one remediation specialist for every 250 applications.
Size of testing/staging team	This depends on the size of the application portfolio. Typically, there is one tester/stager for every 100 applications.

Variable	Description
Remediation time	The rows represent the complexity of applications. AppDNA measures application complexity in terms of the number of files and registry entries. Configurable thresholds define whether an application is considered simple, normal or complex. You can configure the thresholds in Reporting Settings. For more information, see Reporting settings. The columns represent the complexity of the remediation. AppDNA identifies issues in applications by running sophisticated heuristic algorithms during the analysis process. Each algorithm identifies a specific issue and has a recommended remediation action to mitigate that issue. The effort associated with these actions is categorized as easy, medium, or hard. The overall remediation effort for an application is based on the highest effort associated with the algorithms that the application triggers. You can optionally configure the remediation actions in the Algorithm Groups screen. For more information, see Configure algorithms.

- **Results worksheet.** Shows a breakdown of the applications in terms of the type of remediation (easy, medium, and hard) and the application complexity, along with the estimated testing and remediation times.
- **Effort estimation with AppDNA.** Shows an estimation of the total cost of the project if you use AppDNA.
- **Effort estimation without AppDNA.** Shows an estimation of the total cost of the project if you do not use AppDNA.

3. Export the results

You can export all of the Effort Calculator results (along with explanatory information) to a Word document. This requires Microsoft Word to be installed on the same computer as the AppDNA client.

To export this report, click Export on the main toolbar. After a short delay, Microsoft Word opens and displays the exported report.

Export variables

You can export your Effort Calculator variables - as an XML file for later retrieval. This makes it easy to compare different scenarios.

To export your Effort Calculator settings:

1. From the AppDNA menus, choose Administration > Action Administration.
2. On the toolbar in the Action Administration screen, click Export Action Settings.
3. In the Save As dialog box, give the file an appropriate name and save it in an appropriate location.

To import the settings:

1. From the AppDNA menus, choose Administration > Action Administration.
2. On the toolbar in the Action Administration screen, click Import Action Settings.
3. In the Open dialog box, navigate to the file that was previously exported.
4. Click OK.

Variables

August 1, 2018

This topic documents the Effort Calculator variables. You can configure these to meet the needs of your enterprise. When you have finished, click Save on the toolbar at the top of the screen to save the changes.

General variables

These variables customize the report at a high level by defining project-specific information.

Customer name. The name of the company to be used in the report export.

Number of applications in the full portfolio. The total number of applications that you want to migrate to the new platform. This value defaults to the number of applications you have already imported into AppDNA. You can increase this to reflect the size of your actual application portfolio. AppDNA then extrapolates the effort to migrate the entire portfolio from the results for the sample.

Currency – The currency to be used in the report. Typically you express this using the three-character currency code. See http://www.xe.com/iso4217.php for a list of international currency codes.

Working hours per day. The number of hours in a typical working day. This affects all calculations relating to time, and can help improve the accuracy of time estimations.

Average working days in a month. The average number of days in a working month. This allows further refining of the time estimations.

Without AppDNA variables

These variables assist in the accuracy of the project estimation where AppDNA is not being used. This section provides the default values and some alternatives along with explanation about when they might be appropriate.

Smoke testing time. The time in hours to perform an initial install and run test, commonly known as a 'smoke test'. This is not usually an in-depth test.

- **Default Value:** 8 - Average time to complete the initial test phase with no dependencies on external parties or processes.
- **Alternative A:** 24 - When enterprise-specific processes are to be taken into account. For example, when the smoke test includes part of the application certification process and so there are time allotments for application owner expertise for installation, documentation, and initial testing.
- **Alternative B:** 4 - Light smoke-test process with automated installation and an execution script to test functionality at a very high level only.

Applications that are expected to have issues. The number of applications that are expected to have issues as a percentage of the portfolio. The default value is 30%, which is derived from a variety of market sources, from analysts to technical engagement feedback. This varies from organization to organization based on enterprise-specific processes and application readiness.

Applications that are expected to be exceptions. Defines the percentage of applications that cannot be remediated, or where a decision has been made not to remediate. This variable can change dramatically based on the application portfolio's age. An older portfolio typically has a greater percentage of incompatible applications than a new portfolio.

- **Default Value:** 10% - Based on empirical application rationalization data, organizations 'end of life' anywhere between 10% and 30%, depending on enterprise initiatives. Application incompatibility is often a key driver in the retirement decision. If variables such as the portfolio age are unknown, the default value should be used.
- **Alternative A:** 35% - Enterprise-specific mandates around application lifecycle management can stipulate an aggressive application retirement initiative tied to desktop migrations and refreshes.
- **Alternative B:** 5% - Enterprise-specific mandates can also be driven around ensuring that all applications are migrated, regardless of the mixtures of platforms necessary to support them.

Time to identify the cause of a failure and resolve it - This is a per-application estimate of how long in hours it generally takes to identify a failure and fix it when AppDNA is not in use.

- **Default Value:** 24 - Average time associated with a typical manual process around application testing and remediation with no external dependencies. Single point of testing and remediation.
- **Alternative:** 60 - Average time when additional enterprise-specific processes are to be taken into account - such as application owner expertise for installation, in-depth application-to-application testing, application-to-OS image testing from baseline to gold images, with all permutations in between.

With AppDNA variables

AppDNA uses these variables when estimating time and cost for handling the portfolio when AppDNA is in use.

Applications that have MSI installation package. Enter this value as a percentage of the entire portfolio. You import Windows applications into AppDNA using their installation packages. These can be MSI installation packages, App-V .sft or .appv files, or any other type of installation files. MSIs, and .sft and .appv files are more straight-forward to import than other types of installation packages. Effort Calculator takes the figure entered here into account when estimating the time AppDNA will take to process the applications.

AppDNA license cost. This variable can optionally be used to provide a more accurate cost breakdown in the ROI results.

Staffing variables

These variables affect the calculations with and without AppDNA.

Staging time. The average time (in hours) to install an application in the target environment and ensure it is running. The default value is 2 hours.

Size of remediation team. The number of staff that are in the remediation team for the project. This depends on the size of the application portfolio. Typically, there is one remediation specialist for every 250 applications. The default value is 3.

Size of testing/staging team. The number of staff that are in the testing and/or staging team for the project. This depends on the size of the application portfolio. Typically, there is one tester/stager for every 100 applications. The default value is 5.

Remediator cost per day. The average cost per day of remediation staff.

Tester/stager cost per day. The average cost per day of testers and stagers.

Project manager cost per day. The average cost per day of project managers.

Testing and remediation variables

The testing and remediation variables section provides a grid in which you can enter the time it takes to remediate and test applications of different complexities. Enter the time in hours.

Remediation time. Enter the average number of hours it takes to remediate applications of the different complexities.

		Remediation time			Testing time	
Application complexity		Easy	Medium	Hard		
Simple	●	1	2	4	1	hours
Normal	● ●	2	6	8	2	hours
Complex	● ● ●	4	8	24	4	hours

The rows represent the complexity of applications. AppDNA measures application complexity in terms of the number of files and registry entries. Configurable thresholds define whether an application is considered simple, normal or complex. You can configure the thresholds in Reporting Settings. See Reporting settings for more information.

The columns represent the complexity of the remediation. AppDNA identifies issues in applications by running sophisticated heuristic algorithms during the analysis process. Each algorithm identifies a specific issue and has a recommended remediation action to mitigate that issue. The effort associated with these actions is categorized as easy, medium, or hard. The overall remediation effort for an application is based on the highest effort associated with the algorithms that the application triggers. You can optionally configure the remediation actions in the Algorithm Groups screen. See Configure algorithms for more information.

Testing time. Enter the average number of hours it takes to test applications of different complexities.

When you have finished entering the variables, click Save on the toolbar at the top of the screen to save the changes.

Effort Calculator Worksheets

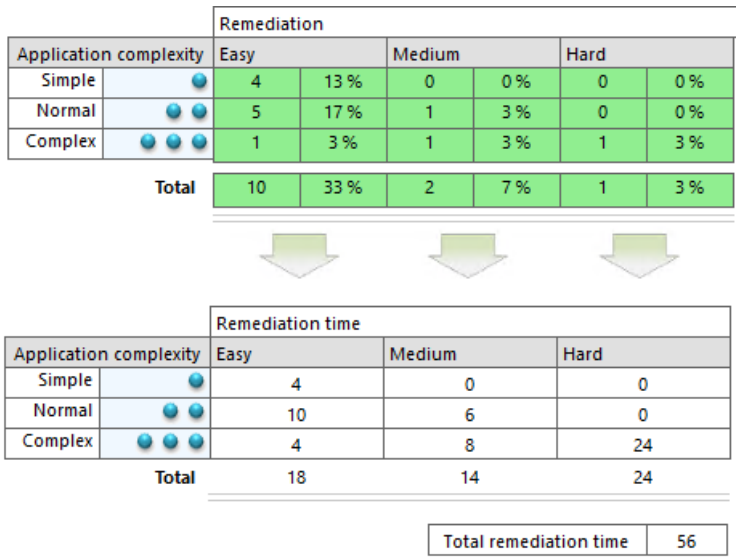
August 1, 2018

Results worksheet

The Results worksheet tab shows:

- The number of applications that require easy, medium, and hard remediation for each application complexity level.
- The number of applications that do not require remediation, broken down into no issues detected (No Issues), need to be tested (To test), and exceptions (Exceptions).
- A breakdown of the remediation and testing hours required for applications that require remediation.
- A breakdown of the number of testing hours required for applications that do not require remediation.
- The total remediation and testing times.

Results worksheet walk through



	Remediation					
Application complexity	Easy		Medium		Hard	
Simple	4	13 %	0	0 %	0	0 %
Normal	5	17 %	1	3 %	0	0 %
Complex	1	3 %	1	3 %	1	3 %
Total	10	33 %	2	7 %	1	3 %

	Remediation time		
Application complexity	Easy	Medium	Hard
Simple	4	0	0
Normal	10	6	0
Complex	4	8	24
Total	18	14	24

Total remediation time	56

In the excerpt from the results worksheet shown above, take a look at the applications that have issues that require an easy level of remediation effort – there are 4 simple applications, 5 normal applications, and 1 complex application.

Now take a look at the “Testing and remediation” variables. This is where you enter the time it takes to remediate applications of different complexities for each of the three categories of remediation effort (easy, medium and hard). Similarly, you enter the time it takes to test applications of the three complexity levels.

The default values for the easy remediation effort are 1 hour for simple applications, 2 hours for normal applications, and 4 hours for complex applications. These values are used to derive the results in the Easy column in the Remediation table:

```
6 simple applications x 1 hour = 6 hours
4 normal complexity applications x 2 hours = 8 hours
3 complex applications x 4 hours = 12 hours
```


AppDNA uses similar calculations to derive the other values in the worksheet.

Effort estimation with AppDNA

The Effort estimation with AppDNA tab shows the total cost of the project using AppDNA, a breakdown of the cost per application, and the remediation and testing times. The report shows results for the selected applications, and extrapolated results for all of the applications in the portfolio.

This tab focuses on applications that were green before remediation (no remediation required), amber after remediation (issues that require testing), and green after remediation (applications with issues for remediation). Applications marked as red are considered exceptions and are not included because they require redevelopment or replacement and fall outside of the scope of issues that can be resolved easily.

The following table explains the table columns:

Column	Description
Applications	The number of applications falling in each of the remediation categories shown on the side ("Green before", "Green after", and "Amber after").
Staging	The time in hours to stage the applications for testing.
Testing	The time in hours to test the applications.
Remediation	The time in hours to remediate the issues.

Notice that the "Green before" and "Amber after" rows do not have any remediation hours. This is because "Green before" requires no testing or remediation and "Amber after" only requires testing.

The total number of hours and days are provided along with the cost and the elapsed days to execute the project. These are dependent on the numbers entered for the "Size of remediation team" and "Size of staging/testing team" variables in the "Staffing variables" sections on the Variables tab.

Effort estimation without AppDNA

The Effort estimation without AppDNA tab shows the total cost of the project without using AppDNA, a breakdown of the cost, and the remediation and testing times. The report shows results for the selected applications and for all the applications in the portfolio.

The following table explains the table columns:

Column	Description
%	The percentage of applications that require staging, testing, and for which issues need to be identified and fixed.
Apps	The number of applications selected.
hr	The time in hours.

The second set of tables show the estimated number of days for staging, testing, and fixing and identifying issues, along with the cost of each stage. In calculating these figures, AppDNA uses the values entered in the Without AppDNA variables section. For example, the percentage for "Fix and identify" comes from the value entered for the "Applications that are expected to have issues" variable. The value entered for the "Time to identify the cause of a failure and resolve it" variable contributes to the time calculations.

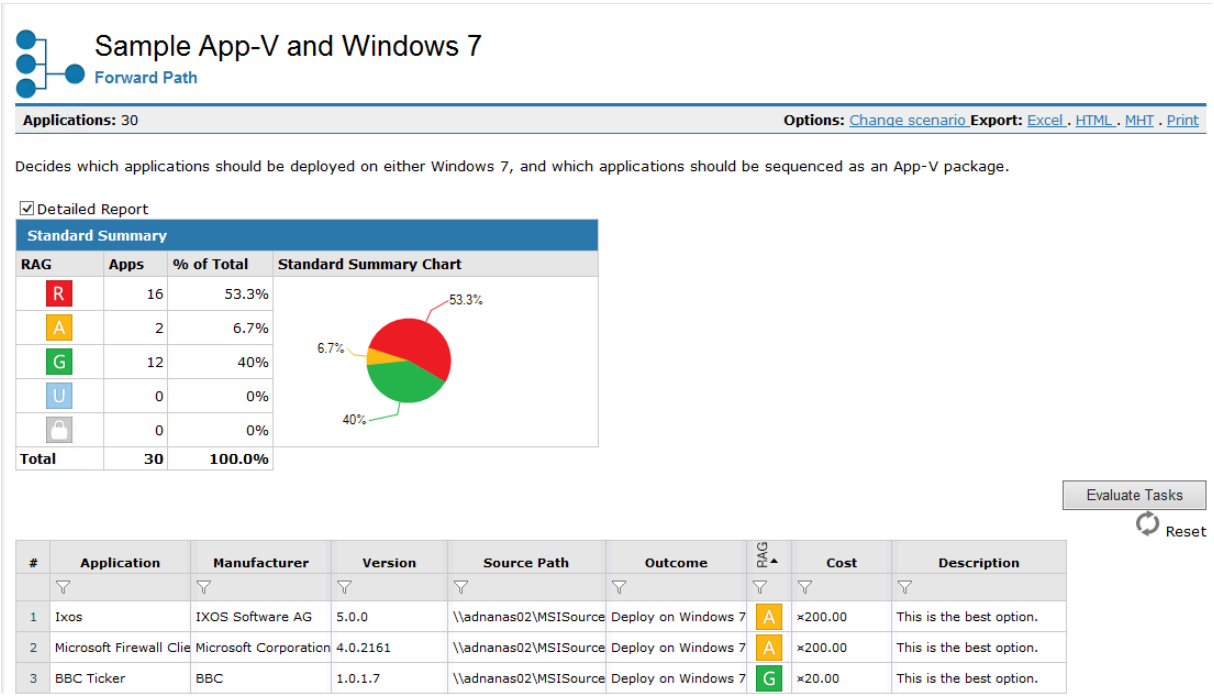
The time to execute the project is calculated in elapsed days. These are dependent on the numbers entered for the "Size of remediation team" and "Size of staging/testing team" variables in the "Staffing variables" section on the Variables tab.

Forward Path

August 1, 2018

Forward Path is a powerful business decision engine in AppDNA that makes it easy to model different deployment scenarios and their impacts. Forward Path is controlled by scenario and task scripts, which you create in the Forward Path Logic Editor. See Forward Path for more information.

Using Forward Path, you can create scenarios that reflect organizational decisions and run task scripts based on the results. For example, when preparing a migration to Windows 7, you could create a Forward Path scenario to determine which applications are suitable for deployment as App-V packages, which should be deployed to the desktop, and which require redevelopment. By associating task scripts with the scenario, you could automate the App-V sequencing, for example.



To open Forward Path, from the side bar, choose Reports: Applications > Forward Path.

To change the scenario, click Change scenario on the Options toolbar, and then select the scenario you want to use from the drop-down list.

Other options that are specific to Forward Path are:

- **Detailed Report** – Select this check box to view a detailed report. Clear this check box to view a condensed report.
- **Evaluate Tasks** – Click this button to open the Forward Path Task Sequencing screen where you can run any task scripts that are associated with the selected Forward Path Scenario.

Run Forward Path tasks

August 1, 2018

Forward Path tasks are typically used to automate the creation of production-ready App-V and XenApp packages, based on logic within the Forward Path report. However, Forward Path tasks can be configured to do many other tasks, such as copying files and sending emails. Forward Path tasks are controlled by Forward Path task scripts that are configured to run based on a value in the Outcome column in a Forward Path report. Forward Path reports are controlled by scenarios.

After you create or import Forward Path scenarios and task scripts, you can run tasks and monitor their status.

To run a Forward Path task

1. From the side bar, choose Select > All Applications.
2. In the Application List, select the applications for which you want to run Forward Path.
3. From the side bar, choose Reports: Applications > Forward Path.
4. In the Forward Path report viewer, select the Forward Path scenario you want to use.

   You can change the default active scenario in the Forward Path Logic Editor.
5. Click Evaluate Tasks.
6. In the Forward Path Task Sequencing screen, click Refresh on the toolbar to ensure you have the latest results.
   - The Outcome column shows the latest results and shows for each application whether there is a task script associated with the value in this column.
   - The MapUNCPathDriveLetter column shows the mapped drive letter if the task script has used the ApplicationDetails.MapUNCPath property to map the \\server\share portion of installation directory to a drive letter.
   - The **Install Command** column shows the command that launches the application installation. If not overwritten by the task script, this shows the Active Directory or Configuration Manager installation command if the application is linked with an Active Directory or Configuration Manager managed application. Otherwise this column shows a command based on the location and method by which the application was imported into AppDNA.
   - The InstallWrkDir column shows the working directory used by the installation command. When this is blank, the default working directory is used.
7. Select the applications for which you want to run the tasks.
8. Click Start on the toolbar.

The lower part of the screen shows the progress and the error log. Some task scripts are dependent on the successful configuration of Install Capture and a virtual machine. See Install Capture for more information.

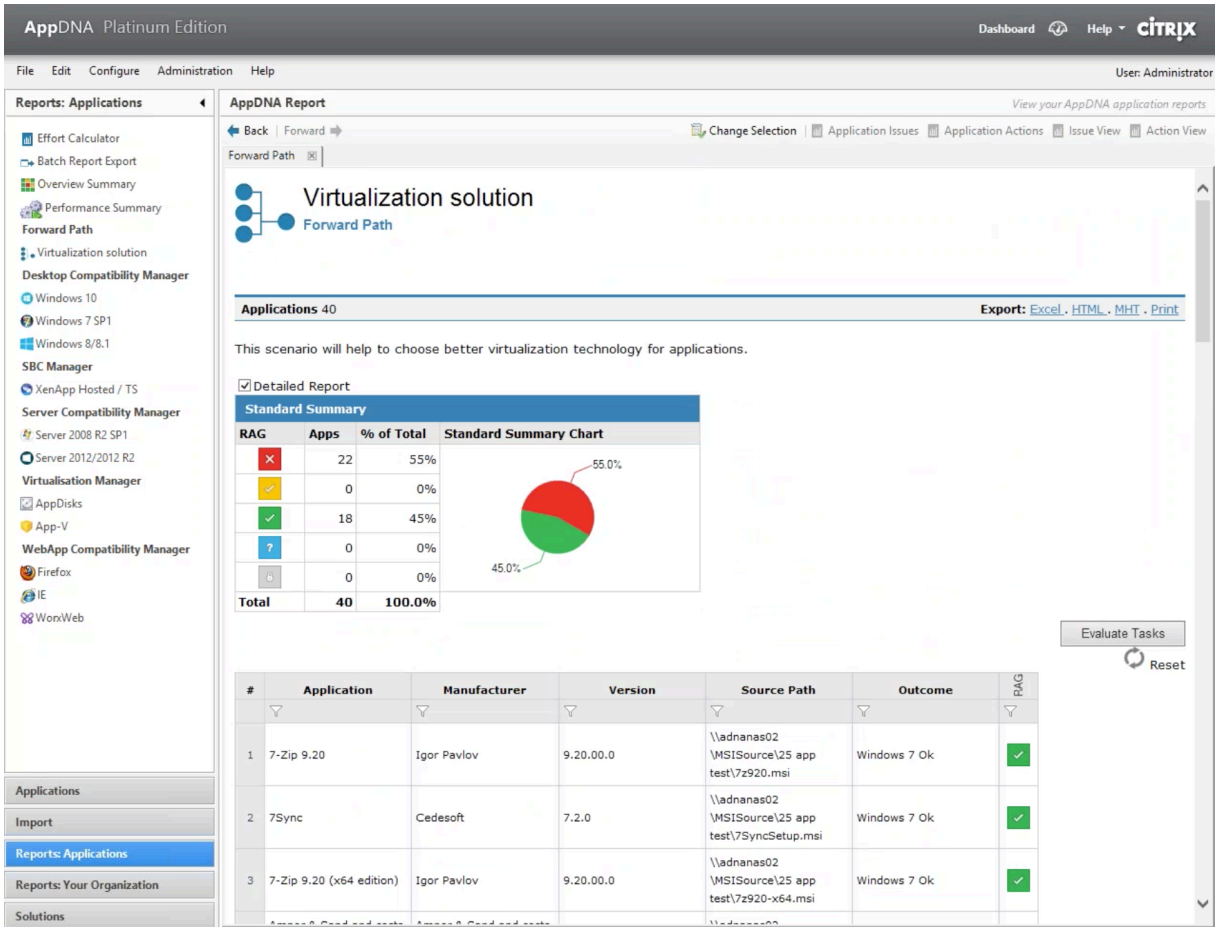
Virtualization solution

August 1, 2018

AppDNA's Virtualization solution provides an analysis of the best path forward for your applications, for example, AppV or XenApp. Built on a forward path script, AppDNA uses the virtualization solution to view installed applications to determine what sorts of algorithms are used; it uses this information

to make recommendations for the best approach for virtualization solutions used by the application. It helps to determine if these applications are better suited for AppV, XenApp and Xendesktop, put on an AppDisk, or allow them to reside in a server or desktop hosted XenApp environment.

To view information related to the virtualization solution feature, select the **Reports Applications** > **Forward Path** > **Virtualization solution**.



Organization reports

August 7, 2018

The organization reports provide summaries of the status of the managed applications that have been deployed to users and computers in entities that are defined in Active Directory or System Center Configuration Manager. In this context, managed applications are applications that are deployed through Active Directory or Configuration Manager.

Important: Before you can view organization reports and see meaningful data, you must load data from Active Directory and/or Configuration Manager. You then must import the managed applications

into AppDNA or link them with applications already imported into AppDNA. See
Integrate data from Active Directory and Configuration Manager for information.

View organization reports

There are two ways to open the organizational reports.

From the Users and Computers screen:

1. From the AppDNA side bar, choose Select > Devices, Users, Groups, or Organizational Units.
2. In the Users and Computers screen, select the entities for which you want to view the report.
3. In the drop-down list on the toolbar, select the report that you want to view, and then click View Report.

Directly from the side bar:

- From the AppDNA side bar, choose Reports: Your Organization > Devices, Users, Groups, or Organizational Units.

The Report Viewer provides a summary that shows the RAG status for the selected report technology of the managed applications deployed to the selected entities. You can drill down to standard AppDNA application reports for those applications.

You can change the selected entities and report at any time by clicking Change Selection on the toolbar. This opens the Users and Computers screen in a separate window. Make your selections and then click Select to apply them.

Note: The organization reports show the status of managed applications that have been imported into AppDNA or linked with applications already imported into AppDNA. These reports do not show the status of applications that are not managed through Active Directory or Configuration Manager. Use the
Discover Applications screen to find out about other applications that are used throughout your organization, as described in
Discover Applications.

Organizational Unit report view

The Organizational Unit report view provides a summary of the status of the managed applications deployed to the users and computers in the selected organizational units and all of the immediate child organizational units.

The summary shows the number of computers and users in each organizational unit and a summary of the RAG status of the managed applications deployed to them. The names of the organizational units that have child organizational units are links that you can click to view a similar report for the child organizational units.

- Click Up to parent to return to the parent organizational unit.
- Click the counts in the Computers and Users columns to view a summary report for those computers and users.
- Click the counts in any of the Applications columns to view the Application Issues report view for those applications.

AD Group and ConfigMgr Collection report views

The Active Directory Group and ConfigMgr Collection report views provide a summary of the status of the managed applications deployed to the users and computers in the selected Active Directory group or ConfigMgr collection.

- Click the counts in the Computers and Users columns to view a summary report for those computers and users.
- Click the counts in any of the Applications columns to view the Application Issues report view for those applications.

Note: The application counts include all managed applications that have been deployed to members of the group, not just those that are assigned to that group. This is a different count from that shown in the
AD & ConfigMgr Collections screen.

Computers report view

The Computers report view provides a summary of the status of the managed applications deployed to the selected computers.

Click the counts in any of the Applications columns to view the Application Issues report view for those applications.

Users report view

The Users report view provides a summary of the status of the managed applications deployed to the selected users.

Click the counts in any of the Applications columns to view the Application Issues report view for those applications.

Export

August 1, 2018

You use the Report Export wizard to perform a bulk export of reports for a given set of applications in a choice of formats – MHT (a single-file Web page, which you can view in a browser and is easy to send to colleagues), Excel, or PDF (Application Issues report view only).

Note: The report export can take many hours if you export reports for a large application portfolio – particularly if you choose to export remediation report views (which require more complex processing).

To open the Report Export wizard, from the menus, choose Tools > Report Export.

On the Welcome page, click Next to begin. The AppDNA Report Export Wizard then takes you through the following steps.

1. **Select the applications**.

   In this step, the wizard provides a list of the applications in your portfolio. You can sort the list and filter it on any column, just like you can in the Application List screen. You can also drag a column header to group the applications by the values in a specific column.

   Select the applications for which you want to export reports and click Next to continue.

2. **Select which reports you want to export**.

   The Report Export wizard does not provide options for selecting the OS images to use. This is because the export always uses the default OS images set for the reports in Edit > Settings on the OS Image Configuration page.

3. **Select which report views you want to export and the formats**.

   The PDF format is only available for the Application Issues report view.

4. **Select your output folder and perform the export**.

   When the report export has finished, AppDNA displays a dialog box that gives you the option of viewing the log. Click Finish to close the AppDNA Report Export Wizard.

Reporting settings

August 1, 2018

The Settings dialog box contains general AppDNA options. To open this dialog box, choose Edit > Settings from the menus.

The options on the Reporting page are:

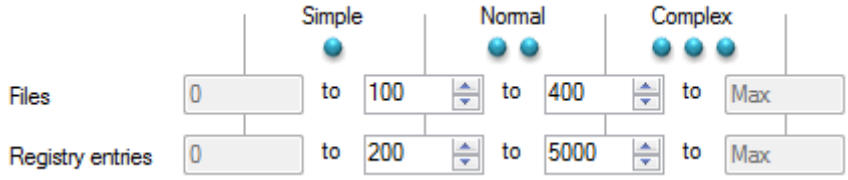
Records per page – Specifies the number of applications that appear on a report view page. When the value is very large (for example, more than 500), performance may deteriorate – for example, scrolling may become jerky and the page may take too long to display. The default is 100.

This setting is automatically updated when you change the number of records on the page in the Report Viewer itself. However, it is useful to be able to change the value here if it has inadvertently been set it to a very large value and the page becomes unusably slow.

This setting does not affect the AppDNA web client. For information about changing the number of records per page in the AppDNA web client, see Report issues.

Show counts in PDF exports – Select this check box to show in the Report Data section of the PDF exports, columns for all of the algorithm groups in the report. These columns show how many times the application has triggered the algorithms in the group. (An application can potentially trigger the same algorithm multiple times – for example, when the same issue is detected in multiple components.) By default, those columns are hidden in PDF exports so that reports with many algorithm groups fit the available space.

Application complexity thresholds – The more files and registry entries an application has, the more complex it is to remediate and test. Therefore application complexity is measured by the number of files and registry entries within the application. AppDNA defines three levels of application complexity – simple, normal, and complex. The thresholds define the lower and upper bounds of what constitutes a normal complexity application.



The default threshold values are based on extensive testing, but you can adjust them if required. The default threshold values are:

	Lower threshold	Upper threshold
Number of files	100	400
Number of registry entries	200	5,000

The following table shows the icon for each application complexity level and provides an example based on the default thresholds.

Icon	Definition	Example
	**Simple** – Applications that have fewer files than the lower files threshold and fewer registry entries than the lower registry entries threshold.	90 files and 150 registry entries.
	**Normal** – Applications whose file or registry entry count is equal to or greater than the respective lower threshold and both counts are less than the upper thresholds.	132 files and 195 registry entries.
	**Complex** – Applications whose file or registry entry count is equal to or greater than the respective upper threshold.	832 files and 5,175 registry entries.

The Effort Calculator uses the application complexity when estimating the time and effort involved in a migration project. In addition, the application complexity icons are shown in some of the report views – for example, the Overview Summary.

Report and license summary

August 1, 2018

The AppDNA dashboard shows the total number of desktop and web applications that have been imported. It also includes summaries that show the state of your application portfolio for each report and the licensing status.

To open the dashboard, click the Dashboard link in the upper right corner of the screen.

Report summary

The Report summary section shows the overall state of the application portfolio for each active report.

The pie charts show the proportion of relevant applications that have an overall red, amber, green, and unanalyzed status for that report. Relevant applications are all desktop (Windows) or web applications, depending on the report. The red, amber, and green status includes all applications that have been analyzed for the report, regardless whether they are locked (unlicensed) or unlocked (licensed) for that report.

The horizontal bars show the number of applications that have been analyzed for the report and how many of these are stale. The application status moves from the analyzed state to stale when a change occurs that makes the stored reporting data out of date, such as when you activate additional algorithms for that report.

Module license summary

The Module license summary section shows a list of the modules included with your license. For each module, the following information is shown:

- The module name.
- The date the license expires. Related reports will not be visible after this date.
- The number of application licenses that have already been used.
- The number of available application licenses. These are licenses that have not yet been applied to an application.

When all of the available licenses have been used, you can manually unlock a few additional applications (up to 10% of the licensed limit) in the Apply Licenses screen. This additional allowance is called the license reserve.

What are inactive licenses?

An inactive license is a license that has been applied to an application that has now been deleted. The license is not available for other applications. By default, the license is automatically re-applied to the application if it is re-imported (desktop applications only). See Fingerprints for more information.

Resolve

June 17, 2019

AppDNA provides information about compatibility issues that have been detected in applications. In AppDNA, the term remediation refers to the process of resolving these issues by making changes to applications or the environment so that the applications work on the target platform.

Remediation reports provide detailed remediation information for a specific application. Sometimes more than one alternative approach is provided. The remediation reports also provide details of the application components that are affected by each issue.

Remediation reports

There are two remediation report views for desktop applications and three for web applications:

- **Remediation Issues** – Provides a breakdown of the issues identified by the algorithms and information about the affected components.
- **Remediation Actions** – Provides a breakdown of the number and type of actions required to remediate the application.
- **Site Map** – (Web applications only.) Provides a summary of the pages, objects, scripts, and style sheets, that the AppDNA directed spider visited, skipped, or failed to capture.

To open a Remediation report:

1. Click Reports: Applications and then click the name of a report, such as Windows 8/8.1, to expand the list of report views.
2. To view Remediation Issues, click Application Issues and then click an application link in the report.

To view Remediation Actions, click Application Actions and then click an application link in the report.

To swap between views, click the Switch to link at the top of the report.

For desktop applications for which AppDNA provides an automatic fix, you can download the fix in the form of an .mst file that contain modifications that can be applied to the application's .msi file during installation to correct issues. Click the Get MST fixes button to download the fix.

You can optionally merge remediation report views for multiple standard reports (not custom reports). For example, you can merge the results for the Windows 8 and App-V reports. To do this:

1. On the Export toolbar, click Merge report.
2. Select the other report or reports that you want to merge with the current one, and click View merged report.

If relevant to the report, the currently selected OS Images are shown at the top of the screen. To change the selection, click Change images on the Export toolbar.

Detail – Shows the application's name, manufacturer, version, installation file, package type, standard RAG status, and the date the remediation report view was generated.

Journal – If the application has any external data or manual journal entries, they are shown in this section. If AppDNA has matched the application with an entry in one of the PCA (shim) database external data sources, this section shows the matching executable (.exe) file(s) and, when relevant, the name

of the shim(s). You can click Accept to convert an external data entry into a standard journal entry. This means that the application's RAG status will be overridden by the corresponding compatibility (journal) status.

The remaining details are different in the Issue view and the Action view.

For the Issue view, there is a list of the algorithms that the application has triggered. For each algorithm, the report shows the module and report name, along with the algorithm and algorithm group, the standard RAG, and the number of times the application has triggered the algorithm. The algorithm name is a link that takes you straight to the detailed information about the algorithm below.

The detailed information about each algorithm shows the description of the group, the manifestation of the problem identified by the algorithm, an explanation of the remediation, and a list of the application's components that triggered the algorithm. These details vary depending on the algorithm.

For the Action view, there is a list of the actions that need to be implemented to fix the issues that the algorithms have uncovered. For each action and action detail combination, the report shows the effort involved, the after action RAG, and the number of issues that need to be addressed. The action detail is a link that takes you straight to the detailed information about it below. This shows details about each algorithm to which the action applies, including the description of the algorithm group, the manifestation of the problem identified by the algorithm, an explanation of the remediation, and a list of the application's components that triggered the algorithm. These details vary depending on the algorithm.

Tip: Use the
Report Export Wizard to export remediation reports for multiple applications.

Standard remediation actions

Remediation reports list the remediation actions and action details for each application. Here are example remediation actions that a report can include:

- Additional testing is required:
  - Application requires functionality testing
  - Assess application security risk
  - Driver compatibility test required
  - Verify application publisher is trustworthy
- Additional XenApp testing required
- Apply Shim
- Change Group Policy
- Change hardware
- Change operating system build:
  - Add certificate trusted list

  - Add non-supported component to OS
  - Add redistributable to OS
  - Run application on 64-bit OS
- Change software
- Deploy using a desktop virtualization technology
- Deploy using an application virtualization technology
- Edit OSD file
- Modifications are required in the App-v Management Console:
  - Create global FTAs
  - Select one application to be FTA provider, change the other application's verb
- Redevelopment required
- Repackage application:
  - Create a Merge Module for shared resource
  - Edit the script file called by the MSI
  - Provide the missing resource or install a redistributable
  - Rename the setup to Setup.EXE
- Sequencing steps need to be followed:
  - Add placeholders in INI files
  - Configure environment variable changes
  - Include missing files in the sequence
  - Publish shortcuts in the Start Menu's startup folder
  - Sequence application with its required service
- Use App-V 5.0

To view the actions for each algorithm available for a report, go to Configure > Modules > Module > Report Name.

What do the green algorithms tell you?

Some of the algorithms built into the AppDNA reports have a green RAG status. Generally, a green RAG status means that the application is ready for user acceptance testing (UAT) on the target platform. However, these algorithms can be broken down into several groups:

- Some algorithms have a green RAG status because they detect an issue that typically only becomes a problem in certain circumstances. If those circumstances apply in your environment, you may want to configure the custom RAG status to amber. For example, the Windows 7 W7_VDEPNX_001 algorithm detects an issue that is relevant only when Data Execution Prevention (DEP) is enabled. This algorithm has a green RAG status because by default DEP is off for general applications. If DEP is enabled in your environment, you may therefore want to change this algorithm's custom RAG status and default action. See Configure algorithms for step-by-step instructions.

- Some algorithms detect things that contradict generally accepted best practice but that do not typically have a compatibility impact. These algorithms therefore have a green RAG status. However, they provide useful information when you are considering which applications to retire, for example. Similarly, if you need to redevelop the application to resolve another issue, you may want to address the best practice issue at the same time.
- Other algorithms have a green RAG status because they detect an issue that only rarely causes a problem. These algorithms provide useful information if after addressing all of the issues identified by the amber and red algorithms, you find the application still has issues.

Remediate web applications

August 1, 2018

The web application compatibility remediation report views provide detailed information about how to rework the web application code to resolve the issues identified. This topic provides information about other remediation options that you can use – for example, if you do not have access to the source code. However, these options should typically be considered a short term solution until the web application can be redeveloped.

Internet Explorer document compatibility

There are a number of compatibility modes in Internet Explorer 8 and later. These compatibility modes determine how web pages are interpreted and displayed. If your web application is not compatible with the target version of Internet Explorer, you can optionally set the web application to use an appropriate compatibility mode. There are several approaches to setting the compatibility mode:

- **Using a Group Policy Object (GPO)** – You can add the web application to one of the following group policies so that it is rendered in IE7 Standards or Quirks document mode, respectively. This approach is useful if the web application is hosted externally and you do not have access to the source code.

Software\Policies\Microsoft\Internet Explorer\Compatibility View\Use Policy List of Internet Explorer 7 sites
Software\Policies\Microsoft\Internet Explorer\Compatibility View\Use Policy List of Quirks Mode sites

See http://technet.microsoft.com/en-us/library/cc985351.aspx for more information.

- **Using a meta tag in the page header** – If you have access to the web application's source code, you can use a meta tag in the page header to specify that the page is to run in a particular mode like this:


```
<head>
  <meta http-equiv="x-ua-compatible" content="IE=Value">
  <title>My page</title>
</head>
```

Where Value is one of the values in the following table.

Value	Description
5	Render the page as if Internet Explorer is running in Quirks document mode, which is similar to how content was rendered in Internet Explorer 5.
7	Ignore the DocType if present and render the page as if Internet Explorer 7 is running in IE7 Standards document mode.
8	Ignore the DocType if present and render the page as if Internet Explorer 8 is running in IE8 Standards document mode.
9	Ignore the DocType if present and render the page as if Internet Explorer 9 is running in IE9 Standards document mode.
EmulateIE7	Respect the DocType and render the page as if Internet Explorer 7 is running in IE7 Standards or Quirks document mode.
EmulateIE8	Respect the DocType and render the page as if Internet Explorer 8 is running in IE8 Standards or Quirks document mode.
EmulateIE9	Respect the DocType and render the page as if Internet Explorer 9 is running in IE9 Standards or Quirks document mode.
Edge	Use the highest mode available. Not recommended in production environments.

See http://msdn.microsoft.com/en-us/library/jj676915(v=vs.85).aspx for more information.

- **Using a custom header on the web server** – If the web application is hosted internally, you can use a meta tag in the HTTP headers on the web server to specify that the entire site is to run in

a particular mode. The details of how to do this vary depending on the type of web server (for example, whether it is IIS or Apache). However, the options are the same as described above for using a meta tag in the page header.

For example, for an IIS server, you can add a section to the web.config file to provide meta tags in HTTP headers like this:

```
‘‘‘
<configuration>
  <system.webServer>
    <httpProtocol>
      <customHeaders>
        <add name=”X-UA-Compatible” value=”IE=8” />
      </customHeaders>
    </httpProtocol>
  </system.webServer>
</configuration>
‘‘‘
```

See http://msdn.microsoft.com/en-us/library/jj676913(v=vs.85).aspx for more information.

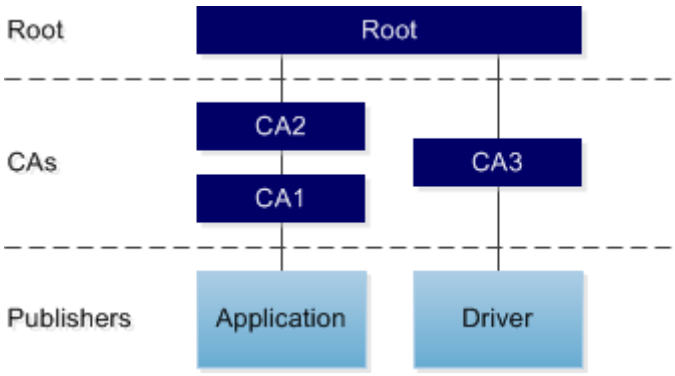
Using a virtual browser environment

When other options fail to resolve the issue, you could consider running the web application natively in the supported version of the browser delivered using a virtualization technology such as Med-V or Citrix Terminal Server.

Digital signatures

August 1, 2018

A digital signature is a mechanism that provides users with assurance that a digital file comes from an identifiable source and has not been tampered with. Digital signatures often include a chain of certificates. The publisher of the digital file generates the digital signature using a certificate issued by a certification authority (CA). The CA is responsible for verifying the publisher’s identity. That CA’s certificate may in turn have been issued by another CA, and so on back to the root CA. (There can be more than one root.) In this way the certificates form a chain, as the following diagram illustrates.



The Windows operating system (OS) stores certificates and lists of trusted and untrusted publishers and CAs on a per-machine and per-user basis. You can use the Certificates snap-in to the Microsoft Management Console to view and manage the certificates that are stored on the OS.

Capture of digital signature DNA

When you import applications into AppDNA, the import process captures information about any digital signatures that are found in the application files. When present, digital signatures are typically in the application's portable executable (PE) files (such as executables and DLLs). However, for drivers, the digital signature can be in an associated catalog file.

The import process extracts and stores the signature's basic details and information about each certificate in the certificate chain. The import process attempts to determine whether the signature is valid within the context of the certificate chain on the AppDNA import machine. However, the results may differ on another machine or OS, or for a different user, if the stored certificate information differs. For this reason, some of the algorithms do additional checks against the selected OS image(s).

The import process does not check certificate revocation lists, because this would slow down the import to an unacceptable degree.

Untrusted signatures on Windows 8 and Windows Server 2012

Both Windows 8 and Windows Server 2012 block files signed by an untrusted publisher from running. The practical impact of this depends on which file is affected. If it is the main application executable, the application will not run – Windows presents the user with a message that explains that the application does not meet the signing requirement. However, if the affected file is a minor DLL, the application may run but will fail when functionality that relies on the DLL is invoked. If the affected file is a kernel-mode driver, it may not be possible to install or run the driver.

Kernel-mode drivers are device drivers that run in "supervisor mode", which provides privileged access to low-level capabilities and performance advantages compared to drivers that run in standard "user mode". If a program that is running in supervisor mode fails, it can cause the entire system to fail.

Windows Server 2012 and 64-bit editions of Windows 8 therefore block the installation and running of kernel-mode drivers that are signed by an untrusted publisher.

Note: Sometimes an application may contain multiple digital signatures from more than one publisher – for example, if the application includes third-party components that are also signed.

Windows 8 and Windows Server 2012 algorithms

The following algorithms detect files that contain an untrusted digital signature. Untrusted means that either the publisher or one of the CAs in the chain appears in the list of untrusted publishers and CAs stored in the target OS image. The results for these algorithms therefore depend on the target OS image that is selected.

- For Windows 8 and Windows 8.1: WIN8_UNTRUSTED_001
- For Windows Server 2012 and Windows Server 2012 R2: W2K12_UNTRUSTED_001

The remediation report views provide information about which file within the application is affected, whether this is a driver, and details of the untrusted certificate.

Remediation

For external applications, contact the manufacturer to obtain an updated version of the application or driver that is signed by a trusted publisher.

If this is not possible, investigate why the publisher or CA is on the untrusted list. You can use the Certificates snap-in to the Microsoft Management Console to remove a publisher from the untrusted list in the OS image. However, this should not be done without first establishing that it is indeed trustworthy and that the application is safe and conforms to security policies.

For instructions for opening the Certificates snap-in, see View or manage your certificates on the Microsoft web site. After you have opened the Certificates snap-in, use the Help to view detailed documentation about viewing and managing certificates.

Manage

June 17, 2019

This section provides documentation of a variety of AppDNA features that you can use to manage your applications.

Quick links to topic sections:

Application list

August 7, 2018

AppDNA provides an application list from which you manage your application portfolio. For example, you can view the list of applications, view application attributes, analyze the application DNA against selected reports, and use the Report Viewer. You can also delete applications from the portfolio and edit an application's name, manufacturer and version number.

You can also sort, group, and filter the application list for analysis and reporting. These features are especially useful if you have a large portfolio.

To open the Application List, click Applications in the AppDNA side bar.

Select applications

To:	Do this:
Select all of the items in the list	Press CTRL+A (or choose Edit > Select All from the menus)
Deselect all of the items in the list	Press CTRL+D (or choose Edit > Deselect All from the menus)
Invert the selection	Press CTRL+I (or choose Edit > Invert Selection from the menus)
Select multiple adjacent items	Click the first item you want to select, then hold down SHIFT and click the last item you want to select. Then press CTRL+M (or choose Edit > Select Marked from the menus)
Select multiple non-adjacent items	Hold down CTRL and click the items you want to select, and then press CTRL+M (or choose Edit > Select Marked from the menus)

To:	Do this:
Deselect multiple adjacent items	Click the first item you want to select, then hold down SHIFT and click the last item you want to select. Then press CTRL+U (or choose Edit > Deselect Marked from the menus)
Deselect multiple non-adjacent items	Hold down CTRL and click the items you want to select, and then press CTRL+U (or choose Edit > Deselect Marked from the menus)
Select applications in a group	From the Group drop-down box on the toolbar, choose the group whose applications you want to select.

Toolbar

Add - Add a new application, or application placeholder or "stub". Creates a new application record in AppDNA, against which you can collect and track information using properties, attributes, and attachments, without the requirement to import the application immediately.

Delete - Deletes selected applications from the AppDNA application portfolio. This does not delete the desktop application fingerprints. This means that if you delete a licensed desktop application and then import it again, it will reuse the same license.

Export Filter - Saves a filter to an XML file for reuse. See Filter applications for more information about setting up, clearing, saving, and importing filters.

Import filter - Imports a previously saved filter and immediately filters the list of applications according to the criteria in the saved filter.

Report type - Use this drop-down list to select a report to view.

View report - Click to view the selected report for the selected items. (An application must be analyzed before you can see meaningful data for it in the reports.)

Analyze - Click to analyze the selected applications. See Analyze applications for more information.

Group - Use this drop-down list to select the applications in a particular group, all of the applications in the list, or to deselect all of the applications in the list.

Key columns in the Application List

To group the applications in the Application List by the data in any of the columns: Drag the header of the column to the Drag a column header here to group by that column bar. When you no longer want

to group the applications, drag the column header back to the header bar.

To include an item in analysis or reports: Select the application.

Application status is as follows:

- **Ready —** The application has been imported successfully and is ready to be analyzed.
- **Analyzed —** The application has been analyzed (for one or more reports).
- **Stale —** The status changes from analyzed to stale if the application needs re-analyzing. This happens when changes are made to the modules, algorithms, or algorithm groups – for example, if algorithms or algorithm groups are switched on or off.

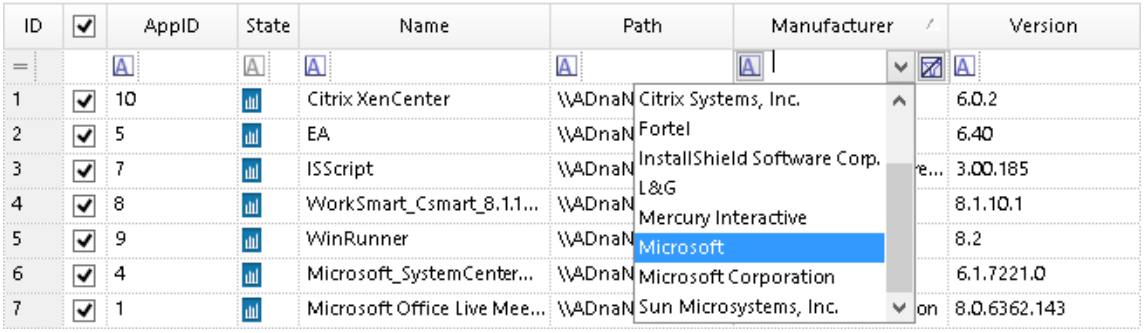
Filter applications

August 1, 2018

Filtering the application list is particularly helpful if you have a large application portfolio. You can save a filter to a file and later import the file to immediately filter the list of applications based on the criteria saved in the filter.

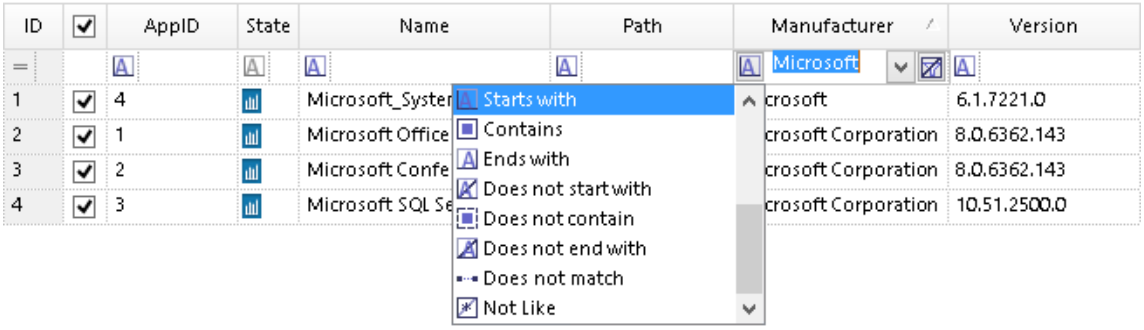
Create a filter

1. In the Application List, click in the text box under the header of the column that contains the values on which you want to filter the applications.
2. Select or type a value to filter on.

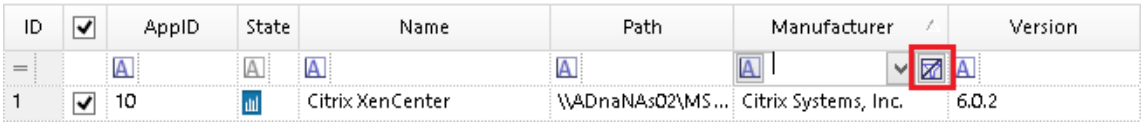


You can specify multiple filters to further restrict the list.

3. To restrict the applications to those that do **not** match a value, enter or select the value, click the icon on the left of the text box, and, from the drop-down list, select the option you want to use.



4. To clear a filter, click the clear filter icon next to the filter.



Save a filter for reuse

You can save a filter as an XML file for reuse.

1. Create the filter.
2. Click Export Filter on the toolbar.
3. In the Save As dialog box, enter a name that will help you identify the filter and select a location and then click Save.

Import a saved filter

1. Click Import Filter on the toolbar.
2. In the Open dialog box, navigate to the saved filter XML file and then click Open.

This automatically and immediately filters the list of applications according to the criteria in the imported filter file.

Application attributes

August 1, 2018

You can record information about applications that is specific to your organization in AppDNA application attributes. An application attribute can contain information such as asset ID, cost center, application status, or owner.

The following attributes are already created:

- **AppID.** An AppID is a unique identifier for an application such as an asset ID. AppID is configured to appear on all reports.

  AppIDs, tracked by many organizations, might be an asset tag number or other tracking number held in a corporate purchasing system or other application. You are responsible for obtaining AppIDs from your corporate system: You can handle that manually, through scripts that you write, or by working with Citrix Consulting to integrate AppDNA with your corporate system. If you do not assign a value to AppIDs, AppDNA assigns them, starting at 1, based on the order in which the applications are imported into AppDNA.

- **Analyzed Date.** The date that an application was analyzed is configured to appear on remediation reports.

To add custom information to applications you:

- **Create an unlimited number of application attributes.** For example, to track application status you might create an attribute named App Status and define a list of values for it: Imported, Analyzed, In test, Failed test, Passed Test, In Production.

  When creating an attribute, use the AppDNA management console to:

  - Choose from a variety of data types: Text field, number, list, yes/no choice, date, or RAG indicator.
  - Define how an attribute is to be reported. You specify whether the attribute will have different or the same values for each report; you choose which reports are to include the attribute.

  Note: Depending on your screen resolution, you might be able to show a limited number of application attributes on the Overview and Assessment reports.

- **Set the value of application attributes.** If you track application information in other IT systems, you can set attribute values by importing a CSV file or by using the AppDNA SDK . You can also set values by directly editing them in the AppDNA management console.

- **View application attribute information.** The reports that include application attributes will contain a column for each attribute.

To create an application attribute

You must use the AppDNA management console to create application attributes.

Note: Users with the administrator role can manage (add, delete, edit) application attribute definitions. All users can change attribute values.

1. From the AppDNA menus, choose Configure > Attributes.

   The Application attributes screen appears.

2. Click New.
3. In the Attribute definition page:
    a) Specify a Name for the attribute.

       This is the label that will identify the attribute on reports.

    b) Specify whether the attribute value will differ per report or should be reported globally.

       Your selection determines which reports can include the attribute. If you select the Per-report attribute check box, the attribute cannot appear on the Application List screen or the Overview Summary report, which include only the data that applies globally to the application.

       - To report different values for an attribute on the various reports, select the Per-report attribute check box.

       For example, suppose that you are creating an attribute, Tested, to indicate whether the application is tested. If the value for Tested might differ for the various operating systems, select the check box.

       - To report the same value for an attribute on the various reports, leave the Per-report attribute check box cleared.

       For example, suppose that you are creating an attribute for cost center. In your organization, the same cost center applies for a particular application, regardless of the operating system. In this case, you would not select the check box.

       After you create an attribute, you cannot change its Per-report attribute setting.

    c) Choose a Data type from the list.

       The data type restricts the attribute value to a particular input format.

       If you choose
       List, the Select or create list page appears.

       - To use a list that is already defined, select Use existing list and then choose the list name from the menu.
       - To create a list, select Create new list, specify a New list name, and then type the list items in the Current items in list box.

       To reorder a list or change its members, see To edit a list, later in this section.

       After you create an attribute, you cannot change its Data type setting.

    d) Click Next.
4. In the Display options page, specify where you want the attribute to appear.

- **Screen: Application List.** Attributes with the same values for all reports, including AppID, appear on the Application List screen by default (unless Per-report attribute is selected).
- **Report: Overview Summary.** Attributes, including AppID, appear on the Overview Summary report by default (unless Per-report attribute is selected).
- **Reports: Application Issues and Application Actions.** To include the attribute on these reports, select the check box.
- **Reports: Remediation Issues and Remediation Actions.** Attributes, including AppID, appear on these application reports by default, regardless of the Per-report attribute option selected.

Consider the space requirements of additional columns when determining which attributes to show in a report.

5. Click Finish.

   The attribute appears in the selected locations.

6. After you complete the changes, click Save.

To import attribute values

Note: Users with the administrator role can import application attribute values.

To set the value of application attributes for multiple applications at a time, you can import the values from a comma-separated values (.csv) file or the AppDNA SDK .

If you import applications from a file, as described in Import from List, you can import the attributes at the same time or subsequently. Before you import attribute values, you must create the application attributes. Creating an attribute automatically adds it to the template import file.

Be sure to re-import your template import file after adding, editing, or deleting attributes.

If you use other methods from the AppDNA management console to import applications, you can import the attributes after the applications are available in AppDNA.

To change attribute values

Note: Users with the administrator or user role can view or change application attribute values.

1. When viewing the Application List screen:
   a) In the Application List screen, select the applications you want to change and then click Properties.
      The properties page appears.
   b) To set the value of an attribute, select the check box for the attribute, enter its value, and then click OK.

2. When viewing an Application Remediation report:
   a) In the Application Remediation report screen, click Properties.
      The properties page appears.
   b) To set the value of an attribute, select the check box for the attribute, enter its value, and then click OK.

To edit a list

You must use the AppDNA interface to create and edit lists.

1. From the AppDNA menus, choose Configure > Application Attributes.

   The Application Attributes Settings appear.

2. Click the Lists tab and then click the list name.
3. Click Edit values and make your changes.
   - To move an item, click it and then use the arrow buttons.
   - To rename an item, click it and then type a new name.
   - To delete an item, click it and then click Delete.
4. After you complete the changes, click OK and then click Save.

To rename or delete an application attribute

Note: Users with the administrator role can rename and delete application attributes.

1. From the AppDNA menus, choose Configure > Application Attributes.

   The Application Attributes Settings appear.

2. Select the attribute and then click Edit or Delete.
3. After you complete the changes, click Save.

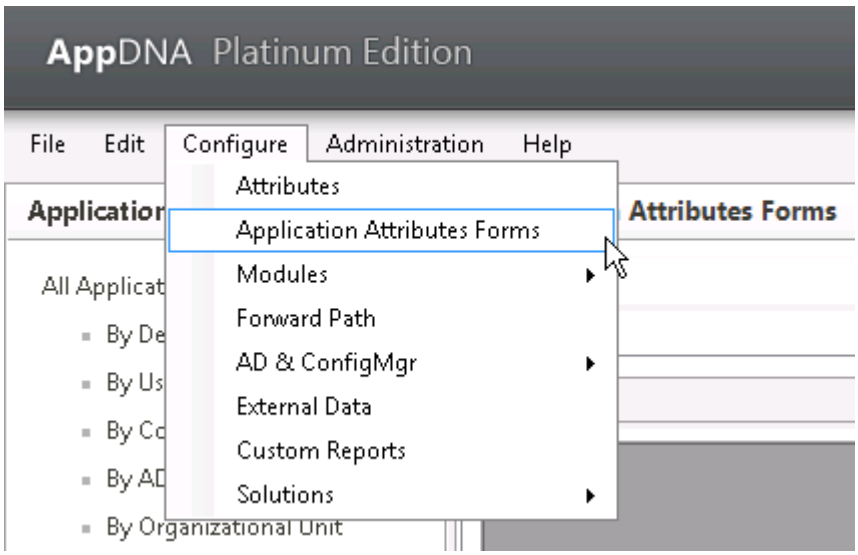
Application attributes forms

August 1, 2018

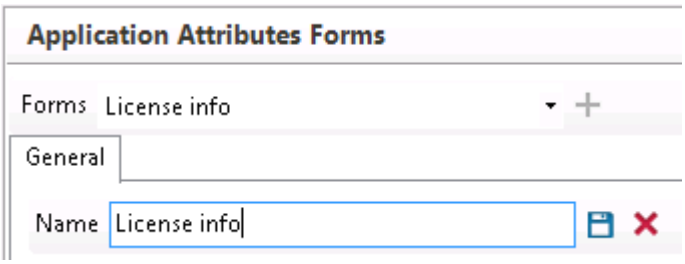
Application attributes forms allow you to create named collections of attributes useful for tagging applications with meaningful internal IDs that can be used to classify applications. Use these internal IDs to tag apps (for example, license costs and renewal dates), then group them into logical containers (forms) which are then available in the properties of an application.

Create an application attributes form

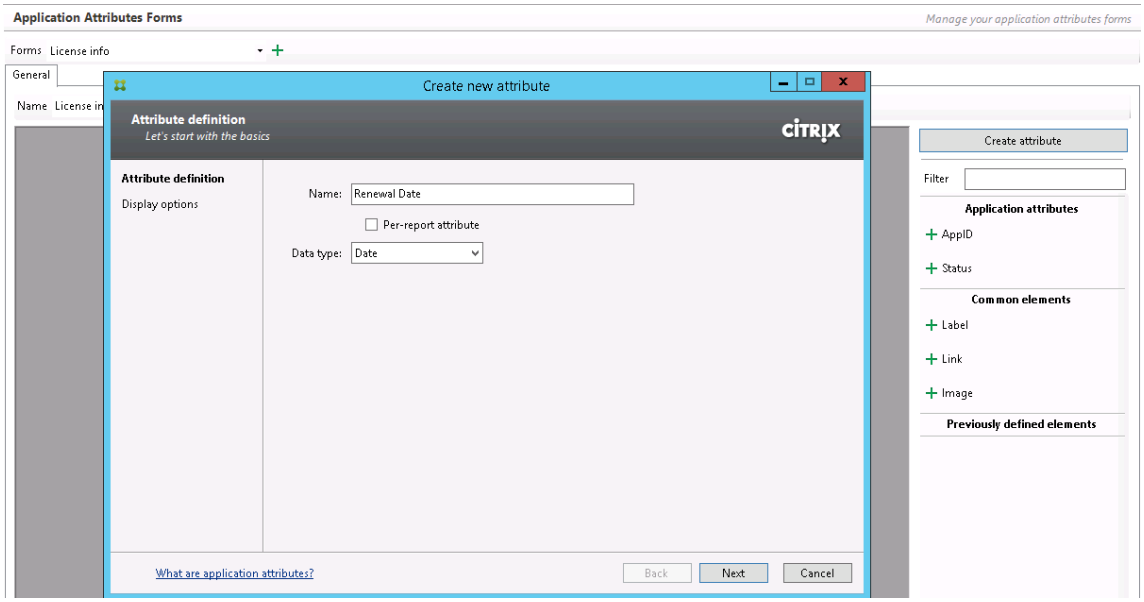
1. From the AppDNA menus, select **Configure** > **Application Attributes Forms**.



2. Click on the **+ icon**, then specify a name for the application attributes form.
3. Click **Save**.

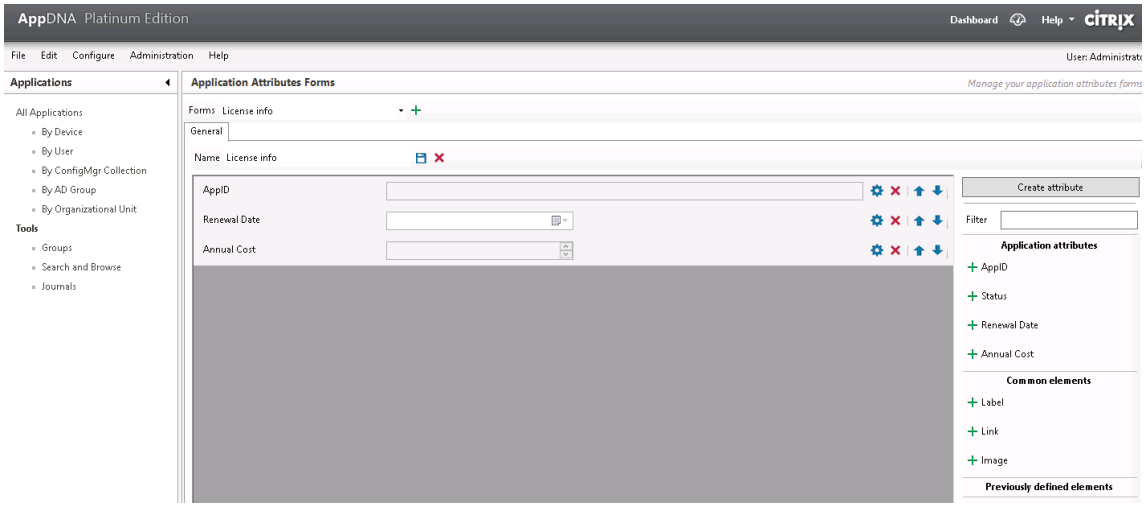


4. Select **Create attribute**, and add new attributes. For example, Renewal Date (Data type: Date) and Annual Cost (Data type: Number).



You can also create new attributes in **Configure** > **Attributes**. These will be displayed on the right-hand side along with any new attributes you create within Application Attributes Forms.

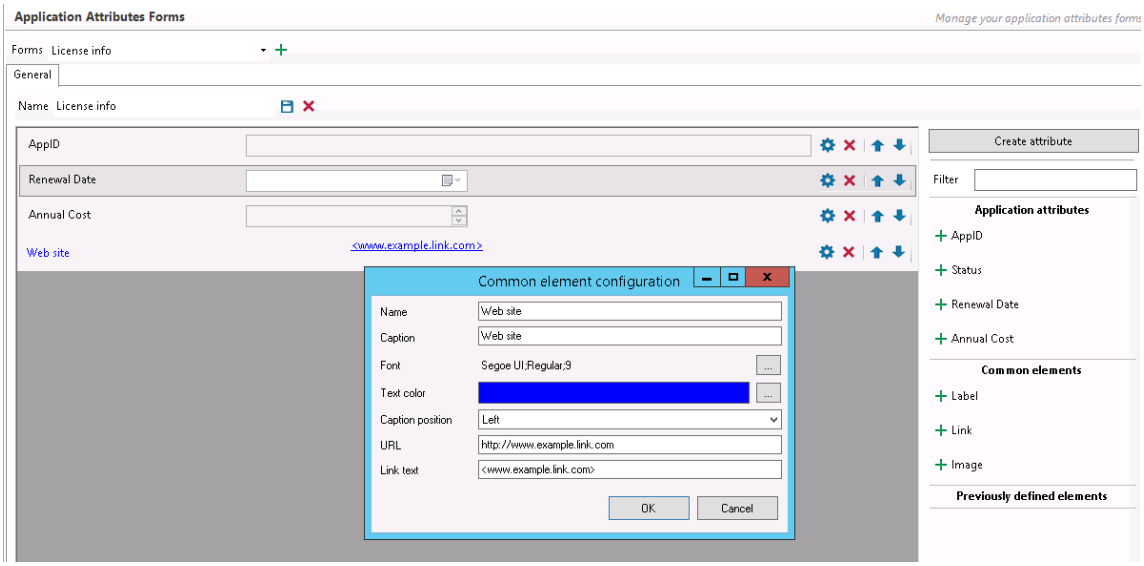
5. To build the form, drag attributes from the right-hand side and drop them on form designer on the left-hand side. These attributes will appear dynamically and can change based on the values assigned to each application.



After adding application attributes, you can add additional attributes which are common to all applications. For example, a link to a web site or a label. These are **Common elements**. **Previously defined elements** shows a list of common elements which have already been configured and saved. You can add these to any Application attributes form.

6. To add a common element, drag it from the right-hand side and drop it on the form designer, for example Link.

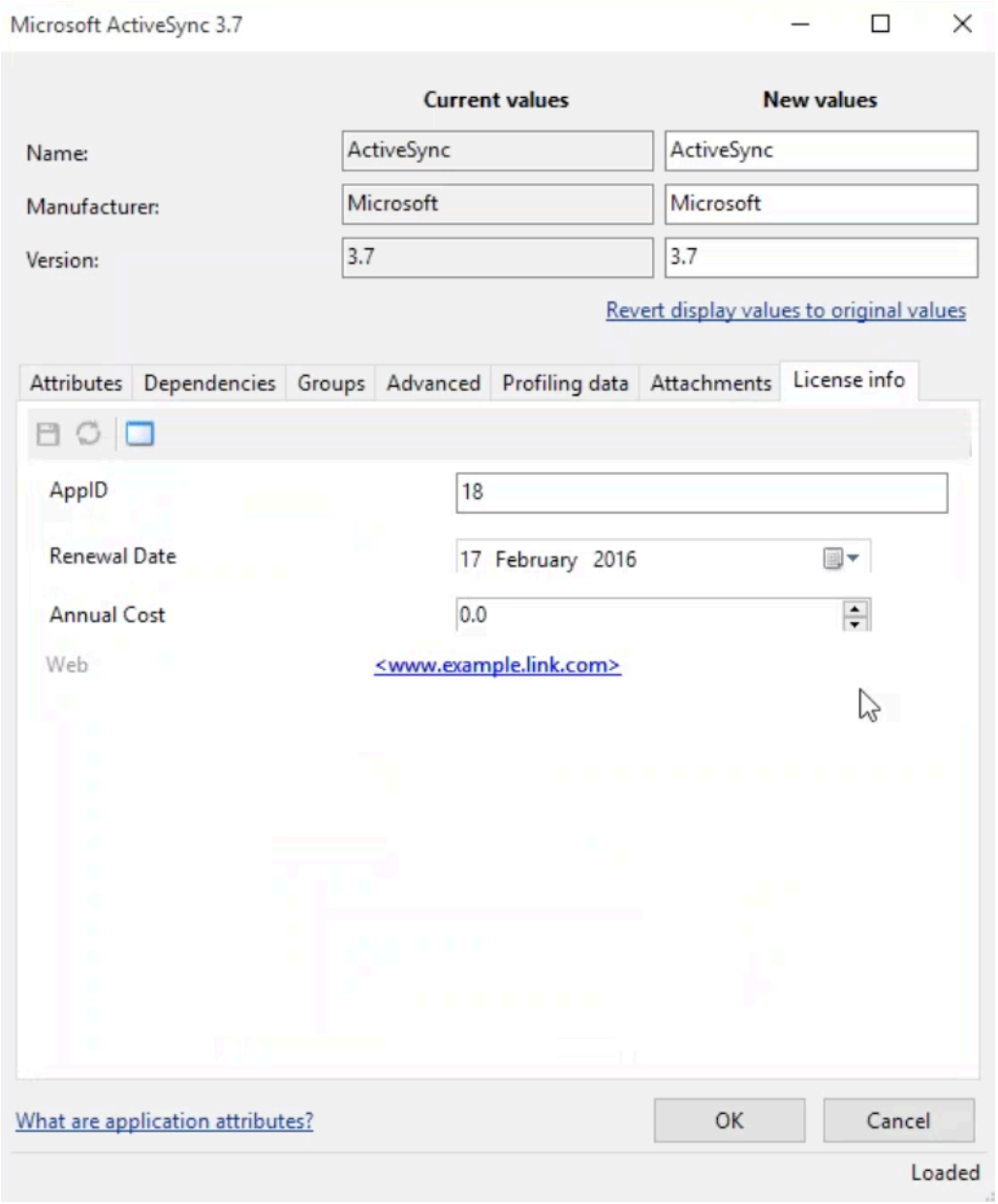
7. Specify the Name, Caption, URL, Link text and click **OK**.



8. Click Save.

Viewing application attributes forms

You can view the application attributes form and update the attributes in **Applications** > **Applications List**, right-click and select **Properties**. The attributes and common elements which you defined in the Application Attributes form are grouped together in a new tab.



You can also view application attribute forms from the AppDNA web client. From the web client, select **Applications**, highlight an application and select **Properties**.

Add applications

August 1, 2018

To support **application lifecycle management**, you can add application placeholders or "stubs" in AppDNA, against which you can collect and track information using properties, attributes, and attach-

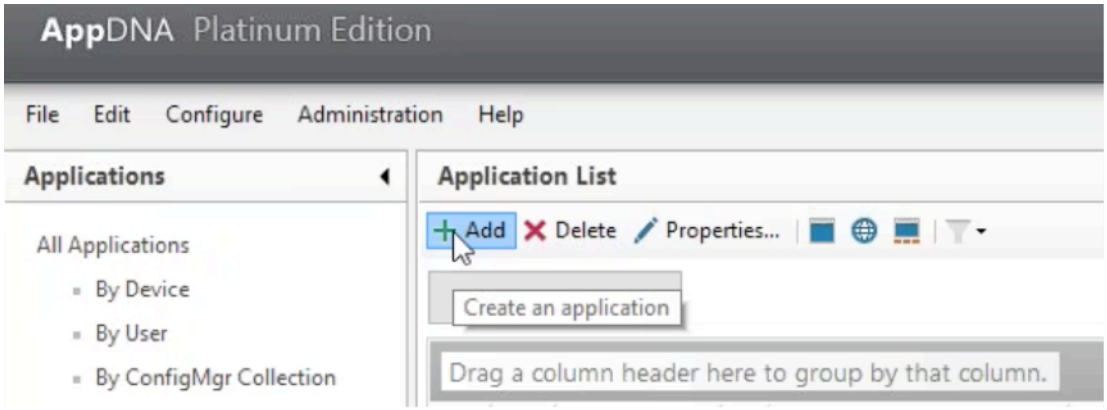
ments without the requirement to import the application immediately.

For example, as an IT administrator, you have received a request for a new financial application. Even if you do not yet have access to the installer, you can still begin to collect and track information about that application as it becomes available.

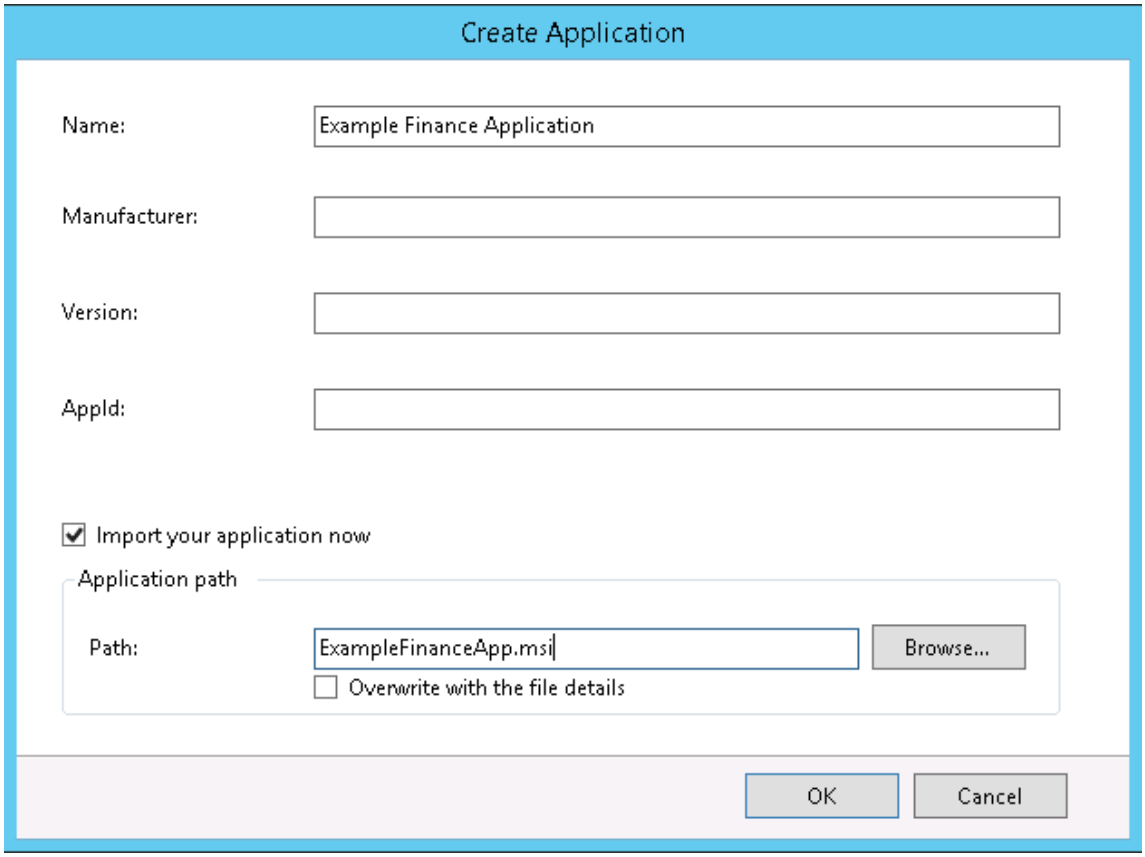
You can import the application as part of the same step if the installer is available. Alternatively, you can import it later.

To add a new application placeholder or “stub”:

1. Select **Applications**.
2. From the Applications List, select **Add**.



3. In Create Application, add a name to represent the application, and optionally specify addtional information.
4. Select the **Import your application now**; click **Browse** to locate the application you want to import.

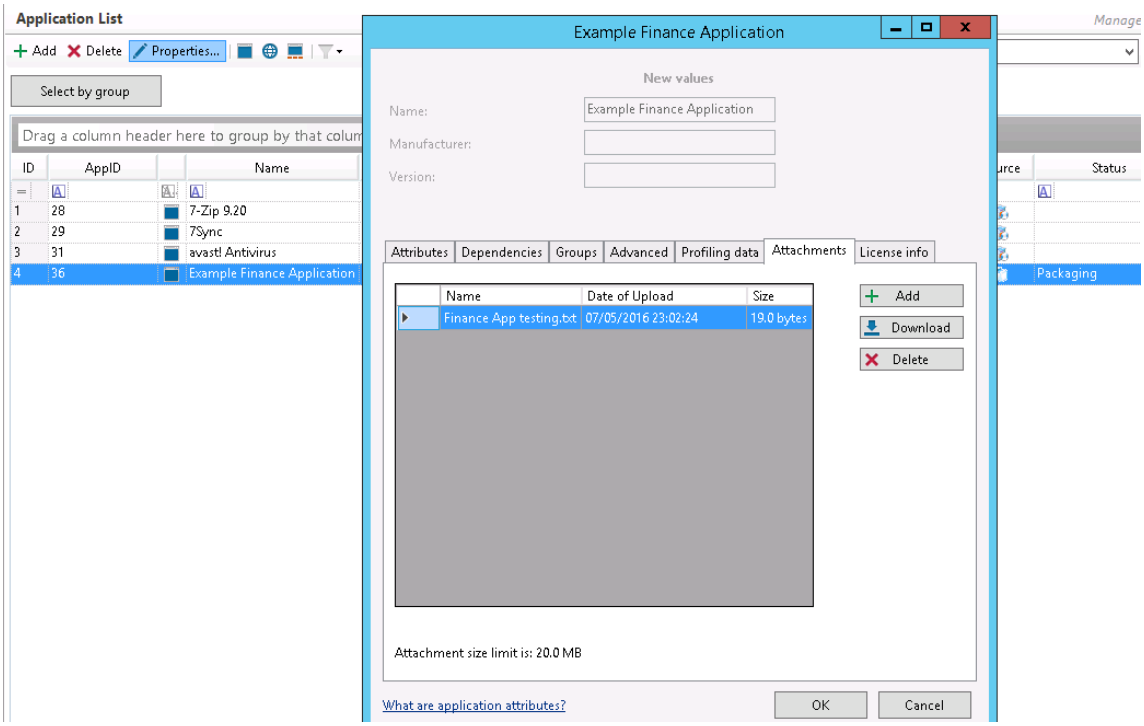


If you do not have access to the installer for the application, leave this blank and import later (right-click on the application stub > Import).

5. Click **OK**.

   The application or application “stub” is added to the application list.

6. Select **Properties** to manage application attributes, attachments and other properties of the application or application “stub”.



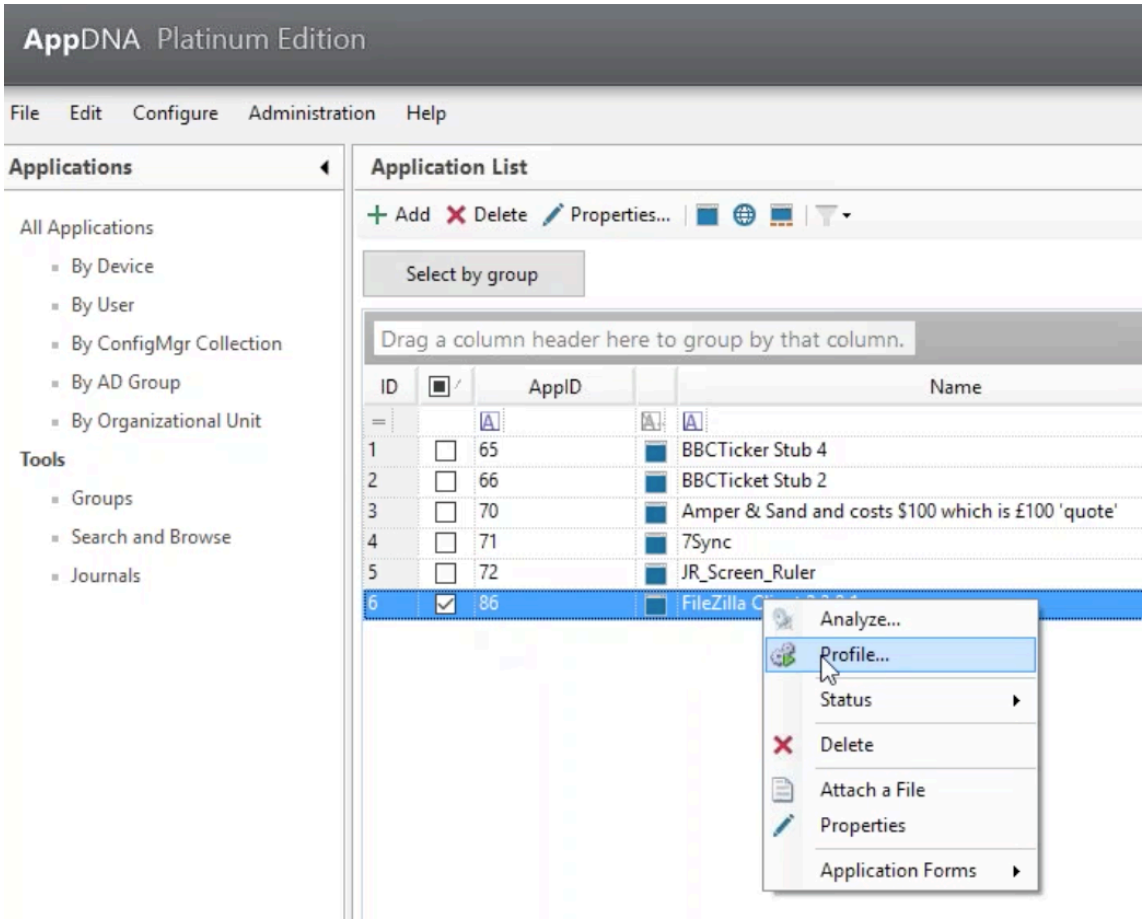
Profile applications

August 1, 2018

Application profiling works in tandem with install capture, however, application profiling collects run-time data from your installed applications. Metrics, like CPU, memory usage, and network utilization are captured while an application is running. Using this information, AppDNA helps you design your virtualization infrastructure requirements. For example, the AppDNA profiling analysis may indicate that a memory intensive application should be spread among multiple RDS servers.

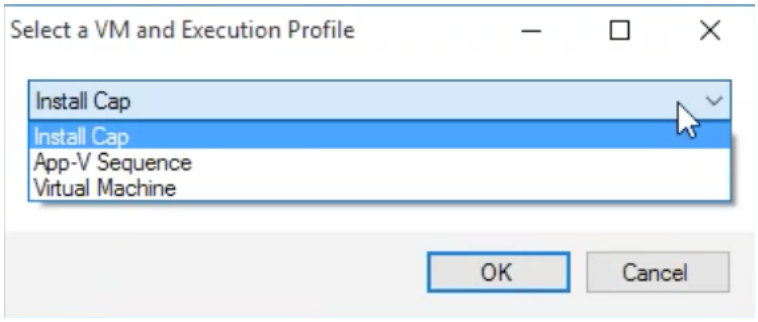
To use application profiling:

1. In the **Applications** tab, select the application you want to profile.
2. Right click to display a context menu; select **Profile**.



Application profiling uses an existing VM configuration profile based on what you specified for install capture.

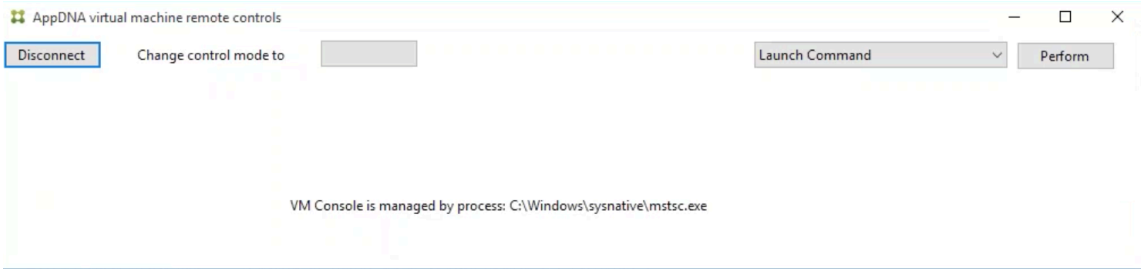
3. In the drop-down menu, select **Install Cap**, click **OK** to begin the profiling process.



AppDNA displays a status message indicating the state of the profiling process.

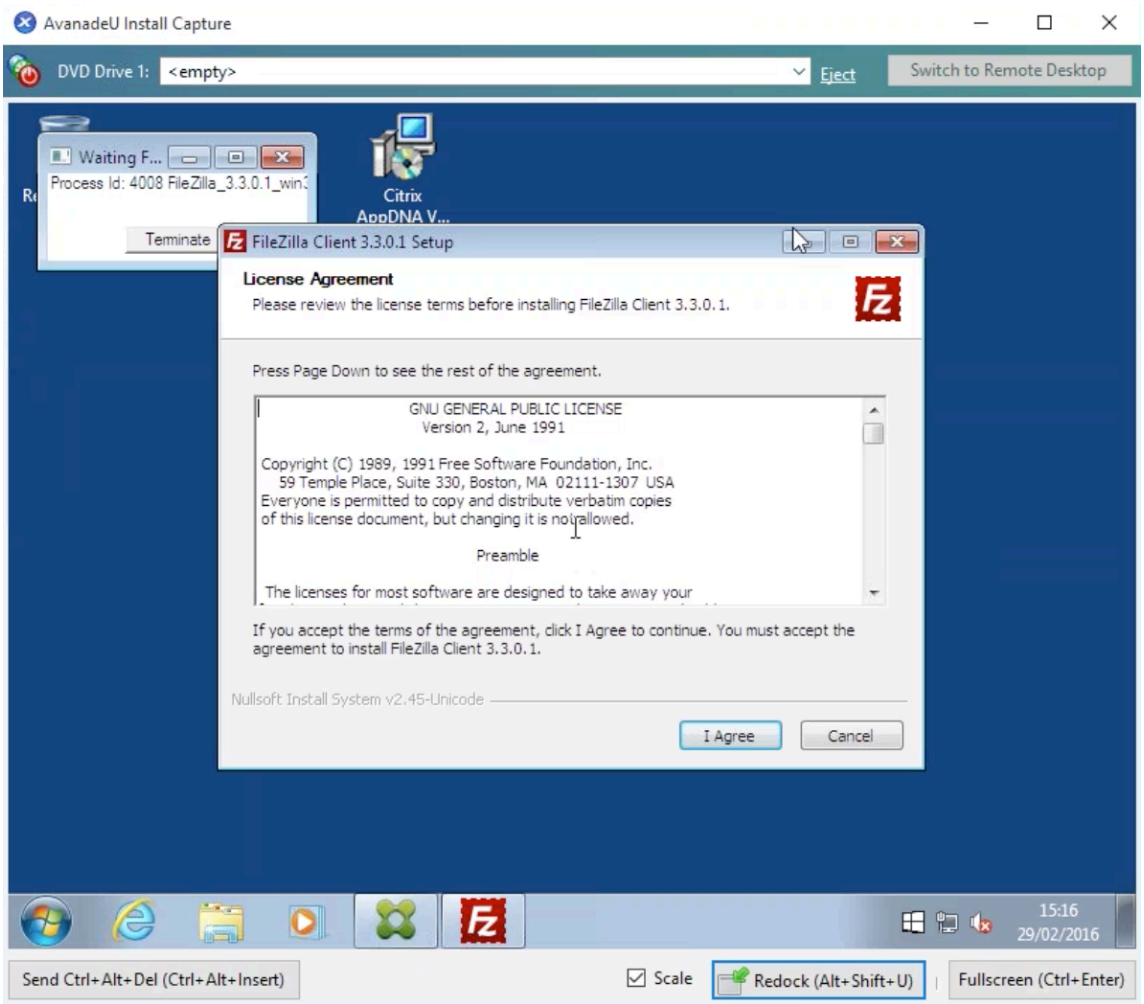
When application profiling begins, AppDNA starts up the machine defined in the selected profile and initiates a RDP session giving you visibility and control over the process.

AppDNA injects (into the machine) the setup file for the application that will be profiled; the application is setup in the same way as it would be for an install capture process, the main difference is that no snapshots of the base OS are taken.



After starting the application profiling process, the auto clicker process is invoked to install the application.

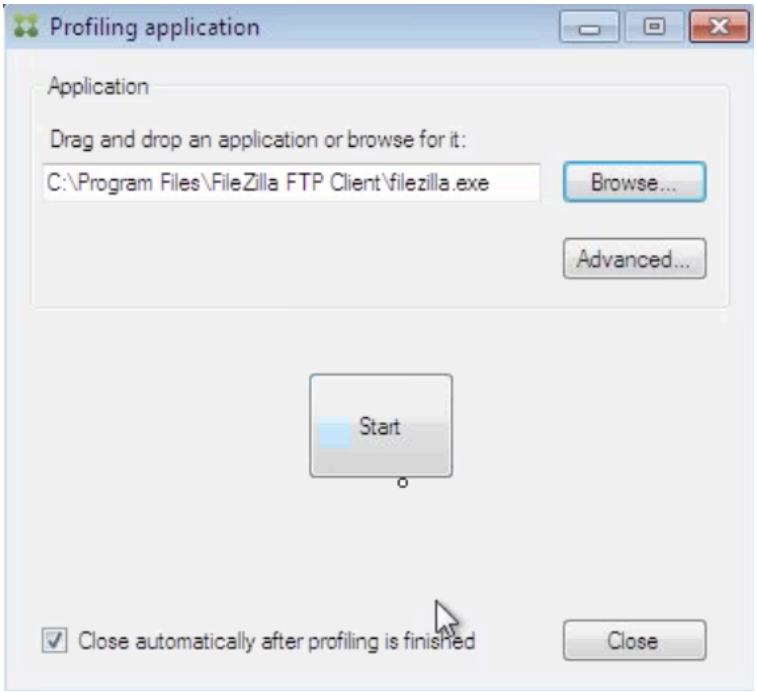
The selected application (in this example, FileZilla) launches its installation Wizard and prompts for RDP connection verification. With auto clicker enabled, no user input is required.



Auto clicker automatically finishes the installation process.

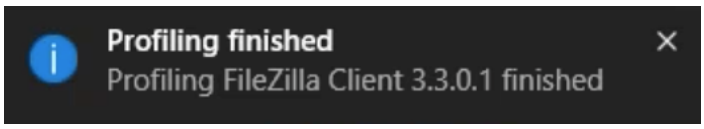
Once auto clicker finishes installing the application, a dialog window appears in the RDS window allowing you to start profiling the application.

4. Click **Start** to begin, or click **Browse** to locate the application's executable file.

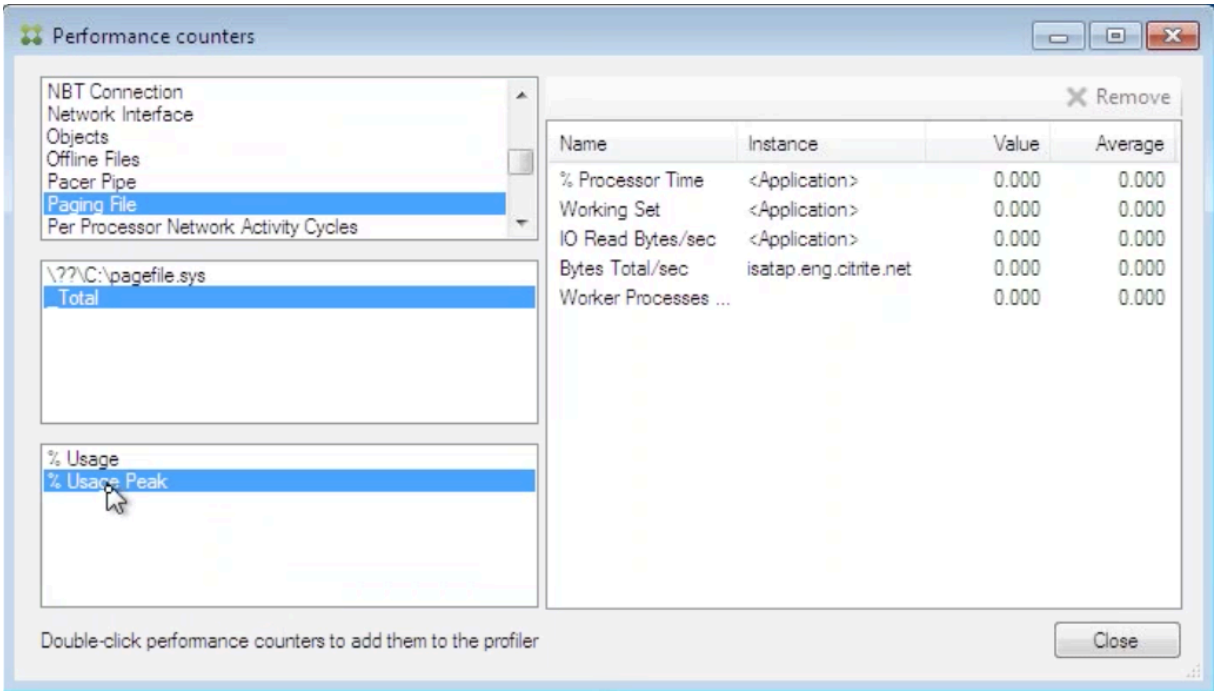


> **Tip**
>
> If the application you want to profile does not automatically launch after clicking **Start**, click **Browse** to locate it and manually launch it.

After clicking Start to initiate app profiling, AppDNA begins scanning the application to determine key metrics. When the process finishes, the interface displays a status message.



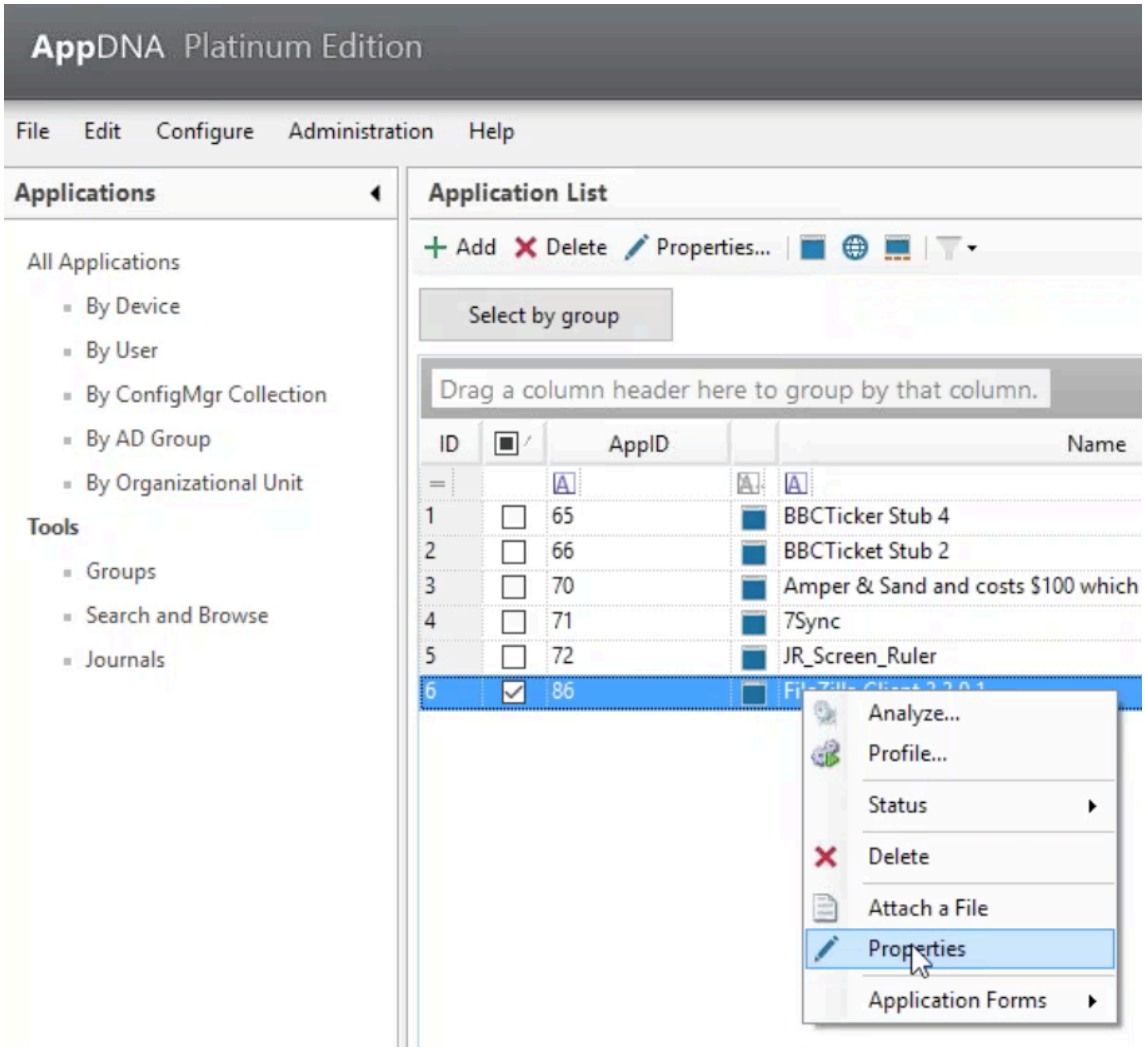
5. To view information related to performance counters, click **Advanced** in the profiling application window.



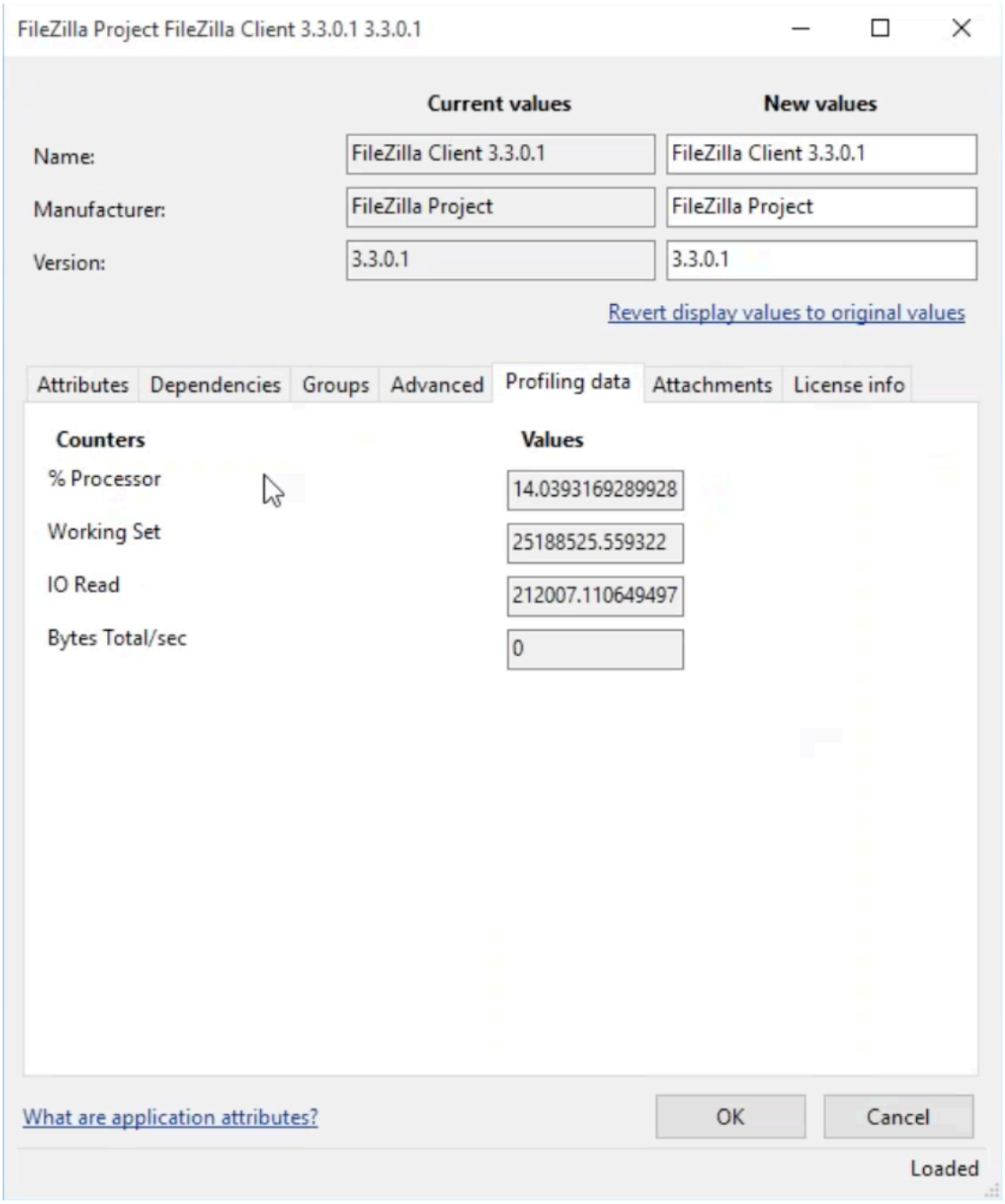
View profiling data

To view application profiling data:

1. Select the application, right click and select **Properties**.



2. In the Properties screen, select the **Profiling data** tab.



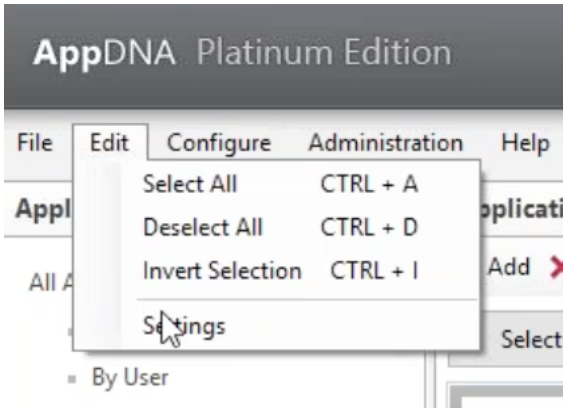
Tip

When using application profiling to display performance metrics for an application, you can set thresholds to address any counters that may exceed an acceptable level. For example, % Processor, Working Set, IO Read, and Bytes Total/sec. Adjust these thresholds using the **Performance data** tab in the **Settings** screen.

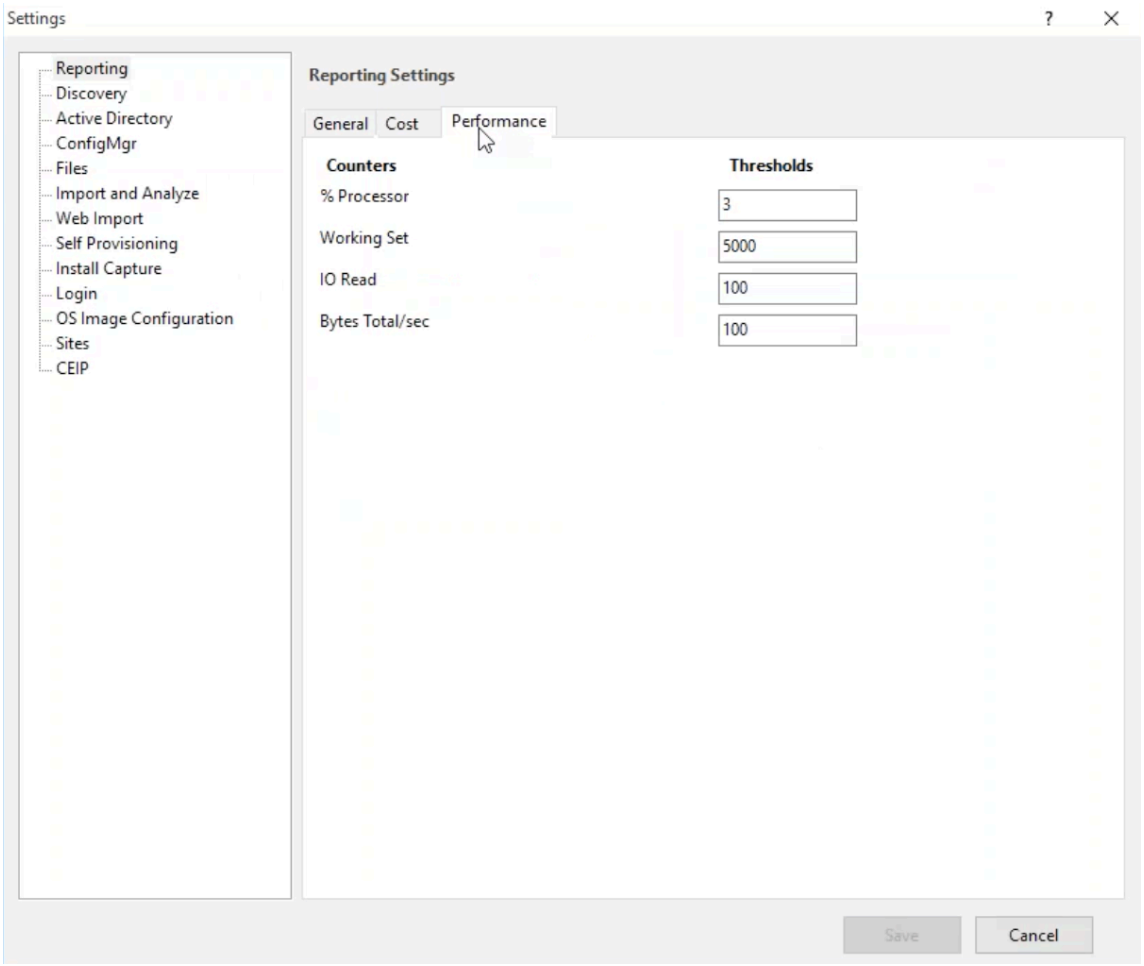
Setting performance related thresholds

To set application profiling performance thresholds:

1. Select **Edit** > **Settings**.



2. In the Settings screen, select **Reporting** > **Performance** tab.
3. In the Performance tab, set thresholds for the following counters:
   - **% Processor**. Displays the threshold for percentage of processor utilized by the selected application.
   - **Working Set**. Defines the amount of memory that a process requires in a given time interval.
   - **IO Read**. Defines the number of input/output reads performed by the application.
   - **Bytes Total/sec**. Represents the total number of bytes used by the application each second.



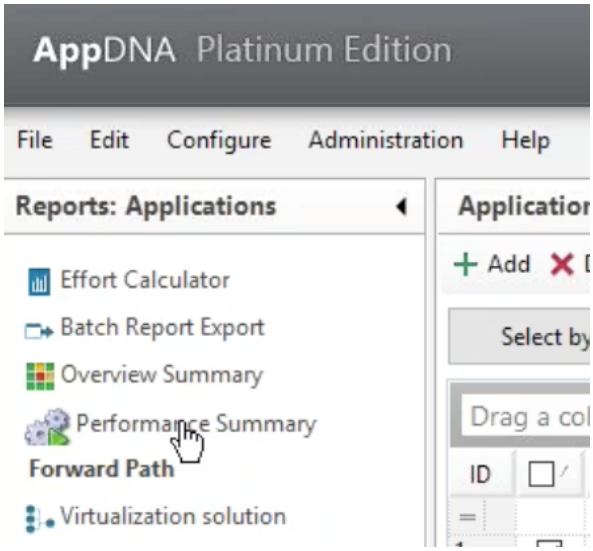
4. Click **Save**.

View additional performance information

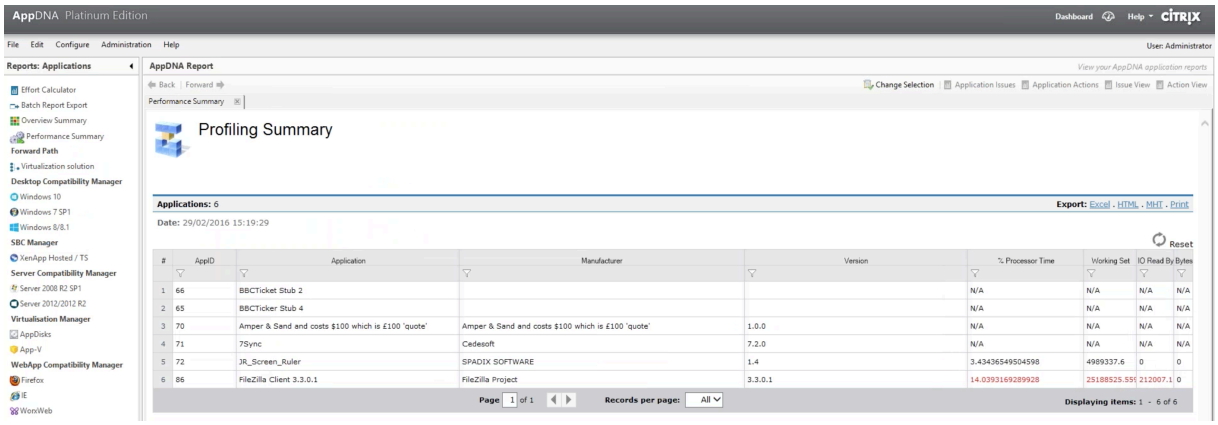
Additional performance information is available for profiled applications.

To view this information:

1. Select **Reports: Applications** > **Performance Summary**.



The **Profiling Summary** screen provides comprehensive, at-a-glance information related to performance characteristics for a profiled application.



> **Tip**
>
> Use the information in the Profiling Summary screen to view thresholds; use the settings screen to set thresholds to improve the performance of your application. For example, if an application uses an extraneous amount of processing, it appears in red. In this example, the application FileZilla allocates a large percentage of available processor. To resolve this, set a lower % Processor threshold in the Settings screen.

Groups

May 5, 2020

Groups are a useful way of organizing applications by user group, location, or application type, for

example. Groups make it easy to review and report on the applications in the group separately from the rest of the portfolio. You can nest groups inside groups.

Use the Manage Groups screen to create and manage application groups, analyze the applications in selected groups, and view reports for the applications in selected groups. A group does not have an overall RAG status and is not shown as a separate item in the Application List or report views.

Create a group

1. From the AppDNA menus, choose Manage > Groups.
2. To nest the new group inside another group, select that group in the tree view on the left side of the Manage Groups screen.
3. On the toolbar, click Create.
4. In the Create Group dialog box, enter a Name and Description.
5. Click the Add button at the bottom of the dialog box.

This creates the new group and displays it in the tree view on the left side of the screen. You can now add applications to the group as described next.

Note: If your edition of AppDNA supports applications managed by Active Directory or Configuration Manager, you can also create groups based on those grouping structures.

Add applications to a group

1. From the AppDNA menus, choose Manage > Groups.
2. In the tree view on the left side of the Manage Groups screen, select the group to which you want to add applications.
3. On the toolbar, click Add to. This opens the Add Applications dialog box.
4. If necessary, you can sort, filter and group applications by a column as described for the Application List.
5. Select the applications you want to add to the group and then click Add.

Note: If your edition of AppDNA supports web applications, you cannot mix desktop and web applications in the same group.

Note: You can also add applications to a group on the
Import Applications screen.

Analyze the applications in a group

1. From the AppDNA menus, choose Manage > Groups.
2. In the Manage Groups screen, select the group(s) that you want to analyze.

3. On the toolbar, click Analyze.
4. Select the reports you want included in the analysis.
5. Click Next on the toolbar. This starts the analysis and opens the Processing Tasks page, which shows the progress. (If you need to cancel the analysis, click Cancel on the toolbar.)
6. When the process finishes, AppDNA displays detailed results. If you want to view the reports now, select the report you want to view and click Finish. Alternatively, you can view reports later.

View reports for the applications in a group

1. From the AppDNA menus, choose Manage > Groups.
2. In the Manage Groups screen, select the group(s) you want included.
3. On the toolbar, select the report that you want to view.
4. On the toolbar, click View Report.

Edit the name and description of a group

1. From the AppDNA menus, choose Manage > Groups.
2. On the left side of the Manage Groups screen, select the group whose details you want to edit.
3. On the toolbar, click Properties.
4. In the Group Properties dialog box, enter the details as required.
5. Click Save.

Journals

August 1, 2018

Use the Journal screen to manually set the compatibility status for applications based on known testing results and to record notes about the testing and remediation of applications. For example, when testing shows that there are issues with an application on a particular platform, you can change the compatibility setting to Known Issues for the corresponding report and enter notes to explain the issues. The amber Known Issues icon will then replace the standard and custom RAG symbols in relevant reports. The journal feature therefore provides a way of manually changing the RAG status for individual applications.

The top part of the Journal screen lists all of the applications in the portfolio. This has features for sorting, filtering and grouping the applications, as described for the Application List.

The lower part of the screen shows details for the application that is selected in the list above. It shows the latest notes that have been entered for the application, the application's details (name, manufacturer, version, and the location of the source files) and a list of any existing manual or external data journal entries that relate to the application. AppDNA handles manual journal entries and external data journal entries through the same journal mechanism. This means that you can delete individual external data journal entries on this screen.

Use the Report drop-down list to select the technology or platform you are working with. The lower part of the screen then shows the application's RAG status for that report and you can create a new journal entry for that report. You cannot change a journal entry, but you can delete a journal entry and add a new one. However, the mechanism is designed to provide a history of entries.

Only the icon of the most recent journal entry is shown on reports. This means that if the latest journal entry is derived from external data, this is shown on relevant reports and the icon from any earlier manual journal entries is not shown. However, this situation generally only arises if you configure the external data after entering manual journal entries. If necessary, you can add the manual journal entry again.

Compatibility status options

Unknown – This is the default setting and the icon is never shown in reports. You can use this option to store notes about the testing and remediation of the application without changing the RAG status in reports.

Compatible – Indicates that testing has shown that the application works on the target technology. When the most recent journal entry has this status, the Compatible icon replaces the standard, custom, and action RAG icons in relevant reports and the RAGs become green.

Known issues – Indicates that testing has shown that the application has issues on the target platform. When the most recent journal entry has this status, the Known issues icon replaces the standard, custom and action RAG icons in relevant reports and the RAGs become amber.

Incompatible – Indicates that testing has shown that the application is incompatible with the target platform. When the most recent journal entry has this status, the Incompatible icon replaces the standard, custom and action RAG icons in relevant reports and the RAGs become red.

Create a journal entry

1. From the AppDNA menus choose Manage > Journals.
2. In the list in the top part of the Journal screen, select the application for which you want to add the journal entry.

3. In the Report drop-down list, select the report to which the entry relates.
4. Select the appropriate compatibility status option.
5. Enter notes that explain the rationale for the compatibility status and record any other relevant information.
6. Click Save (on the toolbar) to save the entry.

Delete a journal entry

1. From the AppDNA menus choose Manage > Journals.
2. In the list in the top part of the Journal screen, select the application for which you want to delete an entry.
3. In the list of journal entries at the bottom of the screen, locate the journal entry that you want to delete. This can be a manually entered journal entry or an external data journal entry.
4. Click the icon in the Delete column.
5. Click Save (on the toolbar) to save your changes.

Search and Browse

August 2, 2018

Use the Search and Browse screen to search for specific files in the application and OS DNA stored in the database and to browse the MSI tables of individual applications.

Search for application files

You can use the Search and Browse screen to find out which applications depend on a specific file, which applications redistribute it, and which OS image provides it. For example, suppose you have a patch that updates a file, and you want to know if it is going to affect any of your applications. You can enter the name of the file and search all the files in every application in your portfolio to see which ones might be affected by the patch.

1. From the AppDNA menus, choose Tools > Search and Browse.
2. In the Search and Browse screen, enter the name of a file in the Search Files text box.
   You can use the percent sign (%) as a wildcard character to represent zero or more characters.
3. Click Submit.

Browse application MSI tables

The MSI tables store information about the changes the application installer will make – for example, which files will be installed and to what location, and which registry entries are created. AppDNA automatically creates MSI tables for all applications, regardless whether they are imported using an .msi file or not.

- From the AppDNA menus, choose Tools > Search and Browse.
- In the Search and Browse screen, click the application's name to browse through the application's MSI tables stored in the database.

Prepare to import

June 17, 2019

You can integrate application intelligence with infrastructure information derived from Active Directory and Microsoft System Center Configuration Manager. That integration provides insight into the managed applications associated with groups of users and whether they are ready to be rolled out on a new platform, for example.

AppDNA can also integrate with Lakeside SysTrack, which audits and tracks actual application use within the enterprise. This feature, called Discover Applications, enables AppDNA to provide information about which applications are used across your enterprise and by how many users and on how many machines.

If you choose to integrate AppDNA with any of those products, you must complete some tasks before you import applications.

Quick links to section topics:

- Integrate data from Active Directory and Configuration Manager
- Discover Applications

Discover Applications

August 2, 2018

This section describes how to use Lakeside SysTrack to discover the applications used in your enterprise. SysTrack integrates with AppDNA. There are other third-party applications that track application use.

Citrix recommends that you use an automated tool for application discovery because it can be very time-consuming to handle that task manually. Typically you take an inventory of applications prior to importing them into AppDNA so that you are aware of all applications used in your enterprise and you are importing only the applications that are in use. This will not only identify any unmanaged applications which could be critical to business, but also tells you what applications are still being used, and whether you have duplicate applications with overlapping functions.

The Discover Applications feature in AppDNA integrates with, and relies upon, Lakeside SysTrack, which audits and tracks actual application use within the enterprise. Before you can use the Discover Applications screen, you need to configure a connection with the SysTrack database. You do this in Discovery settings, which you can open by choosing Edit > Settings from the menus.

Once the connection to the SysTrack database is configured successfully, the Discover Applications screen lists the applications that SysTrack has tracked. This enables you to see which applications are used across your enterprise and by how many users and on how many machines.

To open the Discover Applications screen:

- From the side bar, choose Import & Analyze > Discover Applications.

Note: In this section, discovered application means an application that has been tracked by SysTrack and managed application means an application that is deployed through Active Directory or Configuration Manager.

Quick links:

- Rationalize applications
- Filter discovered applications
- Link discovered and managed applications
- Import discovered applications

Rationalize applications

August 1, 2018

This topic provides an overview of rationalizing applications in the Discover Applications screen. In this context, rationalization involves examining your inventory of applications and deciding which ones to keep (and if relevant to import into AppDNA) and which ones to discard. The Discover Applications screen provides the raw inventory of Windows applications that have been tracked by SysTrack.

As you work through the applications in the Discover Applications screen, you change their rationalization status from the initial Review status to Migrate or Retire. You can do this for individual applications by using the drop-down list in the Rationalize column. To change the rationalization status

for multiple discovered applications, CTRL-click or SHIFT-click the applications in the Rationalize column, then right-click and from the shortcut menu, choose Review, Migrate, or Retire.

Dealing with duplicates – Typically there is some duplication in the applications – particularly those that are not managed. You may find, for example, that an application appears five or six times and the only difference between them is in the build or revision part of a version number that has the form major.minor.build.revision. Typically, you only want to keep or migrate one or two of these – usually the latest one. (Sometimes you may find duplicates that are apparently identical. These have differences in their package or installation unique identifiers – called GUIDs – which are not shown in the main list.

Use the Duplicates Filter discovered applications to restrict the list of applications to those that have duplicates. This also sorts the applications so that they appear in name, manufacturer, and version order. This means that the duplicate applications appear next to each other in the list. Be aware that if you have filtered the list in other ways (for example, on the number of active users), this may have filtered out some of the duplicates. Set the Rationalize status to Migrate for the applications you want to keep and to Retire for those you want to discard.

Installation and usage statistics – The Discover Applications screen has columns that show the number and percentage of machines on which each application has been installed and on which it has been used. Columns also provide a variety of usage statistics. This provides useful information when you rationalize your applications.

You can sort the list of applications by the data in any of the columns (simply click the column header, and click it again to reverse the sort order). You can also filter the list of applications on the data in these columns. There are a number of quick filters that make this easy.

Note: These statistics are provided for each individual application and do not show aggregated statistics for groups of duplicate applications. When you filter on these columns, some of the applications in a group of duplicates may be excluded and some included.

Managed applications – If you manage applications through Active Directory or Configuration Manager, you can link discovered applications with the corresponding managed application. The discovered application then has a check mark in the Managed column.

Export rationalization decisions for review – You can use the Export > Current View option on the toolbar to export your rationalization decisions for review.

Import discovered applications into AppDNA – Once you have decided which applications you want to keep and potentially migrate, you need to import them into AppDNA. In order to do this, you need the application's installation package or App-V (.sft or .appv) file. The installation package can be in the form of a Windows installer package (.msi file) or another type of installation package. If the discovered application is managed through Active Directory or Configuration Manager, you can match the discovered application with the managed application's deployment information and then import

that. For other applications, you can export a list, in which you then fill out the name and location of the installation package before using it to import the applications into AppDNA.

Filter discovered applications

August 1, 2018

Quick filters make it easy to quickly restrict the list of discovered applications, such as according to their rationalization status or the number or percentage of machines on which they are installed. The Filter toolbar in the Discover Applications screen provides several filters.

You can apply multiple quick filters. For example, you can use the Review quick filter to show discovered applications that are marked for review, the Migrate and Retire quick filters to hide discovered applications marked for migration and retirement, respectively, and a Usage quick filter to show only discovered applications that have been used in the past month. Click Clear Filters on the right side of the toolbar to clear all quick filters.

You can also create filters based on the data in any column, as described for the Application List in Filter applications. The Clear Filters button does not clear customer filters. However, you can clear them individually.

The filters in the first set of quick filters have a simple on and off state, which are indicated by the  and icons, respectively. These quick filters are as follows:

- **Duplicates**

   Show only discovered applications that have duplicates. This also sorts the applications so that they appear in name, manufacturer, and version order. This means that the duplicate applications appear next to each other in the list. Applications are considered duplicates if their name and manufacturer are the same.

   Do not restrict the list to discovered applications that have duplicates. This means that the list includes discovered applications for which there are no duplicates.

- **Review**

   Show discovered applications that are marked for review.

   Hide discovered applications that are marked for review.

- **Migrate**

   Show discovered applications that are marked for migration.

   Hide discovered applications that are marked for migration.

- **Retire**

   Show discovered applications that are marked for retirement.

   Hide discovered applications that are marked for retirement.

The second set of quick filters enables you to quickly filter the list of discovered applications based on the percentage of machines they are installed on, the percentage of active machines and users that actually use the applications, and how frequently they are used:

- **Installed machines** – Restrict the discovered applications according to the percentage of machines that they are installed on. For example, the Most option shows applications that are installed on 76-100% of all of the machines that have been identified by SysTrack. The filter drop-down displays the number of applications (apps) that meet each criteria (taking into account any other filters that have been applied).
- **Active machines** – This is similar to the Installed Machines quick filter, except that it restricts the discovered applications according to whether they have actually been used. In this context an active machine is a machine on which the application has actually been used in the period of time that the SysTrack database covers.
- **Active users** – Restrict the discovered applications according to the percentage of users who have actually used them. For example, the Many option shows discovered applications that have been used by 26-75% of users. The filter drop-down list displays the number of discovered applications (apps) that meet each criteria after any other active filters have been applied.
- **Usage** – Restrict the discovered applications according to when they were last used. As with the other quick filters in this group, the drop-down list displays the number of discovered applications (apps) that meet each criteria after any other active filters have been applied.

Link discovered and managed applications

August 1, 2018

If you have imported Active Directory or Configuration Manager data into AppDNA, you can link discovered applications with the managed applications.

Note: After importing or changing the Active Directory and Configuration Manager data, click Refresh on the toolbar to see those changes in this screen.

To link discovered and managed applications

1. From the side bar, choose Import & Analyze > Discover Applications.

2. In the Discover Applications screen, optionally, use the Best Suggestion column to exclude discovered applications for which there is not a match with a managed application:

   a) Select None from the drop-down list in the row immediately below the Best Suggestion column header.
   b) Click the A icon on the left of the drop-down list.
   c) Select Does not equal.

   This restricts the list of discovered applications to those for which there is a suggested match with a managed application.

3. In the list of discovered applications, click the application that you want to link with a managed application.

   If AppDNA finds matching managed applications, it lists all of the installations for those applications. The same application can have multiple installations (for example, Per-system attended, Per-system unattended, Per-user attended, Per-user unattended, Per-system uninstall, and Per-user uninstall).

4. To accept a match, select an installation. Make sure it is an appropriate type of installation and not an uninstall or repair command. If one of the installations with which you want to create the match has been imported, select it. (A check mark in the Imported column indicates the item has already been imported.)

   AppDNA then displays a check mark in the Managed column in the upper part of the window.

5. Click Save on the toolbar.

Import discovered applications

August 1, 2018

To import a desktop application into AppDNA, you need its installation or App-V (.sft or .appv) package file. The installation package can be in the form of its Windows installer package (.msi file) or another type of installation package. For an application that is managed through Active Directory or Configuration Manager, you can simply match the discovered application with the managed application and import that using the Active Directory or Configuration Manager deployment information. For un-managed applications, you need to locate the installation package and specify that in the Import Applications screen. The easiest way to do this is explained below.

Import discovered applications that are managed

Note: You can import only managed applications that are installed by using an MSI package as described below. For other types of installers, use the Managed Applications screen to import them into AppDNA.

1. From the side bar, choose Import & Analyze > Discover Applications.
2. Link the discovered and managed applications as described in Link discovered and managed applications.
3. On the toolbar in the Discover Applications screen, click Add to import list.

   This takes you to the Import Applications screen, where the selected applications that have not already been imported are listed on the Direct Import tab. For information about this, see Direct import.
4. On the toolbar in the Import Applications screen, click Import.

Import discovered applications that are not managed

1. From the AppDNA side bar, choose Import & Analyze > Discover Applications.
2. Filter the list of discovered applications so that it matches the applications you want to import. See Filter discovered applications for information about filtering the list.
3. On the toolbar in the Discover Applications screen, choose Export > Application Import List.
4. In the Save As dialog box, specify a suitable name and location for the export file and click Save.

   This saves the list of applications in a CSV file that you can use as an import list in the Import Applications screen. For more information about using import lists, see Import from List.
5. Open the file in Excel.
6. In the Filename column, enter the name and location of each application's installation package, such as \\server\folder\filename.msi. If it is an .msi, .sft, or .appv file, leave the Execution Profile column blank. If the installation package is in any other format, enter the name of the Execution Profile to be used.
7. Optionally, enter /s in the Silent Switch column and the name of the group you want to import the application into in the Group column.
8. When you have finished adding the details, save the file in CSV format.
9. From the AppDNA side bar, choose Import & Analyze > Import Applications.
10. On the toolbar in the Import Applications screen, click Import from List, select the file you saved in step 8, and then click Import.

This lists the applications on the screen. You can now import the applications in the normal way.

Discovery settings

August 1, 2018

The Settings dialog box contains general AppDNA options. To open the Settings dialog box, choose Edit > Settings from the menus.

Use the Discovery page in the Settings dialog box to enter the connection details for the Lakeside SysTrack database. AppDNA uses the SysTrack database to provide information about the applications used within the enterprise. See Discover Applications for more information.

The options are:

Server name – This identifies the server that hosts the SysTrack database. Enter this as Machine\Instance, where Machine is the name of the machine that hosts the SQL Server installation and Instance is the SQL Server instance if a named SQL Server instance is in use. If a named instance is not in use, omit the backslash (\).

Database name – The name of the SysTrack database in SQL Server.

Authentication – Select the type of authentication to be used to connect to the SysTrack database. The options are:

- **Windows Authentication** – This type of authentication uses the logged on Windows user account when connecting to the database.
- **SQL Server Authentication** – For this type of authentication you must provide an appropriate username and password.

User name – If you chose SQL Server Authentication above, enter the user name to use when AppDNA connects to the SysTrack database. Leave this blank for Windows Authentication.

Password – If you chose SQL Server Authentication above, enter the password to use when AppDNA connects to the SysTrack database. Leave this blank for Windows Authentication.

Test – Click to test the connection. If this is successful, AppDNA displays “Success” and if not, it displays an error message. If necessary, use the information in the error message to correct the problem and then test the connection again.

Click Save to preserve your changes.

Columns

August 1, 2018

This topic provides information about the columns in the Discover Applications screen. You can drag a column to group the discovered applications by the data in that column, as described in Application list.

The columns in the Discover Applications screen are as follows:

Rationalize – The discovered application's rationalization status – this can be Review, Migrate, Retire. Initially discovered applications are in the Review state. You change this manually by using the drop-down list in this column. To change this for multiple discovered applications, CTRL-click or SHIFT-click the applications in this column, right-click and from the shortcut menu, choose Review, Migrate, or Retire.

Name – The name of the application. Click to open the Application Details dialog box, which shows detailed information about the application, including the names of the users who have run the application and the machines on which it has been run. This is useful if, for example, you are having difficulty locating the application's installer and want to contact the people who actually use the application. See Discovered application details for more information.

Manufacturer – The manufacturer of the application.

Version – The application's version number.

Installed machines – The number of computers on which the application has been installed.

% Installed machines – The number of computers on which the application has been installed expressed as a percentage of all of the computers that SysTrack has tracked. This value is rounded to a whole number – which means, for example, that 0% may represent a small number of machines and 100% may not represent all machines.

Active machines – The number of computers on which the application has actually been used in the period of time that the SysTrack database covers.

% Active machines – The number of active computers expressed as a percentage of the total number of computers on which the application is installed.

Active users – The number of users who have actually used the application in the period of time that the SysTrack database covers.

% Active users – The number of active users expressed as a percentage of the total number of users of the application.

Usage count – The total number of times the application has been used in the period of time that the SysTrack database covers.

Usage per year – The usage count divided by the number of years that the SysTrack database covers.

Usage per month – The usage count divided by the number of months that the SysTrack database covers.

Usage per day – The usage count divided by the number of days that the SysTrack database covers.

First usage – The earliest date that SysTrack detected the use of the application.

Last usage – The most recent date that SysTrack has detected the use of the application.

Managed – Indicates whether the application has been matched to an application that is managed through Active Directory or ConfigMgr.

Imported – Indicates whether the managed application with which the discovered application has been matched has been imported into AppDNA.

Best Suggestion – Indicates whether there are any managed applications that are possible matches for the application and if so, how close the match is. Possible values are: Perfect, Excellent, Good, Average, Poor, None. For information about how AppDNA does the matching, see Matching algorithm.

Discovered application details

August 1, 2018

The Application Details dialog box provides detailed information about a selected discovered application. To open the Application Details dialog box, in the Discover Applications screen locate the discovered application whose details you want to view, and click its name.

The Application Details dialog box has three tabs:

Application – Shows the application's name, manufacturer, version, and installation and package identifiers (called GUIDs). Differences in one or both of these GUIDs when all other details are the same can lead to what appears to be duplicate identical applications in the list of discovered applications. They appear to be identical because the GUIDs are not shown in the list.

Users – Lists the domain qualified username of all the users who have used the application recently, along with the date of last use. This is useful if, for example, you are having difficulty locating the application's installer and want to contact the people who actually use the application.

Devices – Lists the names of the computers on which the application has been run, along with the date of last use.

Click OK to close the dialog box.

Matching algorithm

August 1, 2018

When searching for matches between discovered and managed applications, AppDNA compares the application name, manufacturer, and version, and awards points. The Discover Applications screen includes a Best Suggestion value that indicates whether there are any managed applications that are possible matches for the application and if so, how close the match is.

The points awarded are as follows.

Detail	Full Match	Partial Match
Name	50 points	25 + 1 point per word
Manufacturer	10 points	1 point per word
Version	10 points	1 point per word

AppDNA adds the points and assigns a confidence value to the match as follows:

Best Suggestion values	Total Points
Perfect	70
Excellent	More than 50
Good	More than 45 (Partial match on name + full match on manufacturer AND version)
Average	More than 35 (Partial match on name + full match on manufacturer OR version)
Poor	More than 25
No Match	Less than 25

Integrate data from Active Directory and Configuration Manager

August 2, 2018

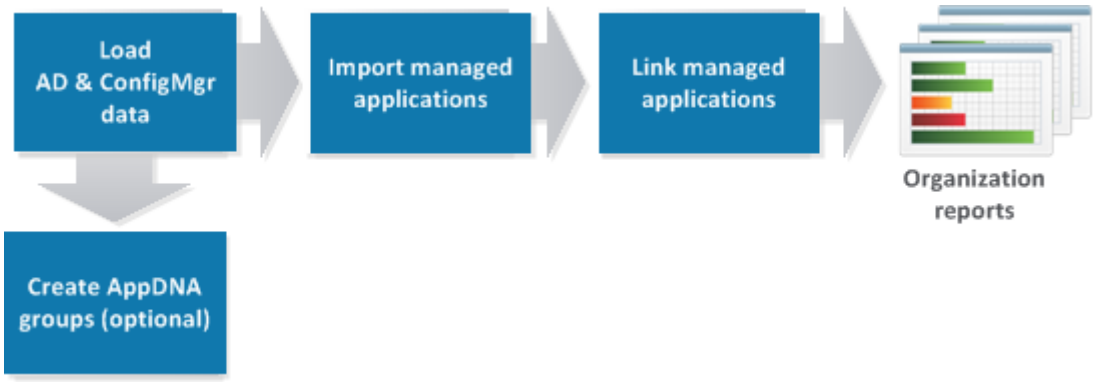
Active Directory and System Center Configuration Manager are two widely used system management tools from Microsoft. They are rich sources of information about the infrastructure of the organization

and the deployed applications. Applications deployed by Active Directory or Configuration Manager are referred to as managed applications in this documentation.

You can load information from Active Directory and Configuration Manager into AppDNA. This has several advantages:

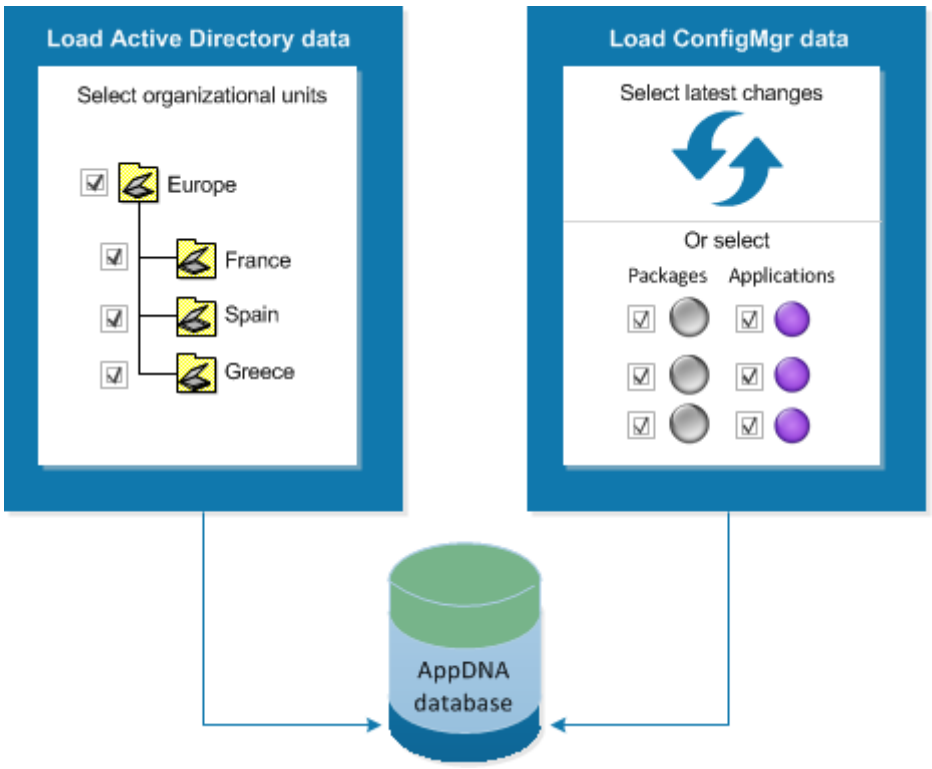
- You can use that deployment information to import the managed applications into AppDNA.
- You can use the organization reports in AppDNA to get an overview of groups of users and computers, and their associated managed applications, and whether they are ready to be rolled out on a new platform, for example.
- Forward Path can utilize the rich deployment data to perform automated tasks, such as sequencing applications for App-V.

The following diagram represents the steps for integrating Active Directory and Configuration Manager data into AppDNA. For the organization reports to provide meaningful data, there are three steps that you must carry out. These, and the optional creating AppDNA groups step, are described briefly under separate headings below, with links to more detailed documentation.



Load Active Directory and Configuration Manager data

The first step is to load the Active Directory and Configuration Manager data. When loading data from Active Directory, you select the organizational units (OUs) that you want to load, and AppDNA automatically loads them into the AppDNA database, along with the associated Active Directory groups, users, and computers, and the deployment information for any applications that have been deployed to those entities. When loading the data from Configuration Manager, you have the choice of automatically loading all of the changes since you last loaded the data or of manually selecting the packages and applications that you want to load (individually or in batches). Regardless which option you choose, AppDNA extracts and loads packages and applications, along with the deployment information, and the details of the associated collections, users, and computers.



You can load the data directly from within AppDNA. Alternatively, you can download a .zip file that contains a stand-alone extraction tool and synchronization data, which you (or the administrator) can use to extract the data on the server. You then load the results into AppDNA. This is useful because the stand-alone tool can be run on the Active Directory domain controller or Configuration Manager server, separately from AppDNA.

Once loaded into AppDNA, managed applications are handled like any other application. In some screens, managed applications are referred to as packages (even if they are deployed using Configuration Manager).

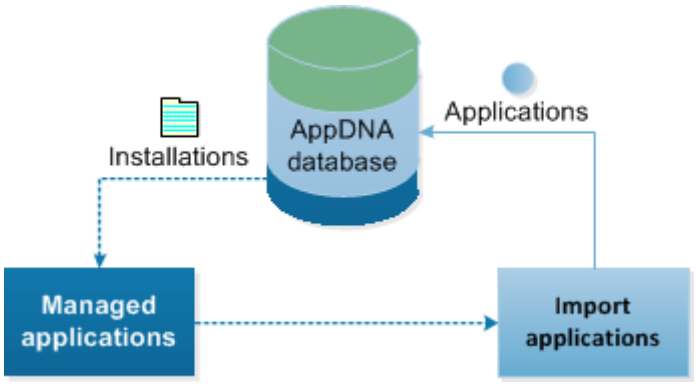
See Load Active Directory and Configuration Manager Data for more information.

Import managed applications

After you have loaded the Active Directory and Configuration Manager data, you can import the applications that have been deployed using them. You do this in the Managed Applications screen, which lists all of the applications managed through Active Directory and Configuration Manager whose deployment information is stored in the AppDNA database. You select the ones you want to import and AppDNA transfers them to the Import Applications screen, where you can import them using the Active Directory or Configuration Manager deployment information (called installations in AppDNA).

For applications that are deployed through the legacy Configuration Manager package and program mechanism, an installation represents a Configuration Manager program. Typically applications that

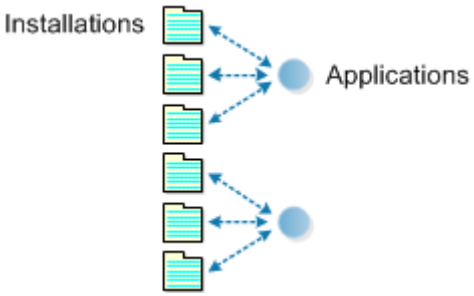
are deployed in this way have multiple installations. For applications that are deployed through the new Configuration Manager 2012 application mechanism, an installation corresponds to a deployment type.



See Import managed applications for more information.

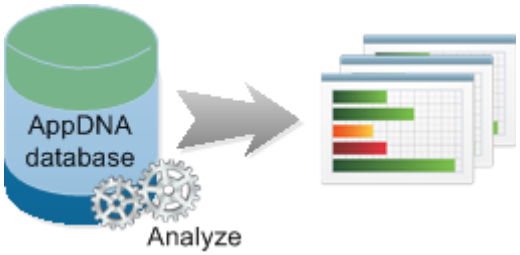
Link managed applications with applications already in AppDNA

You can link managed applications with applications that have already been imported into AppDNA. Depending on how the data has been configured in Configuration Manager, there may be multiple installations for a single managed application. For example, for a single managed application that has been deployed using the Configuration Manager package model, there may be installations called “Per-system attended”, “Per-system unattended”, “Per-user attended”, and “Per-user unattended”, which all point at the same installation package. In this situation all of the installations that relate to the same managed application can be linked to the same application in AppDNA.



See Link managed applications for more information.

View organization reports



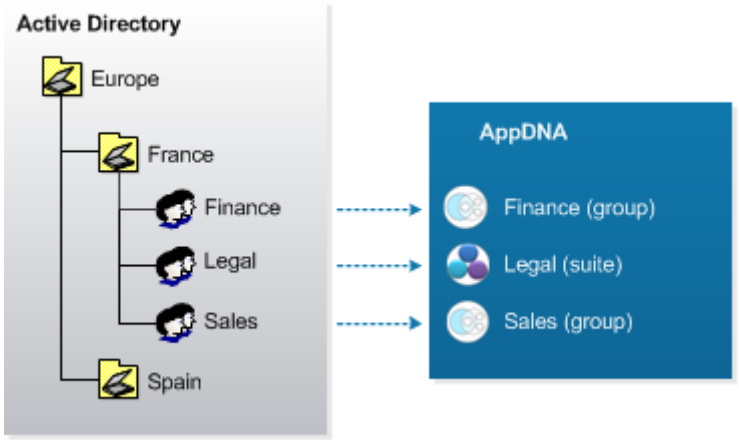
After completing the steps described above and running the standard AppDNA analysis step, you are ready to explore your organization data. You can use the Users and Computers screen to explore the Active Directory and Configuration Manager entities – organizational units, Active Directory groups, Configuration Manager collections, users, and computers. From here you can select groups of users (for example) and view a summary report showing the status of the managed applications that have been deployed to them. You can drill down into the standard AppDNA report views for those applications.

In this way you can view the compatibility status of the managed applications that are deployed to users in key departments, for example.

See Organization data in the Users and Computers screen for more information.

Create AppDNA groups

You can optionally create AppDNA groups based on Active Directory and Configuration Manager grouping structures. AppDNA groups are separate and different from the grouping structures in Active Directory and Configuration Manager. In AppDNA, you use groups to organize your applications – for example, so you can quickly and easily report on the specialized applications used by the finance team.



Because managed applications are deployed to the Active Directory and Configuration Manager grouping structures, it is often useful to create AppDNA groups based on those structures. When

you do this, the applications associated with those structures are automatically added to the new AppDNA group. For example, if you create an AppDNA group based on the Active Directory Finance group, the managed applications that were deployed to that group are automatically added to the new AppDNA Finance group.

Creating an AppDNA group in this way enables you to conveniently report on these applications in AppDNA. This gives you a different view compared to the organization reports, which show the status of all of the applications deployed to the users and computers in the Active Directory group.

For example, users in the Finance Active Directory group may also be in the All Users Configuration Manager collection, to which Microsoft Office applications are deployed. When you view an organization report for the Finance group, you will see the status of the specialized finance applications deployed to the Finance group and also the Microsoft Office applications that are deployed to the All Users Configuration Manager collection. Whereas when you view the standard AppDNA reports for the AppDNA Finance group, you see only the specialized applications that were deployed to the Finance Active Directory group.

Note: If additional applications are subsequently deployed to the Finance Active Directory group (for example), they will not be reflected in the AppDNA group, unless you update it manually.

See Create groups from Active Directory and Configuration Manager collections for more information.

Key Terms

August 1, 2018

This topic provides brief definitions of some key terms used in AppDNA topics related to Active Directory (AD) and Microsoft System Center Configuration Manager. If a term (such as group) has different meanings in AD and Configuration Manager compared to AppDNA, it is prefixed with AD or Configuration Manager to distinguish it from the AppDNA term.

Key AppDNA integration terms

- managed application

  An application that is deployed through Active Directory or Configuration Manager. Once loaded into AppDNA, all managed applications are handled in a standard way, regardless of how they are deployed. In some screens, managed applications are referred to as packages (even if they are deployed using Configuration Manager).

- installation

Represents an installation mechanism used to deploy an application through Active Directory or Configuration Manager. For applications that are deployed through the legacy Configuration Manager package and program mechanism, an installation represents a Configuration Manager program. Typically applications that are deployed in this way have multiple installations. For applications that are deployed through the new Configuration Manager 2012 application mechanism, an installation corresponds to a deployment type.

Active Directory terms

- Active Directory

  A directory service from Microsoft, which provides a central location for network administration and security, single sign-on for user access to networked resources, standardization of access to application data, deployment and update of applications, and synchronization of directory updates across servers. All of the information and deployment settings are stored in a central database.

- organizational unit (OU)

  A container for users, computers, and groups in Active Directory. Every user, computer, and group is located in one specific OU. The Active Directory is organized into a hierarchical tree of OUs. There is flexibility in how the OU tree is structured – some organizations structure it by function, others by geographical location, for example.

- Group Policy Object (GPO)

  A collection of policies that apply to selected Active Directory users or computers. GPOs are linked to OUs and targeted at users and computers. Two conditions must be met in order for a GPO to apply to a particular user or computer. Firstly, the user or computer must belong to an OU or sub-OU to which the GPO is linked. Secondly, the user or computer must be directly targeted or belong to a group to which the GPO is targeted.

- AD package

  A particular type of GPO policy that is used to deploy software. It provides native support for MSI deployment.

- AD group

  Represents a collection of AD users and computers. Membership of a group is static – members are added to a group explicitly. Groups can be nested and members can belong to more than one group.

- AD computer

  Represents the domain account of a computer joined to a Windows domain. This might be a physical or virtual machine or a dummy account that is used for authentication purposes.

- AD user

  Represents the logon account of a user who can log onto a Windows domain – some users represent real people and others represent service accounts and email recipients.

Configuration Manager terms

- System Center Configuration Manager

  A Microsoft systems management tool for managing large groups of Windows-based computer systems. Configuration Manager provides remote control, patch management, software distribution, operating system deployment, network access protection, and hardware and software inventory. Like Active Directory, all of the information and deployment settings are stored in a central database.

- Configuration Manager collection

  Represents a collection of Configuration Manager computers and Configuration Manager users. In Configuration Manager 2007 and earlier, collections can be nested. However, this is not possible in Configuration Manager 2012. Membership of Configuration Manager collections is pseudo-dynamic – members can be added explicitly. However, rules can also be defined which determine which users and computers to include in the collection. The collection is refreshed on a schedule but not each time the collection is queried.

- Configuration Manager computer

  Represents the domain account of a computer joined to a Windows domain. This might be a physical or virtual machine or a dummy account that is used for authentication purposes.

- deployment type

  Contained in a Configuration Manager application, this stores the information that is required to install the application, and rules that specify when and how it is deployed. A Configuration Manager application must have at least one deployment type. Within AppDNA, deployment types are referred to as installations.

- Configuration Manager package

  Represents a folder that contains files. Configuration Manager tracks packages as they are replicated between sites.

- Configuration Manager program

  Represents an operation that is performed on, or with, the files contained within a Configuration Manager package, such as install or uninstall. Within AppDNA, Configuration Manager programs are referred to as installations.

- Configuration Manager application

  Represents an application that is deployed and managed through the Configuration Manager 2012 application model.

- Configuration Manager user

  Represents a user within the enterprise. Typically Configuration Manager discovers users through interrogating Active Directory.

Discovery terms

- SysTrack

  A suite of IT business intelligence products from Lakeside Software. SysTrack includes functionality that audits and tracks application use within the enterprise. AppDNA uses the results of this tracking in the Discover Applications screen.

- discovered applications

  Applications whose usage has been tracked by SysTrack across the organization. Discovered applications are listed on the Discover Applications screen.

Other AppDNA terms

- group

  A logical container for applications in AppDNA. Groups are similar to folders in Windows Explorer – they provide a way of structuring your application portfolio by user group, location, or application type, for example. Groups make it easy to review and report on the applications in the group separately from the rest of the portfolio. A group does not have an overall RAG status and it is not shown as a separate item in reports.

See also

For a more complete glossary of AppDNA terms, see AppDNA glossary.

Load Data

August 1, 2018

To use the Organization Reports feature, which shows the status of managed applications by division or department (for example), you must first load your Active Directory (AD) and System Center Configuration Manager data into AppDNA.

The AppDNA Load AD and ConfigMgr Data wizard provides options to load data directly or indirectly from AD and Configuration Manager. The indirect option involves downloading a tool that can be run remotely from AppDNA – for example, a Configuration Manager administrator can run it on the Configuration Manager server. This is useful when you do not have the required credentials to do this from the AppDNA machine.

AppDNA extracts the AD and Configuration Manager data using a read-only API, which means that it does not change the data in AD or Configuration Manager.

When extracting data from Active Directory, you select the organizational units that you want to load into AppDNA. AppDNA automatically extracts and subsequently loads into the AppDNA database all of the associated AD groups, users, and computers, and the deployment information for any applications that have been deployed through AD to those entities. If you want to extract data from multiple domains (for example, all of the domains that belong to a forest), you need to run through the wizard for each domain.

When extracting data from Configuration Manager, you have the choice to automatically extract all of the relevant changes since the last extraction or to select the packages and applications (individually or in batches) that you want to load. This extracts and loads the selected packages and applications and all of the associated Configuration Manager collections, users, and computers, along with the deployment information. If a package or application that has been deleted is included, AppDNA removes the corresponding Configuration Manager data from the AppDNA database. However, AppDNA retains the associated application if it has been imported into AppDNA while removing any links to the deleted Configuration Manager entities.

Note:

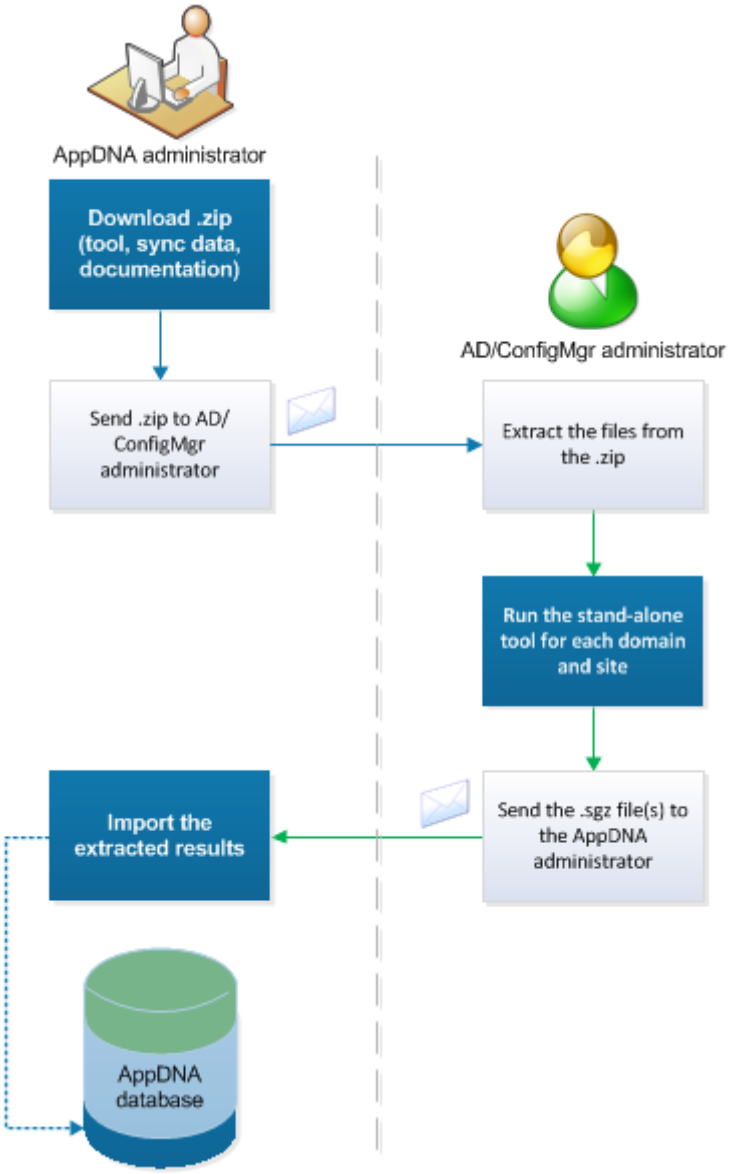
- For best results, load both Active Directory and Configuration Manager data into AppDNA. Typically Active Directory provides rich data about organizational structure and Configuration Manager provides data about applications that are managed centrally.
- Extracting data from a large Configuration Manager site can take a considerable amount of time. The more users and devices there are, the longer the process takes. When extracting data from large Configuration Manager sites, Citrix recommends that you extract the data in batches of 2,000 applications or packages (or a mixture of both) and run the extraction overnight. (In this context, a large Configuration Manager site is one that has a total of more than 5,000 packages and applications, and/or more than 50,000 users or computers.)

Load Active Directory and Configuration Manager data indirectly

August 1, 2018

The option to load Active Directory and Configuration Manager data indirectly enables the data to be extracted on the Active Directory domain controller or Configuration Manager server separately from AppDNA. This means that AppDNA users do not need to request administrator access to that data, and the Active Directory and Configuration Manager administrators do not need to install AppDNA.

The following diagram provides an overview of the procedure.



1. From the AppDNA menus, choose Configure > AD & ConfigMgr > Load Data.

   This opens the Load AD & ConfigMgr Data wizard. By default, the wizard opens on the Load Type

step. However if you have already opened the wizard since you last logged on to AppDNA, the wizard reopens where you previously left off. If necessary, click Previous to return to the Load Type step.

2. In the Load Type step, select Indirect Load, and then click Next.
3. In the Indirect Load step, click Download and save the .zip file in a suitable location.

   The .zip file contains the stand-alone extraction tool, synchronization data, and documentation (.pdf file) for running the tool.
4. Send the .zip file to the person who will be running the stand-alone extraction tool. Typically this is the Active Directory or Configuration Manager administrator. You can send the .zip file in any way – for example, email, FTP, or by placing it on a shared network drive.
5. The administrator runs the stand-alone extraction tool to extract the data.

   For instructions for running the tool, see AD and ConfigMgr Data Extraction Tool or refer to the .pdf file included in the downloaded .zip file.
6. After running the tool, the administrator sends the generated .sgz file(s) to you.
7. Return to the Indirect Load step, under Import the extracted data, click Browse.
8. In the Open dialog box, select the .sgz file that contains the extracted data that you want to load into AppDNA, and then click Open.
9. Click Next.
10. Check the details in the Summary step, and then click Next to start the operation.

    AppDNA displays information that provides an indication of the progress. Depending on the amount of data involved, this process can take a considerable amount of time (several hours, for example). During this time, it is safe to perform other tasks within AppDNA. However, do not exit AppDNA, or turn off your computer, or the AppDNA server computer, until the operation has completed.
11. When the Progress step shows that the operation is complete, click Finish.
12. If the Active Directory or Configuration Manager administrator sent multiple .sgz files, repeat steps 7–11 for the other files.

Load Configuration Manager data

August 1, 2018

This topic provides step-by-step instructions for loading System Center Configuration Manager data into AppDNA in one operation.

1. From the AppDNA menus, choose Configure > AD & ConfigMgr > Load Data.

   This opens the Load AD & ConfigMgr Data wizard. By default, the wizard opens on the Load Type step. However if you have already opened the wizard since you last logged on to AppDNA, the wizard reopens where you previously left off. If necessary, click Previous to return to the Load Type step.

2. In the Load Type step, select System Center Configuration Manager (ConfigMgr), and then click Next.

3. If the ConfigMgr Connection Details step opens, enter the details as follows, and then click Next.

Option	Description
Server	Enter the Configuration Manager server hostname or IP address.
Site	Enter the Configuration Manager Site Code. If you want to extract data from multiple sites, you need to run through the wizard for each site.
Username	If you are running this tool on the Configuration Manager server, leave this blank. Otherwise, either leave this blank to use the credentials of the logged on Windows user or specify a user name to use to connect to the Configuration Manager server. Typically this is a domain-qualified user name of the form: domain\username.
Password	If you entered a user name, specify its password here.

   This step only appears the first time you use the wizard to do a direct load of Configuration Manager data. If you subsequently need to change the details, click Previous to return to the Load Type step. Then choose Edit > Settings from the menus and change the details in Configuration Manager settings, before continuing.

4. In the Extraction Mode step, select one of the following options:

Option	Description
Standard	Select this option if you want to automatically extract all of the relevant Configuration Manager changes since the last data extraction.
Advanced	Select this option if you want to manually select the Configuration Manager packages and applications to extract. Use this option the first time data is extracted from a large Configuration Manager site – that is, a site that has a total of more than 5,000 packages and applications, and/or more than 50,000 users or computers. Then extract the applications and/or packages in batches of, for example, 1,000 applications and 1,000 packages.

5. Click Next.
6. If you chose the Advanced option, in the Advanced Selection step, select the packages, applications, or both packages and applications, that you want to extract for loading into AppDNA (see ConfigMgr Advanced Selection for more on this step). Citrix recommends that you select no more than a total of 2,000 applications and packages. Then click Next.

   (This step does not appear if you chose Standard in the Extraction Mode step.)
7. Check the details in the Summary step, and then click Next to start the operation.

   AppDNA displays information that provides an indication of the progress. Depending on the amount of data involved, this process can take a considerable amount of time (several hours, for example). During this time, it is safe to perform other tasks within AppDNA. However, do not exit AppDNA, or turn off your computer, or the AppDNA server computer, until the operation has completed.
8. When the Progress step shows that the operation is complete, click Finish.

If you want to load data from another Configuration Manager site, repeat the above steps for the next site.

Load Active Directory data

August 1, 2018

This topic provides step-by-step instructions for loading Active Directory (AD) data into AppDNA in one operation.

1. From the AppDNA menus, choose Configure > AD & ConfigMgr > Load Data.

   This opens the Load AD & ConfigMgr Data wizard. By default, the wizard opens on the Load Type step. However if you have already opened the wizard since you last logged on to AppDNA, the wizard reopens where you previously left off. If necessary, click Previous to return to the Load Type step.

2. In the Load Type step, select Active Directory (AD), and then click Next.

3. If the Active Directory Connection Details step opens, enter the details as follows, and then click Next.

Option	Description
Domain controller	Enter the name of the Active Directory domain or leave blank to automatically use the domain to which your machine is connected. If you want to extract data from multiple domains (for example, all of the domains that belong to a forest), you need to run through the wizard for each domain.
Username	Leave blank to use the credentials of the logged on Windows user, or specify a user name to use to connect to Active Directory.
Password	If you entered a user name, specify its password here.

   This step only appears the first time you use the wizard to do a direct load of Active Directory data. If you subsequently need to change the details, click Previous to return to the Load Type step. Then choose Edit > Settings from the menus and change the details in Active Directory settings, before continuing.

4. In the Organizational Units (OUs) step, select the OUs that you want to extract for loading into AppDNA. Typically you want to select the OUs to which applications have been deployed through AD, or that contain the users and devices to which applications have been deployed through Configuration Manager.

   By default, when you select an OU, the wizard automatically selects any sub-OUs. To change this behavior, clear the Automatically select nested OUs check box.

5. Click Next.

6. Check the details in the Summary step, and then click Next to start the operation.

   AppDNA displays information that provides an indication of the progress. Depending on the amount of data involved, this process can take a considerable amount of time (several hours, for example). During this time, it is safe to perform other tasks within AppDNA. However, do not exit AppDNA, or turn off your computer, or the AppDNA server computer, until the operation has completed.

7. When the Progress step shows that the operation is complete, click Finish.

If you want to load data from another domain, repeat the above steps for the next domain.

Reference

August 1, 2018

This section provides detailed reference documentation for the Load AD and ConfigMgr Data wizard, the stand-alone tool, and the Active Directory and ConfigMgr settings dialog boxes.

In this section

Load AD and ConfigMgr Data Wizard

August 1, 2018

You use the Load AD and ConfigMgr Data wizard to import Active Directory (AD) and System Center Configuration Manager data into AppDNA. The wizard has a number of pages that lead you through the process. The options on each page are documented under separate headings below.

To open the Load AD and ConfigMgr Data wizard:

- From the menus, choose Configure > AD & ConfigMgr > Load Data.

Load Type

The Load Type page is the first page in the wizard. (However, if you navigate away from the wizard while you are part way through an operation, the next time you enter the wizard it takes you back to where you were. If necessary, click Previous to return to this page.)

On this page you choose what type of load you want to perform. The options are:

Active Directory (AD) – Select this option to do a direct load of Active Directory data. This means that the data is extracted and loaded into AppDNA in one operation.

System Center Configuration Manager (ConfigMgr) – Select this option to do a direct load of Configuration Manager data. This means that the data is extracted from Configuration Manager and loaded it into AppDNA in one operation.

Indirect – Select this option if you want to extract the data from Configuration Manager or Active Directory (or both) on a different machine – for example, on the Configuration Manager server or Active Directory domain controller. This is useful when you do not have the correct credentials to run the extraction yourself. Use this option to download a .zip file (which contains the extraction tool, synchronization data, and documentation) that you can send, for example, to the Configuration Manager administrator. He or she runs the tool and sends the results back to you. Then you use this option again to load the results into AppDNA.

Click **Next** to continue to the next page.

AD Connection Details

You use the AD Connection Details page to identify the Active Directory domain controller and the credentials to use to connect to it. This page only appears the first time you use the wizard to do a direct load of Active Directory data. If you need to change the details when you subsequently use the wizard, you can do this in Active Directory settings.

The options are:

- **Domain controller** – Enter the name of the Active Directory domain or leave this blank to automatically use the domain to which the AppDNA machine is connected.
- **Username** – Specify the user name to use to connect to the Active Directory domain. Alternatively, leave this blank to use the credentials of the logged on Windows user account. Whether specified or not, the user must be a valid user of the domain.
- **Password** – If you specified a user name above, enter its password here.

Click **Next** to continue to the next page.

Organizational Units (OUs)

The Organizational Units (OUs) page displays the OUs in the selected domain. (If the wizard did not open the AD Connection Details page and you want to change the domain, click the Previous button, and then enter the new domain name in Active Directory settings before continuing.)

Select the OUs that you want to extract to load into AppDNA. Typically you want to select the OUs to which applications have been deployed through AD, or that contain the users and devices to which applications have been deployed through Configuration Manager.

By default, when you select an OU, the wizard automatically selects any sub-OUs. Similarly, if you clear an OU's check box, by default the wizard automatically clears the check boxes for any sub-OUs. To change this behavior, clear the Automatically select nested OUs check box.

Click **Next** to continue to the next page.

ConfigMgr Connection Details

You use the ConfigMgr Connection Details page to identify the Configuration Manager server and site and the credentials to use to connect to them. This page only appears the first time you use the wizard to do a direct load of Configuration Manager data. If you need to change the details when you subsequently use the wizard, you can do this in Configuration Manager settings.

The options are:

- **Server** – Enter the Configuration Manager server hostname or IP address.
- **Site** – Enter the Configuration Manager Site Code.
- **Username** – Leave this blank to use the credentials of the logged on Windows user account or specify the user name to use to connect to the Configuration Manager server. Typically this is a domain-qualified user name of the form: domain\username.

  You must leave the Username and Password boxes blank if you are running the extraction on the Configuration Manager server.
- **Password** – If you specified a user name above, enter its password here.

Click **Next** to continue to the next page.

Extraction Mode

The Extraction Mode page applies to the extraction of Configuration Manager data only. The options are:

- **Standard** – Select this option if you want to automatically extract all of the relevant changes since the last time you loaded Configuration Manager data.

- **Advanced** – Select this option if you want to manually select the applications and packages to load into AppDNA.

Important: Citrix recommends that you use the
Advanced option the first time you extract data from a large Configuration Manager site, and then extract the applications and/or packages in batches of, for example, 1,000 applications and 1,000 packages. (In this context, a large Configuration Manager site is one that has a total of more than 5,000 packages and applications, and/or more than 50,000 users or computers.)

Click **Next** to continue to the next page.

Advanced Selection

When you choose the Advanced extraction mode, you use the Advanced Selection page to select the applications and/or packages that you want to extract from the selected Configuration Manager site for loading into AppDNA. (If the wizard did not open the ConfigMgr Connection Details page and you want to change the server and site combination, click the Previous button to return to the Load Type page, and then enter the new domain name in Configuration Manager settings before continuing.)

Note: Citrix recommends that you select no more than a total of 2,000 applications and packages for extraction at the same time.

For detailed documentation of the features in this page, see ConfigMgr Advanced Selection.

Click **Next** to continue to the next page.

Indirect Load

The Indirect Load page outlines the steps involved in using the Indirect Load approach. There are three steps:

Step 1 – Click the Download button to download a .zip file that contains the extraction tool, synchronization data, and documentation.

Step 2 – Send the .zip file that you downloaded in Step 1 to the Active Directory or Configuration Manager administrator. The administrator then runs the tool to extract the data from Configuration Manager or Active Directory, or both. Documentation for running the tool is available in the .zip file. After the extraction is complete, the administrator sends the .sgz file(s) that the tool generates back to you.

Step 3 – Click Browse to select the .sgz file generated in Step 2, and then click Next to load the results into AppDNA.

Summary

The Summary page provides a summary of the items that have been selected for loading into AppDNA. Check the details and then click Next to start the extraction process. Depending on how much data you are extracting, this can take a considerable amount of time (several hours, for example).

Progress

The Progress page provides information about the status of the extraction and loading of the selected items into AppDNA.

ConfigMgr Advanced Selection

August 1, 2018

When using Advanced extraction mode, you use the Advanced Selection page to select the applications and/or packages that you want to extract from the selected ConfigMgr site for loading into AppDNA.

Note: If the ConfigMgr site contains a very large number of packages or applications, this page takes some time to display them all. However, you can use the page, while this continues. When enough packages and/or applications have been displayed for your purposes, click
Cancel to stop any more from being displayed.

The top part of the page has features that make it easy to select groups of packages and applications for loading into AppDNA. The details are as follows:

- **Selection** – Select this option and then use the check boxes in this section to select or deselect all packages or applications that have been added, changed, or deleted, or that are unchanged since the last time the data was extracted. By default, the Not loaded / New and Modified check boxes are selected.
- **Batching** – Select this option if you want to automatically select the topmost items that are visible on the current tab and deselect any other items. This is useful if you have a very large ConfigMgr deployment and you want to extract data in batches. (This means you need to run the wizard multiple times – once for each batch.) By default 100 items are selected but you can change this.
- **Searching & filtering** – You can enter a text to search for in a specified column. For example, you could enter “Adobe” and select the Manufacturer column to retrieve all of the applications that are manufactured by Adobe. You can also select a range of dates to restrict the list to items added, modified, or deleted within a particular time period.

- **Group by** – Use this drop-down list to group the items in the list by values in one of the columns. For example, if you select Manufacturer, all of the items that have the same manufacturer are grouped together.

The lower part of the page has tabs that list packages and applications. These have additional features that make it easy to sort and filter the lists. There is more information on these features below.

- **Packages** – (Not shown if there are no packages.) This tab lists managed applications that are available for deployment through the ConfigMgr package and program deployment mechanism. This mechanism is available in all versions of ConfigMgr that are supported by AppDNA.
- **Applications** – (Not shown if there are no applications.) This tab lists managed applications that are available for deployment through the ConfigMgr application model. This mechanism is new in ConfigMgr 2012.

Select the applications and packages that correspond to the managed applications that you want to load into or update in AppDNA, or whose status you want to be able to report on by division or department (for example). Citrix recommends that you select no more than a total of 2,000 applications and packages for extraction at the same time.

When you have selected the packages or applications (or both) that you want to extract, click Next. All items that are visible and selected will be extracted. Items that have been excluded from the list by a filter are ignored.

Note:

- If both Packages and Applications tabs are present, all items that are visible and selected on both tabs will be extracted.
- If you select a deleted application or package for extraction, when the extracted data is loaded into AppDNA, AppDNA removes the corresponding ConfigMgr data from the AppDNA database but retains the associated application if it has been imported into AppDNA.

Filtering the list

You can restrict the list to items that have specific values in one or more of the columns. This is particularly useful if you have a large ConfigMgr deployment, because it enables you to reduce the list to a more manageable size. Any items that are excluded from the list by a filter are ignored when you click Next.

- Click in the text box under the header of the column that contains the values on which you want to filter the list. From the drop-down list, select the value that you want to filter on. Alternatively, type the value that you want to filter on in the text box. For example, you can restrict the list to items whose name begins with “A”.
- If you want to restrict the list to items that do not match a value (or that start with a value, for example), click the A icon on the left of the text box. Then from the drop-down list, select the

option you want to use (for example, Starts with or Does not contain).
- To clear a filter, click the icon on the right side of the text box.
- You can set filters on more than one column.

Sorting the list

You can sort the list on the data in any column:

1. Click the column header to sort in ascending order of the values in that column.
2. Click the column header again to sort in descending order.

Grouping by a column

You can group the items in the list by the data in any of the columns. For example, you can group items by manufacturer, status, or date of modification.

- Drag the header of the column (for example, the Status header) to the Drag a column header here to group by that column bar. (Alternatively, select the heading from the Group by drop-down list.)
- This groups the items by the values in that column. For example, when you group by the Status column, all of the items that have a status of New are grouped together.
- Expand the groups to see the items inside.
- Click the header of the column you are grouping the items by to reverse the sort order.
- Drag the column header back to the header bar when you no longer want to group the items. You need to place the column header before or after another column header. Alternatively, from the Group by drop-down list, choose None.

Note: You can also reorder the columns by dragging the column headers.

AD and ConfigMgr Data Extraction Tool

August 1, 2018

The AppDNA AD and ConfigMgr Data Extraction Tool is a stand-alone wizard that you can use to extract data from Active Directory (AD) and System Center Configuration Manager for loading into AppDNA. The tool uses a read-only API to extract the data from AD and Configuration Manager. The extraction tool does not change the AD or Configuration Manager data on the server.

The tool extracts a subset of the AD and Configuration Manager data for loading into AppDNA. Once loaded into AppDNA, the application deployment information can be used to import the managed

applications into AppDNA. After analyzing the applications within AppDNA, users can then view the compatibility status of the managed applications by division or department (for example).

Note:

- For best results, load both Active Directory and Configuration Manager data into AppDNA. Typically Active Directory provides rich data about organizational structure and Configuration Manager provides data about applications that are managed centrally.
- Extracting data from a large Configuration Manager site can take a considerable amount of time. The more users and devices there are, the longer the process takes. When extracting data from large Configuration Manager sites, Citrix recommends that you extract the data in batches of 2,000 applications or packages (or a mixture of both) and run the extraction overnight. (In this context, a large Configuration Manager site is one that has a total of more than 5,000 packages and applications, and/or more than 50,000 users or computers.)

Extract Data from Active Directory

August 1, 2018

This topic provides step-by-step instructions for running the stand-alone AppDNA AD and ConfigMgr Data Extraction Tool to extract data from Active Directory (AD) for loading into AppDNA.

This topic assumes that you have received the ADConfigMgrExportTool.zip package from the AppDNA administrator and that you have stored it in a suitable location in your file system.

> **Note**
>
> The AppDNA AD and ConfigMgr Data Extraction tool does not work on Microsoft Windows Server 2012 R2. The tool requires the installation of Visual C++ Redistributable for Visual Studio 2015. To work around this issue, download Visual C++ Redistributable for Visual Studio 2015 from: https://www.microsoft.com/en-us/download/details.aspx?id=48145

1. In Windows Explorer, locate the ADConfigMgrExportTool.zip package.
2. Right-click the ADConfigMgrExportTool.zip package, and from the shortcut menu, choose Extract All.
3. In the Extract Compressed (Zipped) Folders dialog box, select a suitable location, and then click Extract.
4. When the extraction is complete, in Windows Explorer navigate to the folder that contains the extracted files.
5. Double-click the ADSCCMExportTool.exe file.

   This starts the wizard.

6. In the Source Selection step in the wizard, choose Active Directory (AD), and then click Next.
7. In the Active Directory Connection Details step, enter the details as follows:

Option	Description
Domain controller	Enter the name of the Active Directory domain or leave blank to automatically use the domain to which your machine is connected. If you want to extract data from multiple domains (for example, all of the domains that belong to a forest), you need to run through the wizard for each domain.
Username	Leave blank to use the credentials of the logged on Windows user, or specify a user name to use to connect to Active Directory.
Password	If you entered a user name, specify its password here.

8. Click Next.
9. In the Organizational Units (OUs) step, select the OUs that you want to extract for loading into AppDNA. Typically you want to select the OUs to which applications have been deployed through AD, or that contain the users and devices to which applications have been deployed through Configuration Manager.

   By default, when you select an OU, the wizard automatically selects any sub-OUs. To change this behavior, clear the Automatically select nested OUs check box.
10. Click Next.
11. Check the details in the Summary step, and then click Next.
12. In the Save As dialog box, enter a suitable name and location for the extracted data, and then click Save.

    Note: Ensure the file has an .sgz filename extension.

    The wizard then starts extracting the data and displays information that provides an indication of the progress. Depending on how much data you are extracting, this process can take a considerable amount of time (several hours, for example).
13. When the Progress step shows that the operation is complete, click Finish.
14. If you want to extract data from another domain, repeat steps 5 to 13 for the next domain.

You now need to send the (.sgz) file or files containing the extracted data to the AppDNA administrator for loading into AppDNA.

Extract Data from ConfigMgr

August 1, 2018

This topic provides step-by-step instructions for running the stand-alone AppDNA AD and ConfigMgr Data Extraction Tool to extract data from Configuration Manager for loading into AppDNA.

This topic assumes that you have received the ADConfigMgrExportTool.zip package from the AppDNA administrator and that you have stored it in a suitable location in your file system.

Important: The package also contains the synchronization data that is used to identify the latest changes to the Configuration Manager data. You therefore need a fresh package every time you extract Configuration Manager data from one or more sites. If necessary, contact the AppDNA administrator to request a fresh package.

1. In Windows Explorer, locate the ADConfigMgrExportTool.zip package.
2. Right-click the ADConfigMgrExportTool.zip package, and from the shortcut menu, choose Extract All.
3. In the Extract Compressed (Zipped) Folders dialog box, select a suitable location, and then click Extract.
4. When the extraction is complete, in Windows Explorer navigate to the folder that contains the extracted files.
5. Double-click the ADSCCMExportTool.exe file.

   This starts the wizard.
6. In the Source Selection step in the wizard, choose System Center Configuration Manager (ConfigMgr), and then click Next.
7. In the ConfigMgr Connection Details step, enter the details as follows:

Option	Description
Server	Enter the Configuration Manager server hostname or IP address.
Site	Enter the Configuration Manager Site Code. If you want to extract data from multiple sites, you need to run through the wizard for each site.

Option	Description
Username	If you are running this tool on the Configuration Manager server, leave this blank. Otherwise, either leave this blank to use the credentials of the logged on Windows user or specify a user name to use to connect to the Configuration Manager server. Typically this is a domain-qualified user name of the form: domain\username.
Password	If you entered a user name, specify its password here.

8. Click Next.
9. In the Extraction Mode step, select one of the following options:

Option	Description
Standard	Select this option if you want to automatically extract all of the relevant Configuration Manager changes since the last data extraction.
Advanced	Select this option if you want to manually select the Configuration Manager packages and applications to extract. Use this option the first time data is extracted from a large Configuration Manager site – that is, a site that has a total of more than 5,000 packages and applications, and/or more than 50,000 users or computers. Then extract the applications and/or packages in batches of, for example, 1,000 applications and 1,000 packages.

10. Click Next.
11. If you chose the Advanced option, in the Advanced Selection step, select the packages, applications, or both packages and applications, that you want to extract for loading into AppDNA (see ConfigMgr Advanced Selection for more on this step). Citrix recommends that you select no more than a total of 2,000 applications and packages. Then click Next.

(This step does not appear if you chose Standard in the Extraction Mode step.)

12. Check the details in the Summary step, and then click Next.
13. In the Save As dialog box, enter a suitable name and location for the extracted data, and then click Save.

    Note: Ensure the file has an .sgz filename extension.

    The wizard then starts extracting the data and displays information that provides an indication of the progress. Depending on how much data you are extracting, this process can take a considerable amount of time (several hours, for example).
14. When the Progress step shows that the operation is complete, click Finish.
15. If you want to extract another batch of data, or data from another Configuration Manager site, repeat steps 5 to 14 for the next site.

You now need to send the (.sgz) file or files containing the extracted data to the AppDNA administrator for loading into AppDNA.

Active Directory settings

August 1, 2018

The Settings dialog box contains general AppDNA options. To open the Settings dialog box, choose Edit > Settings from the menus.

Use the Active Directory page in the Settings dialog box to enter the connection details for extracting data from Active Directory (AD).

The options are:

- **Domain controller** – Enter the name of the Active Directory domain or leave this blank to automatically use the domain to which the AppDNA machine is connected.
- **Username** – Specify the user name to use to connect to the Active Directory domain. Alternatively, leave this blank to use the credentials of the logged on Windows user account. Whether specified or not, the user must be a valid user of the domain.
- **Password** – If you specified a user name above, enter its password here.

Click Test to check the connection details.

Click Save to preserve your changes.

Configuration Manager settings

August 1, 2018

The Settings dialog box contains general AppDNA options. To open the Settings dialog box, choose Edit > Settings from the menus.

Use the ConfigMgr page in the Settings dialog box to enter the connection details for extracting data from System Center Configuration Manager.

The options are:

- **Server** – Enter the Configuration Manager server hostname or IP address.
- **Site** – Enter the Configuration Manager Site Code.
- **Username** – Leave this blank to use the credentials of the logged on Windows user account or specify the user name to use to connect to the Configuration Manager server. Typically this is a domain-qualified user name of the form: domain\username.

  You must leave the Username and Password boxes blank if you are running the extraction on the Configuration Manager server.
- **Password** – If you specified a user name above, enter its password here.

Click Test to check the connection details.

Click Save to preserve your changes.

Import managed applications

August 1, 2018

You can import managed applications into AppDNA using the installation media that has been used to deploy them through Active Directory or Configuration Manager.

To import managed applications

1. From the AppDNA side bar, choose Import & Analyze > Managed Applications.
2. On the Managed Applications screen, select from the list the deployed managed applications that you want to import .

   Make sure you select appropriate installations (and not repair or uninstall installations). When a package has several installations, make sure you select only one of them – preferably one that

has been deployed (that is, for which the count in the Users or Computers column is greater than zero).

3. Select toolbar options as needed.

   Execution profiles are used for Install Capture imports only. For MSI packages Citrix recommends using direct MSI import, which is faster and less complicated than Install Capture. Non-MSI packages are always imported using Install Capture.

4. On the toolbar, click Add to import list.

   The Import Applications screen opens. The MSI packages that you selected for import are listed on the Direct Import tab. Any non-MSI packages that you selected for import are listed on the Install Capture tab.

5. When you are ready to import the applications, click Import.

To group applications

When the installations have standard names (such as "Per-system attended") you may find it helpful to group the list by installation. To do this, drag the Installation column to the Drag a column header here to group by that column area above the list. This groups the list by the installation name.

To view the packages in an installation, expand a group. You can then select the type(s) of installation you want to use. Keep in mind that some packages may be deployed using multiple installations, such as Per-system unattended and Per-user unattended.

After grouping applications by installation type and making your selections, you may want to group by the Package column, to check that no items have multiple installations selected. Applications imported through Direct Import are imported only once regardless of the number of installations selected. However, for applications imported through Install Capture, each installation is imported separately.

Importing Managed Applications

August 1, 2018

This topic provides step-by-step instructions for importing applications that are managed through Active Directory or ConfigMgr.

1. From the AppDNA side bar, choose Import & Analyze > Managed Applications.
2. On the Managed Applications screen, select the managed applications that you want to import.

Make sure you select appropriate installations (and not repair or uninstall installations). When a package has several installations, make sure you select only one of them – preferably one that has been deployed (that is, for which the count in the Users or Computers column is greater than zero).

3. Select the options on the toolbar that you require:

   - **Execution Profile** – Execution profiles are used for Install Capture imports only. The default execution profile is called Snapshot. For more information, see Install Capture Options.
   - **Use direct MSI Import** – Select this check box if you want MSI packages to be imported using Direct Import. This is recommended. Clear this check box to use Install Capture instead of direct MSI import for MSI packages. This is not recommended because direct MSI import is faster and less complicated than Install Capture. Non-MSI packages are always imported using Install Capture.

   For information about configuring your system for Install Capture, see Install Capture.

4. On the toolbar, click Add to import list.

   This takes you to the Import Applications screen. The MSI packages that you selected for import are listed on the Direct Import tab. Any non-MSI packages that you selected for import are listed on the Install Capture tab.

5. When you are ready to import the applications, on the toolbar click Import.

   For more information about the import process, see Direct import.

Link managed applications

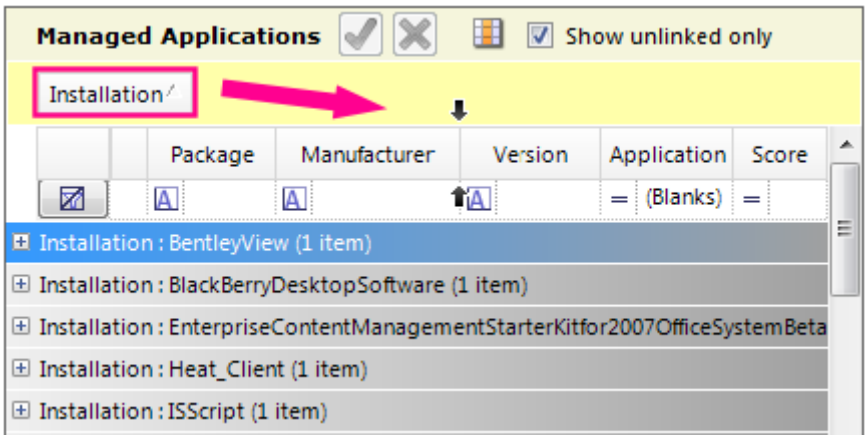
August 1, 2018

Linking applications managed through Active Directory and Configuration Manager with applications that have already been imported into AppDNA is an important step in the configuration of Active Directory and Configuration Manager data. It enables AppDNA to create reports about the RAG status of the applications deployed to Active Directory and Configuration Manager users, computers, groups, and organizational units. Managed applications that you import through the Managed Applications and Discover Applications screens are automatically linked.

To link managed applications: Choose Configure > AD & ConfigMgr > Link Managed Applications.

By default, the left side of the Link Managed Applications screen lists the managed applications and the right side lists the applications that have already been imported into AppDNA. In addition, by default the left side is grouped by the Installation column. You may find it easier to understand this

screen if you ungroup the list so that the managed applications are shown in a flat list. To do this, drag the Installation box to between the Package and Manufacturer column headings.



If you subsequently want to re-group the list by the values in the Installation column, drag the Installation column header back to the yellow bar.

Important: When linking a managed application for which there are multiple installations, ignore any repair and uninstall installations, and link all of the other ones to the same imported application.

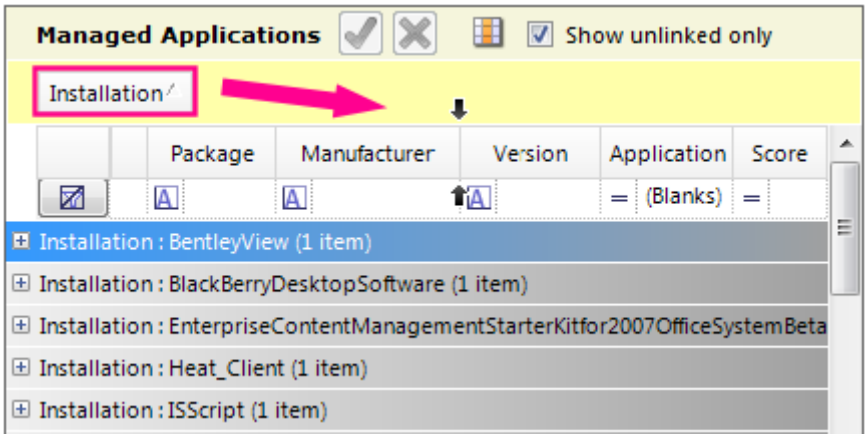
When you click an item, the lower part of the screen shows detailed information about that item.

Auto-match managed applications with imported applications

August 1, 2018

An automatic matching feature enables you to link managed applications with applications that have already been imported into AppDNA.

1. From the AppDNA menus, choose Configure > AD & ConfigMgr > Link Managed Applications.
2. Towards the center of the left side of the Link Managed Applications screen, drag the Installation box to between the Package and Manufacturer column headings.



This presents the list of managed applications as a flat list.

3. In the Matching section at the top, select Match: Managed to Imported in the Mode drop-down box.
4. Enter the Score threshold you want to use, or leave it as the default value of 20.

   AppDNA uses this as the criteria for matching the managed and imported applications. The score is calculated by assigning 10 points for each matching field (Name, Manufacturer, Version, and Path). You can choose which fields to match using the check boxes on the right.
5. Clear the Show unlinked only check box on the left side above the list of managed applications.
6. Clear the Show unlinked only check box on the right side above the list of imported applications.
7. Click Find Matches to begin matching managed and imported applications.

   AppDNA places the name of matched applications in the Application column and the matching score in the Score column, and selects the managed applications whose matching score is greater than or equal to the Score threshold.

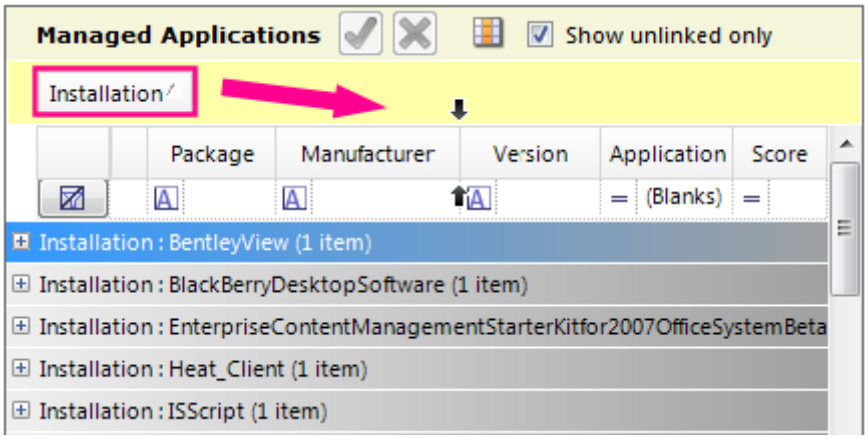
   - AppDNA automatically selects all matched managed applications that have a score greater than or equal to the score threshold, although you can manually change the selections if desired.
   - AppDNA does not select matches with scores less than the threshold. For these, you need to inspect the scores and make a decision about whether to match them and manually select those that you want to match.
8. Review the matches and change the selections as appropriate.
9. Click Save Associations at the top of the screen to save the selected matches.

Manually match managed applications with imported applications

August 7, 2018

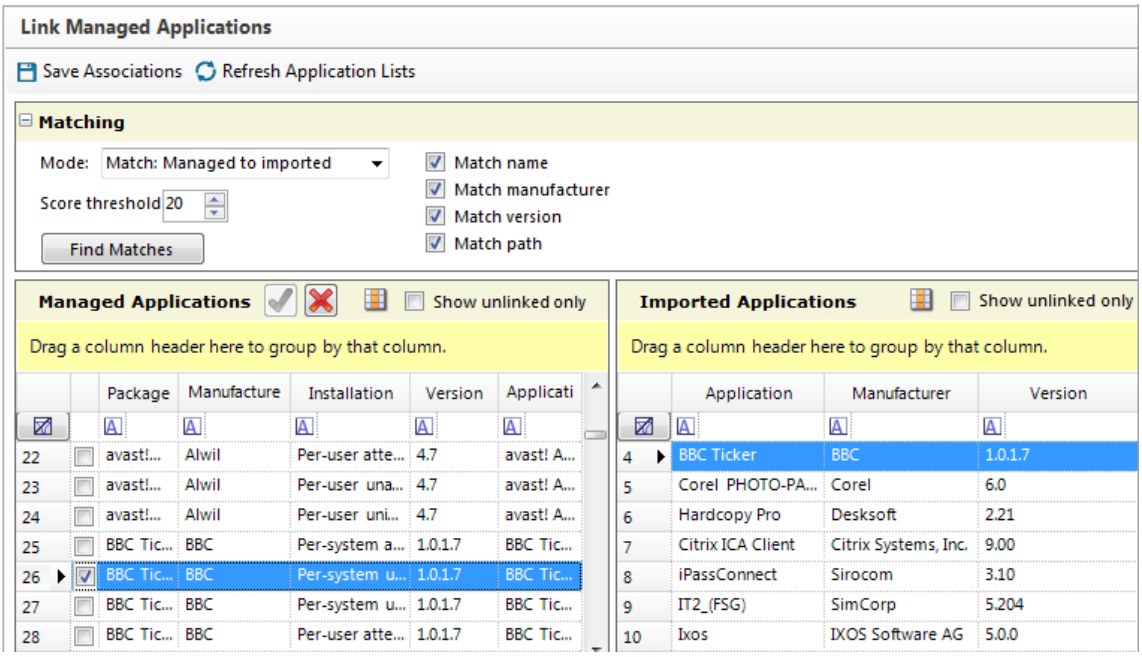
You can also manually link managed applications with applications that have already been imported into AppDNA.

1. From the AppDNA menus, choose Configure > AD & ConfigMgr > Link Managed Applications.
2. Towards the center of the left side of the Link Managed Applications screen, drag the Installation box to between the Package and Manufacturer column headings.



   This presents the list of managed applications as a flat list.
3. In the Matching section near the top, select Match: Managed to Imported in the Mode drop-down box.
4. In the list of managed applications, select the check box next to the managed application that you want to match. If the application has multiple installations, select the check box next to all of them.
5. In the list of imported applications, click the application that you want to match with the selected managed application.
6. To make the association, click the green checkmark on the toolbar in the Managed Applications side of the screen.

   If the Show unlinked only check box is selected, the managed application and imported application both disappear from the list after you match them.
7. To bring them back, clearing the Show unlinked only check box on both sides of the screen.



You can now see the managed application and the imported application that you matched. Notice that the Application column for the managed application shows the name of the matched application.

8. To remove an association, select the managed application, and click the red cross on the toolbar above.

   This removes the linking and the name of the matched application from the Application column.

9. To save the changes, click Save Associations at the top of the screen.

Create groups from Active Directory and Configuration Manager collections

August 1, 2018

You can create groups for your applications, based on grouping structures discovered from Active Directory and Configuration Manager.

It is important to understand that there is not a direct mapping between the grouping structures in Active Directory and Configuration Manager and groups in AppDNA. In AppDNA, groups are simply sets of applications – they help structure and organize the applications in your portfolio. They make it easy to review and report on the applications in the group separately from the rest of your portfolio. In Active Directory and Configuration Manager, the grouping structures represent sets of users and

computers, some of which might represent real people and computers and some might represent dummy accounts used for authentication, for example.

Some of the Active Directory and Configuration Manager grouping structures reflect the organization's structure (such as divisions, departments, and geographical locations) and hardware or software scenarios. For example, there might be an Active Directory group that represents the finance office in London and another that represents designers in France. Similarly, there might be a Configuration Manager collection that manages mobile devices, and another that manages servers running Windows Server 2012.

Active Directory groups and Configuration Manager collections can provide useful insight in AppDNA, because Active Directory and Configuration Manager deploy managed applications to them. So the Active Directory group that represents the French designers may have the specialist applications that the designers use associated with it. If you create an AppDNA group based on this Active Directory group, the managed applications deployed to that Active Directory group are automatically added to the AppDNA group (provided those managed applications have been imported or linked with applications already in AppDNA). You can then conveniently analyze and report on this group of applications in AppDNA.

Note: The number of managed applications shown include only those that have been deployed to the Active Directory group or Configuration Manager collection. This is not necessarily the same as the number of managed applications that have been deployed to the members (users and computers) of the Active Directory group or Configuration Manager collection.

To create a group

1. From the AppDNA menus, choose Configure > AD & ConfigMgr > Manage Groups.
    - The left side of the screen shows the groups that have already been created in AppDNA.
    - The right side of the screen shows the Active Directory organizational units (OUs) and groups, and Configuration Manager collections, in a tree view or a list.
    - The lower part of the screen shows for the item that you select on the right side of the screen either the managed applications deployed to the item or the applications in AppDNA that are linked to them, depending on whether you select the Deployments or Applications option.
2. On the right side of the screen, click the item on which you want to base the new AppDNA group.
3. Drag the item from the right side to where you want to place it in the tree on the left side of the screen. Alternatively, click the item in the tree on the left under which you want the new group to appear and click Create.

    If the Active Directory or Configuration Manager item has child items, AppDNA creates a corresponding set of nested groups. AppDNA automatically adds any applications associated with

the Active Directory group or Configuration Manager collection to the newly created application group. If the Active Directory group or Configuration Manager collection has more than 20 associated applications, AppDNA displays a warning message to check that you want to proceed.

Groups created through the AD & ConfigMgr Collections screen are visible and editable in Manage > Groups.

Add associated applications to a group

To add applications associated with an Active Directory group or Configuration Manager collection to an AppDNA group:

1. From the AppDNA menus, choose Configure > AD & ConfigMgr > Manage Groups.
2. Click the group to which you want to add applications.
3. On the right side of the screen, click the item whose associated applications you want to add to the group and then click Add.

   If the applications that are deployed to the Active Directory group or Configuration Manager collection subsequently changes, you must update the AppDNA group to reflect the changes.

Create Groups

August 1, 2018

1. From the AppDNA menus, choose Configure > AD & ConfigMgr > Manage Groups.
2. On the right side of the screen, click the item on which you want to base the new AppDNA group.
3. Drag the item from the right side to where you want to place it in the tree on the left side of the screen. Alternatively, click the item in the tree on the left under which you want the new group to appear and click Create.

   If the AD or Configuration Manager item has child items, AppDNA creates a corresponding set of nested groups. AppDNA automatically adds any applications associated with the AD group or Configuration Manager collection to the newly created application group. If the AD group or Configuration Manager collection has more than 20 associated applications, AppDNA displays a warning message to check that you want to proceed.

Groups created through the AD & ConfigMgr Collections screen are visible and editable in the Groups screen.

Add associated applications to a group

To add applications associated with an AD group or Configuration Manager collection to an AppDNA group:

1. From the AppDNA menus, choose Configure > AD & ConfigMgr > Manage Groups.
2. Click the group to which you want to add applications.
3. On the right side of the screen, click the item whose associated applications you want to add to the group.
4. Click Add.

If the applications that are deployed to the AD group or ConfigMgr collection subsequently changes, you need to update the AppDNA group to reflect the changes.

Remove applications from a group

1. From the AppDNA menus, choose Configure > AD & ConfigMgr > Manage Groups.
2. In the tree on the left side, select the applications you want to remove.
3. On the toolbar, click Remove.

Organization data in the Users and Computers screen

August 1, 2018

Use the Users and Computers screen to view users, computers, groups, and organizational units (OUs) retrieved from Active Directory and Configuration Manager, and view summary reports that show the status of the managed applications that have been deployed to them. In this context, managed applications are applications that are deployed through Active Directory or Configuration Manager.

This feature enables you to explore your application DNA starting from entry points that come from Active Directory and Configuration Manager. For example, you can run a report for an Active Directory group that represents a critical business unit. The report shows the overall RAG status of the managed applications deployed to the unit. You can drill down to see the summary RAG status of the managed applications deployed to each user in the business unit and to the standard AppDNA application reports for those applications. This, for example, can help you identify business-critical applications that have issues in the target environment. You can use this information to be proactive in deciding which applications to target remediation efforts at and to prioritize remediation efforts.

To open the Users and Computers screen:

- From the AppDNA side bar, choose Select > Devices or Users or Groups or Organizational Units.

The Users and Computers screen has a number of different views. Use the Organizational Units, ConfigMgr Collections, AD Groups, Users, and Computers radio buttons on the toolbar to swap between the different views. Use the features of the screen to explore your Active Directory and Configuration Manager data.

The Organizational Units, ConfigMgr Collections, and AD Groups views are split – you can explore the entities on the left side and when you click one, you can view its members on the right side. OUs and Configuration Manager collections are shown in a tree view. When one of the items in the tree has had managed applications deployed to it, the number of managed applications and the number of imported or linked applications are shown in brackets:

- **Packages** – This represents the number of managed applications deployed to the item through Active Directory or Configuration Manager.
- **Applications** – This represents the number of these managed applications that have been imported into AppDNA or linked with an application already imported.

For example, the following indicates that 12 managed applications have been deployed to the All Windows XP Systems collection and those managed applications are linked to 10 applications in the AppDNA portfolio:

```
All Windows XP Systems [12 Packages, 10 Applications]
```

Usually (but not always) one managed application links to one application in AppDNA. To link the managed applications with applications in AppDNA, either import the managed applications or link them with applications that have already been imported into AppDNA.

AD groups, users, and computers are shown in a grid view. This shows the number of managed applications and the number of imported applications in separate Packages and Applications columns.

Note: When viewing OUs, Configuration Manager collections, or AD groups in this screen and in reports, the application counts include all applications linked to managed applications that have been deployed to members of the group, not just those that are assigned to that group. This is a different count from that shown in the
AD & ConfigMgr Collections screen.

Click a column header to sort by the data in that column. Click the header again to swap between ascending and descending order. You can also filter the data. Click the Clear Filter icon on the far left of the grid to clear all the filters.

For information about the reports, see Organization reports.

Configure

June 17, 2019

This section provides information about how to configure a variety of features in AppDNA.

Quick links to section topics:

- Configure solutions
- Install Capture
- Operating system images
- Modules, reports, and algorithms
- Custom reports
- Forward Path
- External data

Solutions

August 3, 2018

AppDNA solutions provide the information you need to make changes to your application environment, without requiring the assistance of consultants. You provide basic information about your current and target deployments in a Solutions wizard and then review the easy-to-interpret reports to see which applications will work in the new environment, either without changes or after remediation.

Use this solution:	To:
AppDisks	Identify applications that have common dependencies such as .NET, so you can install them on a single common base image.
App-V sequencing	Automate App-V sequencing with success checking and remediation, and launch testing and deployment to App-V servers.
Build assessment	Assess builds to determine whether applications will work on builds of the same OS family.
Interoperability	Analyze for interoperability to discover potential conflicts between applications.
Patch impact analysis	Determine the impact of a Microsoft patch on your portfolio of applications.
XenApp and XenDesktop 7.x upgrade	Prepare for a XenApp or XenDesktop 7.x upgrade from XenApp or XenDesktop.

Use this solution:	To:
XenApp and XenDesktop 7.x adoption	Prepare for a move to XenApp or XenDesktop 7.x from a non-Citrix delivery solution.

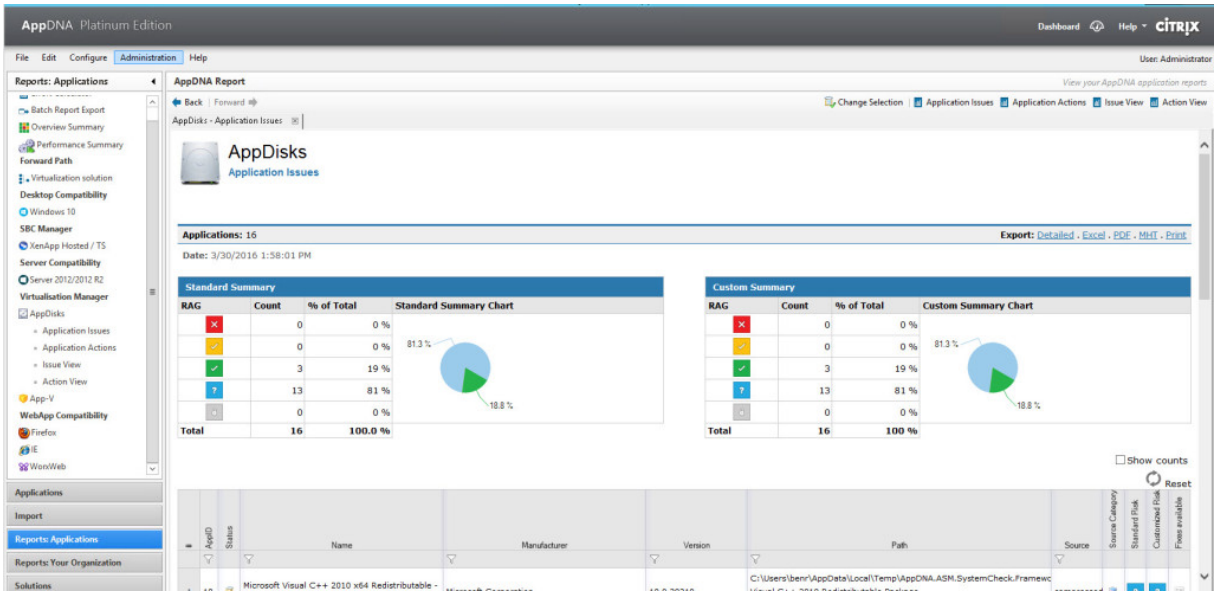
AppDisks

August 2, 2018

AppDisks is an application layering solution introduced in XenApp and XenDesktop 7.8. AppDisks separate applications and groups of applications from the operating system, enabling you to manage them independently.

AppDNA allows XenApp and XenDesktop to perform automatic analysis of applications on a per-AppDisk basis. Using AppDNA helps make the most of the AppDisks feature. Without it, application compatibility is not tested or reported.

AppDNA reports help identify issues and suggest remediation steps. For example, AppDNA can identify applications that have common dependencies such as .NET, so you can install them on a single common base image. AppDNA can also identify applications that load early in the OS startup sequence, so that you can then ensure they behave as expected.



For more information, see the XenApp and XenDesktop AppDisks article.

App-V sequencing

August 1, 2018

Automate and batch the creation of App-V packages from your portfolio of native installers, using AppDNA's knowledge to increase the sequencing success rate.

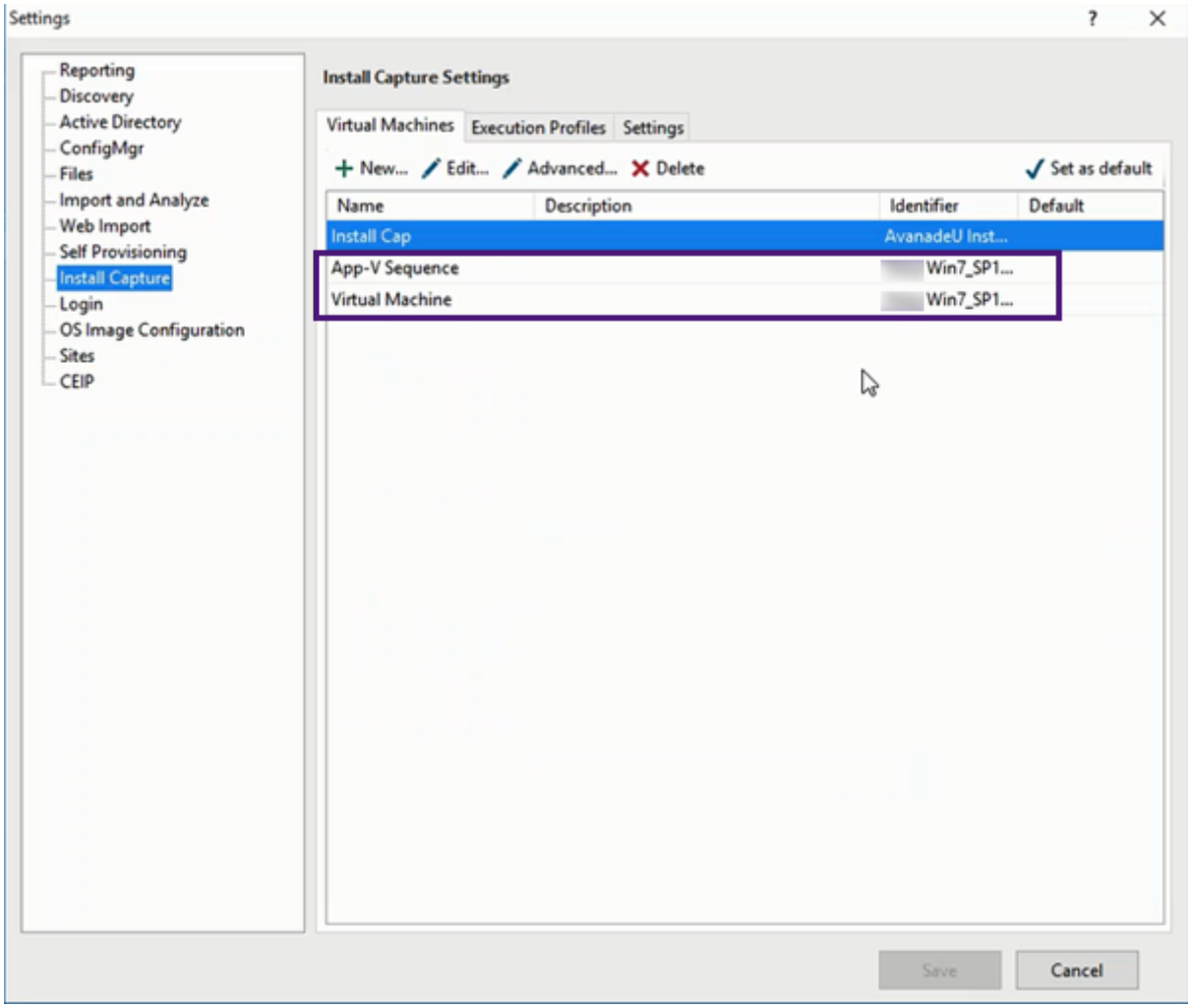
Without the App-V solution, you can import applications and their App-V packages with Import > Applications, however additional software requirements and steps are required to complete the process. For more information, see Direct Import and Install Capture.

Using the App-V Solution wizard, you can automate App-V sequencing with success checking and remediation, and launch testing and deployment to App-V servers. This supports App-V adoption and upgrades in App-V environments.

Prerequisites

Before you start, check:

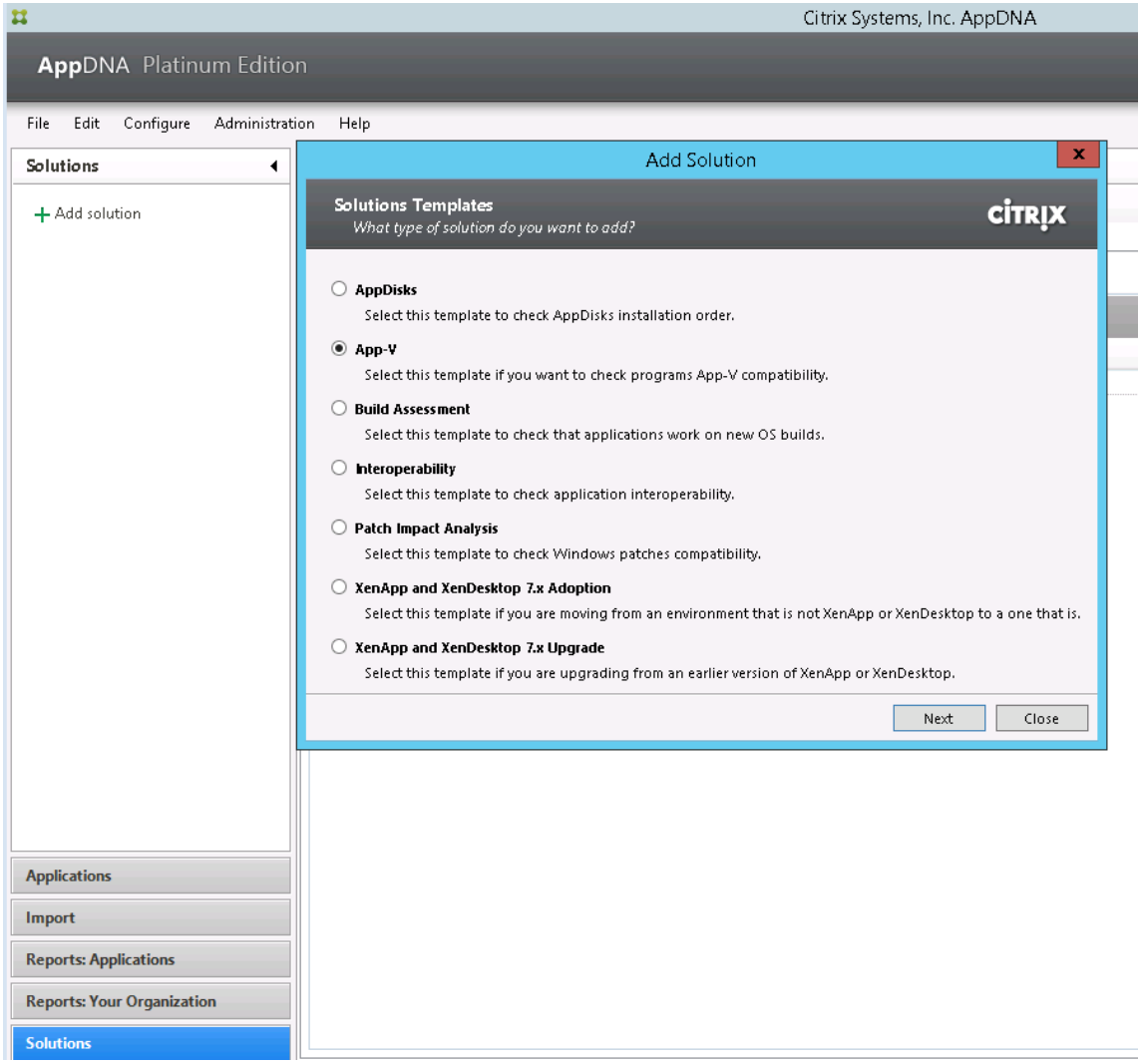
- App-V versions 5.0 and 5.0 SP1 are supported. App-V version 4.6 or earlier versions are not supported
- The App-V sequencing and client components are on the virtual machine where you want to carry out the sequencing.
- You have access to a network share which contains the prerequisite installers for carrying out an App-V capture on a machine. These include:
  - appv_client_setup.exe
  - appv_sequencer_setup.exe
  - AppVPackageRemediationUtility.exe
  - Citrix AppDNA VM Configuration. msi
  - dotNetFx40_Full_x86_x64.exe
- Virtual machine configuration profiles are set up for App-V sequencing in **Edit** > **Settings** > **Install Capture** [optional]. Virtual machines can be added in the third step of the App-V Solution wizard.



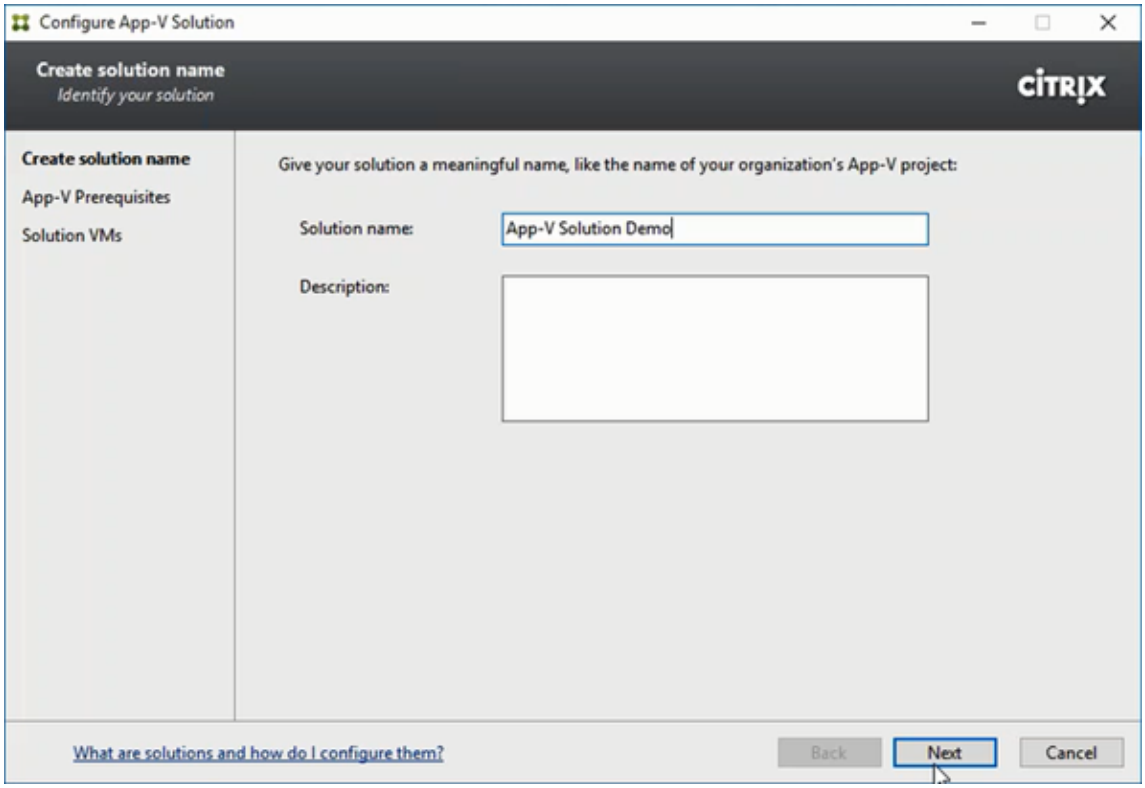
Configure an App-V solution

To configure an App-V solution:

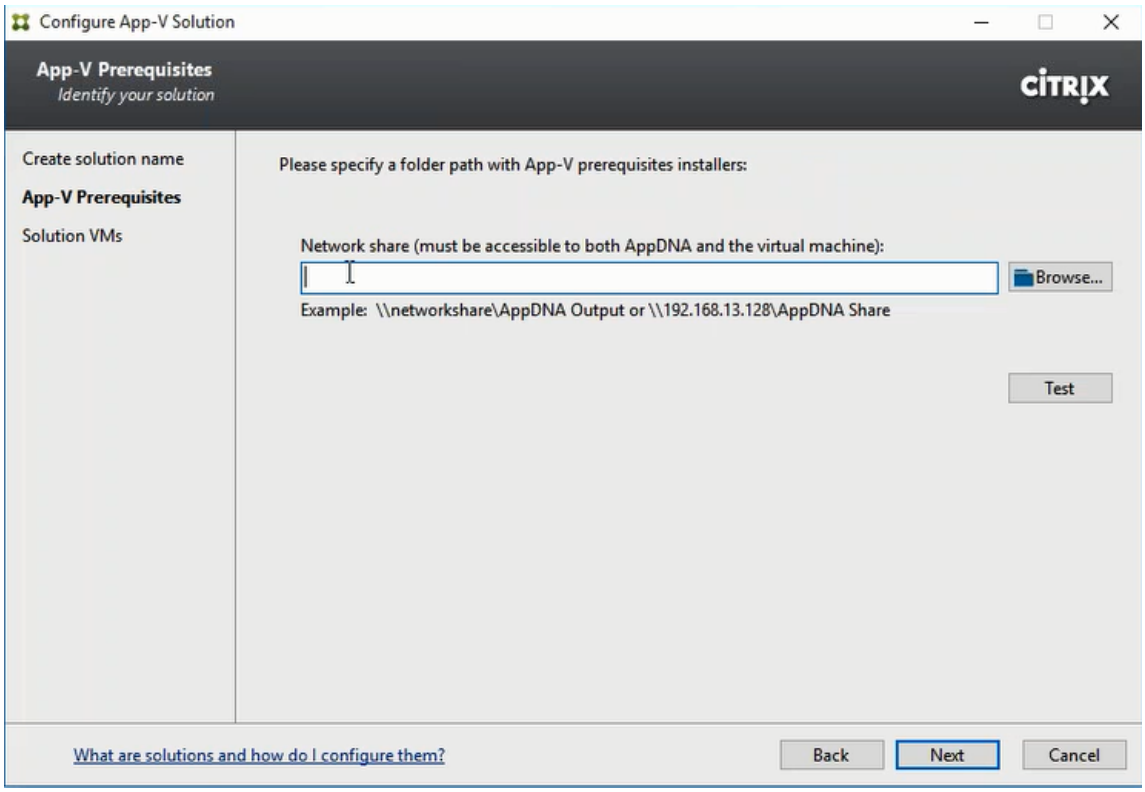
1. Select **Solutions** > **Add solution** > **App-V**.



2. Name the solution, and click **Next**.

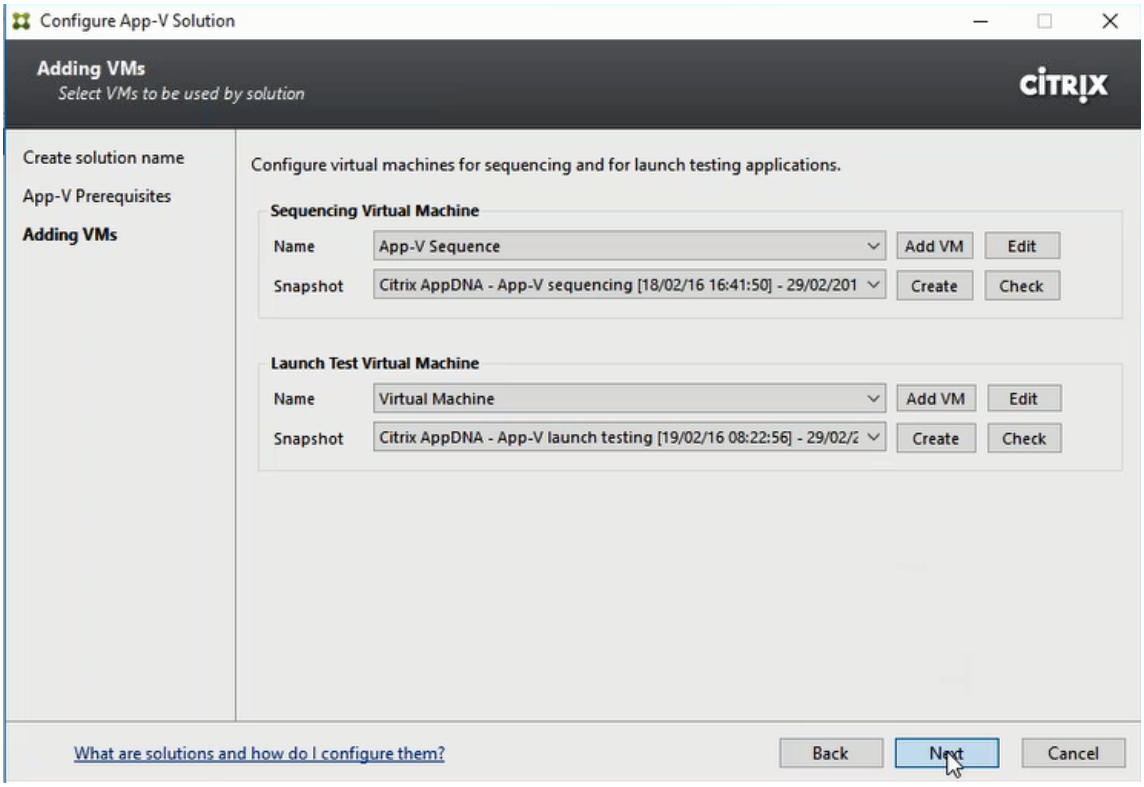


3. Specify or browse to a network share where the App-V prerequisite installers are. For example, \\networkshare\AppDNA Output or \\[IP address]\AppDNA Share. Click **Next**.

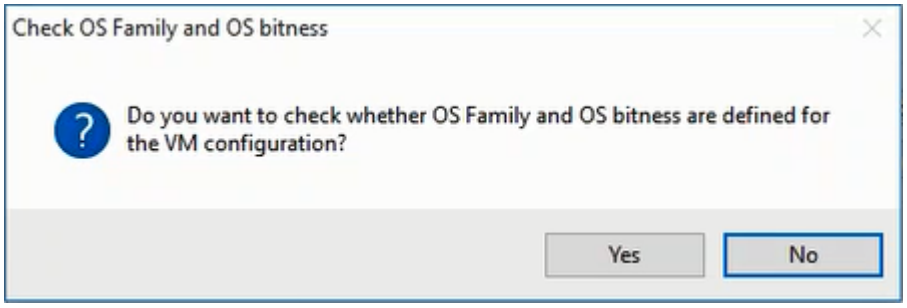


When the virtual machine starts, the prerequisites defined in this step will be installed if they are not already on the machine.

4. Select or add two different virtual machines, which will be used to carry out the App-V sequencing and App-V launch testing. The App-V client cannot be on the same machine as the App-V sequencer. Click **Next**.

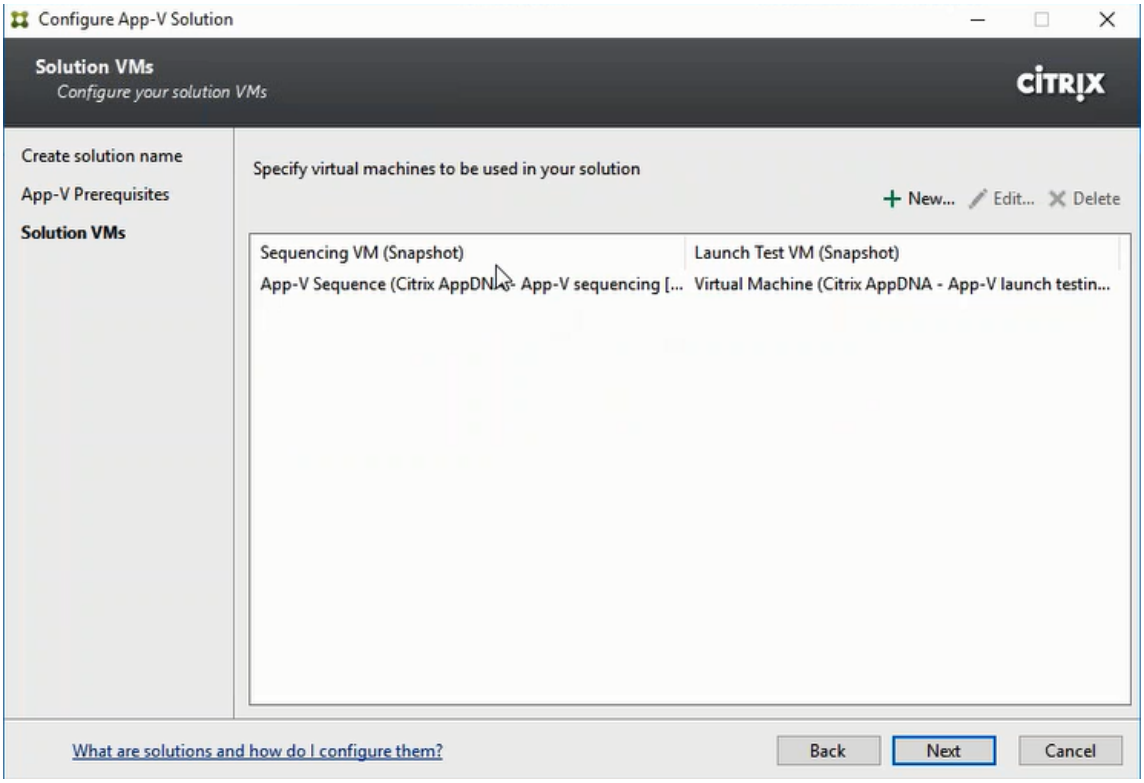


5. Select No or Yes from the Check OS family and OS bitness dialog.

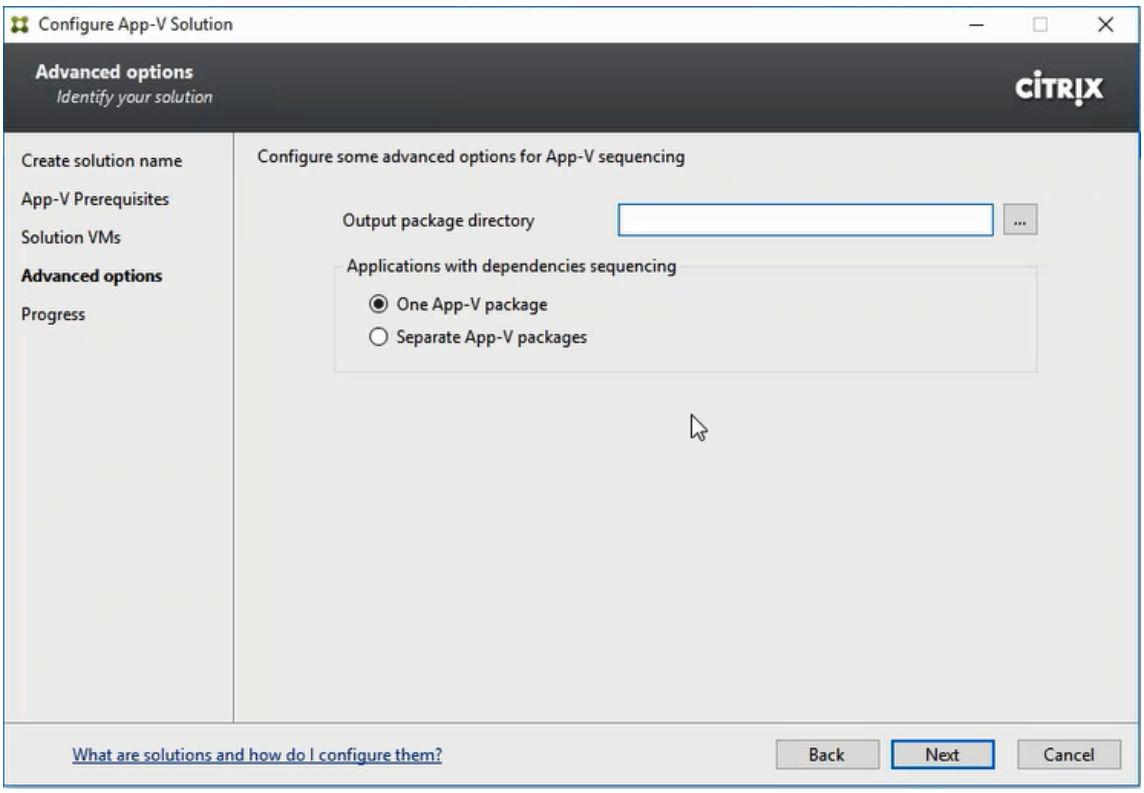


This can be useful for analysis later on. For example, if you set up multiple pairs of machines for App-V sequencing which contain two pairs of 64-bit machines and one pair of 32-bit machines, AppDNA will assess if your package has any 64-bit components on it, and use the 64-bit pairs of machines to carry out the sequencing and profiling on.

6. Review the virtual machines selected so far. Click New to add another pair of virtual machines. Select Edit or Delete to change the virtual machines you have specified. Click **Next**.



7. Select the output directory for the package. This is where the results of the sequencing will be saved. Click **Next**.



8. A progress screen displays while the solution is prepared. When it has finished, click **Close**.

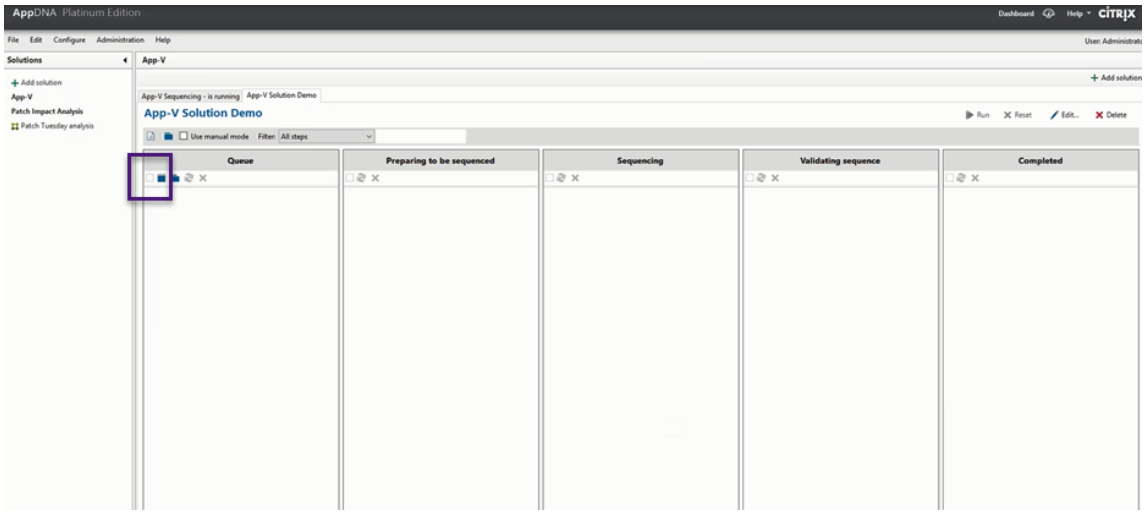
Once you have completed the configuration steps, the **App-V solution dashboard** is displayed.

Process applications with the App-V solution

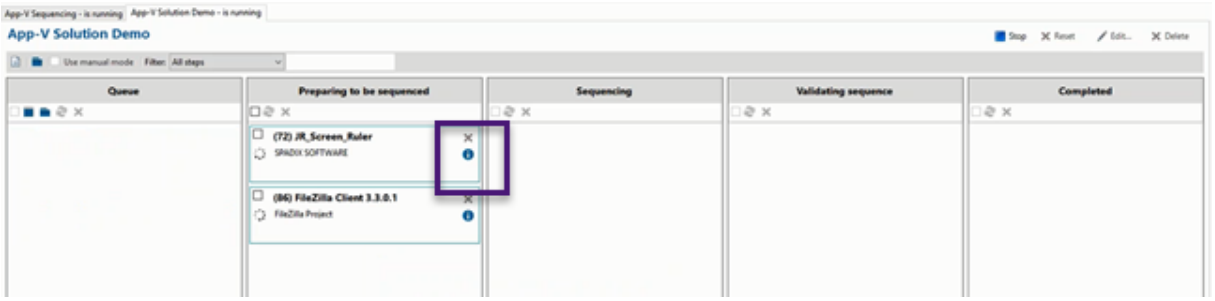
At the end of the App-V solution configuration steps, the App-V solution dashboard displays a series of “swim lanes” corresponding to the App-V sequencing process steps.

To add applications to the process:

1. Select the **Add imported app** icon.



2. Select applications from the list. This adds the applications to the Queue swim lane.
3. Select **Run**.



At any time, select the info icon next to the application to view the workflow details.

Applications which progress through sequencing and launch testing without errors to the Completed swim lane, can form an App-V package which you can have confidence in, as it has already passed a launch test in your target OS.

Assess builds

August 1, 2018

The Build Assessment solution indicates whether applications will work on additional builds of the same OS family. Suppose that your reference build is Windows 8 and you need to know if the applications that work on it will also work on other Windows 8 builds, such as ones customized for call center employees. The Build Assessment solution performs a standard AppDNA analysis on the reference build and compares it to an analysis for each target build.

AppDNA creates the following build assessment reports:

- **Build Assessment Summary Report —** This report indicates for the reference and target builds the number of applications with issues that require fixes or cannot be fixed.
- **Build Assessment Comparison Report —** For each target build compared to the reference build, this report provides a high-level summary of RAGs for each build, a summary of RAGs by algorithm group, and a summary of RAGs for each application.
- **Build Assessment Issues Report —** Similar to the Application Remediation report, this report also includes details about compatibility issues that are image-dependent and that result from GPOs, security and machine lock down policies, and permissions on registry keys or file system entries.

You can mark applications that you have tested in the Configure Build Assessment solution wizard so that AppDNA ignores any potential issues on the reference and target builds. When you indicate an application is tested on the reference build, AppDNA ignores all amber or red RAGs for non-image dependent algorithms on the reference and target builds because those issues do not affect the application in your environment.

To configure a build assessment solution

Before running the Configure Build Assessment Solution wizard, gather the following information.

- The OS family and image name of your reference build
- The image name for each target build

  Tip: The easiest way to work is to import the target build images before starting the wizard.
- Which applications to assess against each target build

  You can assess all applications or choose the ones to assess.
- Which applications work on the reference build

1. In the AppDNA side bar, click Solutions and then click Add solution.

2. In the Solutions Templates page, select Build Assessment and then click Next.

   The solution wizard opens.

3. Identify the solution: In the Solution name page, type a Solution name and Description, to be used in the solution report.
4. Choose a reference build: In the Reference build page, select the OS family and Image that will be the reference point for the assessment.
5. Choose target builds and applications:
   a) In the Target builds page, click New and then select an Image.

      If a target image does not appear in the list, click Import images. You must then cancel the wizard before you can import an image. Follow the on-screen instructions and then return to Step 1 to configure the Build Assessment solution.

   b) After you select a target image, choose applications: In the Applications page, select the applications you want to assess on the target build.
   c) When you are finished with the Configure Builds page, click Next.
6. Specify the applications that work on the reference build: In the Validated Applications page, select an option.
7. To complete the solution:
   a) On the Summary page, click Build to save the solution.
   b) On the Progress page, click Analyze. When the analysis completes, choose report to view and then click Finish.

   To view the reports at any time: In the AppDNA side bar, click Solutions and then click the name of the solution.

To add a target build to a solution

1. In the AppDNA side bar, click Solutions and then click Build Assessment in the Solutions pane.
2. In the Build Assessment pane, locate the solution, click Add build under Target Builds, and then complete the wizard.

To change an application list

Follow these steps to:

- Change the list of applications on the target build to use in the assessment
- Change the list of applications that are validated on the reference build

1. In the AppDNA side bar, click Solutions and then click Build Assessment in the Solutions pane.
2. In the Build Assessment pane, click Edit beside the solution name.
3. Click through the wizard until you reach the page you want to change.
4. After you complete your changes, click Build and then Analyze.

Analyze for interoperability

August 1, 2018

The Interoperability solution enables you to assess the MSI applications to be included in the same image. Conflicts can occur between applications that install the same component (or different versions of the same component) when those applications are upgraded, uninstalled or repaired using the Windows installer. These problems arise because the components have different component IDs within the MSI package. This solution is suitable for testing desktop applications that are installed using a Windows installer (MSI) package only.

The Interoperability solution does not test for potential conflicts caused by installing applications, because in most cases the Windows installer automatically prevents these issues from occurring.

You should run the Interoperability solution after:

- You import a new application

  Be sure to re-analyze all of the applications so you can see all possible conflicts. If you analyze only the new application, the report views show potential conflicts that the new application has with the other applications. However, they will not show potential conflicts that the existing applications have with the new application unless you re-analyze the entire portfolio.

- You delete an application

The Interoperability solution produces the same report views that are provided for standard AppDNA reports.

To configure an Interoperability solution

1. In the AppDNA side bar, click Solutions and then click Add solution.
2. In the Solutions Templates page, select Interoperability and then click Next.

   The solution wizard opens.
3. Identify the solution: In the Solution name page, type a Solution name and Description to be used in the solution report.
4. Choose applications: In the Applications page, select the applications to analyze.

5. To complete the solution:
    a) On the Summary page, click Build to save the solution.
    b) On the Progress page, click Analyze. When the analysis completes, choose report to view and then click Finish.

    To view the reports at any time: In the AppDNA side bar, click Solutions and then click the name of the solution.

To change the application list

1. In the AppDNA side bar, click Solutions and then click Interoperability in the Solutions pane.
2. In the Interoperability pane, click Edit beside the solution name.
3. Click Next and then update the application list.
4. After you complete your changes, click Build and then Analyze.

Patch impact analysis

August 1, 2018

Patch impact analysis determines the impact of a Microsoft patch on your portfolio of applications. It is important to recognize that this does not tell you what the patch does or its criticality, but rather which applications could be affected by it. This helps you plan which applications you want to test and also helps you to understand how invasive a patch might be.

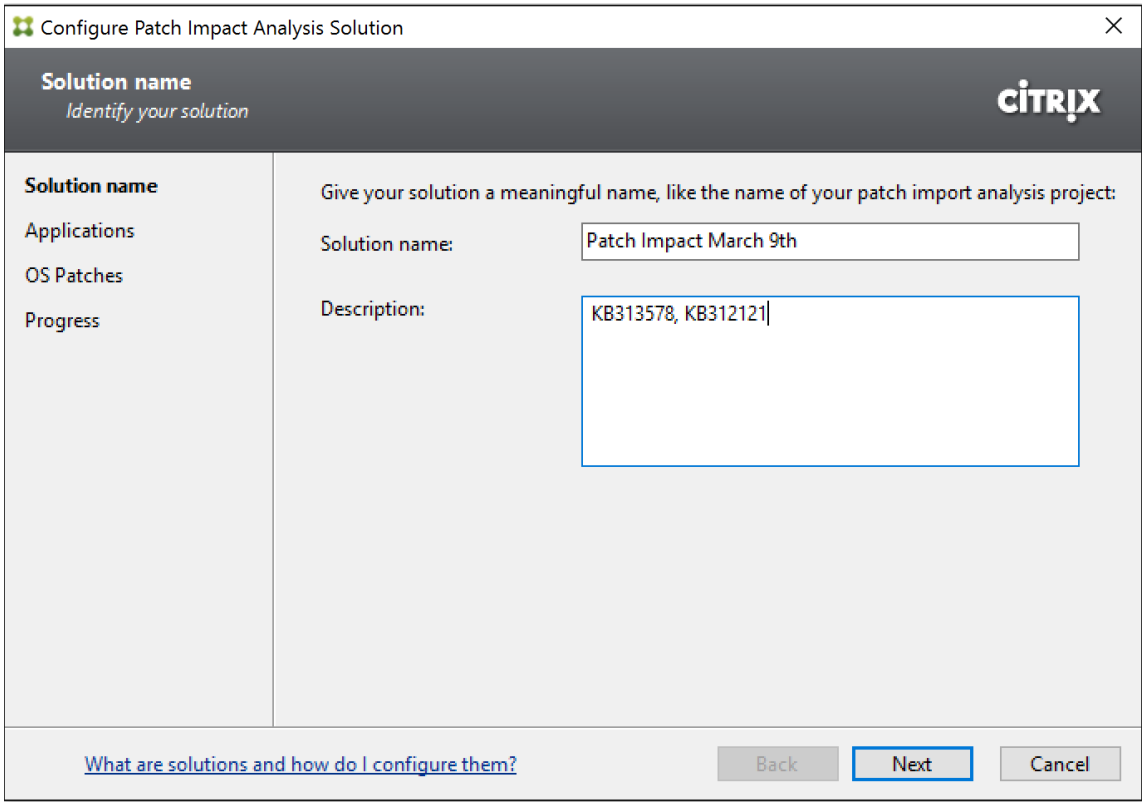
For example, if you have 1000 applications for a given patch, AppDNA may be able to detect that 70 of the applications are directly affected by the patch.

Directly affected means the application directly imports an API from a file being updated by the patch. For example, if application.exe directly imports from mydll.dll and mydll.dll is being updated by the patch, AppDNA will report it as red.

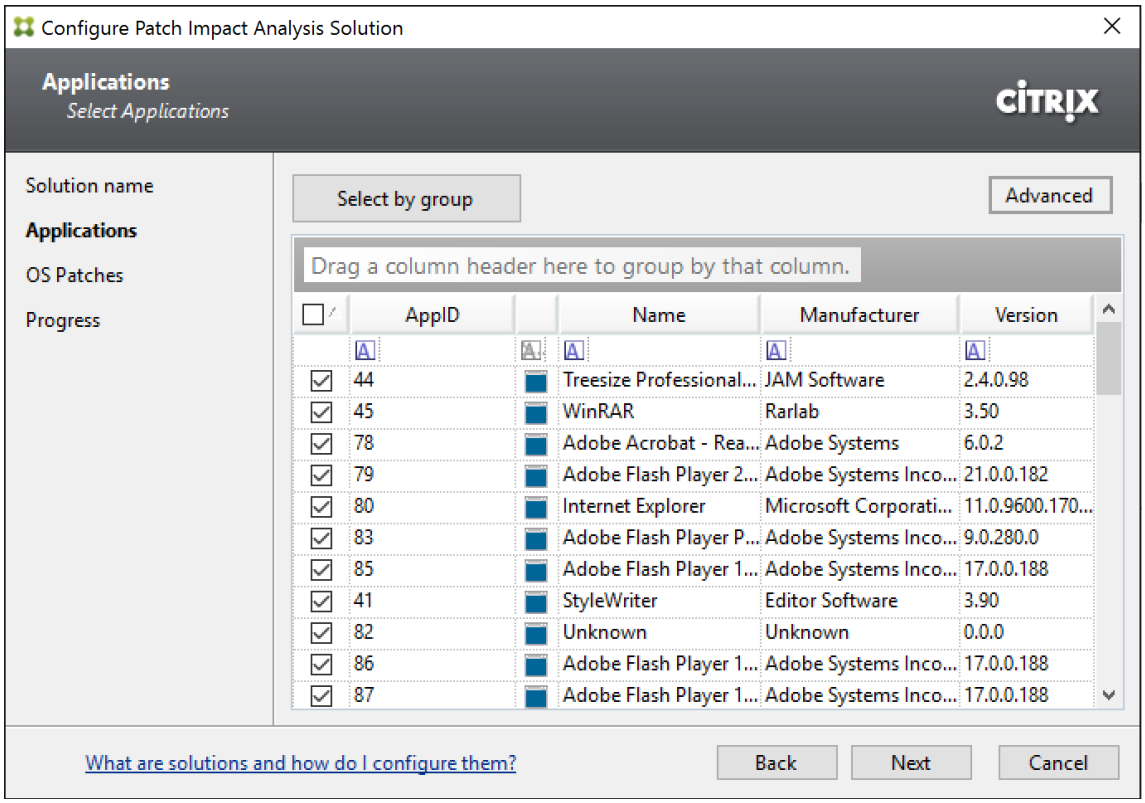
To integrate the Patch Impact Analysis solution with **Windows Server Update Services** (WSUS), the WSUS SDK must be installed on the client. For more information, see Requirements for optional features.

To run patch impact analysis:

1. Go to **Configure** > **Solutions** > **Patch Impact Analysis**.
2. Give the patch impact analysis a name. Click **Next**.

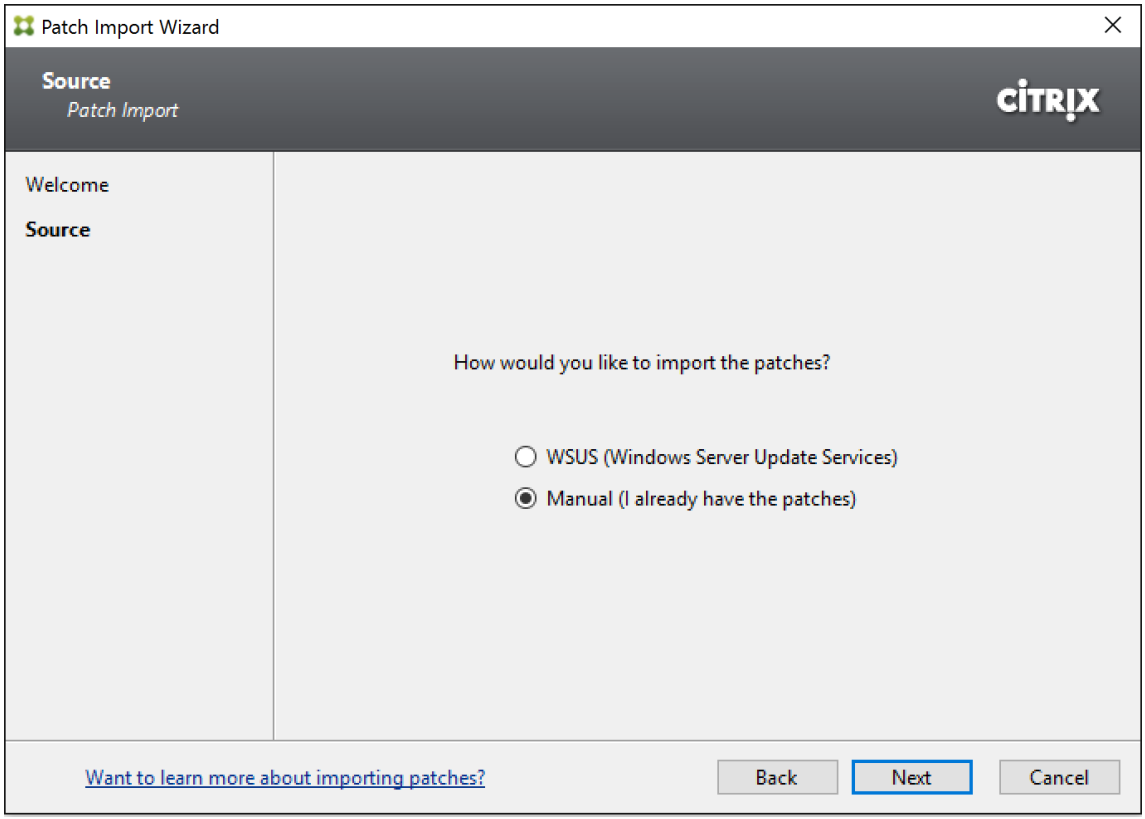


3. Select the applications to analyze. Click **Next**.

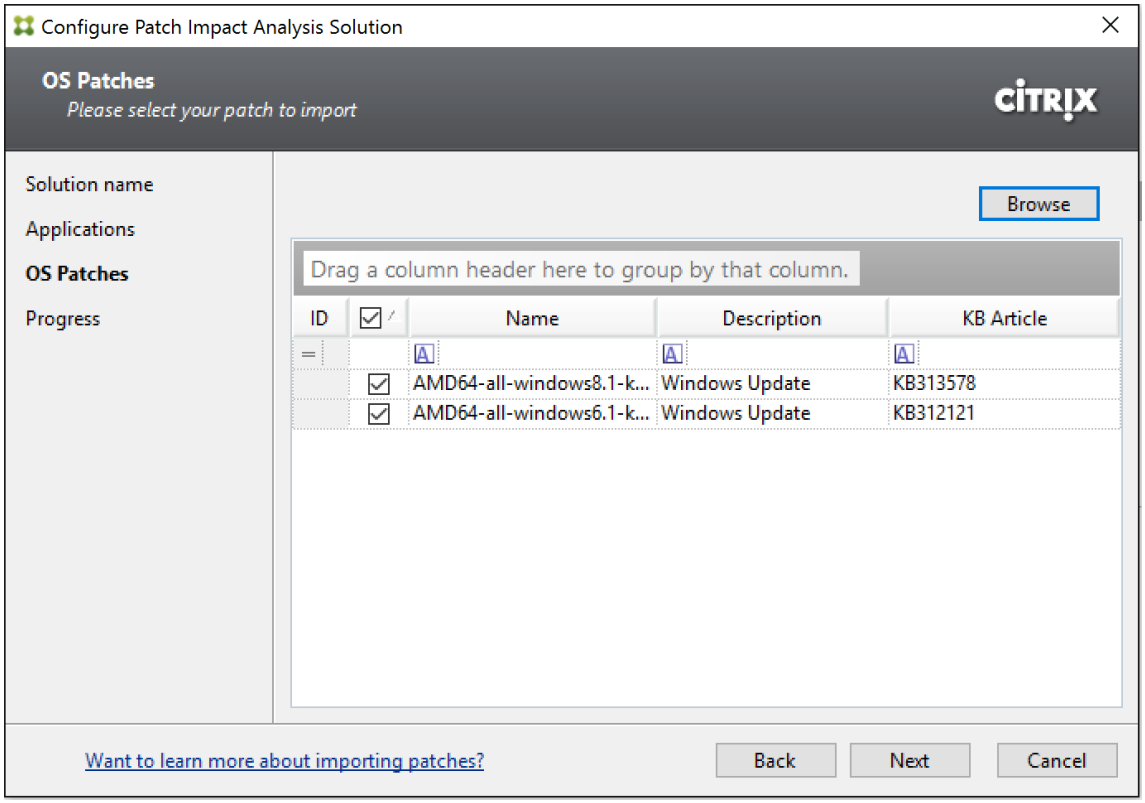


4. Select the method for the patch import.

   Choose **Manual** if you have already downloaded the patches and want to select them from a file share. Choose **WSUS** to use Windows Server Update Services. For WSUS, check you have installed the WSUS SDK on the client (see Requirements for optional features). Click **Next**.



5. Select which patches to analyze the applications against. If the patches are not yet imported, click **Browse** to select the patches.

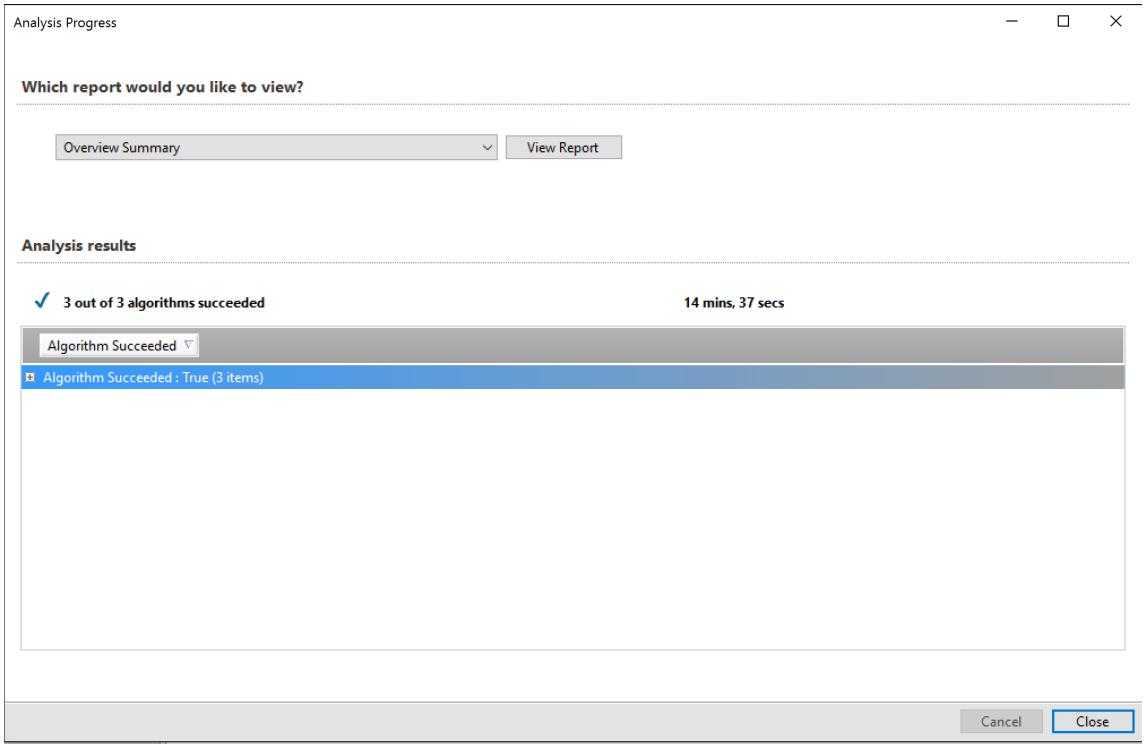


6. Click **Next**.

   The analysis begins by examining the AppDNA database. Information is collected from the patches in a similar way to how information is gathered from other AppDNA collection processes. This information is used to compare the DLLs of the selected apps to those updated as a result of an OS patch upgrade.

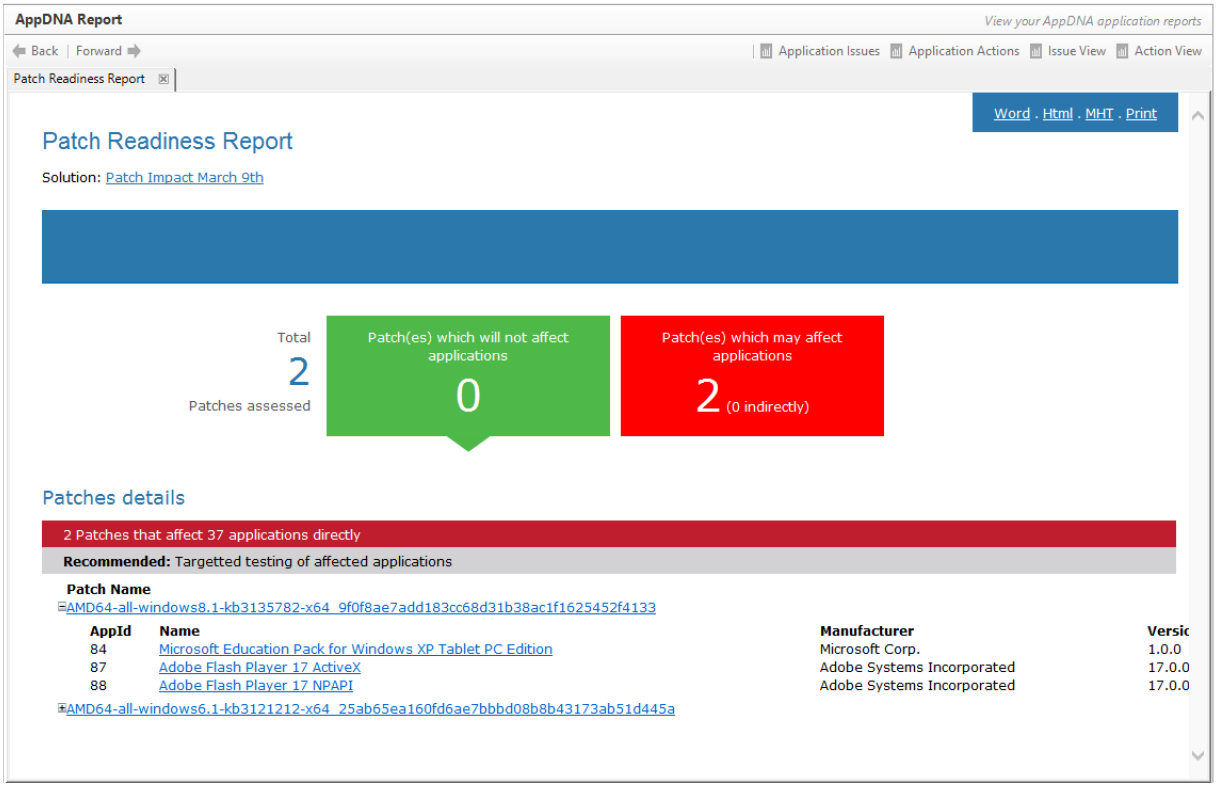
7. Once the analysis preparation is complete, click **Analyze** to being the patch impact analysis process.

8. In the **Analysis results** table, click **+** to expand the table to view algorithms used for the analysis. Use the drop down menu to select which type of report you would like to view, then click **View Report**:



9. After clicking View Report, the screen changes to display the results in the **Patch Readiness Report**.

If the results of a patch import analysis trigger any form of an event, the itemized details will display a hyperlink in the Patch details portion of the screen; clicking one of the links displays additional information for the analyzed content.



Prepare for a XenApp or XenDesktop 7.x upgrade

August 1, 2018

The XenApp and XenDesktop 7.x Upgrade solution provides the information you need when planning how to deliver applications after an upgrade. The solution provides information such as:

- The delivery method available for your applications, either server hosted or desktop hosted.

  Server hosted refers to applications and desktops that reside on a Server OS machine, either physical or virtual. These deployments provide users access to applications from StoreFront, their Start menu, or a URL you provide to them. Applications are delivered virtually and display seamlessly in high definition on user devices.

  Desktop hosted refers to applications and desktops that reside on a virtual Desktop OS machine. These deployments support applications that run on older operating systems and architectures, while providing users with applications that display seamlessly in high-definition.

- The applications that require remediation to work with XenApp or XenDesktop 7.x in your target deployment.
- The applications that will not work with XenApp or XenDesktop 7.x in your target deployment.

Note: For information about upgrading to XenApp or XenDesktop 7.x, refer to the Upgrade topics in the XenApp and XenDesktop 7.x documentation in eDocs.

To configure a XenApp and XenDesktop 7.x Upgrade solution

Before you start, gather the following information.

- For your current XenApp or XenDesktop deployment:
  - The version of XenApp or XenDesktop that you are upgrading
  - The operating system family on which it is installed
  - Whether App-V is used
- The applications you want to deliver
- For your target XenApp or XenDesktop deployment:
  - Whether it will use App-V
    XenDesktop 7.x supports App-V as the preferred technology to stream applications to user devices. It does not support XenApp application streaming.
  - The desktop operating systems to use (if delivering virtual desktops)
    AppDNA provides a default image for the Windows desktop operating systems. You can import custom images, as described in Operating system images.

1. In the AppDNA side bar, click Solutions and then click Add solution.
2. In the Solutions Templates page, select XenApp and XenDesktop 7.x Upgrade and then click Next.

   The solution wizard opens.
3. Identify the solution: In the Solution name page, type a Solution name and Description, to be used in the solution report.
4. Specify your current environment:

   a) In the Platform name page, type a Platform name to identify the platform of your current XenDesktop deployment.

      Including the main characteristics of your platform in the name, such as “Windows 2008 64-bit”, will help you distinguish this platform later in the list of available platforms.

   b) Provide an optional Description of the platform.

   c) Choose your platform parameters.
5. Choose applications: In the Applications page, select the applications you want to include in the upgrade.
6. To review or edit the target platform, click XenDesktop 7.x Upgrade target and then click Edit.

Important: The default target, Windows Server 2012, 64-bit, is the recommended best practice. Other than changing the App-V selection, we recommend that you not change the other target settings unless necessary.

On the Desktop deployment page, change the settings as needed:

- By default, if AppDNA detects major issues with server OS hosting, it uses desktop OS hosting for the operating systems that are selected. To prevent any desktop hosting, clear the Host applications on desktop check box.
- To remove a particular desktop operating system from the analysis, clear the check box for it.
- To choose a different image for a desktop operating system, choose it from the menu.

  The menu lists the default image provided with AppDNA and any custom operating system images that you import, as described in Operating system images.

7. To complete the solution:

   a) After you finish defining the current and target platforms, click Build.
   b) On the Progress page, click Analyze. When the analysis completes, choose report to view and then click Finish.

   To view the reports at any time: In the AppDNA side bar, click Solutions and then click the name of the solution.

To interpret a XenDesktop Upgrade Report

A XenDesktop Upgrade Report lists the applications you selected, sorted under the following categories:

- **Applications that can run… —** No action is required for these applications to run in a XenApp or XenDesktop 7.x environment on the target platform. The deployment method for these applications is server hosted.
- **Applications that require remediation to run… —** These applications can run in a XenApp or XenDesktop 7.x environment on your chosen target platform if you perform remediation. Click the Remediation link in the report for details.
- **Applications that must be deployed using desktop hosting (pooled or dedicated)… —** These applications can run in a XenApp or XenDesktop 7.x environment on your chosen target platform if you deploy them using pooled or dedicated desktops.
- **Applications that cannot be deployed with XenDesktop 7.x —** These applications cannot be deployed using Server OS or Desktop OS machines without redevelopment. Click the Reason link for details.

For more information about Server OS and Desktop OS machines, refer to Plan for hosting desktops and applications in the XenApp and XenDesktop 7.x documentation in eDocs.

To add an existing platform to a solution

1. In the AppDNA side bar, click Solutions.
2. In the Solutions pane, click the solution category and then click Edit across from the solution name.
3. Click the  icon above Existing platforms and then complete the wizard.

   The report reflects the platform you just added.

To build a report for a different platform

1. In the AppDNA side bar, click Solutions.
2. In the Solutions pane, click the solution category and then click Edit across from the solution name.
3. Click Next, click a platform, and then click Build.

Prepare for a move to XenApp or XenDesktop 7.x

August 1, 2018

The XenApp and XenDesktop 7.x adoption solution provides the information you need when planning how to deliver applications after moving from non-Citrix systems to XenApp or XenDesktop. The solution provides information such as:

- The delivery method available for your applications, either server hosted or desktop hosted.

  Server hosted refers to applications and desktops that reside on a Server OS machine, either physical or virtual. These deployments provide users access to applications from StoreFront, their Start menu, or a URL you provide to them. Applications are delivered virtually and display seamlessly in high definition on user devices.

  Desktop hosted refers to applications and desktops that reside on a virtual Desktop OS machine. These deployments support applications that run on older operating systems and architectures, while providing users with applications that display seamlessly in high-definition.
- The applications that require remediation to work with XenApp or XenDesktop 7.x in your target deployment.
- The applications that will not work with XenApp or XenDesktop 7.x in your target deployment.

To configure a XenApp and XenDesktop 7.x Adoption solution

Before you start, gather the following information.

- For your current environment:
  - The operating system family
  - Whether App-V is used
- The applications you want to deliver
- For your target XenApp or XenDesktop deployment:
  - Whether it will use App-V
    XenApp and XenDesktop 7.x supports App-V as the preferred technology to stream applications to user devices. It does not support XenApp application streaming.
  - The desktop operating systems to use (if delivering virtual desktops)
    AppDNA provides a default image for the Windows desktop operating systems. You can import custom images, as described in Operating system images.

1. In the AppDNA side bar, click Solutions and then click Add solution.
2. In the Solutions Templates page, select XenApp and XenDesktop 7.x Adoption and then click Next.

   The solution wizard opens.
3. Identify the solution: In the Solution name page, type a Solution name and Description, to be used in the solution report.
4. Specify your current environment:

   a) In the Platform name page, type a Platform name to identify the platform of your current environment.

   Including the main characteristics of your platform in the name, such as “Windows 8.1 32-bit”, will help you distinguish this platform later in the list of available platforms.

   b) Provide an optional Description of the platform.

   c) Choose your platform parameters.
5. Choose applications: In the Applications page, select the applications you want to deliver after moving to XenDesktop.

   Your existing platform appears in the Solutions platforms page.
6. To review or edit the target platform, click XenDesktop 7.x Adoption target and then click Edit.

   On the Desktop adoption page, change the settings as needed:

   - By default, if AppDNA detects major issues with server OS hosting, it uses desktop OS hosting for the operating systems that are selected. To prevent any desktop hosting, clear the Host applications on desktop check box.

- To remove a particular desktop operating system from the analysis, clear the check box for it.
- To choose a different image for a desktop operating system, choose it from the menu.

  The menu lists the default image provided with AppDNA and any custom operating system images that you import, as described in Operating system images.

7. To complete the solution:

   a) After you finish defining the current and target platforms, click Build.
   b) On the Progress page, click Analyze. When the analysis completes, choose report to view and then click Finish.

   To view the reports at any time: In the AppDNA side bar, click Solutions and then click the name of the solution.

To interpret a XenDesktop Adoption Report

A XenDesktop Adoption Report lists the applications you selected, sorted under the following categories:

- **Applications that can run… —** No action is required for these applications to run in a XenApp or XenDesktop 7.x environment on the target platform. The deployment method for these applications is server hosted.
- **Applications that require remediation to run… —** These applications can run in a XenApp or XenDesktop 7.x environment on your chosen target platform if you perform remediation. Click the Remediation link in the report for details.
- **Applications that must be deployed using desktop hosting (pooled or dedicated)… —** These applications can run in a XenApp or XenDesktop 7.x environment on your chosen target platform if you deploy them using pooled or dedicated desktops.
- **Applications that cannot be deployed with XenDesktop 7.x —** These applications cannot be deployed using Server OS or Desktop OS machines without redevelopment. Click the Reason link for details.

To add an existing platform to a solution

1. In the AppDNA side bar, click Solutions.
2. In the Solutions pane, click the solution category and then click Edit across from the solution name.
3. Click the  icon above Existing platforms and then complete the wizard.

   The report reflects the platform you just added.

To build a report for a different platform

1. In the AppDNA side bar, click Solutions.
2. In the Solutions pane, click the solution category and then click Edit across from the solution name.
3. Click Next, click a platform, and then click Build.

Install Capture

August 1, 2018

You use Install Capture to import Windows applications for which an MSI, SFT, or APPV file is not available. Install Capture installs the application within a virtual machine and creates an MSI file that is then imported into AppDNA. Generally the MSI that is created simply captures the application's DNA for import into AppDNA and is not suitable for actually installing the application. If you have the necessary additional software, the capture process can create usable MSIs and App-V sequences.

Install Capture requires the use of a virtual machine based on one of the following desktop virtualization technologies:

- **Hyper-V** – When using this technology, Install Capture requires a virtual machine for its exclusive use and a Hyper-V user account that provides administrative permissions. The guest operating system must be configured to allow remote desktop connections. Under some configurations, the virtual machine needs the Hyper-V Integration Services to be installed (these are supported on Windows XP SP2 and later). When using Windows 8 Hyper-V Client, the AppDNA client must be installed on the same machine as the Hyper-V Client.
- **VMware vSphere** – When using this technology, you need access to a fully licensed installation of vSphere, a virtual machine for the exclusive use of Install Capture, and a vSphere user account that provides permissions for advanced virtual machine operations through web services (including powering the virtual machine on and off, resetting and suspending the virtual machine, and creating and reverting a snapshot). The virtual machine must be configured to allow remote desktop connections and must have the VMware Tools installed. The vSphere host server must have web services enabled.
- **Citrix XenServer** – When using this technology, you need access to a XenServer host server, a virtual machine for the exclusive use of Install Capture, and XenServer permissions that allow you to create and revert virtual machine snapshots.
- **VMware Workstation** – You can download this from https://www.vmware.com/tryvmware/?p=vmware-workstation&lp=1.

The virtualization technology must be installed and configured in such a way that AppDNA can communicate with the machine that hosts the virtual machine (called the host machine). Depending on

the technology and how it has been configured, this may be the same machine that AppDNA is installed on. For example, for VMware Workstation, AppDNA must be installed on the host machine yet XenServer and vSphere are invariably installed on a different machine from AppDNA.

AppDNA must be able to communicate with the virtual machine's operating system (called the guest operating system). This means that the guest operating system must be connected to the network. If you choose to copy the results (rather than stream them) both AppDNA and the guest operating system must be able to read and write to a designated output folder, either on the host machine or a network share.

The AppDNA client that is running the Install Capture must have exclusive use of the virtual machine.

Within AppDNA you use the Virtual Machine Configuration wizard to create a configuration for the virtual machine that you want to use for the Install Capture. The configuration stores all of the information that Install Capture needs to be able to manage the virtual machine.

This section starts with a general overview of the setup requirements that need to be implemented before running the wizard. The requirements are broken down into a number of generic steps. There are various ways that these steps can be implemented. The generic requirements are followed by details of one possible approach for each of the virtualization technologies plus step-by-step instructions for using the wizard.

Install Capture does not support restarts of the VM.

Set up a virtual machine

August 1, 2018

This topic provides a general overview of the setup requirements for an Install Capture virtual machine. There are a number of possible approaches to how you might implement each of these generic steps.

Typically you would implement these steps before using the Virtual Machine Configuration Wizard within AppDNA. However, the wizard provides an option to open the virtual machine in a console and you can perform the virtual machine setup steps in the console as you work through the wizard. (This does not include the first two steps, because the wizard requires the virtual machine to already exist.)

1. Create a virtual machine (or obtain the virtual machine files) based on one of the technologies listed in Install Capture.

   When capturing Windows applications for testing compatibility with a desktop or server Windows platform, the guest OS should match the OS on which the applications are currently running. For example, if you are preparing for a migration from Windows 7 to Windows 10, the

virtual machine should be based on Windows 7. However, when using the virtual machine to create production MSIs, App-V sequences, or XenApp profiles, the guest OS should normally match the target OS.

The virtual machine should not have anti-virus software running, because this can interfere with the Install Capture process.

To communicate with the virtual machine, AppDNA needs the IP address, or machine or DNS name of the guest OS. Using the machine or DNS name requires an appropriate name resolution mechanism (such as DNS) to be configured on the network. If using the IP address, Citrix recommends that the virtual machine is configured with a static IP address. If the IP address changes, you will need to update the guest OS IP address stored in the virtual machine configuration.

2. Start and stop the virtual machine.

   This is to ensure that the virtual machine is working properly.

3. If you plan to use Install Capture to create virtual application packages, you must install additional software on the virtual machine, such as the App-V Sequencer or XenApp Profiler. This additional software does not come with AppDNA.

   Depending on the additional software, you may need to edit the execution profiles accordingly.

4. Ensure that the user account that will be used to log on to the virtual machine to perform an Install Capture has administrative privileges.

   This user account can be the local administrator account within the virtual machine or another user account that has been added to the Administrators group on the virtual machine.

   Citrix recommends that you configure the virtual machine for automatic log on with this administrative user account and that you suppress any legal notices that appear at logon. This means that you do not need to log on to the virtual machine manually during the Install Capture process.

   Note: If policies do not allow automatic log on (or the suppression of any legal notices), you may want to create the snapshot of the virtual machine while the guest OS is logged on. This means that when AppDNA reverts the virtual machine at the start of the Install Capture, there will be no need for any user interaction.

5. Create a folder on the AppDNA machine or a network share in which to store the Install Capture output files, such as the MSIs for importing into AppDNA. This folder can optionally also be used for the input files.

   Install Capture can handle the output files in two different ways:

   - **Stream results** – With this option, Install Capture initially stores the output files in a staging folder within the virtual machine. Then, after the capture is complete, the output files

are streamed to a folder on the AppDNA machine or a network share. AppDNA requires read-write access to this folder but the virtual machine does not need to access it.

- **Copy results** – With this option, Install Capture stores the output files directly in a folder on the AppDNA machine or a network share. Both AppDNA and the virtual machine require read and write access to this folder. This option is faster than the streaming option. Citrix recommends this option if you intend to run batches of captures unattended, for example, using auto-clicker.

You select the option to use when you create the virtual machine configuration within AppDNA.

The virtual machine also needs access to the location of the input files. You can either store these input files in the same folder as the output, or you can create a separate shared folder for the input files. In all cases the virtual machine needs to have read access to the input files. If you will be importing installation packages from Active Directory or ConfigMgr, the virtual machine also needs access to the Active Directory or ConfigMgr domain and the location of the installation packages.

6. If you plan to use the option to copy the results, take steps to ensure that the virtual machine has read and write access to the folder created in the previous step. If you plan to use the option to stream the results, the virtual machine only requires read access to the folder in which the input files are stored.

   There are a number of ways that you can set up the folder so that the virtual machine has access to it:

   - If you will log on to the virtual machine as a domain user and the shared folder resides on a machine in the same domain or a trusted domain, you can grant that user access to the share.
   - Create a user with the same name and credentials on both the AppDNA machine and the virtual machine. Create a shared folder on the AppDNA machine and grant that user read-/write access to that shared folder. By logging on to the virtual machine with the same credentials to run Install Capture, the shared folder should be accessible from within the virtual machine.
   - Establish a persistent connection to the share from within the virtual machine using appropriate credentials. If the shared folder is on the host machine, you can use the same user credentials that you use to log on to the host machine. If the shared folder resides within a domain, use domain credentials.

7. Install the Citrix AppDNA VM Configuration MSI within the virtual machine, and then restart the virtual machine.

   To do this, you need the installer (called Citrix AppDNA VM Configuration.msi). This comes with AppDNA. It is copied into a Tools subfolder of the AppDNA installation folder when you install AppDNA. The default location is C:\Program Files\Citrix\AppDNA\Tools (C:\Program Files

(x86)\Citrix\AppDNA\Tools on a 64-bit machine).

The version of the VM Configuration MSI must match the version of AppDNA you are running. This means that you need to upgrade the VM Configuration tools on the virtual machine when you upgrade AppDNA.

8. This step applies only if the guest OS supports User Account Control (UAC).

   The Citrix AppDNA VM Configuration MSI installs Remote Admin, which is an AppDNA agent that runs within the virtual machine to provide support for AppDNA to communicate with the virtual machine. If UAC is enabled on the guest OS, every time that Remote Admin starts, Windows opens a UAC dialog box that asks for permission to change the computer. This can be problematic if it happens for every Install Capture, because it requires user interaction and so prevents a batch of captures running unattended.

   The recommended solution is to disable UAC on the virtual machine (for example, as described in http://support.microsoft.com/kb/975787). However, this is not normally necessary on Windows 8 or Windows Server 2012, because the VM Configuration MSI automatically disables UAC on these operating systems.

   If disabling UAC is not possible, create the snapshot while Remote Admin is running as explained in the next step.

9. After completing the above steps, create a snapshot of the virtual machine's state within the virtualization technology. Install Capture uses this snapshot to return the virtual machine to a known state at the start of each capture.

   If the guest OS supports UAC and your security policy does not allow UAC to be disabled, create the snapshot of your virtual machine when Remote Admin is running. This means that Remote Admin will already be running when you run Install Capture and so the UAC dialog box will not appear during the Install Capture process. If you create the snapshot of the virtual machine when the virtual machine is powered off, the UAC prompt will open every time you run Install Capture, which can be disruptive and prevents a batch of captures running unattended.

10. Configure the anti-virus software to disable on-access scanning of the Install Capture output and input folders.

Hyper-V

August 2, 2018

This topic provides an example of how to set up a Hyper-V virtual machine (along with the machine on which AppDNA runs) for use with Install Capture when migrating from Windows 7 to Windows 10.

This example shows one possible approach and is not meant to suggest that this is the only method. For the generic setup requirements, see Set up a virtual machine.

> **Note**
>
> Limitation: Connecting to local Hyper-V generates an error. The workaround is to run AppDNA as an administrator.

Pre-requisites

- Either Hyper-V Server is configured on a separate machine from the one on which AppDNA is running or Windows 10 Hyper-V Client and the AppDNA client are installed on the same Windows 10 machine.
- A Hyper-V virtual machine with a clean build of Microsoft Windows 7 already exists for use with Install Capture. For information about creating a Hyper-V virtual machine, refer to the Hyper-V documentation.
- The virtual machine is connected to the same domain as the machine on which you are running AppDNA (called the AppDNA machine).
- If you are using Hyper-V Server, you know the IP address or DNS name of the Hyper-V host server and have the user name and password of an administrative user account that has permissions to access Hyper-V and control the virtual machine. Alternatively, if you are using Hyper-V Client, your own Windows log on account must have administrative permissions to access Hyper-V and control the virtual machine.

  The user account must be part of the Administrators or Hyper-V Administrators group on the Hyper-V machine. Alternatively, the user account can be granted explicit Hyper-V permissions to control virtual machines, as described in this MSDN article.
- You have the user name and password of an administrative user account for the guest operating system.

In order for the virtual machine to access the shared folder on the AppDNA machine, this example configures the virtual machine for automatic log on with the same domain user account that you use to log on to Windows on the AppDNA machine. (This is called your domain user account below.)

Note: These instructions cover setting up the virtual machine after opening it in a console through Hyper-V Manager. If you do not have access to this, you must ask your Hyper-V administrator to install the Hyper-V Integration Services on the virtual machine and configure it to allow remote desktop connections. You can perform all of the other setup steps when you work through the AppDNA Virtual Machine Configuration wizard, which is documented in the next topic. (The wizard opens the virtual machine in a console.)

Use Hyper-V Manager to open the VM

This section provides instructions for using Hyper-V Manager to open the virtual machine in a console so that you can set up the virtual machine.

1. On the Windows Start menu, choose Administrative Tools > Hyper-V Manager.
2. In the tree in the left pane, select the Hyper-V server on which the virtual machine is hosted. The virtual machines that are hosted on that Hyper-V host appear in the Virtual Machines list.
3. Right-click the virtual machine that you want to use for Install Capture and choose Connect.
4. If the virtual machine is not running, choose Action > Start.
5. When prompted, log on to the virtual machine using an administrative user account.

You are now ready to perform the virtual machine setup tasks that are described below.

Install Hyper-V Integration Services on the VM

In order to use a Hyper-V Windows 7 virtual machine for Install Capture, it must have the Hyper-V Integration Services installed on it. If you do not have access to Hyper-V Manager, ask your Hyper-V administrator to perform this step for you.

Note: The Hyper-V Integration Services are always required when the guest OS is Windows 7 or when you are using Windows 10 Hyper-V Client. They may also be required in some other configurations.

1. In Hyper-V Manager, open the virtual machine and log on to it using an administrative user account.
2. From the menus in the console window, choose Action > Insert Integration Services Setup Disk.
3. In the AutoPlay window, select Install Hyper-V Integration Services. This starts the installation of the Hyper-V Integration Services.
4. When the installation is complete, restart the virtual machine.

Configure the VM to allow remote desktop connections

In order to use the Hyper-V virtual machine for Install Capture, it must be configured to allow remote desktop connections. If you do not have access to Hyper-V Manager, ask your Hyper-V administrator to perform this step for you.

1. Log on to the virtual machine.
2. Open Control Panel > System. (If necessary, first switch to Classic View.)
3. In the System Properties dialog box, click the Remote tab.
4. Under Remote Desktop, select the Allow users to connect remotely to this computer check box.
5. Click OK to preserve your changes.

Enable DCOM on the VM

Communication between the Hyper-V host and the VM requires that DCOM is enabled on the VM. To enable DCOM, see Enable or Disable DCOM. Also verify that port 135 is open for DCOM.

Create the shared folder on the AppDNA machine

These instructions describe how to create a folder on the AppDNA machine and share it so that the virtual machine can read and write to it.

1. Create a folder (for example, C:\AppDNAOutput) on the AppDNA machine to store the Install Capture output.
2. Share the folder and give everyone read and write permissions. For example:
    a) Open Windows Explorer and locate the folder that you want to share.
    b) Right-click the folder and from the shortcut menu, choose Sharing > Advanced Sharing.
    c) Click Advanced Sharing and then in the Advanced Sharing dialog box, select the Share this folder check box.
    d) Click Permissions.
    e) In the Permissions dialog box, click Everyone, and then for Full Control, Change, and Read, select the Allow check box.
    f) Click OK twice.

Note: The virtual machine also needs access to the location of the input files. To use an existing shared folder that contains the applications deployed within your organization, ensure that it is accessible from within the virtual machine. Otherwise you can either store these input files in the same folder as the output, or you can create a separate shared folder for the input files. In all cases the virtual machine must have read access to the input files.

Add your domain user account as an administrator on the VM

Note: It is not necessary to perform this step if your domain user account has already been set up as an administrative user on the virtual machine.

1. Log on to the virtual machine.
2. Open Control Panel > Administrative Tools > Computer Management. (If necessary, first switch to Classic View.)
3. In the tree in the left pane, click System Tools > Local Users and Groups > Groups.
4. In the right pane, double-click Administrators.
5. In the Administrators Properties dialog box, click Add.
6. In the Select Users, Computers, or Groups dialog box, enter your domain-qualified username (for example, Domain\User) in the Enter the object names to select box.

7. Click OK to close the Select Users, Computers, or Groups dialog box.
8. Click OK to close the Administrators Properties dialog box.

Configure the virtual machine for automatic log on

This is an optional step that speeds up Install Capture. If you choose not to perform this step, you will need to log on to the virtual machine manually with your domain user account every time the virtual machine starts up.

On the virtual machine, follow the instructions in http://support.microsoft.com/kb/315231 to set up automatic log on with your domain username.

Turn off simple file sharing on the AppDNA and virtual machines

Carry out the following steps on both the AppDNA machine and the virtual machine.

1. In Windows Explorer, choose **Folder Options** > **View**.
2. Clear the **Use simple file sharing (Recommended)** check box.
3. Click **OK**.

Anti-virus configuration on the AppDNA machine

You must configure the anti-virus software on the AppDNA machine to disable on-access scanning of the Install Capture output and input folders. For example, for Norton Anti-Virus, you disable the auto-protect option for the AppDNA output and input folders.

Verify access to the shared folder

You now need to check that the virtual machine can access the shared folder that you created earlier on the AppDNA machine.

On the virtual machine, type the following into the Windows Start > Run prompt:

```
1  \\<AppDNA machine name>\AppDNAOutput
```

Where <AppDNA machine name> is the name of the AppDNA machine.

If this opens the shared folder on the AppDNA machine, it verifies that the virtual machine can access it. For troubleshooting tips, see Troubleshooting Access to a Shared Folder from the Virtual Machine.

Install the AppDNA VM Configuration MSI on the virtual machine

To do this, you need the installer (called Citrix AppDNA VM Configuration.msi). This comes with AppDNA. It is copied into a Tools subfolder of the AppDNA installation folder when you install AppDNA. The default location is C:\Program Files\Citrix\AppDNA\Tools (C:\Program Files (x86)\Citrix\AppDNA\Tools on a 64-bit machine).

1. Install the Citrix AppDNA VM Configuration MSI within the virtual machine, accepting the default file location.
2. Restart the virtual machine.

Important: Ensure that the AppDNA VM Configuration MSI has the same version number as the version of AppDNA that you are using. This means that you need to upgrade the VM Configuration on the virtual machine when you upgrade AppDNA.

Configure AppDNA to run elevated

Note: This step is relevant only if you are using Windows 8 Hyper-V Client.

If you are using Windows 8 Hyper-V Client, you must run AppDNA to run as an administrator when interacting with the virtual machine – for example, when using the Virtual Machine Configuration wizard or running Install Capture.

You can configure AppDNA so that it is always run as an administrator as follows:

1. If necessary, close AppDNA.
2. In Windows Explorer, locate AppDNA.exe. The following table shows the default location of this file.

Machine type	Default location
64-bit	C:\Program Files\Citrix\AppDNA\Client

3. Right-click the file and from the shortcut menu, choose Properties.
4. Click the Compatibility tab.
5. Under Privilege level, select the Run this program as an administrator check box.
6. Click OK to save the changes.

Take a snapshot of the virtual machine

1. Connect to the virtual machine in Hyper-V Manager.

2. From the menus in the console, choose Action > Snapshot. In the Snapshot Name dialog box, enter a name for the snapshot, and then click Yes.

You are now ready to use the AppDNA Virtual Machine Configuration wizard to set up a virtual machine configuration for use with Install Capture. See Configure a Hyper-V VM for step-by-step instructions.

Configure a Hyper-V VM

August 1, 2018

This topic provides an example of using the Virtual Machine Configuration wizard to set up the virtual machine configuration for a Hyper-V virtual machine.

This example assumes that you have used Hyper-V Manager to set up the virtual machine as explained in Set up a Hyper-V VM for Install Capture or all of the following are true:

- You have the pre-requisites described in Set up a Hyper-V VM for Install Capture.
- If you are using the Windows 8 Hyper-V Client, you have configured AppDNA to run with administrator privileges, as described in Set up a Hyper-V VM for Install Capture.
- Your Hyper-V administrator has installed Hyper-V Integration Services on the virtual machine and configured it to allow remote desktop connections.
- You have performed the AppDNA machine setup tasks described in Set up a Hyper-V VM for Install Capture.

1. Start AppDNA.
2. From the AppDNA menus, choose Edit > Settings.
3. On the Virtual Machines tab, click New and then click Next.
4. In the Virtual Machine Configuration Details step, enter a name and a description for the virtual machine configuration, click Hyper-V, and then click Next.
5. Specify the Hyper-V Host Details for the Hyper-V server or client:
    - **Hyper-V server** – Specify the IP address or DNS name of the Hyper-V host server. Then enter the user name and password of the account to use to connect to Hyper-V. The user name must include the machine name, using the form machinename\user. If this is your domain account, enter your domain-qualified user name (for example, domain\user or user@domain.com).

      Citrix recommends that you use a dedicated Hyper-V user account whose password is set to never expire rather than your standard domain account.

      Important: If the password changes in the future, you will need to run this wizard again to enter the new password.

- **Hyper-V client** – Enter localhost in the Hostname / IP Address box and leave the Username and Password boxes blank. (In this configuration, you must be running AppDNA on the same machine as the Hyper-V client.)

6. In the Hyper-V Virtual Machine step, select the virtual machine that you want to use.

   This should be a dedicated virtual machine for use with Install Capture run from this AppDNA client.

7. In the Hyper-V Snapshot Selection step, select the virtual machine snapshot that you want to use. If you set up the virtual machine as explained in Set up a Hyper-V VM for Install Capture, this is the snapshot you took as the final step. If there are no snapshots in the list, click Create to take a snapshot of the virtual machine now.

   The wizard performs a series of checks. If any of these fail, see Hyper-V Snapshot Selection for troubleshooting information. The wizard then opens the virtual machine in the console. This may take a few minutes, particularly if the guest OS needs to be started. If you did not perform the virtual machine setup steps, perform them in virtual machine when it opens in the console. You will have an opportunity to take another snapshot at the end of the wizard.

8. In the Virtual Machine Connection step, you can generally accept the default values, because the wizard attempts to retrieve the guest operating system's machine name for you and you do not normally need to change the Remote Admin TCP port.

   For more information about this step and instructions for finding out the IP address of the virtual machine, see Virtual Machine Connection.

9. In the Capture Output Location step, select Copy results to network share (faster) and specify the output folder that you created on the AppDNA machine earlier. Make sure you use a UNC path and identify the client or server machine by its host name or IP address – for example, \\AppDNAMachine\AppDNAOutput.

10. In the Virtual Machine State step, select Power off the VM and take a snapshot (Recommended), and then click Next and Finish.

    This closes the wizard and returns you to the Install Capture page in the Settings dialog box, where you should now see the virtual machine configuration.

11. Click Save.

The virtual machine configuration now appears in the list of virtual machine configurations on the Install Capture tab in the Import Applications screen.

vSphere

August 1, 2018

This topic provides an example of how to set up a VMware vSphere virtual machine (along with the machine on which AppDNA runs) for use with Install Capture when migrating from Windows XP to Windows 7. This example shows one possible approach. For the generic setup requirements, see Set up a virtual machine.

Pre-requisites

- VMware vSphere is already installed and configured on a separate machine from the one on which AppDNA is running.
- A vSphere virtual machine with a clean build of Windows XP already exists for use with Install Capture. For information about creating a vSphere virtual machine, refer to the VMware vSphere documentation.
- The virtual machine is connected to the same domain as the machine on which you are running AppDNA (called the AppDNA machine).
- You know the IP address or DNS name of the vSphere host server and have the user name and password of an account that enables you to connect to vSphere and perform advanced virtual machine operations. At a minimum the user account requires permissions to power the virtual machine on and off, to reset and suspend the virtual machine, and to create and revert a snapshot.
- You have the username and password of an administrative user account for the guest operating system.

In order for the virtual machine to access the shared folder on the AppDNA machine, this example configures the virtual machine for automatic log on with the same domain user account that you use to log on to Windows on the AppDNA machine. (This is called your domain user account below.)

Note: These instructions cover setting up the virtual machine in the VMware vSphere Client. If you do not have access to this, you must ask your vSphere administrator to install the VMware Tools on the virtual machine and configure it to allow remote desktop connections. You can perform all of the other setup steps when you work through the AppDNA Virtual Machine Configuration wizard, which opens the virtual machine in a console.

Open a VM in the VMware vSphere Client

This section provides instructions for logging on to the virtual machine in the console in the VMware vSphere Client so that you can set up the virtual machine.

To open the virtual machine in the console in the VMware vSphere Client:

1. On the Windows Start menu, choose All Programs > VMware > VMware vSphere Client. When prompted, enter the connection details.
2. In the tree in the left pane, locate your designated virtual machine.
3. Right-click the virtual machine and from the shortcut menu, choose Open Console.
4. If necessary, click the green arrow button to power on the virtual machine, and when prompted, log on to it.

You are now ready to perform the virtual machine setup tasks that are described below.

Install the VMware Tools on the VM

In order to use the vSphere virtual machine for Install Capture, it must have the VMware Tools installed on it. If you do not have access to the VMware vSphere Client, you can ask your vSphere administrator to perform this step for you.

1. Log on to the virtual machine in the VMware vSphere Client.
2. From the menus in the VMware vSphere Client, choose Inventory > Virtual Machine > Guest > Install/Upgrade VMware Tools.
3. In the Install VMware Tools dialog box, click OK. This starts the VMware Tools installer.
4. Install the VMware Tools, selecting the Typical or Complete option in the Setup Type step.
5. After the installation has finished, restart the virtual machine.

Configure the VM to allow remote desktop connections

In order to use the vSphere virtual machine for Install Capture, it must be configured to allow remote desktop connections. If you do not have access to the VMware vSphere Client, you can ask your vSphere administrator to perform this step for you.

1. Log on to the virtual machine in the VMware vSphere Client.
2. Open Control Panel > System. (If necessary, first switch to Classic View.)
3. In the System Properties dialog box, click the Remote tab.
4. Under Remote Desktop, select the Allow users to connect remotely to this computer check box.
5. Click OK to preserve your changes.

Create the shared folder on the AppDNA machine

These instructions describe how to create a folder on the AppDNA machine and share it so that the virtual machine can read and write to it.

1. Create a folder (for example, C:\AppDNAOutput) on the AppDNA machine to store the Install Capture output.
2. Share the folder and give everyone read and write permissions. For example:
   a) Open Windows Explorer and locate the folder that you want to share.
   b) Right-click the folder and from the shortcut menu, choose Sharing > Advanced Sharing.
   c) Click Advanced Sharing and then in the Advanced Sharing dialog box, select the Share this folder check box.
   d) Click Permissions.
   e) In the Permissions dialog box, click Everyone, and then for Full Control, Change, and Read, select the Allow check box.
   f) Click OK twice.

Note: The virtual machine also needs access to the location of the input files. To use an existing shared folder that contains the applications deployed within your organization, ensure that it is accessible from within the virtual machine. Otherwise you can either store these input files in the same folder as the output, or you can create a separate shared folder for the input files. In all cases the virtual machine must have read access to the input files.

Add your domain user account as an administrator on the VM

Note: It is not necessary to perform this step if your domain user account has already been set up as an administrative user on the virtual machine.

1. Log on to the virtual machine in the VMware vSphere Client using an administrative user account.
2. Open Control Panel > Administrative Tools > Computer Management. (If necessary, first switch to Classic View.)
3. In the tree in the left pane, click System Tools > Local Users and Groups > Groups.
4. In the right pane, double-click Administrators.
5. In the Administrators Properties dialog box, click Add.
6. In the Select Users, Computers, or Groups dialog box, enter your domain-qualified username in the Enter the object names to select box (for example, Domain\User).
7. Click OK to close the Select Users, Computers, or Groups dialog box.
8. Click OK to close the Administrators Properties dialog box.

Configure the virtual machine for automatic log on

This is an optional step that speeds up Install Capture. If you choose not to perform this step, you will need to log on to the virtual machine manually with your domain user account every time the virtual machine starts up.

On the virtual machine, follow the instructions in http://support.microsoft.com/kb/315231 to set up automatic log on with your domain username.

Turn off simple file sharing on the AppDNA and virtual machines

Carry out the following steps on both the AppDNA machine and the virtual machine.

1. In Windows Explorer, from the menus choose Tools > Folder Options. (On Windows 8.1, from the Windows Explorer Organize menu, choose Folder and Search Options.)
2. In the Folder Options dialog box, click the View tab.
3. Clear the Use simple file sharing (Recommended) check box. (For Windows 8.1, clear the Use Sharing Wizard (Recommended) check box.)
4. Click OK.

Anti-virus configuration on the AppDNA machine

You must configure the anti-virus software on the AppDNA machine to disable on-access scanning of the Install Capture output and input folders. For example, for Norton Anti-Virus, you disable the auto-protect option for the AppDNA output and input folders.

Verify access to the shared folder

You now need to check that the virtual machine can access the shared folder that you created earlier on the AppDNA machine.

On the virtual machine, type the following into the Windows Start > Run prompt:

```
1  \\<AppDNA machine name>\AppDNAOutput
```

Where <AppDNA machine name> is the name of the AppDNA machine.

If this opens the shared folder on the AppDNA machine, it verifies that the virtual machine can access it. For troubleshooting tips, see Troubleshooting Access to a Shared Folder from the Virtual Machine.

Install the AppDNA VM Configuration MSI on the virtual machine

To do this, you need the installer (called Citrix AppDNA VM Configuration.msi). This comes with AppDNA. It is copied into a Tools subfolder of the AppDNA installation folder when you install AppDNA. The default location is C:\Program Files\Citrix\AppDNA\Tools (C:\Program Files (x86)\Citrix\AppDNA\Tools on a 64-bit machine).

1. Install the Citrix AppDNA VM Configuration MSI within the virtual machine, accepting the default file location.
2. Restart the virtual machine.

Important: Ensure that the AppDNA VM Configuration MSI has the same version number as the version of AppDNA that you are using. This means that you need to upgrade the VM Configuration on the virtual machine when you upgrade AppDNA.

Take a snapshot of the virtual machine

1. Log on to the virtual machine in the VMware vSphere Client.
2. From the menus in the VMware vSphere Client, choose Inventory > Virtual Machine > Snapshot > Take Snapshot
3. In the Take Virtual Machine Snapshot dialog box, enter a Name and Description for the snapshot, and select the Snapshot the virtual machine's memory check box.
4. Click OK.

You are now ready to use the AppDNA Virtual Machine Configuration wizard to set up a virtual machine configuration for use with Install Capture. See Configure a vSphere VM for instructions.

Configure a vSphere VM

August 1, 2018

This topic provides an example of using the Virtual Machine Configuration wizard to set up the virtual machine configuration for a vSphere virtual machine.

This example assumes that you have used the VMware vSphere Client to set up the virtual machine as explained in Set up a vSphere VM for Install Capture or all of the following are true:

- You have the pre-requisites described in Set up a vSphere VM for Install Capture.
- The vSphere administrator has installed the VMware Tools on the virtual machine and configured it to allow remote desktop connections.
- You have performed the AppDNA machine setup tasks described in Set up a vSphere VM for Install Capture.

1. Start AppDNA.
2. From the AppDNA menus, choose Edit > Settings.
3. On the Virtual Machines tab, click New and then click Next.
4. In the Virtual machine configuration details step, enter a name and a description for the virtual machine configuration, select vSphere, and then click Next.

5. In the vSphere host details step, specify the IP address or DNS name of the vSphere host server. If you are connecting directly to a hypervisor, leave the SSO (Single Sign On) server field blank, otherwise, provide the IP address or DNS name of the single sign-on server as well. Then enter the user name and password.

   Citrix recommends that you use a dedicated vSphere user account whose password is set to never expire rather than your standard domain account. If this is your domain account, enter your domain-qualified user name (for example, domain\user or user@domain.com).

   Important: If the password changes in the future, you will need to run this wizard again to enter the new password.

6. In the vSphere virtual machine step, select the virtual machine that you want to use.

   This should be a dedicated virtual machine for use with Install Capture run from this AppDNA client.

7. In the Snapshot selection step, select the virtual machine snapshot that you want to use. If you set up the virtual machine as explained in Set up a vSphere VM for Install Capture, this is the snapshot you took as the final step. If there are no snapshots in the list, click Create to take a snapshot of the virtual machine now.

   The wizard performs a series of checks and then opens the virtual machine in the console. This may take a few minutes, particularly if the guest OS needs to be started. If you did not perform the virtual machine setup steps, perform them in virtual machine when it opens in the console. You will have an opportunity to take another snapshot at the end of the wizard.

8. In the Virtual machine connection step, you can generally accept the default values, because the wizard attempts to retrieve the guest operating system's machine name for you and you do not normally need to change the Remote Admin TCP port.

   For more information about this step and instructions for finding out the IP address of the virtual machine, see Virtual Machine Connection.

9. In the Capture output location step, select Copy results to network share (faster) and specify the output folder that you created on the AppDNA machine earlier. Make sure you use a UNC path and identify the client or server machine by its host name or IP address – for example, \\AppDNAMachine\AppDNAOutput.

10. In the Virtual Machine State step, select Power off the VM and take a snapshot (Recommended), click Next, and then click Finish.

    This closes the wizard and returns you to the Install Capture page in the Settings dialog box, where you should now see the virtual machine configuration.

11. Click Save.

The virtual machine configuration now appears in the list of virtual machine configurations on the Install Capture tab in the Import Applications screen.

XenServer

November 21, 2018

This topic provides an example of how to set up a Citrix XenServer virtual machine (along with the machine on which AppDNA runs) for use with Install Capture when migrating from Windows 7 to Windows 10. This example shows one possible approach. For the generic setup requirements, see Set up a virtual machine.

Pre-requisites

1. XenServer is already installed and configured on a separate machine from the one on which AppDNA is running.
2. A XenServer virtual machine with a clean build of Windows 7 already exists for use with Install Capture. For information about creating a XenServer virtual machine, refer to the Citrix XenCenter documentation. (XenCenter is a desktop tool that you can use to manage your XenServer environment and deploy, manage, and monitor virtual machines from your Windows desktop machine.)
3. The virtual machine is connected to the same network as the machine on which you are running AppDNA (called the AppDNA machine).
4. The virtual machine is not connected to a domain. For instructions for removing the virtual machine from a domain, see Remove the Virtual Machine from the Domain
5. You know the IP address or DNS name of the XenServer host server and have the username and password of an account that enables you to connect to XenServer and perform advanced virtual machine operations (including creating and rolling back snapshots).
6. You have the username and password of an administrative user account for the guest operating system.
7. The user account has advanced operations" permissions. Typically this means that the user account must have at least the "VM power admin" role.

Open the VM in XenCenter

This section provides instructions for logging on to the virtual machine in the console in XenCenter so that you can set up the virtual machine. If you do not have access to XenCenter, you can do the setup

steps when you work through the AppDNA Virtual Machine Configuration wizard. (The wizard opens the virtual machine in a console.)

To open the virtual machine in the console in XenCenter:

1. On the Windows Start menu, choose All Programs > Citrix > Citrix XenCenter. If prompted, enter the connection details.
2. In the Resources pane on the left side, right-click the virtual machine, and choose Start.
3. Click the Console tab, and log on to the virtual machine as an administrative user.

You are now ready to perform the virtual machine setup tasks that are described below.

Create a user on the AppDNA machine and the virtual machine

1. Create an administrator user account called, for example, appdna, on the AppDNA machine and give it a password that never expires. For example:
   a) Open Control Panel. If necessary switch to Classic View.
   b) In the Administrative Tools group, double-click Computer Management.
   c) Expand the tree in the left pane like this: System Tools > Local Users and Groups > Users.
   d) Click Users and from the Action menu, choose New user.
   e) Type the appropriate information in the dialog box.
   f) Click Create, and then click Close.
   g) Right-click the user and from the shortcut menu, choose Properties.
   h) Click the Member Of tab.
   i) Click Add and then type Administrators in the Enter the object names to select box.
   j) Click Check Names and then click OK.
2. If necessary power on the virtual machine, and use the equivalent steps to create an identical administrator user account on the virtual machine, also with a password that never expires.

Configure the virtual machine for automatic log on

This is an optional step. It speeds up Install Capture because it means that you do not need to log on manually every time the virtual machine starts up.

1. On the virtual machine, open a Windows command window.
2. In the window, enter: control userpasswords2.
3. In the User Accounts dialog box, clear the Users must enter a user name and password to use this computer check box, and then click OK.
4. In the Automatically Log On dialog box, enter the Install Capture user's name and password, and then click OK.
5. If you are using an operating system that supports UAC, disable UAC. See http://support.microsoft.com/kb/975787.

Note: For an alternative method of setting up automatic logon, see http://support.microsoft.com/kb/315231. You must use this mechanism for a domain user account.

Turn off simple file sharing on the AppDNA and virtual machines

Carry out the following steps on both the AppDNA machine and the virtual machine.

1. In Windows Explorer, choose **Folder Options** > **View**.
2. Clear the **Use simple file sharing (Recommended)** check box.
3. Click **OK**.

Create the shared folder on the AppDNA machine

These instructions describe how to create a folder on the AppDNA machine and share it so that the virtual machine can read and write to it.

1. Create a folder (for example, C:\AppDNAOutput) on the AppDNA machine to store the Install Capture output.
2. Share the folder and give everyone read and write permissions. For example:
    a) Open Windows Explorer and locate the folder that you want to share.
    b) Right-click the folder and from the shortcut menu, choose Sharing > Advanced Sharing.
    c) Click Advanced Sharing and then in the Advanced Sharing dialog box, select the Share this folder check box.
    d) Click Permissions.
    e) In the Permissions dialog box, click Everyone, and then for Full Control, Change, and Read, select the Allow check box.
    f) Click OK twice.

Note: The virtual machine also needs access to the location of the input files. To use an existing shared folder that contains the applications deployed within your organization, ensure that it is accessible from within the virtual machine. Otherwise you can either store these input files in the same folder as the output, or you can create a separate shared folder for the input files. In all cases the virtual machine must have read access to the input files.

Anti-virus configuration on the AppDNA machine

You must configure the anti-virus software on the AppDNA machine to disable on-access scanning of the Install Capture output and input folders. For example, for Norton Anti-Virus, you disable the auto-protect option for the AppDNA output and input folders.

Verify access to the shared folder

You now need to check that the virtual machine can access the shared folder that you created earlier on the AppDNA machine.

On the virtual machine, type the following into the Windows Start > Run prompt:

```
\\<AppDNA machine name>\AppDNAOutput
```

Where <AppDNA machine name> is the name of the AppDNA machine.

If this opens the shared folder on the AppDNA machine, it verifies that the virtual machine can access it. For troubleshooting tips, see Troubleshooting Access to a Shared Folder from the Virtual Machine.

Install the AppDNA VM Configuration MSI on the virtual machine

To do this, you need the installer (called Citrix AppDNA VM Configuration.msi). This comes with AppDNA. It is copied into a Tools subfolder of the AppDNA installation folder when you install AppDNA. The default location is C:\Program Files\Citrix\AppDNA\Tools (C:\Program Files (x86)\Citrix\AppDNA\Tools on a 64-bit machine).

1. Install the Citrix AppDNA VM Configuration MSI within the virtual machine, accepting the default file location.
2. Restart the virtual machine.

Important: Ensure that the AppDNA VM Configuration MSI has the same version number as the version of AppDNA that you are using. This means that you need to upgrade the VM Configuration on the virtual machine when you upgrade AppDNA.

Take a snapshot of the virtual machine

This step requires access to XenCenter. If you do not have access to XenCenter, the AppDNA Virtual Machine Configuration wizard provides an option to create a snapshot.

1. Select the virtual machine in the Resources pane on the left side of the XenCenter window.
2. Click the Snapshots tab.
3. On the toolbar, click Take Snapshot.
4. In the Take Snapshot dialog box, enter the Name of the new snapshot and optionally a Description.
5. Under Snapshot mode, select the Snapshot the virtual machine's disks and memory option if it is available. Otherwise select the Snapshot the virtual machine's disks option. The Snapshot mode options depend on the XenServer license.
6. Click Take Snapshot.

You are now ready to use the AppDNA Virtual Machine Configuration wizard to set up a virtual machine configuration for use with Install Capture. See Configure a XenServer VM for step-by-step instructions.

Remove the Virtual Machine from the Domain

August 1, 2018

In some environments, domain policies set firewall and other settings that may interfere with Install Capture. Therefore Citrix recommends that the Install Capture virtual machine is not connected to a domain.

Typically, a XenServer virtual machine is connected to a domain. Use the following instructions to remove a XenServer virtual machine from a domain.

1. In the XenServer console, log on to the virtual machine as an administrative user.
2. Click the Windows Start menu, right-click My Computer, and then choose Properties.
3. In the System Properties dialog box, click the Computer Name tab and then click Change.
4. In the Computer Name Changes dialog box, under Member of, choose the Workgroup option.
5. Enter the name of the workgroup (for example, WORKGROUP).
6. Click OK.
7. Restart the virtual machine.

Configure a XenServer VM

August 1, 2018

This topic provides an example of using the Virtual Machine Configuration wizard to set up the virtual machine configuration for a XenServer virtual machine.

This example assumes the following:

- Either you have set up the virtual machine as explained in Set up a XenServer VM for Install Capture. This requires Citrix XenCenter.
- Or you have the pre-requisites and have performed the AppDNA machine setup tasks described in that topic, and you have a suitable virtual machine but have not performed the virtual machine setup tasks. This does not require XenCenter.

1. Start AppDNA.
2. From the AppDNA menus, choose Edit > Settings.
3. In the Settings dialog box side bar, click Install Capture.

4. On the Virtual Machines tab, click New and then click Next.
5. In the Virtual machine configuration details step, enter a name and a description for the virtual machine configuration, select XenServer, and then click Next.
6. In the XenServer host details step, specify the IP address or DNS name of the XenServer host server. Then enter the user name and password of the account to use to connect to XenServer. If this is your domain account, enter your domain-qualified user name (for example, domain\user or user@mydomain.com).

   Citrix recommends that you use a dedicated XenServer user account whose password is set to never expire rather than your standard domain account.

   Note: If the password changes in the future, you will need to run this wizard again to enter the new password.
7. In the XenServer virtual machine step, select the virtual machine that you want to use, and then click Next.

   This should be a dedicated virtual machine for use with Install Capture run from this AppDNA client.
8. In the Snapshot selection step, select the virtual machine snapshot that you want to use. If you set up the virtual machine as explained in Set up a XenServer VM for Install Capture, this is the snapshot you took as the final step. If there are no snapshots in the list, click Create to take a snapshot of the virtual machine now.
9. Click Next to display the virtual machine in the console.

   The wizard performs a series of checks. If any of these fail, refer to Troubleshoot.

   If you did not perform the virtual machine setup steps described in Set up a XenServer VM for Install Capture, perform them in virtual machine when it opens in the console. You will have the option to take another snapshot at the end of working through the wizard.
10. In the Virtual machine connection step, enter the IP address of the virtual machine. Generally you do not need to change the Remote Admin TCP port.
11. In the Capture Output Location step, select Copy results to network share (faster) and specify the output folder that you created on the AppDNA machine earlier. Make sure you use a UNC path and identify the client or server machine by its host name or IP address – for example, \\AppDNAMachine\AppDNAOutput.
12. In the Virtual machine state step, select Power off and take snapshot (recommended), click Next, and then click Finish.

    The Install Capture page in the Settings dialog box displays the virtual machine configuration.
13. Click Save.

The virtual machine configuration appears in the list of virtual machine configurations on the Install Capture tab in the Import Applications screen.

VMware Workstation

August 1, 2018

This example provides step-by-step instructions for setting up a VMware Workstation virtual machine and its host machine for use with Install Capture when migrating from Windows 7 to Windows 10. This example shows one possible approach.

For the generic setup requirements, see Set up a virtual machine.

Note: This example assumes that a suitable Windows 7 virtual machine is already available.

Install and configure the VM

1. Install VMware Workstation on the host machine.
2. Launch VMware Workstation from the Windows Start > Programs menu.
3. In the VMware Workstation console, click Open Existing VM or Team.
4. In the Open dialog box, browse to the VMX file that represents the Windows XP virtual machine, and then click OK.
5. On the virtual machine's tab in the VMware Workstation console, click Edit virtual machine settings.

   The Virtual Machine Settings dialog box opens.
6. On the Hardware tab, click Network Adapter, and in the Network Connection section, select Bridged: Connected directly to the physical network.
7. Click OK to save your changes.
8. On the virtual machine's tab in the VMware Workstation Console, click Power on this virtual machine.

   The virtual machine starts.
9. Open a browser on the virtual machine and open a web page on the Internet to show that the bridged connection is working.
10. In the VMware Workstation console, click the red square on the toolbar to power off the virtual machine.

Turn off simple file sharing on the AppDNA and virtual machines

Carry out the following steps on both the AppDNA machine and the virtual machine.

1. In Windows Explorer, choose **Folder Options > View**.
2. Clear the **Use simple file sharing (Recommended)** check box.
3. Click **OK**.

Create the shared folder on the AppDNA machine

These instructions describe how to create a folder on the AppDNA machine and share it so that the virtual machine can read and write to it.

1. Create a folder (for example, C:\AppDNAOutput) on the AppDNA machine to store the Install Capture output.
2. Share the folder and give everyone read and write permissions. For example:
    a) Open Windows Explorer and locate the folder that you want to share.
    b) Right-click the folder and from the shortcut menu, choose Sharing > Advanced Sharing.
    c) Click Advanced Sharing and then in the Advanced Sharing dialog box, select the Share this folder check box.
    d) Click Permissions.
    e) In the Permissions dialog box, click Everyone, and then for Full Control, Change, and Read, select the Allow check box.
    f) Click OK twice.

Note: The virtual machine also needs access to the location of the input files. To use an existing shared folder that contains the applications deployed within your organization, ensure that it is accessible from within the virtual machine. Otherwise you can either store these input files in the same folder as the output, or you can create a separate shared folder for the input files. In all cases the virtual machine must have read access to the input files.

Create a user on the AppDNA machine and the virtual machine

1. Create an administrator user account called, for example, appdna, on the AppDNA machine and give it a password that never expires. For example:
    a) Open Control Panel. If necessary switch to Classic View.
    b) In the Administrative Tools group, double-click Computer Management.
    c) Expand the tree in the left pane like this: System Tools > Local Users and Groups > Users.
    d) Click Users and from the Action menu, choose New user.
    e) Type the appropriate information in the dialog box.
    f) Click Create, and then click Close.

g) Right-click the user and from the shortcut menu, choose Properties.
h) Click the Member Of tab.
i) Click Add and then type Administrators in the Enter the object names to select box.
j) Click Check Names and then click OK.

2. If necessary power on the virtual machine, and use the equivalent steps to create an identical administrator user account on the virtual machine, also with a password that never expires.

Configure the virtual machine for automatic log on

This is an optional step. It speeds up Install Capture because it means that you do not need to log on manually every time the virtual machine starts up.

1. On the virtual machine, open a Windows command window.
2. In the window, enter: control userpasswords2.
3. In the User Accounts dialog box, clear the Users must enter a user name and password to use this computer check box, and then click OK.
4. In the Automatically Log On dialog box, enter the Install Capture user's name and password, and then click OK.
5. If you are using an operating system that supports UAC, disable UAC. See http://support.microsoft.com/kb/975787.

Note: For an alternative method of setting up automatic logon, see http://support.microsoft.com/kb/315231. You must use this mechanism for a domain user account.

Verify access to the shared folder

You now need to check that the virtual machine can access the shared folder that you created earlier on the AppDNA machine.

On the virtual machine, type the following into the Windows Start > Run prompt:

```
\\<AppDNA machine name>\AppDNAOutput
```

Where <AppDNA machine name> is the name of the AppDNA machine.

If this opens the shared folder on the AppDNA machine, it verifies that the virtual machine can access it. For troubleshooting tips, see Troubleshooting Access to a Shared Folder from the Virtual Machine.

Install the AppDNA VM Configuration MSI on the virtual machine

To do this, you need the installer (called Citrix AppDNA VM Configuration.msi). This comes with AppDNA. It is copied into a Tools subfolder of the AppDNA installation folder when you

install AppDNA. The default location is C:\Program Files\Citrix\AppDNA\Tools (C:\Program Files (x86)\Citrix\AppDNA\Tools on a 64-bit machine).

1. Install the Citrix AppDNA VM Configuration MSI within the virtual machine, accepting the default file location.
2. Restart the virtual machine.

Important: Ensure that the AppDNA VM Configuration MSI has the same version number as the version of AppDNA that you are using. This means that you need to upgrade the VM Configuration on the virtual machine when you upgrade AppDNA.

Anti-virus configuration on the AppDNA machine

You must configure the anti-virus software on the AppDNA machine to disable on-access scanning of the Install Capture output and input folders. For example, for Norton Anti-Virus, you disable the auto-protect option for the AppDNA output and input folders.

Take a snapshot of the virtual machine

1. Click the red Stop button to shut down the guest operating system within the virtual machine.
2. In the VMware Workstation console, from the VM menu, select Snapshot > Take a Snapshot to create a snapshot of the virtual machine's state.

You are now ready to use the AppDNA Virtual Machine Configuration wizard to set up a virtual machine configuration for use with Install Capture. See Configure a VMware Workstation VM for instructions.

Configure a VMware Workstation VM

August 1, 2018

This topic provides example instructions for using the Virtual Machine Configuration wizard to set up the virtual machine configuration for a VMware Workstation virtual machine. This example assumes that you have already set up the virtual and host machines as explained in Set up a VMware Workstation VM for Install Capture.

1. Start AppDNA.
2. From the menus, choose Edit > Settings.
3. On the left side of the Settings dialog box, click Install Capture.
4. On the Virtual Machines tab, click New and then click Next.

5. In the Virtual machine configuration details step, enter a name and description for the virtual machine configuration, and then select VMware Workstation.
6. In the VMware Workstation virtual machine step, specify the path to the virtual machine's VMX file.
7. In the Virtual machine snapshot step, select the snapshot that you created when you were setting up the virtual machine and then click Next. The virtual machine opens within the console and the wizard performs a series of checks.
8. In the Virtual machine connection step, enter the IP address of the virtual machine. Generally you do not need to change the Remote Admin TCP port.
9. In the Capture Output Location step, select Copy results to network share (faster) and specify the output folder that you created on the AppDNA machine earlier. Make sure you use a UNC path and identify the client or server machine by its host name or IP address – for example, \\AppDNAMachine\AppDNAOutput.
10. In the Virtual machine state step, select Power off and take snapshot (recommended), click Next, and then click Finish.

    The Install Capture page in the Settings dialog box displays the virtual machine configuration.
11. Click Save.

The virtual machine configuration appears in the list of virtual machine configurations on the Install Capture tab in the Import Applications screen.

Execution profiles

August 1, 2018

Execution profiles define the tasks and resources that run on the capture machine during an Install Capture or Self-Provisioning application capture.

Some execution profiles perform more advanced tasks, such as packaging. You can also use execution profiles in Forward Path task scripts to perform actions (such as sequencing or running testing regimes) on applications based on the analysis results.

This topic provides a list of the execution profiles that are installed with AppDNA and explains how to activate them, and how to change the default. This is followed by instructions for running execution profiles, and information about the advanced execution profiles and the Edit Execution Profile dialog box.

Note: Install Capture is always performed on a virtual machine, but a Self-Provisioning capture can be performed on any type of machine (physical or virtual). For convenience, the term capture machine

is used in this section to represent both the Install Capture virtual machine and the Self-Provisioning client machine.

Standard execution profiles

The execution profiles that come with AppDNA as standard are as follows:

- **Snapshot -** Creates an MSI for importing the application's DNA into the AppDNA database. This profile captures all the installation and configuration screens to form the installation instructions.
- **App-V 5.1 Sequencer** – Creates App-V 5.1 sequences as well as an MSI for importing the application's DNA into the AppDNA database – the MSI is not usable as an installer. This execution profile requires the App-V Sequencer 5.1 to be installed on the virtual machine. See App-V 5.1 Sequencer execution profile for more information.
- **App-V 5.0 Sequencer** – Creates App-V 5.0 sequences as well as an MSI for importing the application's DNA into the AppDNA database – the MSI is not usable as an installer. This execution profile requires the App-V Sequencer 5.0 to be installed on the virtual machine.

Note: Both 5.1 and 5.0 execution profiles support 5.0 and 5.1 Sequencer, however the 5.1 Execution profile is recommended because it gives access to all the App-V sequencing features.

To change the default execution profile

1. From the AppDNA menus, choose Edit > Settings.
2. In the side bar in the Settings dialog box, click Install Capture or Self Provisioning, depending on where you want to use the execution profile.
3. Click the Execution Profile tab.
4. Click the execution profile that you want to set as the default, and then click Set as default.
5. Click Save to preserve your changes and close the Settings dialog box.

App-V 5.1 Sequencer execution profile

August 1, 2018

You can use the App-V 5.1 Sequencer execution profile with Install Capture, Self-Provisioning, or Forward Path to package applications for deployment using the App-V Client 5.1.

By default, this execution profile generally installs the application on the capture machine twice – once for sequencing and once outside of the sequencer to capture the application into an MSI for import into AppDNA. You can optionally suppress the second installation. If you do this when running

the execution profile from Install Capture, the generated .appv package is automatically imported. Because the .appv file is prepared for the virtual environment, it does not include all of the application DNA for a native Windows environment. For example, it may omit information about drivers and registry settings. Therefore Citrix recommends the default behavior if you want to analyze the application for a native Windows environment.

Set up the capture machine

To run the App-V 5.1 Sequencer execution profile, perform the following additional setup on the capture machine:

- Ensure that the capture machine has the same operating system and configuration as the client machine on which the App-V application will run.
- Turn off Windows Defender and Windows Search on the capture machine.
- Install Microsoft App-V 5.1 Sequencer on the capture machine.
- Ensure that Windows PowerShell is configured as described below.

For general instructions:

- To set up a virtual machine for Install Capture or Forward Path, see Install Capture.
- To set up a Self-Provisioning capture machine, see Install the Self-Provisioning client.

PowerShell configuration

This execution profile uses Windows PowerShell, which is a pre-requisite of the Microsoft App-V Sequencer 5.1. This execution profile requires PowerShell to be configured with a particular setting. If you install the Citrix AppDNA VM Configuration MSI after PowerShell is installed, the installer will attempt to automatically configure PowerShell for you. If this is not possible or you install PowerShell after you install the AppDNA VM Configuration MSI, configure PowerShell as follows:

1. Open the PowerShell command window.
2. Type in the following and then press RETURN:

```
1 Set-ExecutionPolicy Unrestricted
```

3. Type Yes and then press RETURN.

If you are setting up a virtual machine for Install Capture or Forward Path, you must do this before you create the snapshot of the virtual machine.

One or two installations?

As mentioned earlier, by default this execution profile generally installs the application on the capture machine twice. To suppress the installation outside of the sequencer, give the ImportAppv replaceable a value of True.

By default the execution profile installs the application once only when:

- You run the execution profile from Install Capture and the input file is an MSI, and you select the Load input file check box.
- You run the execution profile from Forward Path, and the SequenceName or App:Name replaceable has been specified, or the input file is an MSI.

Output

The output of running the execution profile is stored in a subfolder within the main output folder defined in the virtual machine configuration (Install Capture and Forward Path) or in the Self-Provisioning client. How the subfolder is named depends on how you run the execution profile – when run through Install Capture or Forward Path, the subfolder's name is derived from the name of the input file and the date and time stamp. When run through Self-Provisioning, the name of the folder is based on the instruction file's identifier.

The execution profile generates the following output:

- An MSI for importing into AppDNA (if the application was installed on the capture machine twice).
- Installation instructions in the form of an HTML page that references images of each installation step.
- An _AppVSequence subfolder that stores the output of the sequencer. You can control the naming of the output files.

The execution profile names the files generated by the sequencer as follows. If more than one of these apply, the highest in the list always take precedence.

1. If the SequenceName replaceable is specified, this is always used.
2. If the input file is derived from Active Directory or ConfigMgr, the App:Name replaceable (which automatically stores the application name) is used.
3. If the input file is an MSI, the MSI product name is used.
4. If the input file is not an MSI, the execution profile attempts to retrieve the application name. If this is not successful, the name of the installation file is used.

Replaceables

The following table provides details of the replaceables that you can use to configure the App-V 5.1 Sequencer execution profile.

Name	Description
ImportAppv	Set this to a value of True if you want to load the generated .appv package into AppDNA rather than capturing a separate MSI specifically for importing into AppDNA. Setting this value to True suppresses the second installation of the application on the capture machine. This is suitable when you have already analyzed the application within AppDNA and now simply want to sequence the application.
MsiSilentSwitch	Use to pass additional options to msiexec for MSI installations (for example, -qb - for silent installs). See http://technet.microsoft.com/library/cc759262(v=ws.10).aspx for information about the msiexec command line options.
LaunchEditor	Set this to True if you want the execution profile to automatically launch the generated .appv package in the App-V Sequencer for editing after the sequencing has finished.
PromptForPrerequisites	Set this to True if you want the execution profile to prompt the user to install any prerequisites before running the sequencer.
WaitForSmbIdle	Specifies the time in seconds to wait for the network share access to cease before completing the task. This is useful to avoid problems caused by a stateful firewall preventing network share access on subsequent tasks.
UseAutoClick	Set this to –use-autoclick if you want the execution profile to run with auto-clicker on by default. Set this to an empty string if you want auto-clicker to be off by default.

The profile contains replaceables prefixed App-V for each of the possible parameters that the PoSh command New-AppVSequencerPackage will accept:

AppV-InstalledFilesPath

AppV-FullLoad (Defalt = False)

AppV-InstallMediaPath

AppV-Installer (Default = IC media path)

AppV-Name (Default = Installer name)

AppV-Path (Default = IC output directory)

AppV-PrimaryVirtualApplicationDirectory

AppV-TemplateFilePath

AppV-AcceleratorFilePath

The profiler will use default values for parameters as above unless otherwise specified at import time.

The profile supports all 3 parameter sets exposed by New-AppVSequencerPackage. It will validate and automatically detect the intended parameter set and will fail if there is a conflict.

ByInstallerFullLoad

AppV-Installer

AppV-Name

AppV-Path

AppV-FullLoad

AppV-PrimaryVirtualApplicationDirectory (Optional – Sequence does not use PVAD if empty)

AppV-TemplateFilePath (Optional)

ByPackageAcceleratorInstallMedia

AppV-Name

AppV-Path

AppV-AcceleratorFilePath (Must Specify)

AppV-InstallMediaPath (Must Specify)

ByPackageAcceleratorInstalledFiles

AppV-Name

AppV-Path

AppV-AcceleratorFilePath (Must Specify)

AppV-InstalledFilesPath (Must Specify)

For more information

- http://technet.microsoft.com/en-us/library/jj713438.aspx

Run an execution profile

August 1, 2018

How you run an execution profile depends on whether you are using Install Capture, Self-Provisioning, or Forward Path. This topic provides instructions for all of these.

To run an execution profile using Install Capture

Note: Install Capture uses a virtual machine configuration to store all of the information that AppDNA requires to connect to and manage the virtual machine.

1. On the Install Capture tab in the Import Applications screen, click Browse, Search, or Import from List on the toolbar to select the .exe or other installation file that you want to import.

   Ensure that you specify the files using a UNC path (such as \\192.168.50.20\Source\application.exe or \\MachineName\Source\application.exe).

2. In the list of applications on the Install Capture tab, select the check box to the left of the application against which you want to run the execution profile.

3. On the toolbar in the Install Capture tab, select the virtual machine configuration that you want to use.

   The virtual machine configuration specifies the details of the virtual machine on which the execution profile will run. This virtual machine must be set up appropriately for the execution profile. For example, the App-V 5.1 Sequencer execution profile requires Microsoft Application Virtualization 5.1 Service Pack 1 to be installed.

4. In the list of applications on the Install Capture tab, click the + to the left of the application name to open the application's options panel. Then in the first drop-down list, select the execution profile that you want to run.
5. On the toolbar in the Install Capture tab, click Import. This starts the Install Capture processing, as defined by the selected execution profile and on the virtual machine specified in the virtual machine configuration. When the capture finishes, the application is automatically imported into AppDNA.

Note: If you have customized execution profiles, customized versions won't be upgraded. The built-in versions of the execution profiles will be upgraded. You may want to consider refreshing your customized profiles. For more information, see Execution Profiles.

To run an execution profile using Self-Provisioning

Self-Provisioning provides a mechanism for the application capture to be driven by an expert end user who does not have access to AppDNA itself. In summary, the procedure is as follows:

1. The administrator uses the Self-Provisioning tab in the main AppDNA Import Applications screen to set up the instructions for the capture.

   During this procedure, the administrator selects the execution profile to be used in a similar way to selecting the execution profile for Install Capture.
2. The administrator arranges for the Self-Provisioning client machine to be set up for the specific execution profile.

   For example, the App-V 5.1 Sequencer execution profile requires Microsoft Application Virtualization 5.1 to be installed.
3. The administrator sends the instructions to the end user who then runs the capture on the Self-Provisioning client machine.

   For more information, refer to Self-Provisioning.

To run an execution profile using Forward Path

Forward Path is controlled by scenario and task scripts. A Forward Path task script can run an execution profile. To do this, call the ProductionManager.RunExecutionProfile function in the task script. This function has the following syntax:

```
Public Shared Sub RunExecutionProfile ( _
    controller As IActionController, _
    profile As ExecutionProfileBuilder, _
    profile_replaceable_values As Dictionary(Of String, String), _
```



```
    vm_config_name As String _
)
```

Parameter	Description
controller	This object is automatically passed into the script when it runs and provides access to information about the current application, for example.
profile	Use to pass the name of the execution profile.
profile_replaceable_values	Use to pass a list of replaceable name and value pairs.
vm_config_name	Use to pass the name of the virtual machine configuration to use.

For example:

```
Dim replaceables As New Dictionary(Of String, String)

' Set the SequenceName replaceable
replaceables.Add("SequenceName", controller.Application.Name)

' Activate auto-clicker
replaceables.Add("UseAutoClick", "--use-autoclick")

ProductionManager.RunExecutionProfile(controller, _
    "App-V 5.1 Sequencer", replaceables, "App-V VM Configuration")
```

See Forward Path for more information.

Edit an execution profile

August 1, 2018

The Self-Provisioning and Install Capture execution profiles differ in that the Self-Provisioning execution profiles store additional text for display to the expert user. In all other respects the two types of execution profiles are the same.

Note: Before you edit an execution profile, Citrix recommends that you create a backup of it. To do this, click

Export in the
Execution Profiles tab in Install Capture or Self-Provisioning Settings.

To configure an execution profile for use in Install Capture, Forward Path Tasks, or Self-Provisioning:

- From the Install Capture Settings page or the Self-Provisioning Settings page: Click New or Edit on the Execution Profiles tab.
- Click the Customize button next to the Execution Profile drop-down list on the Install Capture or Self-Provisioning tab in the Import Applications screen. This edits the execution profile for the current application only.

The Edit Execution Profile dialog box includes the following:

Name – The name of the execution profile. Do not include a colon (:) in the name. This will ensure that the name will not conflict with an internal replaceable defined by Citrix in the future.

Manually execute the commands – This check box controls whether the user must step through the execution of the commands manually.

Commands tab and Replaceables tab – The following sections describe those tabs.

Commands tab

Use the Commands tab in the Edit Execution Profile dialog to view and edit the commands in an execution profile. The top part of the Commands tab lists the execution profile commands in the sequence in which they run. Use the buttons on the right side to add a new command, delete a command, or change the order of the commands.

The lower part of the Commands tab provides detailed information about the command that is selected above. The information is split between the Command and User Interface tabs as follows:

Command tab

The Commands tab shows general information about the command, including the command type, which is either Command Line or Write Unicode File.

The Command Line options are:

- **Command** – This must consist of an executable followed by arguments. It can include placeholders called replaceables that are replaced by a value provided at run time. The syntax for including a replaceable is: $(replaceable_name), where replaceable_name is the name of the replaceable (for example, $(AppToolsFolder)).
- **Wait type** – Defines the command's wait behavior. The options are to continue without waiting, to wait for the process launched by the command to finish, or to wait for a process tree to finish. Typically a command that launches an installation waits for it to finish, whereas a command that launches the screen capture utility continues without waiting.

- **Show window** – Controls how the window launched by the command is to be shown. For descriptions of the possible values, see http://msdn.microsoft.com/en-us/library/windows/desktop/ms633548(v=vs.85).aspx.
- **Fail on unexpected exit code** – Indicates whether the command should fail if the exit code is not as expected. For a command that launches an installer, by default AppDNA considers a non-zero exit code to be a failure. There is an informal convention that installers should return zero for success and a non-zero value for a failure. However, this convention is not followed by all installers. Clear this check box if success or failure is not indicated by the exit code. To set a different exit code, select this check box and then enter the code that indicates success in the Expected exit code box.
- **Expected exit code** – This parameter is ignored unless "Fail on unexpected exit code" is selected. This value is the exit code that indicates success. By default, this is zero.

  Occasionally installers do not return a non-zero exit code when there is a failure. When this happens, by default AppDNA assumes that the capture has succeeded, imports the DNA captured, and marks the import as successful – although in fact no real application DNA was captured at all. In this situation, the captured DNA consists of any minor changes that the failed attempt to install the application made to the underlying operating system. When you know that an installer does not follow the convention of returning a zero exit code on success, use this option to specify the success exit code in the execution profile for that application.
- **Capture output** – Indicates whether the command writes the standard output (stdout) and standard error (stderr) streams into the Install Capture or Forward Path log. This is useful for troubleshooting command line executables that write an error string.

The Write Unicode File options are:

- **Target file path** – The location in which the command creates the file.
- **Expand replaceables in contents** – Specifies whether the command expands replaceables before writing them to the file. When this option is selected, the command replaces anything of the form $(XXX) with the appropriate run-time value before writing it to the file. For example, $(AppToolsFolder) is replaced with its run-time value, such as C:\Program Files\Citrix\AppDNA\VM Configuration. When this option is cleared, the command writes the replaceable to the file as it is; for example, $(AppToolsFolder).

User Interface tab

The options on the User Interface tab control how the command appears to the user when it is run in the stand-alone Self-Provisioning tool.

- **Show as step** – Indicates whether the command is presented to the user as a step.
- **Allow the user to edit the command before execution** – Indicates whether the user can edit the command before running it.

Replaceables tab

Use the Replaceables tab in the Edit Execution Profile dialog box to define replaceable values to be used when the execution profile is run. Any values you enter here override any values entered in the Self-Provisioning page in the Settings dialog box or in the Configure Virtual Machine dialog box.

Note: Sometimes you may want to override a replaceable value entered on this tab for a single application. It is possible to do this for the most commonly used replaceables in the Quick Edit Parameter box in the Import Applications screen.

To specify a replaceable value:

- If the replaceable whose value you want to change is in the list, select it and click Edit. This opens the Edit Replaceable dialog box, in which you can enter or paste the new value.
- If the replaceable whose value you want to define does not appear in the list, click New. This opens the Edit Replaceable dialog box, in which you can enter the new replaceable and its value.

The following list shows replaceables that are used internally. AppDNA automatically sets the values of these replaceables and you do not need to do this manually.

- App:InstallCommand
- App:InstallDriveLetter
- App:InstallWrkDir
- App:Manufacturer (Only used in Forward Path task scripts.)
- App:Name (Only used in Forward Path task scripts.)
- App:Version (Only used in Forward Path task scripts.)
- Capture:ImportInputFile
- Capture:InputFile
- Capture:Mode
- Capture:OutputFile
- Capture:OutputDirectory

Note: These replaceables have a colon (:) in their name. This indicates that this is an internal replaceable defined by Citrix. If you create your own replaceables, make sure that they do not include a colon in the name. This will ensure that the name will not conflict with an internal replaceable provided by Citrix in the future. The part of the name before the colon provides an indication of how the replaceable is used. For example, App indicates that the replaceable provides information about the application that is being processed and Capture indicates that it relates to the current capture state.

Install Capture configuration reference

August 1, 2018

This section provides detailed documentation for managing virtual machine configurations.

Quick links:

- Virtual Machine Configuration Wizard
- Virtual Machine Configuration Dialog Box
- Changing the Remote Admin Port

VM Configuration Wizard

August 1, 2018

You use the Virtual Machine Configuration wizard to create virtual machine configurations for use with:

- **Install Capture** – You use Install Capture to import desktop applications for which an .msi, .sft, or .appv file is not available. Install Capture installs the application within a virtual machine and creates an .msi file which is then imported into AppDNA. Generally the .msi file that is created simply captures the application's DNA for import into AppDNA and is not suitable for actually installing the application. The capture process can create usable MSIs or App-V sequences. This requires the App-V sequencer, which is not provided with AppDNA, to be installed in the virtual machine.
- **Forward Path tasks** – You can use Forward Path tasks to automate the use of Install Capture, typically to sequence or package applications.

Note: For simplicity, this documentation refers only to Install Capture. However, it applies equally to Forward Path tasks that automate the use of Install Capture.

The wizard connects to the underlying virtualization technology and, for example, retrieves a list of the virtual machines that are available. It also attempts to start the virtual machine and optionally open it in the console. This means that you can control the virtual machine and do any necessary setup on it whilst the wizard is open, if necessary. If you complete the wizard steps successfully, the virtual machine configuration should be fully functional.

Pre-requisites

Before you can use this wizard to add a new virtual machine configuration, you need to install a suitable virtualization technology and set up and configure a virtual machine and the AppDNA machine as described in Install Capture.

Open the wizard

1. From the AppDNA menus, choose Edit > Settings.

2. On the left side of the Settings dialog box, click Install Capture.
3. Click the Virtual Machines tab.
4. If you want to create a new virtual machine configuration, click New.
5. If you want to view or edit an existing virtual machine configuration, select it in the list and then click Edit.

Virtual Machine Configuration Details

August 1, 2018

The Virtual Machine Configuration Details step is the second step in the Virtual Machine Configuration Wizard.

Configuration name – Enter a unique name to identify the virtual machine configuration.

Description – (Optional.) Enter additional information about the virtual machine configuration to help identify its purpose.

Virtual machine provider – Select the virtual machine technology that you are using. Provider names that are shown in bold have been detected as installed on your machine. For a list of currently supported providers, see Install Capture.

Note: In certain circumstances some of the providers (in particular Hyper-V, vSphere, and XenServer) may not appear in the list of providers. To resolve this problem, cancel out of the wizard and restart AppDNA.

VMware Workstation Virtual Machine

August 1, 2018

In the VMware Workstation Virtual Machine step in the Virtual Machine Configuration Wizard, you specify the .vmx file that represents the VMware Workstation virtual machine that you want to use for Install Capture.

Path to VMware Workstation .vmx file – Specify the name and location of the VMware Workstation .vmx file. You can click Browse to navigate and select the file. The virtual machine must have at least one snapshot. If the virtual machine does not have any snapshots, you need to use VMware Workstation to create one before you select the .vmx file in this step. See Set up a virtual machine for more information.

Test – Click to confirm that AppDNA can connect to VMware Workstation and open the specified .vmx file. If you do not click this button, the wizard performs this check when you click Next.

VMware Workstation VM Snapshot

August 1, 2018

In the VMware Workstation VM Snapshot step in the Virtual Machine Configuration Wizard, you specify the virtual machine snapshot that you want to use for Install Capture. AppDNA uses this to revert the virtual machine to a clean state before performing the capture.

Virtual machine snapshot – Select the snapshot that you want to use as the base state for the virtual machine during Install Capture. If necessary, you can make changes to the virtual machine while you are using this wizard. A later step in this wizard provides an option to create a new snapshot so that any changes you make to the virtual machine are saved. This new snapshot then replaces the snapshot you select here as the base state for the virtual machine during Install Capture.

Do not display the VM console – Clear this check box (the default) if you want AppDNA to display the VMware Workstation virtual machine console so that you can make changes to the virtual machine while you are using this wizard. Select this check box if you do not want the wizard to display the VMware Workstation console.

Test – Click to confirm that AppDNA is able to control the virtual machine. If successful, AppDNA reverts the virtual machine to the selected snapshot and starts up the virtual machine. If you do not click this button, the wizard performs these steps when you click Next.

Hyper-V Host Details

August 1, 2018

In the Hyper-V Host Details step in the Virtual Machine Configuration Wizard, you enter the details required to connect to the Hyper-V server that hosts the virtual machine that you want to use for Install Capture.

Hostname / IP Address – Type the IP address or DNS name of the Hyper-V host server – for example: 182.31.32.28 or server.domain.com. If Hyper-V is installed on the same machine on which you are running AppDNA, you can enter localhost.

Username – If Hyper-V is installed on a different machine from the one on which you are running AppDNA, type the Hyper-V user name. The user name must include the machine name, using the form

machinename\user. If this is your domain account, enter your domain-qualified user name (for example, domain\user or user@mydomain.com). However, Citrix recommends that you use a dedicated Hyper-V user account whose password is set to never expire rather than your standard domain account. If Hyper-V is installed on the same machine that you are running AppDNA on, leave the user name blank. Your Windows user account will then be used.

This user account (whether explicitly specified or not) must be part of the Administrators or Hyper-V Administrators group on the Hyper-V server. Alternatively, the user must have been granted explicit Hyper-V permissions to control virtual machines. For information about how to do this, see MSDN.

Password – If you entered a user name, type the account password.

Important: If this password changes in the future, you will need to run this wizard again to enter the new password.

Test – Click to confirm that AppDNA can connect to the specified Hyper-V host server. If you do not click this button, the wizard performs this check when you click Next.

Hyper-V Virtual Machine

August 1, 2018

In the Hyper-V Virtual Machine step in the Virtual Machine Configuration Wizard, you select the Hyper-V virtual machine that you want to use for Install Capture.

Virtual machine – The wizard lists the virtual machines that are available on the Hyper-V host server specified in the previous step. Select the virtual machine that you want to use. This should be a dedicated virtual machine for use with Install Capture run from this AppDNA client. Run AppDNA as an administrator.

Configure AppDNA to run as administrator

1. If necessary, close AppDNA.
2. In Windows Explorer, locate the main AppDNA executable (called appTitude.exe). The table below shows the default location of this file.
3. Right-click the file and from the shortcut menu, choose Properties.
4. Click the Compatibility tab.
5. Under Privilege level, select the Run this program as an administrator check box.
6. Click OK to save the changes.

Machine type	Default location
64-bit	C:\Program Files\Citrix\AppDNA\Client

Hyper-V Snapshot Selection

August 1, 2018

In the Hyper-V Snapshot Selection step in the Virtual Machine Configuration Wizard, you select the Hyper-V virtual machine snapshot that you want to use.

Snapshot – Select the virtual machine snapshot that you want to use as the base snapshot for Install Capture. If necessary, you can make changes to the virtual machine while you are using this wizard. A later step in this wizard provides an option to create a new snapshot so that any changes you make to the virtual machine are saved. This new snapshot then replaces the snapshot you select here as the base state for the virtual machine during Install Capture.

Create – If the virtual machine does not have any snapshots, click this button to create a snapshot based on the current state of the virtual machine.

Do not display the VM console – Clear this check box (the default) if you want AppDNA to display the virtual machine in a console so that you can make changes to the virtual machine while you are using this wizard. Select this check box if you do not want the wizard to display the virtual machine in a console.

Test – Click to confirm that AppDNA is able to control the virtual machine. If successful, AppDNA reverts the virtual machine to the selected snapshot, starts up the virtual machine and, depending on the option selected, displays it in the console. If you do not click this button, the wizard performs these steps when you click Next.

The Hyper-V virtual machine console

The console displays the virtual machine. Use the options at the top of the console window as follows:

- **Always on top** – Select this check box (the default) to keep the console window on top of all the other windows that you have open. Clear this check box if you want to bring other windows in front of the console window. This is useful if you have a small screen.
- **Reconnect** – Click to reconnect with the virtual machine after restarting it.

To send the CTRL+ALT+DELETE key press combination to the virtual machine, press CTRL+ALT+END.

vSphere Host Details

August 1, 2018

In the vSphere Host Details step in the Virtual Machine Configuration Wizard, you enter the details required to connect to the vSphere host server that you want to use for Install Capture.

Hostname / IP Address – Type the IP address or DNS name of the vSphere host server (this is the vSphere ESXi Hypervisor server, not the VMware vCenter server) – for example, 182.31.32.28 or server.domain.com.

Username – Type the user name for a local user account on the ESXi. Citrix recommends that you use a dedicated vSphere user account whose password is set to never expire rather than your standard domain account. For instructions on creating the account, refer to "Create a local user account on the host (hypervisor)" below.

At a minimum, the user account requires permissions to power the virtual machine on and off, to reset and suspend the virtual machine, and to create and revert a snapshot. For instructions for assigning these privileges to a vSphere user account, see "Assign privileges to a vSphere user account" below.

Password – Type the account password.

Important: If the password changes in the future, you will need to run this wizard again to enter the new password.

Test – Click to confirm that AppDNA can connect to the specified vSphere host server. If you do not click this button, the wizard performs this check when you click Next.

Create a local user account on the host (hypervisor)

1. Log on to the VMware vSphere Client using an administrative user account and enter the IP address of the hypervisor host (not the vCenter server).
2. Go to Home > Inventory.
3. Select the host and then click the Local Users And Groups tab.
4. Right-click in the window and then choose Add.
5. Enter the requested details and then click OK.

Assign privileges to a vSphere user account

An administrator can assign privileges to the vSphere user account as follows:

1. Log on to VMware vSphere Client using an administrative user account.
2. Go to Home > Administration > Roles.

3. Right-click in the window and then choose Add.
4. Enter a name for the role, such as Install Capture user, and select the following privileges:
    - Virtual machine > Interaction > Power Off
    - Virtual machine > Interaction > Power On
    - Virtual machine > Interaction > Reset
    - Virtual machine > Interaction > Suspend
    - Virtual machine > State > Create snapshot
    - Virtual machine > State > Revert to snapshot
5. Click OK.
6. Go to Home > Inventory.
7. On the Permissions tab, right-click and then choose Add Permission.
8. In the Assign Permissions dialog box, click Add.
9. In the Select Users and Groups dialog box, select the user to which you want to assign the permissions, and then click Add.
10. Click OK. This returns you to the Assign Permissions dialog box, where the user now appears on the left side.
11. In the drop-down box on the right side of the Assign Permissions dialog box, select the role you created earlier.
12. Click OK.

vSphere Virtual Machine

August 1, 2018

In the vSphere Virtual Machine step in the Virtual Machine Configuration Wizard, you select the vSphere virtual machine that you want to use for Install Capture.

Virtual machine – The wizard lists the virtual machines that are available on the vSphere host server specified in the previous step. Select the virtual machine that you want to use. This should be a dedicated virtual machine for use with Install Capture run from this AppDNA client.

vSphere Snapshot Selection

August 1, 2018

In the vSphere Snapshot Selection step in the Virtual Machine Configuration Wizard, you select the vSphere virtual machine snapshot that you want to use.

Snapshot – Select the virtual machine snapshot that you want to use as the base snapshot for Install Capture. If necessary, you can make changes to the virtual machine while you are using this wizard. A later step in this wizard provides an option to create a new snapshot so that any changes you make to the virtual machine are saved. This new snapshot then replaces the snapshot you select here as the base state for the virtual machine during Install Capture.

Create – If the virtual machine does not have any snapshots, click this button to create a snapshot based on the current state of the virtual machine.

Do not display the VM console – Clear this check box (the default) if you want AppDNA to display the virtual machine in a console so that you can make changes to the virtual machine while you are using this wizard. Select this check box if you do not want the wizard to display the virtual machine in a console.

Test – Click to confirm that AppDNA is able to control the virtual machine. If successful, AppDNA reverts the virtual machine to the selected snapshot, starts up the virtual machine and, depending on the option selected, displays it in the console. If you do not click this button, the wizard performs these steps when you click Next.

The vSphere virtual machine console

The console displays the virtual machine. Use the options at the top of the console window as follows:

- **Always on top** – Select this check box (the default) to keep the console window on top of all the other windows that you have open. Clear this check box if you want to bring other windows in front of the console window. This is useful if you have a small screen.
- **Reconnect** – Click to reconnect with the virtual machine after restarting it.

To send the Ctrl-Alt-Delete key press combination to the virtual machine, press Ctrl-Alt-End.

XenServer Host Details

August 1, 2018

In the XenServer Host Details step in the Virtual Machine Configuration Wizard, you enter the details required to connect to the XenServer host server that you want to use for Install Capture.

Hostname / IP Address – Type the IP address or DNS name of the XenServer host server – for example: 182.31.32.28 or server.domain.com.

Username – Type the XenServer user name. If this is your domain account, enter your domain-qualified user name (for example, domain\user or user@domain.com). However, Citrix recommends

that you use a dedicated XenServer user account whose password is set to never expire rather than your standard domain account.

This user account must have VM advanced operations permissions on the XenServer. Typically this means that the user account must have at least the VM power admin role.

Password – Type the account password.

Important: If the password changes in the future, you will need to run this wizard again to enter the new password.

Test – Click to confirm that AppDNA can connect to the specified XenServer host server. If you do not click this button, the wizard performs this check when you click Next.

Snapshot Selection

August 1, 2018

In the Snapshot Selection step in the Virtual Machine Configuration Wizard, you select the XenServer virtual machine snapshot that you want to use.

Snapshot – Select the virtual machine snapshot that you want to use as the base snapshot for Install Capture. If necessary, you can make changes to the virtual machine while you are using this wizard. A later step in this wizard provides an option to create a new snapshot so that any changes you make to the virtual machine are saved. This new snapshot then replaces the snapshot you select here as the base state for the virtual machine during Install Capture.

Create – If the virtual machine does not have any snapshots, click this button to create a snapshot based on the current state of the virtual machine.

Do not display the VM console – Clear this check box (the default) if you want AppDNA to display the virtual machine in a console so that you can make changes to the virtual machine while you are using this wizard. Select this check box if you do not want the wizard to display the virtual machine in a console.

Test – Click to confirm that AppDNA is able to control the virtual machine. If successful, AppDNA reverts the virtual machine to the selected snapshot and starts up the virtual machine and, depending on the option selected, displays it in the console. If you do not click this button, the wizard performs these steps when you click Next.

The XenServer virtual machine console

The console displays the virtual machine. Use the options at the top of the console window as follows:

- **Fit to window** – Select this check box to fit the virtual machine to the console window.
- **Always on top** – Select this check box (the default) to keep the console window on top of all the other windows that you have open. Clear this check box if you want to bring other windows in front of the console window. This is useful if you have a small screen.
- **Ctrl-Alt-Delete** – Click to send the Ctrl-Alt-Delete key press combination to the virtual machine (there is no other way of sending this key combination to the virtual machine).
- **Reconnect** – Click to reconnect with the virtual machine after restarting it.

XenServer Virtual Machine

August 1, 2018

In the XenServer Virtual Machine step in the Virtual Machine Configuration Wizard, you select the XenServer virtual machine that you want to use for Install Capture. The AppDNA client that is running the Install Capture must have exclusive use of the virtual machine.

Virtual machine – The wizard lists the virtual machines that are available on the XenServer host server specified in the previous step. Select the virtual machine that you want to use. This should be a dedicated virtual machine for use with Install Capture run from this AppDNA client.

Virtual Machine Connection

August 1, 2018

In the Virtual Machine Connection step in the Virtual Machine Configuration Wizard, you specify the connection details that AppDNA needs in order to communicate with the virtual machine.

Guest operating system IP address or machine name – Enter the IP address or host name of the guest OS. If the guest OS is connected to the domain, enter the fully qualified domain name. (This includes the domain suffix, such as mymachine.domain.net.) Depending on the virtualization technology that you are using, the wizard attempts to extract the host name and displays it for you. If the wizard is successful in this, Citrix recommends that you use the host name that is displayed.

AppDNA uses the IP address or host name to make a network connection with the guest OS during Install Capture. If you specify the IP address and it subsequently changes, you will need to run this wizard again to save the new value (otherwise Install Capture will fail). Citrix therefore recommends that wherever possible, you use the fully qualified domain name or configure the guest OS with a static IP address.

Note: See “Find out the IP address of the virtual machine” below for information about to find out the IP address.

Remote Admin TCP port – The port that Remote Admin listens on within the virtual machine. The default port is 54593. Generally you do not need to change this. However, in some circumstances you may need to use a different port – for example, if you are unable to allow the default port through the virtual machine’s firewall. For instructions on how to change the port that Remote Admin listens on, see Changing the Remote Admin Port.

Note: Remote Admin is an AppDNA agent that runs within the virtual machine during operations that take place on a virtual machine. Remote Admin provides support for AppDNA to communicate with the virtual machine.

Test – Click to confirm that AppDNA is able to connect to Remote Admin within the virtual machine.

Find out the IP address of the virtual machine

On the virtual machine, open a command prompt and enter the following:

```
ipconfig
```

This displays the TCP/IP network configuration values, including the IP address. If both IPv6 and IPv4 addresses are present, use the IPv4 address.

Ping the virtual machine

To do this, open a command prompt on the AppDNA machine and type the following:

```
ping <Virtual Machine ID>
```

Where <Virtual Machine ID> is the IP address, or machine or DNS name of the guest OS. This should match what you have entered in the wizard page.

If AppDNA can communicate with the virtual machine, you will see ping replies, such as:

```
Reply from 192.168.50.21: bytes=32 time<1ms TTL=128
```

Capture Output Location

August 1, 2018

In the Capture Output Location step in the Virtual Machine Configuration Wizard, you specify where you want the Install Capture output (such as MSI files and screen shots of the installation) to be stored. There are two different ways that the output can be handled and which option you choose determines the requirements for the output location.

Stream results (simple) – In this option, the output is streamed from the virtual machine to a folder on the host machine or a network share after the capture is complete. Because the virtual machine does not require access to this folder, this option is easier to set up than the Copy results to network share option. However, Install Capture takes longer. In addition, if the capture does not complete for any reason, the results up to the point of failure are lost. This option is therefore **not** recommended if you plan to run batches of captures unattended (for example, using auto-clicker).

- **Store results in** – Specify the location in which you want the output files that are streamed from the virtual machine to be stored. AppDNA requires read-write access to this folder but the virtual machine does not need to access it.

Note: During the capture process itself the results are stored temporarily in a folder on the virtual machine. By default, this is C:\AppDNA, but if necessary, you can change this in the Virtual Machine Configuration dialog box after you have completed creating the virtual machine configuration in this wizard.

Copy results to network share (faster) – This option copies the results from the virtual machine to a folder on the host machine or a network share to which both AppDNA and the virtual machine have read and write access. Use this option if you may want to run batches of captures unattended (for example, using auto-clicker).

- **Network share** – Specify where you want the virtual machine to copy the output files to. This must be a location to which both the host machine and the virtual machine have read-write access. For example, a local path such as c:\temp\appdna will not work. Typically you use a UNC path of the form \\server\share\path. However, you can use a mapped network drive, provided that the same drive letter is mapped to the same location on both the AppDNA machine and the virtual machine.

Test – Click to check that both AppDNA and the virtual machine can access the location you have specified.

VMware Workstation Virtual Machine State

August 1, 2018

In the VMware Workstation Virtual Machine State step in the Virtual Machine Configuration Wizard, you specify the state in which you want the wizard to leave the virtual machine when you finish working

through the wizard steps. If you choose one of the options to take a snapshot, the option you select also controls the state to which AppDNA reverts the virtual machine at the start of each Install Capture.

The options are:

- **Power off and take snapshot (recommended)** – If you choose this option, the wizard powers off the virtual machine and takes a snapshot of its state when you click Finish on the last page of the wizard. This new snapshot replaces the snapshot you selected earlier as the snapshot to be used for Install Capture. In addition, this option means that AppDNA restarts the virtual machine at the start of each Install Capture. For example, if you use Install Capture to import five applications, AppDNA restarts the virtual machine five times (once at the start of each capture). Although slower than the next option (which suspends the virtual machine before taking the snapshot), Citrix recommends this option because it ensures that the virtual machine is in a clean state at the start of every Install Capture.
- **Suspend and take snapshot** – If you choose this option, the wizard suspends the virtual machine and takes a snapshot of its state when you click Finish on the last page of the wizard. This new snapshot replaces the snapshot you selected earlier as the snapshot to be used for Install Capture. In addition, this option means that AppDNA starts the virtual machine from a suspended state at the start of each Install Capture. This generally reduces the startup time but may be less reliable than restarting from the powered off state.
- **Revert to snapshot** – If you choose this option, when you click Finish on the last page of the wizard, the wizard discards any changes made to the virtual machine and reverts it to the snapshot you selected earlier. Choose this option if you are running through the wizard to check an existing configuration or to change the output location, for example.
- **Leave running, I will stop it myself** – If you choose this option, when you click Finish on the last page of the wizard, the wizard leaves the virtual machine running and you need to shut it down yourself before you attempt to run an Install Capture. If you have made any changes to the virtual machine while using this wizard and you want to save those changes and use them in Install Capture, you need to take a snapshot of the new state. You then need to run through this wizard again and select the new snapshot on the VMware Workstation VM Snapshot page.

Virtual Machine State (Hyper-V)

August 1, 2018

In the Virtual Machine State step for Hyper-V in the Virtual Machine Configuration Wizard, you specify the state in which you want the wizard to leave the Hyper-V virtual machine when you finish working through the wizard steps. If you choose one of the options to take a snapshot, the option you select also controls the state to which AppDNA reverts the virtual machine at the start of each Install Capture.

The options are:

- **Power off the VM and take a snapshot (recommended)** – If you choose this option, the wizard powers off the virtual machine and takes a snapshot of its state. This option means that AppDNA restarts the virtual machine at the start of each Install Capture. For example, if you use Install Capture to import five applications, AppDNA restarts the virtual machine five times (once at the start of each capture). Although slower than the "Suspend the VM and take a snapshot" option, Citrix recommends this option because it ensures that the virtual machine is in a clean state at the start of every Install Capture.
- **Revert to snapshot** – If you choose this option, the wizard discards any changes made to the virtual machine while working through the wizard and reverts the virtual machine to the existing snapshot. Choose this option if you are running through the wizard to check an existing configuration or to change the output location, for example.
- **Leave running, I will stop it myself** – If you choose this option, the wizard leaves the virtual machine running. You then need to shut the virtual machine down yourself before you attempt to run an Install Capture.
- **Suspend the VM and take a snapshot** – If you choose this option, the wizard suspends the virtual machine and takes a snapshot of the its state. This option means that AppDNA starts the virtual machine from a suspended state at the start of each Install Capture. This generally reduces the startup time but may be less reliable than restarting from the powered off state.
- **Take a snapshot of the VM and leave it running** – If you choose this option, the wizard takes a snapshot of the virtual machine and leaves it running. You then need to shut the virtual machine down yourself before you attempt to run an Install Capture.

Virtual Machine State (vSphere)

August 1, 2018

In the Virtual Machine State step for vSphere in the Virtual Machine Configuration Wizard, you specify the state in which you want the wizard to leave the vSphere virtual machine when you finish working through the wizard steps. If you choose one of the options to take a snapshot, the option you select also controls the state to which AppDNA reverts the virtual machine at the start of each Install Capture.

The options are:

- **Power off the VM and take a snapshot (recommended)** – If you choose this option, the wizard powers off the virtual machine and takes a snapshot of its state. This option means that AppDNA restarts the virtual machine at the start of each Install Capture. For example, if you use Install Capture to import five applications, AppDNA restarts the virtual machine five times (once at the start of each capture). Although slower than the "Suspend the VM and take a snapshot" option,

Citrix recommends this option because it ensures that the virtual machine is in a clean state at the start of every Install Capture.

- **Revert to snapshot** – If you choose this option, the wizard discards any changes made to the virtual machine while working through the wizard and reverts the virtual machine to the existing snapshot. Choose this option if you are running through the wizard to check an existing configuration or to change the output location, for example.
- **Leave running, I will stop it myself** – If you choose this option, the wizard leaves the virtual machine running. You then need to shut the virtual machine down yourself before you attempt to run an Install Capture.
- **Suspend the VM and take a snapshot** – If you choose this option, the wizard suspends the virtual machine and takes a snapshot of the its state. This option means that AppDNA starts the virtual machine from a suspended state at the start of each Install Capture. This generally reduces the startup time but may be less reliable than restarting from the powered off state.
- **Take a snapshot of the VM and leave it running** – If you choose this option, the wizard takes a snapshot of the virtual machine and leaves it running. You then need to shut the virtual machine down yourself before you attempt to run an Install Capture.

Virtual Machine State (XenServer)

August 1, 2018

In the Virtual Machine State step in the Virtual Machine Configuration Wizard, you specify the state in which you want the wizard to leave the XenServer virtual machine when you finish working through the wizard steps. If you choose one of the options to take a snapshot, the option you select also controls the state to which AppDNA reverts the virtual machine at the start of each Install Capture.

The options are:

- **Power off and take snapshot (recommended)** – If you choose this option, the wizard powers off the virtual machine and takes a snapshot of its state. This option means that AppDNA restarts the virtual machine at the start of each Install Capture. For example, if you use Install Capture to import five applications, AppDNA restarts the virtual machine five times (once at the start of each capture). Although slower than the next option (which suspends the virtual machine before taking the snapshot), Citrix recommends this option because it ensures that the virtual machine is in a clean state at the start of every Install Capture.
- **Suspend and take snapshot** – If you choose this option, the wizard suspends the virtual machine state and takes a snapshot of its state. This option means that AppDNA starts the virtual machine from a suspended state at the start of each Install Capture. This generally reduces the startup time but may be less reliable than restarting from the powered off state.

- **Revert to snapshot** – If you choose this option, the wizard discards any changes made to the virtual machine while working through the wizard and reverts the virtual machine to the existing snapshot. Choose this option if you are running through the wizard to check an existing configuration or to change the output location, for example.
- **Leave running, I will stop it myself** – If you choose this option, the wizard leaves the virtual machine running. You then need to shut the virtual machine down yourself before you attempt to run an Install Capture.

Virtual Machine Configuration Summary

August 1, 2018

This page provides a summary of the configuration options and settings you have chosen in the Virtual Machine Configuration wizard.

After viewing the summary, you may decide you want to make some adjustments to the configuration. How you do this depends on which virtualization technology you are using.

- If the Back button is enabled, you can click it to go back to the relevant step. After making any changes, you then need to click Next on each step until you return to this summary screen in order to complete the configuration.
- If the Back button is not enabled, click Finish to close the wizard. Then click Save to save your changes and close the Settings dialog box. If necessary, you can then open the Settings dialog box again and edit the virtual machine configuration.

Click Finish to exit the wizard, and then click Save in the Settings dialog box. When you go into the Import Applications screen, you will then see the new virtual machine configuration in the Virtual Machines drop-down list on the Install Capture tab.

VM Configuration Dialog Box

August 1, 2018

The Virtual Machine Configuration dialog box is a feature for advanced users to edit virtual machine configurations for use with Install Capture or Forward Path Tasks. Open the Configure Virtual Machine dialog box by clicking Advanced in Install Capture Settings.

Note: Unless you have advanced knowledge of this area, it is recommended that you edit virtual machine configurations by using the Virtual Machine Configuration wizard.

The Configure Virtual Machine dialog box has a number of tabs:

- Virtual Machine Settings
- Remote Admin
- Replaceables
- Optional Configuration
- Provider Plugin (only for some providers)

These are documented under separate headings below. The options vary according to the provider you select on the first tab.

Virtual Machine Settings tab

Use the Virtual Machine Settings tab in the Virtual Machine Configuration dialog box to view and define basic settings for the virtual machine configuration.

Name. This identifies the virtual machine configuration. The name must be unique within the list of configurations.

Description. Provide an informative description to help identify the purpose of the configuration in the future.

Provider. This shows the virtual machine technology that is in use for this configuration. The options in the drop-down list correspond to the supported technologies listed in Install Capture. Citrix recommends that you do not change the provider here. If you want to change the provider, it is better to create a new configuration for that provider in the normal way.

Output Location. The location in which the Install Capture output (MSI files, screen shots of the installation, etc.) is stored. How this folder must be configured depends on whether the Stream VM Output check box is selected:

- When the Stream VM Output check box is selected, this is a folder on the host machine or a network share. The virtual machine does not require access to this folder, but AppDNA does.
- When the Stream VM Output check box is cleared, this must be a location to which both the host machine and the virtual machine have read and write access. The location can be a mapped network drive or a full UNC path, such as \\AppDNAMachine\AppDNAOutput.

Note: Sometimes the capture output files may require a deep folder structure that can exceed the maximum Windows path length of 260 characters. To overcome this limitation, you can specify a UNC path in the form \\?\UNC\server\share.

Stream VM Output. Select this option if you want Install Capture to stream the output from the virtual machine back to a folder on the host machine or a network share after the capture is complete. This is easier to set up than writing the output to a folder that both the virtual machine and AppDNA can access. However, it is slower. Clear this check box if you want Install Capture to copy the results from the virtual machine to a folder on the host machine or a network share to which both AppDNA and the virtual machine have read and write access.

VM Output Staging Location. When the Stream VM Output check box is selected, this specifies the folder on the virtual machine in which Install Capture temporarily stores the output before streaming it back to the Output Location folder on the host machine or network share. You cannot use the \\?\UNC\ long path notation for this setting.

VM Identifier (Name). (Not relevant for VM Provider Plugins.) The unique name given to the virtual machine when it was created. For a VMware Workstation virtual machine, this is the full path to the VMX file – for example, C:\Virtual Machines\VVMXPSP3-01\VVMXPSP3-01.vmx.

Action Timeout. (Not relevant for VM Provider Plugins.) Specifies the time-out period in seconds for the control of the virtual machine, such as locating it, starting it up and reverting it to a snapshot. The time these actions take depends on the virtualization technology and the size of the virtual machine images. The default is 1,200 seconds.

"Installation Needs Input" Timeout. The period in seconds for which Install Capture should wait for an installation (or any other execution profile command) to complete. When a command does not complete within this time, AppDNA displays a message indicating that you should look at the running virtual machine to see if input is needed. This is useful when trying to do many Install Captures with silent install commands, and one unexpectedly waits for input. The default is 1,200 seconds.

"Abort Installation" Timeout. The period in seconds that Install Capture should wait when there is no activity before ending an installation and continuing to the next one. The default is 2,400 seconds (40 minutes). This is deliberately a long period because some large applications take a considerable amount of time to install. If you are using auto-clicker and leaving batches of captures to run overnight (for example), you may want to reduce this time-out period to speed up progress through the batch if some captures fail. However, this may cause the capture of some large applications to fail. You may therefore want to reduce the period to 1,200 seconds (for example) if you are using auto-clicker and set it back to the default value before doing any manual captures.

Base Snapshot Path. (VMware Workstation only.) This defines the snapshot within the virtual machine that is to be used as the base state of the virtual machine for each Install Capture process. In VMware Workstation, snapshots can form a tree and you specify the path to the snapshot you want to use like this: Snapshot1\InstallCaptureBaselineSnapshot.

Remote Admin tab

Use the Remote Admin tab in the Virtual Machine Configuration dialog box to define how AppDNA communicates with Remote Admin, which is an AppDNA agent that runs within the virtual machine.

VM Guest Machine Name. The IP address or machine name of the virtual machine. AppDNA uses this to make a network connection with the guest OS. Do not include backslashes (\).

VM Control using. The protocol that AppDNA uses to connect with Remote Admin within the virtual

machine. The default is TCP. The Named Pipe protocol is deprecated and is supported only for configurations created in previous versions of AppDNA.

Named Pipe Username. The user name for the named pipe, when the Named Pipe protocol is in use. Specify the fully qualified account name of a user. This should have the form VM_MACHINE_NAME\USERNAME for a local administrator account and DOMAIN_NAME\USERNAME for a domain account that can log into the virtual machine. If you leave this value blank, set the local security policy on the virtual machine to allow anonymous access for named pipes.

Named Pipe Password. The password for the named pipe, when the Named Pipe protocol is in use and a named pipe user account is specified above.

TCP Port. The port that Remote Admin listens on. The default is 54593. You can change the port by running Remote Admin (remoteadmin.exe) with the parameter -tcp_port=<port>, where <port> is the new port. For information about changing the port that Remote Admin listens on, see Changing the Remote Admin Port.

Troubleshoot Errors. Select this check box if you want AppDNA to open a troubleshooting user interface if particular errors are encountered while performing an Install Capture. You can use the troubleshooting user interface to connect to Remote Admin, run commands, and perform other troubleshooting steps within the virtual machine. Then when you perform the "Finished" action, AppDNA ends the Install Capture, closes the troubleshooting interface, and moves on to the next Install Capture, if there is one. Errors that relate to connecting to Remote Admin and running the Install Capture commands trigger the troubleshooting interface. Clear this check box for the default behavior.

Replaceables tab

Use the Replaceables tab in the Virtual Machine Configuration dialog box to define replaceable values to be used in the execution profiles that are run on this virtual machine configuration. However, the replaceable values you define here are overridden if values are explicitly defined for those replaceables in the execution profile itself or in the Quick Edit Parameter box in the Import Applications screen.

Replaceables are placeholders that are replaced by a value provided at run time. The syntax for including a replaceable in the execution profile is: $(replaceable_name), where replaceable_name is the name of the replaceable.

The AppToolsFolder replaceable is used to specify the location of the tools installed on the virtual machine by the Citrix AppDNA VM Configuration MSI. By default, these are installed to C:\Program Files\Citrix\AppDNA\VM Configuration. The default value for the AppToolsFolder replaceable uses the %APPDNAVMCONFIG% environment variable, which is created by the AppDNA VM Configuration MSI and stores the actual installed location of the tools.

To define a replaceable value for this virtual machine configuration:

- If the replaceable whose value you want to change for this virtual machine is in the list, select it and click Edit. This opens the Edit Text dialog box, where you can enter or paste the new value.
- If the replaceable whose value you want to define does not appear in the list, click New. This opens the Edit Replaceable dialog box, where you can enter the new replaceable and its value.

There are a number of replaceables that are used internally in the execution profiles. AppDNA automatically sets the values of these replaceables and you do not need to do this manually. For a full list of these, see Edit an execution profile.

Optional Configuration tab

Use the Optional Configuration tab in the Virtual Machine Configuration dialog box to view and define Install Capture settings for the virtual machine configuration.

VM Cleanup Action. Defines how Install Capture leaves the virtual machine after completing an Install Capture process. The option you select here affects the capture times. The options are: Suspend, Leave Running and Power Off. Note that Install Capture always reverts the virtual machine to its original state before each capture, regardless which option you select here.

Provider Plugin tab

Use the Provider Plugin tab in the Virtual Machine Configuration dialog box to view and define settings for providers that are based on a plugin, such as the XenServer and vSphere providers. This tab appears only for plugin-based providers.

Provider Assembly Path. The path to the VM provider plugin's assembly.

Provider Code Type. The class in the VM provider plugin's assembly that interacts with the virtual machine technology.

Use Remoting. Some VM provider plugins provide support for remoting even when the underlying technology does not. Select this check box to tell the provider to communicate with the remote provider implementation. Note that the listener on the remote machine must be running and listening.

Remote Provider Machine Address. The hostname or IP address of the machine hosting the remote provider implementation. This is relevant only when the Use Remoting check box is selected.

TCP Port. The TCP port that the remote provider implementation is listening on. This is relevant only when the Use Remoting check box is selected.

Configuration Settings. Use this section to define any other settings that are required. These settings have the form of a name and value pair.

- To define a new configuration setting, click New. This opens the Edit Value dialog box. Enter the name of the setting and its value and then click OK.
- To edit an existing configuration setting, select it in the list and click Edit. This opens the Edit Value dialog box, where you can edit the existing value.

The Hyper-V plugin settings are as follows:

- hostname - The IP address or DNS name of the Hyper-V host server.
- username - The user name of the account that AppDNA uses to access Hyper-V. This is stored in an encrypted form if you entered it through the Virtual Machine Configuration Wizard. If you enter the user name here, it is not encrypted.
- password - The password of the account that AppDNA uses to access Hyper-V. This is stored in an encrypted form if you entered it through the Virtual Machine Configuration wizard. If you enter the password here, it is not encrypted.
- virtualmachine - The name of the Hyper-V virtual machine to be used for Install Capture.
- snapshot - The internal identifier of the snapshot to be used for Install Capture.
- vmaddress - The machine or DNS name or the IP address of the guest OS.
- vmstate - The option chosen in the Hyper-V Virtual Machine State step in the Virtual Machine Configuration wizard.

The vSphere plugin settings are as follows:

- hostname - The IP address or DNS name of the vSphere host server.
- username - The user name of the account that AppDNA uses to access vSphere. This is stored in an encrypted form if you entered it through the Virtual Machine Configuration Wizard. If you enter the user name here, it is not encrypted.
- password - The password of the account that AppDNA uses to access vSphere. This is stored in an encrypted form if you entered it through the Virtual Machine Configuration wizard. If you enter the password here, it is not encrypted.
- virtualmachine - The name of the vSphere virtual machine to be used for Install Capture.
- snapshot - The name of the snapshot to be used for Install Capture.
- vmstate - The option chosen in the vSphere Virtual Machine State step in the Virtual Machine Configuration wizard.

The XenServer plugin settings are as follows:

- hostname - The IP address or DNS name of the XenServer host server.
- username - The user name of the account that AppDNA uses to access the XenServer. This is stored in an encrypted form if you entered it through the Virtual Machine Configuration Wizard. If you enter the user name here, it is not encrypted.
- password - The password of the account that AppDNA uses to access the XenServer. This is stored in an encrypted form if you entered it through the Virtual Machine Configuration wizard. If you enter the password here, it is not encrypted.
- virtualmachine - The name of the XenServer virtual machine to be used for Install Capture.

- vmstate - The option chosen in the XenServer Virtual Machine State step in the Virtual Machine Configuration wizard.

Changing the Remote Admin Port

August 2, 2018

Remote Admin is an AppDNA agent that runs within the virtual machine during Install Capture. Remote Admin is automatically installed within the virtual machine when you install the Citrix AppDNA VM Configuration MSI. The MSI configures Remote Admin to start automatically when the virtual machine powers up and to listen for connections from the AppDNA client on port 54593.

The port can be changed by launching RemoteAdmin.exe from the command line in the virtual machine and including the following parameter:

```
-tcp_port=port
```

Where port is the new port.

This needs to be done each time Remote Admin is launched. What this means in practice depends on the state of the virtual machine to which Install Capture reverts the virtual machine at the start of each Install Capture. This state is determined by the state of the virtual machine when you create the snapshot that Install Capture uses. To help you understand how this works, some background information follows.

For each Install Capture, AppDNA does the following:

1. Connects with the virtual machine provider and reverts the virtual machine to the snapshot specified in the virtual machine configuration. The state of the virtual machine when the snapshot was taken controls the state to which AppDNA reverts the virtual machine.
2. Uses Remote Admin to run the capture tasks within the virtual machine.
3. Suspends the virtual machine (or shuts it down or leaves it running). (Suspension is the default action. To change this, use the VM Cleanup Action option in the Virtual Machine Configuration Dialog Box.)

How Remote Admin is launched depends on the state of the virtual machine when AppDNA reverts to it in step 1:

- **Running** – If the guest OS is running and the user logged on, Remote Admin is already running and it is not launched again.
- **Powered off** – If the virtual machine is powered off, once the virtual machine powers on Remote Admin is started up using the command stored in the following registry key in the virtual machine: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.

Therefore how you configure Remote Admin to use a different port depends on the state of the virtual machine when the Install Capture snapshot is taken. Step-by-step instructions are provided below for each option.

How you create a snapshot depends on the virtualization technology you are using. However, for all of the technologies, the final step in the Virtual Machine Configuration Wizard provides options to create a snapshot in either a suspended or powered off state. You can therefore perform the following steps in the virtual machine as you work through the wizard.

To change the Remote Admin port for a suspended state snapshot

Follow these instructions before you suspend the virtual machine and create the snapshot to which Install Capture will revert the virtual machine.

1. On the virtual machine open the Windows Task Manager.
2. On the Applications tab in Task Manager, click RemoteAdmin and then click End Task.
3. Open a command prompt and type the following:

   ```
   "location\RemoteAdmin.exe"-tcp_port=port
   ```

   Where location is the location of RemoteAdmin.exe. By default this is C:\Program Files\Citrix\AppDNA\VM Configuration on a 32-bit virtual machine (C:\Program Files (x86)\Citrix\AppDNA\VM Configuration on a 64-bit virtual machine) and port is the new port number.

This starts Remote Admin and configures it to use the new port number. You can now suspend the virtual machine and create the snapshot.

To change the Remote Admin port for a powered off state snapshot

Follow these instructions before you power off the virtual machine and create the snapshot to which Install Capture will revert the virtual machine.

1. On the virtual machine, click Start > Run.
2. Type Regedit, and then click OK.
3. In the Registry Editor, browse to the following location:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
   ```

4. In the right pane, double-click RemoteAdmin.exe.
5. In the Edit String dialog box, add the following after the existing value:

   ```
   -tcp_port=port
   ```

   Where port is the new port number. (Ensure there is a space before -tcp_port.)

6. Click OK and then close the Registry Editor.

This configures the virtual machine to use the new port number when Remote Admin starts up. You can now power off the virtual machine and create the snapshot.

Operating system images

August 1, 2018

AppDNA comes with a set of default OS images that you can use. However, importing your own images enables AppDNA to base its analysis on the images used in your environment.

You can import more than one image for an OS family, such as Windows Server 2012 or Windows 10. Storing more than one image is useful when your organization has two (or more) standard corporate builds of the OS – one for laptops and one for desktops, for example. When more than one OS image has been imported into AppDNA for an OS, you can choose which of those images to use when you view a report. For an overview of how OS images are used in AppDNA, see Operating systems.

Use the following general steps to import an OS image:

1. To open the Operating Systems screen, choose Import & Analyze > Operating Systems.

   The Operating Systems screen lists all of the OS images that have already been imported.

2. To import a new OS, click Download Snapshot Manager. Use Snapshot Manager to create an MSI based on the clean corporate image or a clean virtual machine. For more information, see Create an MSI for your OS image.

3. After Snapshot Manager creates an MSI file, click Import from MSI. For more information, see Import an OS image.

4. To configure the relationships between your OS images, click OS Image Relationships. For more information, see Configure OS image relationships

   You must configure each OS image to define its relationships with any other OS images with which you want it compared. For example, suppose you are preparing for a Windows 10 migration and you import your standard corporate desktop and laptop OS images for both Windows 10 and Windows 7. You need to set the relationship between the Windows 10 and Windows 7 desktop images and between the Windows 10 and Windows 7 laptop images. You can do this as you import each image. Alternatively, you can set the relationships of all the images after you have imported them.

   Note: After importing multiple OS images, you can define which one is the default for each report in
   Edit > Settings > OS Image Configuration.

Create an MSI for your OS image

August 1, 2018

This section describes how to create a snapshot MSI of your OS image so you can then import it into AppDNA.

Note: Snapshot Manager uses the %SYSTEMDRIVE% environment variable to detect the drive where the OS is installed.

1. From the AppDNA side bar, choose Import & Analyze > Operating Systems.
2. On the toolbar in the Operating Systems screen, click Download Snapshot Manager.
3. Save SnapshotManager.exe to a suitable location.
4. If necessary, copy SnapshotManager.exe to the machine whose OS image you want to capture.
5. In Windows Explorer, right-click SnapshotManager.exe and choose Run as administrator.
6. Select the location to store the output files and click OK.

   This opens a command prompt and starts the creation of the OS image MSI. Depending on the OS and the size of the build, the process can take anywhere from 30 minutes to around 2 hours to complete.
7. When the creation of the MSI is complete, a dialog box opens showing the name and location of the MSI snapshot file. Click OK to close the dialog.
8. If necessary, copy the following files to the machine where AppDNA is installed:

   <os_image_name>.msi
   <os_image_name>.msi.xml
   <os_image_name>.msi_predumper.xml
   <os_image_name>.msi_predumper_output.xml

You can now import the OS image into AppDNA, as described in Import an OS image.

Import an OS image

August 2, 2018

1. From the side bar, choose Import & Analyze > Operating Systems.
2. On the toolbar in the Operating Systems screen, click Import from MSI and then complete the following tasks:
   - OS image details

- Image relationships
- OS image import results

OS image details

1. Enter the following details:

   Location of MSI file. Specify the OS image MSI that you want to import. The OS image MSI must be located in the same folder as the three XML files that are also generated by Snapshot Manager:

   <os_image_name>.msi
   <os_image_name>.msi.xml
   <os_image_name>.msi_predumper.xml
   <os_image_name>.msi_predumper_output.xml

   Create new image. Select this option to create a new OS image within AppDNA (the default). Then enter the name and description:

   - **OS image name.** Enter a name that will enable users to identify the OS image within AppDNA. Citrix recommends that the name includes the name of the OS family and any other essential identifying information. For example, “Windows 10 - standard laptop image”.
   - **OS image description.** Enter additional information that further explains the purpose of this OS image.

   Overwrite existing image. Select this option to overwrite an existing OS image within AppDNA, and then select the OS image that you want to overwrite. This option is available only for OS images that you have imported. You cannot overwrite the system OS images (the OS images that come with AppDNA).

2. When you have finished entering the image information, click Next to move to the next step.

Image relationships

1. On the left side, under Are you moving, select one of the following options:

   To this operating system image. Select this option if the new OS image represents an OS (such as Windows 8.1) to which you are preparing to migrate. The right side of the screen then lists the available legacy OS images.

   From this operating system image. Select this option if the new OS image represents an OS that you are migrating from. The right side of the screen then lists the available target OS images.

2. On the right side of the screen, select the OS image(s) that you want AppDNA to compare with the OS image you are configuring. Deselect any OS images that are not relevant.

   For best results, select only those images that are relevant to the analysis that you want to perform.

   When you import the first image in a pair, you cannot select the other one because it has not been imported yet. You can therefore leave this section blank and configure the image later in the Operating Systems screen.

3. Click Next to start the import of the OS image.

Example

Suppose you are migrating from Windows 7 to Windows 10 and want to import desktop and laptop images for both Windows 7 and Windows 10.

- When you import and configure the Windows 7 laptop image, select From this operating system image and then select the Windows 10 laptop image as the target image.
- When you configure the Windows 10 laptop image, select To this operating system image and then select the Windows 7 laptop image as the legacy image.

After that, perform the equivalent steps for the desktop images. When you run the analysis for the Windows 10 report, AppDNA compares the changes between the Windows 7 and Windows 10 laptop images and between the Windows 7 and Windows 10 desktop images. To view the reports, choose whether to view the report for the laptop images or the desktop images.

This example describes setting up OS image relationships in which there is a one-to-one relationship between the images. However, this is not a requirement. For example, you could import one legacy OS image and four target OS images and configure all four of the target OS images with the single legacy OS image.

OS image import results

When the import is complete, AppDNA shows the results and which reports require re-analyzing in order for the new OS image to be reflected in reports.

1. If you want to start the analysis now, click Analyze.
2. If you want to import further OS images before running an analysis, click Previous to return to the Operating Systems screen. You can then run the analysis later in the normal way.

Configure OS image relationships

August 1, 2018

1. From the AppDNA side bar, choose Import & Analyze > Operating Systems.
2. In the list of OS images in the Operating Systems screen, select the OS image that you want to configure.
3. On the toolbar, click OS Image Relationships.
4. On the left side, under Are you moving, select one of the following options:

   To this operating system image. Select this option if the new OS image represents an OS (such as Windows 10) to which you are preparing to migrate. The right side of the screen then lists the available legacy OS images.

   From this operating system image. Select this option if the new OS image represents an OS that you are migrating from. The right side of the screen then lists the available target OS images.
5. On the right side of the screen, select the OS image(s) that you want AppDNA to compare with the OS image you are configuring. Deselect any OS images that are not relevant.

   For best results, select only those images that are relevant to the analysis that you want to perform.
6. Click Save on the toolbar to preserve your changes.

   Depending on the changes you have made to the configurations, you may now need to analyze your applications in order for the changes to be reflected in reports. If this is necessary, the Analyze button on the far right side of the toolbar is enabled. If necessary, click Analyze to analyze the applications. Alternatively, you can analyze the applications later in the normal way.

Example

Suppose you are migrating from Windows 7 to Windows 10 and want to import desktop and laptop images for both Windows 7 and Windows 10.

- When you import and configure the Windows 7 laptop image, select From this operating system image and then select the Windows 10 laptop image as the target image.
- When you configure the Windows 10 laptop image, select To this operating system image and then select the Windows 7 laptop image as the legacy image.

After that, perform the equivalent steps for the desktop images. When you run the analysis for the Windows 10 report, AppDNA compares the changes between the Windows 7 and Windows 10 laptop

images and between the Windows 7 and Windows 10 desktop images. To view the reports, choose whether to view the report for the laptop images or the desktop images.

This example describes setting up OS image relationships in which there is a one-to-one relationship between the images. However, this is not a requirement. For example, you could import one legacy OS image and four target OS images and configure all four of the target OS images with the single legacy OS image.

Delete an OS image

August 1, 2018

You can delete OS images that have been imported through the Operating Systems screen, but you cannot delete the OS images that come with AppDNA (these are called system images).

If there is only one OS image for an OS family that is relevant for the reports included with your license, do not delete it.

1. From the AppDNA side bar, choose Import & Analyze > Operating Systems.
2. In the list of OS images in the Operating Systems screen, select the OS image that you want to delete.
3. On the toolbar, click Delete Image.

If the OS image was set as a default OS image for a report in OS image configuration settings, AppDNA automatically resets that default. If images for the relevant OS family have been imported, AppDNA sets the most recent one as the default. If there are no imported images for the OS family, AppDNA uses the system image. If necessary, change this in Edit > Settings > OS Image Configuration.

OS image settings

August 1, 2018

The Settings dialog box contains general AppDNA options. To open this dialog box, choose Edit > Settings from the menus.

Use the OS Image Configuration page to specify default OS images for reports. The page lists reports that have algorithms that analyze the application DNA against OS images from one or more OS family. For example, the Windows 10 report analyzes the application DNA against the previous OS (such as Windows 7) as well as against Windows 10.

If multiple OS images are available for an OS family, you need to specify which one is the default for associated reports. The default images are used by Effort Calculator, the Overview Summary report, and the Report Export wizard, and they are selected by default for relevant reports.

For each report, specify the OS image(s) that you want to use as the default. Then click Save to preserve your changes.

The OS images that are available for selection in the drop-down boxes in this dialog box depend on the report and how you have configured it. For example, suppose you configured the Windows 10 report by specifying that your legacy Windows platform is Windows 7. For the Windows 10 report, you would then be able to choose between the available Windows 7 images in the Prior OS Image drop-down box and the available Windows 10 images in the Target OS Image drop-down box. If only one OS image is available, you do not need to make a choice.

The text No OS algorithms active for this report means that the algorithms that analyze the application DNA against an OS image have been turned off for this report – for example, in the Algorithm Groups screen.

Notes:

- If your edition supports custom reports, AppDNA automatically adds entries to this dialog box for any custom reports that include one or more OS image-dependent algorithm.
- Reports that are turned off are not shown.
- You can delete your own OS images in the Operating Systems screen. If you delete an OS image that was set as a default image for a report, AppDNA resets that default to the last image that was imported for that OS family. If necessary, you can change this in this dialog box.

Modules, reports, and algorithms

August 1, 2018

This section describes how to perform advanced configuration that impacts an analysis and its results.

A module is a collection of reports for a particular context, such as Windows client or server. A report is made up of a suite of algorithms that relate to a target technology, such as Windows 8, against which the application DNA is evaluated. The algorithms are organized into algorithm groups.

To configure AppDNA modules:

- From the menus, choose **Configure** > **Modules** > **Management**.

The Module Management screen lists the reports. AppDNA shows a logo for each report. This helps identify the technology when you view reports.

- To control which modules are shown: Use the **Filter Modules** drop-down list on the right-side of the toolbar to select an option.
- To turn reports on and off: Use the **Enabled** check box. Turning off reports that are not relevant reduces unnecessary processing time. After you change the settings, click Save. If you turn a report on, you must analyze your applications before you can view the results.
- To drill down into the algorithms used in a report: Click **View Module**. You can view the algorithm version history, turn algorithms and algorithm groups on and off, set custom RAGs, and customize algorithm remediation actions.
- To download an XML representation of all of the modules and any customizations: Click **Export**. This is useful if you want to provide a module template for use in other AppDNA databases.
- To load a module template that has been previously exported: Click **Import**.

Note: If you are working in an environment where multiple clients are connected to the same database, any changes you make in this screen will affect all of the users.

Configure modules wizard

August 1, 2018

You use the Configure Modules wizard to configure AppDNA to meet the needs of your enterprise. Each module provides a collection of reports for a particular context. For example, the Desktop Compatibility Manager module contains the Windows 7 and Windows 8.1/8 reports. The reports indicate whether your applications will have any compatibility issues on a particular platform or technology.

Depending on the number of applications involved, analysis is a time and resource-consuming process and it creates report data that is stored in the database. This wizard therefore walks through the key modules and asks you to specify what projects your enterprise is currently working on and some related details. The wizard then activates and customizes the reports that are relevant and turns off the reports and algorithms that are not relevant to your current projects. This makes analysis faster, means that the reports do not identify issues that are not relevant to your environment, and stops your database from storing irrelevant data.

The wizard also creates a Forward Path scenario (called “My Enterprise Selections”) tailored for your projects. You can use this to run a Forward Path report that shows the red, amber, and green (RAG) status of each application for the projects you are working on. For example, if you specify that you are working on Windows 8 and Windows Server 2012 R2 migration projects, and an App-V virtualization project, the Forward Path report has columns that show the RAG status of applications for Windows 8, Windows Server 2012 R2, and App-V. You can use this scenario as a template when creating your own scenarios.

AppDNA automatically runs this wizard when an administrator first logs into AppDNA after installing

AppDNA or connecting to a new database. You can return to this wizard at any time to change your selections. If your changes then result in an additional report being activated, you need to analyze your applications for that report before you can view the results. Similarly, if your changes activate additional algorithms in a report that is already active, you need to analyze your applications again for that report.

To open the Configure Modules wizard:

- From the menus, choose Configure > Modules > Wizard.

Note:

- The changes you make in this wizard affect the entire AppDNA database and therefore all of the users who use the database.
- After running this wizard, you can refine the configuration of the reports further – for example, to turn off algorithms that test for compatibility with optional features that are not relevant to your environment. See Configure algorithms for more information.

Desktop compatibility

This step configures AppDNA for Windows desktop migration projects.

My enterprise is working on a Windows desktop migration project - Select this option if you are planning or working on a Windows desktop migration project, and then select the following:

- **From** - Select the operating system (OS) you are migrating from (you can select more than one). This is referred to as the legacy OS.

  Some of the report algorithms test applications for dependencies on features that are in the legacy OS but not the target OS. The wizard activates the algorithms of this type that relate to the legacy versions of Windows that you select here and deactivates the others. These algorithms are in the “Obsolete components” algorithm group.

- **To** - Select one or more of the following:
  - **Windows 7** - Select this option if you are moving to Windows 7. This activates the Windows 7 report.
  - **Windows 8/8.1** - Select this option if you want to test your applications for compatibility with Windows 8 or 8.1. This activates the Window 8/8.1 report.
  - **Windows 10** - Select this option if you want to test your applications for compatibility with Windows 10. This activates the Windows 10 report.

- **We use English versions of Windows only** - Clear this check box if you use other non-English language versions of Windows, whether fully localized or Multilingual user interface (MUI). (See below for information on these terms.)

My enterprise is not working on a Windows desktop migration project at this time - Select this option if you do not need information about Windows desktop migration.

Desktop language compatibility

Note: This step appears only if you clear the
We use English versions of Windows only check box in the Desktop compatibility step.

Microsoft provides two approaches to handling Windows language versions:

- **Fully localized** - In this approach, folder, file, and object names are translated at the New Technology File System (NTFS) level and the in-built user accounts are also translated. In addition, elements such as menus and dialog boxes in the user interface are fully translated.
- **Multilingual user interface (MUI)** - In this approach, language packs are installed on top of the English or language-neutral version of Windows. This provides a fully translated user interface, but does not translate folder, file, object, or in-built account names.

The Windows 7 and Windows 8 reports include algorithms that test applications for dependencies on French and German localized versions of Windows, which may present issues if they are run on an English or other localized version - or when moving from a fully localized to an MUI approach.

From - Select the language handling approach that you are moving from.

To - Select the language handling approach to which you are moving.

The wizard configures the algorithms in the “Globalization issues” algorithm group based on your selections in this section.

Server compatibility

This step configures AppDNA for Windows server migration projects.

My enterprise is working on a Windows server migration project - Select this option if you are planning or working on a Windows server migration project, and then select the following options:

- **From** - Select the OS you are migrating from (you can select more than one).

  Some of the report algorithms test applications for features that are contained in the legacy but not the target OS. The wizard activates the algorithms of this type that relate to the legacy versions of Windows that you select here and deactivates the others. These algorithms are in the “Obsolete components” algorithm group.

- **To** - Select one or more of the following:

  – **Windows Server 2008 R2** - Select this option if you are moving to Windows Server 2008 R2. This activates the Windows Server 2008 R2 report

  - **Windows Server 2012/2012 R2** - Select this option if you want to use the Window Server 2012 report to test your applications for Windows 2012. This activates the Windows 2012 report.
  - **Windows Server 2016** - Select this option if you want to use the Window Server 2016 report to test your applications for Windows 2016. This activates the Windows 2016 report.

- **Report for a Server Core build** - Select this check box if you want to test your applications for a Server Core deployment. Server Core provides a minimal environment that has limited functionality but typically requires lower maintenance. This option activates algorithms that detect applications that may have issues if they are run on a Server Core build - for example, because they interact with graphical features that are not available.

My enterprise is not working on a Windows server migration project at this time - Select this option if you do not need information about a Windows server migration project.

Application virtualization

Note: This step appears only if you are licensed for the Virtualization feature (App-V compatibility analysis).

This step configures AppDNA for App-V application virtualization projects.

My enterprise is working on an application virtualization project – Select this option if you are planning or working on an application virtualization project. Then select the version of App-V for which you want to test your applications. AppDNA turns off algorithms that are not relevant to the version of App-V that you select.

My enterprise is not working on an application virtualization project at this time – Select this option if you do not need information about an application virtualization project.

Virtualization platform

Note: This step appears only if you selected an application virtualization technology in the previous step but did not choose a desktop or server platform in an earlier step.

Select the Windows platform(s) for which you want to assess App-V.

Web browser

This step configures AppDNA to test Web applications for compatibility with Firefox, Internet Explorer, and Citrix Secure Web, in any combination.

My enterprise is working on adopting new Web browsers - Select this option if you are want to test Web applications for compatibility with Firefox, Internet Explorer, or Secure Web. Then select the browsers for which you want to test your Web applications.

Note: Because Firefox is a standards-based browser and variations between versions tend to be minor, AppDNA does not prompt you to specify a Firefox version.

My enterprise is not working on adopting new Web browsers at this time - Select this option if you do not want to test your Web applications.

XenApp hosted

Note: This step appears only if you are licensed for the SBC feature.

This step configures AppDNA to check applications for suitability for XenApp hosted in the data center, which presents the application on the user's device and relays user actions, such as keystrokes and mouse actions, back to the application in the data center. Potentially many users can use each application simultaneously. This poses a particular set of challenges.

Important: When you are moving to a XenDesktop environment from another system, we recommend that you use the XenDesktop Adoption solution instead of the XenApp Hosted report. The XenDesktop Adoption solution provides a more complete picture of application compatibility with XenDesktop based on your current environment. The XenApp Hosted report only indicates if an application that already runs on a server platform will work with XenApp.

My enterprise is working on a XenApp hosted project - Select this option if you are planning or working on a XenApp hosted project. Then select the version of XenApp for which you want to test your applications.

My enterprise is not working on a XenApp hosted project at this time - Select this option if you do not need information about a XenApp hosted project.

Click Configure to the save your changes and configure the modules.

Configure algorithm groups

August 2, 2018

You can view the algorithm groups and algorithms that make up an AppDNA report, view the algorithm version history, turn algorithms and algorithm groups on and off, set custom RAGs, change the remediation actions for specific algorithms, and add new remediation actions by using the Algorithm Groups screen.

The Algorithm Groups screen has two views – List View and Detail View. Use the options on the toolbar to swap between the two views. The List View lists the algorithm groups with the algorithms they contain nested inside. Click Expand Collapse on the toolbar to show and hide the algorithms. When the algorithms are hidden, you can show the algorithms in a particular group by clicking the + to the left of the group's name.

After you make changes in this screen, you need to click Save on the toolbar to preserve your changes. Click Export to download an XML representation of all of the algorithms and algorithm groups for the current report and any customizations that you have made to the custom RAGs and in terms of turning algorithms on and off. This is useful if you want to provide a report template to other AppDNA installations. Click Import to load a template that has been previously exported.

Note: After you turn an algorithm or algorithm group on or off, you need to re-analyze your applications so that the changes are reflected in reports. Re-analysis is not required if you only change the custom RAGs or customize actions.

To open the Algorithm Groups screen:

Either:

1. From the AppDNA menus, choose Configure > Modules > Management.
2. On the Module Management screen, find the report whose algorithms you want to view or customize, and click the View Module button under the report logo.

Or:

- From the AppDNA menus, choose Configure > Modules > Module > Report Name, where Module and Report Name identify the report whose algorithms you want to view or customize.

Custom RAGs

Each algorithm has a custom RAG. Initially this is the same as the standard RAG that is built into the algorithm. However, sometimes you may want to raise an amber status to red or lower it to green, for example, depending on the specific needs of your organization. You can do this by using the drop-down list in the Custom RAG column.

Algorithm	Description	RAG	Custom RAG	Action	Action Detail	Complexity	Action RAG
W7_DRV_001	Unsigned driver identified	G	G Green	No Remediation	No Remediation required	Easy	G
W7_DRV_002	Signed driver identified by	G	G Green	No Remediation	No Remediation required	Easy	G
W7_DRV_003	Display driver that	R	R Red	Redevelopment R	The application needs to be redevelop	Hard	R
W7_DRV_004	Drivers designed for legacy	A	A Amber	Additional Testin	Driver Compatibility Test Required.	Hard	A
W7_DRV_007	Kernel-mode print driver	R	R Red	Redevelopment R	The application needs to be redevelop	Hard	R
W7_DRV_008	Driver that depends on	A	A Amber	Additional Testin	Driver Component requires further test	Hard	A

Actions

For each algorithm, AppDNA has a default remediation action. However, you can change this by using the drop-down list in the Action column. Each action has:

- An action detail, which provides more remediation information.
- An effort complexity indicator, which indicates how difficult the remediation is to carry out. The possible values are Easy, Medium, and Hard.
- An action RAG, which indicates what the application's RAG status will be after the remediation action has been implemented.

For example, consider an algorithm that has an red custom RAG. If the remediation action can easily correct the identified issues, its action RAG is green. However, if the only remediation option is to redevelop the application or to consider it an exception, its action RAG is red. The action RAG therefore enables you to quickly identify the applications that can be fixed in-house with a medium to low level of effort, and those that require more complex development or replacement.

As mentioned above, each action has one or more action details defined. You can refine the remediation actions by using the drop-down list in the Action Detail column. You can see which is the suggested action detail for the issue identified by the algorithm, because it is marked with a gray check mark in the Sug column in the drop-down list. This does not change if you select another action detail.

If the default actions and action details that are supplied do not meet the exact needs of your project, it is possible to create custom remediation actions. See Add a remediation action for more information.

When you have finished customizing the actions, click Save on the toolbar to preserve your changes.

Example

The Windows 7 algorithm, OBS7_MISSING_001, identifies applications that are dependent on a file that is not provided by the target OS image or any of the other applications in the portfolio. As a result, the application may fail or not work correctly on Windows 7.

There are a few solutions available to address this issue depending on what is desired in the environment. The standard RAG for this algorithm is amber and the default action is to package the missing file with the application. The action RAG is green, which indicates that after you have performed the action, the issue is likely to be resolved. However, you could also resolve this issue by installing the missing file on the OS build, or deploying the file with the application using App-V. If you prefer to take one of these approaches, you could change the default action accordingly. If you feel that none of these actions is appropriate, and you actually think the application should be redeveloped or replaced, you could change the action to "Redevelopment required" and the custom RAG to red. The "Redevelopment required" has a red action RAG, to indicate that complex development and/or replacement is required. The following table shows these actions along with their action details and action RAGs, and the suggested custom RAG setting.

Action	Action Detail	Custom RAG	Action RAG
Package	Provide the missing resource	Amber	Green
Change OS	Add redistributable to the OS	Amber	Green
Application virtualization	Deploy the application using a virtualization technology, such as App-V	Amber	Green
Redevelopment required	The application needs to be redeveloped to solve this issue	Red	Red

See Configure algorithms

Configure algorithms

August 1, 2018

The initial configuration you perform using the Configure Modules wizard provides global settings for algorithms and algorithm groups. This topic describes how to customize algorithms, RAG status, and remediation actions.

Turn algorithms and algorithm groups on and off

Turning off algorithms and algorithm groups that are not relevant reduces unnecessary processing and focuses the report results on your actual needs. For example, some of the reports test for compatibility with features that are optional. If your enterprise does not use (or plan to use) any of the optional features, you can turn off the associated algorithms to speed analysis.

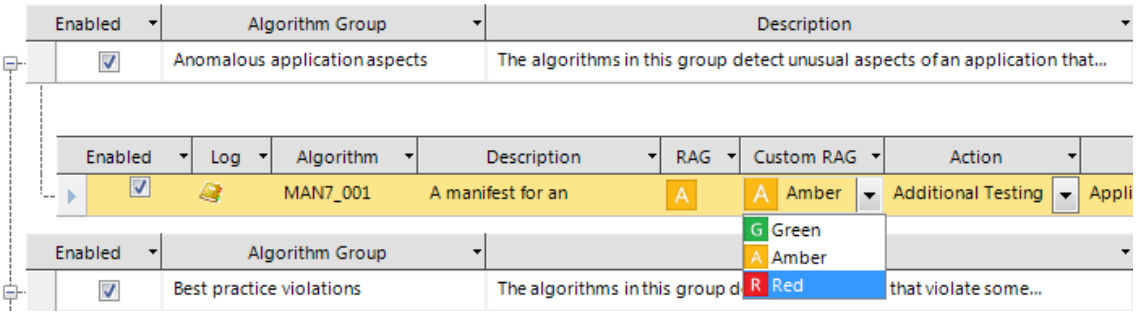
1. From the AppDNA menus, choose Configure > Modules > Module > Report, where Module and Report identify the report whose algorithms you want to turn on or off.
2. In the Algorithm Groups screen, locate the algorithm group or algorithm that you want to turn on or off.
3. Clear or select the Enabled check box to turn the algorithm group or algorithm off or on.

4. Click Save on the toolbar to preserve your changes.
5. Re-analyze your applications so that the changes are reflected in reports.

Set custom RAGs

The standard RAG status of an application is determined by the algorithms built into the report. However, sometimes you might want to raise an amber status to red or lower it to green, depending on the specific needs of your organization. By default, the custom RAG is the same as the standard RAG.

1. From the AppDNA menus, choose Configure > Modules > Module > Report, where Module and Report identify the report that contains the algorithm whose custom RAGs you want to set.
2. In the Algorithm Groups screen, click List View on the toolbar.
3. Locate the algorithm whose custom RAG you want to set.
4. In the Custom RAG column, select the new value.

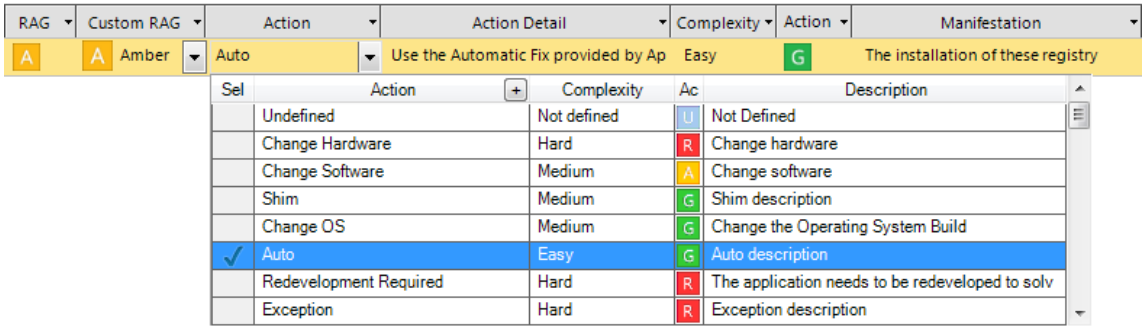


5. Click Save on the toolbar to preserve your changes.

Change remediation actions

Just as sometimes you may want to customize the RAGs, you may sometimes also want to customize an algorithm's remediation actions – for example, to require additional testing.

1. From the AppDNA menus, choose Configure > Modules > Module > Report, where Module and Report identify the report that contains the algorithm whose action you want to change.
2. In the Algorithm Groups screen, click List View on the toolbar.
3. Locate the algorithm whose remediation actions you want to customize.
4. From the drop-down list in the Action column, select the action you require.

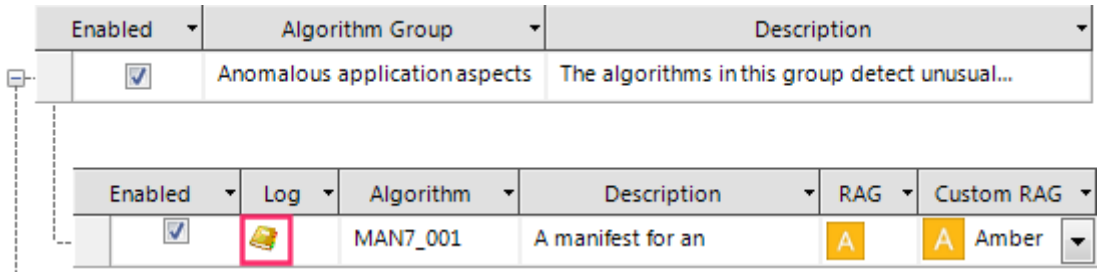


5. Depending on the action, you may need to customize the action detail. To do this, from the drop-down list in the Action Detail column, select the action detail you require.
6. Click Save on the toolbar to preserve your changes.

Notice that changing the remediation action sometimes automatically changes the action RAG (also known as the remediation RAG). The action RAG provides an indication of the application's RAG status after the remediation action has been implemented.

View the algorithm version history

1. From the AppDNA menus, choose Configure > Modules > Module > Report, where Module and Report identify the report that contains the algorithm.
2. In the Algorithm Groups screen, click List View on the toolbar.
3. Locate the algorithm whose version history you want to view.
4. Click the icon in the Log column.



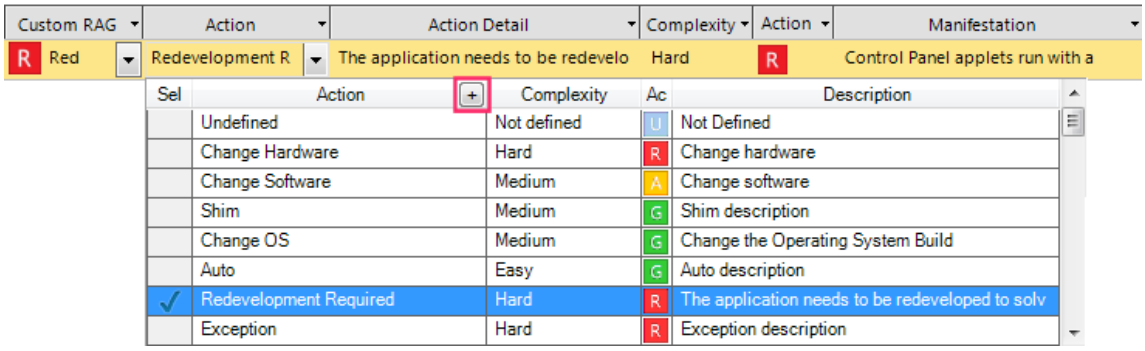
The Algorithm Version History displays the algorithm's version history, including whether it was installed by the latest upgrade to AppDNA and whether it has been used in an analysis.

Add a remediation action

August 1, 2018

Each algorithm has an associated remediation action, which defines the type of remediation that is required to fix the issue that the algorithm identifies. You can change the action associated with algorithms in the Algorithm Groups screen. However, sometimes if the default actions and action details that are supplied do not meet the exact needs of your project, it is possible to create custom remediation actions.

1. From the AppDNA menus, choose Configure > Modules > Module > Report, where Module and Report identify the report.
2. In the Algorithm Groups screen, click Change to List View on the toolbar.
3. Locate the algorithm for which you want to add the new action, and click the down arrow in the Action column.



4. In the drop-down box, click the + button on the right of the Action column header.
5. In the Assign Actions to Algorithms dialog box, click the blue + button to the right of the Action Name.
6. In the Add Action dialog box, enter a name and description for the new action, set the effort complexity of the action, and the action RAG.

   The name must follow these rules:

   - The first character must be a Latin letter (a through z, A through Z).
   - Subsequent characters can be Latin letters or numbers (digits 0 through 9).
   - The name must not be a SQL Server reserved word. For the full list of these, see http://msdn.microsoft.com/en-us/library/aa238507(SQL.80).aspx.
   - The name can contain spaces and a maximum of 40 characters.

7. Click OK to close the Add Action dialog box.
8. Before you can use your new action, you need to create at least one action detail: In the Assign Actions to Algorithms dialog box, click the blue + sign to the right of the Action Detail.
9. In the Add Action Detail dialog box, fill out the details and click OK.

   The name must follow the same rules as listed above.

10. In the tree view in the Assign Actions to Algorithms dialog box, select the check boxes next to the modules, reports and algorithms with which you want to associate the new action.
11. Click OK to close the dialog box.
12. Click Save on the toolbar.

Export and import algorithms

August 1, 2018

The export feature in the Algorithm Groups screen exports all of the algorithms and algorithm groups for the current report and includes any customizations that you have made to the custom RAGs and in terms of turning algorithms on and off. It does not include any customizations that you have made to the actions. However, the Export customizations screen provides an option to export action customizations.

To export an XML template of all of the algorithms and algorithm groups in the current report

1. From the AppDNA menus, choose Configure > Modules > Module > Report, where Module and Report identify the report whose algorithms you want to export.
2. On the toolbar in the Algorithm Groups screen, click Export.
3. In the Save As dialog box, enter a name and appropriate location for the exported file.
4. Click OK.

To import an XML template

1. From the AppDNA menus, choose Configure > Modules > Module > Report, where Module and Report identify the report whose algorithms you want to import.
2. On the toolbar in the Algorithm Groups screen, click Import.
3. In the Open dialog box, navigate to the file that was previously exported.
4. Click OK.

Export customizations

August 1, 2018

Use the Action Administration screen to export customizations made to remediation actions and action details in the Algorithm Groups screen and variables you have defined in the Effort Calculator. The export is stored as an XML file that can later be imported.

Note: This export does not export any modifications that you have made to the custom RAGs or in terms of turning algorithms on or off. You can export these through the Algorithm Groups screen. See Export and import algorithms for more information.

To export action settings

1. From the AppDNA menus, choose Administration > Action Administration.
2. In the Action Administration screen, select the report whose actions you want to export.
3. On the toolbar, click Export Action Settings.
4. Give the file a name and save it in an appropriate location.
5. Click OK.

To import action settings

1. From the AppDNA menus, choose Administration > Action Administration.
2. On the toolbar in the Action Administration screen, click Import Action Settings.
3. Navigate to the file that was previously exported.
4. Click OK.

Standard remediation actions

August 3, 2018

Standard actions

The following table provides a list of the standard remediation actions that are built into AppDNA. Each action has one or more associated action details. You can change the action and action detail that is associated with an algorithm and you can also add your own custom actions and action details, as described in Add a remediation action.

Action	Effort	Action RAG	Description
Additional testing required	Hard	Amber	Additional testing is required
Additional XenApp testing required	Medium	Green	Additional XenApp testing required
Application virtualization	Easy	Green	Deploy using an application virtualization technology.
App-V 5.0	Easy	Green	Use App-V 5.0
App-V Management Console modifications	Easy	Green	Modifications are required in the App-v Management Console
Auto	Easy	Green	Use an automatic fix
Change GPO	Easy	Green	Change Group Policy
Change hardware	Hard	Red	Change hardware
Change OS	Medium	Green	Change operating system build
Change software	Medium	Amber	Change software
Desktop virtualization	Easy	Green	Deploy using a desktop virtualization technology
Edit OSD file	Easy	Green	The OSD file requires editing
Exception	Hard	Red	Remediation is not possible (the application may need to be redeveloped or decommissioned)
Firefox in-house redevelopment required	Medium	Green	The Web application needs to be redeveloped to solve this issue

Action	Effort	Action RAG	Description
Firefox redevelopment required	Hard	Red	The Web application needs to be redeveloped to solve this issue
Firefox remediations	Easy	Green	Firefox remediations are required to get Web pages to work as expected
IE infrastructure changes	Medium	Amber	Environment infrastructure changes are required
IE in-house redevelopment required	Medium	Green	The web application needs to be redeveloped to solve this issue
IE redevelopment required	Hard	Red	The application needs to be redeveloped
IE remediations	Easy	Green	Remediation to get web pages to work as expected
No remediation required	Easy	Green	No remediation is required
Redevelopment required	Hard	Red	The application must be redeveloped to remediate the issue
Repackage	Easy	Green	The application must be repackaged or the MSI edited to remediate the issue
Sequence	Easy	Green	Sequencing steps need to be followed
Sequence	Hard	Green	Sequencing steps need to be followed

Action	Effort	Action RAG	Description
Sequence advanced	Medium	Green	Advanced sequencing steps need to be followed
Shim	Medium	Green	A shim will be applied to the application to remediate the issue
Undefined	Not defined	Undefined	No action is defined for remediation
Virtualizationexception	Hard	Red	Remediation may not be possible
Secure Web in-house redevelopment required	Medium	Green	The web application needs to be redeveloped to solve this issue
Secure Web redevelopment required	Medium	Green	The web application needs to be redeveloped to solve this issue
Secure Web remediations	Easy	Green	Secure Web remediations are required to get web pages to work as expected
XenApp	Easy	Green	XenApp steps need to be followed

Standard action details

This section lists the action details that are available for each of the standard actions.

Additional testing required

Action detail	Description
Application requires functionality testing	Application requires functionality testing

Action detail	Description
Assess application security risk	Assess application security risk
Driver compatibility test required	Driver compatibility test required
Driver component requires further testing	Driver component requires further testing
Verify application publisher is trustworthy	Verify application publisher is trustworthy

Additional XenApp testing required

Action detail	Description
Additional testing may be required	Additional testing may be required

Application virtualization

Action detail	Description
Deploy application using an application virtualization technology, such as App-V	Deploy application using an application virtualization technology, such as App-V

App-V 5.0

Action detail	Description
Microsoft prescriptive guidance for sequencing Office 2010	Follow the Microsoft prescriptive guidance for sequencing Office 2010 applications
Use App-V 5.0	Use App-V 5.0

App-v Management Console modifications

Action detail	Description
Create global FTAs	Create global FTAs

Action detail	Description
Select one application to be FTA provider, change the other application's verb	Select one application to be FTA provider, change the other application's verb

Auto

Action detail	Description
Use the automatic fix provided by AppDNA	The application needs the automatic fix provided by AppDNA

Change GPO

Action detail	Description
Change the corresponding group policy	Change the corresponding group policy

Change hardware

Action detail	Description
Replace underlying hardware	Replace underlying hardware

Change OS

Action detail	Description
Add certificate trusted list	Add certificate trusted list
Add non-supported component to OS	Add non-supported component to OS
Add redistributable to OS	OS build should include this dependency, a redistributable may be available
Change registry keys on the build	Change registry keys on the build
Deploy core applications to OS	Deploy core applications to OS

Action detail	Description
Deploy applications unsuitable for virtualization to OS	Deploy applications unsuitable for virtualization to OS
Disable Dep NX protection on the OS	Disable Dep NX protection on the OS
Edit GPO to allow anonymous RPC and allow port 135 on the firewall	Edit GPO to allow anonymous RPC and allow port 135 on the firewall
Edit registry to repair GINA chaining on Windows Server 2003	Edit registry to repair GINA chaining on Window Server 2003, select a different action for Server 2008 and above
Enable only IP v4	Enable only IP v4 on the build for the installed network adapters
Enable the 16-bit subsystem	Enable the 16-bit subsystem
Open the port to allow communication	Open the port to allow communication
Relax permission on the local intranet zone	Relax permission on the local intranet zone
Run application on 64-bit OS	Run application on 64-bit OS
Run Interactive Service Detection Service	The Interactive Server Detection Service will need to be enabled on the OS build

Change software

Action detail	Description
Replace or update vendor software	Replace or update vendor software

Desktop virtualization

Action detail	Description
Deploy application using a desktop virtualization technology, such as Med-V	Deploy application using a desktop virtualization technology, such as Med-V

Edit OSD file

Action detail	Description
Edit FTA section	Edit FTA section
Enable LOCAL_INTERACTION_ALLOWED policy	Enable LOCAL_INTERACTION_ALLOWED policy
Split the application into pieces and use DSC to create inter-package dependencies	Split the application into pieces and use DSC to create inter-package dependencies
Use DSC to create inter-package dependencies	Use DSC to create inter-package dependencies

Exception

Action detail	Description
Remediation not possible	There is no remediation available for this application

Firefox in-house redevelopment required

Action detail	Description
Explicitly opt-in to HTML parsing for XSLT if your output depends on HTML parsing rules: <xsl:output method=”html”>	Explicitly opt-in to HTML parsing for XSLT if your output depends on HTML parsing rules: <xsl:output method=”html”>
Migrate to the standardized XSL namespace: <xsl:stylesheet xmlns:xsl=”http: //www.w3.org/1999 /XSL/Transform”>	Migrate to the standardized XSL namespace: <xsl:stylesheet xmlns:xsl=”http: //www.w3.org/1999 /XSL/Transform”>
Redevelop the page to adjust changes to the table object model in Firefox	Redevelop the page to adjust changes to the table object model in Firefox
Redevelop the page to trim white spaces where it is needed	Redevelop the page to trim white spaces where it is needed
Redevelop the site so that it does not use legacy properties	Redevelop the site so that it does not use legacy properties
Redevelop the site so that the eval method is called directly	Redevelop the site so that the eval method is called directly
Redevelop the site without using the cached pointers to call methods	Redevelop the site without using the cached pointers to call methods

Action detail	Description
Use the standardized xml-stylesheet processing instruction for loading XSLT: <?xml-stylesheet type=”text/xsl” href=”my.xslt”?>	Use the standardized xml-stylesheet processing instruction for loading XSLT: <?xml-stylesheet type=”text/xsl” href=”my.xslt”?>

Firefox redevelopment required

Action detail	Description
BASE elements need to be moved inside the HEAD of the document	BASE elements need to be moved inside the HEAD of the document
Create the element and add the attributes individually by using the setAttribute API or create the element inside a parent	Create the element and add the attributes individually by using the setAttribute API or create the element inside a parent element by using the innerHTML API
If your page contains these filters, please remove or replace them	If your page contains these filters, please remove or replace them
Move the nested OBJECT so that it is the outermost OBJECT	Move the nested OBJECT so that it is the outermost OBJECT
Redevelop page to use supported DHTML behaviors	Redevelop page to use supported DHTML behaviors
Redevelop the page so that it does not use Document APIs via document fragments	Redevelop the page so that it does not use Document APIs via document fragments
Redevelop the page so that it uses full tag names while calling getElementsByTagName	Redevelop the page so that it uses full tag names while calling getElementsByTagName
Redevelop the page to avoid using return statement in Javascript protocols	Redevelop the page to avoid using return statement in Javascript protocols
Redevelop the site so that it does not use conditional comments	Redevelop the site so that it does not use conditional comments
Redevelop the site so that it does not use namespaces	Redevelop the site so that it does not use namespaces
Redevelop the site so that it does not use XML data islands	Redevelop the site so that it does not use XML data islands
Redevelop the site using a fixed height for IFrames	Redevelop the site using a fixed height for IFrames

Action detail	Description
Redevelop the site without the arguments. caller property	Redevelop the site without the arguments. caller property
Remove references to external domains	Remove references to external domains using the src attribute for script tags
Remove URL paths to gopher and telnet resources	Remove URL paths to gopher and telnet resources
Remove XMB images and use alternative image format	The application needs to be redeveloped to remove XMB images and use an alternative image format such as .png
Replace API call with compliant	Discontinued or unsupported API calls should be replaced with new or supported one
Replace CDF with the new RSS feed	The application needs to be redeveloped to replace CDF with the new RSS feed
Replace functionality of ActiveX components which are unsupported by Firefox	Replace functionality of ActiveX components which are unsupported by Firefox
Replace window on document where it is needed	Replace window on document where it is needed
Rework the page to add the element to document.documentElement instead	Rework the page to add the element to document.documentElement instead
The application needs to be redeveloped so that files are created on the web server and a clickable link is provided to users to	The application needs to be redeveloped so that files are created on the web server and a clickable link is provided to users to download the file
The application needs to be redeveloped to use the compliant naming standards	The application needs to be redeveloped to use the compliant naming standards
The application needs to be redeveloped to use the correct extension for style sheets	The application needs to be redeveloped to use the correct extension for style sheets

Firefox remediations

Action detail	Description
Disable Show Mixed Content in Firefox	Disable Show Mixed Content in Firefox
Do not use COM components which are unsupported by Firefox	Do not use COM components which are unsupported by Firefox

Action detail	Description
Pre-install the component on the build	Pre-install the component on the build
Use the correct extension for style sheets	Use the correct extension for style sheets
Whitelist these class IDs in the IE8 Ax GPO	Whitelist these class IDs in the IE8 Ax GPO

IE infrastructure changes

Action detail	Description
Add X-UA-Compatible header to your web page/IIS header to force it to run in IE7 Standards Mode	Add X-UA-Compatible header to your web page/IIS header to force it to run in IE7 Standards Mode
Add X-UA-Compatible header to your web page/IIS header to force it to run in IE8 Standards Mode	Add X-UA-Compatible header to your web page/IIS header to force it to run in IE8 Standards Mode
Run web site natively in IE6 using virtualization technology	Run web site natively in IE6 using virtualization technology
Run web site natively in IE7 using virtualization technology	Run web site natively in IE7 using virtualization technology
Run web site natively in IE8 using virtualization technology	Run web site natively in IE8 using virtualization technology
Use a custom header on the web server to set IE8 Standards document compatibility mode	Use a custom header on the web server to set IE8 Standards document compatibility mode
Use a custom header on the web server to set IE9 Standards document compatibility mode	Use a custom header on the web server to set IE9 Standards document compatibility mode
Use a GPO to run the web page in IE7 compatibility mode	Use a GPO to run the web page in IE7 compatibility mode

IE in-house redevelopment required

Action detail	Description
Change the title attribute on the link element or style element that contains the style sheet instead	Change the title attribute on the link element or style element that contains the style sheet instead

Action detail	Description
Explicitly opt-in to HTML parsing for XSLT if your output depends on HTML parsing rules: <xsl:output method=”html”>	Explicitly opt-in to HTML parsing for XSLT if your output depends on HTML parsing rules: <xsl:output method=”html”>
Migrate to the standardized XSL namespace: <xsl:stylesheet xmlns:xsl=”http: //www.w3.org/1999 /XSL/Transform”>	Migrate to the standardized XSL namespace: <xsl:stylesheet xmlns:xsl=”http: //www.w3.org/1999 /XSL/Transform”>
Redevelop the page to adjust changes to the table object model in IE9	Redevelop the page to adjust changes to the table object model in IE9
Redevelop the page to adjust removed iframe	Redevelop the page to adjust removed iframe
Redevelop the page to trim white spaces where it is needed	Redevelop the page to trim white spaces where it is needed
Redevelop the page to use the getAttribute API to retrieve the value of user-defined content attributes	Redevelop the page to use the getAttribute API to retrieve the value of user-defined content attributes
Redevelop the site so that it does not use legacy properties	Redevelop the site so that it does not use legacy properties
Redevelop the site so that it uses CCS3, SVG and other widely supported standards instead of DX filters	Redevelop the site so that it uses CCS3, SVG and other widely supported standards instead of DX filters
Redevelop the site so that the eval method is called directly	Redevelop the site so that the eval method is called directly
Redevelop the site without using the cached pointers to call methods	Redevelop the site without using the cached pointers to call methods
Remove administrative DLLs and OCXs that are embedded in web pages	Remove administrative DLLs and OCXs that are embedded in web pages
Use the standardized xml-stylesheet processing instruction for loading XSLT: <?xml-stylesheet type=”text/xsl” href=”my.xslt”?>	Use the standardized xml-stylesheet processing instruction for loading XSLT: <?xml-stylesheet type=”text/xsl” href=”my.xslt”?>

IE redevelopment required

Action detail	Description
Base elements need to be moved inside the HEAD of the document	Base elements need to be moved inside the HEAD of the document
Bypass window.close prompt by adding window.open((‘’, ‘_self’) to the closeWin function	Bypass window.close prompt by adding window.open((‘’, ‘_self’) to the closeWin function
Change the file type from an image file to plain text	Change the file type from an image file to plain text
Create a 64 Bit version of the COM component	Create a 64 Bit version of the COM component
Create the element and add the attributes individually by using the setAttribute API or create the element inside a parent element	Create the element and add the attributes individually by using the setAttribute API or create the element inside a parent element by using the innerHTML API
If your page contains these filters, please remove or replace them	If your page contains these filters, please remove or replace them
Move the nested OBJECT so that it is the outermost OBJECT	Move the nested OBJECT so that it is the outermost OBJECT
Redevelop page to use supported DHTML behaviors	Redevelop page to use supported DHTML behaviors
Redevelop the page so that it does not use Document APIs via document fragments	Redevelop the page so that it does not use Document APIs via document fragments
Redevelop the page so that it uses full tag names while calling getElementsByTagName	Redevelop the page so that it uses full tag names while calling getElementsByTagName
Redevelop the page to avoid using a return statement in JavaScript protocols	Redevelop the page to avoid using a return statement in JavaScript protocols
Redevelop the page to remove manual binding, if support for older versions needed, use version conditional adding of binding	Redevelop the page to remove manual binding, if support for older versions needed, use version conditional adding of binding
Redevelop the site so that it does not use COM controls that expose Window’s Journal Hooks functions	Redevelop the site so that it does not use COM controls that expose Window’s Journal Hooks functions
Redevelop the site so that it does not use conditional comments	Redevelop the site so that it does not use conditional comments
Redevelop the site so that it does not use namespaces	Redevelop the site so that it does not use namespaces

Action detail	Description
Redevelop the site so that it does not use XML data islands	Redevelop the site so that it does not use XML data islands
Redevelop the site so that it does not write to protected locations	Redevelop the site so that it does not write to protected locations
Redevelop the site so that it uses SVG, Raphael JavaScript Library and other widely supported standards instead of VML	Redevelop the site so that it uses SVG, Raphael JavaScript Library and other widely supported standards instead of VML
Redevelop the site to avoid mixing native XML and MSXML objects	Redevelop the site to avoid mixing native XML and MSXML objects
Redevelop the site to make it DEP aware	Redevelop the site to make it DEP aware
Redevelop the site using a fixed height for IFrames	Redevelop the site using a fixed height for IFrames
Redevelop the site without the arguments. caller property	Redevelop the site without the arguments. caller property
Remove direct animation with another technology	The application needs to be redeveloped to replace direct animation with another supported technology
Remove references to external domains	Remove references to external domains using the src attribute for script tags
Remove URL paths to gopher and telnet resources	Remove URL paths to gopher and telnet resources
Remove XMB images and use alternative image format	The application needs to be redeveloped to remove XMB images and use an alternative image format such as .png
Replace API call with compliant	Discontinued or unsupported API call should be replaced with new or supported one
Replace CDF with the new RSS feed	The application needs to be redeveloped to replace CDF with the new RSS feed
Replace window on document where it is needed	Replace window on document where it is needed
Rework the page to add the element to document.documentElement instead	Rework the page to add the element to document.documentElement instead

Action detail	Description
The application needs to be redeveloped so that files are created on the web server and a clickable link is provided to users to	The application needs to be redeveloped so that files are created on the web server and a clickable link is provided to users to download the file
The application needs to be redeveloped so that the existence of an attribute is checked	The application needs to be redeveloped so that the existence of an attribute is checked
The application needs to be redeveloped to use the compliant naming standards	The application needs to be redeveloped to use the compliant naming standards
The application needs to be redeveloped to use the correct extension for style sheets	The application needs to be redeveloped to use the correct extension for style sheets
Use a character set that isn't UTF-7 if the script needs to run	Use a character set that isn't UTF-7 if the script needs to run
Use the correct case and matching	The application needs to be redeveloped to use the correct case and matching

IE remediations

Action detail	Description
Add site to trusted zone	Use the ActiveX Installer Service and configure policy settings using either Approved Installation Sites for ActiveX Controls or ActiveX Installation Policy for Sites in Trusted Zones
Disable DEP in IE	Disable DEP in IE
Disable Show Mixed Content in IE	Disable Show Mixed Content in IE
Edit the registry to remove repeats and older versions	Edit the registry to remove repeats and older versions
Patch your ASP.NET server	Patch your ASP.NET server
Pre-install the component on the build	Pre-install the component on the build
Relax Internet security settings	Relax the Internet security settings for ActiveX if the reduced risk of security is acceptable
Relax the Internet security settings by enabling scriptlets	Relax the Internet security settings by enabling scriptlets

Action detail	Description
Relax the Internet security settings to enable status bar updates	Relax the Internet security settings to enable status bar updates
Remove the kill bit	Remove the kill bit by creating the unkill registry key
Set the Safe for Scripting and Safe for Initialization value	Set the Safe for Scripting and Safe for Initialization value in the registry key using the ActiveX controls CLSID
Train users on the new functionality	Train users on the new functionality
Unblock the Internet security setting Script ActiveX controls marked safe for scripting	Unblock the Internet security setting Script ActiveX controls marked safe for scripting
Update current JavaScript framework to the latest version	Update current JavaScript framework to the latest version
Use the 32 bit version of IE	Use the 32 bit version of IE
Whitelist these class ids in the IE8 Ax GPO	Whitelist these class ids in the IE8 Ax GPO

No remediation required

Action detail	Description
Install admin rights	Ensure install user has admin rights
No Remediation Required	No Remediation Required

Redevelopment required

Action detail	Description
The application needs to be redeveloped to solve this issue	Redevelopment sub-action description

Repackage

Action detail	Description
Add the necessary customizations	Add the necessary customizations
Change the default installation path	Use an MST (Microsoft Transform) to modify the installation path or change it manually
Condition out the components	Condition out the components that install these resources
Create a Merge Module for shared resource	Create a Merge Module for shared resource
Disable DEP using MSI	Disable DEP using the MSI
Edit the custom action	Edit the custom action
Edit the MSI	Edit the MSI
Edit the script file called by the MSI	Edit the script file called by the MSI
Elevate the custom action	Elevate the custom action
Install this pre-requisite	Install this pre-requisite
Package application using Windows Installer for deployment to desktop	Package application using Windows Installer for deployment to desktop
Provide a substitute technology	Provide a substitute technology
Provide the missing resource	Provide the missing resource or install a redistributable
Relax permissions on the local machine	Relax permissions on the local machine using LockPermission for example
Remove the Lock Permissions	Remove the Lock Permissions
Remove this condition	Remove this condition
Rename the setup to Setup.EXE	Rename the setup to Setup.EXE
Suppress the reboot	Suppress the reboot
Sync component GUIDs	Sync component GUIDs
Transform the MSI to change ALLUSERS	Transform the MSI to change ALLUSERS
Transform the MSI values	Change the values in the MSI to be the new correct paths

Sequence### (Easy effort)

Action detail	Description
Add placeholders in INI files	Add placeholders in INI files
Add relationship link in the sequence	Add relationship link in the sequence
Compress the SFT file	Compress the SFT file
Create dummy ODBC entries on the sequencer workstation	Create dummy ODBC entries on the sequencer workstation
Include missing files in the sequence	Include missing files in the sequence
Manually create shortcut to correct executable	Manually create shortcut to correct executable
Publish shortcuts in the Start Menu's startup folder	Publish shortcuts in the Start Menu's startup folder
Resolve install related shortcuts and remove from the sequence	Resolve install related shortcuts and remove from the sequence
Sequence application with its required service	Sequence application with its required service
Sequence with applications that depend on it	Sequence with applications that depend on it
Split application into pieces	Split application into pieces
Use Dynamic Suite Composition	Associate the application with its dependency using Dynamic Suite Composition

Sequence### (Hard effort)

Action detail	Description
Deploy the service separately from the App-V package	Associate the application with its dependency using Dynamic Suite Composition

Sequence advanced

Action detail	Description
Configure environment variable changes	Configure environment variable changes
Configure user specific data to be installed within the sequence without using Active Setup	Configure user specific data to be installed within the sequence without using Active Setup

Action detail	Description
Further investigation required, sequence if feasible	Further investigation required, sequence if feasible
Use Office Deployment Tool	Use the Office Deployment Tool to create the App-V package

Shim

Action detail	Description
Apply CorrectFilePaths Shim	The application needs the CorrectFilePaths shim applied
Apply DisableNX Shim	The application needs the DisableNX shim applied
Apply HideCursor Shim	The application needs the HideCursor shim applied
Apply IgnoreMessageBox Shim	The application needs the IgnoreMessageBox shim applied
Apply RunAsAdmin Shim	The application needs the HideCursor shim applied
Apply RunAsAdmin or RunAsInvoker Shim	The application needs the RunAsAdmin or RunAsInvoker shim included, depending on whether it is administrative in nature
Apply RunAsInvoker Shim	The application needs the RunAsInvoker shim applied
Apply SessionShim Shim	The application needs the SessionShim applied
Apply VirtualRegistry Shim	The application needs the VirtualRegistry applied
Apply WRPDllRegister Shim	The application needs the WRPDllRegister Shim applied
Apply WRPMitigationLayer Shim	The application needs the WRPMitigation Shim applied
Apply WRPRegDeleteKey Shim	The application needs the WRPRegDeleteKey shim applied

Undefined

Action detail	Description
Not Defined	Not Defined

Virtualization exception

Action detail	Description
Remediation possible if splitting out component to OS	Remediation possible if splitting out component to OS
Remediation may be possible with extensive testing	Remediation may be possible with extensive testing

Secure Web in-house redevelopment required

Action detail	Description
Explicitly opt-in to HTML parsing for XSLT if your output depends on HTML parsing rules: <xsl:output method=”html”>	Explicitly opt-in to HTML parsing for XSLT if your output depends on HTML parsing rules: <xsl:output method=”html”>
Migrate to the standardized XSL namespace: <xsl:stylesheet xmlns:xsl=”http: //www.w3.org/1999 /XSL/Transform”>	Migrate to the standardized XSL namespace: <xsl:stylesheet xmlns:xsl=”http: //www.w3.org/1999 /XSL/Transform”>
Redevelop the page to adjust changes to the table object model in Secure Web	Redevelop the page to adjust changes to the table object model in Secure Web
Redevelop the page to trim white spaces where it is needed	Redevelop the page to trim white spaces where it is needed
Redevelop the site so that it does not use legacy properties	Redevelop the site so that it does not use legacy properties
Redevelop the site so that the eval method is called directly	Redevelop the site so that the eval method is called directly
Redevelop the site without using the cached pointers to call methods	Redevelop the site without using the cached pointers to call methods

Action detail	Description
Use the standardized xml-stylesheet processing instruction for loading XSLT: <?xml-stylesheet type=”text/xsl” href=”my.xslt”?>	Use the standardized xml-stylesheet processing instruction for loading XSLT: <?xml-stylesheet type=”text/xsl” href=”my.xslt”?>

Secure Web redevelopment required

Action detail	Description
Base elements need to be moved inside the HEAD of the document	Base elements need to be moved inside the HEAD of the document
Create the element and add the attributes individually by using the setAttribute API or create the element inside a parent element	Create the element and add the attributes individually by using the setAttribute API or create the element inside a parent element by using the innerHTML API
If your page contains these filters, please remove or replace them	If your page contains these filters, please remove or replace them
Move the nested OBJECT so that it is the outermost OBJECT	Move the nested OBJECT so that it is the outermost OBJECT
Redevelop page to use supported DHTML behaviors	Redevelop page to use supported DHTML behaviors
Redevelop the page so that it does not use Document APIs via document fragments	Redevelop the page so that it does not use Document APIs via document fragments
Redevelop the page so that it uses full tag names while calling getElementsByTagName	Redevelop the page so that it uses full tag names while calling getElementsByTagName
Redevelop the page to avoid using a return statement in JavaScript protocols	Redevelop the page to avoid using a return statement in JavaScript protocols
Redevelop the site so that it does not use conditional comments	Redevelop the site so that it does not use conditional comments
Redevelop the site so that it does not use namespaces	Redevelop the site so that it does not use namespaces
Redevelop the site so that it does not use XML data islands	Redevelop the site so that it does not use XML data islands

Action detail	Description
Redevelop the site so that it uses SVG, Raphael JavaScript Library and other widely supported standards instead of VML	Redevelop the site so that it uses SVG, Raphael JavaScript Library and other widely supported standards instead of VML
Redevelop the site using a fixed height for IFrames	Redevelop the site using a fixed height for IFrames
Redevelop the site without the arguments. caller property	Redevelop the site without the arguments. caller property
Remove references to external domains	Remove references to external domains using the src attribute for script tags
Remove URL paths to gopher and telnet resources	Remove URL paths to gopher and telnet resources
Remove XMB images and use alternative image format	The application needs to be redeveloped to remove XMB images and use an alternative image format such as .png
Replace API call with compliant	Discontinued or unsupported API call should be replaced with new or supported one
Replace CDF with the new RSS feed	The application needs to be redeveloped to replace CDF with the new RSS feed
Replace functionality of ActiveX components which are unsupported by Secure Web	Replace functionality of ActiveX components which are unsupported by Secure Web
Replace window on document where it is needed	Replace window on document where it is needed
Rework the page to add the element to document.documentElement instead	Rework the page to add the element to document.documentElement instead
The application needs to be redeveloped so that files are created on the web server and a clickable link is provided to users to download the file	The application needs to be redeveloped so that files are created on the web server and a clickable link is provided to users to download the file
The application needs to be redeveloped to use the compliant naming standards	The application needs to be redeveloped to use the compliant naming standards
The application needs to be redeveloped to use the correct extension for style sheets	The application needs to be redeveloped to use the correct extension for style sheets
Use a character set that isn’t UTF-7 if the script needs to run	Use a character set that isn’t UTF-7 if the script needs to run

Secure Web remediations

Action detail	Description
Disable Show Mixed Content in Secure Web	Disable Show Mixed Content in Secure Web
Do not use COM components which are unsupported by Secure Web	Do not use COM components which are unsupported by Secure Web
Pre-install the component on the build	Pre-install the component on the build
Use the correct extension for style sheets	Use the correct extension for style sheets
Whitelist these class ids in the IE8 Ax GPO	Whitelist these class ids in the IE8 Ax GPO

XenApp

Action detail	Description
Develop a silo plan	Develop a silo plan
Enable virtual IP for published applications	Enable virtual IP for published applications
Ensure Password Manager Agent is last GINA installed on the system	Ensure Password Manager Agent is last GINA installed on the system
Isolate/redirect data written to local machine registry keys	Isolate/redirect data written to local machine registry keys
Use Universal Printer Driver to manage printing	Use Universal Printer Driver to manage printing

Configure algorithms for Windows desktop reports

August 1, 2018

The Configure Modules wizard automatically performs the basic configuration of the algorithms in the Windows 8/8.1 and 7 reports, based on your selections. This topic provides information about optional advanced configuration that you may want to consider.

Question	Suggested configuration when the answer is “yes”
Is IPv6 deployed in your environment?	Set the W8_NET_002 or W7_NET_002 algorithm’s custom RAG status to red and the default action to “Redevelopment required”.
Do you consider Help to be a crucial part of an application?	Set the W8_DEP_009 or W7_DEP_009 algorithm’s custom RAG status to amber and set the default action and action detail combination to “Change OS: Install this pre-requisite”.
Are you planning to deploy on a 64-bit edition of Windows desktop?	Set the W8_DRV_001 or W7_DRV_001 algorithm’s custom RAG status to amber and change the default action to reflect the desired remediation approach.
Do you have a group policy that does not allow unsigned drivers?	Set the W8_DRV_001 or W7_DRV_001 algorithm’s custom RAG status to amber and change the default action to reflect the desired remediation approach.
Is your environment locked down?	Set the W8_BP_001 or W7_BP_001 and the W8_BP_003 or W7_BP_003 algorithms’ custom RAG status to amber and change their default actions to reflect the desired remediation approach.
Does your firewall block TCP/IP traffic?	Set the W8_WSK_00 or W7_WSK_00 algorithm’s custom RAG status to amber and change the default action to reflect the desired remediation approach.
Are you planning changes in the environment, such as a change to mapped drives or UNC paths?	Configure all of the algorithms in the “Hard-coded paths” algorithm group so that their custom RAG status is amber and their default actions reflect the desired remediation approach.
Do you typically deploy applications on a per-system basis using a tool such as Microsoft System Center Configuration Manager?	Configure all of the algorithms in the “Deployment issues” algorithm group so that their custom RAG status is amber and their default actions reflect the desired remediation approach.

Question	Suggested configuration when the answer is "yes"
Are you working in an all-English environment but are interested in some of the best practice issues detected by the algorithms in the "Globalization issues" group?	Consider configuring the algorithms in the "Globalization issues" group so that their custom RAG status is amber and their default actions reflect the desired remediation approach.
Do you want to be alerted when applications have dependencies on potentially obsolete versions of Office?	Consider configuring the algorithms in the "Office dependencies" group so that their custom RAG status is amber and their default actions reflect the desired remediation approach.

See Configure algorithm groups and Configure algorithms for information about how to configure the algorithms.

Custom reports

August 1, 2018

Custom reports are reports that you define. You can base custom reports on existing algorithms and algorithm groups or new ones that you write. For example, suppose you are preparing to migrate to Windows Server 2012 and a 64-bit platform and want one combined report rather than separate reports for each platform. You can create a custom report that is based on the algorithms in both the Windows Server 2012 and the 64-bit reports. You can also create new algorithms based on your own specialized knowledge of your environment.

Limitations

AppDNA does not restrict the number of custom reports that you can create or the number of algorithm groups you can add to a custom report. However, each additional custom report adds to the size of the database and adds another column to the Overview Summary report. This can eventually lead to the Overview Summary report becoming unreadable or all of the available disk space being used up. Similarly each algorithm group adds a column to the Application Issues report view and a bar to the bar chart in the Issues View. These can become unreadable if you add too many algorithm groups. The Application Actions report view and the Actions View can be affected in a similar way if you add too many algorithms.

Desktop applications vs. web applications

Important: Citrix recommends that you do not mix web application algorithms and desktop application algorithms in a custom report and that you name your custom reports carefully to make it clear whether they are designed for desktop or web applications.

The Custom Reports Manager screen is flexible and it does not restrict you from adding a mixture of web and desktop algorithms in a custom report. Similarly, AppDNA does not restrict which applications you can analyze against a custom report. This means that it is possible to create a custom report that mixes algorithms from both desktop and web applications. Depending on the algorithms involved, this may not make much sense.

OS image-dependent algorithms

Some of the AppDNA algorithms test applications for dependencies on features that are provided by the operating system (OS). When relevant, these tests interrogate the OS image DNA that has been loaded into the AppDNA database – for example, to find out whether features have been enabled in the image. These are called image-dependent algorithms.

If you add any image-dependent algorithms to a custom report, AppDNA adds an entry for the custom report to the OS image settings. Use this to select the default OS image for the custom report.

Note: You cannot add image-dependent algorithms from more than one AppDNA report to the same custom report. If you attempt to do this, AppDNA displays a message explaining that this is not possible.

For an overview of how AppDNA uses OS images, see Operating systems.

Templates for new algorithms

AppDNA comes with a number of templates for creating new algorithms in custom reports. When you create a new algorithm that you define yourself, you select the template you want to use from a drop-down list on the final page of the New Algorithm wizard (as described in Create custom reports).

Each template defines an issue that, when found in an application, triggers the algorithm. The template defines a generic issue and you enter a specific value. For example, if the generic issue is that the application contains a particular file or installs to a specific path, you enter the particular file or path that causes the problem.

The templates provide an example value that you then edit to meet your specific requirements. You can use the percent sign (%) as a wildcard character to match zero or more characters. The following table lists the templates that are available and the example value.

Application triggers algorithm if	Example value
It has a specific file	filetofind.ini
It installs to a specific path	D:\SomePath%
It sets a specific registry entry	HKEY_LOCAL_MACHINE\Software\MyApplication
It has an INI file that contains specific contents	FileContentMatchString
Its installer contains a custom action with specific contents	CustomActionMatchString
It imports APIs from a particular file	msvbvm%.dll

When using the registry entry template, you can search for a key and value name. To do this, prefix the value name with two backslashes (\\). For example, to find all services with a port value, use: HKEY_LOCAL_MACHINE\%services%\\port.

Advanced users can create raw SQL queries to define the logic for new custom report algorithms. However, Citrix cannot guarantee that these will work in future versions of AppDNA because the structure of the database may change from version to version.

Custom Reports Manager screen

Use the Custom Reports Manager screen to create and manage custom reports.

To open the Custom Reports Manager screen:

- From the AppDNA menus, choose Configure > Custom Reports.

The Custom Reports Manager screen is split vertically:

Right side – Displays a tree view that lists all of the existing reports. You can expand the reports to see the algorithm groups they contain and in turn you can expand the algorithm groups to see the algorithms inside. Reports that are unlicensed are not available.

Left side – Displays any custom reports that have already been created – also in a tree view. You can right-click the items on the left side to access a shortcut menu, which provides options to add, edit, copy, and delete items, and view and change their properties. The options in the shortcut menu vary according to the type of item. For example, you cannot edit an algorithm that you have copied from one of the standard reports, although you can delete it from the custom report. If the left side is blank, it means that no custom reports have been created.

You can drag algorithm groups and individual algorithms from the standard reports on the right side of the screen to a custom report on the left side. This effectively copies the items into the custom report. You can also create algorithms that you define yourself, as described below. You can copy

algorithms that you define yourself from one custom report or group to another. To do this, find the new algorithm on the left side of the screen, right-click and from the shortcut menu, choose Copy to.

To search the standard reports on the right side of the screen for algorithms and algorithm groups by all or part of their names: Use the Search button on the toolbar. For example, you can search for algorithms and algorithm groups that have the text “driver” in their name.

After creating a custom report, you need to analyze your applications against it before you can view the results in the Report Viewer. You can optionally initiate the analysis in this screen after you have finished creating the report. To do this, click Analyze on the toolbar. Alternatively, you can run the analysis later in the normal way.

To download an XML representation of an entire custom report, or selected algorithm groups and algorithms within a custom report: Click Export on the toolbar. This is useful for providing a custom report to other AppDNA installations or performing a backup. To load a custom report that was previously exported, click Import on the toolbar. To import algorithm groups into an existing custom report, right-click the custom report in the tree on the left side of the screen and choose Import Groups. To import algorithms into the group, right-click a custom report algorithm group and choose Import Algorithms.

Overview

August 1, 2018

Custom reports are reports that you define yourself. You can base custom reports on existing algorithms and algorithm groups or new ones that you write yourself. For example, suppose you are preparing to migrate to Windows 7 and a 64-bit platform and want one combined report rather than separate reports for each platform. You can create a custom report that is based on the algorithms in both the Windows 7 and the 64-bit reports. You can also create new algorithms based on your own specialized knowledge of your environment. This topic supplements the Custom reports topic with key considerations when creating custom reports.

Limitations

AppDNA does not restrict the number of custom reports that you can create or the number of algorithm groups you can add to a custom report. However, each additional custom report adds to the size of the database and adds another column to the Overview Summary report. This can eventually lead to the Overview Summary report becoming unreadable or all of the available disk space being used up. Similarly each algorithm group adds a column to the Application Issues report view and a bar to the bar chart in the Issues View. These can become unreadable if you add too many algorithm groups.

The Application Actions report view and the Actions View can be affected in a similar way if you add too many algorithms.

Desktop applications vs. web applications

The Custom Reports Manager screen is flexible and it does not restrict you from adding a mixture of web and desktop algorithms in a custom report. Similarly, AppDNA does not restrict which applications you can analyze against a custom report. This means that it is possible to create a custom report that mixes algorithms from the IE and Windows 7 reports, for example. You could then analyze both desktop and web applications against this custom report. Depending on the algorithms involved, this may not make much sense.

Important: Citrix therefore recommends that you do not mix web application algorithms and desktop application algorithms in a custom report and that you name your custom reports carefully to make it clear whether they are designed for desktop or web applications.

OS image-dependent algorithms

Some of the AppDNA algorithms test applications for dependencies on features that are provided by the operating system (OS). When relevant, these tests interrogate the OS image DNA that has been loaded into the AppDNA database – for example, to find out whether features have been enabled in the image. These are called image-dependent algorithms.

If you add any image-dependent algorithms to a custom report, AppDNA adds an entry for the custom report to the OS image settings. Use this to select the default OS image for the custom report.

Note: You cannot add image-dependent algorithms from more than one AppDNA report to the same custom report. If you attempt to do this, AppDNA displays a message explaining that this is not possible.

For an overview of how AppDNA uses OS images, see Operating systems.

Templates for new algorithms

AppDNA comes with a number of templates for creating new algorithms in custom reports. When you create a new algorithm that you define yourself, you select the template you want to use from a drop-down list on the final page of the New Algorithm wizard (as described in Create custom reports).

Each template defines an issue that, when found in an application, triggers the algorithm. The template defines a generic issue and you enter a specific value. For example, if the generic issue is that the application contains a particular file or installs to a specific path, you enter the particular file or path that causes the problem.

The templates provide an example value that you then edit to meet your specific requirements. You can use the percent sign (%) as a wildcard character to match zero or more characters. The following table lists the templates that are available and the example value.

Application triggers algorithm if	Example value
It has a specific file	filetofind.ini
It installs to a specific path	D:\SomePath%
It sets a specific registry entry	HKEY_LOCAL_MACHINE\Software\MyApplication
It has an INI file that contains specific contents	FileContentMatchString
Its installer contains a custom action with specific contents	CustomActionMatchString
It imports APIs from a particular file	msvbvm%.dll

When using the registry entry template, you can search for a key and value name. To do this, prefix the value name with two backslashes (\\). For example, to find all services with a port value, use: HKEY_LOCAL_MACHINE\%services%\\port.

Advanced users can create raw SQL queries to define the logic for new custom report algorithms. However, Citrix cannot guarantee that these will work in future versions of AppDNA because the structure of the database may change from version to version.

Create custom reports

August 1, 2018

Custom report naming rules

Custom report names and algorithm group and algorithm identifiers must follow these rules:

- The first character must be a Latin letter (a through z, A through Z).
- Subsequent characters can be Latin letters or numbers (digits 0 through 9).
- The name or identifier must not be a SQL Server reserved word. For the full list of these, see http://msdn.microsoft.com/en-us/library/aa238507(SQL.80).aspx.
- The name or identifier can be a maximum of 40 characters.

Additionally:

- Custom report names can contain spaces.
- Algorithm or algorithm group identifiers can contain the underscore (_) character.

Create a custom report

1. From the AppDNA menus, choose Configure > Custom Reports.
2. On the toolbar in the Custom Reports Manager screen, click New.
3. In the New Custom Report dialog box, enter a Name and Description for the new custom report.

   The name must conform to the custom report naming rules described earlier. Citrix recommends that the name makes it clear whether the custom report is targeted at desktop or web applications.
4. Click OK.

   This closes the dialog box and adds the new custom report to the left side of the screen.
5. Create algorithm groups and algorithms in the custom report as described below.
6. Click Save on the toolbar to preserve your changes.

Create an algorithm group in a custom report

Before you can create an algorithm group, the custom report must already exist.

To create an algorithm group based on an existing algorithm group:

1. In the tree view on the right side of the Custom Reports Manager screen, locate the algorithm group on which you want to base the new algorithm group.
2. Drag the algorithm group to your custom report on the left side of the screen. This adds the algorithm group and all of its algorithms to the custom report.
3. If you want to change the name of the group, right-click it in the tree view, and from the shortcut menu, choose Properties.
4. In the Properties dialog box, enter the new name and click OK.
5. Click Save on the toolbar to preserve your changes.

To create a new algorithm group that you define yourself:

1. Locate your new custom report on the left side of the Custom Reports Manager screen.
2. Right-click the custom report and from the shortcut menu, choose New Group.
3. In the New Custom Report Group dialog box, enter a unique Identifier for the algorithm group and a Name and Description. The identifier must conform to the custom report naming rules described above.
4. Click OK to close the dialog box.

5. Add algorithms to the group as described below.
6. Click Save on the toolbar to preserve your changes.

Create an algorithm in a custom report

Before you can create an algorithm in a custom report, the algorithm group must already exist.

To create an algorithm in a custom report based on an existing algorithm:

1. In the tree view on the right side of the Custom Reports Manager screen, locate the algorithm you want to add to the algorithm group in your custom report.
2. Drag the algorithm to the required algorithm group in your custom report on the left side of the screen.
3. Click Save on the toolbar to preserve your changes.

To create a new algorithm that you define yourself:

1. On the left side of the Custom Reports Manager screen, locate the algorithm group to which you want to add the new algorithm.
2. Right-click the algorithm group, and from the shortcut menu, choose New Algorithm.
3. On the first page of the New Algorithm wizard, enter a unique Identifier and Name for the algorithm.

   The identifier must conform to the custom report naming rules described above. The convention is to use an identifier of the following form: XXX_nnn, where XXX is a three letter code and nnn is a three digit number.
4. Click Next to move to the next page in the wizard.
5. On the second page of the wizard, enter a Manifestation, which should explain what will make this algorithm trigger, and a Remediation, which should explain how to resolve the issue. Then click Next.
6. On the third page of the wizard, select the RAG status to be applied to applications that trigger this algorithm. Red means that the application will fail, amber means that the application may work but with some issues, and green means that the application is ready for UAT testing. Then click Next.
7. On the fourth page of the wizard, select the Action and Action Detail that will remediate the problem identified by the algorithm. (If the drop-down lists do not include a suitable action and action detail, select the closest available options and then add new actions later in the Algorithm Groups screen.)
8. Click Next.

9. On the fifth page of the wizard, define the logic for the algorithm. There are two ways of doing this:
    - The recommended way is to select the option that describes the issue from the drop-down list and then enter the appropriate value in the associated text box.
    - Advanced users can choose to edit the raw query. This opens the Create or edit the SQL query for an algorithm.
10. Click Save to preserve your changes.

Import and export custom reports

August 1, 2018

You can download an XML representation of an entire custom report, or selected algorithm groups and algorithms within a custom report. This is useful if you want to provide a custom report to other AppDNA installations or to back up a custom report.

To export a custom report or selected algorithms and algorithm groups

1. From the AppDNA menus, choose Configure > Custom Reports.
2. In the Custom Reports Manager screen, click Export on the toolbar.
3. In the Custom Reports Export dialog box, select the items that you want to export.
4. Click Export.
5. In the Save As dialog box, enter a name for the file and the location to save it in.
6. Click OK.

To import a custom report as a new custom report

1. From the AppDNA menus, choose Configure > Custom Reports.
2. In the Custom Reports Manager screen, click Import on the toolbar.
3. Navigate to the file that was previously exported.
4. Click OK.
5. Select the items that you want to import.
6. Click Import.

To import algorithm groups into a custom report

1. From the AppDNA menus, choose Configure > Custom Reports.

2. On the left side of the Custom Reports Manager screen, locate the custom report into which you want to import the exported algorithm groups.
3. Right-click the custom report, and from the shortcut menu, choose Import Groups.
4. Navigate to the file that was previously exported.
5. Click OK.
6. Select the items that you want to import.
7. Click Import.

To import algorithms into an algorithm group in a custom report

1. From the AppDNA menus, choose Configure > Custom Reports.
2. On the left side of the Custom Reports Manager screen, locate the algorithm group into which you want to import the exported algorithms.
3. Right-click the algorithm group, and from the shortcut menu, choose Import Algorithms.
4. Navigate to the file that was previously exported.
5. Click OK.
6. Select the items that you want to import.
7. Click Import.

Create or edit the SQL query for an algorithm

August 1, 2018

Jun 04, 2018

Advanced users can use the Algorithm Implementation dialog box to create or edit the raw SQL query that comprises the logic for an algorithm in a custom report.

The Algorithm Implementation dialog box is split in two horizontally:

- **Top part** – A text editing box in which you create and edit the SQL query.
- **Lower part** – Displays the results of the query when you click Test SQL.

Open the Algorithm Implementation dialog box

You can open the Algorithm Implementation dialog box when you create a new custom report algorithm that you define yourself:

1. On the left side of the Custom Reports Manager screen, locate the algorithm group in which you want to create the new algorithm.

2. Right-click the algorithm group and from the shortcut menu, choose New Algorithm.
3. Work through the New Algorithm wizard in the normal way.
4. On the fifth page of the wizard, choose the Advanced option and then click Go to. This opens the Algorithm Implementation dialog box.

For custom report algorithms that were created using the Advanced option, you can open the Algorithm Implementation dialog box like this:

1. Locate the algorithm in the left side of the Custom Reports Manager screen.
2. Right-click and from the shortcut menu, choose Edit implementation.

Note: You cannot open the Algorithm Implementation dialog box for a custom report algorithm based on an algorithm supplied by Citrix.

Specifications

- The SQL query must be a SELECT statement that returns data relating to the applications that trigger the algorithm.
- The first column in the results set must be the application ID.
- You must include the {APP_IDS} tag, which is replaced at run time with the list of currently selected applications. Typically, you put this tag in the WHERE clause.
- If you use the AS syntax to give tables or columns an alias, the alias name must conform to the rules for regular identifiers regardless of whether it is enclosed in brackets ([ ]) or double quotation marks (“ “). For example, an alias name must not contain spaces or apostrophes (‘). See http://msdn.microsoft.com/en-us/library/aa223962(SQL.80).aspx for more information about regular identifiers.

For comprehensive documentation of the SELECT statement, see http://msdn.microsoft.com/en-us/library/aa259187(SQL.80).aspx.

Caution: Citrix cannot guarantee that queries you write will work in future versions of AppDNA, because the structure of the database may change from version to version.

Example

When you open the dialog box when creating a new algorithm, the top part of the dialog contains an example query as follows:

```
pre codeblock 1 SELECT mf.[application_id], mf.[long_filename] , mf.[
target_path], mf.[version], mf.[version_number], mf.language 2 FROM [dbo
].[msi_file] mf 3 4 WHERE 5 ( 6 mf.[language] NOT LIKE '%1033%'7 AND 8 (mf
.[language] != '0'9 AND 10 mf.[language] is NOT null 11 AND 12 mf.[language
```



```
] != ''13 )14 )15 AND mf.application_id IN ( { APP_IDS } )16 ORDER BY mf.[
application_id]
```

This retrieves all the applications that contain any files that are not US English.

Lines 1-2 – Selects six named columns from the dbo.msi_file table, which is given the alias mf.

Line 3 – The WHERE clause defines a filter that restricts the results to those that meet the following criteria:

- **Lines 6-12** – The value in the language column does not match the language code for US English and is not blank, zero or Null.
- **Line 15** – And the application ID is included in the list of currently selected application IDs that replace the {APP_IDS} tag at run time.
- **Line 16** – Orders the results by the application ID.

This example provides a starting point only and is not meant to be prescriptive. You can use SQL Server Management Studio to browse the tables in the AppDNA database. However, note that Citrix cannot guarantee that queries you write will work in future versions of AppDNA because the structure of the database may change from version to version.

Forward Path

August 1, 2018

Forward Path is a powerful business decision engine that is built into AppDNA. Forward Path makes it possible to model different deployment scenarios and compare their impacts. You can create scenarios that reflect organizational decisions and create different automation task scripts based on the results. For example, when preparing a migration to Windows 8, you could create a Forward Path scenario to determine which applications are suitable for deployment as App-V packages, which should be deployed to the desktop, and which require redevelopment.

By associating task scripts with the various outcomes, you can automate the App-V sequencing and MSI packaging using Install Capture. This requires a virtual machine that has been set up and configured as explained in Install Capture.

Forward Path scenario

A Forward Path scenario is a script that defines the logic for a Forward Path report. The logic is applied to each application that is selected for inclusion in the report. The report has columns for application name, manufacturer, version, and source path, and the scenario logic provides values for an Outcome column and optionally for Cost, RAG, and Description columns, and up to 20 custom columns. If the

logic puts RAG values in any of the custom columns, AppDNA automatically generates a pie chart summary of the results for that column when you run the report.

Note: The
Configure Modules wizard automatically creates a scenario called My Enterprise Selections tailored for your projects. AppDNA automatically updates this scenario if you change options in the Configure Modules wizard. You cannot edit the My Enterprise Selections scenario directly. However, you can use it as a template for your own scenarios.

Forward Path task script

Forward Path tasks are typically used to automate the creation of production-ready App-V and XenApp packages, based on logic within the Forward Path report. However, Forward Path tasks can be configured to do many other tasks, such as copying files and sending emails.

A Forward Path task script is a script that defines an action to be performed for a value in the Outcome column generated by a Forward Path scenario. For example, if an application virtualization scenario marks an application with a green RAG status, a task script can automatically sequence that application using the App-V sequencer and publish the sequence to a test environment for immediate testing.

To run any task scripts that are associated with the selected Forward Path Scenario, click Evaluate Tasks in the Forward Path report viewer.

- To change which applications are selected, go to the Application List screen.
- To change the active scenario for the duration of your AppDNA session, select the scenario you require in the Forward Path report viewer. (You can change the active scenario more permanently in the Forward Path Logic Editor.)
- To run the task scripts associated with the selected applications, click Start.
- To evaluate the active scenario for the selected applications, click Refresh on the toolbar. The information that appears includes the following:
  - The MapUNCPathDriveLetter column shows the mapped drive letter if the task script has used the ApplicationDetails.MapUNCPath property to map the \\server\share portion of installation directory to a drive letter.
  - The **Install Command** column shows the command that launches the application installation. If not overwritten by the task script, this shows the Active Directory or Configuration Manager installation command if the application is linked with an Active Directory or Configuration Manager managed application. Otherwise this column shows a command based on the location and method by which the application was imported into AppDNA.
  - The InstallWrkDir column shows the working directory used by the installation command. When this is blank, the default working directory is used.

Create and edit Forward Path scripts

August 7, 2018

To create and edit Forward Path scenario and task scripts, use the Forward Path Logic Editor. By default, you write scenario and task scripts in Visual Basic .NET 2.0 (VB .NET). For comprehensive Visual Basic .NET documentation, see http://msdn.microsoft.com/en-gb/library/2x7h1hfk.aspx.

- See Forward Path specifications for more information about the structure of the scripts.
- See Forward Path example for a step-by-step tutorial.

To open the Forward Path Logic Editor:

- From the AppDNA menus, choose Configure > Forward Path.

By default, the Forward Path Logic Editor screen is divided into three sections. These are described under separate headings below.

Main toolbar

The main toolbar at the top of the screen has the following options:

New Scenario – Creates a new scenario script. When you click this button, AppDNA opens a dialog box where you can enter the new scenario's name and description. When you click OK, AppDNA creates a basic scenario and opens it in the Editor window, ready for you to edit it.

New Task Script – Creates a new task script and associates it with a specific value in a scenario's Outcome column. When you click this button, AppDNA opens the Forward Path Task Script dialog box, which lists the possible values in the Outcome column for the scenario that is open in the Editor. Select the value with which you want to associate the task script, enter a description, and click OK. See "Forward Path Task Script dialog box" below for more information.

Test – Use to test simple scenario scripts. This runs the script against the applications that are currently selected in the Application List and displays the results on the Output tab. However, this feature does not support some of the advanced Forward Path features, such as grouping. For more advanced scenarios, you need to test your scenario by displaying it in the Report Viewer in the normal way.

Export – Export one or more scenario and task scripts to an XML file – for example, to create a backup. This opens the Forward Path Scenario Export dialog box where you can select the scripts that you want to export.

Import – Import a previously exported scenario or task script file.

Main section (top left)

The main section of the screen has two tabs as follows:

Editor tab – Use to create and edit Forward Path scenarios and task scripts. The toolbar provides the following options:

Save – Save any changes you have made to the script that is open in the Editor.

Properties – View and edit the name and description of the script that is currently open in the Editor.

Show and hide – Click to view or hide the Errors and Side-by-Side Viewer (located at the bottom of the screen).

Separate window – Open the Editor in a separate window.

Task Script Help – View documentation of the AppDNA APIs that are available to task scripts.

Output tab – Displays the output of your scenario script when you click Test on the main toolbar. The output is shown as a flat list without additional formatting information, even if the scenario includes advanced functionality that groups the applications. For more advanced scenarios, you need to test your scenario by displaying it in the Report Viewer in the normal way.

Explorer (right side)

The Explorer provides three tabs as follows:

Scenarios – Lists the sample scenarios that come with AppDNA and any other scenarios that are available. Click a scenario to open it in the Editor and view its description at the bottom of the Explorer tab. One scenario is shown in bold to indicate that it is the active scenario. This means that it is selected by default when you view the Forward Path report. To mark a scenario as the active scenario, right-click it and from the shortcut menu, choose Set as Active.

Task Scripts – Lists the sample task scripts that come with AppDNA and any other task scripts that are available. Click a task script to open it in the Editor. Task scripts are shown as active or inactive. Active means that it is associated with the active scenario.

Property Explorer – Lists the AppDNA properties that you can use in a scenario script. The property names are mostly self-explanatory. However, the MOE properties relate to data imported from Active Directory and ConfigMgr, and the RAG property is the custom RAG.

Errors and Side by Side viewer (bottom left)

The Errors and Side by Side viewer has two tabs:

Errors / Warnings – Displays any errors or warnings that are detected in the current script.

Side by Side Viewer – Use to view another script side-by-side with the one you are editing in the main Editor. To do this, select the scenario or task script on the Explorer tab, right-click and choose View side by side.

Forward Path Task Script dialog box

The Forward Path Task Script dialog box opens when you do one of the following:

1. Click New Task Script on the main toolbar.
2. Right-click a scenario on the Scenario Explorer tab and choose New Task Script from the shortcut menu.

The options in the Forward Path Task Script dialog are:

Associated outcome – Lists the possible values that can be generated for the Outcome column by the scenario that is currently open in the Editor window.

My outcome was not listed – Select this check box to refresh the list of possible values in the Associated Outcome drop-down list. If the value you expect still does not appear, make sure that you have saved any changes to the scenario script and check that the correct scenario is open in the Editor.

Description – It is good practice to enter a full description.

Forward Path specifications

August 2, 2018

Script language

By default all scenario and task scripts are compiled as Visual Basic .NET 2.0 (VB .NET). For comprehensive Visual Basic .NET documentation, see http://msdn.microsoft.com/en-gb/library/2x7h1hfk.aspx.

You can choose to compile task scripts (but not scenarios) as C# 2.0. To do this, start the task script with the following string:

```
1 Language CSharp
```

However, the AppDNA script editor supports syntax highlighting only for Visual Basic .NET.

Assembly references

Scenario and task scripts are compiled in memory to a .NET assembly. They can therefore utilize the entire .NET Framework and any other assemblies in the Global Assembly Cache (GAC). For example, you can use any of the classes available in the System.Collections.Generic namespace. (See the MSDN Library for documentation of this namespace.)

Task scripts have an automatic reference to the AppDNA.AppTitude.Scripting assembly.

You can specify assemblies by using the LoadAssembly extension syntax. For example:

```
LoadAssembly System.Windows.Forms.dll
```

If the assembly is not in the GAC, you must specify the complete path. This does not impact the use of Import with namespaces.

VB .NET <multiline_string> extension

When the language is VB .NET, you can use the following syntax for strings:

```
<multiline_string>xxxx</multiline_string>
```

Where xxxx is a string. Before compilation, the parser turns this into a VB .NET string literal. This makes it easier to specify strings that span multiple lines within the script than is possible using standard VB .NET syntax.

For example:

```
Dim s As String  = <multiline_string>;
   '---Some vbscript
   Option Explicit
   Wscript.Echo "string"
   </multiline_string>
```

Becomes:

```
Dim s As String  = "" & Microsoft.VisualBasic.Constants.vbCRLF & __
"   '---Some vbscript" & Microsoft.VisualBasic.Constants.vbCRLF & _
"   Option Explicit" & Microsoft.VisualBasic.Constants.vbCRLF & _
"   Wscript.Echo ""string""" & Microsoft.VisualBasic.Constants.vbCRLF &
    _
"   "
```


Required scenario script format

A basic Forward Path scenario script consists of a function that defines the output columns in the Forward Path report. The following example is the basic scenario that is created when you click New Scenario on the main toolbar.

```
Public Function ForwardPath(ByVal currentApplication As Application) As
    Output

' TODO: Your new Forward Path Logic definition must be defined here.
' For Help, please refer to the sample Forward Path scripts which
' have been provided.

    Dim myForwardpathresult As New Output()

    myForwardpathresult.Outcome = "Sample Outcome"
    myForwardpathresult.Cost = 100
    myForwardpathresult.RAG = RAG.Green

    ForwardPath = myForwardpathresult

End Function
```

The signature of the function is important and the function must return an Output object that defines at least one output column. If you want to associate task scripts with the scenario, you must define the Outcome output column.

Notice that an Application object is passed into the function. The function is run for every application that is currently selected and the Application object that is passed into the function represents the application that is currently being processed.

Use the Property Explorer on the right side of the Forward Path Logic Editor screen to explore the structure of the Application and Output objects. (The Output object is shown as the ForwardPathReportOutput in the Property Explorer.)

The scenario script can include additional functions that allow you aggregate application data by group and to generate report-level totals. See Grouped Forward Path reports for more information.

Required task script format

Task scripts must have the following form:

```
Imports AppDNA.AppTitude.Scripting

```



```
Public Class ScriptClass

    Public Function Start(controller As IActionController) As
       TaskStatusEnum
        ' Do stuff
        Start = TaskStatusEnum.Complete
    End Function

End Class
```

The names and accessibility of the class and the signature of the function are important. Beyond that, any VB .NET constructs are valid.

Click Task Script Help on the toolbar to view documentation of the AppDNA APIs that are available to task scripts.

Forward Path example

August 1, 2018

This example walks you through creating a simple Forward Path scenario and task script.

Create the scenario

1. From the AppDNA menus, choose Configure > Forward Path.
2. On the toolbar in the Forward Path Logic Editor, click New Scenario.
3. In the Forward Path Script Name dialog box, enter a name and description for the new scenario, and then click OK.

   This creates a new scenario and opens it in the Editor. The new scenario script is as follows:

```
1 Public Function ForwardPath(ByVal currentApplication As
   Application)
As Output
2    ' TODO: Your new Forward Path Logic definition must be
   defined here.
3    ' Refer to the sample Forward Path scripts which have been
   provided.
4    Dim myForwardpathresult As New Output()
5
6    myForwardpathresult.Outcome = "Sample Outcome"
```



```
7     myForwardpathresult.Cost = 100
8     myForwardpathresult.RAG = RAG.Green
9
10    ForwardPath = myForwardpathresult
11
12 End Function
```

4. This is a functional scenario script, although it is not of any practical use. To understand how it works, click Test on the Editor toolbar.

   This evaluates the scenario against the applications that are currently selected in the Application List and opens the results on the Output tab.

   Notice that the value in the Outcome column is “Sample Outcome” for each application, and similarly the value in the RAG and Cost columns are “Green” and 100 for all of the selected applications. This is because the values for these columns are “hard-coded” in the script in lines 6-8.

   Notice that the Description and Customfield columns are empty because the scenario does not provide values for these columns.

5. Change the value of the RAG column to reflect the application’s actual RAG for the Windows 7 report. Change line 8 in the scenario script as follows:

   ```
   1 myForwardpathresult.RAG = currentApplication.Modules.Windows7.RAG
   ```

   This sets the value in the RAG column to the application’s Windows 7 RAG status. (This assumes that the application has already been analyzed for the Windows 7 report. If this report is not available, choose another report that is available. Use the Property Explorer to discover how to refer to the other reports.)

6. Click Test to see the results.

   The values in the RAG column reflect the actual RAG values.

7. Next make the value in the Outcome column depend on the Windows 7 RAG status. To do this, replace line 6 with an If statement, like this:

   ```
   1 If (currentApplication.Modules.Windows7.RAG = RAG.Green) Then
   2   myForwardpathresult.Outcome = ”OK for Windows 7”
   3 Else
   4   If (currentApplication.Modules.Windows7.RAG = RAG.Amber) Then
   5     myForwardpathresult.Outcome = ”Remediation required”
   6   Else
   7     myForwardpathresult.Outcome = ”Redevelopment required”
   8   End If
   9 End If
   ```


This statement tests whether the application's Windows 7 RAG status is green. If it is, the script writes "OK for Windows 7" in the Outcome column and if not, it tests whether the Windows 7 RAG status is amber. If it is amber, the script writes "Remediation required" into the Outcome column and otherwise writes "Redevelopment required" to the Outcome column – because if the RAG status is not green or amber, it must be red (assuming the application has been analyzed and unlocked).

8. Click Test to see the results.

   Notice that now the values in the Outcome column reflect the logic in the If statement.

This is a deliberately trivial example that is designed to introduce how Forward Path works. To see some more realistic examples, use the Scenarios Explorer to browse the sample scenarios that come with AppDNA and use the Property Explorer to explore the properties that are available to the scenario scripts.

Note: The
Output object is shown as
ForwardPathReportOutput in the Property Explorer.

For example, you can use the Output.Display property to control the width and visibility of the standard columns in reports, like this:

```
myForwardpathresult.Display.Application.Width = 250
myForwardpathresult.Display.Manufacturer.Width = 100
myForwardpathresult.Display.Version.Width = 50
myForwardpathresult.Display.SourcePath.Visible = false
myForwardpathresult.Display.Outcome.Width = 400
```

Similarly you can use the Output.CustomFieldn.Display properties to control the width and visibility of the custom field columns:

```
myForwardpathresult.CustomField1.Display.Width = 50
myForwardpathresult.CustomField2.Display.Width = 100
```

These properties control the display of the columns when you run the report. They do not control the columns on the Output tab in the Forward Path Logic Editor.

Create a task script

We will now create a task script that is associated with the "Redevelopment required" value in the Outcome column created by our example scenario script.

1. Open the example script we created in the previous step in the Editor.

2. On the main toolbar, click New Task Script.

   This opens the Forward Path Task Script dialog box, which lists the possible values in the Outcome column for the scenario that is open in the Editor.

3. From the drop-down list, select Redevelopment required, enter a description, and click OK.

   This creates a new task script and opens it in the Editor. The new task script is as follows:

```
1  ' This sample script kicks off an Install Capture of the given file
2  ' as well as interacts with the gui
3  LoadAssembly System.Windows.Forms.dll
4
5  Imports AppDNA.AppTitude.Scripting
6  Imports System.Collections.Generic
7
8  Public Class ScriptClass
9
10   Public Function Start(controller As IActionController) As TaskStatusEnum
11     ' If you need to override or provide replaceable to the
12     ' execution profiles add then to this dictionary
13
14     Dim replaceables As Dictionary(Of String, String)
15     ' replaceables.Add( "replaceablename", "value")
16
17    ' This informs the controller that it can abort if the user cancels
18     controller.AbortOnCancel()
19
20     ' This lets you run the execution profile for a given app using a given VM
21     ProductionManager.RunExecutionProfile(controller, "Snapshot",
22 replaceables, "Default VM Configuration")
23
24     ' Add you own actions
25     controller.GUI.ProgressPercent = 100
26     Start = TaskStatusEnum.Complete
27   End Function
28
29 End Class
```

   This is a skeleton task script that starts an Install Capture.

4. We will change the lines that relate to Install Capture (lines 11 – 21) with code that will send an

email. However, first we will add the following lines after line 6 to import the namespaces we need to send an email:

```
1 Imports System.Net.Mail
2 Imports System.Net
```

5. Now replace the Install Capture code (now lines 13 – 23) with the following:

```
1 ' This informs the controller that it can abort if the user
     cancels
2 controller.AbortOnCancel()
3
4 Dim myClient As New SmtpClient("<validsmtpserver>")
5 myClient.Credentials = New NetworkCredential("<
     emailaccountusername>",
6     "<emailaccountpassword>")
7
8 Dim MainMessage As String = ""
9
10 Dim Message As New MailMessage()
11 Dim Address As New MailAddress("<fromaddress>", "AppDNA
     Notification")
12 Dim ToAddress As New MailAddress("<recipientemailaddress>")
13
14 MainMessage = MainMessage + "<html>"
15 MainMessage = MainMessage + "<head>"
16 MainMessage = MainMessage + "<title>AppDNA Notification</title>"
17
18 MainMessage = MainMessage + "</head>"
19 MainMessage = MainMessage + "<body>"
20
21 MainMessage = MainMessage + "Hello,"
22 MainMessage = MainMessage + "<br />"
23 MainMessage = MainMessage + "<br />"
24 MainMessage = MainMessage + "Application needs redevelopment."
25 MainMessage = MainMessage + "<br />"
26 MainMessage = MainMessage + "Application Name: " + controller.
     Application.Name
27 MainMessage = MainMessage + "<br />"
28 MainMessage = MainMessage + "Source Path: " + controller.
     Application.SourcePath
29 MainMessage = MainMessage + "<br />"
30 MainMessage = MainMessage + "Goodbye."
31 MainMessage = MainMessage + "<br />"
32 MainMessage = MainMessage + "</body>"
```



```
MainMessage = MainMessage + "</html>"

Message.Body = MainMessage
Message.IsBodyHtml = True
Message.From = Address
Message.To.Add(ToAddress)

Message.Subject = "AppDNA Notification"

myClient.Send(Message)
```

6. Replace <validsmtpserver>, <emailaccountusername>, <emailaccountpassword>, <fromaddress> and <recipientemailaddress> with appropriate values for your environment.
7. Click Save to preserve your changes.
8. Now let's run the task script:

   a) From the AppDNA side bar, choose Reports: Applications > Forward Path.
   b) In the Forward Path report viewer, select the Forward Path scenario we created earlier.
   c) Click Evaluate Tasks.

   This opens the Forward Path Task Sequencing screen, which lists the applications that have been processed by the Forward Path scenario and shows whether they have a task script associated with them.

9. Select an application that has a task script associated and click Start on the toolbar.

   This runs the task script for that application. The Status column shows whether the script was run successfully. When an error occurs, it is shown in the lower part of the screen. In this example, the script fails if you have not entered appropriate mail parameters for your environment (step 6 above).

- To see some more examples, use the Task Scripts Explorer to browse the sample task scripts that come with AppDNA.
- For information about running an execution profile from a task script, see Run an execution profile.

Create links to remediation report views

August 1, 2018

This topic explains how to configure your Forward Path reports so that the name of each application included in the report is a link to the application's remediation report view. You can create the link to

the remediation report view of a single report or to a combination of any of the standard reports (this links to the merged remediation report view).

Here is a snippet from a Forward Path report that shows the application name appearing as a link:

#	Application	Manufacturer	Version
1	Analysts Notebook	i2	6.01
2	ActiveSync	Microsoft	3.7
3	BBC Ticker	BBC	1.0.1.7
4	Hardcopy Pro	Desksoft	2.21
5	Citrix ICA Client	Citrix Systems, Inc.	9.00

You specify the link in the Forward Path scenario using the RemediationModules property on the Output object (also known as the ForwardPathReportOutput object). You can create the link to the remediation report view for a single report or to a merged remediation report view. For example, you can create a link to the Windows 7 remediation report view like this:

```
Dim myForwardpathresult As New Output()
' ...
myForwardpathresult.RemediationModules.Add("Win7Module")
```

To create a link to the merged Windows 7 and App-V remediation report views, add another line like this:

```
myForwardpathresult.RemediationModules.Add("VirtualisationRuleModule")
```

By default, the link takes you to the remediation issues view. If you want it to go to the remediation actions view, add the following line:

```
myForwardpathresult.RemediationView = RemediationView.Actions
```

Note: The
RemediationModules property is an object of the standard .NET
List class (see the
MSDN Library for documentation).

The following table lists the IDs that define the various AppDNA reports. For the link to work correctly, the report must be licensed and the application analyzed for that report.

To specify this report:	Use this ID:
Security	SecurityModule
Windows 10	Win10Module
Windows 8/8.1	Win8Module
Windows 7	Win7Module
Windows Server 2016	Win2016Module
Windows Server 2012/2012 R2	Win2012Module
Windows Server 2008 R2	Win2008R2Module
XenApp Hosted	XenAppRuleModule
App-V	VirtualisationRuleModule
AppDisks	AppDisksModule
Internet Explorer (IE)	IEModule
Firefox	FFModule
Secure Web	WorxWebModule

Link to custom report remediation views

You can link to a single custom report's remediation report view. To do this, you need to know the custom report's identifier. Typically this is the same as the custom report's name (with any spaces removed). For example, if you create a custom report using the default name of "My New Custom Report", its identifier is typically MyNewCustomReport. However, there are exceptions. For example:

- If you rename the custom report, the identifier remains unchanged.
- If you create another custom report with the same name as a previous one whose name has been changed, the identifier is the same as the previous one, but with _1 appended.

Note: Linking to merged custom report remediation report views is not supported.

The complete scenario

Here is the example scenario we created in the Forward Path example, that has been expanded to create links to the remediation report views:

```
Public Function ForwardPath(ByVal currentApplication _
  As Application) As Output

```



```
  Dim myForwardpathresult As New Output()

  If (currentApplication.Modules.Windows7.RAG = RAG.Green) Then
    myForwardpathresult.Outcome = "OK for Windows 7"
  Else
    If (currentApplication.Modules.Windows7.RAG = RAG.Amber) Then
        myForwardpathresult.Outcome = "Remediation required"
    Else
        myForwardpathresult.Outcome = "Redevelopment required"
    End If
  End If

  myForwardpathresult.Cost = 100
  myForwardpathresult.RAG = _
    currentApplication.Modules.Windows7.RAG

  ' Create links to the merged Windows 7 and App-V
  ' remediation report views.
  myForwardpathresult.RemediationModules.Add("Win7Module")
  myForwardpathresult.RemediationModules.Add("VirtualisationRuleModule"
      )

  ' Specify that the link goes to the action view.
  myForwardpathresult.RemediationView = _
    RemediationView.Actions

  ForwardPath = myForwardpathresult
End Function
```

Use Effort Calculator variables in a Forward Path scenario

August 1, 2018

This topic provides an introduction to the use of the Effort Calculator variables in your Forward Path scenario. This topic uses an example to introduce the use of these features.

About the Effort Calculator variables

Effort Calculator estimates the cost and effort involved in remediating your application portfolio for a target platform (represented by one of the AppDNA reports). The calculation uses two main types of variables:

- **User-defined variables** – These store values such as how much a tester, remediator, and project manager cost per day, the number of hours in a typical working day, how long it takes on average to remediate applications of different complexities (simple, normal, and complex), taking into account the difficulty of the remediation action (easy, medium, or hard). You can set these variables separately for each AppDNA report in the Effort Calculator screen.
- **Application-level variables** – These are derived from the AppDNA analysis and include the complexity of the application (this is based on the number of files and registry entries the application has), and the difficulty (or complexity) of the actions that need to be taken to remediate the application for the selected report.

Using this information Effort Calculator estimates the expected cost of migrating the entire application portfolio to the new platform. You can now use these variables in your Forward Path scenario – for example, to estimate the cost of remediating each application. This topic provides a relatively simple example of how to do this. One of the sample scenarios that comes with AppDNA provides a more complex and sophisticated example.

For detailed information about the Effort Calculator variables and how they are used, see Effort Calculator.

Retrieving the user-defined Effort Calculator variables

You can access the user-defined Effort Calculator variables through the EffortCalculatorSettings object, which you retrieve through the Host object. The Host object is implicitly available to the entire scenario script. Here is a snippet that retrieves the EffortCalculatorSettings object for the Windows 7 report:

“‘ pre codeblock
Private Dim vars As EffortCalculatorSettings

’ Get the Windows 7 Effort Calculator settings object.
vars = Host.GetEffortCalculatorSettings(“Win7Module”)

```
Notice that we have used the Windows 7 internal report identifier to
    retrieve the Effort Calculator variables for Windows 7. For a list
    of the report identifiers, see [Create links to remediation report
    views](/en-us/dna/current-release/configure/forward-path/dna-forward
    -path-remediation-links.html).

You can see all of the properties of the EffortCalculatorSettings
    object in the Property Explorer on the right side of the [Forward
    Path Logic Editor screen](/en-us/dna/current-release/configure/
    forward-path/dna-forward-path-logic-editor.html). The names of the
    properties closely relate to the text shown for the variables in the
     Effort Calculator screen. For example, the AppStagingHours property
```



```
      corresponds to the Staging time variable in the Staffing variables
    section of the Effort Calculator screen. We will use this variable
    in the example that follows.

It is possible to set the values of these variables in your scenario
    for use in that scenario, like this:

''' pre codeblock
vars.TesterStagerCostPerDay = 23
```

Note: This does not change or overwrite the variables that Effort Calculator uses.

About the example

To illustrate how to use the two types of Effort Calculator variables to calculate the estimated costs of remediating applications in your Forward Path scenario, we will walk through an example scenario. We will build it up in stages, in an attempt to make it easy to understand.

Here is a screenshot of the output the example creates:

#	Application	Manufacturer	Version	Outcome	RAG	Cost	Application Complexity	Action RAG	Action Complexity
1	Analysts_Notebook	i2	6.01	Remediate	R	$5,000.00	Complex	A	Hard
2	iPassConnect	Sirocom	3.10	Redevelop	R	$2,000.00	Medium	R	Hard
3	avast! Antivirus	Alwil	4.7	Remediate	R	$1,400.00	Medium	G	Medium
4	Ixos	IXOS Software AG	5.0.0	Remediate	A	$1,400.00	Medium	G	Medium
5	StyleWriter	Editor Software	3.90	Remediate	R	$600.00	Simple	G	Medium
6	Hardcopy Pro	Desksoft	2.21	Stage UAT	G	$200.00	Simple	G	--
7	BBC Ticker	BBC	1.0.1.7	Stage UAT	G	$200.00	Simple	G	--

Note: The examples in this topic use the underscore (_) notation to break long lines into two or more lines. This is so that the example code snippets render correctly when included in a PDF. See the MSDN Library for more on this notation.

Initialize the variables

AppDNA includes a Forward Path scenario function called Initialize(). If present in the scenario, AppDNA automatically calls this at the start of the processing. We will use this to initialize variables that

we will use later in the scenario. For more information about the Initialize() function, see Grouped Forward Path reports.

Before the Initialize() function, we declare some variables that we will use throughout the script.

“‘ pre codeblock
‘ Declare variables for use throughout the script.
Private Dim vars As EffortCalculatorSettings
Private Dim testingPerHour As Decimal = 0
Private Dim remediationPerHour As Decimal = 0

```
Here is the Initialize() function:

‘‘‘ pre codeblock
Public Overrides Sub Initialize()

   ’ Get the Windows 7 Effort Calculator settings object.
   vars = Host.GetEffortCalculatorSettings(”Win7Module”)

   ’ Calculate the testing and remediation cost per hour.
   testingPerHour = vars.TesterStagerCostPerDay / _
      vars.NormalAppTestingHours
   remediationPerHour = vars.RemediatorCostPerDay / _
      vars.NormalAppTestingHours

   ’ Sort the report in descending order of cost.
   Settings.ApplicationSortBy = ”Cost”
   Settings.ApplicationSortDescending = true
End Sub
```

Notice that we are calculating the hourly testing and remediation costs. We do this by dividing the values stored in the variables that represent the tester or remediator cost per day by the value stored in the normal number of working hours in a day variable.

At the end of the Initialize() function, we set the sort order to be in descending order of the values in the Cost column. In this column we will display the calculated cost of remediating the application and staging it for UAT.

The main function

Here is the main ForwardPath() function. AppDNA automatically calls this once for every application that is selected when you run the report. Explanatory notes follow the example.

“‘ pre codeblock

Public Function ForwardPath(ByVal currentApplication _
As Application) As Output

Dim result As New Output()

’ We will use three custom columns.
result.CustomField1.Name = “Application Complexity”
result.CustomField2.Name = “Action RAG”
result.CustomField2.Value = _
currentApplication.Modules.Windows7.ActionRAG
result.CustomField3.Name = “Action Complexity”

’ Set the culture on the Cost column to US English,
‘ so that the US dollar currency symbol is used.
result.Display.Cost.Culture = “en-US”

’ Test the application’s main RAG status, because
‘ the remediation depends on this.
Select Case currentApplication.Modules.Windows7.RAG

```
1   Case Rag.Green
2
3      ’ The RAG is green, so no remediation is necessary
4      ’ and the application can be staged for UAT.
5      result.Outcome = ”Stage UAT”
6      result.RAG = RAG.Green
7
8      ’ No remediation is required, so the cost is of
9      ’ the staging only.
10     result.Cost = testingPerHour * vars.AppStagingHours
11     result.CustomField3.Value = ”--”
12
13     ’ Convert the unfriendly application complexity
14     ’ ”RAG” to a text.
15     Select Case currentApplication.Complexity
16        Case RAG.Red
17           result.CustomField1.Value = ”Complex”
18        Case RAG.Amber
19           result.CustomField1.Value = ”Medium”
20        Case RAG.Green
21           result.CustomField1.Value = ”Simple”
22     End Select
23
24  Case Rag.Amber
25
26     ’ The RAG is amber, so the application needs
```



```
27        ' remediation.
28        result.RAG = RAG.Amber
29        result.Outcome = "Remediate"
30
31        ' The cost calculation is more complicated,
32        ' so we will do it in a separate "GetCost()"
33        ' function.
34        result.Cost = GetCost(currentApplication, result)
35
36    Case Rag.Red
37
38        ' The RAG is red - we need to check the action
39        ' RAG to see if remdiation is possible.
40        result.RAG = RAG.Red
41
42        ' If the action RAG is red, the application
43        ' cannot be remediated.
44        If (currentApplication.Modules.Windows7.ActionRAG = _
45           RAG.Red) Then
46
47           result.Outcome = "Redevelop"
48           result.CustomField3.Value = "Hard"
49
50           ' Convert the unfriendly application complexity
51           ' "RAG" to a text and set an arbitrary
52           ' replacement/redevelopment cost.
53           Select Case currentApplication.Complexity
54              Case RAG.Red
55                 result.CustomField1.Value = "Complex"
56                 result.Cost = 3000
57              Case RAG.Amber
58                 result.CustomField1.Value = "Medium"
59                 result.Cost = 2000
60              Case RAG.Green
61                 result.CustomField1.Value = "Simple"
62                 result.Cost = 1000
63           End Select
64
65        ' The action RAG is not red, so remediation is
66        ' possible.
67        Else
68           result.Outcome = "Remediate"
69           result.Cost = GetCost(currentApplication, result)
70        End If
71
```



```
72    Case Else
73
74       ' Catch all for applications that have not been
75       ' analyzed or that are locked.
76       result.Outcome = "Unknown"
77       result.RAG = RAG.Unknown
78       result.CustomField1.Value = "--"
79       result.CustomField3.Value = "--"
80       result.Cost = 0
```

End Select

result.Display.SourcePath.Visible = false

ForwardPath = result

End Function

```
1  Notice that this function starts by setting up three custom columns (
       called CustomFieldn) - these are the three right-most columns in
       the screenshot of the output above. We use these as follows:
2
3  | Column  | Displays |
4  | ---| --- |
5  | CustomField1 | The application complexity. Forward Path stores this
       as a red/amber/green "RAG". We translate these values into Complex/
       Medium/Simple texts in the script. |
6  | CustomField2 | The application's action RAG. We get the value using
       the Application.Modules.Windows7.ActionRAG property.|
7  | CustomField3 | The complexity/difficulty of the application's
       remediation action. We will retrieve the value for this column later
        in the script.  |
8
9  The Cost column is automatically displayed in currency format. By
       default, Forward Path uses the currency symbol for the regional
       settings on the user's computer. In an international environment,
       this means that the currency symbol may vary depending on the
       settings on the device of the person viewing the report. (For
       example, it might display the euro sign for a user in France, the UK
        pound sign for a user in England, and the US dollar sign for a user
        in the United States.) In this example, we will therefore specify
       the US dollar symbol so that this will always be displayed
       regardless of the user's regional settings. To do this, we set the
       Culture property on the Cost column to "en-US", which indicates the
       United States.
10
```



```
11 The main body of the function consists of a Select Case statement that
       tests the application's Windows 7 RAG status and provides different
       processing depending on that status. Let's look at how we handle
       each value:
12
13 -  **Green RAG** - The application can go straight to UAC. So we
       calculate the cost of staging the application by multiplying the
       cost of testing per hour (which we calculated in Initialize()) by
       the Effort Calculator variable that stores the number of hours it
       takes to stage an application for testing. We set the action
       complexity to "--" because remediation is not necessary, and we use
       another Select Case statement to test the application's complexity
       and convert the unfriendly "RAG" value into a text.
14 -  **Amber RAG** - The application needs remediation. We call the
       GetCost() function to calculate the remediation cost. We will look
       at this shortly.
15 -  **Red RAG** - We first test the action RAG. If it is red, it means
       that the application cannot be remediated and needs to be
       redeveloped or replaced. We then use a Select Case statement to test
        the application complexity like we did for the green RAG. However,
       this time we set an arbitrary replacement cost based on the
       complexity of the application. For applications that can be
       remediated (that is, their action RAG is green or amber), we call
       the GetCost() function to calculate the remediation cost.
16 -  **Other RAG values** - We handle all other RAG values by using a
       Case Else statement. This will handle applications that have not
       been analyzed and those that are locked (unlicensed).
17
18 ## Calculate the remediation cost
19
20 Here is the GetCost() function, which we called in the main function to
        calculate the remediation costs of amber applications and red ones
       that can be remediated. Explanatory notes follow the example.
21
22 ``` pre codeblock
23 Private Function GetCost(app As Application, _
24    cols As Output) As Decimal
25
26    Dim remediationCost As Decimal = 0
27    Dim testingCost As Decimal = 0
28
29    ' 1. Using the triggered algorithms, get the
30    ' algorithm with the hardest action. We will use this
31    ' in our calculations.
32    Dim maxAlgorithm As TriggeredRule = _
```



```
33          (From r in app.TriggeredRules _
34          Where r.ModuleIdentifier = "Win7Module" _
35          Where r.Action.Complexity = ActionComplexity.Hard Or _
36          r.Action.Complexity = ActionComplexity.Medium Or _
37          r.Action.Complexity = ActionComplexity.Easy _
38          Order By r.Action.Complexity Descending _
39          Select r).FirstOrDefault()
40
41      ' 2. Display the algorithm's action complexity.
42      cols.CustomField3.Value = maxAlgorithm.Action.Complexity
43
44      ' 3. The remediation cost depends on the application
45      ' complexity.
46      Select Case app.Complexity
47
48          ' A complex application.
49          Case RAG.Red
50
51              cols.CustomField1.Value = "Complex"
52
53              ' The remediation cost also depends on
54              ' the complexity of the action. So we will
55              ' calculate the time based on the number of
56              ' hours held in the Effort Calculator matrix.
57              Select Case maxAlgorithm.Action.Complexity
58                  Case ActionComplexity.Easy
59                      remediationCost = remediationPerHour * _
60                          vars.ComplexAppEasyRemediationHours
61                  Case ActionComplexity.Medium
62                      remediationCost = remediationPerHour * _
63                          vars.ComplexAppMediumRemediationHours
64                  Case ActionComplexity.Hard
65                      remediationCost = remediationPerHour * _
66                          vars.ComplexAppHardRemediationHours
67                  Case Else
68                      remediationCost = remediationPerHour * _
69                          vars.ComplexAppMediumRemediationHours
70              End Select
71
72              If app.Modules.Windows7.ActionRAG = RAG.Amber Then
73
74                  ' Add the additional post-remediation testing
75                  ' because the application has an amber action RAG.
76                  testingCost = testingPerHour * _
77                      vars.ComplexAppTestingHours
```

```
78
79          End If
80
81       ' A medium-complexity application.
82       Case RAG.Amber
83
84          cols.CustomField1.Value = "Medium"
85
86          Select Case maxAlgorithm.Action.Complexity
87             Case ActionComplexity.Easy
88                remediationCost = remediationPerHour * _
89                   vars.NormalAppEasyRemediationHours
90             Case ActionComplexity.Medium
91                remediationCost = remediationPerHour * _
92                   vars.NormalAppMediumRemediationHours
93             Case ActionComplexity.Hard
94                remediationCost = remediationPerHour * _
95                   vars.NormalAppHardRemediationHours
96             Case Else
97                remediationCost = remediationPerHour * _
98                   vars.NormalAppMediumRemediationHours
99          End Select
100
101         If app.Modules.Windows7.ActionRAG = RAG.Amber Then
102
103            ' Add the additional post-remediation testing
104            ' because the application has an amber action RAG.
105            testingCost = testingPerHour * _
106               vars.NormalAppTestingHours
107
108         End If
109
110      ' A simple application.
111      Case RAG.Green
112
113         cols.CustomField1.Value = "Simple"
114
115         Select Case maxAlgorithm.Action.Complexity
116            Case ActionComplexity.Easy
117               remediationCost = remediationPerHour * _
118                  vars.SimpleAppEasyRemediationHours
119            Case ActionComplexity.Medium
120               remediationCost = remediationPerHour * _
121                  vars.SimpleAppMediumRemediationHours
122            Case ActionComplexity.Hard
```

```
123                remediationCost = remediationPerHour * _
124                   vars.SimpleAppHardRemediationHours
125             Case Else
126                remediationCost = remediationPerHour * _
127                   vars.SimpleAppMediumRemediationHours
128          End Select
129
130          If app.Modules.Windows7.ActionRAG = RAG.Amber Then
131
132             ' Add the additional post-remediation testing
133             ' because the application has an amber action RAG.
134             testingCost = testingPerHour * _
135                vars.SimpleAppTestingHours
136
137          End If
138
139    End Select
140
141    ' 4. Add the remediation and testing costs,
142    ' and the cost of staging for UAT.
143    GetCost = remediationCost + testingCost + _
144       (testingPerHour * vars.AppStagingHours)
145
146 End Function
```

The following notes relate to the numbers in the comments in the above example:

1. We use the current application's Windows 7 TriggeredRules property. This property is a collection of TriggeredRule objects, which represent all of the algorithms that the application triggered during analysis for Windows 7. From this collection, we get the algorithm that has the hardest remediation action. We will use this to calculate the cost of remediating the application.

2. We display the complexity (difficulty) of the algorithm's remediation action in CustomField3.

3. We then use a Select Case statement again to test the application's complexity. We will provide different processing for each complexity. Let's look at how we handle a complex application:

- First we use another Select Case statement to test the complexity (difficulty) of the action associated with the algorithm we retrieved in step 1. Then for each of the possible action complexities, we calculate the remediation cost by multiplying the remediation cost per hour (calculated in Initialize()) by the Effort Calculator variable that represents the time it takes to remediate a complex application of the corresponding action complexity.
- We then check whether the action RAG is amber – because this means that the application needs additional testing after the remediation has been implemented. If the action RAG is amber, we calculate the testing cost by multiplying the testing cost per hour (calculated in Initialize()) by

the Effort Calculator variable that represents the time it takes to test a complex application.

The code for medium-complexity and simple applications mirrors the code for the complex application, but each time we select the Effort Calculator variables for medium and simple applications, respectively.

4. Finally, we add the remediation and testing costs we calculated to the cost of staging the application for UAT and set this into the return value.

For an example that calculates the remediation costs by taking into account the actions associated with all of the algorithms triggered by the application, see the sample scenario that comes with AppDNA.

Grouped Forward Path reports

November 21, 2018

This topic provides an overview of the advanced Forward Path functionality that you can use to group applications by categories defined in the script (such as suitability for deployment on a particular platform) or by the AppDNA application group to which the applications belong. You can aggregate application values at the group level – for example, to create subtotals for each group – and create totals at the report level. This means, for example, that if application groups represent business units, you can create a Forward Path report that groups the applications by business unit and shows subtotals for each one.

Overview

The following image shows a snippet of a Forward Path report in which the applications have been grouped based on their RAG status for the Windows 7 and App-V reports. For each group, the total cost of remediation is shown, along with a count of the applications in the group. You can expand each group to view the applications inside. The total row at the top shows the totals for the entire report.

#	Group	Cost	Count	Link
	Total	$982.00	5	
1	App-V	$170.00	1	More information
2	Retire	$713.00	1	More information
3	Windows 7	$99.00	3	More information

#	Application	Manufacturer	Version	Outcome	RAG	Cost
1	Hardcopy Pro	Desksoft	2.21	Windows 7 OK	G	$33.00
2	Citrix ICA Client	Citrix Systems, Inc.	9.00	Windows 7 OK	G	$33.00
3	BBC Ticker	BBC	1.0.1.7	Windows 7 OK	G	$33.00

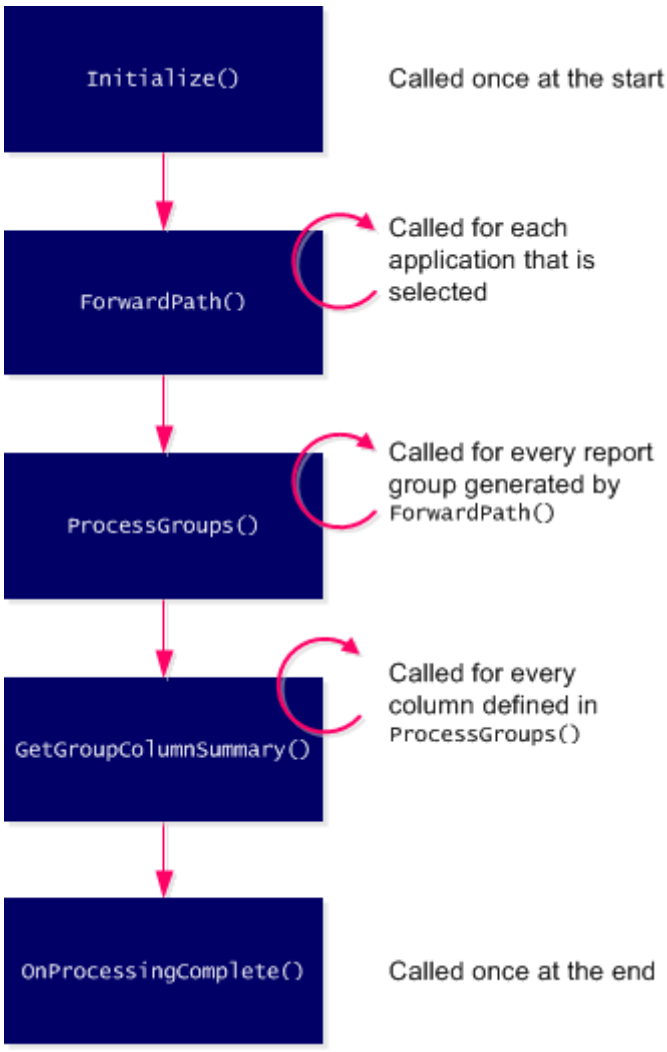
We will build up the Forward Path scenario that generated this report in the examples that follow. In order to make the examples as simple as possible, we will use a hard-coded remediation cost for each application. In real life, you would probably calculate this based on the application complexity and the remediation that is required. For an example that calculates costs in this way, see Use Effort Calculator variables in a Forward Path scenario.

The scenario functions

The scenario for a grouped Forward Path report typically implements the following standard Forward Path functions:

- Initialize() – AppDNA automatically calls this function once at the start of the script. Typically this function initializes variables.
- ForwardPath() – This is the standard function that all Forward Path scenarios must implement. AppDNA calls this function once for every application that is selected when you run the report. In a grouped Forward Path report, this function creates categories (called report groups) into which the applications are placed. The report groups can be created by the logic in the code or they can be based on application groups to which the applications already belong.
- ProcessGroups() – AppDNA calls this function once for every report group that is generated by the ForwardPath() function. This function defines the group-level report columns and the values they contain.
- GetGroupColumnSummary() – AppDNA calls this function once for each column defined in the ProcessGroups() function. Typically this function defines the report-level totals.
- OnProcessingComplete() – This is an optional function that AppDNA calls once after all the rest of the processing is complete. You can use this function to perform any final processing before the report is displayed.

The following diagram shows how AppDNA calls the functions when you run the report. The diagram is followed by the specification of each of the advanced functions, along with an example that together create the report shown in the Overview section above.



Note: Some of the examples in this topic use the underscore (_) notation to break long lines into two or more lines. This is so that the example code snippets render correctly when included in a PDF. See the
MSDN Library for more on this notation.

Initialize()

If specified in the scenario, AppDNA automatically calls the Initialize() function once at the start of the script. The Initialize() function must have the following signature:

```
1 Public Overrides Sub Initialize()
2     ' Enter your code here.
3 End Sub
```

In this example we will use the Initialize() function to initialize variables that we will use to store application values so that they can be aggregated at the group level. However, first we must declare the

variables that we want to use throughout the scenario. Because we will use these variables in more than one function, we will define them at the start of the script (before the Initialize() function), like this:

```
' Declare a Dictionary variable to store the remediation
' costs for each application in the group.
Private Dim costs As Dictionary(Of String, List(Of Integer)) _
   = New Dictionary(Of String, List(Of Integer))

' Declare string variables that store the names of the
' report groups.
Private Dim win7group As String = "Windows 7"
Private Dim appvgroup As String = "App-V"
Private Dim othergroup As String = "Retire"
```

In this example, we have declared a Dictionary variable called costs. See the MSDN Library for documentation of this standard .NET class. The dictionary variable can store a collection of keys and values. In this example, the key is a string (which we will use to store the report group name) and the value is a List of integers (which we will use to store the remediation costs for all the applications in the report group). See the MSDN Library for documentation of the List class.

As well as the dictionary, we have declared three string variables to store the names of the three report groups that we will create.

Now we are ready to implement the Initialize() function. Here it is:

```
Public Overrides Sub Initialize()
   costs.Add(win7group, New List(Of Integer))
   costs.Add(appvgroup, New List(Of Integer))
   costs.Add(othergroup, New List(Of Integer))
End Sub
```

In this example, we have simply added an item to our costs dictionary variable for each of our three report groups. We have specified the item keys using the three string variables that we declared earlier to store the names of the report groups.

ForwardPath()

The ForwardPath() function is the standard function that all Forward Path scenarios must implement. The ForwardPath() function must have the following signature:

```
Public Function ForwardPath(ByVal currentApplication _
   As Application) As Output
      ' Enter your code here.
```



```
End Function
```

In this example we will separate the applications into three report groups – we add applications that have a green Windows 7 RAG status to the “Windows 7” report group, we add applications that have a green App-V RAG status to the “App-V” report group, and we add the rest of the applications to a “Retire” report group. For each application, we will add a random hard-coded number to the dictionary to represent the cost of remediating the application:

```
Public Function ForwardPath(ByVal currentApplication _
   As Application) As Output

   Dim result As New Output()

   ' Is the application green for Windows 7?
   If (currentApplication.Modules.Windows7.RAG = RAG.Green) _
     Then
      result.Outcome = "Windows 7 OK"
      result.RAG = RAG.Green
      result.Cost = 33

      ' Add the application to the "Windows 7" group.
      result.ReportGroups.Add(win7group)

      ' Add the remediation cost to the dictionary variable.
      costs.Item(win7group).Add(33)
   Else

      ' Is the application green for App-V?
      If (currentApplication.Modules.AppV.RAG = RAG.Green) Then
         result.Outcome = "App-V OK"
         result.RAG = RAG.Green
         result.Cost = 170

         ' Add the application to the "App-V" group.
         result.ReportGroups.Add(appvgroup)

         ' Add the remediation cost to the dictionary variable.
         costs.Item(appvgroup).Add(170)
      Else

         ' The application is not green for Windows 7 or App-V.
         result.Outcome = "Not suitable for migration."
         result.RAG = RAG.Red
         result.Cost = 713
```



```
37
38          ' Add the application to the "Retire" group.
39          result.ReportGroups.Add(othergroup)
40
41          ' Add the replacement cost to the dictionary variable.
42          costs.Item(othergroup).Add(713)
43       End If
44    End If
45
46    result.Display.SourcePath.Visible = false
47
48    ForwardPath = result
49
50 End Function
```

Notice that we have used If … Then … Else statements to divide the applications into the three report groups based on the RAG status for the Windows 7 and App-V reports. We could have based the report groups on the application group to which the applications belong. A later example in this topic will show you how to do that.

Note: It is possible to add the same application to more than one group. If you do this, when your run the report, the application will appear under each group to which it has been added and its values will be aggregated into each group's totals. This may result in the application's values being added to the report total more than once. Depending on the report, this could potentially be misleading. It is up to you as the script author to ensure that applications are not added to more than one group unless this is your intention.

ProcessGroups()

If it is specified in the scenario, AppDNA calls the ProcessGroups() function for each report group generated by the ForwardPath() function. Typically you use the ProcessGroups() function to define the columns that appear at the group-level in the Forward Path report.

The ProcessGroups() function must have the following signature:

```
1 Public Overrides Sub ProcessGroup(group As _
2    ForwardPathReportGroup)
3       ' Enter your code here.
4 End Sub
```

Notice that the ForwardPathReportGroup object is passed into this function. This represents the current report group. It has two properties: Name, which is a String that stores the group's name, and

CustomColumns, which is a dictionary of strings. You use the CustomColumns property to specify the names of the columns that are shown at the group level and what they contain.

Here is an example:

```
Public Overrides Sub ProcessGroup(group As _
   ForwardPathReportGroup)

   ' 1. Define a report group column to show the total
   ' cost for the applications in the group and format it
   ' as currency.
   group.Columns.Item("Cost").Value = _
      costs.Item(group.Name).Sum()
   group.Columns.Item("Cost").Format = "{
 0:C }
 "
   group.Columns.Item("Cost").Culture = "en-US"

   ' 2. Define a report group column to show the number of
   ' applications in the group.
   group.Columns.Item("Count").Value = _
      costs.Item(group.Name).Count

   ' 3. Define a report group column that has a link to
   ' further information.
   group.Columns.Item("Link").Value = _
   "<a target=""_blank"" href=""http://www.google.com"">More
      information</a>"

End Sub
```

Notice that we have defined three columns:

1. This defines the Cost column, which shows the total remediation cost of the applications in each group. To get the total cost, we are using the List.Sum() method to aggregate all the cost values stored for the group in the costs dictionary variable. The List class has other aggregation functions that you can use to get the average, minimum, or maximum value (for example) stored for the group. See the MSDN Library for documentation of the List class.

   Notice that we have set the Format property on the column to {0:C} (which specifies that the value is a currency). And we have set the Culture property to a value of en-US to specify that the currency symbol is the US dollar symbol. See the Sort and format Forward Path reports for more on formatting the output.

2. This defines the Count column, which shows the number of applications in each group. This time we are using the List.Count() method to get the number of items (which represent applica-

tions) stored for the group in the costs dictionary variable.

3. This defines the Link column, which includes HTML code that defines a hard-coded hyperlink. This is an over-simplistic example that demonstrates that you can include HTML code in the column.

Note: AppDNA automatically generates a column that shows the group name. This is called the "Group" column.

GetGroupColumnSummary()

If it is specified in the scenario, AppDNA automatically calls the GetGroupColumnSummary() function for each column defined in the ProcessGroups() function, plus the auto-generated "Group" column (which stores the group name). The GetGroupColumnSummary() function must have the following signature:

```
Public Overrides Function GetGroupColumnSummary(groupColumnName _
   As String) As String
      ' Enter your code here.
End Function
```

Notice that the name of the column is passed into the function as a String and the function returns a string, which is the text that is inserted in the corresponding column in the report total row.

You use the GetGroupColumnSummary() function to define the report-level values. For example:

```
Public Overrides Function GetGroupColumnSummary(groupColumnName _
   As String) As String

   If groupColumnName = "Group" Then

      ' Put the text "Total" in the automatically-generated
      ' "Group" column.
      GetGroupColumnSummary = "<b>Total</b>"

   Else If groupColumnName = "Cost" Then

      ' Declare a variable to store the total cost.
      Dim sum As Decimal = 0

      ' Iterate through the costs variable to get the total cost.
      For Each key As String In costs.Keys
         sum += costs.Item(key).Sum()
      Next

```



```
        ' Format the total as currency.
        GetGroupColumnSummary = _
           String.Format(New _
              System.Globalization.CultureInfo("en-US"), _
              "{
  0:C }
", sum)

    Else If groupColumnName = "Count" Then

        ' Declare a variable to store the overall count.
        Dim count As Integer = 0

        ' Iterate through the costs variable to get the total
        ' count.
        For Each key As String In costs.Keys
           count += costs.Item(key).count()
        Next

        GetGroupColumnSummary = String.Format(count)

    Else

        ' Leave the "Link" column blank.
        GetGroupColumnSummary = ""

    End If

End Function
```

AppDNA calls this function once for each group column we defined in the ProcessGroups() function, plus the auto-generated "Group" column. We therefore use an If … Then … Else statement to test which column is being processed. Let's look at what we are doing for each column:

1. This is the auto-generated Group column. For this column, we are simply generating the text "Total". Notice that we have enclosed the text in tags. These are standard HTML tags that specify that the text should be rendered as bold. You can use any HTML code in any of the columns.

2. This is the Cost column. To get the total for the report, we declare a working variable. Then we iterate through all the items in the global costs dictionary variable and add their total values to the working variable, which we then return.

   The return value is a string. We have used the String.Format() method to format the cost value as a currency and we have used the CultureInfo class to specify the US dollar currency symbol.

See the MSDN Library for documentation on formatting strings.

3. For the Count column, we have used a similar technique to generate a total value for the report.
4. We have left the Link column blank.

This brings us to the end of the code in the scenario that was used to generate the Forward Path report shown at the beginning of this topic. Later in this topic we will learn how to create report groups based on the AppDNA application group to which the applications already belong.

OnProcessingComplete()

If it is specified in the scenario, AppDNA automatically calls the OnProcessingComplete() once after all the rest of the processing is complete. You can use this function to perform any final processing before the report is displayed.

The OnProcessingComplete() function must have the following signature:

```
Public Overrides Sub OnProcessingComplete()
   ' Enter your code here.
End Sub
```

Group by the AppDNA application group

In this section, we will change the scenario to group the applications according to the application group to which they already belong. If any application is not a member of a group, it will appear in an Ungrouped category.

Within the scenario, you can find out which group an application belongs to, through the Application.Groups property. Applications can belong to more than one group. Just as noted above, if you add all of the groups to the report, the application will appear under each group that it belongs to. Consequently, depending on how you author the script, there is a possibility that application remediation costs can be added into the report total more than once.

These functions contain detailed comments that explain how they work.

```
Public Function ForwardPath(ByVal currentApplication _
   As Application) As Output

   Dim result As New Output()

   If (currentApplication.Modules.Windows7.RAG = RAG.Green) Then
      result.Outcome = "Windows 7 OK"
      result.RAG = RAG.Green
```



```
    Else
       ' If the RAG for Windows 7 is not green,
       ' check if it's green for App-V
       If (currentApplication.Modules.AppV.RAG = RAG.Green) Then
          result.Outcome = "App-V OK"
          result.RAG = RAG.Green
       Else
          result.Outcome = "Not suitable for migration."
          result.RAG = RAG.Red
       End If
     End If

    ' We're temporarily using a hard-coded cost.
    result.Cost = 713

    ' Iterate through the groups to which the application
    ' belongs.
    For Each group As String In currentApplication.Groups

       ' Add the application to the corresponding report group.
       result.ReportGroups.Add(group)

       ' Check whether the group has already been added to our
       ' global dictionary variable.
       If costs.ContainsKey(group) Then

          ' Add the application's cost to the global variable.
          costs.Item(group).Add(713)
       Else

          ' Add the group to the global variable and then
          ' add the application's cost.
          costs.Add(group, New List(Of Integer))
          costs.Item(group).Add(713)

       End If
    Next

    ForwardPath = result

End Function

Public Overrides Sub ProcessGroup(group As ForwardPathReportGroup)

    If costs.ContainsKey(group.Name) Then
```

```
54        group.Columns.Item("Count").Value = _
55           costs.Item(group.Name).Count
56        group.Columns.Item("Cost").Value = _
57           costs.Item(group.Name).Sum()
58        group.Columns.Item("Cost").Format = "{
59  0,-10:C }
60  "
61        group.Columns.Item("Cost").Culture = "en-US"
62        group.Columns.Item("Link").Value = _
63        "<a href=""http://www.google.com"">More information</a>"
64     End If
65
66  End Sub
```

Hide the display of groups

Sometimes you may want to display a grouped report without the grouping. You can do this by using the ForwardPathReportSettings.DisplayGroups property. This property is automatically set to true when you include group handling code in your scenario. However, you can explicitly set it to false in your scenario to hide the display of the groups in the report.

The Settings object (which is of type ForwardPathReportSettings) is available throughout the scenario. Typically you set the property in the Initialize() function, like this:

```
1  Settings.DisplayGroups = false
```

To show the group again, simply comment this line out.

Sort and format Forward Path reports

August 2, 2018

This topic provides information about how you can control the sort order of the Forward Path report and the formatting of the application data.

Sort the application list

You can sort the application list in the Forward Path report based on the data in any of the columns. For example, you can sort the applications by their name, manufacturer, RAG status, or the values in any of the other columns.

You set the sort order using the Settings object, which is available throughout the scenario. The Settings object is of type ForwardPathReportSettings. If you look in the Property Explorer (on the right side of the Forward Path Logic Editor) you will see the properties on this object.

Typically you set the sort order in the Initialize() function. For example, the following sorts the applications by the values in the RAG column:

```
Public Overrides Sub Initialize()

    ' Sort the report on the RAG column.
    Settings.ApplicationSortBy = "Rag"

End Sub
```

By default, the sort is in ascending order (lowest to highest value). For RAG values, this is green, amber, red. To reverse this (to red, amber, green), add another line like this:

```
Settings.ApplicationSortDescending = true
```

In a grouped report, you can set the sort order of the groups like this:

```
Settings.GroupSortBy = "Cost"
```

By default, this sorts the groups on the values in the group Cost column in ascending order. You can change it to descending order, like this:

```
Settings.GroupSortDescending = true
```

Note: Conventions for sorting data vary from culture to culture. By default, the conventions defined by the user's regional settings are used. However, you can override this using the Culture property as explained below.

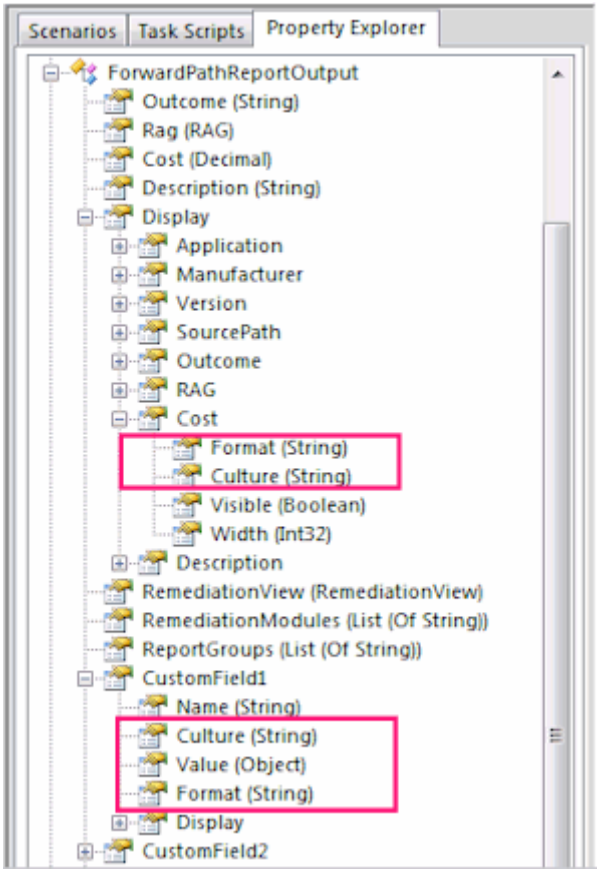
Format the column data

The following properties enable you to format report columns:

- **Format** – Use this to specify how you want the data formatted. For example, you can specify that numeric data is to be formatted as a percentage value or as a currency. You specify the formatting using a standard composite formatting string (only the zero index item can be used). We provide more information and examples below.
- **Culture** – By default the user's regional decimal separator and currency symbol is used when formatting currency and decimal values. However, if you are working in an international environment, this can mean that the currency symbol will vary according to the locale settings on

the end user's device. You can use the Culture property to override the default behavior (so that, for example, the currency symbol does not change depending on the regional settings of the device on which the report is being viewed). You specify the culture using a combination of the ISO 639 two-letter lowercase culture code associated with a language and the ISO 3166 two-letter uppercase subculture code associated with a country or region. For example, if you want to use the United States dollar symbol, you would specify the value as en-US. More information and examples follow.

The following screenshot of the Property Explorer highlights these properties for the standard Cost column and the first CustomField column. Notice that you find these properties for the standard columns (such as the Outcome, Rag, Cost, and Description columns) under the Display node. Whereas for the CustomField columns, the properties are under the CustomField itself.



Note: By default, the
Cost column is formatted as currency.

Set the Format property

You specify the formatting using a standard composite formatting string (only the zero index item can be used). For example, you can format a column as a percentage, like this:


```
result.CustomField1.Format = "{
 0:P }
 "
```

This multiplies the numeric value stored in the column by 100 and converts it to a string that represents a percentage in the output. For example, the value 0.05 is rendered as 5.00 % when the report is run in the UK using the default UK culture setting.

You can format a column as a currency value, like this:

```
result.CustomField1.Format = "{
 0:C }
 "
```

This displays the numeric value with two decimal places and the currency symbol. By default the currency symbol is taken from the user's regional settings – for example, £75.00 using the UK regional settings. You can override this using the Culture property.

Set the Culture property

You specify the culture using a combination of the ISO 639 two-letter lowercase culture code associated with a language and the ISO 3166 two-letter uppercase subculture code associated with a country or region (such as en-US for United States English).

For example, you can set the Culture property to Japanese like this:

```
result.CustomField1.Culture = "ja-JP"
```

If the column is a currency, it will have the Yen currency symbol.

You can set the culture to Spanish, like this:

```
result.CustomField1.Culture = "es-ES"
```

External data

August 1, 2018

External data is application compatibility and remediation data that originates outside of AppDNA.

AppDNA uses the external data during the analysis process, looking for matching applications in the external data sources. When there is a match between the application being analyzed and the application record in the external data source, AppDNA overwrites the application's standard RAG value or adds an overlay or icon to the standard RAG icon.

Note: The information in the external data sources has not been independently verified by Citrix.

You can configure:

- How AppDNA matches the external data with the applications in AppDNA - for example, whether the matching is case sensitive and how white space is handled.
- Additional reports to associate with the external data source.

Types of external data

Currently AppDNA provides two different types of external data:

Readiness lists. These are based on application compatibility lists provided by Microsoft to IT professionals. Applications that are marked as compatible in this list have been verified as working on the target platform by the software publisher or the Microsoft Windows logo testing program. AppDNA matches applications in AppDNA with applications in the list by the name, manufacturer, and version. By default this matching is case insensitive and ignores white space – but you can configure this. External data icons that derive from a readiness list indicate the following:

- **Green**. The application is marked as compatible with the target version of Windows.
- **Amber**. The application may require an upgrade in order to work on the associated version of Windows.
- **Red**. The application is not compatible with the associated version of Windows.

PCA (shim) databases. These are based on Microsoft's system application compatibility database, which is part of the Program Compatibility Assistant (PCA) that is built-in to the operating system. Unlike the readiness lists, AppDNA does not match applications based on the name, manufacturer, and version. Instead, AppDNA matches executable (.exe) files within the application to executable files listed in the database. External data icons that derive from a PCA database indicate the following:

- **Green.** The application has a compatibility issue that PCA will automatically shim. The remediation report views show the name of the shim.
- **Amber.** The application has a compatibility issue that is not considered severe. By default, this will result in a soft block PCA message at run time, which will interrupt the user experience.
- **Red.** The application has a severe compatibility issue that will result in PCA blocking it at run time (known as a hard block message).

External data sources

Data source	Applies to
Microsoft Windows 7 App Readiness List	Windows 7 SP1, Windows Server 2008 R2 SP1
Microsoft Windows 7 Shim Database	Windows 7 SP1, Windows Server 2008 R2 SP1
Microsoft Windows 8 App Readiness List	Windows 8, Windows 8.1, Windows Server 2012, Windows Server 2012 R2
Microsoft Windows 8 Shim Database	Windows 8, Windows 8.1, Windows Server 2012, Windows Server 2012 R2
Microsoft Windows 10 Shim Database	Windows 10, Windows Server 2016

To configure the external data source

1. From the AppDNA menus, choose Configure > External Data.

   Note: You need to be logged in as an AppDNA user who has the administrator role to be able to make changes on this screen.

2. In the list of external data sources in the External Data Administration screen, select the data source to configure.
3. In the Configuration section, select the options that you want to use when matching applications in the data source with applications in your AppDNA portfolio.
4. In the Data Source Context section, select the reports to which you want the external data source to apply.
5. Click Save to preserve your changes.
6. To apply your changes to your application portfolio, click Apply External Data on the main toolbar.

   This removes any existing external data journal entries for the affected applications and creates new external data journal entries. AppDNA automatically applies the external data to applications when they are first analyzed. Generally it is therefore only necessary to use this tool when you have explicitly made changes to the configuration of a data source.

Convert an external data entry to a journal entry

AppDNA uses the journal mechanism to handle external data. When AppDNA applies the external data to your application portfolio, it creates a special external data journal entry for each matching application and report combination. If necessary, you can delete individual external data journal entries in the Journal screen.

AppDNA can show only one icon that derives from the journal mechanism on an application's RAG status in the report views. This means that if you add a Compatible, Known issues, or Incompatible manual journal entry after an external data journal entry was created for the same application and report combination, the manual journal entry's icon overwrites the application's RAG status in the report views and the external data journal entry's icon is not shown. (If you want to add a manual journal entry – for example, to record testing notes – but you do not want it to overwrite the application's RAG status, use the Unknown journal entry type.)

You can convert an individual external data entry for an application to a standard journal entry. This means that the application's RAG status will be overridden by the corresponding compatibility (journal) icon.

1. Open the Application Issues or Application Actions report view for the relevant report.
2. Click the name of the application that has the external data entry.

   The Remediation report view for that application opens.
3. In the list of journal entries in the summary section of the report view, identify the external data entry that you want to convert.
4. In the column on the right, click Accept.

Configure External Data Source

August 1, 2018

1. From the AppDNA menus, choose Configure > External Data.
2. In the list of external data sources in the External Data Administration screen, select the data source that you want to configure.
3. In the Configuration section, select the options that you want to use when matching applications in the data source with applications in your AppDNA portfolio.
   - **Ignore Whitespace.** Select this check box if you want AppDNA to ignore extra space and tab characters when matching applications. This is the default. Clear this check box if you want AppDNA to take differences in white space into account when matching applications.
   - **Case Insensitive.** Select this check box if you want AppDNA to match applications case insensitively. This is the default. Clear this check box if you want AppDNA to match applications case sensitively.
4. In the Data Source Context section, select the reports to which you want the external data source to apply.
5. On the main toolbar, click Save to preserve your changes.
6. If you want to apply your changes to your application portfolio, click Apply External Data on the main toolbar.

Convert to Journal Entry

August 1, 2018

You can convert an individual external data entry for an application to a standard journal entry. This means that the application's RAG status will be overridden by the corresponding compatibility (journal) icon.

1. Open the Application Issues or Application Actions report view for the relevant report.
2. Click the name of the application that has the external data entry. This opens the Remediation report view for that application.
3. In the list of journal entries in the summary section of the report view, identify the external data entry that you want to convert.
4. In the rightmost column, click Accept.

Licenses

June 17, 2019

AppDNA integrates with the Citrix licensing system. All new AppDNA licenses are issued through www.citrix.com. However, if you are familiar with the Citrix licensing system, you will notice that there are some important differences between how you work with AppDNA licenses compared to how you work with the licenses for other Citrix products.

This topic provides an overview of the key features of AppDNA licensing, how it differs from the licensing of other Citrix products, and compatibility with earlier versions of AppDNA. This is followed by links to topics that provide more detailed information.

Key features of AppDNA licensing

- Citrix XenDesktop and XenApp Platinum retail licenses provide access to all AppDNA features. Platinum evaluation, demo, and not for resale licenses are not supported for activation.
- AppDNA licenses are applied to the AppDNA database. This means that if you have multiple AppDNA databases, each one is licensed separately.
- AppDNA licenses are tied to the machine on which the AppDNA licensing service is installed. (This is normally the machine on which the AppDNA server is installed.) If you move the AppDNA licensing service from one machine to another, you need to transfer the licenses for your AppDNA database.

Key differences with the licensing of other Citrix products

- You administer AppDNA licenses through www.citrix.com and the Configure AppDNA Environment wizard.
- The number of AppDNA licenses that are available and purchased relate to the number of applications and not the number of users. AppDNA licensing does not restrict the number of users that can use AppDNA. A Platinum XenApp and XenDesktop license makes AppDNA available for import, analysis and reporting of an unlimited number of applications.
- Internally AppDNA licensing is handled by the AppDNA licensing service rather than the Citrix license server. This means that you do not need to separately install the Citrix licensing components.
- Although it is possible to import AppDNA license files to the Citrix License Administration Console, this does not affect the licensing of AppDNA. Similarly, you do not administer AppDNA license files through the Citrix License Administration Console.
- For AppDNA Standard and Enterprise editions: Always download your AppDNA licenses separately from the licenses for other Citrix products.

Compatibility with earlier versions of AppDNA

- When you upgrade to the latest AppDNA release from AppDNA 6.0 or earlier, your old licenses are automatically upgraded to work with the Citrix licensing scheme when you upgrade your database.
- License files issued for AppDNA 6.0 and earlier (these have a .clf filename extension) cannot be used to directly activate AppDNA. When necessary, customers who have valid .clf license files can log on to www.citrix.com and download new Citrix licenses that match their existing entitlements.
- AppDNA licenses issued through www.citrix.com do not restrict the ability to install the AppDNA licensing service on a virtual machine. However, evaluation versions of AppDNA downloaded from www.citrix.com/tryit cannot be installed on a virtual machine.
- In all new installations, the AppDNA licensing service is installed on the same machine as the AppDNA server. However, AppDNA supports existing installations where the AppDNA licensing service is installed on a separate machine from the AppDNA server.
- Licenses issued through www.citrix.com are not compatible with AppDNA 6.0 and earlier.

Inspect

August 1, 2018

You can inspect your AppDNA licenses in the Configure AppDNA Environment wizard. The Inspect Licenses page in the wizard displays information about the licenses that are applied to your database. There are two tabs:

Details. The top part of this tab shows some general properties and the lower part shows the modules. The top part of the tab shows the following:

- **License ID.** This is the internal ID that the AppDNA licensing service assigns to the license.
- **Client ID.** This is the internal ID that the AppDNA licensing service assigns to the database.
- **Installation ID.** This is the internal ID that the AppDNA licensing service assigns to the AppDNA installation.
- **Subscription Advantage.** This shows the date that your Citrix Subscription Advantage membership expires. When you are a current member of this program, you are eligible to upgrade to the latest release of AppDNA.
- **Production Manager.** Enables Install Capture and Self-Provisioning to be used to package applications for App-V or XenApp. This requires additional software (that does not come with AppDNA) to be installed on the capture machine.

For each module, the following details are shown:

- **Module.** The module name. For a full list of the names of the modules and their reports, see the table below. For more information about the reports in each module, see Standard AppDNA reports.
- **Limit.** The number of applications for which you can view the application and remediation report views of the reports in this module.

  For XenApp and XenDesktop Platinum licenses, there is no limit to the number of applications for which you can view reports. For other retail (non-evaluation) licenses, applications are locked and reports are unavailable after you exceed the number of applications licensed.
- **Available.** The number of free application licenses.
- **Start.** The date the license started.
- **End.** The date the license expires. Reports will not be visible after this date.

License files. This shows the license files that have been applied to the database.

Module and report names

Module	Reports
Desktop Compatibility Manager (DCM)	Windows 10, Windows 8/8.1, Windows 7 SP1
SBC Manager	XenApp Hosted

Module	Reports
WebApp Compatibility Manager	Internet Explorer (IE), Firefox, Secure Web
Production Manager	Patch Impact
Compliance Manager	Security
Virtualization Manager	AppDisks, App-V
Server Compatibility Manager	Windows Server 2016, Windows Server 2012/2012 R2, Windows Server 2008 R2 SP1
Custom Reports	

To inspect your licenses:

1. From the Windows Start menu on the AppDNA server machine, choose Programs > Citrix AppDNA > Management Tools > Configure AppDNA.
2. In the first step in the Configure AppDNA Environment wizard, choose Licensing, and then click Next.
3. In the License Management step, choose Inspect, and then click Next.
4. In the Choose Database step, choose the database whose license you want to inspect, and then click Next.

Activate

August 1, 2018

The main reason you activate a license is when you move from trial mode to a XenApp and XenDesktop Platinum license.

When you activate a XenApp and XenDesktop Platinum license, it is imported into the AppDNA licensing service and applied to a specific AppDNA database.

Note: Activating a Platinum license automatically unlocks applications.

To activate a license file:

1. From the Windows Start menu on the AppDNA server machine, choose Citrix AppDNA > Management Tools > Configure AppDNA.
2. In the first step in the Configure AppDNA Environment wizard, choose Licensing.
3. In the License Management step, choose Activate.

4. In the Choose Database step, choose the database for which you want to activate a license.
5. To activate AppDNA using a XenDesktop or XenApp Platinum license, select Activate a XenDesktop or XenApp Platinum license.
    a) In the Machine box, enter the host name or IP address of the machine on which the XenDesktop or XenApp license server is installed.
    b) Enter the license server port in the Port box. By default, this is 27000. However, sometimes a different port is used. If in doubt, contact your XenDesktop or XenApp administrator.
6. If a System Check fails, refer to System Check issues.
7. Click Next to activate the license file.

    When the activation has finished, the wizard displays a message if you must unlock the applications in the Apply Licenses screen.

Apply

August 1, 2018

> **Note**
>
> Apply Licenses only applies to trial mode.

Use the Apply Licenses screen to unlock applications so that you can view them in the application and remediation views of the reports included with your license. Whether you need to do this depends on what type of license you have:

- If you have an evaluation or trial license, you can choose whether AppDNA unlocks the applications automatically during analysis or you unlock them yourself in this screen. When you evaluate AppDNA, you typically import more applications than you have licenses for, and then use the EstateView and Effort Calculator to get an overview of the state of your application portfolio. You can then unlock a few applications to get an understanding of the richness of the detailed information that AppDNA can provide about individual applications. You may find it useful to carefully choose which applications you want to unlock, rather than leave it to AppDNA to do this automatically.

To open the Apply Licenses screen:

- From the AppDNA menus, choose Manage > Licenses.

The Apply Licenses screen lists the applications in your portfolio and shows the number of licenses used and unused. There are columns for the reports in each of these modules and to the left of these,

there is a Licensing column. This shows whether the applications have been unlocked for that module – an empty check box indicates that an application is locked and a check mark indicates that the application is unlocked.

Select the Show all check box on the toolbar to swap between showing all applications for all modules and only those that are locked (the default).

For general information about AppDNA licensing, see Licenses.

To auto-unlock applications

Auto unlock unlocks a representative sample of your application portfolio based on the RAG status – aiming for 50% green, 25% amber and 25% red.

1. From the AppDNA menus, choose Manage > Licenses.
2. On the toolbar in the Apply Licenses screen, click Auto Unlock.

To unlock an application manually

Caution: Ensure that you do not unlock desktop applications for any web applications.

1. From the AppDNA menus, choose Manage > Licenses.
2. In the list of applications in the Apply Licenses screen, find the application or applications that you want to unlock.
3. For each application that you want to unlock, select the check box in the column that represents the reports that you want to view.
4. Click Manual Unlock on the toolbar.

Transfer

August 1, 2018

AppDNA licenses are tied to the AppDNA database and the machine on which the AppDNA licensing service is installed. If you need to move the AppDNA licensing service from one machine or environment to another, you need to transfer the licenses for all of your AppDNA databases as described below.

The AppDNA licensing service is automatically installed when you install a complete AppDNA server installation. Therefore if you need to move your AppDNA server installation from one machine to another, you need to transfer the licenses for your database. Moving your AppDNA licensing service is typically as simple as installing the complete AppDNA server installation on the new machine. A standalone AppDNA licensing service installation is available if required. However, Citrix recommends that

the AppDNA licensing service is on the same machine as the AppDNA server machine whenever possible.

Note: It is not necessary to transfer licenses if you simply want to move a database from a SQL Server installation on one machine to a SQL Server installation on another machine - provided there is no change in the location of the AppDNA licensing service.

Transferring a license involves the following steps:

1. **Export the license transfer token.** This exports a license transfer token from the database and saves it to a file. During this step you need to enter the name of the new AppDNA licensing service machine. After exporting the token, the database will be unlicensed until you complete the import steps.
2. **Import the license transfer token.** Run this step after the AppDNA licensing service is set up on the new machine. In this step, you import the license transfer token (which unlocks the database) and reactivate the license against the new AppDNA licensing service.

You need to do these two steps for each AppDNA database that is affected by the AppDNA licensing service move. Instructions are provided for each of these steps under separate headings below.

Export the license transfer token

1. From the Windows Start menu on the AppDNA server machine, choose Citrix AppDNA > Management Tools > Configure AppDNA.
2. In the first step in the Configure AppDNA Environment wizard, choose Licensing and then click Next.
3. In the License Management step, choose Transfer and then click Next.
4. In the Transfer License step, select the database whose license you want to transfer.

   If the database whose license you want to transfer does not appear in the list of databases, click Cannot see the database in the list to open the Enter Database Details dialog box. See Transfer License for more information about this dialog box.
5. Select Export, and then click Next.
6. Specify the name and location for the exported license token file.
7. Specify the name of the new AppDNA licensing service machine.

   The exported license token will be tied to this machine. You must specify this correctly, or the database will become permanently unusable. If you do not yet know the name of the machine on which the AppDNA license server will be installed, cancel the export now and start it again when you are sure of the machine name.

8. Click Next to export the license transfer token. AppDNA then asks you to confirm that you have specified the new AppDNA licensing service name correctly.
9. When the export has finished, click Close to exit the wizard.

Note: If you are moving the AppDNA database to a new SQL Server installation as part of the Licenses server move, the database must be backed up after the the license token has been exported.

You now need to import the license transfer token and, if necessary, reactivate the license, as explained next.

Import the license transfer token

Perform this step after you have moved the AppDNA licensing service to the new machine. Typically you do this by installing the complete AppDNA server installation on the new machine.

1. From the Windows Start menu on the AppDNA server machine, choose Citrix AppDNA > Management Tools > Configure AppDNA.
2. In the first step in the Configure AppDNA Environment wizard, choose Licensing and then click Next.
3. In the License Management step, choose Transfer and then click Next.
4. In the Transfer License step, select the database whose license you want to transfer.

   If the database whose license you want to transfer does not appear in the list of databases, click Cannot see the database in the list to open the Enter Database Details dialog box. See Transfer License for more information about this dialog box.
5. Select Import, and then click Next.
6. Specify the name and location of the exported license token file.
7. Specify the name of the new AppDNA licensing service machine. This must be the same as that specified in Step 7 of the export procedure.

   You can generally accept the default port number of 8079. See Import Transfer Token to Unlock Database for more information about this.
8. Click Next to import the license transfer token and unlock the database.
9. Click Next to complete the operation.

Typically you now need to add the database to the AppDNA web site, as described in Add an existing AppDNA database. However, this is not necessary if you moved only the AppDNA licensing service and not the AppDNA server.

Administer

June 17, 2019

This section provides documentation of a variety of features that you can use to administer and configure your AppDNA installation.

Quick links to topic sections:

- Users
- Roles
- Task locks
- Sites
- Databases
- AppDNA web site
- Fingerprints
- Configure AppDNA Environment wizard

Users

June 17, 2019

You can view, create, and modify user accounts for AppDNA and also configure user accounts for integrated login.

Quick links:

- About integrated login
- Add Users Manually
- Import users from Active Directory

Integrated Login

September 2, 2019

Integrated login is an optional feature that enables AppDNA users to be logged into AppDNA automatically using their Windows user account credentials. This means that the login screen is by-passed and users do not need to enter their user name and password.

Users who have integrated login accounts can turn off automatic login – for example, if they temporarily need to login with an administrator account to perform an admin task. To do this, clear the Enable Auto Integrated Login check box in Login settings.

> **Note:**
>
> You cannot log on to the AppDNA web client using an integrated login account.

Enable Integrated Login

To configure integrated login you must configure the AppDNA user account, and configure IIS.

Configure the AppDNA user account

You can import users individually from Active Directory (AD) or specify an AD Group from which user accounts will be imported automatically the first time they log in.

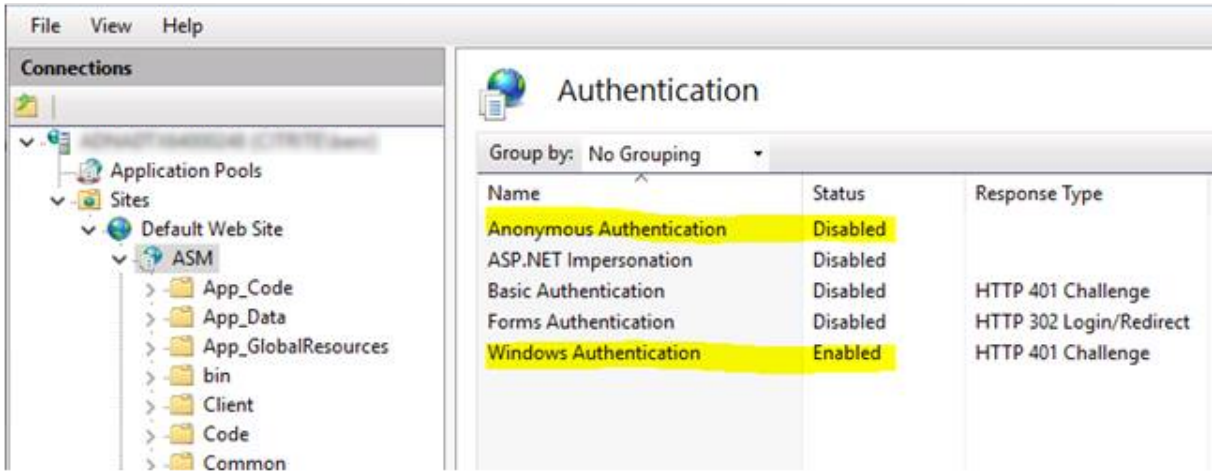
1. From the AppDNA menus, choose **Administration > User Management**.
2. In the User Management screen toolbar, click **Add From AD** in the toolbar, then find the required user or AD Group in the standard AD search and browse dialog.

> **Important:**
>
> To add AD Groups to AppDNA, the account running the AppDNA application pool in IIS must have permissions to read AD Group information from Active Directory. The default account *ApplicationPoolIdentity* can only discover individual user accounts.

Configure Internet Information Services

Use the Internet Information Services (IIS) Manager to configure the following IIS Authentication Settings for the AppDNA Web Application node:

- Anonymous Authentication—Disabled.
- Windows Authentication—Enabled.



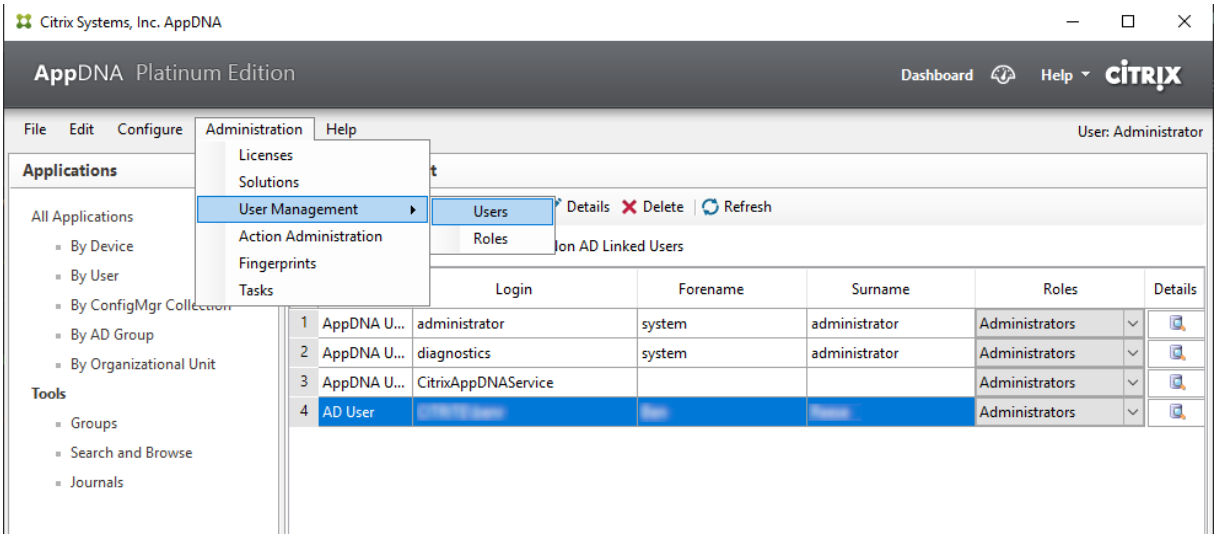
When IIS is configured this way and the Server Manager Console has the IE Enhanced Security Configuration enabled, users are prompted for their domain credentials when they navigate to the AppDNA web client, or the first time they view a report in the AppDNA desktop client. This is true for users using native (non-AD-integrated) AppDNA accounts, as well as those with AD-integrated AppDNA accounts.

To prevent users being prompted for their domain credentials in these situations, you can add the FQDN of the AppDNA server (for example `http://APPDNASERVER.domain.xxx`) to the *Local Intranet* zone, or add it to the *Trusted Sites* zone and set **Automatic logon with current username and password** on the Trusted sites zone.

Disable Integrated Login

To disable the integrated login feature in AppDNA:

1. From the AppDNA menus, choose **Administration > User Management > Users**.
2. Delete all AD User or AD Group related accounts in the linked users list.
3. Optionally, in IIS, reconfigure the AppDNAppPool to use an account that does not have permissions to read AD information. For example, use the default Application Pool Identity.



Integrated login FAQ

Does integrated login require contact with Active Directory?

Yes. The AppDNA web server needs to be able to contact Active Directory to either create a new user account in the AppDNA database, or to verify that a user linked to an AD Group has (or still has) membership of the specified group.

Does the AppDNA user account need to be updated when the Windows password changes?

No. AppDNA does not know or store the user's password. Authentication occurs by using secure Windows user tokens.

Can I change an existing AppDNA user account to an integrated login account?

No. Native AppDNA, and AD User or Group linked accounts, are mutually exclusive.

Add User

May 15, 2019

To add an AppDNA user account manually

1. From the AppDNA menus, choose **Administration > User Management**.
2. In the User Management screen toolbar, click **Add**.
3. On the first tab, type a username and password for the user.
4. Optionally, enter more detailed information for the user on the additional tabs.

5. If you want the user to take advantage of the integrated login feature, click **Add From AD** in the toolbar, then find the required user details in the standard AD search and browse dialog. For more information, see About integrated login.
6. After the user is added to the list, select a Role for the user from the list.
7. To add more details for the user click the **Details** icon. This opens General, Address, Telephones, and Organization tabs in the lower part of the screen.
8. When you have finished modifying any user details, click **Save** in the toolbar.

Import users from Active Directory

May 10, 2019

To import users from Active Directory, AppDNA must be connected to the Active Directory domain and be running with credentials that grant read access to the user accounts within that domain.

Active Directory groups authentication is supported. In order for Active Directory groups to be able to be added to AppDNA, the AppDNA server must be running as a domain user.

To import users from an Active Directory domain

1. From the AppDNA menus, choose **Administration > User Management**.
2. In the User Management screen toolbar, click **Add from AD**.
3. Complete the Windows Active Directory Object Picker. For information, refer to the Microsoft documentation.

   AppDNA searches Active Directory for matching users and adds them to the list of users in the User Management screen, and automatically saves them to the database.
   New users are automatically selected and the **Integrated Login** check box is selected for each one. This means that the users are automatically configured for integrated login.
4. After you change any of the default properties imported from Active Directory, or assign users to different roles, select the relevant user rows then click **Save**.

Login settings

May 15, 2019

The Settings dialog box contains general AppDNA options. To open this dialog box, choose **Edit > Settings** from the menus.

Enable Auto Integrated Login – Select this check box to use integrated login. This means that you will automatically be logged into AppDNA using your Windows user account credentials if your AppDNA administrator has configured integrated login for your user account. Clear this check box to prevent AppDNA from logging you in automatically using integrated login. For more information on integrated login, see Integrated login.

> **Note:**
>
> You cannot log on to the AppDNA web client using an integrated login account.

Clear Remembered Credentials – Click this button to clear the stored login name.

Click **Save** to preserve your changes.

Roles

August 1, 2018

Each AppDNA user is assigned a role, which controls the tasks the user can perform in AppDNA. By default, AppDNA has these roles with defined privileges that you cannot change:

- **Users** – Can select applications, view reports, and create application groups.
- **Administrators** – Has User privileges and can also perform all of the administration functions.

You might need to add custom roles for users such as third-party consultants, security analysts, or test engineers.

To manage roles:

- From the AppDNA menus, choose Administration > Roles.

The top part of the Role Management screen lists the existing roles. A check mark in the System Role column on the right side indicates a built-in role. You cannot change these roles.

The lower part of the screen lists all possible privileges and shows which ones are selected for the currently selected role. For non-system roles, select a check box to enable a privilege and clear a check box to disable a privilege. Click Save to commit changes.

Task locks

August 1, 2018

AppDNA places a lock on critical tasks so that another user cannot delete or modify the data while an analysis is being performed. Generally, AppDNA releases the locks at the end of the task. However, in certain circumstances (such as a restarting the server) this does not happen. You then need to release the locks manually.

To release task locks

1. From the AppDNA menus, choose Administration > Tasks.

   The Tasks screen shows the status of all of the imports and analyses being processed by all of the AppDNA clients connected to the same AppDNA web site.

2. On the toolbar, click Release Locks.

   Caution: The
   Refresh Report Data button on the far right side of the toolbar refreshes the report data for all applications and all active reports and combinations of OS images. This can take a long time, particularly if you have a large application portfolio. This button should be used only on the advice of Citrix AppDNA support staff.

Sites

August 1, 2018

A site is a named database and AppDNA web site combination. AppDNA uses a site to connect the AppDNA client to the specified database.

- You can specify the site you want to use when you log on to AppDNA, unless you use integrated or automatic login.
- After you are logged on, you can switch the database by using the Switch Site list in the lower left corner of the AppDNA screen.
- You can change the default site that appears for both of those controls.

To manage sites:

- From the AppDNA menus, choose Administration > Sites.

Add or remove a site

The ability to have multiple databases is useful for companies who want to test their web applications separately from their desktop applications, for example. Using multiple databases is also useful for

system integrators who need to test several customers' application portfolios at the same time. Typically every site uses a different database but all sites use the same AppDNA web site. When all sites use the same AppDNA web site, you need to upgrade all of the databases that they point at when you install a new version of AppDNA.

You can add or remove sites for the current AppDNA client machine and user.

To add a site

1. In the upper part of the Manage Sites screen, click Retrieve Available Databases.
2. Click the database on which you want to base the new site and then click Add Selection to List.

   AppDNA creates a new site based on this database.
3. Click the new site in the Site List, enter the site details and location, and then click Save.

To remove a site

- Select a site in the Site List, click Remove, and then click Save.

Deleting a site does not delete the associated database.

Define the default site

AppDNA connects to the default site. To change the default site:

- Select a site in the Site List, click Set Default, and then click Save.

Import or export a site

To standardize on the site names and configuration across multiple AppDNA client machines and users, click Export on the Manage Sites toolbar to export the sites. Then send the exported file to the other AppDNA users and ask them to import it on their own machines (click Import on the Manage Sites toolbar).

When you export a site, AppDNA stores in an XML file the configuration settings of all sites listed.

Add a site

August 1, 2018

You can configure AppDNA to connect to an additional site manually. The database must already exist. See Create an AppDNA database for information about creating a new database.

To add a site:

1. From the AppDNA menus, choose Administration > Sites.
2. In the upper part of the Manage Sites screen, click Retrieve Available Databases.

   This populates the Web Server Databases box with a list of available databases.

   If you cannot see the database in the list, you may need to add the database to your installation. (See Add an existing AppDNA database for more information about how to do this.)
3. Click the database on which you want to base the new site, and click Add Selection to List.

   This creates a new site based on this database.
4. Click the new site in the list of sites on the left side.
5. Click in the fields on the right side and enter the details.
   - **Name** – The unique name of the site. Citrix recommends that the name of the site reflects its use.
   - **Description** – Enter additional descriptive information here.
   - **AWS Path** – The path to the web site files.
   - **Database Identifier** – The database identifier expressed as Machine\Instance:Database, where Machine is the name of the machine that hosts the SQL Server installation, Instance is the SQL Server instance if a named SQL Server instance is in use (omit this and the backslash character (\) if a named instance is not in use), and Database is the name of the database. If you created the new site using the Add Selection to List button, you do not need to change this.
   - **URL** – The URL of the AppDNA Web site.
   - **Web server Type** – Enter IIS.
6. When you have finished, click Save to commit the changes.

You can define one site as the default site as described in Editing and Deleting Sites.

Edit and Delete

August 1, 2018

The default site is automatically selected on the AppDNA Logon screen, but you can select a different site to use when you log on if necessary. However, if you use integrated or automatic login, the Logon screen is not shown. If you want to change the site on the Logon screen, you therefore need to switch off integrated or automatic login in Login Settings in order to make the Logon screen appear. Alternatively, you can switch site while working in AppDNA by using the Switch Site pop-up list in the lower left corner of the main AppDNA screen.

Define the default site

1. From the AppDNA menus, choose Administration > Sites.
2. In the AppDNA Client Site List in the Manage Sites screen, select the site that you want to make the default site.
3. On the Site List toolbar, click Set Default.
4. Click Save on the main toolbar.

Rename a site

1. From the AppDNA menus, choose Administration > Sites.
2. In the AppDNA Client Site List in the Manage Sites screen, click the site that you want to rename.
3. Click in the Name field on the right side of the screen and edit the text as required.
4. Click Save on the main toolbar.

Delete a site

1. From the AppDNA menus, choose Administration > Sites.
2. In the AppDNA Client Site List in the Manage Sites screen, select the site you want to remove.
3. On the AppDNA Site List toolbar, click Remove.
4. On the main toolbar, click Save.

This removes the site from the list of available sites to connect to.

Note: Deleting a site does not delete the associated database.

Import and Export

August 1, 2018

You can export and import site settings. This is useful if, for example, you want to standardize on a site name and configuration across multiple AppDNA client machines and users. Simply set up the site on one machine and export the settings. Then send the exported file to the other AppDNA users and ask them to import it into AppDNA on their own machines.

Export site settings

1. From the AppDNA menus, choose Administration > Sites.
2. On the main toolbar in the Manage Sites screen, click Export.

3. In the Save As dialog box, give the export file a name that will help you identify it and select where you want to save it.
4. Click Save.

This downloads an XML file that stores the configuration settings of all the sites in the list.

Import site settings

1. From the AppDNA menus, choose Administration > Sites.
2. On the main toolbar in the Manage Sites screen, click Import.
3. In the Open dialog box, browse to the site file that was exported earlier.
4. Click Open.

Databases

August 1, 2018

A single AppDNA web site can handle multiple databases. Within AppDNA, you switch between databases by using sites. A site is a named database and AppDNA web site combination. You specify which site you want to use when you log on to AppDNA. AppDNA then uses the site to connect the AppDNA client to the specified database. Once you are logged on, you can switch database by using the Switch Site pop up list in the lower left corner of the main AppDNA screen.

When you use the Configure AppDNA Environment wizard to add a database, the wizard automatically creates a new site that you can use to connect to that database in AppDNA. The name of this site is displayed on the final page of the wizard. Make a note of the site name so that you can use it to connect to the database when you log on to AppDNA.

If you have multiple AppDNA clients connected to the same AppDNA web site, and you want all of the clients to access the new database, you need to add the new site on each client. See Sites for more information.

The remainder of this section describes how to create new databases and add existing databases to an AppDNA installation.

Create an AppDNA database

August 1, 2018

Note: The wizard creates new databases in the default database file location set in SQL Server. To store the database files in a different location, change the default location in SQL Server before you follow the steps below.

1. From the Windows Start screen or menu on the AppDNA server machine, choose Programs > Citrix AppDNA > Management Tools > Configure AppDNA.
2. In the first step in the Configure AppDNA Environment wizard, choose Reconfigure installation, and then click Next.
3. In the Existing Configuration step, click Add database, and then click Next.
4. In the Database creation step, specify the details as follows:
    - **Server name** – Enter this as Machine\Instance, where Machine is the name of the machine that hosts the SQL Server installation and Instance is the SQL Server instance if a named instance is in use. If a named instance is not in use, omit the backslash (\).
    - **Database name** – The name of the new database. Defaults to AppDNADB. If the database administrator has created an empty database for you to use, enter its name here. Otherwise enter a name that does not already exist within the SQL Server instance.
    - **Database authentication** – Enter the credentials for connecting to SQL Server to create the database.
        - **Windows authentication** – This type of authentication uses the logged on Windows user account when connecting to the database. The user account must have a password.
        - **SQL Server authentication** – Enter the user name and password.
5. Click Next and then, in the AppDNA web site credentials step, specify the credentials that the AppDNA web site is to use when connecting to the database after it is created. The options are:
    - **Use the built-in IIS application pool identity**.
    - **Use these credentials** – Specify the credentials to be used. For a production system, Citrix recommends an AppDNA-specific service account that has a password that does not expire (not the account used to create the database).
6. In the License Database step you can choose to activate a commercial AppDNA license or run AppDNA in trial mode for up to 30 days.
    - **Run in trial mode** – Select this option to run AppDNA in trial mode for up to 30 days. This provides no limit to the number of applications that you can import and for which you can view the EstateView and Effort Calculator reports views. However, you can only view the results in the other report views for up to five applications.
    - **Activate a XenDesktop or XenApp Platinum license** – Select this option to activate AppDNA using a XenDesktop or XenApp Platinum license.
        - **Platinum license server machine** – Enter the host name or IP address of the machine on which the XenDesktop or XenApp License Server is installed.
        - **Port** – Enter the license server port. By default, this is 27000. However, sometimes a different port is used. If in doubt, contact your XenDesktop or XenApp administrator.

7. Click Next to move to the System Check step. See System Check issues for information about the checks and what to do if they fail.
8. Click Configure to start the creation of the database. This takes some time. When the process has finished, a summary page appears. Note the name of the site. You will need it to log on to AppDNA.

Note: You can rename the site after you have logged into AppDNA. For more information, see Sites.

Add an existing AppDNA database

August 1, 2018

This topic provides step-by-step instructions for adding an existing database to your AppDNA installation – for example, an old database that is located on a different SQL Server machine. The wizard will automatically upgrade the database if necessary and create a site that you can use to connect to the database within AppDNA.

1. From the Windows Start screen or menu on the AppDNA server machine, choose Programs > Citrix AppDNA > Management Tools > Configure AppDNA.
2. In the first step in the Configure AppDNA Environment wizard, choose Reconfigure installation, and then click Next.
3. In the Existing Configuration step, click Add existing database, and then click Next.
4. In the Add Existing Database step, specify the details as follows:
    - **SQL Server instance** – Enter this as Machine\Instance, where Machine is the name of the machine that hosts the SQL Server installation and Instance is the SQL Server instance if a named instance is in use. If a named instance is not in use, omit the backslash (\).
    - **Authentication** – In this section you enter the credentials for connecting to the SQL Server database.
      Regardless which authentication method is in use, the user must have the bulkadmin server role and the db_owner database role.
        - **Windows authentication** – This type of authentication uses the logged on Windows user account when connecting to the database. The user account must have a password set.
        - **SQL Server authentication** – This activates two additional prompts in which you enter the user name and password.
5. Click Connect to populate the Database name drop-down list with the AppDNA databases that exist on the specified SQL Server instance.
6. Select the database that you want to add.
7. Click Next to move to the System Check step.

8. Click Next to start the process. If necessary, this upgrades the database to the current version of AppDNA.
9. When the process has finished, the wizard provides a summary page. Note the name of the site. You need to select this in the Site drop-down list in the Logon screen to connect to this database.

To connect to the new database in AppDNA, when you logon to AppDNA select the site whose name you noted in step 9.

Note: If necessary, you can rename the site after you have logged into AppDNA. For more information, see
Sites.

Web site

August 2, 2018

The AppDNA web site enables local intranet users to view reporting results from the AppDNA web client.

To change the web site credentials used to access the AppDNA database

If the password on the user account changes, you must update the credentials on the AppDNA web site. To do that, start the AppDNA configuration wizard, choose Reconfigure installation, choose Reconfigure system, select the database, and then, in the AppDNA web site credentials step, specify the credentials. Click through to complete the wizard.

Note: When necessary, this procedure automatically performs an IIS reset. This will make any other web sites hosted by IIS on this server unavailable for a brief interval.

For more information about working with the configuration wizard, see
Configure a server installation.

To change the web site port

Note: Although it is possible to change the AppDNA web site name, this is not recommended.

By default, the AppDNA web site uses port 8199. Citrix recommends that you change the port only if the default port is already in use. To do that, start the AppDNA configuration wizard, choose Reconfigure installation, choose Reconfigure system, select the web site, and then, in the Web site Configuration step, enter the new port number. Do not use a well-known port, such as ports in the range 0 – 1023, or 3500. Click through to complete the wizard.

When you change the web site port, the configuration wizard updates the AppDNA server site list (an XML file). If there are any AppDNA clients connected to the web site, you must copy the updated site list file to each client machine.

Note: Citrix recommends that you back up the client site list file before you perform the following steps.

1. On the AppDNA server machine, copy the SiteList.xml file, which is located in the following folder:

   `%ProgramData%\App-DNA\AppTitude`

2. Close AppDNA on each client machine.
3. Paste the SiteList.xml file that you copied in step 1 to the following folder on every client machine:

`%AppData%\App-DNA\AppTitude`

Change Web site Credentials

August 1, 2018

This topic provides instructions for changing the credentials that the AppDNA web site uses to access the database. You need to do this when the password on the user account changes.

Note: When necessary, this procedure automatically performs an IIS reset. This will make any other web sites hosted by IIS on this server unavailable for a brief interval.

1. Stop AppDNA clients before running the configuration wizard.

   Running the configuration wizard performs an IIS reset. An IIS reset terminates import and analysis sessions on running AppDNA clients connected to a web server that hosts both the AppDNA web site and database.

2. From the Windows Start menu on the AppDNA server machine, choose Programs > Citrix AppDNA > Management Tools > Configure AppDNA.
3. In the first step in the Configure AppDNA Environment wizard, choose Reconfigure installation, and then click Next.
4. In the Existing configuration step, choose Reconfigure system, and then click Next.
5. In the Edit configuration step, select Web site database credentials, and then click Next.
6. In the Choose database step, select the database whose credentials you want to change, and then click Next.

7. In the AppDNA web site credentials step, specify the credentials that the AppDNA web site is to use when connecting to the database after it is created. The options are:
   - **Use the built-in IIS application pool identity**.
   - **Use these credentials** – Specify the credentials to be used. For a production system, Citrix recommends an AppDNA-specific service account that has a password that does not expire (not the account used to create the database).

   See Web site credentials for more information.
8. Click Next to move to the System Check step. See System Check issues for information about the checks and what to do if they fail.
9. Click Configure to change the credentials.
10. Click Close to exit the wizard.

Web site credentials

August 1, 2018

In the AppDNA Web Site Credentials step in the Configure AppDNA Environment wizard, you specify the credentials that the AppDNA web site uses internally when connecting to the database. In a production system, Citrix recommends that you use an AppDNA-specific service account that has a password that does not expire.

Note: The AppDNA web site referred to here is part of the AppDNA product – it is not an external web site. The AppDNA web site enables local intranet users to view reporting results from the AppDNA web client. This does not require the installation of any AppDNA software.

Configure a local service account for me – (Available only if the SQL Server installation is on the local machine and the logged on user has permissions to create a Windows user account.) This option automatically configures a Windows user account called AppDNASvcAccount on the local machine. If this account does not already exist, the wizard creates it and generates a random password that does not expire. This option is the default if it is available and you are configuring a new AppDNA server installation or creating a new database.

If necessary, the generated password can be reset later by a local administrator in Control Panel > User Accounts. However, if the password is changed in this way, you then need to reconfigure the web site to use the new password.

Use these credentials – In this option you enter the credentials that you want the AppDNA web site to use internally when connecting to the database.

- **Authentication type** – This determines the authentication mechanism to be used when the AppDNA web site connects to the SQL Server database.
  - **Windows authentication** – In this type of authentication, the AppDNA web site uses the user account under which it is running to connect to the database. You can specify the user name and password of the account you want the AppDNA web site to run under. Citrix recommends that in a production system, this is a service account that has a password that does not expire. For an installation using trial mode, you can typically use the currently logged in user account.
    This account must have local administrator privileges as described in Prepare to install.
  - **SQL Server authentication** – This type of authentication uses specific SQL Server logon details, which you enter below.
- **User name** – If you chose SQL Server authentication, enter the user name that the AppDNA web site is to use to connect to SQL Server. If you chose Windows authentication, specify the domain-qualified Windows username – for example, domain\username.
- **Password** – If you entered a user name, you must enter the account password. If the user account does not have a password, you need to set up a password for the account before proceeding.

Change Port

August 2, 2018

By default, the AppDNA web site uses port 8199 if it is an IIS-based web site, and 7199 if you are using the built-in personal web server (PWS). Citrix recommends that you change the port only if the default port is already in use.

Note: Although it is possible to change the AppDNA web site name, this is not recommended.

1. From the Windows Start menu on the AppDNA server machine, choose Programs > Citrix AppDNA > Management Tools > Configure AppDNA.
2. In the first step in the Configure AppDNA Environment wizard, choose Reconfigure installation, and then click Next.
3. In the Existing Configuration step, choose Reconfigure system, and then click Next.
4. In the Edit Configuration step, select Web site, and then click Next.
5. In the Web site Configuration step, enter the new port number. Do not use a well-known port, such as ports in the range 0 – 1023, or 3500.
6. Click Next to move to the System Check step. If a check fails, refer to Troubleshoot.
7. Click Configure to start the reconfiguration of the web site.
8. Click Close to exit the wizard.

If there are any AppDNA clients connected to the AppDNA web site, you now need to update the client machines as explained next.

Update the client machines

AppDNA uses sites to make a connection between the AppDNA client and the AppDNA web site. Internally sites are defined in XML files. When you change the web site name or port, or both, the wizard updates the AppDNA server's XML site list. You can copy this to the client machine to update the client lists as described below.

Note: Citrix recommends that you back up the client site list XML file before you copy over the server file.

1. On the AppDNA server machine, copy the SiteList.xml file, which is located in the following folder:

   `%ProgramData%\App-DNA\AppTitude`

2. Close AppDNA on the client machine.
3. Paste the SiteList.xml file that you copied in step 1 to the following folder on every client machine:

   `%AppData%\App-DNA\AppTitude`

Upgrade from PWS to IIS

August 1, 2018

This topic provides instructions for upgrading from the built-in AppDNA personal web server (PWS) to the full IIS-based production web server.

1. Uninstall AppDNA.
2. Install and configure IIS. For system requirements, refer to System requirements for AppDNA 7.8.
3. Install AppDNA as explained in Install AppDNA.
4. Configure AppDNA as explained in the Configure a server installation. Be sure to select the Production Web Server option.
5. Follow the instructions in Add an existing AppDNA database to add your existing database to the new AppDNA web site.

Fingerprints

August 1, 2018

An application's fingerprint is a combination of its product name, manufacturer, version number, and the number of files and registry entries it has. When a desktop application is first imported into AppDNA, its fingerprint is stored. If the application is imported into AppDNA again, by default the application is considered the same if the fingerprint is identical or has not changed by more than 10%. This is significant because AppDNA licensing restricts the number of applications for which you can view reports.

Deleting an application from your portfolio does not delete the application's fingerprint. This means that if you import the same application again, AppDNA remembers it and considers it the same application (provided the fingerprint has not changed by more than 10%). If the application was unlocked when it was deleted, it remains unlocked when you re-import it and the same license is re-used. However, if the fingerprint has been deleted, the application is considered a different application and unlocking it uses a new license.

You can click the pencil icon in the Edit column to edit the application's display details, just like you can in the Application List. An exclamation mark (!) in the Manufacturer column indicates that the application's display name, manufacturer, or version has been changed. This does not affect the application's fingerprint itself.

To view and delete desktop application fingerprints:

- From the AppDNA menus, choose Administration > Fingerprints.

Note: If you delete an application's fingerprint, the next time you import that application, AppDNA will consider it to be a new application.

Configure AppDNA Environment wizard

August 1, 2018

You use the Configure AppDNA Environment wizard to do the initial configuration of AppDNA immediately after installing AppDNA or upgrading to a new version. Subsequently you use this wizard for advanced management and configuration tasks. Typically these are performed on the machine where the AppDNA web server is installed.

The options in the first step in the Configure AppDNA Environment wizard are:

Configure new installation – (New installation only.) Select this option if you have just installed AppDNA.

- **For a server installation**, this option sets up the AppDNA web server and web site, creates the SQL Server database, and enables you to activate your license or choose to run AppDNA in trial mode for 30 days.
- **For a client installation**, this option sets up the connection to the AppDNA web site and database.

Reconfigure installation – (Existing installation only.) Select this option if you have an existing AppDNA installation and you want to add a new or existing database, or edit your AppDNA server configuration.

Upgrade installation – (Existing installation only.) This option upgrades an existing AppDNA database to a new version of AppDNA. Select this option if you have installed a new version of AppDNA.

Important: When necessary, the wizard will perform an IIS reset. Therefore, stop AppDNA clients before starting the wizard. An IIS reset makes any other web sites hosted by IIS on this server unavailable for a brief interval. An IIS reset terminates import and analysis sessions on running AppDNA clients connected to a web server that hosts both the AppDNA web site and database.

Licensing – Select this option to inspect your AppDNA licenses, activate a new license, or transfer a license.

To open the Configure AppDNA Environment wizard

The Configure AppDNA Environment wizard opens automatically after you install AppDNA. To open it later:

- From the Windows Start > Programs screen or menu, choose Citrix AppDNA > Management Tools > Configure AppDNA.

Configure Client

August 2, 2018

In the Configure Client step in the Configure AppDNA Environment wizard, you configure the connection with the AppDNA web site.

Web site URL – Enter the URL of the AppDNA web site to which you want to connect. Specify the URL as follows:

```
http://server:port/AppDNA
```

Where the variables are as described in the following table.

Variable	Description
server	The AppDNA server host name or IP address.
port	The AppDNA web site port number. This is usually 8199.
AppDNA	The name of the AppDNA web site. This is usually AppDNA.

Example:

```
http://AppDNAserverMachine:8199/AppDNA
```

If you do not know what to enter here, contact your AppDNA administrator.

The wizard creates a site for each AppDNA database that is connected to the AppDNA web site that you specify here. A site is a named database and AppDNA web site combination. You specify which site you want to use when you log on to AppDNA. AppDNA then uses the site to connect the AppDNA client to the specified AppDNA web site and database. Once you are logged in, you can switch site by using the Switch Site pop up list in the lower left corner of the main AppDNA screen.

Web Server

August 1, 2018

The Web Server step in the Configure AppDNA Environment wizard creates an AppDNA web server based on IIS. You must already have IIS installed and configured on your machine.

Important: The wizard will perform an IIS reset as part of the configuration. Therefore, stop AppDNA clients before running the wizard. An IIS reset makes any other web sites hosted by IIS on this server unavailable for a brief interval. An IIS reset terminates import and analysis sessions on running AppDNA clients connected to a web server that hosts both the AppDNA web site and database.

Web Site Configuration

August 1, 2018

You use the Web Site Configuration step in the Configure AppDNA Environment wizard to change the AppDNA web site details.

The options are:

- **Web site name** – This shows the name of the AppDNA web site. By default, this is AppDNA. Although it is possible to change this, Citrix recommends that you do this only with direction from Citrix AppDNA support.
- **Port** – Enter the AppDNA web site port. The port defaults to 8199. You can change this to another port number, provided it is not a commonly used port (such as ports in the range 0 – 1023, or 3500). Citrix recommends that you change the port only if the default port is already in use.

Important: Changing the web site name or port (or both) does not automatically make corresponding changes to the references to the web site on any other machines on which the AppDNA client is installed. After making the changes in this wizard, update all client machines as described in Web site.

Choose Database

August 1, 2018

In the Choose Database step in the Configure AppDNA Environment wizard, you select the database that you want to use.

Database – From the drop-down list, select the database that you want to use. The list shows all of the databases for which the AppDNA web site has references. If you cannot see the database that you want to use in this list, you need to add the database to your AppDNA web site. See Add Existing Database for more information.

Backup (recommended) – (Upgrades only.) Select this check box (the default) if you want the wizard to automatically perform a backup of the database before upgrading it. Clear this check box if you have already performed a backup in SQL Server.

Error: The wizard cannot detect any AppDNA databases – What you need to do if the wizard displays this message depends on whether you have used AppDNA before and already have an AppDNA database:

- If you already have one or more AppDNA databases, click Close to exit the wizard. Then run the wizard again to add the database(s) to the web site. See Add Existing Database for step-by-step instructions.
- If you do not have an AppDNA database, click Close to exit the wizard. Then start the wizard again, and choose the Configure new installation option. This creates a new database.

Database Creation

August 1, 2018

AppDNA stores data in a Microsoft SQL Server database. The Database Creation step in the Configure AppDNA Environment wizard configures the database.

Note: The wizard creates the new database in the default database file location set in SQL Server. To store the database files in a different location, change the default location in SQL Server before you run the wizard.

Server name – Enter this as Machine\Instance, where Machine is the name of the machine that hosts the SQL Server installation and Instance is the SQL Server instance if a named instance is in use. If a named instance is not in use, omit the backslash (\). If the SQL Server uses a non-standard port, specify it using the Machine,Port notation, where Port is the custom port number.

Database name – The name of the new database. If the database administrator has created an empty database for you to use, enter its name here. Otherwise accept the default name, AppDNADB, or enter a name that does not already exist within the SQL Server instance.

Database authentication – The credentials for connecting to SQL Server when creating the database. The user account must have the sysadmin server role.

- **Windows authentication** – This type of authentication uses the logged on Windows user account when connecting to SQL Server. When using this type of authentication, the logged on user must have a Windows user account that has a password set.
- **SQL Server authentication** – Enter the user name and password to use to connect to SQL Server and create the database and database tables.

License Database

August 1, 2018

In the License Database step in the Configure AppDNA Environment wizard, you can activate a license or choose to run AppDNA in trial mode. In AppDNA, licenses are applied to the database and control which features you can use.

Run in trial mode – (Not available if the trial period has expired.) Select this option if you want to run AppDNA in trial mode for up to 30 days. This provides no limit to the number of applications that you can import and for which you can view the EstateView and Effort Calculator reports views. However, you can only see results in the other report views for up to five applications.

Activate a XenDesktop or XenApp Platinum license – Select this option to activate AppDNA using a Platinum license.

- **Platinum license server machine** – Enter the host name or IP address of the machine on which the Citrix License Server is installed.
- **Port** – Enter the license server port. By default, this is 27000. However, sometimes a different port is used. If in doubt, contact the XenDesktop or XenApp administrator.

Note:

- Activating your license may involve an IIS reset. Therefore, stop AppDNA clients before activating your license. An IIS reset makes any other web sites hosted by IIS on this server unavailable for a brief interval. An IIS reset terminates import and analysis sessions on running AppDNA clients connected to a web server that hosts both the AppDNA web site and database.
- You cannot activate a trial license on a database that already has a retail license activated.

Advanced

Use the Advanced button if the AppDNA license server is running on a different machine or if you need to specify a different port.

Server name or IP address – This defaults to localhost. If the AppDNA license server is installed on a separate machine, enter the host name or IP address.

Port – By default the AppDNA licensing service uses port 8079.

- If this is a new installation and this port is already in use, you must reconfigure the license server to use another port and enter that port number here. For more information, see Licensing issues.
- If the AppDNA license server has already been configured to use a different port, enter that port number here.

Add Existing Database

August 1, 2018

In the Add Existing Database step in the Configure AppDNA Environment wizard, you select an existing AppDNA database to add to your AppDNA web site. For example, you can use this feature to add an old database that is located on a different SQL Server machine to your AppDNA web site. The wizard will automatically upgrade the database if necessary and create a site that you can use to connect to the database within AppDNA.

Server name – Enter this as Machine\Instance, where Machine is the name of the machine that hosts the SQL Server installation and Instance is the SQL Server instance if a named instance is in use. If a named instance is not in use, omit the backslash (\). If the SQL Server uses a non-standard port, specify it using the Machine,Port notation, where Port is the custom port number.

Authentication – In this section you enter the credentials for connecting to SQL Server. Regardless which authentication method is in use, the user must have the bulkadmin server role and db_owner database role.

- **Windows authentication** – This type of authentication uses the logged on Windows user account when connecting to the database.
- **SQL Server authentication** – This opens two additional prompts:
  - **User name** – Enter the user name to use to connect to SQL Server.
  - **Password** – Enter the password to use to connect to SQL Server.

Connect – Click to connect to SQL Server. The wizard then lists the names of the AppDNA databases on the specified server in the Database drop-down list.

Database – Select the name of the database you want to add to your AppDNA installation. If necessary, the wizard will automatically upgrade the database.

Click Next to move to the next step.

For step-by-step instructions for opening the Add Existing Database step, see Add an existing AppDNA database

Existing Configuration

August 1, 2018

In the Existing Configuration step in the Configure AppDNA Environment wizard, you specify which aspect of your existing configuration you want to configure.

The options are:

- **Reconfigure system** – Choose this option to edit your AppDNA server configuration – for example, to reconfigure the web site to use a different port or to enter a new password for the user account that the AppDNA web site uses to connect to the database. When you click Next, the Edit Configuration step opens.
- **Add database** – Choose this option to create a new AppDNA database and a site that you can use to connect to it within AppDNA. When you click Next, the Database Creation step opens.

  Having multiple databases is useful if you want to test your web applications separately from your desktop applications, for example. Using multiple databases is also useful for system

integrators who need to test several customers' application portfolios at the same time. See Databases for more information.

- **Add existing database** – Choose this option to add an existing AppDNA database to your AppDNA installation. For example, you can use this option to add an old database that is located on a different SQL Server machine to your AppDNA web site. The wizard will automatically upgrade the database if necessary and create a site that you can use to connect to the database within AppDNA. When you click Next, the Add Existing Database step opens.

To open the Existing Configuration step

1. From the Windows Start > Programs menu on the AppDNA server machine, choose Citrix AppDNA > Management Tools > Configure AppDNA.
2. In the first step in the Configure AppDNA Environment wizard, choose Reconfigure installation, and then click Next.

Edit Configuration

August 1, 2018

In the Edit Configuration step in the Configure AppDNA Environment wizard, you specify whether you want to edit your web site database credentials or to reconfigure your AppDNA web site.

The options are:

- **Web site database credentials** – Select this option to change the SQL Server logon details that the AppDNA web site uses when connecting to the database. For example, use this option if you need to change the web site's SQL Server account password. When you click Next, the Web Site Credentials step opens.
- **Web site** – Select this option to reconfigure the AppDNA web site name or port, or both. When you click Next, the Web Site Configuration step opens.

To open the Edit Configuration step

1. From the Windows Start > Programs menu on the AppDNA server machine, choose Citrix AppDNA > Management Tools > Configure AppDNA.
2. In the first step in the Configure AppDNA Environment wizard, choose Reconfigure installation, and then click Next.
3. In the Existing Configuration step, click Reconfigure System, and then click Next.

License Management

August 1, 2018

The License Management step in the Configure AppDNA Environment wizard, provides a number of license management options.

Note: For an overview of AppDNA licensing, see
Licenses.

The options in this step are:

- **Activate** – Choose this option to activate Citrix licenses – for example, after buying a full license after running in trial mode. When you activate a license, it is imported into the AppDNA license server and applied to a specific AppDNA database. You can also activate additional licenses against a database that is already licensed. After you click Next, you choose the database to license and then you download and activate the license. See License Database for more information.
- **Inspect** – Choose this option to inspect the licenses that have been applied to a database. When you click Next, you choose the database whose licenses you want to inspect before moving to the Inspect License step.
- **Transfer** – AppDNA licenses are tied to the AppDNA database and the machine on which the AppDNA license server is installed. If you need to move the AppDNA license server from one machine or environment to another, you need to transfer the licenses for all your AppDNA databases using this option. When you click Next, the Transfer License step opens.

  It is not necessary to transfer licenses if you simply want to move a database from a SQL Server installation on one machine to a SQL Server installation on another machine – provided there is no change in the location of the AppDNA license server.
- **Advanced** – Choose this option to inspect the state of the AppDNA license server. When you click Next, you choose the database whose license server's state you want to inspect before moving to the Advanced Licensing step.

To open this step

1. From the Windows Start > Programs menu on the AppDNA server machine, choose Citrix AppDNA > Management Tools > Configure AppDNA.
2. In the first step in the Configure AppDNA Environment wizard, select Licensing, and then click Next.

Transfer License

August 1, 2018

You use the Transfer License step in the Configure AppDNA Environment wizard when you need to transfer an AppDNA database's licenses because, for example, you are moving your AppDNA server from one machine to another. For an overview of the license transfer procedure and when you need to use it, see Transfer Licenses.

The options in the Transfer License step are:

- **Database** – Select the database for which you want to transfer the license.

  If the database whose license you want to transfer does not appear in the list of databases, click Cannot see the database in the list. This opens the Enter Database Details dialog box, which is described below.

- **Export** – Select this option to export the transfer token from the database. When you click Next, the Export Transfer Token step opens.

  During this step you must provide the new AppDNA license server's machine name. It is important that you specify this correctly, because otherwise you will not be able to complete the transfer process. After exporting the token, the database will be unlicensed until you complete the import steps.

- **Import** – Select this option when you have already exported the transfer token from the database and you have moved the AppDNA license server to the new machine. When you click Next, the Import Transfer Token to Unlock Database step opens.

  In this option, you specify the transfer token that you previously exported and the location of the new license server. This unlocks the database so that you can view reports. The final step in this option is to go to www.citrix.com to reallocate your licenses to the new license server machine and then activate them within AppDNA. You will then be able to view all of the relevant reports again.

Enter Database Details dialog box

The Enter Database Details dialog box opens when you click Cannot see the database in the list.

The options are:

Server name – Enter this as Machine\Instance, where Machine is the name of the machine that hosts the SQL Server installation and Instance is the SQL Server instance if a named instance is in use. If a named instance is not in use, omit the backslash (\). If the SQL Server uses a non-standard port, specify it using the Machine,Port notation, where Port is the custom port number.

Database name – The name of the database in SQL Server.

Authentication – This determines the authentication mechanism for connecting to SQL Server. The options are:

- **Windows authentication** – This type of authentication uses the logged on Windows user account when connecting to the database.
- **SQL Server authentication** – This opens two additional prompts:
  - **User name** – Enter the user name to use when connecting to SQL Server.
  - **Password** – Enter the password to use when connecting to SQL Server.

Click OK to close the dialog box and use the selected database.

To open this step

1. From the Windows Start > Programs menu on the AppDNA server machine, choose Citrix AppDNA > Management Tools > Configure AppDNA.
2. In the first step in the Configure AppDNA Environment wizard, select Licensing, and then click Next.
3. In the License Management step, choose Transfer .

Export Transfer Token

August 2, 2018

The Export Transfer Token step is part of the license transfer procedure in the Configure AppDNA Environment wizard. In this step you export the database license token to a file, which you later import back into the database after you have installed the AppDNA license server on the new machine. See Transfer Licenses for an overview of the license transfer procedure.

The options are:

Transfer token file path – Specify the name and location for the exported license token file.

License server machine name – Specify the name of the new AppDNA license server machine. The exported license token will be tied to this machine. You must specify this correctly, or the database will become permanently unusable. If you do not yet know the name of the machine on which the AppDNA license server will be installed, cancel the export now and start it again when you are sure of the machine name.

Click Next to export the license transfer token. AppDNA then asks you to confirm that you have specified the new AppDNA license server name correctly. When you confirm, the Export License step opens.

Export License

August 2, 2018

The Export License step is part of the license transfer procedure in the Configure AppDNA Environment wizard. In this step AppDNA exports the license transfer token to the file you specified in the previous step. This locks the database. After this process has finished, click Close to exit the wizard.

You are now ready to move the AppDNA license server to the new machine. Typically you do this by installing the AppDNA server on the new machine.

You then need to import the transfer token into the database in order to unlock the database and reactivate the license against the new AppDNA license server location. For step-by-step instructions, see “Import the license transfer token” in Transfer Licenses.

Import Transfer Token to Unlock Database

August 1, 2018

The Import Transfer Token to Unlock Database step is part of the license transfer procedure in the Configure AppDNA Environment wizard. In this step you import the database license token that you previously exported.

The options are:

Transfer token file path – Specify the name and location of the exported license token file.

Server name or IP address – Specify the name or IP address of the new AppDNA license server machine. This must be the same as that entered in the License server machine name box during the export step.

Port – Enter the AppDNA license server port. This defaults to 8079 and typically you do not need to change it.

Click Next to import the license transfer token. This takes you to the Reallocate License File step.

Reallocate License File

August 1, 2018

In the Reallocate License File step, you reallocate your Citrix license file after importing the license transfer token into the database. This step does not appear when your license configuration does not need reallocating.

Important: If you are using an IIS-based web server, activating your license may involve an IIS reset. Therefore, stop AppDNA clients before activating your license. An IIS reset makes any other web sites hosted by IIS on this server unavailable for a brief interval. An IIS reset terminates import and analysis sessions on running AppDNA clients connected to a web server that hosts both the AppDNA web site and database.

Activate now – Select this option to reallocate your license now. Then log on to www.citrix.com to reallocate your license to the new AppDNA license server machine and download the new license file (see http://support.citrix.com/article/CTX126167 for instructions). To do this you must enter the name of the machine that hosts the new AppDNA license server.

- **License server machine name** – This shows the name of the AppDNA license server machine. Click Copy to copy this to the clipboard for pasting into www.citrix.com.
- **Location of license file** – Enter the name and location of the Citrix license file after you download it.

Important: If you purchased multiple Citrix products, make sure you download your AppDNA license(s) separately from the other product licenses.

I'll do this later – Select this option to allocate the license file later. You may not be able to view reports until you reallocate the license.

Inspect imported licenses – Click this button to view details of the licenses you are importing. The information corresponds to that shown in the Inspect Licenses option.

Import License

August 1, 2018

The Import License step in the Configure AppDNA Environment wizard is part of the license transfer procedure. In this step AppDNA imports the license transfer token you specified in the previous step and reactivates your license, if you chose to do that now. After this process has finished, click Close to exit the wizard.

Next steps

Typically you now need to add the database to the AppDNA web site. See Add an existing AppDNA database for step-by-step instructions.

Note: Adding the database to the web site is not necessary if you moved only the AppDNA license server and not the AppDNA server.

Advanced Licensing

August 1, 2018

The Advanced Licensing step in the Configure AppDNA Environment wizard shows the state of the AppDNA license server.

Server machine name – Specify the name of the AppDNA license server machine.

Port – Enter the AppDNA license server port. This defaults to 8079 and typically you do not need to change it.

Connect – Click to connect to the AppDNA license server. This populates the page with information from the AppDNA license server and lists the individual licenses.

To view the details of a specific license, select it in the list, select **View License** from the drop-down list and then click **Perform**. This displays detailed information about that license. This corresponds to the information shown on the Inspect License page.

To open the Advanced Licensing step

1. From the Windows Start > Programs menu on the AppDNA server machine, choose Citrix AppDNA > Management Tools > Configure AppDNA.
2. In the first step in the Configure AppDNA Environment wizard, choose Licensing, and then click Next.
3. In the License Management step, choose Advanced, and then click Next.
4. In the Choose Database step, choose the database, and then click Next.

Configuration progress

August 1, 2018

The Progress page in the Configure AppDNA Environment wizard shows the progress of the configuration task. How long the task takes depends on what is being configured and the resources available on the local machine. Configuring a new AppDNA server installation and creating a new database are long-running tasks and may take an hour or more. Upgrading a large database may also take a significant amount of time.

After the configuration is complete, the wizard displays a summary of the changes. For example, when you configure a new AppDNA server installation or create a new database, the wizard shows:

- The name of the new database.
- The type of authentication used to connect to the SQL Server installation to create the database.
- The name of the site, which you can use to connect to the database when you logon to AppDNA.
- If the wizard created a Windows user account for AppDNA to use internally, its name is shown. The wizard creates a random password for this user account. A local administrator can later change this in Control Panel > User Accounts. However, if the password is changed in this way, you then need to reconfigure the web site to use the new password.

Migrate

June 17, 2019

The topics in this section provide a step-by-step guide on how to use AppDNA for several common application migration scenarios. These topics include how to get started and describe how to use the many features of AppDNA to take advantage of its automated application compatibility testing, application deployment outcome modeling, application preparation and remediation, and virtualization processes.

Quick links to topic sections:

- Migrate Windows desktop and server applications
- Migrate to XenDesktop 7.0
- Migrate Windows applications to App-V 5.0
- Migrate applications without install routines

Migrate Windows desktop and server applications

August 1, 2018

The following steps guide you through a migration plan using AppDNA from beginning to end. These steps include our best practices for application migrations, as well as detailed information for using the AppDNA software as part of your migration plan.

Step 1. Determine the applications used in your environment

Discover your applications. To prevent unexpected delays in the migration plan, you must discover which applications are being used in your environment.

Perform an inventory and rationalization of those Windows applications using tools such as Lakeside SysTrack. It's important to monitor the environment over a 6 week to 2 month period at quarter and/or year end. This will not only identify any unmanaged applications which could be critical to business, but also tells you what applications are still being used, and whether you have duplicate applications with overlapping functions.

Step 2. Use AppDNA to integrate with Lakeside SysTrack database (optional)

Use the Discover Applications screen to configure AppDNA to integrate with Lakeside SysTrack.

Step 3. Rationalize discovered applications

When data about discovered applications is complete, the next step involves rationalizing discovered applications in the AppDNA Discover Applications screen. In this context, rationalization involves examining your inventory of applications and deciding which ones to keep and, if relevant, to import into AppDNA. The Discover Applications screen provides the raw inventory of Windows applications that have been tracked by Lakeside SysTrack.

Note: Click Discovered Applications for information about duplicate applications, installation, and usage statistics.

Step 4. Track discovery results

Track discovery results using the format that works best for you. Use an Excel spreadsheet, or if using Lakeside SysTrack, integrate it with the AppDNA software. The integration enables you to:

- Change the rationalization status from review to migrate or retire.
- Filter duplicate applications to easily determine which version to keep.
- Review installation and usage statistics.
- Link discovered applications with corresponding managed applications if using Microsoft Active Directory (AD) or Microsoft System Center Configuration Manager (Configuration Manager).

Step 5. Import AD and Configuration Manager data into AppDNA (optional)

To import your managed applications using the installation media that has been used to deploy them through AD or Configuration Manager, first load your AD and Configuration Manager data into AppDNA

using the Load AD and ConfigMgr Data wizard.

Decide whether to load the data directly or indirectly. You have the option to load AD and Configuration Manager data indirectly which enables the data to be extracted on the AD domain controller or Configuration Manager server separately from AppDNA. As a result, AppDNA users do not need to request administrator access to the AD and Configuration Manager data, plus the AD domain and Configuration Manager administrators do not need to install AppDNA.

Note: For best results, import both AD and Configuration Manager data. Typically AD provides rich data about organizational structure and Configuration Manager provides data about applications that are managed centrally.

Step 6. Distribute application discovery information for review and rationalize the application list

Review application discovery findings with the application owners in the business and go through a rationalization process. Decisions must be made as to which applications to keep, consolidate, or retire.

Track the decisions using the format that works best for you, a simple spreadsheet or within AppDNA.

Step 7. Start locating installation source files for non-managed applications

Locate installation source files for applications not being managed through AD or Configuration Manager. This always takes longer than most companies anticipate and can severely impact the migration plan.

1. Use the template file provided by AppDNA to define a list of applications to import.
2. To download a template file for importing a batch of applications:
    a) Choose Import > Applications from the side menu bar.
    b) Click Import from List on the toolbar in the Import Applications screen.
    The template Import List file is a comma-separated values (.csv) file used to define a list of applications to import into AppDNA.

Step 8. Import custom OS images into AppDNA

Import your own custom operating system (OS) images that are used in your environment. Although AppDNA comes with its own set of default OS images that can be used, importing your own images has the advantage that AppDNA can then base its analyses on the images you use in your environment and thus provide more accurate results.

Step 9. Group applications by criticality or business units

Group applications by criticality or business unit to ensure your migration plan focuses on what is most important in your organization and to make it easy to review and report on applications in the group separately from the rest of the portfolio.

Use the Manage Groups screen in AppDNA to create and manage application groups, analyze the applications in selected groups, and view reports for the applications in selected groups.

Step 10. Import non-managed (MSI, SFT, APPV) applications into AppDNA

Import non-managed applications, starting with the most critical ones or with the business unit that you plan on deploying to first, using the Import Applications screen.

Note: This process only imports what we refer to as the application's DNA into the AppDNA database. To check compatibility of an application against a given platform, the next step involves analyzing the data against a set of heuristic algorithms.
Use these tabs in the Import Applications screen:

Direct import. Use to import applications for which you have a Windows Installer (MSI) or App-V (SFT or APPV) package. This is the quickest way to get the application DNA into the database.

Install Capture. Use to import applications for which you do not have a Windows installer (MSI) or App-V (SFT or APPV) package. Install Capture uses a virtual machine to capture the details of the application's installation and configuration into an MSI which is then imported.

Tip: AppDNA splits importing the application data and analyzing the data into two separate processes. We recommend that you import applications during normal working hours and start an analysis in the evening when there is less traffic on the network. Additionally, only one analysis can be run at a time and reports cannot be generated during an analysis.

Step 11. Import non-managed applications (setup executable, scripts, file copies) into AppDNA

Import non-managed applications for which an MSI, SFT or APPV file is not available by using the Install Capture tab. Start with the most critical ones or with the business unit that you plan on deploying to first. Install Capture installs the application within a virtual machine and creates an MSI file that is then imported into AppDNA.
Note: Before you can import applications using Install Capture, you need access to a suitable virtualization technology. You must set up and configure a virtual machine that can communicate with the AppDNA client. For more information, see Configure Install Capture.
Tip: If an Install Capture installation requires the computer to be restarted, choose the I will restart my

computer later (or equivalent) option. The Install Capture will fail if you restart the virtual machine during the Install Capture process.

Step 12. Import managed applications into AppDNA

Import managed applications that you decide to keep into AppDNA. The application is installed using the installation media that has been used to deploy them through AD or Configuration Manager. After importing the application 'DNA' you can link applications discovered using Lakeside SysTrack with the managed applications that have been imported.
Note: Make sure you select appropriate installations (and not repair or uninstall installations). When a package has several installations, make sure you select only one of them, preferably one that has been deployed (that is, for which the count in the Users or Computers column is greater than zero).

Step 13. Link managed applications

If you have already imported applications into AppDNA prior to importing AD or Configuration Manager data, use the Link Managed Applications screen to link applications managed through AD and Configuration Manager with applications that have already been imported into AppDNA.
Note: This is an important step in the configuration of AD and Configuration Manager data. It enables AppDNA to create reports about the RAG status of the applications deployed to AD and Configuration Manager users, computers, groups, and organizational units. Managed applications that you import through the Managed Applications and Discover Applications screens are automatically linked.

Step 14. Check application compatibility against platforms and check interoperability between applications

After applications are imported, the next step is to analyze the applications against the platform for which you are checking compatibility. Use the Interoperability solution to check for conflicts between applications.

Step 15. Analysis report options

The results of the analysis are presented in a set of report views. You can access the report views from the Reports: Applications section of the side bar. This shows the module names in bold followed by their report names. Click a report name to see the report view options, which are the same for all reports. Each report view provides a different view onto the results.

Familiarize yourself with the reports and determine which format works best for the different levels of teams that will be reviewing the data.

To view reports for selected applications:

1. From the AppDNA side bar, choose Select > All Applications.
2. In the Application List screen, select the applications you want to include in the report.
3. On the toolbar in the Application List, select the report you want to view in the drop-down list and click View Report. Alternatively, from the AppDNA side bar, choose Reports: Applications > Module > Report > Report view, where Module, Report and Report view identify the report view that you want to see.

For a description of the report views and their intended audience, see
Report Views following this table.

Step 16. Prioritize applications based on RAG/criticality

Prioritize your applications based on the returned RAG status combined with your business needs. If you grouped your applications accordingly, use the group filter to view the report for applications belonging to the same group so you can focus on your most critical applications first and prioritize based on the RAG status within each group.

Citrix recommends using the Issues View report for the desired operating system to prioritize applications by RAG status as this view will enable you to also determine the type of remediation required, and therefore, the specialty required to remediate the issue, such as Developer or Packager.

- **Red.** Red applications are those with no workaround and should be retired and replaced, redeveloped, or hosted on a virtual desktop running the legacy operating system required. Review the application issues report for the individual application (click the application name to go to the detailed remediation report). Although an application may be marked as Red, the issue could be with a component that doesn't get used in your environment. Work closely with application owners to determine the best course of action and start planning how to proceed. If replacement and redevelopment are not options that can happen within the timescale of the migration, look for legacy alternatives such as hosting the application on a virtual desktop running the legacy OS.
- **Amber.** Amber applications require some form of workaround, such as shimming, OS build changes, or repackaging. Review the application issues report for the individual application. Click the application name to go to the detailed remediation report.
- **Green.** Green applications are ready for User Acceptance Testing (UAT).

Before pushing an application through to production, arrange for application owners to start testing the applications right away. If an application has issues, go back to the report for the individual application and review anything triggered. An application with a RAG of Green can trigger an algorithm, however, these mainly are related to Best Practice violations such as hardcoded paths. If you notice

it's a problem in your environment that needs to be addressed before applications progress to UAT, you can change the RAG associated with the algorithm.

Step 17. Assign Remediation Actions

Review report data for a given platform to get an idea of the types of problems the applications in your organization will have. You can then determine what type of remediation to assign to the applications.

This is useful for deciding whether it is more cost effective to make a change to the OS build or to fix each individual application. For example, a common issue that is encountered is Session 0 Isolation. You can instantly see which applications and how many applications are affected so you can make the right decision on a remediation option.

Step 18. Determine the person or group required to remediate the application

Determine the person or group required to remediate the application. Use the Issues View report to determine whether the application needs to be remediated by an in-house developer, packager, IT Administrator (for issues such as OS build changes) or a replacement by the ISV. Send the appropriate team or person the Remediation View report for the application. To view the Remediation View, go to the Application Issues View and click the link for the application name.

You can send the Remediation report in a Word, PDF, HTML, or MHT format.

Step 19. Send the application to UAT

Send the application to UAT when it has a Green or Amber RAG that requires functional testing, or when you are ready to test the application following remediation. Ensure that you involve your expert users during the UAT process.

Step 20. Deploy the application

If UAT is successful, deploy the application to the compatible operating system.

Report views

Report	Description	Used By
Application Issues	An overview of the status of the selected applications for the issues that have been encountered. Click the application name to drill down to the application's remediation report view, which provides detailed information about how to fix the issues.	IT Administrators, Developers, Packagers, Sequencers
Remediation View	A detailed view of the issues encountered in a specific application, along with information about the issue and suggested remediation options.	IT Administrators, Developers,Packagers, Sequencers
Application Actions	An overview of the status of the selected applications that provides the types of actions to take to fix the issues. Click the application name to drill down to the application's remediation report views.	IT Administrators, IT Management
Issues View	An overview of the various issues that have been encountered. For each issue, this report view provides a list of applications that are affected. Click the application name to drill down to the application's remediation report views.	IT Administrators, IT Management

Report	Description	Used By
Actions View	An overview of the various remediation action types that need to be implemented to fix the issues that have been encountered. For each action type, this report view provides a list of applications that are affected. Click the application name to drill down to the application's remediation report views.	IT Administrators, IT Management

Migrate to XenDesktop 7.0

August 3, 2018

AppDNA application migration software reduces the time, cost, and risk associated with Citrix XenDesktop migrations by automating application compatibility and overall application migration. AppDNA accelerates virtualization adoptions for XenDesktop, XenApp and Microsoft App-V with automated application testing, remediation, and virtualization processes. There is no one-size-fits-all answer to supporting a diverse application portfolio and evolving workforce, and it might seem confusing to determine the Citrix model that provides the best fit for your applications.

Making a decision on the Citrix model that works best for your workforce involves understanding the use cases, deployment models, and benefits of XenDesktop. You should start with Citrix Project Accelerator to get guidance on how to deploy XenDesktop successfully, including customized architecture recommendations and hardware requirements. You'll then be ready to leverage AppDNA to accelerate your XenDesktop migration.

AppDNA not only automates the manual application compatibility testing processes, but also enables you to model potential application deployment outcomes and to automate application preparation and remediation processes, which accelerate time to deployment. This topic explains how to configure and extend AppDNA to combine compatibility results and automation for outcomes based on the Citrix preferred technology stack as listed in the following tables.

Table 1. Citrix preferred technology stack

Citrix preferred technology stack	Requirements
XenDesktop 7.6 or 7.5 on Windows Server 2012 R2/2012 or 2008 R2 SP1	Suitable for hosting applications on Windows Server 2012 R2/2012 or 2008 R2 SP1; Suitable for delivering applications through Microsoft Remote Desktop Services technology
App-V 5.0 on Windows Server 2012 R2/2012 or 2008 R2 SP1, Windows 8.1/8/7 (32- or 64-bit)	Suitable for application virtualization; Suitable for Windows Server 2012 R2/2012, Windows Server 2008 R2 SP1, or Windows 8.1/8/7
XenApp 6.5 FP2 on Server 2008 R2	Suitable for hosting on Server 2008 R2;Suitable for x64 platform;Suitable for delivering applications using Microsoft Remote Desktop Services technology
VM Hosted Apps delivered by XenDesktop on Windows 8/7 (32- or 64-bit)	Not suitable for hosting on a Server 2008 R2 platform due to vendor support; Not suitable for delivering using Microsoft Remote Desktop Services technology; Suitable for hosting on Windows 8/7 desktop platform; Suitable for applications that might have heavy resource requirements and that usually require system isolation, must run standalone, and are infrequently accessed
Windows 8/7 (32- or 64-bit) virtual desktops delivered by XenDesktop 7	Not suitable for hosting on a Server 2012 or Server 2008 R2 platform due to vendor support; Not suitable for delivering using Microsoft Remote Desktop Services technology; Suitable for hosting on Windows 7 desktop platform; Suitable for users with more than two applications that have heavy resource requirements, must run standalone, and are frequently accessed; Suitable for applications that might need vendor licensing restrictions

Table 2. Citrix preferred technology stack (legacy platforms)

Citrix preferred technology stack (legacy)	Requirements
XenApp 5.0 on Server 2003	Not suitable for hosting on a Server 2008 R2 platform due to vendor support; Not suitable for hosting on an x64 platform due to application limitations; Suitable for delivering using Microsoft Remote Desktop Services technology
VM Hosted Apps delivered by XenDesktop 5 on Windows XP	Not suitable for hosting on a Server 2012, Server 2008 R2, or Windows 8/7 platform due to vendor support; Not suitable for delivering using Microsoft Remote Desktop Services technology; Suitable for hosting on a Windows XP desktop platform only; Suitable for applications that might have heavy resource requirements and that usually require system isolation, must run standalone, and are infrequently accessed

Get started

To start making decisions about the Citrix model that provides the best fit for your applications, perform each of the following steps.

Note: If you are new to AppDNA, consider using the AppDNA XenDesktop 7 Adoption solution wizard before continuing. That wizard provides an overview of adoption issues that will help you plan how to deliver applications after moving from non-Citrix systems to XenDesktop. After you review the report provided by the wizard, continue with the following steps.

Step 1. Discover applications through inventory and rationalization

To prevent unexpected delays in the migration plan, you must discover which applications are being used in your environment. Application discovery involves performing an inventory and then rationalizing that inventory to determine which applications to migrate or retire and which applications are duplicates that require review.

Performing an inventory and rationalization manually can be a very time-consuming task. There are several third-party products that can assist with inventory and rationalization.

It's important to monitor the environment over a 6 week to 2 month period at quarter and/or year end. This will not only identify any unmanaged applications which could be critical to business, but also tells you what applications are still being used, and whether you have duplicate applications with overlapping functions.

Step 2.Prepare your AppDNA environment

Setup and configure the AppDNA environment as outlined in the next section of this topic. This includes setting up the AppDNA and configuring it for use with the AppDNA Forward Path feature and AppDNA Execution Profile scripts used for the suggested solution.

The AppDNA Forward Path feature is a powerful business decision engine that is built into AppDNA and makes it possible to model different deployment scenarios and compare their impacts.

Step 3. Locate source media

You can directly import MSI and App-V (SFT, APPV) files.

Non-MSI files require the AppDNA Install Capture feature, which uses a virtual machine to capture the application into an MSI.

The AppDNA Self-Provisioning tool can also be used to capture non-MSI files. Self-Provisioning allows the capture process to be driven by an application expert who does not have access to AppDNA. The AppDNA administrator prepares and publishes control information that enables the application expert to perform the installation. The capture takes place on a separate machine (virtual, physical, or VDI) from AppDNA.

Step 4. Import Active Directory and/or Configuration Manager data

To import your managed applications using the installation media that has been used to deploy them through Active Directory (AD) and System Center Configuration Manager (Configuration Manager), first load your AD and Configuration Manager data into AppDNA using the https://docs.citrix.com/en-us/categories/legacy-archive/appdna.htmlLoad AD and ConfigMgr Data wizard.

Decide whether to load the data directly or indirectly. You have the option to load AD and Configuration Manager data indirectly which enables the data to be extracted on the AD domain controller or Configuration Manager server separately from AppDNA. As a result, AppDNA users do not need to request administrator access to the AD and Configuration Manager data, plus the AD domain and Configuration Manager administrators do not need to install AppDNA.

Note: For best results, import both AD and Configuration Manager data. Typically AD provides rich data about organizational structure and Configuration Manager provides data about applications that are managed centrally.

Step 5. Use the AppDNA reports

Reports for XenDesktop 7 migration, later in this section, guides you through the reports that you'll need to help you make decisions. It also covers the Forward Path scripts, which simplify decision making by modeling your business needs, providing solutions, and enabling you to automate the desired output for compatible applications, such as App-V 5.0 sequences and MSIs.

Step 6. Manage ongoing application evolution

As new applications enter the environment and as new service packs, patches and upgrades impact the environment, use AppDNA to manage and model the changes that affect applications and end users.

AppDNA configuration

Follow these steps to configure AppDNA for your XenDesktop 7.0 migration path solution.

Step 1. Create groups to organize applications by priority

Create AppDNA groups to organize the applications accordingly. This can be by priority or business unit. Once your group is created and applications are imported and analyzed, you can use the group to determine priority within the group based on the complexity of the problems encountered.

Step 2. Request access to AppDNA extensions

Request access to the AppDNA Extensions Podio site (https://citrix.podio.com/appdna-extensions). To request access to that site, email appdnafeedback@citrix.com.

Step 3. Create a VM for Install Capture (non-MSIs) and Forward Path automation

Create a Virtual Machine on supported technology to use with Install Capture and Forward Path. The VM should use the same operating system that the applications run on.

Install Capture is used as part of the import process to install and capture non-MSI applications before importing the application DNA into the AppDNA database.

Forward Path is used to determine outcomes for applications and automate processes, such as to create Microsoft App-V 5.0 sequences using MSI/EXE source media. The virtual machine should use the operating system that you are moving to.

Step 4. Configure a VM for capturing non-MSIs and Forward Path Automation

Review the general overview of the AppDNA Install Capture setup requirements. At the end of that overview are links to each of the following virtualization technologies. The details for configuring your VM vary depending on the underlying virtualization technology:

- XenServer
- Hyper-V
- vSphere
- VMware Workstation

The virtualization technology topics include instructions for creating a shared output folder. Additional folder configuration is required when using the App-V 4.6 to 5.0 Conversion profile:

1. On the host machine, create a source folder location that the VM has full access to, such as, \xxx.xxx.xx\AppDNA_Output\AppV_Convert\v5 (no spaces). Within the location created above, create one folder for each application, including the application's OSD and SFT files.
2. This will be your Source Folder that must be defined in the Replaceables tab of the execution profile: \xxx.xxx.xx\AppDNA_Output\AppV_Convert\v5\appname.

Step 5. Install Required Software on Virtual Machine

Install the software on the virtual machine that will be used to automate converting Microsoft App-V 4.6 sequences to Microsoft App-V 5.0 and to create Microsoft App-V 5.0 sequences.

Microsoft App-V 5.0
PowerShell 3.0

Step 6. Download Forward Path Scripts and Execution Profiles

From the AppDNA Extensions Podio site:

1. Click the Extensions button at the top of the page.
2. Click [FP] XenDesktop Decision.
3. Under Files, right-click the latest version of [FP] XenDesktop Decision.xml, select Save target as…, and then save the file to your local machine.

Step 7. Import Forward Path Scripts into AppDNA

To import the downloaded forward path script into AppDNA:

1. Log on to AppDNA and then choose Configure and Forward Path.
2. In the Forward Path Logic Editor screen, click the Import button.

3. Browse to the downloaded forward path script, select it, and click Open.
4. Click Import.
5. Click OK in the message that the file has been successfully imported,

Step 8. Import App-V 5.0 Sequencer Execution Profile into AppDNA

To import the App-V 5.0 Sequencer execution profile script into AppDNA:

Note: App-V 5.0 Sequencer.xml is installed by default to C:\Program Files\Citrix\AppDNA\Client\Execution Profiles or C:\Program Files (x86)\Citrix\AppDNA\Client\Execution Profiles.

1. Log on to AppDNA and then choose Edit and Settings.
2. In the Settings dialog box, click Install Capture.
3. Click the Execution Profile tab.
4. Click Import (in the lower part of the dialog box).

In the Load Profiles dialog box:

1. Browse to the location of the execution profile file downloaded from Podio.
2. Select the execution profile file that you want to activate and then click Open.

In the Execution Profiles tab, click the imported execution profile, click the Edit button, and then click the Replaceables tab.
Select the SourceFolder location replaceable, click the Edit button, enter the path to the Source files, and then click OK.
Select the TargetFolder location replaceable, click the Edit button, enter the path to the Target folder, and the click OK.
Click Save to preserve your changes and then close the Settings dialog box.

Reports for XenDesktop 7 migration

The following table lists the reports required for the XenDesktop 7 Migration path solution. These reports will provide the data you need to help with decision making.

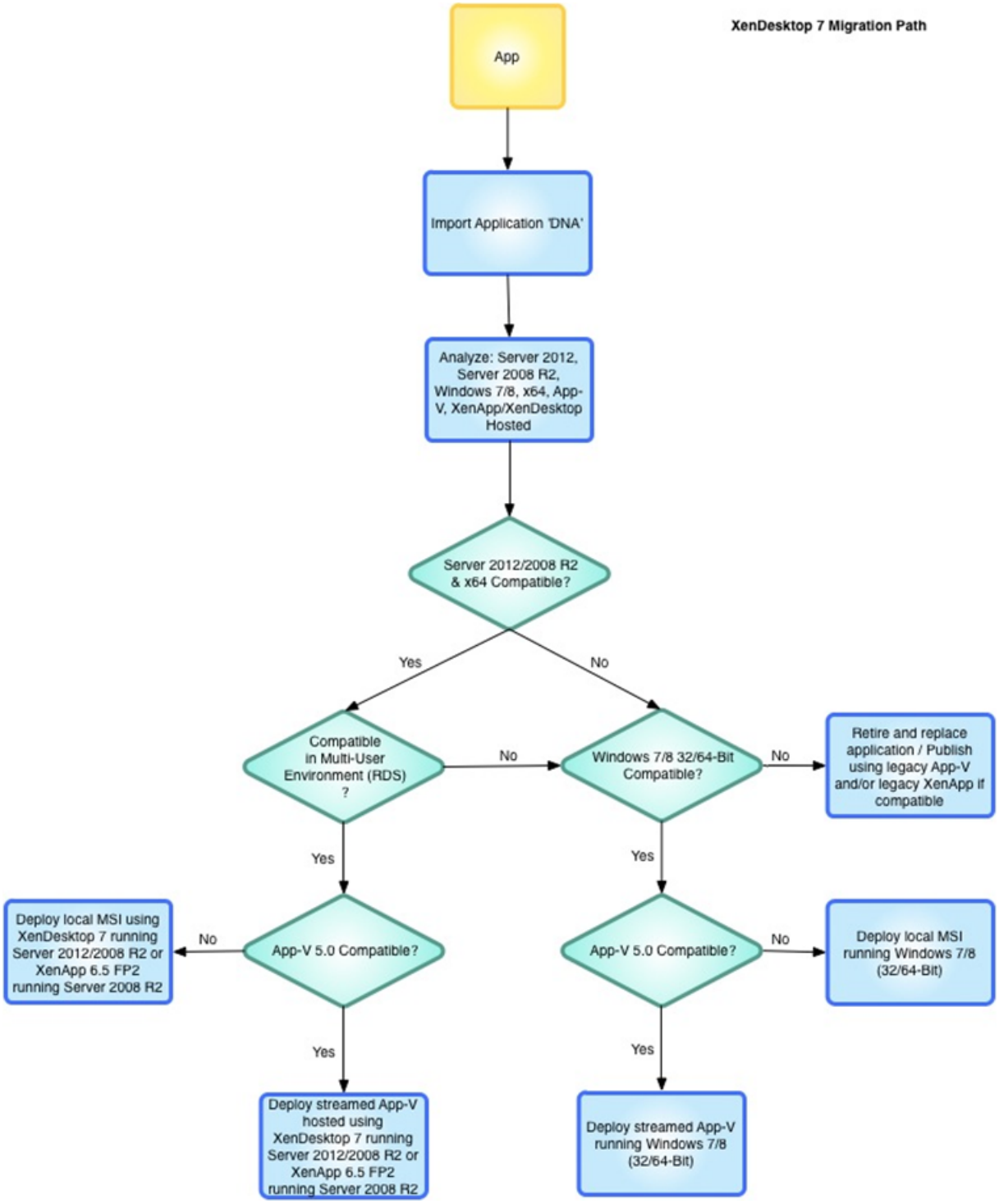
To access the reports, click Reports: Applications in the side bar.

Reports	Description
Forward Path	Reflects scenarios based on organizational decisions and used to run automation task scripts based on the results. For example, when preparing a migration to Windows 7, you could create a Forward Path scenario to determine which applications are suitable for deployment as App-V packages, which should be deployed to the desktop, and which require redevelopment. The following are potential outcomes for the Forward Path script: Deploy streamed App-V hosted using XenDesktop 7 running Server 2012/Server 2008 R2 or XenApp 6.5 FP2 running Server 2008 R2; Deploy local MSI hosted using XenDesktop 7 running Server 2012/Server 2008 R2 or XenApp 6.5 FP2 running Server 2008 R2; Deploy streamed App-V hosted using XenDesktop 7 running Server 2012; Deploy local MSI hosted using XenDesktop 7 running Server 2012; Deploy streamed App-V hosted using XenDesktop 7 running Server 2008 R2 or XenApp 6.5 FP2 running Server 2008 R2; Deploy local MSI hosted using XenDesktop 7 running Server 2008 R2 or XenApp 6.5 FP2 running Server 2008 R2; Deploy local MSI running Windows 7/8 (32/64-Bit); Deploy streamed App-V running Windows 7/8 (32/64-Bit); Retire and replace application/Publish using legacy App-V and/or legacy XenApp if compatible. **Note:** You can further customize the Forward Path script to tailor it to your environment and business decisions. The App-V 5.0 Sequencer Execution Profile is assigned as a Task Script to automate App-V 5.0 sequencing for outcomes that include App-V as a good candidate for application streaming. To access the Forward Path report, choose Reports: Applications > Forward Path. To select the XenDesktop 7 Decision report, click Change Scenario and then click the drop-down list.

Reports	Description
Overview Summary	Provides a high-level dashboard view of the state of your application portfolio across all active reports. For each of the selected applications, it shows the overall RAG (red, amber, green) status for each of the active reports. On the rows that relate to an application, you can click the RAG icons to access the Remediation report views for that application. These provide the remediation details required for the application to work using the selected platform.
XenApp Hosted/TS	Tests desktop applications for suitability for deployment in a shared server-hosted environment.
App-V 5.0	Tests desktop applications for suitability with Microsoft Application Virtualization (App-V) 4.5, 4.6 SP1, or 5.0.
Windows 8/7	Determine compatibility of the application on the target OS by going directly to the specific OS report. Drill down to the specific issues, download automated fixes, and get more information on how the application can be remediated.
Server 2008 R2/2012	Determine compatibility of the application on the target OS and dive deeper into the details for what is required to remediate the application by clicking on the application name to go straight to the full remediation details.

XenDesktop 7 Migration steps

This section outlines the recommended process for XenDesktop 7 migrations using AppDNA after your AppDNA environment is set up. The XenDesktop 7 migration path is summarized in the following flowchart.



Step 1. Import application DNA

For applications in an MSI format, select Import & Analyze > Applications > Direct Import.

For application in a Non-MSI format, select Import & Analyze > Applications > Install Capture.

Step 2. Analyze the application

Analyze the application against App-V, XenApp Hosted, Windows 7/8, 64-bit, Server 2012, and Server 2008 R2. Use the Interoperability solution to determine which applications can be hosted on the same server.

Step 3. Run Forward Path script (XenApp Hosted)

Run the forward path script [FP] XenDesktop 7.0 Decision.xml to check the compatibility of the applications against XenApp Hosted, Server 2012, Server 2008 R2, x64, Windows7/8 and App-V. The script also provides a review of the suggested outcome based on the Citrix preferred technology stack.

To access the Forward Path report, choose Reports: Applications > Forward Path. To select the XenDesktop 7 Decision report, click Change Scenario and then click the drop-down list. To run task scripts, click Evaluate Tasks.

Step 4. Remediate

Review the Forward Path report data and prioritize applications based on RAG status:

- Green – Run task scripts (if one is available) and proceed to UAT.
- Amber – Check the detailed remediation report to determine what has been flagged and if it needs remediation or functional testing.
- Red – Check the detailed remediation report to determine if the component flagged can/should be remediated and the action you want to take (i.e. re-development, local installation on Windows 7/8, deploy on legacy platform, retire and replace). Check the Overview report for the best fit platform.

Click the application name within the Forward Path report to go directly to the detailed remediation data for an application.

Step 5. Run Task Script

Run the task script for applications that are suitable for App-V 5.0 Sequencing.

Click the Start button to run automated task scripts and create App-V 5.0 sequences.

Step 6. Test output for applications compatible for App-V 5.0

Locate the output files created and perform functionality testing.

Step 7. Submit to User Acceptance Testing

Submit the applications to User Acceptance Testing (UAT), ensuring that the expert users are involved in the process.

Tap into the extendable features of AppDNA by using the Forward Path script to send an email to the group performing UAT when an App-V 5.0 sequence is ready to be deployed and tested.

Step 8. Find alternatives for applications not compatible with a given solution

For applications that are not compatible (cannot be remediated or remediation is deemed too costly) use AppDNA to determine if a legacy deployment option is more cost effective. Otherwise, consider retiring and replacing the application.

Use the Overview Summary report to get a quick look at the best possible platform for your application.

Compatibility checks

The following table lists the potential outcomes based on compatibility check results.

Compatibility check results	Outcomes
Compatible with App-V, Windows Server 2012/2008 R2 (including x64) and XenApp Hosted (and Windows 7/8)	Deploy streamed App-V hosted using XenDesktop 7 running Windows Server 2012/2008 R2 or XenApp 6.5 FP2 running Server 2008 R2
Compatible on Windows Server 2012/2008 R2 (including x64) and XenApp Hosted (and most likely Windows 7/8)	Deploy local MSI hosted using XenDesktop 7 running Windows Server 2012/2008 R2 or XenApp 6.5 FP2 running Windows Server 2008 R2
Compatible on App-V, Windows Server 2012 (including x64), and XenApp Hosted (and most likely Windows 7/8)	Deploy streamed App-V hosted using XenDesktop 7 running Windows Server 2012
Compatible on Windows Server 2012 (including x64) and XenApp Hosted (and most likely Windows 7/8)	Deploy local MSI hosted using XenDesktop 7 running Windows Server 2012

Compatibility check results	Outcomes
Compatible with App-V, Windows Server 2008 R2 (including x64) and XenApp Hosted (and most likely Windows 7/8)	Deploy streamed App-V hosted using XenDesktop 7 running Windows Server 2008 R2 or XenApp 6.5 FP2 running Windows Server 2008 R2
Compatible on Windows Server 2008 R2 (including x64), and XenApp Hosted	Deploy local MSI hosted using XenDesktop 7 running Windows Server 2008 R2 or XenApp 6.5 FP2 running Windows Server 2008 R2
Compatible on Windows 7/8 (32/64-Bit)	Deploy local MSI running Windows 7/8 (32/64-Bit)
Compatible on App-V, Windows 7/8 (32/64-Bit)	Deploy streamed App-V running Windows 7/8 (32/64-Bit)
Compatible on Windows Server 2012 or 2008 R2, but not compatible for multi-user environment (RDS) and not compatible for Windows 7/8 (32/64-Bit)	Retire and replace application/Publish using legacy App-V and/or legacy XenApp if compatible.
Not compatible on Windows Server 2012/2008 R2, Windows 7/8 (32/64-Bit)	Retire and replace application/Publish using legacy App-V and/or legacy XenApp if compatible

Migrate Windows applications to App-V 5.0

August 3, 2018

This topic explains the steps required to use AppDNA to migrate your Microsoft Windows applications to Microsoft App-V 5.0 or from Microsoft App-V 4.6 to 5.0.

Get started

To start making decisions about the Citrix model that provides the best fit for your applications, perform each of the following steps.

Step 1. Discover your applications

To prevent unexpected delays in the migration plan, you must discover which applications are being used in your environment. Use the integration features within AppDNA to discover applications being used in your environment (Lakeside Software SysTrack) and to import your managed applications using the installation media that has been used to deploy them through Active Directory (AD) or Microsoft System Center Configuration Manager (Configuration Manager) integration.

Step 2. Perform inventory and rationalization

To perform an inventory and rationalization of the Windows applications used in your enterprise, use tools such as Lakeside SysTrack. It's important to monitor the environment over a 6 week to 2 month period at quarter and/or year end. This will not only identify any unmanaged applications which could be critical to business, but also tells you what applications are still being used, and whether you have duplicate applications with overlapping functions.

Step 3. Prepare your AppDNA environment

Setup and configure the AppDNA environment as outlined in the next section of this topic. This includes setting up the AppDNA and configuring it for use with the AppDNA Forward Path feature and AppDNA Execution Profile scripts used for the suggested solution.

The AppDNA Forward Path feature is a powerful business decision engine that is built into AppDNA and makes it possible to model different deployment scenarios and compare their impacts.

Step 4. Locate source media

You can directly import MSI and App-V (SFT, APPV) files.

Non-MSI files require the AppDNA Install Capture feature, which uses a virtual machine to capture the application into an MSI.

The AppDNA Self-Provisioning tool can also be used to capture non-MSI files. Self-Provisioning allows the capture process to be driven by an application expert who does not have access to AppDNA. The AppDNA administrator prepares and publishes control information that enables the application expert to perform the installation. The capture takes place on a separate machine (virtual, physical, or VDI) from AppDNA.

Step 5. Import AD and/or Configuration Manager data

To import your managed applications using the installation media that has been used to deploy them through Active Directory (AD) and System Center Configuration Manager (Configuration Manager), first load your AD and Configuration Manager data into AppDNA using the Load AD and ConfigMgr Data wizard.

Decide whether to load the data directly or indirectly. You have the option to load AD and Configuration Manager data indirectly which enables the data to be extracted on the AD domain controller or Configuration Manager server separately from AppDNA. As a result, AppDNA users do not need to request administrator access to the AD and Configuration Manager data, plus the AD domain and Configuration Manager administrators do not need to install AppDNA.

Note: For best results, import both AD and Configuration Manager data. Typically AD provides rich data about organizational structure and Configuration Manager provides data about applications that are managed centrally.

Step 6. Choose the appropriate scenario

For Windows applications that are already sequenced using Microsoft App-V 4.6, follow the process using the Microsoft App-V 4.6 to App-V 5.0 Decision forward path script.

For Windows applications that are already imported into Citrix AppDNA, or applications that have not been sequenced or imported into Citrix AppDNA, follow the process using the Microsoft App-V 5.0 Decision forward path script.

Step 7. Use the AppDNA reports

Reports for migration of Windows applications to App-V 5.0, later in this section, guides you through the reports that you'll need to help you make decisions. It also covers the Forward Path scripts, which simplify decision making by modeling your business needs, providing solutions, and enabling you to automate the desired output for compatible applications, such as App-V 5.0 sequences and MSIs.

Step 8. Manage ongoing application evolution

As new applications enter the environment and as new service packs, patches and upgrades impact the environment, use AppDNA to manage and model the changes that affect applications and end users.

AppDNA configuration

Follow these steps to configure AppDNA for the migration of Windows applications to App-V 5.0.

Step 1. Create groups to organize applications by priority

Create AppDNA groups to organize the applications accordingly. This can be by priority or business unit. Once your group is created and applications are imported and analyzed, you can use the group to determine priority within the group based on the complexity of the problems encountered.

Step 2. Request access to AppDNA scripts

Citrix has a library of non-supported Forward Path and Execution Profile scripts that are available for download. The scripts are customized to model business decisions around applications and to automate processes (such as Microsoft App-V 5.0 application sequences and MSIs).

This solution uses an execution profile script that ships with AppDNA as well as the following scripts which are available for download:

- [EP] Converter_App-V4.6_to_App-V5.0
- [FP] Microsoft App-V 4.6 to App-V 5.0 Decision
- [FP] Microsoft App-V 5.0 Decision

To access the scripts, set up a Podio account and send an email to appdnafeedback@citrix.com requesting access to the AppDNA Extensions Podio site.

Step 3. Create a VM for Install Capture (non-MSIs) and Forward Path automation

Create a Virtual Machine on supported technology to use with Install Capture and Forward Path. The VM should use the same operating system that the applications run on.

Install Capture is used as part of the import process to install and capture non-MSI applications before importing the application DNA into the AppDNA database.

Forward Path is used to determine outcomes for applications and automate processes, such as to convert Microsoft App-V 4.6 sequences to Microsoft App-V 5.0 or create Microsoft App-V 5.0 sequences using MSI/EXE source media. The virtual machine should use the operating system that you are moving to.

Step 4. Configure a VM for capturing non-MSIs and Forward Path Automation

Review the general overview of the AppDNA Install Capture setup requirements. At the end of that overview are links to each of the following virtualization technologies. The details for configuring your VM vary depending on the underlying virtualization technology:

- XenServer
- Hyper-V
- Microsoft Virtual Server
- vSphere
- VMware Workstation
- VMware Server

The virtualization technology topics include instructions for creating a shared output folder. Additional folder configuration is required when using the Microsoft App-V 4.6 to Microsoft App-V 5.0 Execution Profile:

1. On the host machine, create a source folder location that the VM has full access to, such as, \xxx.xxx.xx\AppDNA_Output\AppV_Convert (no spaces).
2. Within the location created above, create one folder for each application, including the application's OSD and SFT files. This will be your Source Folder that must be defined in the Replaceables tab of the execution profile: \xxx.xxx.xx\AppDNA_Output\AppV_Convert.
3. Also create a subfolder, such as v5, to be the Target Folder: \xxx.xxx.xx\AppDNA_Output\AppV_Convert\v5.

Step 5. Install Required Software on Virtual Machine

Install the software on the virtual machine that will be used to automate converting Microsoft App-V 4.6 sequences to Microsoft App-V 5.0 and to create Microsoft App-V 5.0 sequences.

- Microsoft App-V 5.0
- PowerShell 3.0

Step 6. Import Microsoft App-V 5.0 Sequencer Execution Profile into AppDNA

To import the App-V 5.0 Sequencer execution profile script into AppDNA:

Note: App-V 5.0 Sequencer.xml is installed by default to C:\Program Files\Citrix\AppDNA\Client\Execution Profiles or C:\Program Files (x86)\Citrix\AppDNA\Client\Execution Profiles.

1. Log on to AppDNA and then choose Edit > Settings.
2. In the Settings dialog box, click Install Capture.
3. Click the Execution Profile tab.
4. Click Import (in the lower part of the dialog box).

5. In the Load Profiles dialog box:
    a) Browse to the location of the execution profile file downloaded from Podio.
    b) Select the execution profile file that you want to activate and then click Open.

Step 7. Download Forward Path Scripts and Execution Profiles

From the AppDNA Extensions Podio site:

1. Click the Extensions button at the top of the page.
2. Click [EP] Converter_App-V4.6_to_App-V5.0.
3. Under Files, right-click the latest version of [EP] Converter_App-V4.6_to_App-V5.0.xml, select Save target as…, and then save the file to your local machine.
4. Go back to the list of extensions and click [FP] Microsoft App-V 5.0 Decision.
5. Under Files, right-click the latest version of [FP] Microsoft App-V 5.0 Decision.xml, select Save target as…, and then save the file to your local machine.

Step 8. Import Microsoft App-V 4.6 to Microsoft App-V 5.0 Execution Profile into AppDNA

Import the Microsoft App-V 4.6 to App-V 5.0 Converter execution profile script downloaded from Podio into Citrix AppDNA:

1. Log on to AppDNA and then choose Edit > Settings.
2. In the Settings dialog box, click Install Capture.
3. Click the Execution Profile tab.
4. Click Import (in the lower part of the dialog box).
5. In the Load Profiles dialog box:
    a) Browse to the location of the execution profile file downloaded from Podio.
    b) Select the execution profile file that you want to activate and then click Open.
    c) In the Execution Profiles tab, click the imported execution profile, click the Edit button, and then click the Replaceables tab.
    d) Select the SourceFolder location replaceable, click the Edit button, enter the path to the Source files (such as \xxx.xxx.xx\AppDNA_Output\AppV_Convert), and then click OK.
    e) Select the TargetFolder location replaceable, click the Edit button, enter the path to the Target folder (such as \xxx.xxx.xx\AppDNA_Output\AppV_Convert\v5), and the click OK.
    f) Click Save to preserve your changes and then close the Settings dialog box.

Step 9. Import Forward Path Scripts into AppDNA

To import the downloaded Microsoft App-V 4.6 to App-V 5.0 Decision and/or Microsoft App-V 5.0 Decision forward path script into AppDNA:

1. Log on to AppDNA and then choose Configure > Forward Path.
2. In the Forward Path Logic Editor screen, click the Import button.
3. Browse to the downloaded forward path script, select it, and click Open.
4. Click Import.
5. Click OK in the message that the file has been successfully imported.

Step 10. Configure Forward Path Scripts: Microsoft App-V 4.6 to App-V 5.0 Decision, Microsoft App-V 5.0 Decision

These forward path scripts check the compatibility of applications against Microsoft App-V and Windows 7. There are 8 task scripts assigned to both Forward Path scripts taking into account options to automate the creation/conversion of App-V sequences on both Windows 7 x64 and x32.

To configure the scripts to match your AppDNA environment:

1. Log on to AppDNA and then choose Configure > Forward Path.
2. In the Scenarios tab, click Microsoft App-V 4.6 to App-V 5.0 Decision or Microsoft App-V 5.0 Decision.
3. Click the Editor tab to view and edit the scripts.
4. You can edit the scripts to reference a different operating system or to make other changes to meet the needs of your environment.
5. To change the operating system referenced, use the Property Explorer tab on the right side of the window.

Expand Applications > Modules to see a list of operating systems and how they should be referenced. Replace references to Windows7 with the desired operating system.

Step 11. Configure Task Scripts

The forward path scripts you downloaded and imported have eight task scripts assigned to them to enable you to automate the creation of Microsoft App-V 5.0 sequences or conversion of Microsoft App-V 4.6 to Microsoft 5.0 sequences. The task scripts need to be configured to reference your Citrix AppDNA virtual machine name and the execution profile that should be used to automate the process.

To configure a Forward Path Task Script:

1. In the Scenarios tab, expand the Forward Path script node that you want to edit.
   You will see the contents of the selected task script in the Editor tab. There is a task script enabling you to automate the Microsoft App-V process for both Windows 7 32-bit and 64-bit. You can delete any task scripts you don't plan to use.
2. Scroll down to line 21. The task scripts are already populated with the execution profiles to be used, such as 'App-V 5.0 Sequencer' for the Microsoft App-V 5.0 Decision.

Example:

```
ProductionManager.RunExecutionProfile(controller, ”Execution Profile Name”, replaceables, ”Default VM Configuration”)
```

Change to:

```
ProductionManager.RunExecutionProfile(controller, ”App-V 5.0 Sequencer”, replaceables, ”Your VM Name as shown in Install Capture Settings”)
```

3. To verify the name of your virtual machine, go to Edit > Settings from the AppDNA menu. In the left pane, select Install Capture. Use the name displayed in the Name column on the Virtual Machine tab.
4. Click Save to save the changes.
5. Repeat for each task script.

Reports for migration of Windows applications to App-V 5.0

The following table lists the reports required for the migration of Windows applications to App-V 5.0. These reports will provide the data you need to help with decision making.

To access the reports, click Reports: Applications in the side bar.

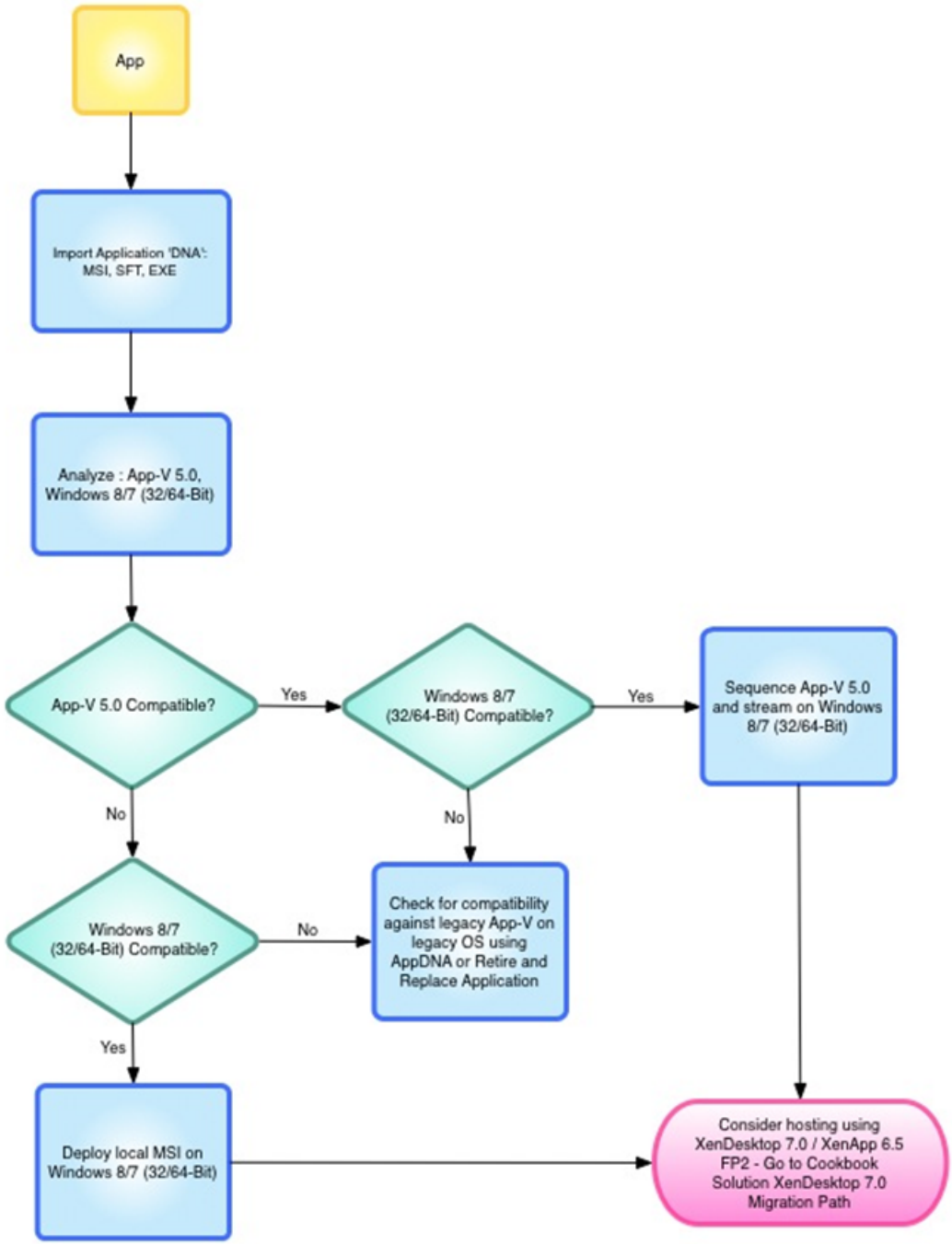
Reports	Description
Forward Path	Reflects scenarios based on organizational decisions and used to run automation task scripts based on the results. Potential outcomes for the Forward Path script include deploy on Windows 7 x64 as App-V Package and retire/replace or find alternative platform. The Forward Path report is used to reflect organizational decisions and run task scripts based on the results. There are two Forward Path reports configured for this solution: **Microsoft App-V 5.0 Decision** - used to determine if applications are good candidates to be sequenced using Microsoft App-V 5.0. If an application is a good candidate for sequencing using Microsoft App-V 5.0 a task script will be provided that automates the sequencing process. App-V 5.0 Sequencer execution profile is referenced in Task Scripts to automate Microsoft App-V 5.0 sequencing for outcomes that include Microsoft App-V as a good or possible candidate for application streaming. **Microsoft App-V 4.6 to App-V 5.0 Decision** – used to convert Microsoft App-V 4.6 sequences to App-V 5.0 for outcomes that include Microsoft App-V as a good or possible candidate for application streaming. [EP]Converter_App-V4.6_to_App-V5.0 is referenced in Task Scripts to automate the conversion of Microsoft App-V 4.6 to App-V 5.0 sequences for outcomes that include Microsoft App-V as a good or possible candidate for application streaming. To access the Forward Path report click Reports: Applications > Forward Path. Click the Change Scenario button and then click the drop-down list to select the Microsoft App-V 5.0 Decision or Microsoft App-V 4.6 to App-V 5.0 Decision report. Note: You can further customize the Forward Path script to tailor it to your environment and business decisions.

Reports	Description
Overview Summary	Provides a high-level dashboard view of the state of your application portfolio across all active reports. For each of the selected applications, it shows the overall RAG (red, amber, green) status for each of the active reports. On the rows that relate to an application, you can click the RAG icons to access the Remediation report views for that application. These provide the remediation details required for the application to work using the selected platform.
Microsoft App-V 5.0	Tests desktop applications for suitability with Microsoft Application Virtualization (App-V) 4.5, 4.6 SP1, or 5.0.
Microsoft Windows 8/7	Determines compatibility of the application on the target OS by going directly to the specific OS report. Drill down to the specific issues, download automated fixes, and get more information on how the application can be remediated.

Windows applications to App-V 5.0 migration steps

This section details the recommended process for migrating Microsoft Windows applications to Microsoft App-V 5.0, including the stages involved in assessing the application for compatibility against App-V 5.0, Windows 8/7, and Server 2012/2008 R2, 64-Bit. It also covers how to automate the conversion of App-V 4.6 sequences to App-V 5.0 and how to create App-V 5.0 sequences.

The flowchart shows you how to engage AppDNA into your migration and business-as-usual process.



Step 1. Import application DNA

For applications in an MSI format, select Import & Analyze > Applications > Direct Import.

For application in a Non-MSI format, select Import & Analyze > Applications > Install Capture.

Step 2. Analyze the application

Analyze the application against Microsoft Windows8/7, x64 and App-V. Include Server 2012/2008 R2 if the application will be hosted on a Microsoft server platform.

Step 3. Run Forward Path script

Run the forward path script Microsoft App-V 4.6 to App-V 5.0 Decision to check the compatibility of applications sequenced using Microsoft App-V 4.6 against Microsoft Windows 8/7, x64, and App-V 5.0 and get a review of the applications that are good or potential candidates for App-V 5.0.

Run the forward path script Microsoft App-V 5.0 Decision to check the compatibility of applications against Microsoft Windows 8/7 and App-V 5.0 and get a review of the applications that are good or potential candidates for App-V 5.0.

1. To access the Forward Path reports: Choose Reports: Applications > Forward Path. Click Change Scenario and then click the drop-down list to select the Microsoft App-V 4.6 to App-V 5.0 Decision or Microsoft App-V 5.0 Decision report.
2. To run task scripts, click Evaluate Tasks.

Step 4. Remediate

Review the Forward Path report data and prioritize applications based on RAG status:

- Green – Run task scripts (if one is available) and proceed to User Acceptance Testing (UAT).
- Amber – Check the detailed remediation report to determine what has been flagged and if it needs remediation or functional testing. Run task script (if available) and proceed to UAT.
- Red – Check the detailed remediation report to determine if the component flagged can/should be remediated and the action you want to take (that is, re-development, local installation on Windows 7/8, deploy on legacy platform, or retire and replace). Check the Overview report for the best fit platform.

Note: Click the application name within the Forward Path report to go directly to the detailed remediation data for an application.

Step 5. Run Task Script

Run the task script for applications that are suitable for App-V 5.0. These will be indicated by a Yes in the Automated Task Script column.

Click the Start button to run automated task scripts and either convert Microsoft App-V 4.6 sequences to Microsoft App-V 5.0 sequences or create Microsoft App-V 5.0 sequences.

Step 6. Test output for applications compatible for App-V 5.0

Migrate Windows applications to App-V 5.0

Step 7. Submit to User Acceptance Testing

Submit the applications to UAT, ensuring that the expert users are involved in the process.

Tap into the extendable features of AppDNA by using the Forward Path script to send an email to the group performing UAT when an App-V 5.0 sequence is ready to be deployed and tested.

Step 8. Find alternatives for applications not compatible with a given solution

For applications that are not compatible (cannot be remediated or remediation is deemed too costly) use AppDNA to determine if a legacy deployment option is more cost effective. Otherwise, consider retiring and replacing the application.

Use the Overview Summary report to get a quick look at the best possible platform for your application.

Migrate applications without install routines

August 2, 2018

You may have applications that can be executed by simply copying files into a folder stored on a computer, perhaps adding some registry keys or performing other manual changes to get the application working. AppDNA deals with those types of applications, enabling you to reduce the time, cost and risk for OS migration and virtualization technology adoptions by automating application compatibility and overall application migration.

AppDNA not only helps you determine if an application without an installation routine is compatible with an OS or virtualization technology, it also captures the application source and optionally produces a usable installation routine that can be added to your managed application library.

Even though you can easily create your own installer outside of AppDNA, using AppDNA enables you to reduce the overhead of managing your applications (cost, effort, and staff). Since you are already going through a capturing process with AppDNA to get the application source into the required format to run compatibility checks, it makes sense to use your third-party application packaging and virtualization software to create usable output so you can focus your expertise where it is really needed on the more difficult tasks.

AppDNA provides three ways to accomplish capturing your application source to import the application DNA for compatibility analysis and automating processes. The option used depends on the output desired and who will perform the installation/configuration (expert user, developer, or packager/sequencer). The following table outlines the options, how they can be used, and the potential use cases.

AppDNA capturing feature

Install Capture

Description

- Configures (copies files, creates registry keys, adds services, and so on) and captures desktop applications within a virtual machine that is launched during the AppDNA software import process.
- Supports launching .exe files, but in the absence of a setup executable, you can point the Install Capture feature to a placeholder executable, such as notepad.exe or cmd.exe. This allows the Install Capture feature to launch a configured virtual machine that you can then use to copy files, create registry keys, add services, and so on.
- Creates an .msi file that can then be imported into AppDNA. Cannot be used for deployment.
- Runs within the AppDNA software environment, from the AppDNA server or a machine configured with the AppDNA client.
- Optionally, you can package applications into usable installers or sequence applications using Microsoft App-V (just a few examples of the types of things you can automate).
- AppDNA automatically imports the .msi created as part of the Install Capture process.

Use cases

- Configuration requires more than copying a set of files (that is, creating registry keys, adding a service, and so on).
- You want the AppDNA software to automatically import the MSI created upon completion.
- You want to automate the creation of usable output (i.e. packages and sequences).
- Administrators are responsible for capturing the application.

AppDNA capturing feature

Self-Provisioning

Description

- Stand-alone tool that configures (copies files, creates registry keys, adds services, and so on) and captures desktop applications for import into AppDNA database using any type of machine (virtual, physical, or VDI).
- Supports launching .exe files, but in the absence of a setup executable, you can point the Self-Provisioning feature to a placeholder executable, like notepad.exe or cmd.exe. This allows Self-Provisioning to launch a configured virtual machine that you can then use to copy files, create registry keys, add services, and so on.
- Runs independently from the AppDNA software environment.
- Default setting creates an .msi file that can then be imported into the AppDNA software database. Cannot be used for deployment.
- Optionally, you can package applications into usable installers or sequence applications using Microsoft App-V (just a few examples of the types of things you can automate).
- Output created can be placed on a shared location for administrators to import the .msi into the AppDNA software database and perform an analysis to determine application compatibility.

Use Cases

- Configuration requires more than copying a set of files (that is, creating registry keys, adding a service, and so on).
- You want to enable expert users, developers, packagers/sequencers to do their own configurations and captures without being tied to the AppDNA software environment.
- You want to automate the creation of usable output (that is, packages and sequences).

AppDNA capturing feature

MSI Converter

Description

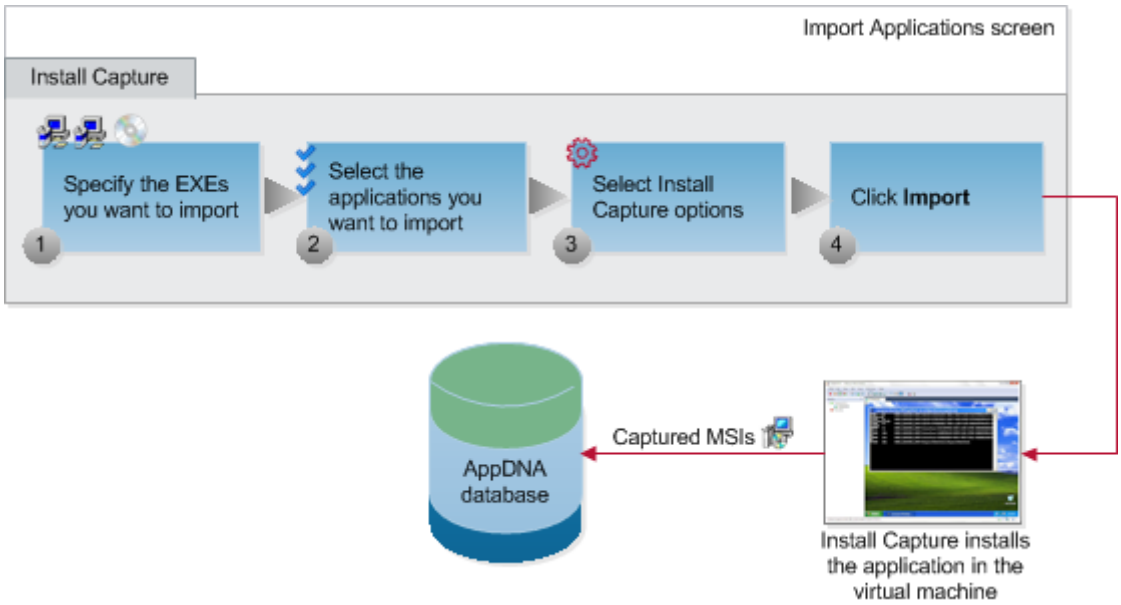
- Standalone tool that provides an alternative mechanism to generate an MSI file from a set of application source files in a folder. Originally designed for converting web application source files into an MSI, but can be used on any files.
- Runs independently from the AppDNA software environment.
- Output created can be placed on a shared location for administrators to import the .msi into the AppDNA software database and perform an analysis to determine application compatibility.

Use Cases

- You only have files to capture.
- You want to perform the capture outside of the AppDNA software environment.
- No interest in creating usable output (that is, packages and sequences). Runs independently from the AppDNA software environment.

Install Capture feature

This section shows an example of how you can use Install Capture to capture an application that does not have an installation routine and requires manual configuration. The following diagram shows the process that AppDNA follows.



Note: These steps assume you
configured a virtual machine that can integrate with your AppDNA environment.

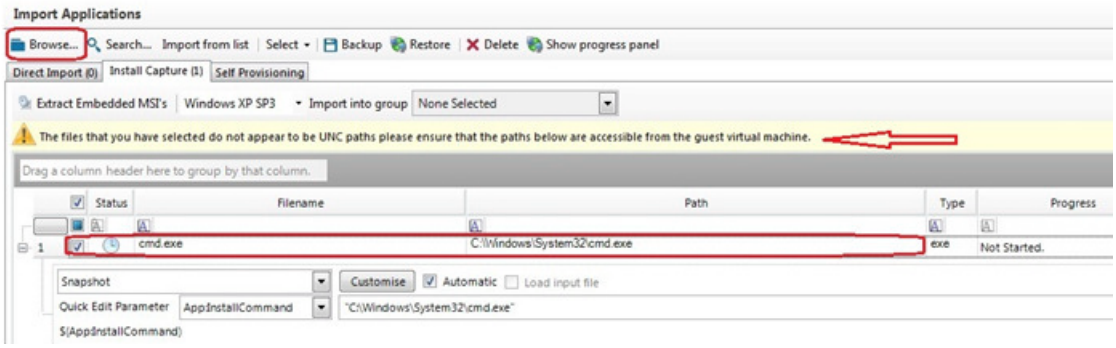
To import applications using Install Capture:

1. From the AppDNA side bar, choose Import & Analyze > Applications.
2. Click the Install Capture tab.
3. On the Install Capture tab, select the .exe or other installation files that you want to import.
4. Click Browse to select a placeholder executable.

   You can use anything, provided it exists on the virtual machine in the path specified. This example uses cmd.exe.

Note: When selecting applications that have an install routine, use a UNC path such as \\MyServer\MyApplications\MyApplication.exe. The path you specify must be accessible from the virtual machine, otherwise the import will fail.

After you select the files, AppDNA lists them on the screen. As shown in the screen shot, the AppDNA software displays a warning about the hard-coded path. This is acceptable since cmd.exe is in the same location on the virtual machine.



This example uses the default AppDNA software execution profile called Snapshot. For information about the more advanced AppDNA software execution profiles which you can use to automate other processes, see Execution Profiles.

Note: Citrix also has a library of non-supported execution profiles that are available for download from the Citrix AppDNA Extensions Podio site. These extensions are customized to automate the processes of interest to our customers. To access the extensions, create a Podio account and send an email to appdnafeedback@citrix.com requesting access to the site.

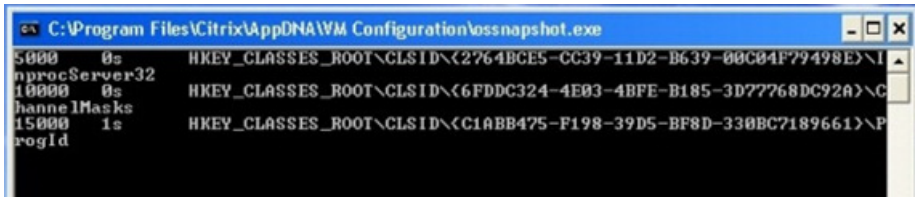
The Snapshot execution profile has three main steps:

1. **Before snapshot** – Performs an analysis of the virtual machine's state, including its complete file system and registry entries.
2. **Launch command** – Runs the application's non-MSI installer. In this example, there is no installation routine, so you launch cmd.exe. While cmd.exe is open, you then add files and anything else that needs to be captured for the application.
3. **After snapshot** – Performs a second analysis of the virtual machine's state when the installation routine has finished (in this case, when you close the cmd.exe window), including its complete file system and registry entries.

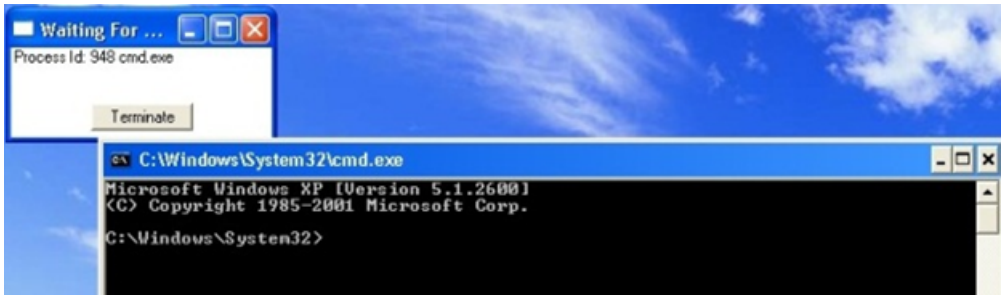
The difference between the state of the virtual machine in the before and after snapshots represents the changes made by installing the application. The capture process uses this information to generate an .msi file for importing into the AppDNA database and then resets the state of the virtual machine back to how it was before the installation. Click Import on the right side of the toolbar to start capturing the application DNA for loading into the AppDNA database.

After you click Import for applications on the Install Capture tab, the AppDNA Virtual Machine Remote Controls window opens.

The processing that takes place is controlled by the execution profile. When the Snapshot execution profile is in use, the Execution profiles “before snapshot” is the first action that is run on the virtual machine.

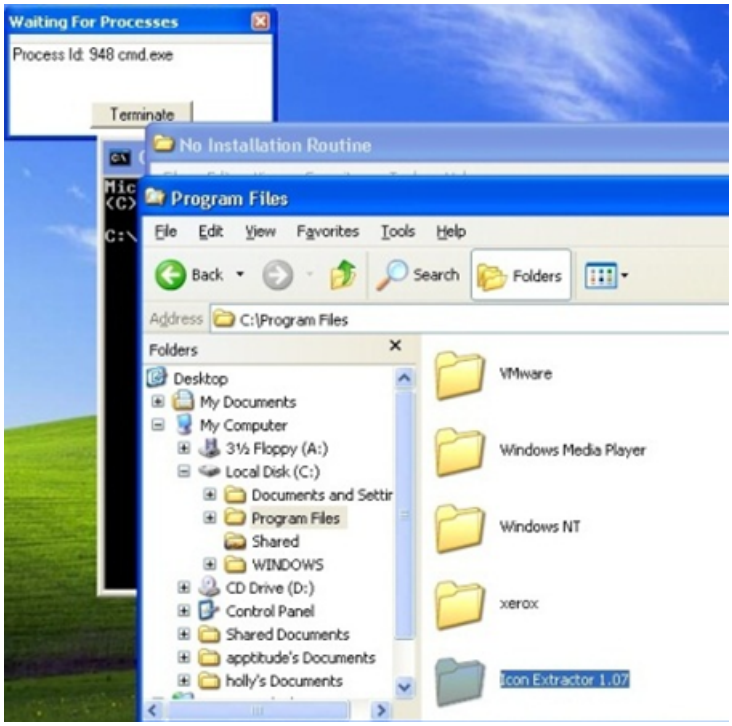


After the “before snapshot” has completed, the installation runs, which in this case is cmd.exe.

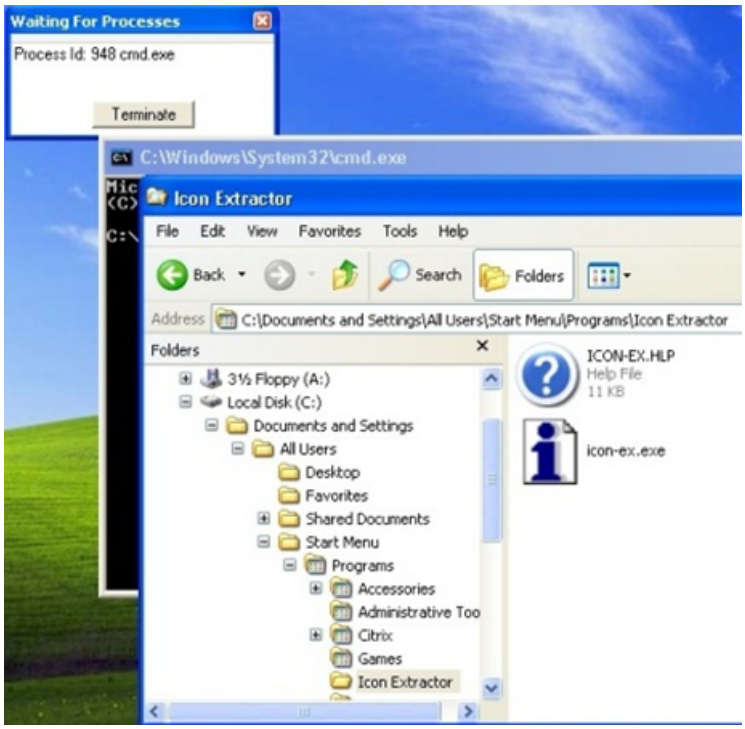


Leave cmd.exe open until after you make all configuration changes required for the application. Keep in mind that cmd.exe acts as setup.exe. The AppDNA execution profile script goes to the next step after the installation finishes and you close the cmd window.

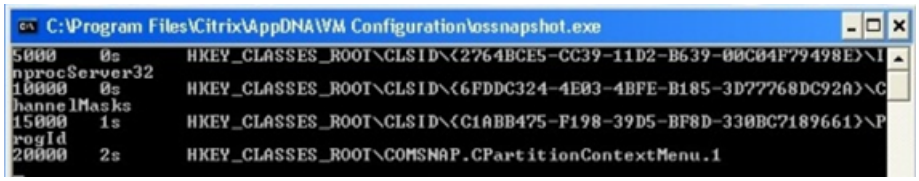
The following screen shot shows the result of copying from a network share the folder, Icon Extractor 1.07, into c:\program files. That folder contains the required application files.



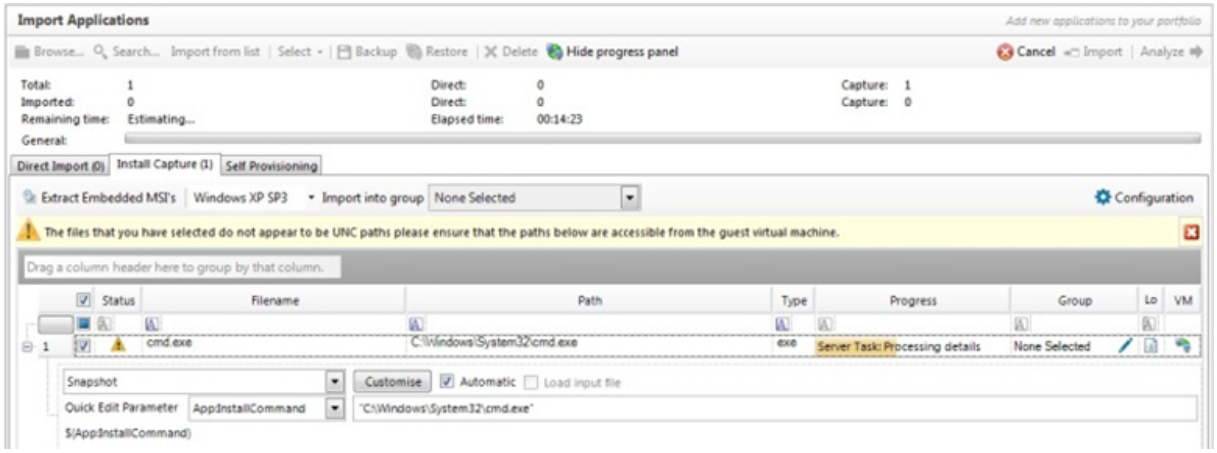
You also add the necessary shortcuts to the Start Menu. No other files are needed for this application without an installation routine. Of course, you may have an application that requires the creation of a service, environment variable, ODBC entry, and so on.



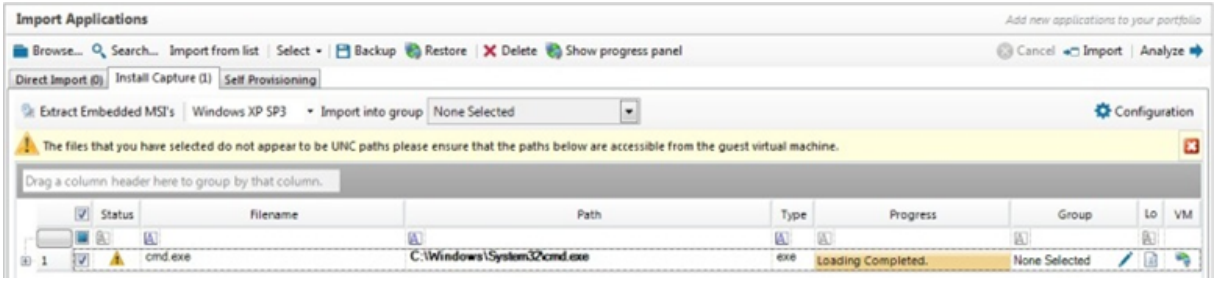
After you finish configuring the application, you can close the cmd.exe window. The “after snapshot” begins (assuming the Snapshot execution profile is in use).



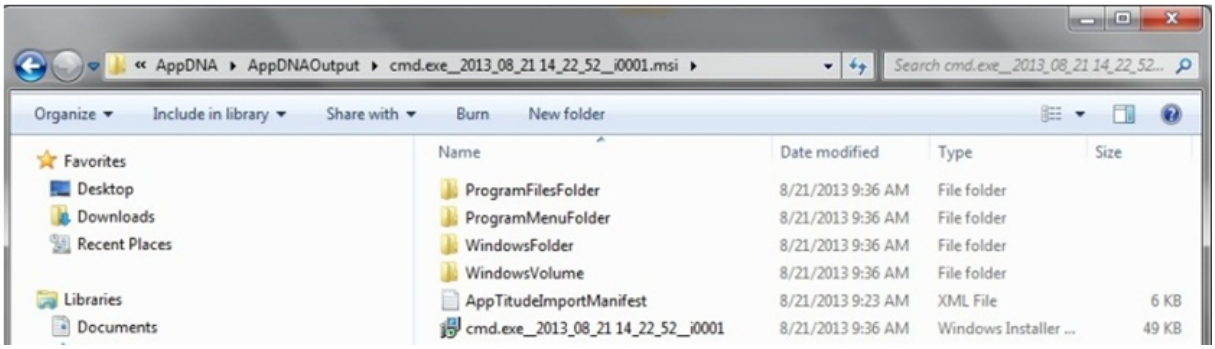
When the after snapshot completes, the AppDNA Snapshot execution profile copies the output to the designated network share and begins loading the newly created MSI into the database. When the import finishes, the AppDNA Virtual Machine Remote Controls window closes and the Install Capture tab displays the progress of the MSI import process.



Typically, the progress bar will be green indicating the installer returned a successful exit code. In this case, because no installer was used, AppDNA receives a non-zero exit code resulting in an amber progress bar. You can ignore that warning and proceed with analyzing the application against the desired modules to check compatibility. To do that, click the Analyze button now or after you have several applications to analyze.

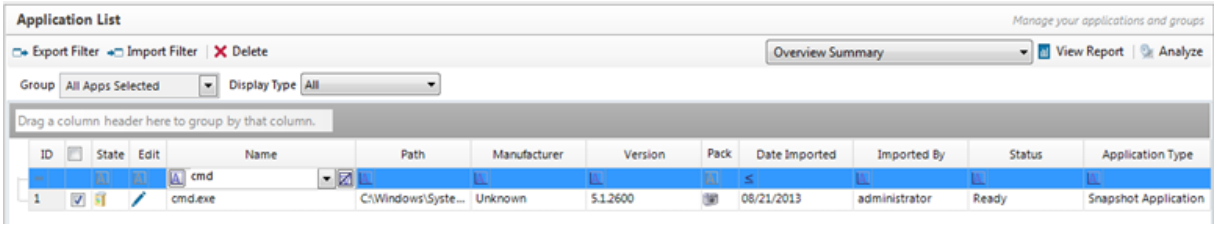


The analysis creates a folder with the name of cmd.exe in the designated output location as defined in the AppDNA configuration settings. The folder contains the MSI created and the extracted source files.



If you wait to analyze the application, click Select > All Applications in the side bar. You can filter the Application List screen to view only what was just imported.

In this screen, you can change the name to reflect the real name of the product by clicking the pencil icon to the left of the Name column.

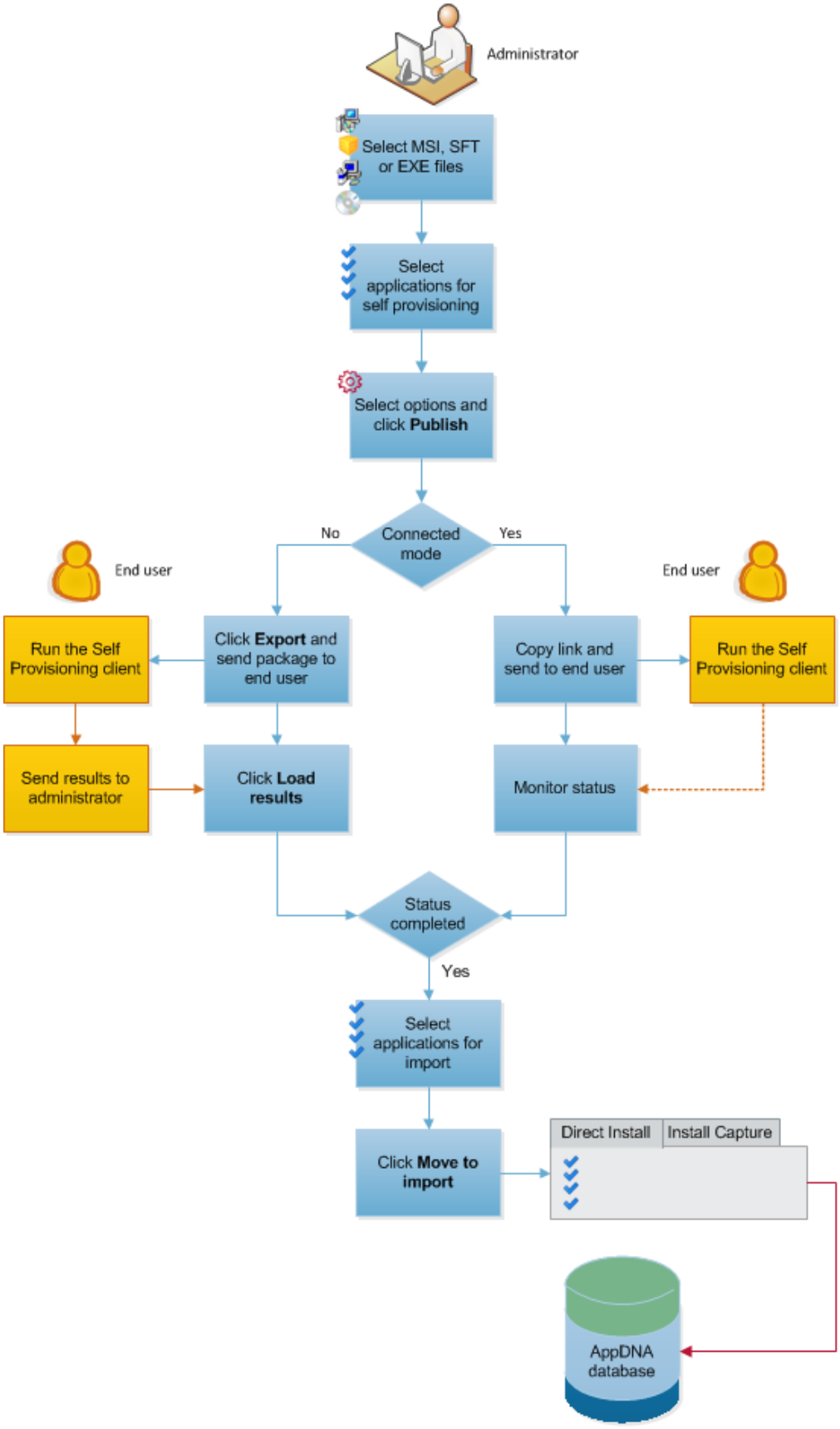


When ready to analyze, make sure the application is selected and click the Analyze button.

Self-Provisioning feature

This section shows an example of how you can use the stand-alone Self-Provisioning feature to capture an application that does not have an installation routine and requires manual configuration. The following diagram shows the process that AppDNA follows.

This example uses the disconnected mode. In that mode, the Self-Provisioning client and the AppDNA client are on different networks and do not both have access to the same network file share. AppDNA wraps the client instruction files and execution profile into a package that the administrator sends to the end user. The end user in turn sends the output of the Self-Provisioning client to the administrator.



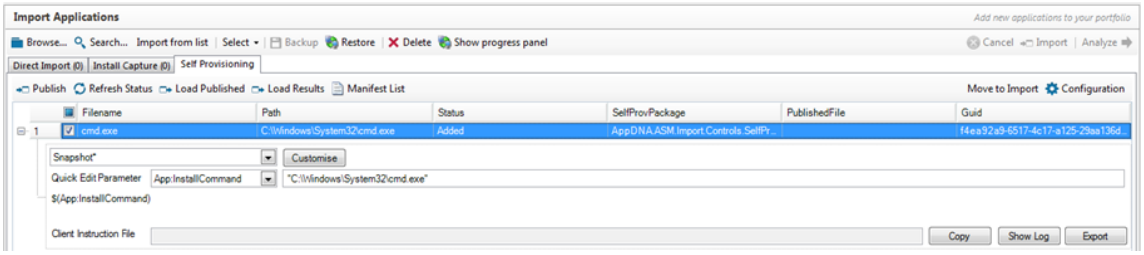
Note: These steps assume you have a configured an AppDNA Self-Provisioning client.

To prepare the application for Self-Provisioning:

1. From the AppDNA side bar, choose Import & Analyze > Applications.
2. Click the Self-Provisioning tab.
3. Select the installation file that you want to capture. Just like the Install Capture feature, this would typically be a setup executable that is referenced using a UNC path.

   This example of capturing an application that does not have an installation routine and needs to be manually configured uses cmd.exe C:\Windows\System32\cmd.exe.

   After you have selected the files, AppDNA lists them on the screen.



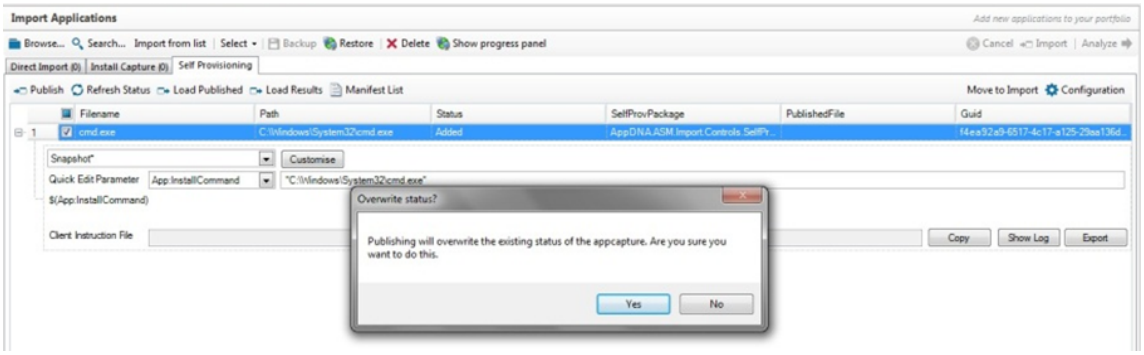
   This example uses the default AppDNA software execution profile called Snapshot. For information about the more advanced AppDNA software execution profiles which you can use to automate other processes, see Execution Profiles.

   Note: Citrix also has a library of non-supported execution profiles that are available for download from the Citrix AppDNA Extensions Podio site. These extensions are customized to automate the processes of interest to our customers. To access the extensions, create a Podio account and send an email to appdnafeedback@citrix.com requesting access to the site.

   Note: Before you start using Self-Provisioning, you must configure the output path in the Self-Provisioning settings. Click
   Configuration on the
   Self-Provisioning tab toolbar to open the
   Self-Provisioning Settings.

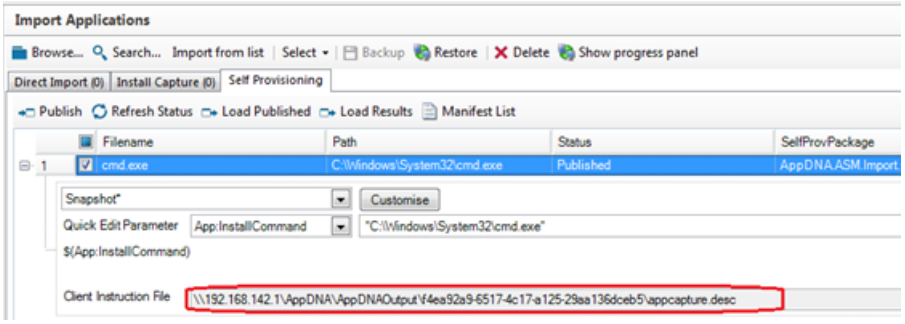
4. Select the application(s) you want to include and then click Publish.

   AppDNA presents a warning that this will overwrite the existing status of the selected applications.



5. Click Yes to confirm.

   AppDNA then updates the screen with the details of the client instruction file for each selected application.



6. Click Export (to the right of the client instruction file) to create a package to send to the end user (expert user or developer) who will run the Self-Provisioning client. This opens the Export Self-Provisioning Package dialog box:

   - Input file from client perspective – Specify the name and location of the application's installation package, relative to the Self-Provisioning client machine.
   - Folder where the capture results are to be stored – Specify the default location where the Self-Provisioning client will write the output of the application capture. The end user can specify a different location during the application capture. Make sure you specify this relative to the Self-Provisioning client machine.
   - Exported package path – Specify the name and location of the package that is to be sent to the end user who will run the Self-Provisioning client.

   Next send the exported package to the user who will perform the Self-Provisioning in the standalone Self-Provisioning client.

   The end user will go through a capture process similar to the AppDNA Install Capture feature process.

   End-users performing the configuration must install the AppDNA Self-Provisioning client. The installers, in a Tools subfolder of the AppDNA installation folder, are:

   Citrix AppDNA Self-Provisioning Client.msi

Citrix AppDNA VM Configuration.msi

The MSIs created can be imported into AppDNA using the Direct Import tab in the Import Applications Screen. See Direct import for more information.

MSI Converter

The AppDNA MSI Converter is a stand-alone tool that is installed as part of AppDNA and provides an alternative to generating an MSI file from a set of application source files in a folder. The original intent of the MSI Converter was to convert web application source files into an MSI so that the web application could be checked for compatibility; however, you can use this option on any files.

Note: To install the AppDNA stand-alone web capture tools, you need the installer (called Citrix AppDNA Web Application Capture.msi). This comes with AppDNA. It is copied into a Tools subfolder of the AppDNA installation folder when you install AppDNA.

This procedure provides instructions for using the Stand-Alone Web Application Source to MSI Converter to generate an MSI from one or more folders containing application source files.

1. From the Windows Start menu, choose Citrix AppDNA > Web Application Source to MSI Converter.
2. If necessary, click Configure on the toolbar to change options.

   For information about these options and those in the next step, see Stand-alone Web Application Source to MSI Converter.
3. Click Select, Search for Folders or Import List to select the folders that contain the web application source files that you want to convert.

   The selected folder(s) appear in the window.
4. Select the folder(s) for which you want to create an MSI.
5. Click Start.

The MSI Generator shows whether the processing is successful in the Status column. Completed means that the processing finished successfully. If the processing is not successful, click the Refresh button to view the log. This provides information that you can use to troubleshoot the problem.

Output

The output from the Stand-Alone Web Application Source to MSI Converter is located in the folder that is specified in the Configuration dialog box. The output for each application is stored in a separate folder, whose name is derived from the folder name and the date and time stamp.

You can then import the MSIs into AppDNA using the Direct Import tab in the Import Applications Screen. See Direct import for more information.

SDK

June 17, 2019

The AppDNA software development kit (SDK) enables you to provide AppDNA within a process or user interface that your users are familiar with, or within a simple web page. In this way, users avoid having to spend time on familiarization with the AppDNA user interface because the AppDNA tasks are meshed seamlessly into their usual workflows.

For more information on the AppDNA SDK—including an SDK introduction, descriptions of the data available, how to develop using the AppDNA SDK, and examples—see https://developer-docs.citrix.com/.

Troubleshoot

June 17, 2019

Installation issues

How to enable AppDNA verbose logging

Note: For more information on all types of logging in AppDNA, see CTX219766.

If you are having issues installing Citrix AppDNA, these steps show you how to enable the collection of detailed installation log files on the AppDNA server.

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

To enable verbose logging on the AppDNA server, complete the following procedure:

1. Open the **Run** dialog box.
2. Type **regedit** and click **OK**.
3. In the User Access Control dialog, click **Yes**.
4. In the registry editor, browse to the key HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\AppDNA\appTit
5. Find or create the registry setting **VerboseLogging** (REG_DWORD) and change the value to **1**.

When AppDNA detects that this registry value has been set, it writes the verbose logs to **%temp%\AppDNAVerboseLog.log**.

Note that for the server processes this will be the temp directory for the identity that the AppDNAAppPool is running under in IIS. By default this will be the build in “ApplicationPoolIdentity” and the temporary directory will be C:\windows\temp.

Logs are captured separately for the client and server processes (unless they are running as the same user).

Use a text editor to read the contents of the AppDNAVerboseLog.log file.

To disable the verbose logging, change the VerboseLogging registry value to **0**.

A similar process can be followed to turn on verbose logging for the Citrix AppDNA Service, **QueueProcessor**. To enable verbose logging for the QueueProcessor service, follow steps 1-4 above. In step 5, find or create the registry value **QueueProcessorVerboseLogging**. Messages are written to the windows event log (rather than a file) in:

EventViewer > Application and Service Logs > AppDNA > Source = AppDNA Service

Logon issues

“The request failed with HTTP status 503: Service Unavailable”

This error might mean that the password that the AppDNA web site uses to connect to the AppDNA database has expired or has been changed. To correct this issue, see Web site.

Login fails with a “The operation has timed out” error

This error sometimes occurs because one of the AppDNA services or another service that AppDNA relies on is not running.

Check the IIS services

1. Open IIS Manager: On the Windows Start screen or menu select Programs > Accessories > Run, type inetmgr, and then click OK.
2. Check that the IIS server is running and if not, start it.

   To do this, in the Actions panel on the right side of the window, under Manage Server, click Start. The Start link is disabled if the server is running.
3. If the IIS Server is running, check that the AppDNAAppPool is running and if not, start it.

   To do this, expand the tree on the left side of the IIS Manager window and click Application Pools. Click AppDNAAppPool in the middle panel and then click Start in the panel on the right. The Start link is disabled if the AppDNAAppPool is running.

4. If the IIS Server and AppDNAAppPool are running, check that the AppDNA web site is running and if not, start it.

   To do this, expand the Sites node in the tree view on the left side of the IIS Manager window and click the AppDNA web site (by default, this is called AppDNA). Then click Start in the panel on the right. The Start link is disabled if the AppDNA web site is running.

If you restarted any of the IIS services, try logging on to AppDNA again. Otherwise, check that the SQL Server Instance service is running and if necessary start it, as follows:

1. Open the Windows Services window (Control Panel > Administrative Tools > Services).
2. In the list of services, locate the SQL Server instance used for the AppDNA database.
3. If the Status column is blank, click Start to start the service. If this is successful, close the Windows Services window. You should now be able to log on to AppDNA.

The request failed with HTTP status 407: Proxy authentication required

This error occurs if Internet Explorer is configured to use a proxy server for your LAN. You can work around this issue as follows:

1. From the menus in Internet Explorer, choose Tools > Internet Options.
2. On the Connections tab in the Internet Options dialog box, click LAN settings.
3. Under Proxy server in the Local Area Network (LAN) Settings dialog box, select the Bypass proxy server for local addresses check box.
4. Click OK.

Licensing issues

This section provides information to help you troubleshoot licensing problems, including those that cause the AppDNA banner to go red. When this happens, look at the explanatory message in the Module license summary section of the Dashboard. This generally makes it clear whether the problem is caused by AppDNA not being able to contact the AppDNA licensing service or by a problem with the actual licensing of the database itself. Information follows for each of these root causes under separate headings.

You can continue to use AppDNA with the licensing problem and the red banner. However, the functionality is very restricted - you can import applications, but most other features are blocked. Once the licensing issue is resolved, the blocked features will be available again.

AppDNA cannot contact the licensing service

If AppDNA displays a message that it cannot contact the licensing service, it may mean that the AppDNA license server is not running. You can check this and if necessary restart it as follows:

1. Open the Windows Services window (Control Panel > Administrative Tools > Services).
2. In the list of services, locate the AppDNA LicenseServer.
3. If the Status column is blank, it means that the service has not started. Click Start to start the service. If this is successful, close the Services window.
4. Restart AppDNA.

Database licensing broken after moving the AppDNA server or transferring a license

AppDNA licenses are tied to both the database and the machine on which the AppDNA licensing service is running when the license is activated. Problems can arise when the link between the license in the database and the licensing service location is broken – for example, because you have moved your AppDNA server from one machine to another, or you have started, but not completed, the two-stage procedure for transferring a license.

- To make the database usable with a licensing service on a different machine, transfer the license from the AppDNA licensing service on the old machine to the new machine.
- If you have started the license transfer procedure – for example, you exported the license token but have not imported it back into the database with the new license server location – complete the procedure. The database will then become available again.

For more information, refer to Transfer Licenses.

Note: Typically, the licensing service runs on the same machine as the AppDNA server. However, this may not be the case if you have upgraded from an earlier version of AppDNA.

Default license server port is not available

By default the AppDNA licensing service uses port 8079. If that port is not available, change it as follows.

1. Close AppDNA on the server and all connected AppDNA clients.
2. Locate the AppDNA licensing service files.

   The default location is C:\Program Files[(x86)]\Citrix\AppDNA\License Server.
3. Open remoting.config in a text editor.
4. In the following line, change 8079 to a different port number and then save the file. `<channel ref=”tcp”port=”8079”bindTo=”0.0.0.0”>`
5. From the Windows Start screen or menu, choose Control Panel > Administrative Tools > Services.
6. In the Windows Services panel, locate the AppDNA licensing service in the list of services and click Start or Restart on the toolbar to restart the AppDNA licensing service.

Import and analysis issues

"This transaction has completed and can no longer be used"

This error message can occur during analysis or any type of import. It is generally caused by the database not having enough disk space to expand.

1. Open Microsoft SQL Server Management Studio and connect to the SQL Server instance that hosts the AppDNA database.
2. Check the SQL Server logs to confirm whether lack of disk space is the problem.

   To do this, in the tree view on the left side, open the Management > SQL Server Logs folder. View the recent logs and look for text that says that there is not enough space on disk. If disk space is the issue, follow the steps below.
3. Make sure that the AppDNA database data file and log file are allowed to grow.

   In the tree view on the left side, open the Databases folder. Then right-click the AppDNA database and from the shortcut menu, choose Properties. This opens the Database Properties dialog box. Click Files in the side bar and ensure that both the data file and the log file are configured to grow in small chunks (for example, by 10%) and that there is no maximum size set.
4. Set the database recovery model to simple.

   In the Database Properties dialog box, click Options in the side bar, and ensure that the Recovery model is set to Simple.
5. Check the available disk space and if necessary, increase the free disk space by cleaning up unwanted data or upgrading the hardware.

Import of App-V packages (.sft or .appv) fails

When you import .sft or .appv packages, AppDNA automatically unpacks their contents into an intermediate folder, preserving the original directory structure. This fails if the total number of characters in the resulting file path exceeds the Windows limit (typically 256 characters). When this happens, the import log file contains the text: create_deep_dir.

By default, AppDNA unpacks .sft and .appv files into the temporary folder specified in File settings. However, you can specify a separate intermediate folder for .sft and .appv files in the SFT intermediate folder box in Import and analyze settings.

To resolve this issue, set a very short file path for the SFT intermediate folder. AppDNA does not automatically clear this folder. If necessary, you can delete the unpacked files manually after the import has finished.

Import succeeded but my application does not contain the expected DNA

This occasionally occurs with applications that have been imported through Install Capture or Self-Provisioning when the installation fails but the installer does not follow the convention of returning zero for success and a non-zero value for a failure. When this happens, by default AppDNA assumes that the capture has succeeded, imports the DNA captured, and marks the import as successful – although in fact no real application DNA was captured at all. In this situation, the captured DNA consists of any minor changes that the failed attempt to install the application made to the underlying operating system.

If you ran the capture using auto-clicker, the installation may have failed because it was waiting for user input. Therefore, run the capture again without auto-clicker. This may enable the installation, and therefore the capture, to complete successfully.

Alternatively, if you know that an installer does not follow the convention of returning a zero exit code on success, you can specify the success exit code in the execution profile for that application. See Edit an execution profile for information about how to do this.

OS image import fails with Error 404: File not found

When the import of an OS image fails with a "404: File Not Found" error, it generally means that limits on the size of the maximum content length has been exceeded in IIS. To increase the maximum allowed content length, refer to the instructions under "Optimize IIS" in Optimize AppDNA.

Report issues

Report views are very slow to display

This problem sometimes occurs when the number of records per page has inadvertently been set to a very large value. If the page is so slow that it is unusable, navigate away from the report view and change the number of records per page, as follows.

1. From the Edit menu in AppDNA, choose Settings.
2. In the side bar of the Setting dialog box, click Reporting.
3. In the Records per page box, enter a lower value (for example, 200).
4. Click Save.

To change the number of records per page in the web client:

- Append the following to the report view's URL:
  `&FRMKEY_PAGE_SIZE=n`

Where n is the required default page size, as shown in the following example. For clarity, this URL is shown on multiple lines. In practice the URL must be entered as one unbroken string.

```
http://appdna-machine:8199/appdna/Reporting/AssessmentReport.aspx? FRMKEY_TOKEN
=1dd82045-b9a3-4840-af46-75e112bfcbb0 &FRMKEY_MODULE_ID=Win8Module &FRMKEY_CUSTOMISATI
=&FRMKEY_POSTIMAGE=-2147483637 &FRMKEY_PREIMAGE=-2147483647&FRMKEY_RESOLUTION
=app_group_summary &FRMKEY_PAGE_SIZE=5
```

Images fail to display in report views

This problem has been encountered when first viewing reports after installing AppDNA on Windows 8. The problem was caused by an incomplete configuration of Internet Information Services (IIS).

To resolve this problem:

1. Close AppDNA and stop AppDNA clients.
2. On the AppDNA server machine, make sure that all required IIS features are enabled. For more information, refer to System requirements for AppDNA 7.6.
3. Use the iisreset command to reset IIS.

Effort Calculator is unreadable

The main Effort Calculator screen is not readable when the “Make it easier to read what’s on your screen” display option in Control Panel is used to increase the size of the text and other items on your screen by, for example, 125%. This option is sometimes on by default on Windows 8.

When this option is in use, Effort Calculator increases the size of the text. This causes the text to be truncated or to run over other items making them unreadable. Some other reports are affected in a similar way.

The solution is to reset the display size to the 100% setting in Control Panel > Display.

PDF export fails

If you attempt to perform a PDF export after installing Adobe Reader but before you have actually run Adobe Reader or opened a PDF file, the PDF export fails with an error (“This app can’t be activated when UAC is disabled”). This is because the AppDNA PDF export does not work until you have accepted the Adobe Reader license agreement.

To resolve this issue, open a PDF file on the machine on which you are running AppDNA and accept the Adobe Reader license agreement.

Columns overlap in the Report Data section of the PDF exports

When a report has a large number of algorithm groups, the columns in the Report Data section of the PDF exports may overlap and become unreadable. To resolve this issue, clear the Show counts in PDF exports check box in Reporting settings and then run the PDF export again.

System Check issues

August 1, 2018

The System Check step in the Configure AppDNA Environment wizard performs a number of checks on your system. The checks that are performed depend on what you are doing and how your environment is configured.

Some of the checks test for critical issues that must be fixed before you can proceed and some are warnings that it may be safe to ignore. When some checks fail, the wizard provides an option to fix them. This section explains what the wizard attempts to do if you use this option and what you can do to fix the problem yourself if there is no automatic fix or the automatic fix fails.

Current machine checks

Free disk space – Checks that the drive on which the operating system is installed has the minimum required space for a new installation. The wizard does not provide an automatic fix for this issue. If necessary, clean up the disk to free up disk space.

You can ignore this if you know that sufficient disk space is available, perhaps because you are doing an upgrade, which requires less free disk space.

AppDNA license server is running – Checks that the AppDNA license server is running. This is a critical issue. The automatic fix option attempts to start the AppDNA license server.

- If the automatic fix fails, start the AppDNA license server manually.
- By default, the AppDNA license server uses port 8079. If this port is already in use, you may need to configure it to use a different port. Alternatively, if the AppDNA license server has been configured to use a different port, you may need to return to the License Database step to enter the correct port number.
- If the AppDNA license server is located on a different machine, check that you entered its machine name and port correctly in the License Database step. Check that the machine is running and the network cable is plugged in. Check whether the firewall is blocking access.
- Check the Windows event log in the Windows Event Viewer.
- For more information, see Licensing issues.

SQL Server checks

Roles – If you are creating a new database, the wizard checks that the user account has the sysadmin server role. For other database operations, the wizard checks that the user has the bulkadmin server role and db_owner database role.

This is a critical issue. The wizard does not provide an automatic fix for this issue. The database operation is likely to fail without the correct roles. If necessary, you can assign the roles or return to the step where you entered the database credentials and enter a different user account. If you are using Windows authentication, click Cancel to exit the wizard and then start again under a different user account.

Database collation – Checks that the collation defined for the database is Latin1_General_CI_AS. This is a critical issue. The wizard does not provide an automatic fix for this issue.

SQL Server collation – Checks that the collation defined for the SQL Server instance is Latin1_General_CI_AS. This is a critical issue. The wizard does not provide an automatic fix for this issue. If necessary, click Cancel to exit the wizard, configure the SQL Server instance to use the required collation, and then run the wizard again.

Version – This checks that the SQL Server version is one of the supported versions. This is a critical issue. The wizard does not provide an automatic fix for this issue. If necessary, click Cancel to exit the wizard, install one of the supported versions of SQL Server, and then run the wizard again.

Internet Explorer (IE) checks

JavaScript – Checks that JavaScript is enabled in Internet Explorer. This is a critical issue because JavaScript is required to view AppDNA reports.

Unencrypted forms – Checks that unencrypted forms are enabled in Internet Explorer. This is a critical issue because unencrypted forms must be enabled to view AppDNA reports.

IIS checks

These checks are performed only if you are configuring a complete installation and are using an IIS web server.

Common HTTP features – Checks that common HTTP features are enabled in IIS. This is a critical issue. The automatic fix option attempts to enable the common HTTP features. If this is successful, you need to restart your computer before continuing.

ASP .NET – Checks that ASP .NET is enabled. This is a critical issue.

IIS pipeline mode – Checks that IIS pipeline mode is set to Classic. This is a not a critical issue – you can run AppDNA without the pipeline mode set to Classic. However, it is recommended and improves performance. The automatic fix option attempts to set the IIS pipeline mode to Classic.

Idle time out – Checks that the application pool idle time-out is zero. This is a not a critical issue – you can run AppDNA without this IIS setting. However, it is recommended and improves performance. The automatic fix option attempts to set the application pool idle time-out to zero.

Ping – Checks that ping is disabled for the application pool. This is a not a critical issue – you can run AppDNA with ping enabled for the application pool. However, disabling ping is recommended and improves performance. The automatic fix option attempts to disable ping for the application pool.

AppPool recycling – Checks that recycling of the application pool is set to zero. This a not a critical issue – you can run AppDNA without this setting. However, it is recommended and improves performance. The automatic fix option attempts to set the application pool recycling to zero.

Machine name – Checks that your machine name meets the IIS requirements for a domain name.

Web site connect user is local administrator – Checks that the web site user account is a member of the local Administrators group. If necessary, return to the Web site credentials step and enter a user account that is a member of the local Administrators group.

Active Directory and Configuration Manager issues

August 2, 2018

"Access is denied" error

The "Access is denied" error can occur when you enter the Active Directory or Configuration Manager connection details or when you extract data using that connection.

Typically this error occurs for one of the following reasons:

- The user account does not have the required permissions, as described in Requirements for optional features.
- Distributed COM (DCOM) is not enabled on the computer from which you are trying to connect to Active Directory or Configuration Manager. For information, refer to Enable or Disable DCOM.

"Failed to load file" error

When importing managed applications that have been deployed through Configuration Manager, AppDNA requires access to the installation files. Typically this is achieved using UNC paths and access to

file server shares is through Active Directory domain authentication. If an import fails and the import log contains a message similar to the following, examine the installation file path and ensure that it is accessible to AppDNA. For Install Capture imports, the installation files must also be accessible to the Install Capture virtual machine.

Failed to load file: <MSI file name> due to error
The system cannot open the device or file specified.

Failed to load file: <MSI file name> due to error
Access is denied.

The failure could be a result of running AppDNA under a Windows user account that does not have access to the required network shares. It could also be a result of paths expressed using drive letters rather than UNC paths. The required drive letters must then be mapped to the correct network share for the import to be successful. When using Install Capture, you need to do this on virtual machine.

Install Capture issues

August 2, 2018

This section provides some troubleshooting tips for problems that occur during an Install Capture.

Note: Many Install Capture issues can be diagnosed and resolved by re-running the Virtual Machine Configuration Wizard (which performs a number of checks and provides targeted troubleshooting information when problems occur).

Enable the Troubleshoot Errors option

The Install Capture Troubleshoot Errors option opens a troubleshooting user interface if particular errors are encountered when performing an Install Capture. You can use the troubleshooting user interface to connect to Remote Admin, run commands, and perform other troubleshooting steps within the virtual machine. Then when you perform the Finished action, AppDNA ends the Install Capture, closes the troubleshooting interface, and moves on to the next Install Capture, if there is one.

To enable troubleshooting from Install Capture

1. From the AppDNA menus, choose Edit > Settings.
2. Click Install Capture.
3. On the Virtual Machines tab, select the virtual machine configuration you are using, and click Advanced.

4. In the Virtual Machine Configuration dialog box, select the Troubleshoot Errors check box and then click OK and Save.

Virtual Machine Configuration Check

August 2, 2018

By default, AppDNA performs a number of checks on the virtual machine configuration when you click Import in the Import Applications screen if any applications are selected for import on the Install Capture tab.

Connection to the Hyper-V server fails

During a virtual machine configuration check, the connection to the Hyper-V server fails with this error message if DCOM is not enabled:

The Hyper- connection failed because Hyper-V does not exist on the specified server, or DCOM is not enabled. Full Error: The RPC server is unavailable. [Exception from HRESULT: 0x800706BA]

To enable DCOM, see Enable or Disable DCOM. Also verify that port 135 is open.

"Connecting to Remote Admin agent" fails

The "Connecting to Remote Admin agent" check fails if the virtual machine has an old version of the Citrix AppDNA VM Configuration tools installed on it. Click the link to see the detailed error message, which will tell you if this is the problem. See Upgrade AppDNA tools for step-by-step instructions for upgrading the Citrix AppDNA VM Configuration tools.

The "Connecting to Remote Admin agent" check also fails if the virtual machine requires any user interaction when AppDNA reverts the virtual machine – for example, if the virtual machine snapshot was taken when the virtual machine was powered off (as recommended) but the virtual machine was not configured for automatic logon. The "Connecting to Remote Admin agent" check fails in these circumstances because the virtual machine waits for you to log on before Remote Admin starts up. However, AppDNA does not open the virtual machine in the console and so you cannot log on. This scenario does not cause a problem during Install Capture, provided you are present to physically log on to the virtual machine when it opens in the console.

If the "Connecting to Remote Admin agent" check fails for any other reason, rerun the Virtual Machine Configuration wizard to diagnose the problem as explained next.

Diagnose problems

Citrix recommends that use the Virtual Machine Configuration wizard to troubleshoot issues. To do this:

1. From the AppDNA menus, choose Edit > Settings.
2. On the left side of the Settings dialog box, click Install Capture.
3. In the Install Capture page, click the Virtual Machines tab.
4. In the list of virtual machine configurations, select the one that you are using and then click Edit.

   This opens the virtual machine configuration in the Virtual Machine Configuration Wizard. Work through the steps in the wizard. When you click Next on each step, the wizard performs a number of checks and provides information about any problems.
5. Click Save to preserve your changes.

Turn off these VM configuration checks

You can permanently turn off these automatic checks as follows:

1. From the AppDNA menus, choose Edit > Settings.
2. On the left side of the Settings dialog box, click Install Capture.
3. In the Install Capture page, click the Settings tab.
4. Select Skip virtual machine system check.
5. Click Save.

Virtual Machine Does Not Start

August 2, 2018

This topic provides troubleshooting tips for when the virtual machine does not start when attempting to perform an Install Capture.

- For common XenServer errors, see “XenServer errors” below.
- If you are using Windows 8 Hyper-V Client, this problem occurs if AppDNA is not run as an administrator. For instructions for configuring AppDNA so that it always runs as an administrator, see “Configure AppDNA to run as administrator” below.
- If you are using vSphere or Hyper-V, click the icon in the VM column on the Install Capture tab. If this displays a “No such host is known” error, see “Remote Desktop Connection window does not open (vSphere or Hyper-V)” below.

- Check that the virtualization technology is installed, configured, and is running, and the virtual and AppDNA machines have been set up as described in Install Capture.
- Attempt to start and stop the virtual machine outside of AppDNA in order to confirm that the virtual machine is working correctly.
- Check that the virtual machine configuration is set up correctly within AppDNA. The easiest way to do this is to select the configuration on the Virtual Machine tab in Install Capture settings and click Edit. This opens the Virtual Machine Configuration Wizard, which performs checks and provides useful feedback when things go wrong. In particular:
  - Check that the virtual machine's IP address (or DNS or machine name) is correct. If the virtual machine's IP address has changed, you need to update it in the wizard.
  - If relevant for the virtualization technology, check that the user name and password for logging into the server are correct. If the password has expired, you need to enter the new password in the wizard.
  - If any of the steps in the wizard fail, refer to Troubleshoot.
- Set up automatic log on to the virtual machine, as described for each of the supported technologies in Install Capture.

XenServer errors

Unable to prepare the virtual machine for use. Could not authenticate session. Check your access credentials and try again.

This error means that the username and password that Install Capture uses to log on to XenServer are invalid. Typically this means that the password has expired. The username and password are stored in the virtual machine configuration in encrypted form.

To correct this error, use the Virtual Machine Configuration Wizard to edit the virtual machine configuration and enter the new password. Make sure you save your changes. Then start the Install Capture again.

AppDNA is unable to revert the virtual machine to the selected snapshot. This is because the user account provided for accessing XenServer is not authorized to perform the operation.

This error means that the user account that Install Capture uses to log on to XenServer does not have the permissions required to revert the virtual machine. The username and password are stored in the virtual machine configuration in encrypted form.

The solution to this problem is to arrange for your XenServer user account to have the necessary permissions. Typically, you need the "VM power admin" role).

Configure AppDNA to run as administrator

1. If necessary, close AppDNA.

2. In Windows Explorer, locate the main AppDNA executable (called appTitude.exe). The table below shows the default location of this file.
3. Right-click the file and from the shortcut menu, choose Properties.
4. Click the Compatibility tab.
5. Under Privilege level, select the Run this program as an administrator check box.
6. Click OK to save the changes.

Machine type	Default location
64-bit	C:\Program Files\Citrix\AppDNA\Client

Remote Desktop Connection window does not open (vSphere or Hyper-V)

If you are using a vSphere or Hyper-V virtual machine, AppDNA attempts to open it in a Remote Desktop Connection window. This can fail in certain circumstances, such as when the AppDNA machine is joined to a domain but the virtual machine is not or the reverse. When this happens, configuring the hosts file on the AppDNA machine with the address of the guest OS can sometimes resolve the issue. The hosts file is a local file that Windows uses to map host names to IP addresses so that it can identify machines on the network.

To find out whether these steps are relevant:

1. If you have not already done so, find the application on the Install Capture tab, and click the icon in the VM column.
2. If AppDNA displays a “No such host is known” error in the AppDNA virtual machine remote controls window, try to ping the virtual machine from the AppDNA machine using the IP address or host name used to identify the guest OS in the virtual machine configuration.
3. If the ping is successful, follow the steps described below to configure the hosts file on the AppDNA machine with the address of the guest OS.
4. If the ping is unsuccessful, these steps may not be relevant. Instead, check that the virtual machine configuration is set up correctly within AppDNA. The easiest way to do this is to select the configuration on the Virtual Machine tab in Install Capture settings and click Edit. This opens the Virtual Machine Configuration Wizard, which performs checks and provides useful feedback when things go wrong.

To configure the hosts file on the AppDNA machine:

1. Locate the hosts file on the AppDNA machine. This file is typically named “hosts” and its location varies depending on which version of Windows you are using. On Windows 7, it is typically located in C:\Windows\System32\drivers\etc.
2. Open the file in a text editor, such as Notepad.

3. Add a line to the file that specifies the IP address and the host name of the guest OS separated by a tab character. For example:

   ```
   10.72.105.79 Win7HyperV
   ```

4. Save the file.

For information about the ping command and how to find out the IP address of the guest OS, see Virtual Machine Connection.

Before Snapshot Does Not Run

August 1, 2018

This topic provides troubleshooting tips for when the "Before snapshot" does not run when attempting to perform an Install Capture.

Note: Many Install Capture issues can be diagnosed and resolved by re-running the Virtual Machine Configuration Wizard (which performs a number of checks and provides targeted troubleshooting information when problems occur).

Check Remote Admin

Open the Windows Task Manager on the virtual machine and check whether RemoteAdmin.exe is running.

- If RemoteAdmin.exe is not running, it generally means that you need to install the AppDNA VM Configuration MSI. You may also need to take another snapshot of the virtual machine.
- If RemoteAdmin.exe is running, it may be that the virtual machine configuration is looking for it in the wrong location. Establish its location on the virtual machine. (The default location is C:\Program Files\Citrix\AppDNA\VM Configuration, or C:\Program Files (x86)\Citrix\AppDNA\VM Configuration on a 64-bit virtual machine.) Then check where AppDNA is looking for it and if necessary correct it.

Check and correct where AppDNA is looking for RemoteAdmin.exe:

1. From the AppDNA menus, choose Edit > Settings.
2. On the left side of the Settings dialog box, click Install Capture.
3. On the Virtual Machines tab, select the virtual machine configuration you are using and click Advanced. This opens the Virtual Machine Configuration Dialog Box.
4. Click the Replaceables tab and check that the value of the AppToolsFolder replaceable matches the correct location of RemoteAdmin.exe on the virtual machine. The default value for the AppToolsFolder replaceable uses the %APPDNAVMCONFIG% environment variable, which is cre-

ated by the AppDNA VM Configuration MSI and stores the actual installed location of Remote Admin.

5. If necessary correct the value of the AppToolsFolder replaceable.
6. Click OK and Save.

Note: If you have created your own execution profile or are using an older execution profile, the AppToolsFolder replaceable may not be used to specify the location of Remote Admin. You may then need to edit the execution profile to specify the correct location. See Edit an execution profile for more information.

If the virtual machine is still running, close down the virtual machine. Then start the Install Capture again. If this is not successful, follow the steps described in Troubleshooting Remote Admin connectivity.

No problem with Remote Admin

If, after checking and correcting problems related to Remote Admin as described above, you find that the virtual machine starts up but the "before" snapshot still does not run:

- Select the Troubleshoot Errors option for the VM in Edit > Settings.
- Check that the operating system in the virtual machine automatically logs in at startup.
- Check that the host and virtual machine IP addresses are valid.
- Check that the AppDNA machine can ping the virtual machine, and vice versa.
- Check that you can browse to the AppDNA machine from the virtual machine by using the UNC path (\\xxx.xxx.xxx.xxx\).
- Check that there are no login prompts when browsing to and from the virtual machine and that any passwords are saved or cached.

Installation Fails

August 1, 2018

This topic provides troubleshooting tips for when the installation step fails during an Install Capture – for example, if the virtual machine closes during the installation and the import fails. This may be because an unexpected error was encountered during the installation.

To troubleshoot issues:

1. Launch the virtual machine independently of AppDNA.
2. Check that you can browse from the virtual machine to the location of the installation package (as specified on the Import Applications screen) .

3. Attempt to launch the installation manually from the virtual machine using the same UNC path that was specified on the Import Applications screen.

This should reveal any errors, such as that the virtual machine cannot access the file, the file is missing, incorrect permissions, or the location of the installation file was not specified using a UNC path. If you are using a mapped drive, see "Mapped drive issues" below.

Check that there are no security warnings or prompts when launching the installation. If there are, the problem may be a characteristic of the specific installer. Try running the capture in manual mode.

After you have addressed any issues:

1. Close down the virtual machine.
2. If necessary, on the Install Capture tab in the Import Applications screen, correct the path to the installation file so that it is specified correctly using a UNC path.
3. Then try the import through AppDNA again.

If the installation continues to fail:

- Enable the Troubleshoot Errors option.
- If the problem is specific to a single application, run the capture in manual mode.

Mapped drive issues

If you are using a mapped drive for the input or output location, check that the same drive letter is mapped to the same location on both the AppDNA machine and the virtual machine.

If the guest OS is Windows 7, Windows 8, or another OS that supports User Access Control (UAC) and UAC is not completely disabled, a mapped drive that was created using the net use command may be inaccessible to Remote Admin during Install Capture. This can lead to Install Capture failing.

If you encounter this issue, instead of using net use, map the drive using the Map network drive option in Windows Explorer, and select the Reconnect at logon check box. Typically, this resolves the issue. For an alternative solution, see http://support.microsoft.com/kb/937624.

After Snapshot Does Not Run

August 2, 2018

This topic provides troubleshooting tips for when the Install Capture installation is successful, but the "After snapshot" does not run.

- Enable the Troubleshoot Errors option.
- Check to see if the issue affects another application, or just this application.

- If you are using the option to copy results, check that the output path is accessible from the virtual machine, that it can be written to, and that it does not require the input of user credentials.
- If the problem persists, run the after snapshot command manually in a command window to capture any other error messages.

Import Fails

August 1, 2018

This topic provides troubleshooting tips for when the Install Capture installation and "After snapshot" are successful, but the import of the MSI fails.

- Check that Direct Import is functioning correctly.
- Check that there is available space in the temporary directory and the SQL Server database.
- Check whether you can import the MSI that was generated in the output location using Direct Import.

Note: While the after snapshot can appear to complete, the problem may occur at the end of the after snapshot. To check whether the Install Capture completed, check for an MSI and associated folders in the output folder.

Remote Admin Connectivity

August 2, 2018

This topic provides troubleshooting tips for when there is a problem connecting to Remote Admin on the virtual machine during an Install Capture. Typically this will manifest as the "Before snapshot" failing to run.

Note: Remote Admin is an AppDNA agent that runs within the virtual machine during operations (such as Install Capture) that take place on a virtual machine. Remote Admin provides support for AppDNA to communicate with the virtual machine.

- If the virtual machine was started from a powered off state, check whether it has finished starting. Displaying the virtual machine in the console makes it easier to determine when the virtual machine has started.
- Check whether RemoteAdmin.exe is running on the virtual machine. To do this, open the Windows Task Manager on the virtual machine.

- If Remote Admin is running, check that the version of the Citrix AppDNA VM Configuration installed in the virtual machine matches the version of AppDNA you are using. To check the version of the Citrix AppDNA VM Configuration on the virtual machine, open Control Panel > Programs and Features. Click Citrix AppDNA VM Configuration in the list of programs to view the support information. To check the version of AppDNA you are running, from the AppDNA menus, choose Help > About.
- If Remote Admin is not running and you installed the Citrix AppDNA VM Configuration MSI on the virtual machine while you were working through this wizard, make sure that you have restarted the virtual machine. If you have done this and Remote Admin is not running, you may need to start Remote Admin manually. To do this, locate RemoteAdmin.exe in Windows Explorer on the virtual machine, and then double-click it. By default, RemoteAdmin.exe is located in C:\Program Files\Citrix\AppDNA\VM Configuration (or C:\Program Files (x86)\Citrix\AppDNA\VM Configuration on a 64-bit virtual machine). Then use the Windows Task Manager to check that it is running.
- Otherwise if Remote Admin is not running, it generally means that you need to install the Citrix AppDNA VM Configuration MSI on the virtual machine.
- If Remote Admin is running, check that you can ping the virtual machine from the AppDNA machine using the IP address or host name entered here, as described in "Ping the virtual machine" below. If the ping fails, check that the IP address or host name entered above is correct. If the virtual machine is connected to the domain, you must use the fully qualified domain name.
- Ensure that there is no firewall in the virtual machine or on the AppDNA client machine that is blocking the TCP communication with Remote Admin.
- If you chose not to display the virtual machine in the console, cancel out of the wizard and then start again. This time use the option to display the virtual machine in the console.

Confirm TCP communication is available to Remote Admin

You can use the Windows telnet command to confirm that TCP communication is available to Remote Admin. With the virtual machine running, from another Windows machine (but not the virtual machine) use telnet to connect to the machine.

To do this, type the following syntax at a command prompt:

```
telnet <guest OS netbios name or IP address> <port>
```

For example:

```
telnet InstallCaptureOS 54593
```

If the command console turns blank, it means a connection has been made. You should then immediately close the console using CTRL+] (If you do not do this, AppDNA will not be able to connect until Remote Admin is restarted in the virtual machine.)

Note: If
telnet is not installed, you can install it from
Control Panel > Programs and Features. Click
Turn Windows features on or off. This opens the Windows Features dialog box. Select the
Telnet Client check box and click
OK.

If telnet reports an error such as “Connecting to <machine>…Could not open connection to the host, on port <port>: Connect failed”, check that Remote Admin is running in the virtual machine, and ensure that it is listening on the correct port.

To do this, run the following at a command prompt in the virtual machine:

```
netstat -ab
```

If these conditions are satisfied, ensure that name resolution is working correctly, and that the correct name or IP address is being used. In addition, ensure that there is no firewall in the virtual machine or on the AppDNA client machine that is blocking the TCP communication with Remote Admin.

Access to the Shared Folder

August 1, 2018

Sometimes during the initial setup of a virtual machine for Install Capture, you may find that the virtual machine cannot access the shared folder where the input files (and the output files if you are using the option to copy the results) are stored. When this happens, you can use the following steps to attempt to determine the cause.

Note: These instructions assume that the shared folder is on the AppDNA machine. If the shared folder is on a different machine (such as a network share), adjust the instructions accordingly.

Test the virtual network adapter

Ensure the virtual network adapter is working properly within the virtual machine. To do this, open a command prompt on the virtual machine and type the following:

```
1 ping <Virtual machine IP address>
```

If the adapter is working properly you will see ping replies, such as:

```
1 Reply from 192.168.50.21: bytes=32 time<1ms TTL=128
```


If you do not see ping replies, repeat the configuration steps for the virtual machine network on the virtual machine.

Test the virtual network

To test the virtual network, type the following in a command prompt on the virtual machine:

```
ping <AppDNA machine IP address>
```

If the virtual network is working properly you will see ping replies from the virtual server host, such as:

```
Reply from 192.168.50.20: bytes=32 time<1ms TTL=128
```

If you do not see ping replies, check whether the firewall on the virtual machine or the AppDNA machine is restricting access to ICMP traffic and if so, correct it.

Test that the virtual machine can see the shared folder

To test that the virtual machine can see the shared folder on the AppDNA machine, type the following in a command prompt on the virtual machine:

```
net view \\<AppDNA machine IP address>
```

This should show the shared folder. If not, it means that the firewall on the virtual machine or the AppDNA machine is restricting access to SMB / CIFS traffic, or the user logged on to the virtual machine does not have the necessary privileges. If necessary, correct the issues.

List the files in the shared folder

Type the following in a command prompt on the virtual machine:

```
dir \\<AppDNA machine IP address>\<Shared folder>
```

This should show a listing of the files in the shared folder. If not, it means that the firewall on the virtual machine or the AppDNA machine is restricting access to SMB / CIFS traffic, or the user logged on to the virtual machine does not have the necessary privileges. If necessary, correct the issues.

Test that the virtual machine can access the shared folder

On the virtual machine, check that you can access the shared folder on the AppDNA machine. For example, type the following into the Windows Start > Run prompt:

```
\\<AppDNA machine IP address>\<Shared folder>
```

If this opens the shared folder on the AppDNA machine, it verifies that the virtual machine can access it.

Forward Path Script

August 1, 2018

Windows Script Host Error: Logon failure: unknown user name or bad password Code 8007052E

This error indicates that the virtual machine does not have access to a file path passed in the Forward Path script – typically in the $(App:InstallWrkDir) replaceable.

Installation of managed application fails

When using Forward Path to run Install Capture tasks on managed applications imported from Active Directory or ConfigMgr, the installation does not start if the path to the installation media is no longer valid. For example, this can happen if you have linked the managed applications to applications already imported into AppDNA from another location.

The solution is to re-map the path to the installation in the task script as follows:

```
Dim ImportedSourcePath As String = controller.Application.SourcePath
Dim WantedSourcePath As String = ImportedSourcePath.Replace
    (”\\Server\Share\Folder”, ”\\NewServer\NewShare\NewFolder”)
controller.Application.SourcePath = WantedSourcePath
controller.Application.InstallCommand =
    controller.Application.InstallCommand.Replace (”\\Server\Share\
       Folder”,
    ”\\NewServer\NewShare\NewFolder”)
```


Glossary

June 17, 2019

- **action RAG**

The RAG (red, amber, green) status of an application as it would be after the defined remediation actions have been implemented. For example, if the standard RAG is amber but remediation options are available, the action RAG would typically be green. However, if the standard RAG is red and the only remediation option is to redevelop the application, the action RAG is also red to indicate that complex development and/or replacement is required. The action RAG is sometimes known as the after action RAG or remediation RAG.

- **Active Directory**

A directory service from Microsoft, which provides a central location for network administration and security, single sign-on for user access to networked resources, standardization of access to application data, deployment and update of applications, and synchronization of directory updates across servers. All of the information and deployment settings are stored in a central database.

- **Action View**

A report view that provides a breakdown of the prevalence of the actions required to remediate the applications in your portfolio.

- **algorithm**

AppDNA uses algorithms to validate the suitability, interoperability, conflicts, and performance of applications on a variety of target platforms and virtualization environments. The algorithms are heuristic rather than based on rigid rules and are grouped into reports that relate to a target technology (such as Windows 7). Each algorithm is designed to identify applications that would potentially have a specific issue on the target platform. Applications that are identified as having this issue are said to trigger the algorithm. Algorithms are sometimes referred to as rules.

- **application DNA**

Metadata about the building blocks of an application, such as files, registry keys, and text-based information extracted from file headers. AppDNA uses this information to predict how the application will behave on a target platform.

- **application report view**

A report view that comes in two flavors, both of which provide access to detailed remediation reports for each application included in the report – Application Issues provides a summary of the standard and custom RAGs for the applications included in the report and shows the number of times each application has triggered an algorithm in each algorithm group; Application Actions provides a summary

of the standard and action RAG status of the applications included in the report, and of the actions required to remediate them.

- **client instruction files**

Control files used by the Self-Provisioning client to perform the capture or packaging task. Client instruction files are not human-readable instructions intended for end users.

- **complexity RAG**

An indicator of the complexity of an application. This is based on the number of files and registry entries the application has. You can set thresholds that define the three complexity levels (simple, normal, and complex) in Reporting Settings. The complexity RAG of an application is generally indicated by one or more circle. One circle indicates a simple application, two indicates a normal application, and three indicates a complex application.

- **custom RAG**

The standard RAG status of an application is determined by the algorithms built into the report. However, sometimes organizations want to raise an amber status to red or lower it to green, for example, depending on their specific needs. You can set the custom RAG for each algorithm in the Algorithm Groups screen. By default, the custom RAG is the same as the standard RAG.

- **Custom Report Manager**

Provides the ability to create new reports, algorithms, and algorithm groups based on existing algorithms or on new ones that you define yourself.

- **Direct Import**

The method by which a Windows application is imported into AppDNA when an .msi, .sft, or .appv file is available. This is the quickest way to get the application's DNA imported into the database.

- **discovered applications**

Applications whose usage has been tracked by SysTrack across the organization. Discovered applications are listed on the Discover Applications screen.

- **Effort Calculator**

Estimates the time, cost, and effort associated with migrating a portfolio of applications to a new platform.

- **Estate View**

A report view, available only for trial licenses, that provides a high-level overview of the state of your application portfolio on the target technology.

- **execution profile**

Controls the tasks and resources that are run on the virtual machine during an Install Capture. The default execution profile defines three stages, which analyze the virtual machine's state (including its complete file system and registry), installs the application, and then performs a second analysis of the virtual machine's state, respectively. The difference between the state of the virtual machine before and after the installation represents the changes made by installing the application. Execution profiles are also used in a similar way by Self-Provisioning.

- **external data**

Compatibility and remediation data that originates outside of AppDNA. For example, Microsoft provides information about applications that are known to work on Windows 7 and the Program Compatibility Assistant (PCA) database.

- **fingerprint**

A combination of an application's product name, manufacturer's name, version number, and the number of files and registry entries it has. When a Windows application is first imported into AppDNA, its fingerprint is stored. If the application is imported into AppDNA again, by default the application is considered the same if the fingerprint is the same or has not changed by more than 10%. However, you can override this behavior.

- **Forward Path**

A business decision engine that makes it possible to model different deployment scenarios and compare their impacts.

- **group**

A logical container for applications in AppDNA. Groups are similar to folders in Windows Explorer – they provide a way of structuring your application portfolio by user group, location, or application type, for example. Groups make it easy to review and report on the applications in the group separately from the rest of the portfolio. A group does not have an overall RAG status and it is not shown as a separate item in reports.

- **import**

The process by which application and OS image DNA is loaded into the AppDNA database.

- **Install Capture**

The process by which Windows applications are imported into AppDNA when an .msi, .sft, or .appv file is not available. Install Capture installs the application within a virtual machine and creates an MSI file which is then imported into AppDNA. Generally the MSI that is created simply captures the application's DNA for import into AppDNA and is not suitable for actually installing the application. With the necessary additional software, the capture process can create App-V sequences or XenApp packages.

- **integrated login**

An optional feature that enables AppDNA users to be logged into AppDNA automatically using their Windows user account credentials. This means that the logon screen is by-passed and the user does not need to enter their username and password.

- **Issue View**

A report view that provides a breakdown of the number of applications that triggered each algorithm within the report.

- **managed application**

An application that is deployed through Active Directory or Configuration Manager.

- **module**

A collection of reports for a particular context, such as Windows client or server. A report is made up of a suite of algorithms that relate to a target technology, such as Windows 8 or Windows Server 2012, against which the application DNA is evaluated. The algorithms are organized into algorithm groups.

- **MSI file**

Windows application installation package file. MSI files contain a relational database of text information about the application's files and registry entries. Some MSI files also contain the application's binary files, and sometimes the binary files are compressed and packaged in one or more separate CAB files or are uncompressed and unpackaged.

- **MST files**

Files used in conjunction with MSI files to transform or manipulate the installation package. MST files are not relevant to non-MSI installation files.

- **MST fix**

The way that MST files are delivered in AppDNA. The MST files contain modifications that are applied to an MSI file during installation to correct issues.

- **Non-MSI file**

A Windows application installation file that is not in the form of an MSI file. Typically non-MSI installation files are in the form of an EXE and sometimes they contain one or more MSI files.

- **RAG**

Refers to whether the application is marked as red, amber, or green. Green means that the application is likely to work on the target platform as it is and is ready for user acceptance testing (UAT) (although there may be issues that need to be addressed); amber means that it may fail or have impaired functionality although remediation is possible; red means that the application is likely or certain to fail. Some report views also provide the after action RAG (or remediation RAG), which shows what the RAG status would be after all the defined remediation actions have been implemented.

- **remediation report views**

Report views that provide detailed remediation information for individual applications along with an MST fix option, where relevant. There are two views – Remediation Issues and Remediation Actions. Web applications that have been captured by using the AppDNA directed spider have an additional Site Map view.

- **Remote Admin**

An AppDNA agent that runs within the virtual machine during operations (such as Install Capture) that take place on a virtual machine. Remote Admin provides support for AppDNA to communicate with the virtual machine.

- **replaceable**

A placeholder in an execution profile that is replaced by a value provided at run time.

- **reports**

Reports contain the algorithms that encapsulate the analysis that AppDNA performs on your applications to determine whether the application will have any compatibility issues on a particular platform or technology. The results can be presented in a variety of report views – Application Issues, Application Actions, Issue View, Action View, and the detailed Remediation report views. Trial licenses also provide an Estate View, a high-level view helpful for proof-of-concept installations.

- **scenario**

A script that defines the logic for a Forward Path report. The logic is applied to each application that is selected for inclusion in the report. The report has columns for application name, manufacturer, version, and source path, and the scenario logic provides values for an Outcome column and optionally for Cost, RAG, and Description columns, and up to 20 custom columns. If the logic puts RAG values in any of the custom columns, AppDNA automatically generates a pie chart summary of the results for that column when you run the report.

- **Self-Provisioning**

An alternative mechanism for capturing desktop applications for import into AppDNA and, depending on which execution profiles are available, for packaging applications for App-V or XenApp, for example. The capture and packaging take place on a separate machine from AppDNA. This can be any type of machine (virtual, physical, or VDI). Self-Provisioning can be used to delegate the responsibility for capturing and packaging applications to end users.

- **SFT file**

The largest and most important file in an App-V application. It contains all of the application's assets, including files and registry entries. In App-V 5.0, there is no longer an .sft file – it has been replaced by the .appv package.

- **shim**

A general computing term that refers to a small file of executable code that allows legacy applications to work after features that they rely on become obsolete. Shims are not intended to be a permanent solution but rather a temporary solution until the applications can be updated to no longer use the obsolete features.

- **site**

A named database and AppDNA web site combination. You specify which site you want to use when you log on to AppDNA. AppDNA then uses the site to connect the AppDNA client to the specified AppDNA web site and database. Once you are logged in, you can switch site (and therefore database) by using the
Switch Site pop up list in the lower left corner of the main AppDNA screen. The ability to have multiple databases is useful for companies who want to test their web applications separately from their desktop applications, for example. Using multiple databases is also useful for system integrators who need to test several customers' application portfolios at the same time.

- **spider**

A program that automatically crawls over web pages, following links, and creating copies of all of the pages visited.

- **standard RAG**

The RAG (red, amber, green) status of an application determined by the algorithms built into the report.

- **System Center Configuration Manager**

A Microsoft systems management tool for managing large groups of Windows-based computer systems. Configuration Manager provides remote control, patch management, software distribution, operating system deployment, network access protection, and hardware and software inventory. Like Active Directory, all of the information and deployment settings are stored in a central database.

- **SysTrack**

A suite of IT business intelligence products from Lakeside Software. SysTrack includes functionality that audits and tracks application use within the enterprise. AppDNA uses the results of this tracking in the Discover Applications screen.

- **task script**

A script that defines an action to be performed for a value in the Outcome column generated by a Forward Path scenario. For example, if an application virtualization scenario marks an application with a green RAG status, a task script can automatically sequence that application using the App-V sequencer and publish the sequence to a test environment for immediate testing.

- **virtual machine configuration**

A collection of configuration settings that enables Install Capture to fire up and communicate with the virtual machine and retrieve the generated output. You can create multiple virtual machine configurations to meet different requirements and then select the one you want to use when you start the Install Capture.

