KACE® Desktop Authority 11.3.2

Installation and Upgrade Guide

© 2025 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document..

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

20 Enterprise, Suite 100

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

> **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

> An information icon indicates supporting information.

Desktop Authority - Installation and Upgrade Guide
Updated - October 2025
Version - 11.3.2

Contents

Introduction **4**

Scope **5**

Desktop Authority versions **6**

Installation backup **8**

Frequently asked installation questions **9**

Installation worksheet **10**

Installing Desktop Authority for the first time **12**

Upgrading Desktop Authority **27**
- Express upgrade 28
- Custom upgrade 28
- Uninstall 41

Uninstalling Desktop Authority **42**

Registration **49**

Desktop Authority ports and configurations **53**

File Paths **57**
- Server side 57
- Client side 59

About us **61**
- Technical support resources 61
  - Tools 61

Index **62**

1

Introduction

Desktop Authority is a desktop and server management platform for Microsoft Windows™. Desktop Authority's design strives to provide a top-tier end-point management solution with a strong focus on ease-of-installation and ease-of-use for the network administrator.

2

Scope

This document aims to describe the protection mechanism of Desktop Authority component *SLAgent* being used in the DA Client Software.

Desktop Authority versions

Desktop Authority is supported in three versions, Desktop Authority Professional, Desktop Authority Standard and Desktop Authority Essentials. Desktop Authority Essentials is a scaled down version of Desktop Authority Professional. It does not include the following standard features included by default in the full version -- Software Management, USB/Port Security, Hardware and Software Inventory and Custom Reporting and the Desktop Authority Remote Management tool.

NOTE: Currently only the Standard version of Desktop Authority is available for purchase by new customers.

Feature	Professional/Standard	Essentials
Desktop Configuration	✓	✓
Power Management	✓	✓
Group Policy Template Import	✓	✓
Wake On LAN	✓	✓
Role Based Administration	✓	
Remote Management and Control	✓	
Reporting of user logons and activity	✓	
Reporting of administrator activity	✓	
Software Deployment	✓	

Feature	Professional/Standard	Essentials
Hardware and software inventory	✓	

Desktop Authority is licensed based on the total number of unique seats which are managed in whole or part by Desktop Authority. A “Seat” is a desktop, laptop, or workstation computer, or thin-client session or any other user computing device.

For answers to any Desktop Authority Licensing questions refer to our licensing Knowledge Base article (186762).

4

Installation backup

It is strongly recommended to perform all of the following backup steps in order to assure a successful recovery should your upgrade fail for any reason. Without these backups, we will be unable to support you should you need to recover your Desktop Authority data.

- The Installer will prompt to backup existing databases during the install process.
- In addition to performing a backup of the databases, it is also good practice to backup existing Profiles before upgrading. Right-click on each profile name and select “Export Profile…”. Select a location to save the profile and click **OK**. Repeat for each profile.

Frequently asked installation questions

Why does the installation require Administrative rights?

The user performing the installation of Desktop Authority is required to have Administrative privileges on the member server it is being installed to. Desktop Authority is not alone in this requirement. Most software installations require this privilege level as well.

With Administrative privileges, Desktop Authority will be able to install any of the required prerequisites, extract the installation files, install and configure IIS as well as install the Ops Master service and write to the HKLM registry on the server.

Where should Desktop Authority be installed to?

It is recommended that Desktop Authority to be installed on a Member Server within the network rather than a Domain Controller. This recommendation is made based on the notion that most companies do not like to install programs to their Domain Controllers because disk space is used, the registry may be modified and there exists the possibility that the server may need to be rebooted. To avoid all of this and protect a Domain Controller from unwanted changes, opt to install Desktop Authority to a Member Server on the network.

Installation worksheet

Use the following worksheet to prepare for your Desktop Authority installation. It will help you gather all of the information required by the install prior to getting started.

Database requirements

Desktop Authority can install a local instance of MS SQL Server Express Edition or can use an existing SQL Server Instance. On Windows Server 2008, Microsoft SQl Server 2008 R2 Express will used. On all other supported operating systems, Microsoft SQL Server 2014 R2 Express will be used. Select the appropriate option in the dialog.

If you plan to install a local instance of MS SQL Server Express, Desktop Authority will install the necessary software. You will be prompted for an SA password.

MS SQL Server Express Credentials
SA Password

If you will be using an existing SQL Server Instance (2008, 2008 R2, 2012, 2014, 2016, 2017), you will need to know the server name and optionally the instance name. It must be entered in the form of SERVERNAME\INSTANCE.

MS SQL Server Credentials
SEVERNAME\ [INSTANCE]

MS SQL Server Authentication
SA Username

Desktop Authority required services

The Desktop Authority Master services are comprised of the Operations and Manager services and are background services that are used to push data through the system. The Operations and Manager services can be configured using the same user account.

The Operations service is a background service that is used to manage and configure Desktop Authority's plugins. The ETLProcessor and ReportScheduler plugins are used to manage collected data and execute scheduled

reports. The Operations service requires a user account that is a local administrator of the Operations Master server.

The Operations service uses port 8017, by default, for communications. If this port is in use, choose another available port to use for this service.

Operations Service Credentials
Username (Domain\username)
Password
Port

The Manager service is used to manage the Web based Manager, replication, and connectivity and communication between the Manager and the database. It requires a user account that is a local administrator of the Operations Master server and any other servers that will run Desktop Authority services. This service account is also used when browsing out to Active Directory objects, files and folders and for GPO deployment unless the system preference option, 'Use current user rights for browsing resources' is selected.

The Manager service uses port 8085, by default, for communications. If this port is in use, choose another available port to use for this service.

Manager Service Credentials
Username (Domain\username)
Password
Port

Choosing a Super User

During the install you will be prompted to select a user or group who will be given Super User status and will therefore have access to all features of Desktop Authority.

Super User Group or User Account
Super User/Group (Domain\username)

IIS configuration

Desktop Authority's web based Console uses IIS to host the application. The IIS Application pool identity is used to allow IIS to host web applications/virtual folders as standalone processes to avoid application crashes. IIS requires access to port 443. Domain user credentials are required so it can log information to the database. If Windows Authentication is chosen for the SQL database authentication, the account selected for the IIS Application pool will need to have login access to the database.

IIS Application Identity Pool
Username (Domain\username)
Password

Installing Desktop Authority for the first time

The Desktop Authority installation requires administrative rights. If you are not logged on as an administrator, please log on as an administrator before beginning the installation.

Are you upgrading your current version of Desktop Authority? Desktop Authority 11.3.2 supports upgrades from Desktop Authority 9.3 or later. If you have an earlier version of Desktop Authority, you must upgrade to 9.3 first.

The Desktop Authority installation wizard will walk you through a series of dialogs prompting for information that is needed to install and configure Desktop Authority for your organization. Follow the wizard by entering the requested information and clicking Next to advance to the following page. Click Back to go to the prior page. Click Cancel to abort the install.

Note: If the installation is aborted, all configurations previously entered during the installation process are saved and used the next time the installation is run.

Desktop Authority supports Microsoft SQL Server and Express Editions of 2008, 2008 R2, 2012, 2014, 2016, 2017, and 2019. If you are using a version of SQL Server prior to 2008, please read the Knowledge Base article which describes how to convert your data to a newer version for use with Desktop Authority.

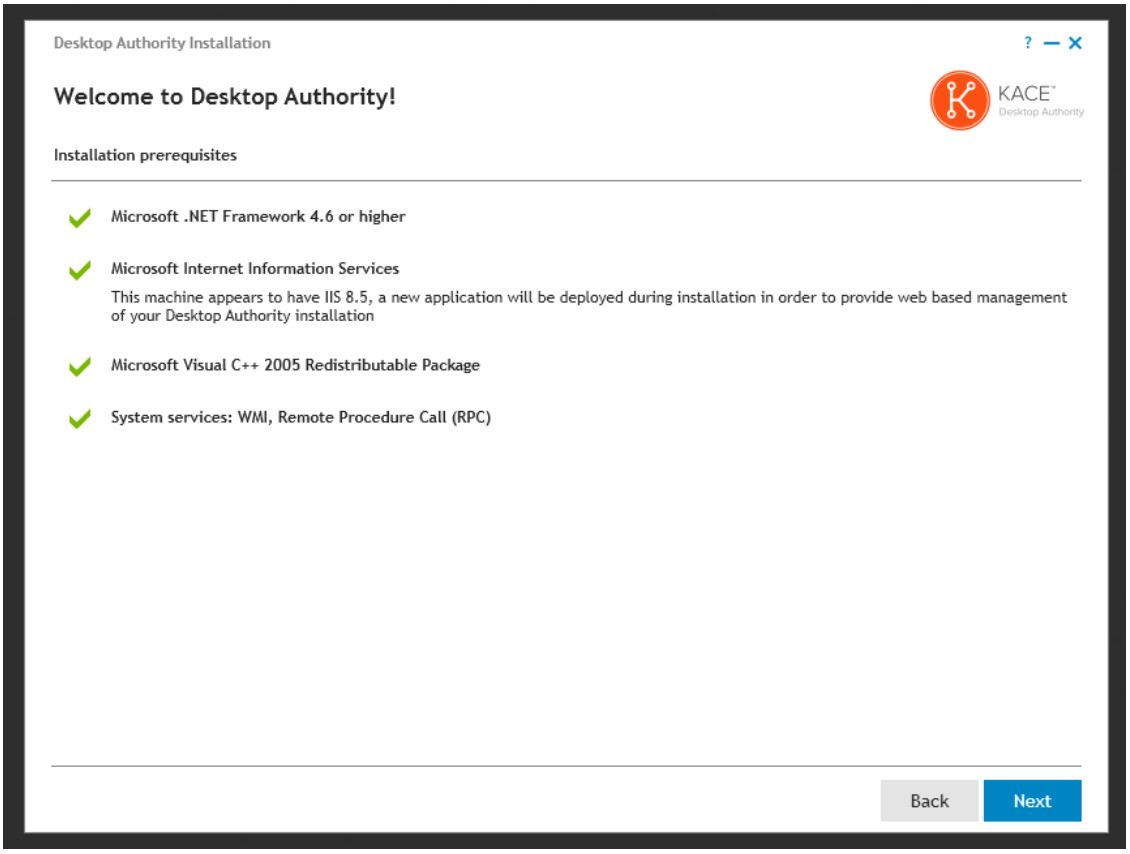
1. Begin the installation by double-clicking on the DesktopAuthority.exe icon. The software prerequisites and hardware requirements will be checked and the setup files will be extracted and executed. This initial step of the install will also check privileges, the OS version, determine if .NET 4.6 is installed and present the license agreement for approval. If .NET 4.6 is not found, the installer will attempt to download it and then install it. The License Agreement must be accepted and .NET 4.6 must be detected or the installer will not continue.

   NOTE: Some Anti-Virus programs have been known to interfere with Desktop Authority processes. This version of Desktop Authority uses a new folder structure on all desktop computers. Be sure to update your Anti-Virus folder exceptions to include scanning of the following folders:

   - C:\Desktop Authority
   - C:\Program Files (x86)\Quest

   TIP: In the event there is no Internet connection, .NET 4.6 can be downloaded from http://webservices.scriptlogic.com/links/?DADownloads=dotnetfx35&Ver=11.0 and installed prior to continuing with the installation.

2. The next dialog describes the required prerequisite components that Desktop Authority will install, if necessary. Click the install option for each prerequisite component that is not already installed as indicated by the yellow warning icon.



The prerequisite components include:

- Microsoft .NET Framework 4.6
  http://webservices.scriptlogic.com/links/?DADownloads=dotnetfx46&Ver=11.0
- Microsoft IIS 7, 7.5, 8, 8.5 or 10 depending upon the Operating System of the server

  - IIS 7 will be installed to 2008 servers
  - IIS 7.5 will be installed to 2008 R2 servers
  - IIS 8.0 will be installed to 2012 servers
  - IIS 8.5 will be installed to 2012 R2 servers
  - IIS 10 will be installed to 2016 and 2019 servers

The default installation of IIS does not install a few components that are required by Desktop Authority. If these components are missing, the Desktop Authority install will allow you to install the missing components by pressing the Add Features button.

These extra IIS components include the following:

HTTP Errors, Application Development, ASP.NET, .NET Extensibility, ISAPI Extensions, ISAPI

Filters, Tracing, Windows Authentication, Dynamic Content Compression, IIS Management Scripts and Tools and Management Services.

- Microsoft SQL Server 2008 R2 Express Edition (only required if this is the selected database during the install)http://webservices.scriptlogic.com/links/?DADownloads=SQLExpressx64&Ver=11.0 x64 versionhttp://webservices.scriptlogic.com/links/?DADownloads=SQLExpressx86&Ver=11.0 x86 version
- Microsoft Visual C++ 2005 Redistributable Package http://webservices.scriptlogic.com/links/?DADownloads=vcredistx86&Ver=11.0 x86 version http://webservices.scriptlogic.com/links/?DADownloads=vcredistx64&Ver=11.0 x64 version

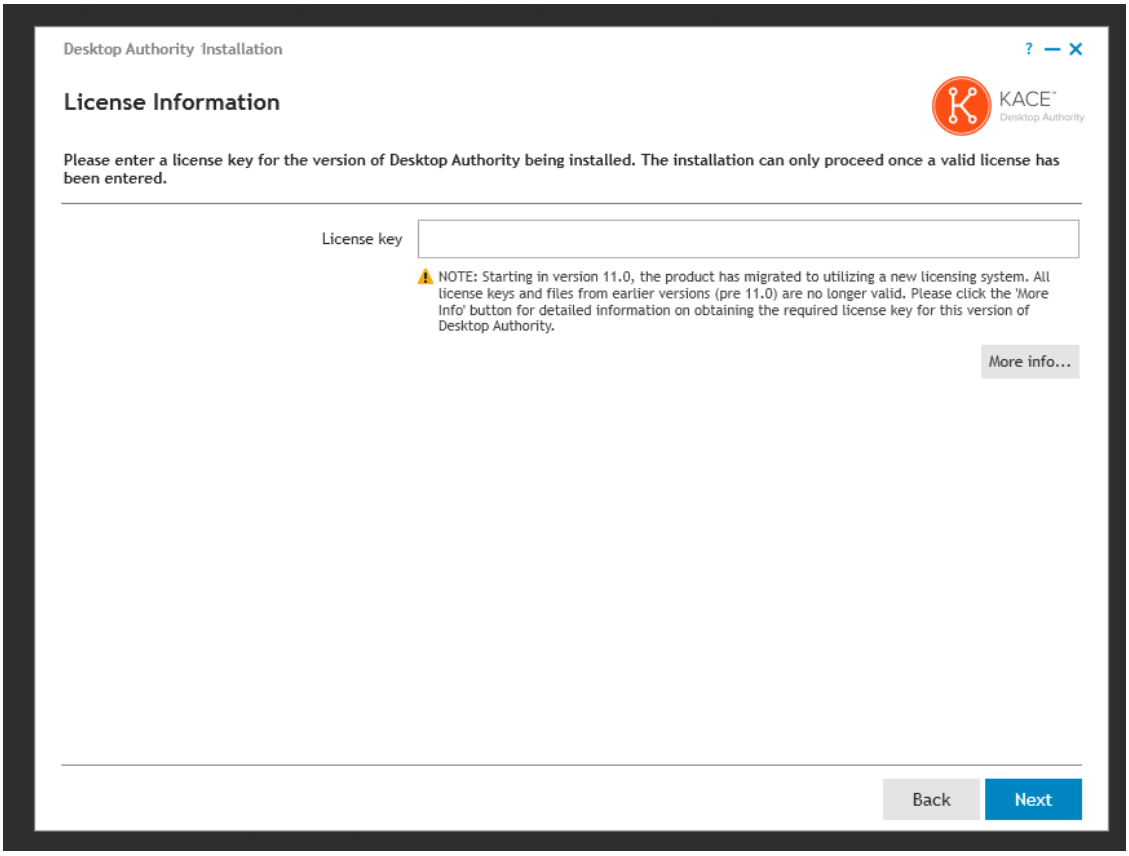
In addition, the installer will configure the following:

- Windows Firewall Exceptions (This will enable an exception for the File and Printer Sharing service)
- WMI and Remote Procedure Call (RPC) system services are used to install and configure Desktop Authority services remotely. They will be turned on during installation.

Note: If there is no Internet connection available on the machine where Desktop Authority is being installed to, the prerequisite components can be downloaded prior to starting the installation and placed in a folder of your choice. During the install, you will be prompted to choose the file path.

Once all prerequisites are installed click **Next** to continue.

3. Enter your license key.



Click **Next** to continue.

4. Desktop Authority requires an instance of either Microsoft SQL Server 2008, 2008 R2, 2012, 2014, 2016, 2017, 2019 or Microsoft SQL Server 2008, 2008 R2, 2012, 2014, 2016, 2017, 2019 Express Edition. The database is used to store all configurations as well as a data collection repository for reporting. Desktop Authority can install a new instance of SQL Server Express or use an existing SQL Server instance. On Windows Server 2008, Microsoft SQl Server 2008 R2 Express will used. On all other supported operating systems, Microsoft SQL Server 2014 R2 Express will be used. Select the appropriate option in the dialog.

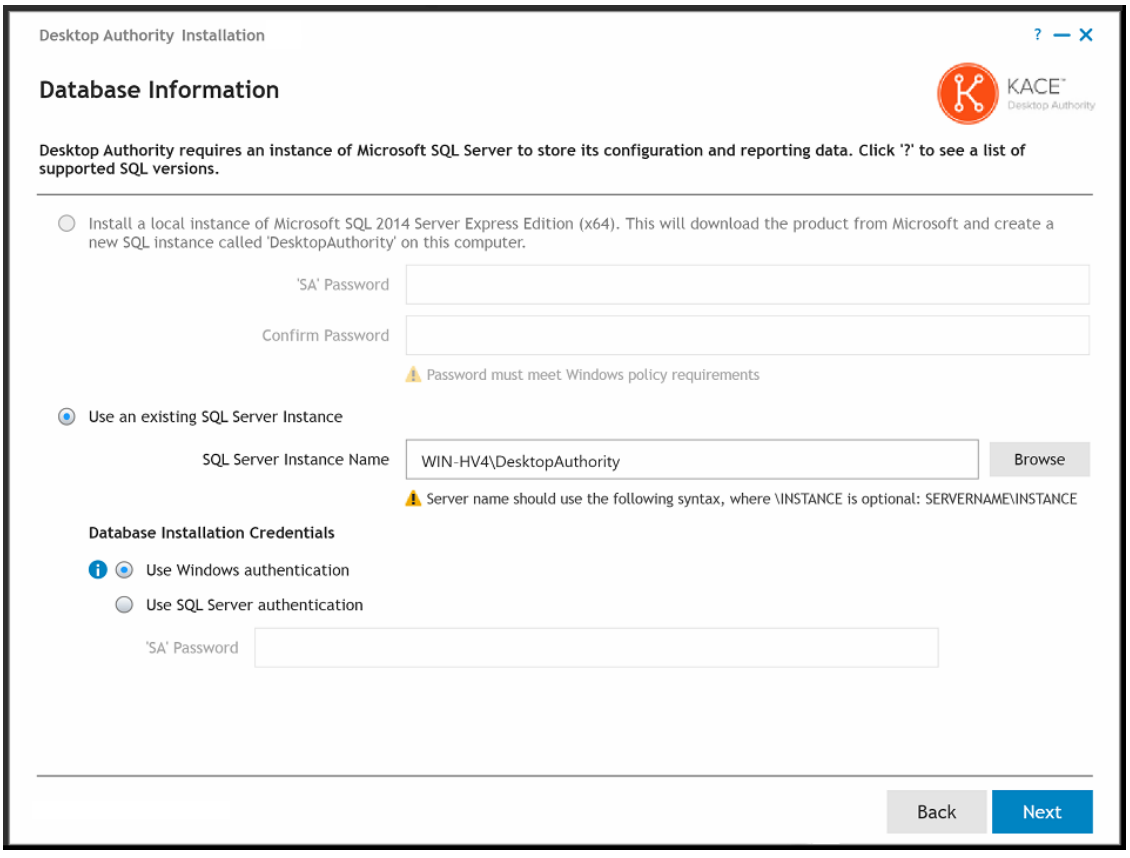
   When selecting to have Desktop Authority install a local instance of SQL Express, you must supply an 'SA' password. The new instance will be installed using Mixed Mode authentication (uses both Windows Authentication and SQL Server Authentication) which requires an 'SA' account. This password is required and must meet the password complexity policies set for the domain.

   When selecting to use an existing SQL Server instance, type in the SERVERNAME\INSTANCE or press the Browse button to select an existing instance. During an upgrade, the SQL Server Instance Name will automatically be entered for you. After choosing an existing SQL Server instance, select an authentication method for it. Select either Windows or SQL Server authentication.

   > ⓘ Note: To use Windows Authentication for an existing instance of Microsoft SQL Server, you must ensure that the user ID that you are currently logged into Windows with is assigned to the SQL Server 'System Administrators' server role.

   If Microsoft SQL 2008 R2 Server Express Edition (x86/x64) is being used, it will be downloaded at this point, if necessary.

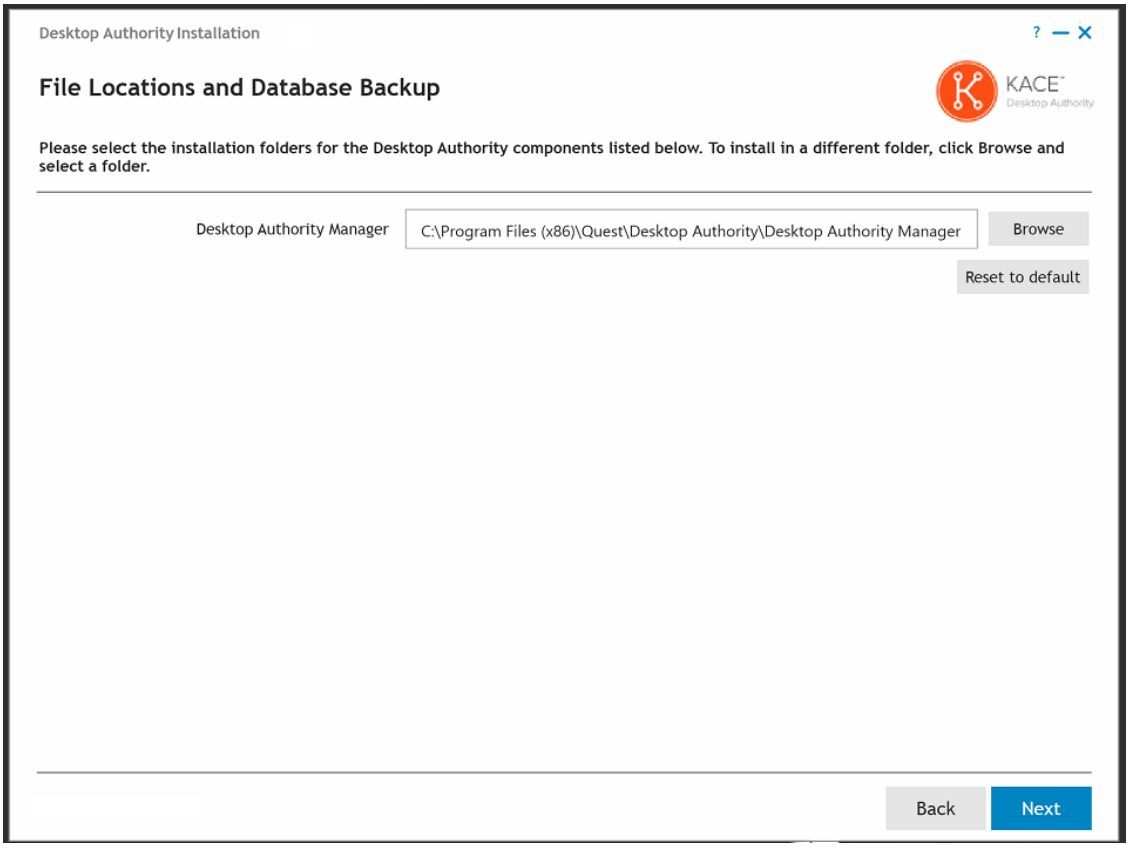
   - http://webservices.scriptlogic.com/links/?DADownloads=SQLExpressx64&Ver=11.0 x64 version
   - http://webservices.scriptlogic.com/links/?DADownloads=SQLExpressx86&Ver=11.0 x86 version



Click **Next** to continue.

5. Select a path and destination folder for the SQL Server Express Database (if selected) and the Desktop Authority Manager. Please reference the File Paths table in the appendices for default path locations. Press the **Browse** button next to the desired component to select a different path. Once the file locations are set, click **Next** to continue.

   Note: The SQL Server Express Database installation folder option will only be available when Desktop Authority is installing a local instance of Microsoft SQL Server Express Edition.



6. The Desktop Authority Master services are composed of the Operations and Manager services and are background services that are used to push data through the system. The Operations and Manager services can be configured using a single user account.

   The Operations service (formerly known as the Master service) is a background service that is used to manage and configure Desktop Authority's plugins. It will reach out to each server on the network where the Desktop Authority Administrative service is installed (SLETL$ share). The user account used to configure this service must have appropriate permissions to access the share. The ETLProcessor and ReportScheduler plugins are used to manage collected data and execute scheduled reports. The Operations service requires a user account that is a local administrator of the Operations Master server.

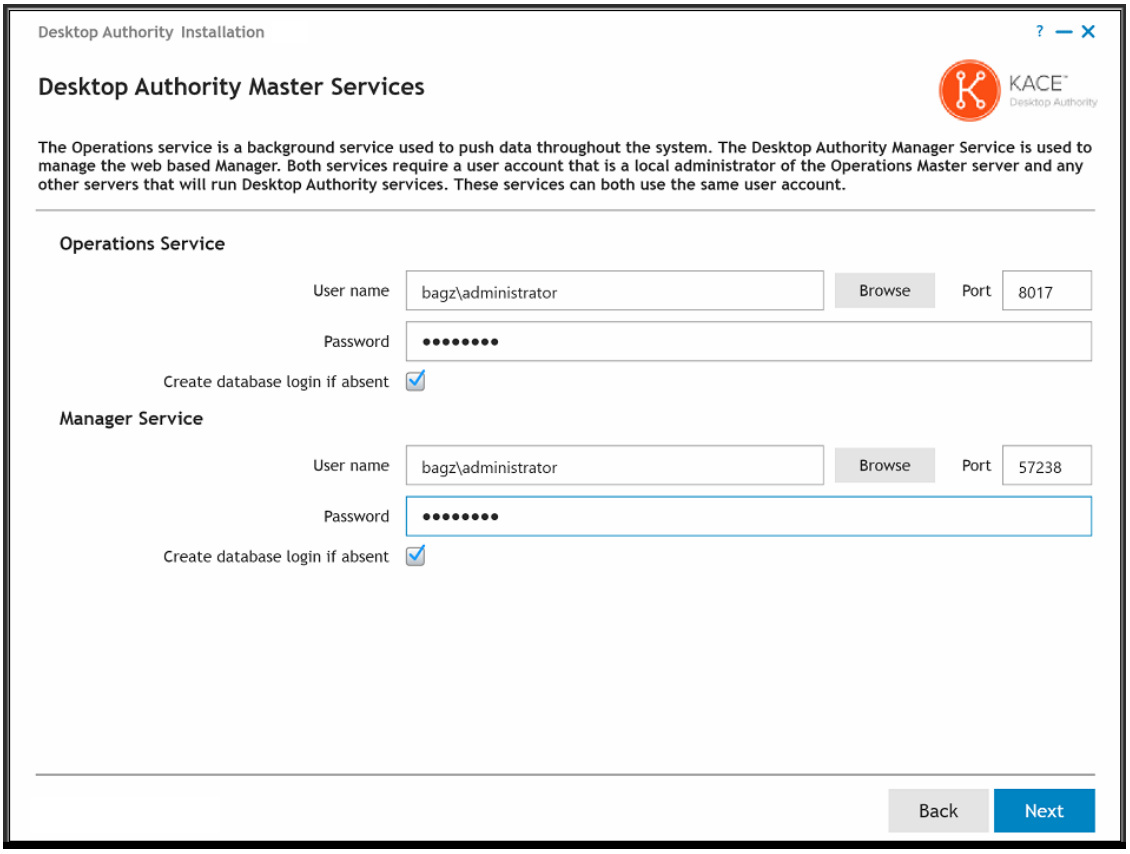
   The Desktop Authority Manager service (formerly known as the OpsMaster service) is used to manage the Web-based Manager, replication, assign scripts, and connectivity and communication between the Manager and the database. It requires a user account that is a local administrator of the Operations Master server and any other servers that will run Desktop Authority services. This service account is also used when browsing out to Active Directory objects, files and folders and for GPO deployment, unless the system preference option, 'Use current user rights for browsing resources' is selected. This option can be changed in the Desktop Authority Setup Tool on the Global System Settings tab.

   The default ports for these services are 8017 and 57238. If either of these ports are being used, a new port must be selected. The installer will check each port for usage and will notify you if they are currently in use. However, if you know that some other application uses either of these ports (but is not currently running) be sure to change them on this dialog. These ports may be changed at a later point in time using the Desktop Authority Setup tool.

   Click the **Browse** button to select an appropriate user account and enter the credentials for each service. Check the box to create a database login if necessary.

   Modify the default ports if necessary.

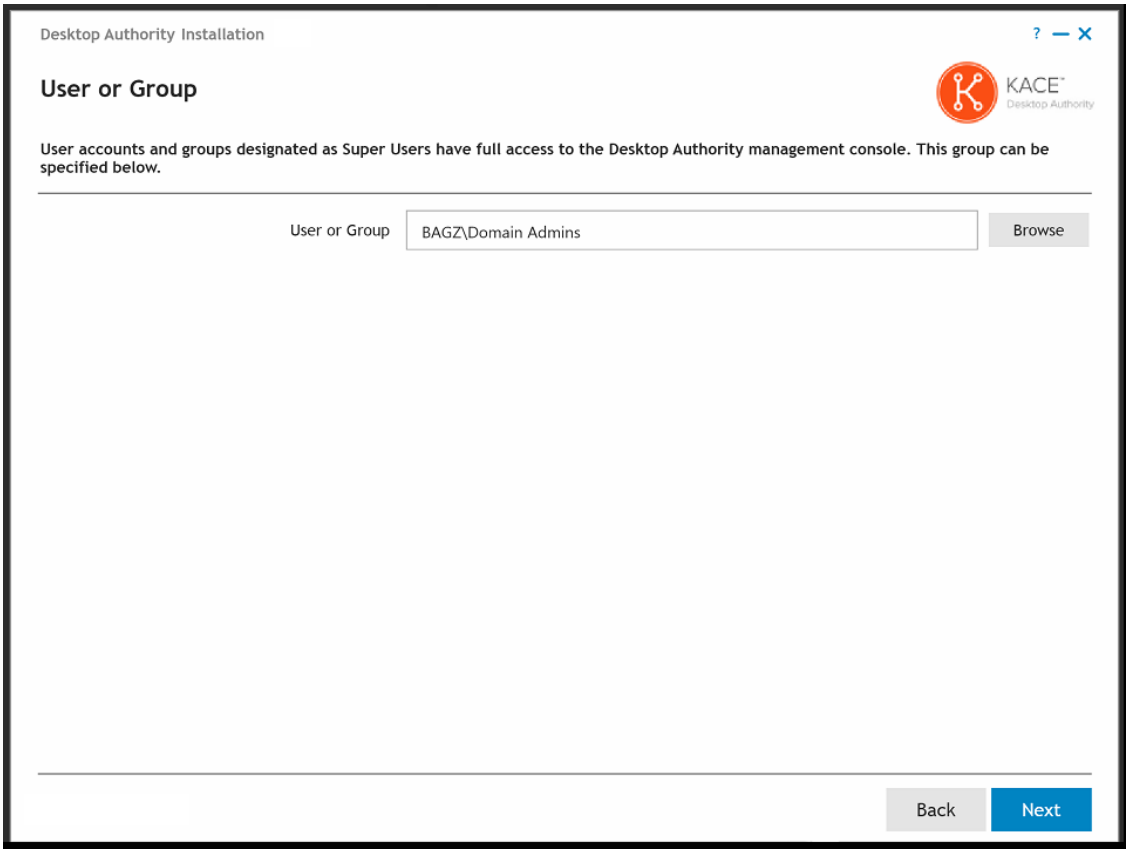
   > Note: If Windows Authentication is chosen for the SQL database installation credentials, the accounts selected for the Operations and Manager services should have login access to the database. Select the **Create database login if absent** checkbox to allow the installer to create a SQL login for these accounts. Otherwise, they should be created manually. This option is only available when Windows Authentication is chosen for SQL.



Click **Next** to continue.

7. The User or Group dialog gives you the opportunity to designate a User or Group as the Super User(s). Any user (or users within a group) designated as a Super User will be given full control in the Desktop Authority Manager. Click the **Browse** button to select the appropriate User or Group.

   Note: The user account of the person installing Desktop Authority will automatically be added as a Super User.



Click **Next** to continue.

8. ## IIS Application Pool

> Note: The IIS Application pool identity section is available when using SQL Windows Authentication only.

The IIS Application pool identity is used to allow IIS to host web applications/virtual folders as standalone processes to avoid application crashes. Select a Domain User account for the IIS Application pool to use. This account will automatically be granted the necessary permissions if needed.

If Windows Authentication is chosen for the SQL database installation credentials, the account selected for the IIS Application pool will need to have login access to the database. Select the **Create database login if absent** checkbox to allow the installer to create a SQL login for these accounts. Otherwise, they should be created manually.

Website Configuration

The Website Configuration dialog is used to configure the Web based console (Manager). These configurations are made in Internet Information Services (IIS).

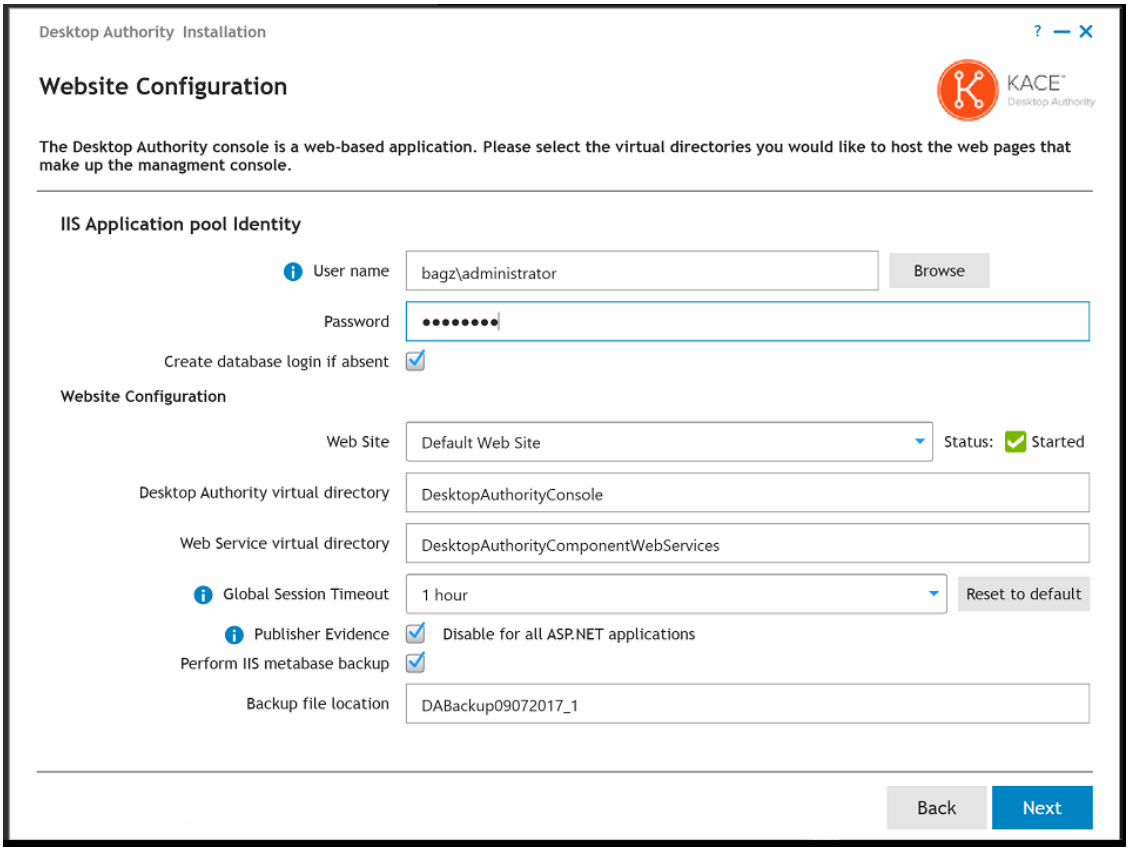
The Web Site selection allows you to configure Desktop Authority to use a site other than the default site in IIS. If you choose to use a site other than the default, it must be created prior to getting to this part of the installation. The selected site must have an HTTP port binding defined for it.

Specify Desktop Authority and Web Service virtual directories. Please reference the File Paths table in the appendices for default path locations. IIS Virtual directories are mapped to these folders.

The Global Session Timeout value is the maximum amount of time the Desktop Authority Console can sit idle before logging the user out due to inactivity. This timeout value can be overwritten for individual users in the Desktop Authority Console Preferences dialog.

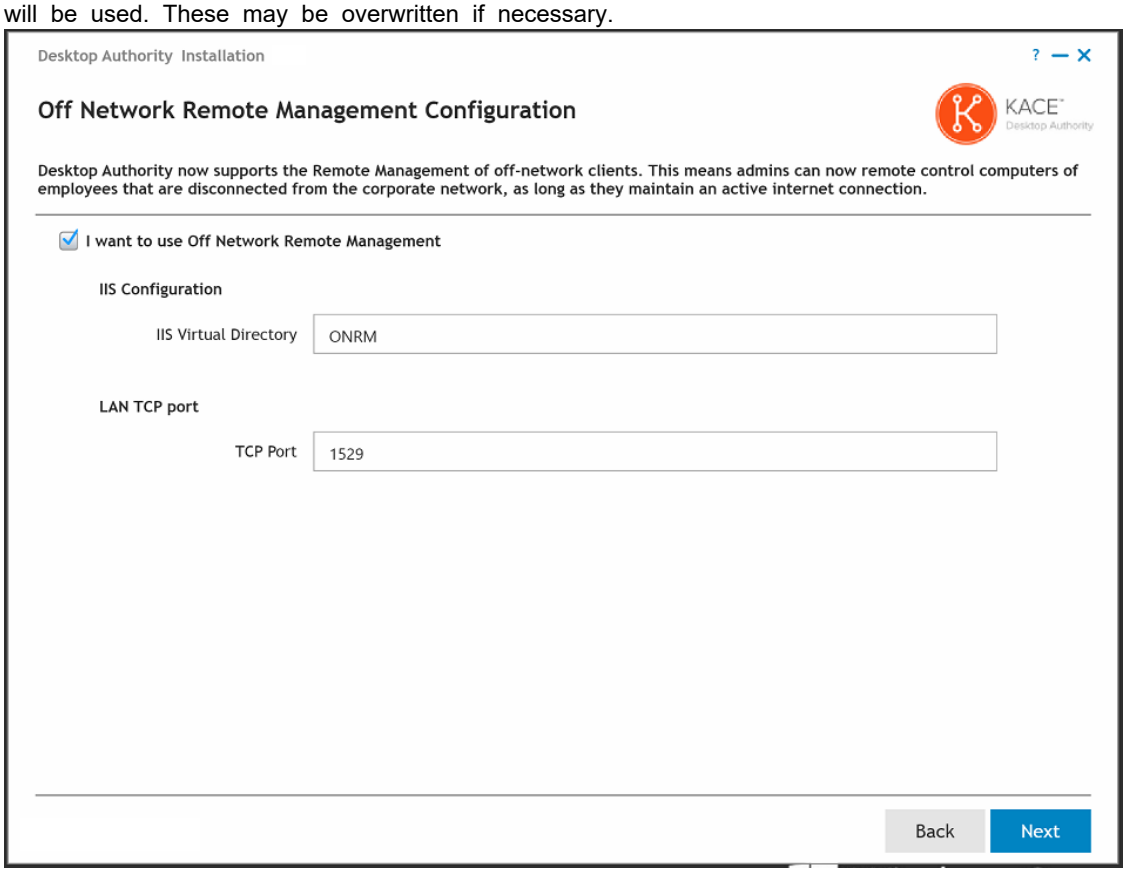
Publisher Evidence will disable for all ASP.NET applications to disable .NETs automatic validity checking of Authenticode signed signatures at startup. If publisher evidence is not disabled, some services may fail to start correctly at boot time due to lengthy delays imposed by the verification process.

Since Desktop Authority updates IIS, you have the option of performing a backup of IIS before any changes are made. It is recommended to always perform this backup of IIS since there is a possibility that other applications on the same site may conflict with each other. If there are any IIS problems following the install, the backup can be restored. Select the IIS metabase Backup option to enable the backup. The backup file created in the %systemroot%\system32\inetsrv\MetaBack folder. The default file name is created using a date, time format.



Click **Next** to continue.

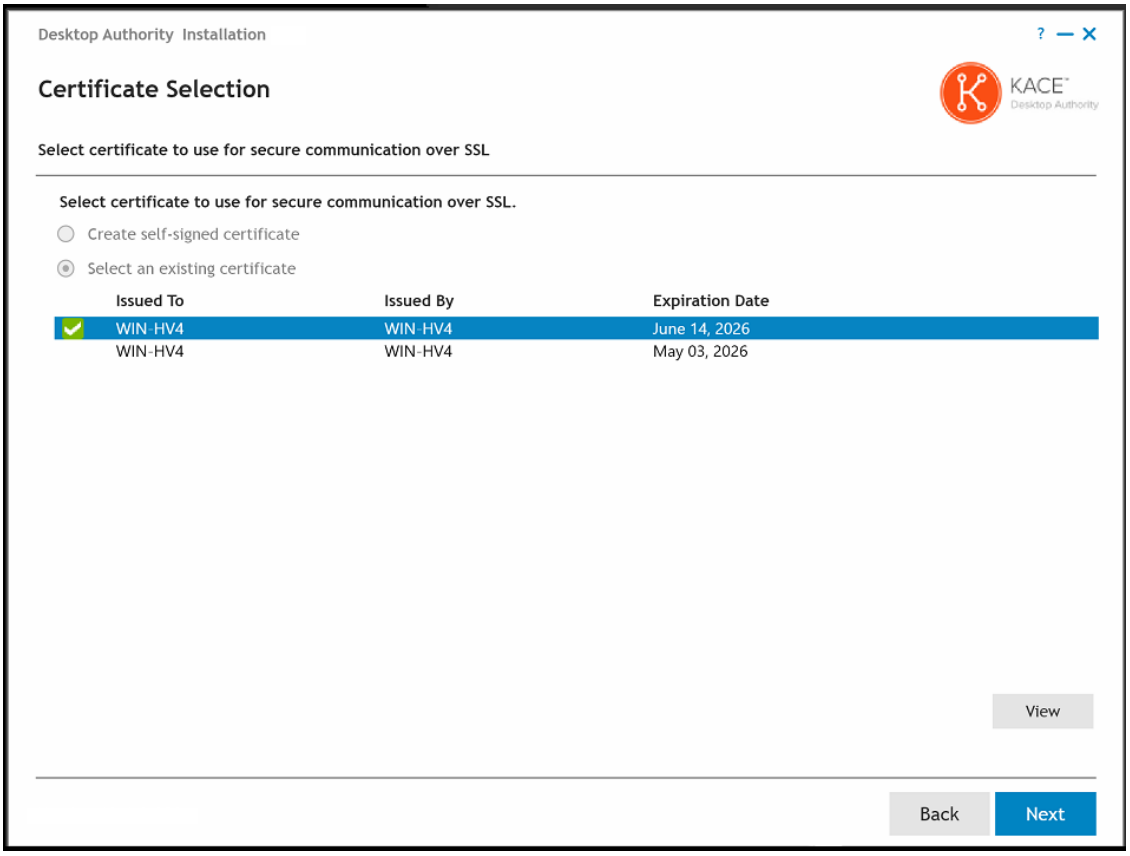
9. In order to remotely manage a client that is off-network, you must configure the feature here during install (or later in the DA Setup tool). Turn on the feature by selecting the **I want to use Off Network Remote Management** check box. A default **IIS Virtual Directory** and **LAN TCP Port** will be used. These may be overwritten if necessary.



10. Security certificates are used to ensure secure communication traffic.

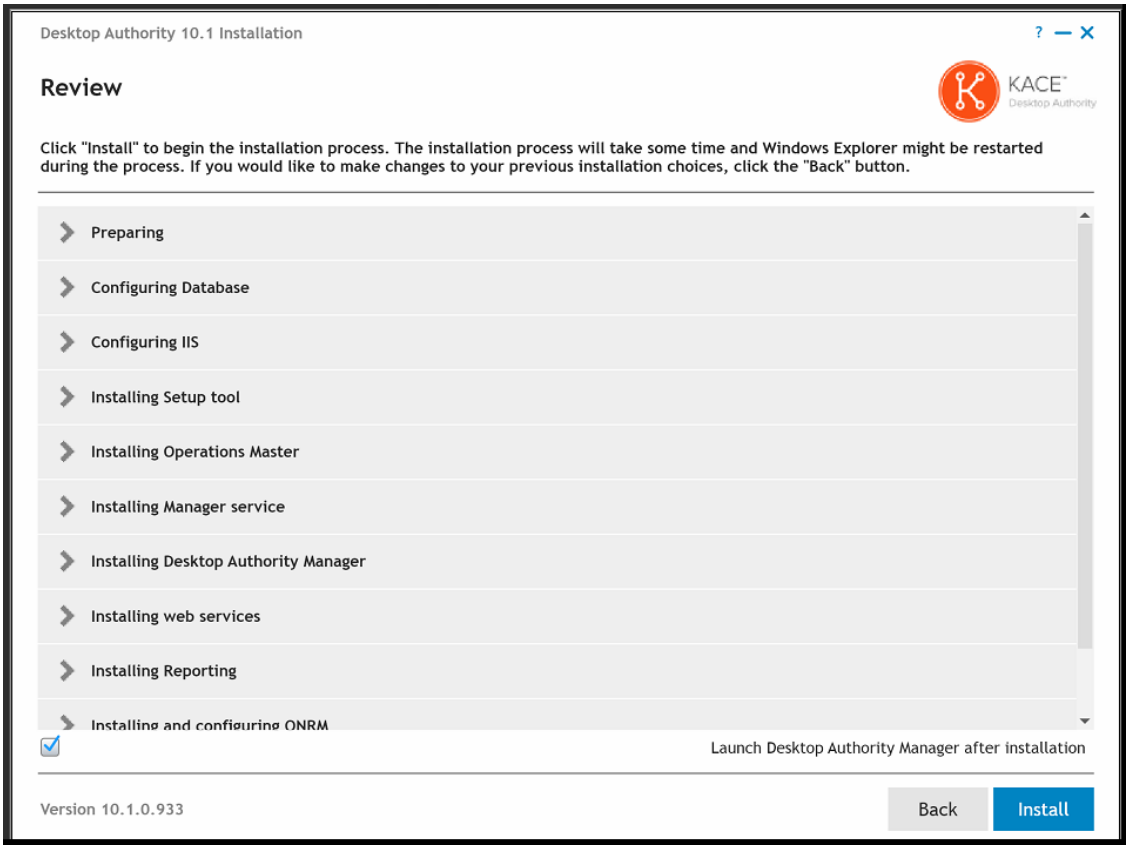
    If there are no certificates available on the server, select the **Create self-signed certificate** option and a new self-signed certificate will be created automatically for use with Desktop Authority.

    However, if there are installed certificates on the server and none with the Desktop Authority name, choose either to create a new self-signed certificate or select an existing certificate to use. If a previous Desktop Authority certificate is found, it will be selected from the list of existing certificates.



Click **Next** to continue.

11. The installation is about to begin. To run Desktop Authority following the installation of its files, click the *Launch Desktop Authority Manager after installation* checkbox. Click **Install** to proceed with the installation.



12. Once **Install** is clicked, the installation will begin. As the install proceeds, each section of the process will automatically be expanded to show the details and progress of the installation. If an error is detected, you may click on the section where the error is shown for more detailed information. You will be given an option to roll back the installation. Depending upon the error that occurred, the roll back may be mandatory or optional.

    Once the installation is complete, click the **Finish** button. If you previously chose to load Desktop Authority following the installation, the Desktop Authority web console will be loaded in your default browser. You will be presented with a login dialog.

13. Login to the Desktop Authority console by using a valid Active Directory user name, password and domain.

Quest
Desktop Authority™
BAGZ\adminx
Password
Domain: BAGZ
Use Windows authentication
Log In

Upgrading Desktop Authority

The Desktop Authority Installation will detect your current version of Desktop Authority. If this version of Desktop Authority is prior to Desktop Authority 9, you will be prompted with a dialog to remove it. **ALL data will be saved during the removal process; however you should always perform a backup before installing any product upgrade.**

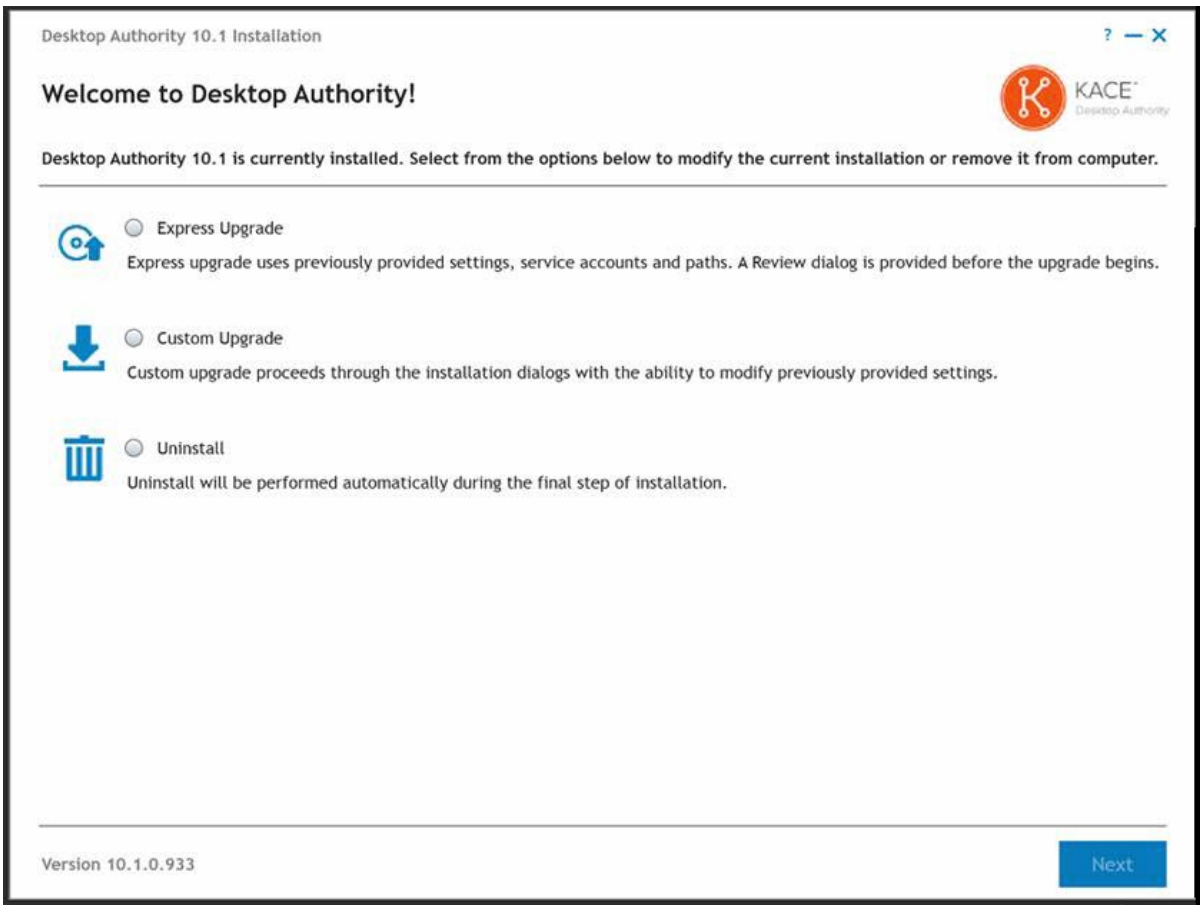
Note: The upgrade process will check all MS Office element settings. Any element with a selected version of MS Office that is no longer supported (anything prior to Office 2010) will be automatically changed to the auto-detect version of the Application/suite. A notification will appear during the installation if this occurs.

NOTE: All settings from the prior version of Desktop Authority User Management Internet Explorer object will be automatically integrated into the new User Management Web Browser object.

1. Begin the installation by double-clicking on the DesktopAuthority.exe icon. The software prerequisites and hardware requirements will be checked and the setup files will be extracted and executed. This initial step of the install will also check privileges, the OS version, determine if .NET 3.5 SP1 is installed and present the license agreement for approval. If .NET 4.6 is not found, the installer will attempt to download it and then install it. The License Agreement must be accepted and .NET 4.6 must be detected or the installer will not continue.

   In the event there is no Internet connection, .NET 4.6 can be downloaded from http://webservices.scriptlogic.com/links/?DADownloads=dotnetfx46&Ver=11.0 and installed prior to continuing with the installation.

2. Once the setup files are extracted the installation process will begin and the prior version of Desktop Authority will be identified. You will be given the opportunity to modify the current installation by upgrading it or removing it.



Express upgrade

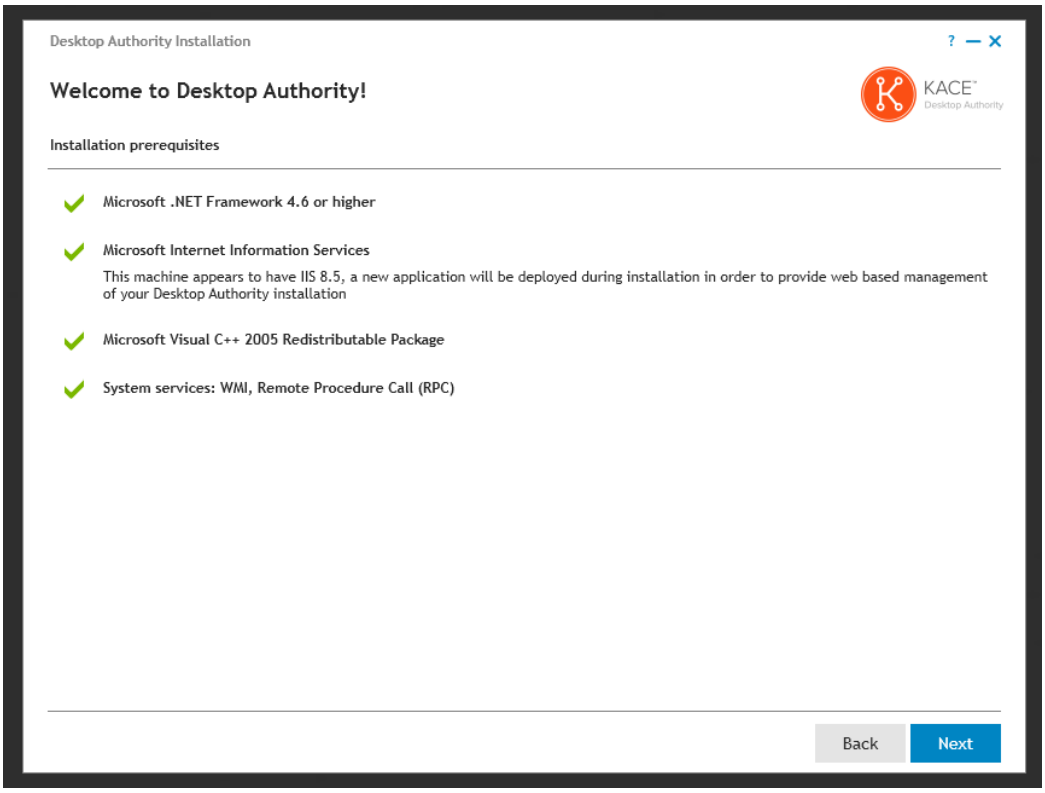
Choosing **Express upgrade** will skip the typical installation dialogs, confirm prerequisites and go directly to the Review dialog. You will, however, be given the opportunity to back up the databases.

Click **Next** to continue the upgrade and install the new application.

NOTE: Prior to the Express Upgrade option being made available, the installer first confirms the existing certificate meets all requirements of the newer version of Desktop Authority being installed. If a certificate requirement has not been met (e.g. existing certificate does not have a Subject Alternative Name), the Express Upgrade option will be disabled and the Custom Upgrade option must be used.

Custom upgrade

3. Choosing **Custom upgrade** option allows you to proceed through the installation dialogs with permission to modify existing settings.



The prerequisite components include:

- Microsoft .NET Framework 4.6 http://webservices.scriptlogic.com/links/?DADownloads=dotnetfx46&Ver=11.0
- Microsoft IIS 7, 7.5, 8, 8.5 or 10 depending upon the Operating System of the server

  - IIS 7 will be installed to 2008 servers
  - IIS 7.5 will be installed to 2008 R2 servers
  - IIS 8.0 will be installed to 2012 servers
  - IIS 8.5 will be installed to 2012 R2 servers
  - IIS 10 will be installed to 2016 and 2019 servers

The default installation of IIS does not install a few components that are required by Desktop Authority. If these components are missing, the Desktop Authority install will allow you to install the missing components by pressing the Add Features button.

These extra IIS components include the following:

HTTP Errors, Application Development, ASP.NET, .NET Extensibility, ISAPI Extensions, ISAPI Filters, Tracing, Windows Authentication, Dynamic Content Compression, IIS Management Scripts and Tools and Management Services.

- Microsoft SQL Server 2008 R2 Express Edition (only required if this is the selected database during the install)
  http://webservices.scriptlogic.com/links/?DADownloads=SQLExpressx64&Ver=11.0 x64 version
  http://webservices.scriptlogic.com/links/?DADownloads=SQLExpressx86&Ver=11.0 x86 version
- Microsoft Visual C++ 2005 Redistributable Package
  http://webservices.scriptlogic.com/links/?DADownloads=vcredistx86&Ver=11.0 x86 version
  http://webservices.scriptlogic.com/links/?DADownloads=vcredistx64&Ver=11.0 x64 version

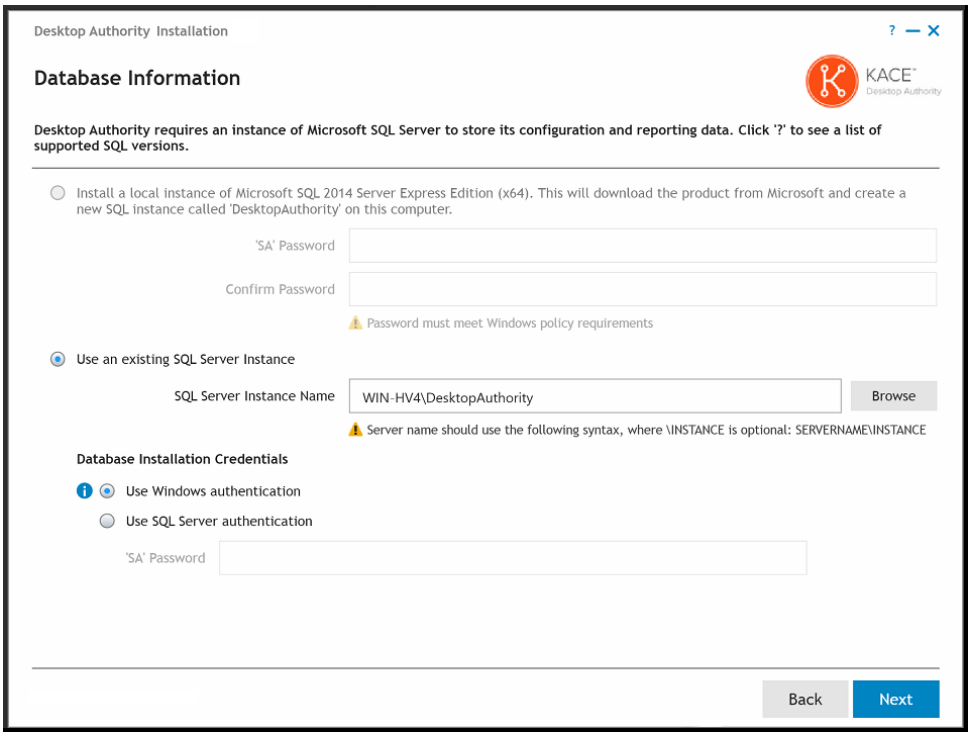
In addition, the installer will configure the following:

- Windows Firewall Exceptions (This will enable an exception for the File and Printer Sharing service)
- WMI and Remote Procedure Call (RPC) system services are used to install and configure Desktop Authority services remotely. They will be turned on during installation.

Note: If there is no Internet connection available on the machine where Desktop Authority is being installed to, the prerequisite components can be downloaded prior to starting the installation and placed in a folder of your choice. During the install, you will be prompted to choose the file path.

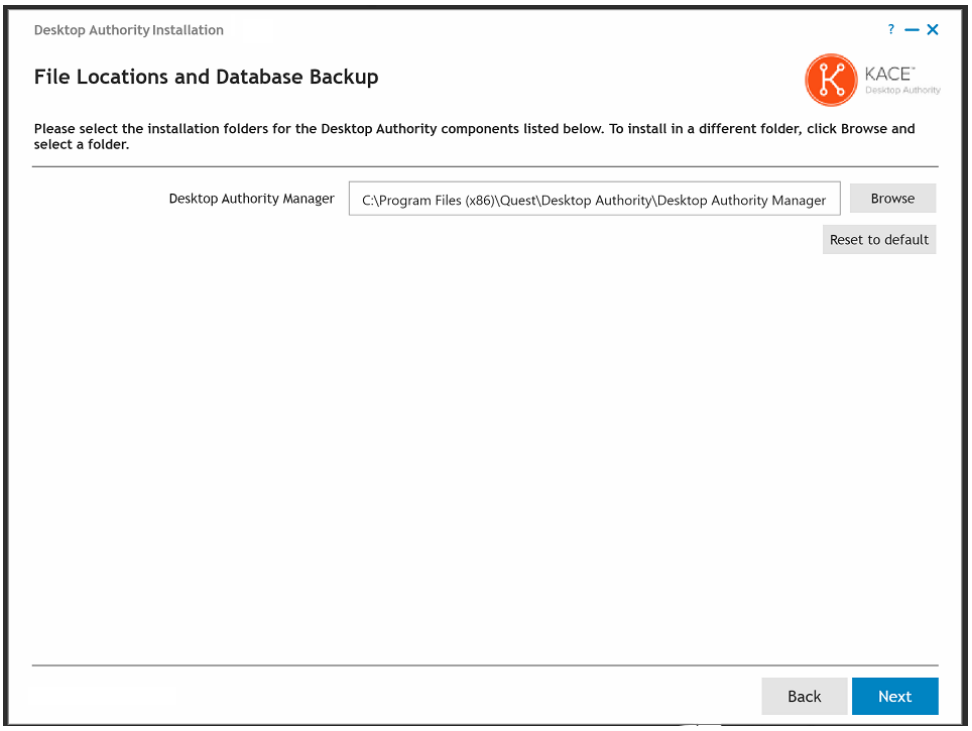
Once all of the prerequisites have been installed and confirmed on the Operations Master, the installation may continue. Click **Next** to continue.

4. Upgrading Desktop Authority requires the credentials to be entered for the existing database instance. Enter the credentials for the database and click **Next** to continue.



5. The file locations are displayed on the following dialog. No changes are necessary here. The Desktop Authority upgrade will be installed on top of the existing version.

   At this point, the database files can be backed up. If you do not have a safe backup of your files already, select the check box next to each database and specify the location of the backup file.



Click **Next** to continue.

6. The Desktop Authority Master services are composed of the Operations and Manager services and are background services that are used to push data through the system. The Operations and Manager services can be configured using a single user account.

   The Operations service (formerly known as the Master service) is a background service that is used to manage and configure Desktop Authority's plugins. It will reach out to each server on the network where the Desktop Authority Administrative service is installed (SLETL$ share). The user account used to configure this service must have appropriate permissions to access the share. The ETLProcessor and ReportScheduler plugins are used to manage collected data and execute scheduled reports. The Operations service requires a user account that is a local administrator of the Operations Master server.

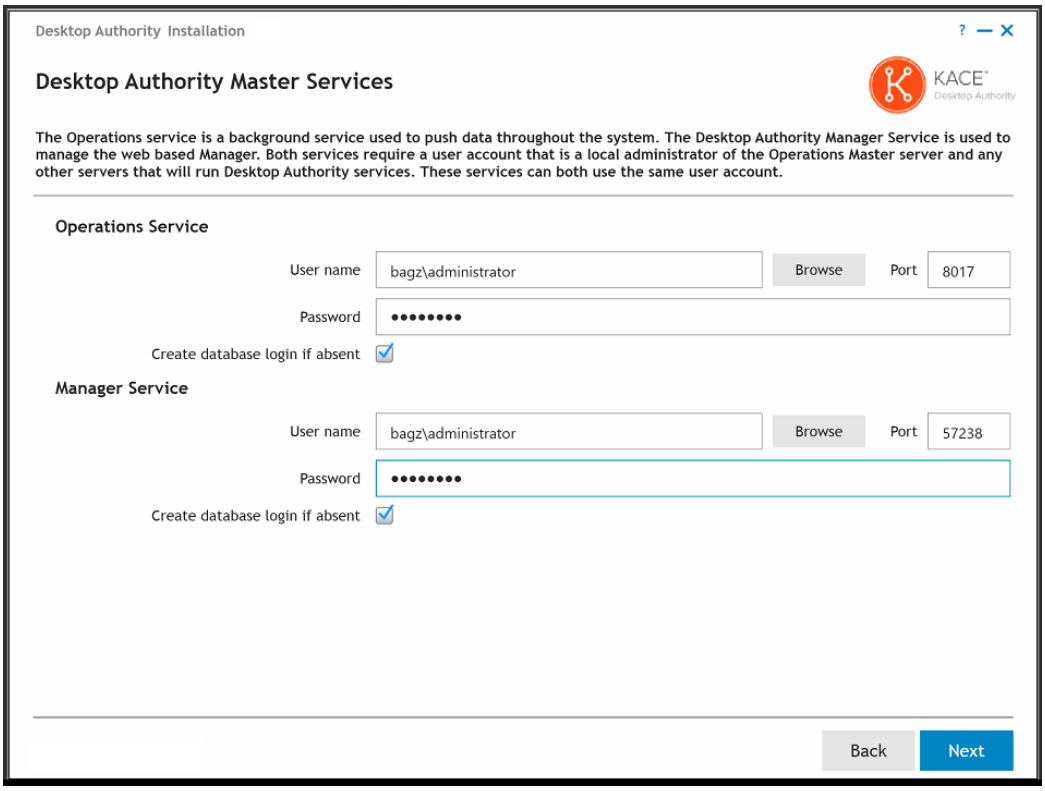
   The Desktop Authority Manager service (formerly known as the OpsMaster service) is used to manage the Web-based Manager, replication, assign scripts, and connectivity and communication between the Manager and the database. It requires a user account that is a local administrator of the Operations Master server and any other servers that will run Desktop Authority services. This service account is also used when browsing out to Active Directory objects, files and folders and for GPO deployment, unless the system preference option, 'Use current user rights for browsing resources' is selected. This option can be changed in the Desktop Authority Setup Tool on the Global System Settings tab.

   The default ports for these services are 8017 and 57238. If either of these ports are being used, a new port must be selected. The installer will check each port for usage and will notify you if they are currently in use. However, if you know that some other application uses either of these ports (but is not currently running) be sure to change them on this dialog. These ports may be changed at a later point in time using the Desktop Authority Setup tool.

   Click the **Browse** button to select an appropriate user account and enter the credentials for each service. Check the box to create a database login if necessary.

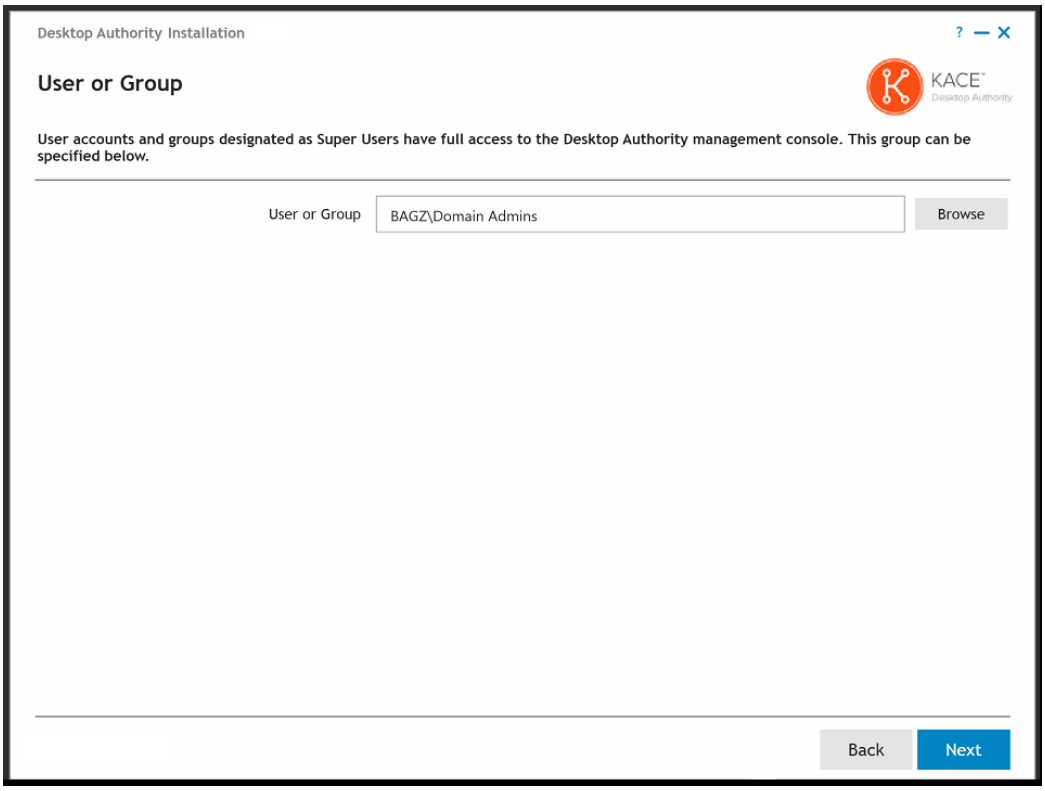
   Modify the default ports if necessary.

   > Note: If Windows Authentication is chosen for the SQL database installation credentials, the accounts selected for the Operations and Manager services should have login access to the database. Select the **Create database login if absent** checkbox to allow the installer to create a SQL login for these accounts. Otherwise, they should be created manually. This option is only available when Windows Authentication is chosen for SQL.



7. The User or Group dialog gives you the opportunity to designate a User or Group as the Super User(s). Any user (or users within a group) designated as a Super User will be given full control in the Desktop Authority Manager. Click the **Browse** button to select the appropriate User or Group.

   Note: The user account of the person installing Desktop Authority will automatically be added as a Super User.


Desktop Authority Installation
User or Group
KACE
Desktop Authority
User accounts and groups designated as Super Users have full access to the Desktop Authority management console. This group can be specified below.
User or Group
BAGZ\Domain Admins
Browse
Back
Next

8. ## IIS Application Pool

> Note: The IIS Application pool identity section is available when using SQL Windows Authentication only.

The IIS Application pool identity is used to allow IIS to host web applications/virtual folders as standalone processes to avoid application crashes. Select a Domain User account for the IIS Application pool to use. This account will automatically be granted the necessary permissions if needed.

If Windows Authentication is chosen for the SQL database installation credentials, the account selected for the IIS Application pool will need to have login access to the database. Select the **Create database login if absent** checkbox to allow the installer to create a SQL login for these accounts. Otherwise, they should be created manually.

Website Configuration

The Website Configuration dialog is used to configure the Web based console (Manager). These configurations are made in Internet Information Services (IIS).

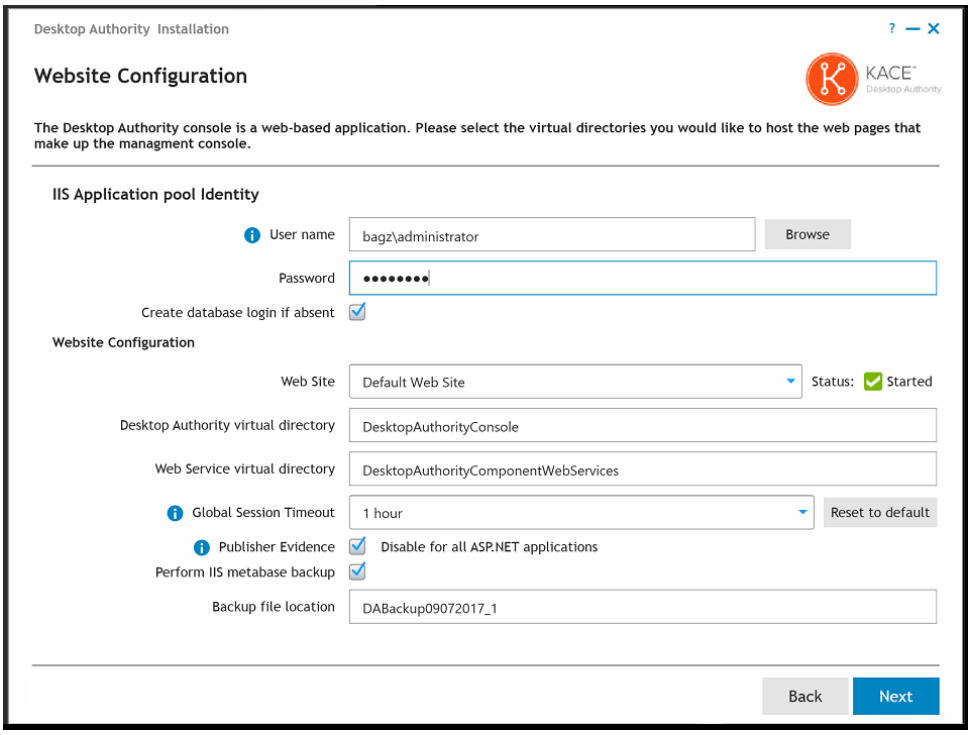
The Web Site selection allows you to configure Desktop Authority to use a site other than the default site in IIS. If you choose to use a site other than the default, it must be created prior to getting to this part of the installation. The selected site must have an HTTP port binding defined for it.

Specify Desktop Authority and Web Service virtual directories. Please reference the File Paths table in the appendices for default path locations. IIS Virtual directories are mapped to these folders.

The Global Session Timeout value is the maximum amount of time the Desktop Authority Console can sit idle before logging the user out due to inactivity. This timeout value can be overwritten for individual users in the Desktop Authority Console Preferences dialog.

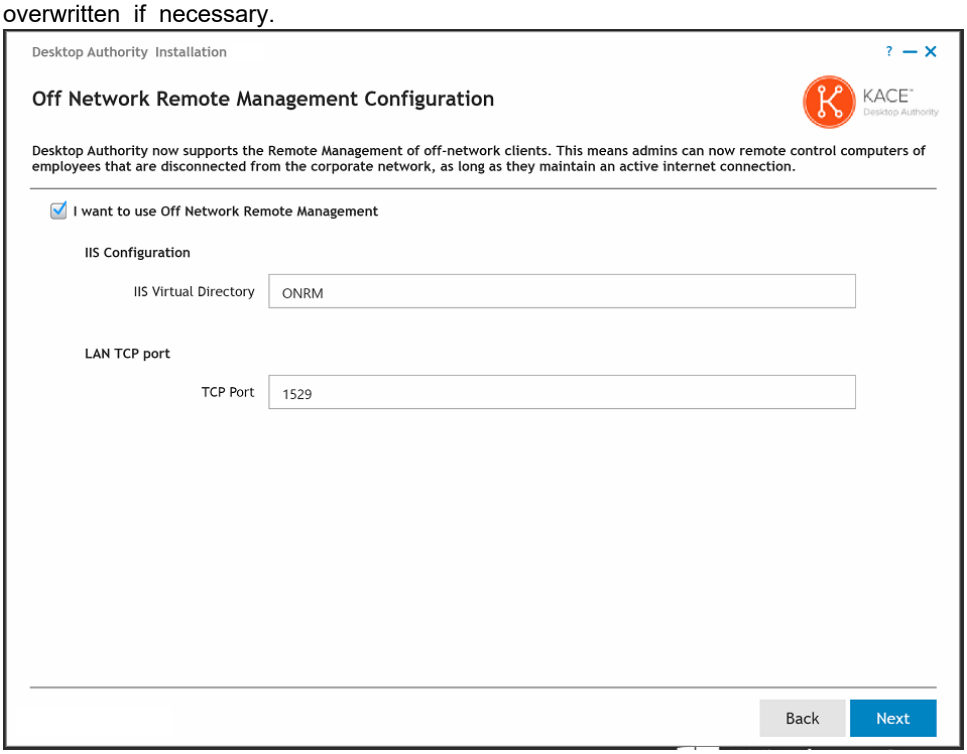
Publisher Evidence will disable for all ASP.NET applications to disable .NETs automatic validity checking of Authenticode signed signatures at startup. If publisher evidence is not disabled, some services may fail to start correctly at boot time due to lengthy delays imposed by the verification process.

Since Desktop Authority updates IIS, you have the option of performing a backup of IIS before any changes are made. It is recommended to always perform this backup of IIS since there is a possibility that other applications on the same site may conflict with each other. If there are any IIS problems following the install, the backup can be restored. Select the IIS metabase Backup option to enable the backup. The backup file created in the %systemroot%\system32\inetsrv\MetaBack folder. The default file name is created using a date, time format.

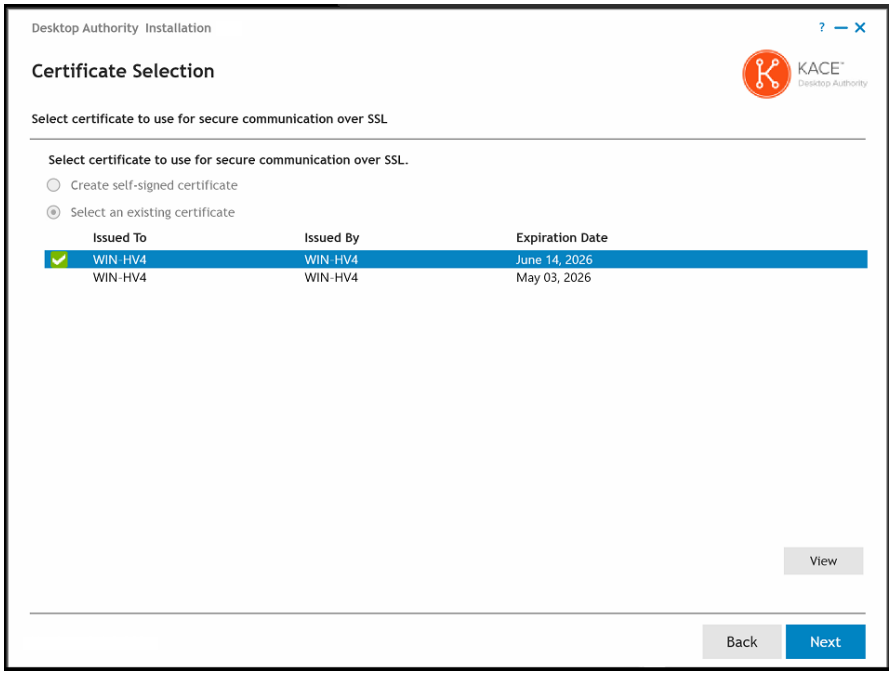


Click **Next** to continue.

9. In order to remotely manage a client that is off-network, you must configure the feature here during install (or later in the DA Setup tool). Turn on the feature by selecting the **I want to use Off Network Remote Management** check box. A defulat **IIS Virtual Directory** and **LAN TPC Port** will be used. These may be overwritten if necessary.

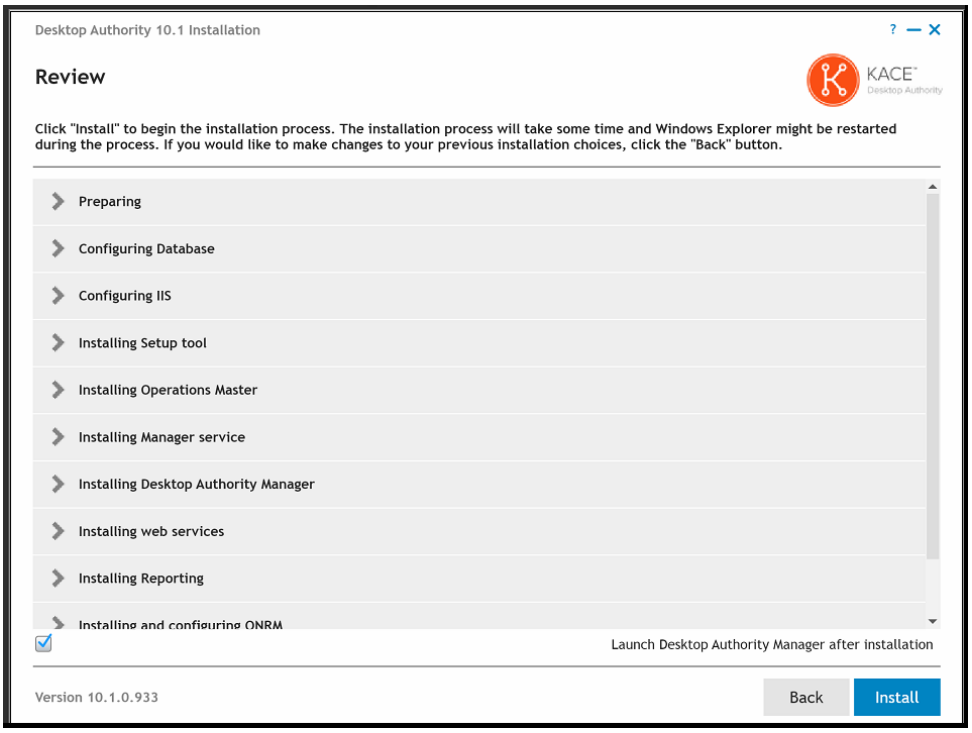


10. In an upgrade situation, there will be a certificate that was created at an earlier time by Desktop Authority. This certificate will be automatically selected. If another certificate is to be used, select that one instead. Click View to look at the selected certificate details.



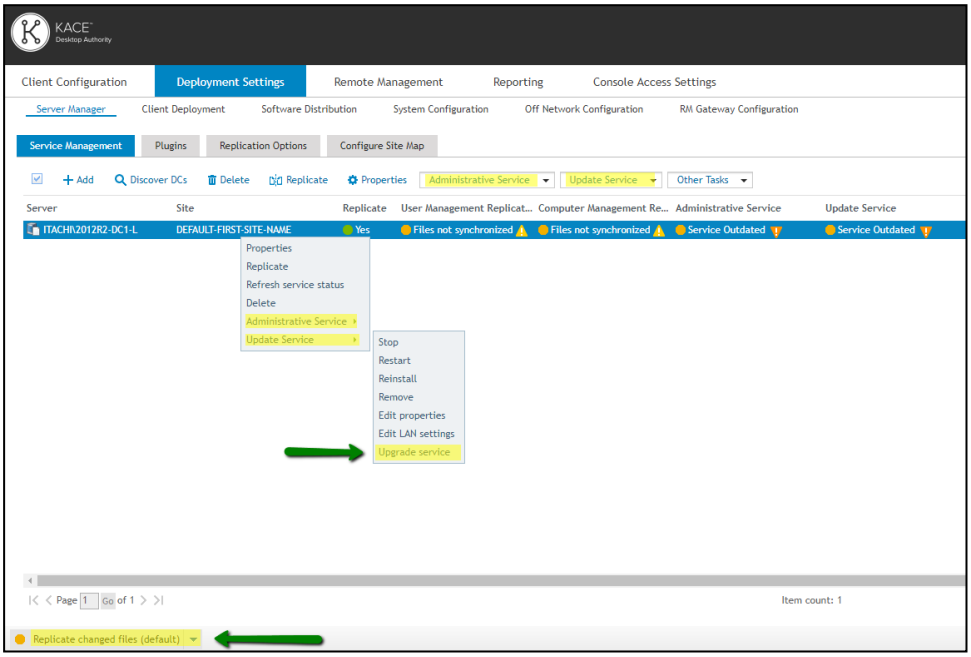
Click **Next** to continue.

11. The installation is about to begin. To run Desktop Authority following the installation of its files, click the *Launch Desktop Authority Manager after installation* checkbox. Click **Install** to proceed with the installation.


Desktop Authority 10.1 Installation
Review
KACE
Desktop Authority
Click "Install" to begin the installation process. The installation process will take some time and Windows Explorer might be restarted during the process. If you would like to make changes to your previous installation choices, click the "Back" button.
Preparing
Configuring Database
Configuring IIS
Installing Setup tool
Installing Operations Master
Installing Manager service
Installing Desktop Authority Manager
Installing web services
Installing Reporting
Installing and configuring ONRM
Launch Desktop Authority Manager after installation
Version 10.1.0.933
Back
Install

12. Click install to complete the upgrade.

13. Once the upgrade has completed, login to the Desktop Authority console and navigate to the **Service Management** tab. From there, you will need to complete the mandatory process of upgrading all outdated Administrative and Update Services. You can see all outdated services in the list, notated by a yellow triangle warning icon. The upgrade of these services can be initiated via the right-click or drop-down menu options within the console.



Once all services have been upgraded (showing a green status), a replication must be performed in order to fully complete the upgrade.

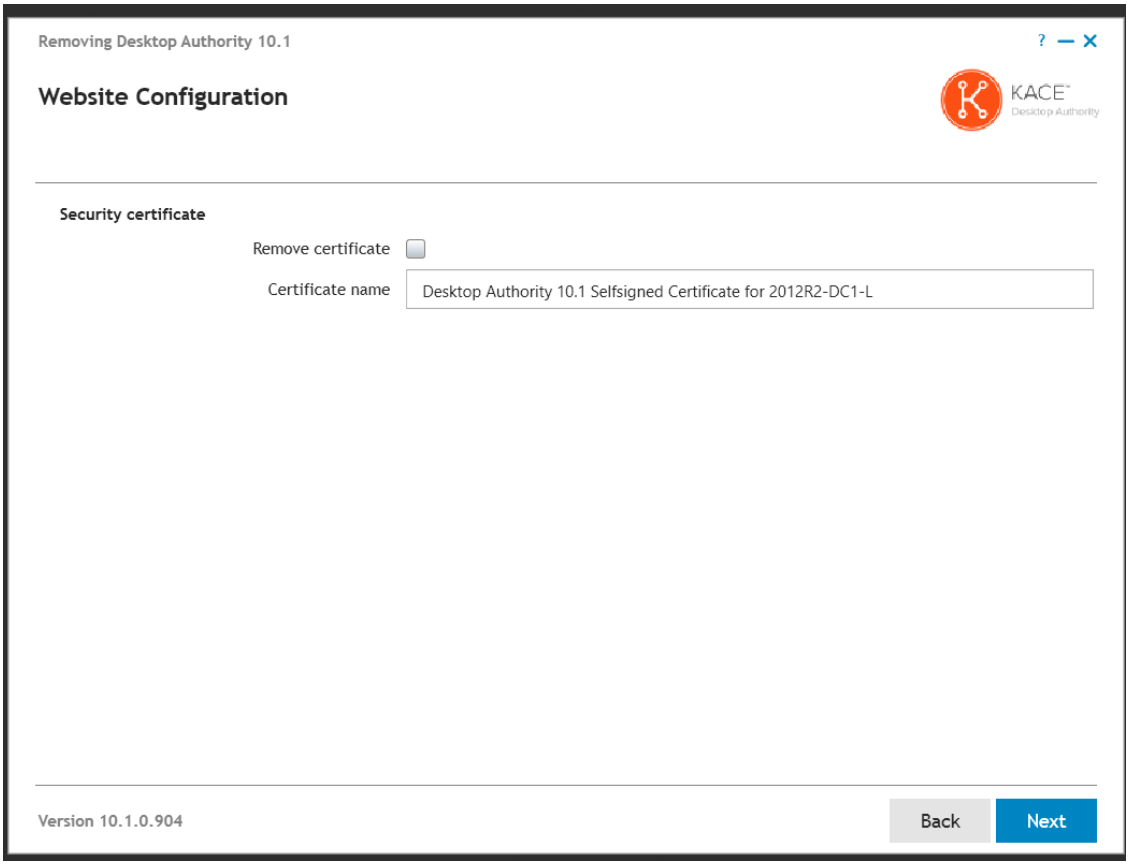
Uninstall

The **Uninstall** option is used to remove the currently installed version of Desktop Authority. When removing the prior version of Desktop Authority, the database will be left intact and be available for the new installation of Desktop Authority. See Uninstalling Desktop Authority for further details.

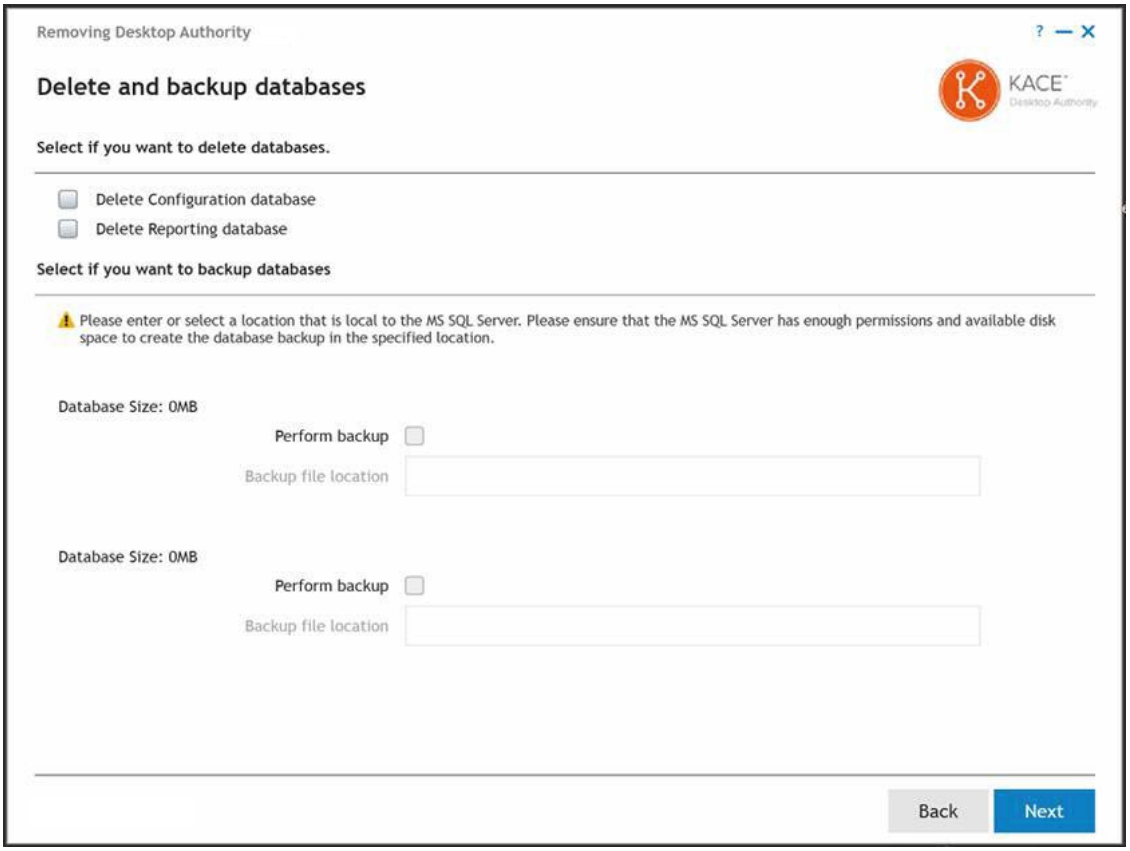
Uninstalling Desktop Authority

NOTE: Prior to starting the Desktop Authority uninstallation process, all instances of the Administrative and Update services should be removed, unless the intent is for Desktop Authority is to be reinstalled once the uninstallation has completed. This is done on the Service Management tab within the console. You must right-click on each server and select each service and Remove. This needs to be done for each service on each server.

1. To begin the Desktop Authority uninstallation process, go to Control Panel | Programs and Features (or Add/Remove Programs) applet. Highlight Desktop Authority in the programs list and select Uninstall.
2. The first dialog, Website Configuration, gives you the opportunity to remove the security certificate used by Desktop Authority. This may be a Desktop Authority self-signed certificate or some other certificate on your system. Select the **Remove certificate** box to remove the configured certificate. Click **Next** to continue.



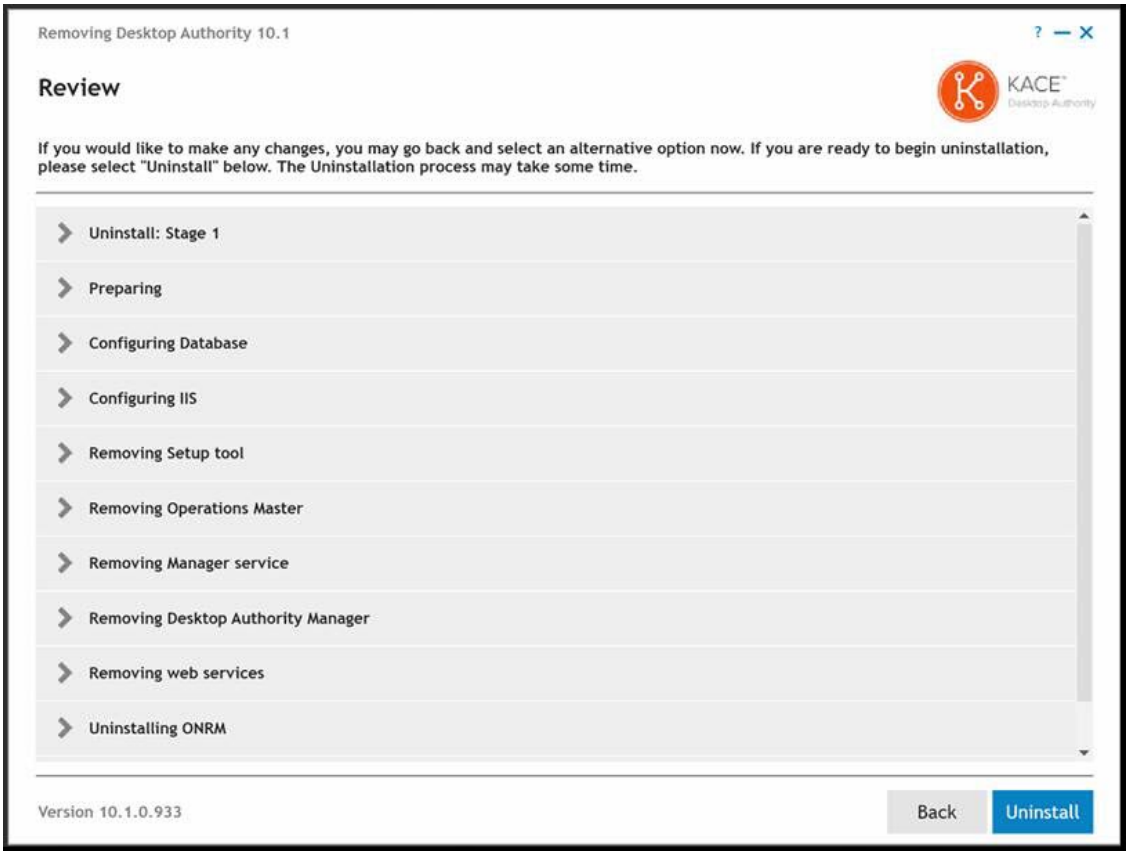
3. During the uninstall process, you have the option to backup and/or delete your databases. Select the box next to each database to be backed up and/or deleted and click **Next** to continue.



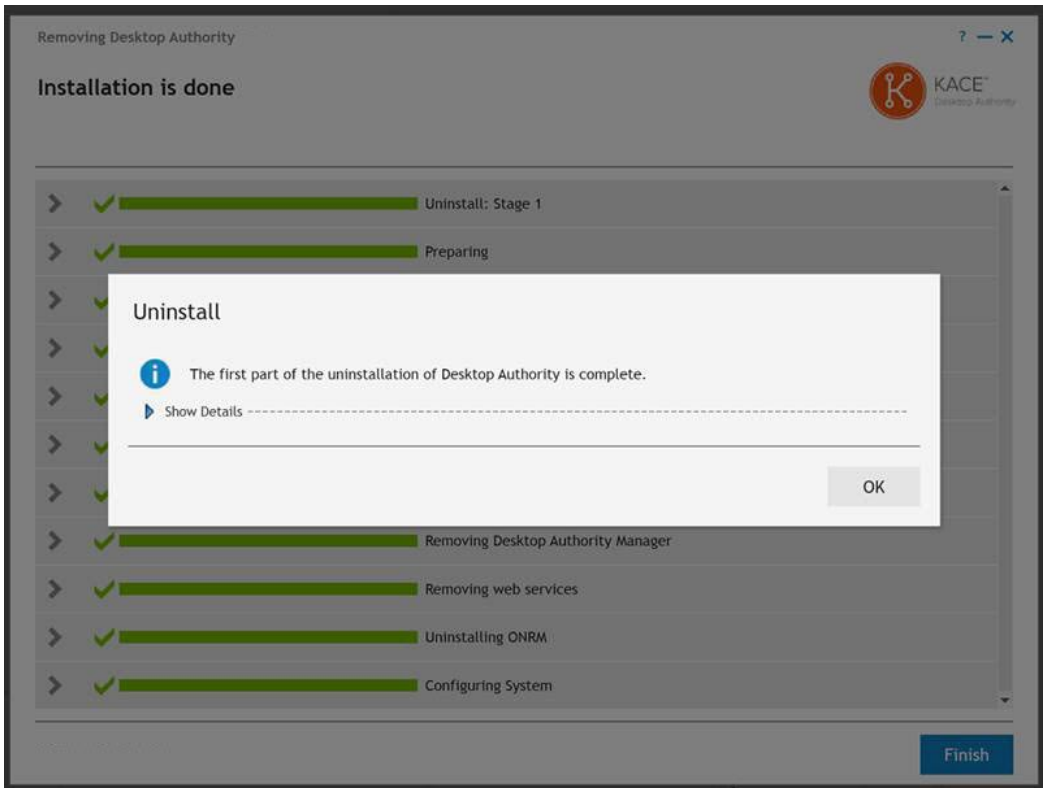
4. The next step is to remove the assigned logon scripts from Active Directory. If you would like to remove these scripts, make sure the checkbox is selected. Unselect the checkbox to leave the scripts assigned.

Click **Next** to continue.

5. Click **Uninstall** to start the uninstall process.

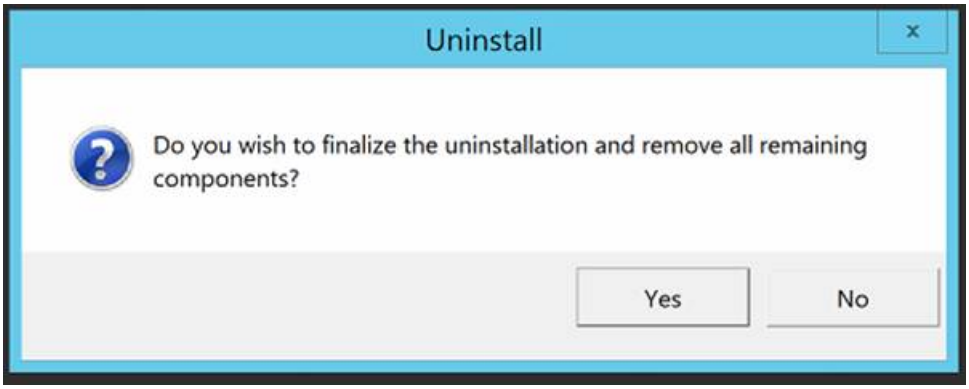


Once this uninstall process is complete you will be notified that the first part of the process is complete. This part of the process removes all of Desktop Authority from the necessary servers. This process also configures a GPO that will remove all client side services. Since not all computers are available at all times, the removal process via the GPO on client computers may take a few days to complete.



Click **OK** and then **Finish** to complete the first part of the uninstallation.

6. At a later date, once you are comfortable that the client-side services have been removed, run the Uninstall a second time to remove the DA GPO and remaining pieces.



Click **Yes** to begin the removal of the remaining Desktop Authority components.

7. The following dialog will review the steps to be taken in order to remove the remaining components.

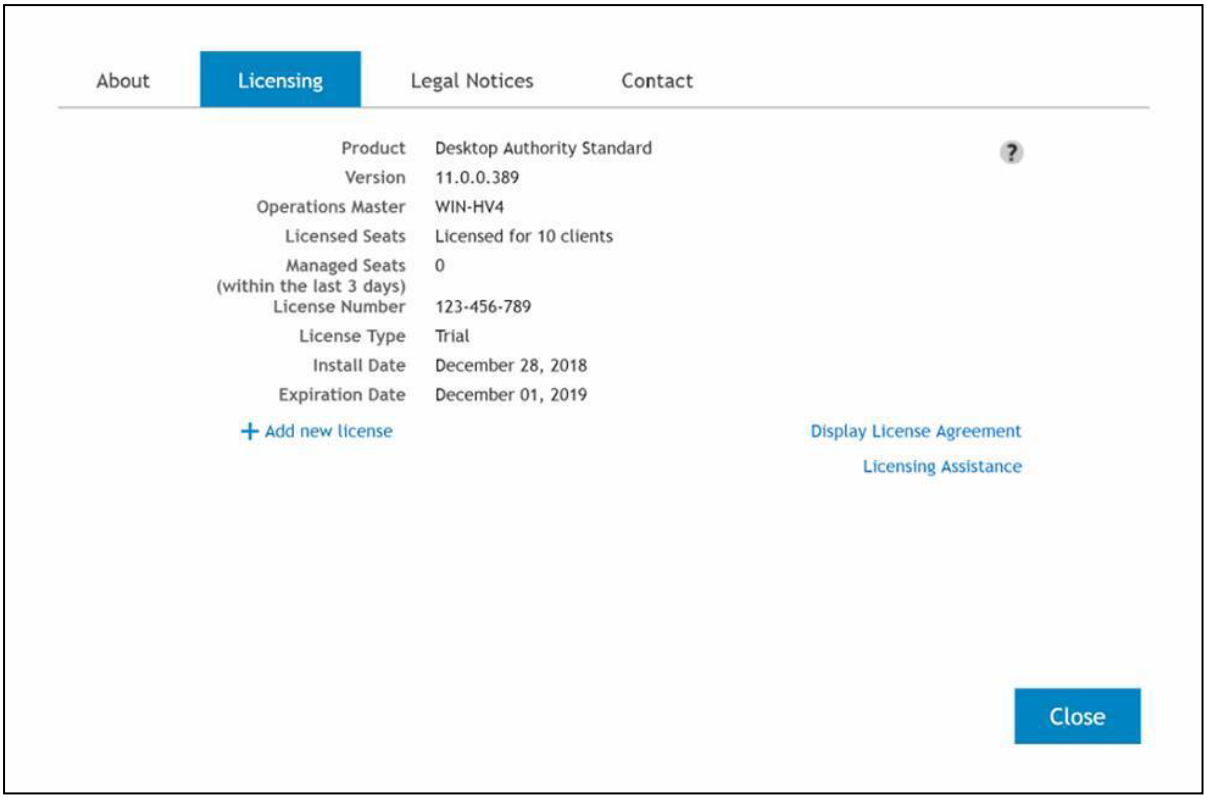
Click **Uninstall** to start the removal process. Once complete, click **Finish** to complete the uninstallation.

Registration

You must register your new license key after a purchase to remove the evaluation time period or if the evaluation has expired. A license key is provided at the time of purchase. All configurations made during the trial are still available after the product is registered. You can continue using all features immediately following the registration process.

Enter the provided registration key code by clicking the Registration link on the bottom of the Desktop Authority console.

The following dialog opens within the Desktop Authority Manager.



The Registration window shows the following product information:

Product

The name of the installed product.

Version

The version of the installed product.

Operations Master

The Operations Master designates the computer to which Desktop Authority is installed to.

Licensed Seats

Displays the number of seats purchased. In evaluation mode, this will display the number of days remaining in the evaluation period.

Managed Seats

The number of active computers that have the Desktop Authority client installed on it, thus it is managed by Desktop Authority. A terminal server is counted as one licensed seat.

License Type

Shows the license type, Trial or Perpetual.

Install Date

The date the product was installed or updated.

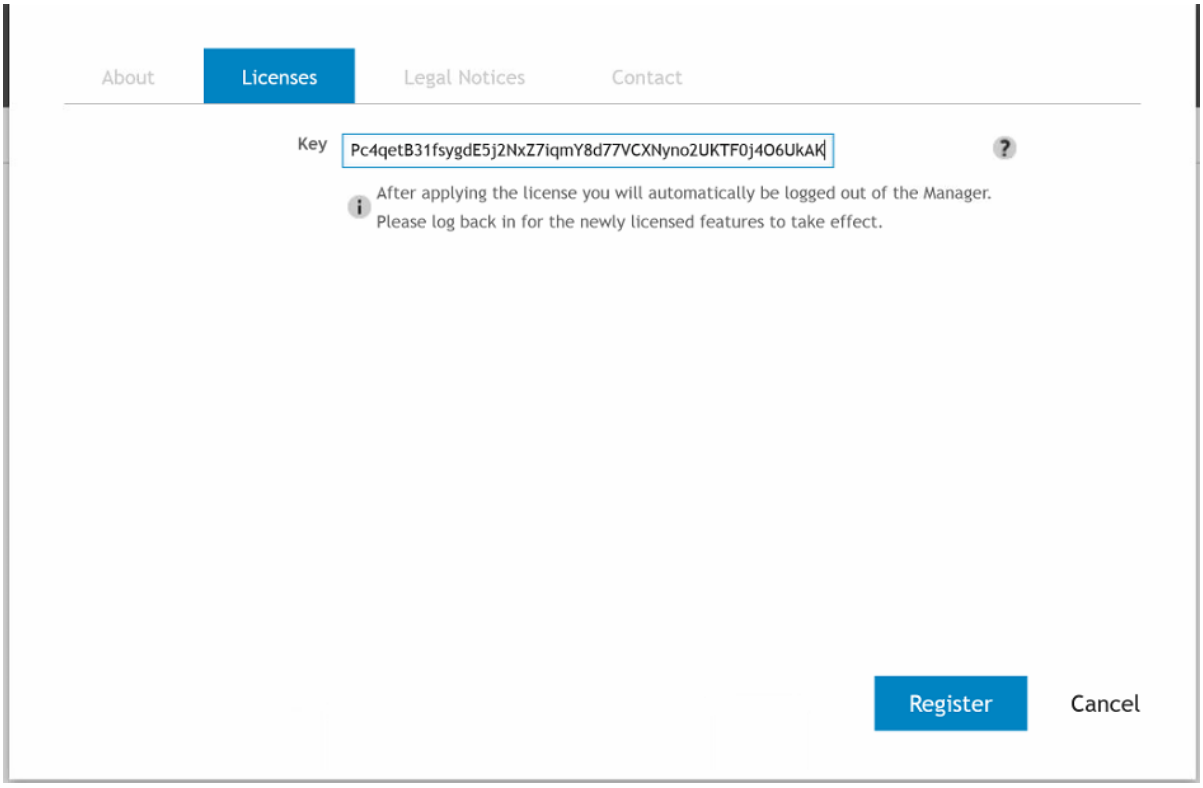
Expiration Date

The date the trial will expire. Shows for trial versions only.

Add new license

Click **Add new license** to add the license key after purchase.

Fill in the license key and click **Register**.



.

After clicking Register, the license is verified. If correct, you will be prompted to replicate the change to the domain controllers. Click **Yes** to replicate the registration data or No to replicate the data at a later time. The registration process does not become effective until the data is replicated.

Once the product is registered and the information is replicated, Desktop Authority Manager will display the license information.

Updated registration information is not displayed on the Desktop Authority Manager dashboard or on client machines until the users log back onto the network after the registration information is entered and replicated through the system.

Desktop Authority ports and configurations

Please refer to the File Paths appendix for the correct path(s) based on the version of Desktop Authority you are using.

Installs

- .NET Framework 4.6
- IIS (IIS 7 will be installed to 2008 servers, IIS 7.5 will be installed to 2008 R2 servers, IIS 8 will be used on 2012 servers, IIS 8.5 will be used on 2012 servers, IIS 10 will be used on 2016 and 2019 servers)
- MS Visual C++ 2005 Redistributable Package

SQL

User has a choice of

- Installing MS SQL 2014 Server Express Edition
- Using an existing instance of MS SQL (2008, 2008 R2, 2012, 2014, 2016, 2017)

Databases

There are two databases created by the installation of Desktop Authority.

- DAConfiguration
- DAReporting

Super Users

- Active Directory User or group account. No special permissions needed.

Paths

- SQL Server 2014 Express Database - C:\Program Files (x86)\Quest\Desktop Authority\Desktop Authority Manager\Database
- Desktop Authority Manager - C:\Program Files (x86)\Quest\Desktop Authority\Desktop Authority Manager
- Data collection repository - %programfiles%\Quest\Desktop Authority\ETL Cache
- Download cache folder - %programfiles%\Quest\Desktop Authority\Update Service\Cache\
- DA virtual directory – DesktopAuthorityConsole
- Web Service virtual directory - DesktopAuthorityComponentWebServices
- IIS metabase backup – DABackup[ddmmyyyy]

Firewall exceptions

- File and printer sharing
- Desktop Authority Update Service
- Installer creates 2 inbound firewall exception rules
- Desktop Authority Update Service

  Enabled,
  Allow connection,
  Program: C:\Program Files (x86)\Quest\Desktop Authority\Update Service\Daupdsvc.exe,
  All computers,
  All users,
  Protocol: TCP,
  All ports,
  Any IP Address,
  Domain profile

- Desktop Authority Update Service

  Enabled,
  Allow connection,
  Program: C:\Program Files (x86)\Quest\Desktop Authority\Update Service\Daupdsvc.exe,
  All computers,
  All users,
  Protocol: UDP,
  All ports,
  Any IP Address,
  Domain profile

Security certificate

Desktop Authority uses a security certificate for use with the DesktopAuthorityConsole web site in IIS.

Desktop Authority defaults to creating and installing its own secure self-signed server certificate during the installation process. A self-signed certificate is one that is signed and verified legitimate by the creator of the certificate. You can, however, choose to select a certificate that already exists on the server. This may be the case during an upgrade of Desktop Authority. In most cases, it is recommended to allow Desktop Authority to create a self-signed certificate.

Services installed by DA

- **Operations Service** – (*Formerly known as the DA OpsMaster Service*) The Operations Service is a background service that is used to manage and configure Desktop Authority's plugins. The ETLProcessor and ReportScheduler plugins are used to manage collected data and execute scheduled reports.

  This service requires the credentials for a user account that is local admin of OpsMaster server and any other servers that that host the DA Administrative services in order to collect data.
  This service moves files from the server that hosts the DA Administrative service (default path - C:\Program Files\Quest\Desktop Authority\etl cache) to the OpsMaster server where Desktop Authority is installed to (default path - C:\Program Files\Quest\Desktop Authority\Desktop Authority Manager\OpsMasterService\ETLFileRepository). Since the ETLProcessor plugin connects to the "\\ServerName\slETL$ (file://servername/slETL$)" share, the user account configured for the Operations Service must have access to that share where the DA Administrative service is installed to.
  The Operations service is given SA access to the SQL database server during the installation of Desktop Authority.
  The installation defaults this service to port 8017, but it can be changed during the install, to suit the specific environment. This port can also be changed using the Desktop Authority Setup Tool.

- **DA Manager Service** – (*New service introduced in DA 9.0*) The Manager Service is used to manage the Web based Manager, replication, and connectivity and communication between the Manager and the database.

  This service requires the credentials for a user account that is local administrator of OpsMaster server and any other servers that will host Desktop Authority services.
  The Manager Service is given SA access to the SQL database server during the installation of Desktop Authority.
  The installation defaults this service to port 8085, but it can be changed during the install to suit the specific environment. This port can also be changed using the Desktop Authority Setup Tool.

- **DA Administrative Service** – The DA Administrative service enables Desktop Authority to perform tasks that require administrative rights without sacrificing user-level security at the workstation. This service helps Desktop Authority perform these specialized tasks by installing a client version of the DA Administrative service to each client machine and a complementary version of the DA Administrative service to one or more Domain Controllers within the domain.

  This service requires two unique user accounts. The Server user account (server side service) must have Local Admin rights to all workstations. In most circumstances, this account will be one that is a member of the Domain Admins group.
  The Client User account (client side service) is used on each workstation to make registry changes, install software, add printers, synchronize time and perform any other task that may require elevated privileges during the logon, logoff or shutdown events. The Client User account (client side service) should be a member of the Domain Users group.

- **Update Service** – The Update Service is used for the Software Management. The Update Service offers an encrypted and secure connection to Quest owned websites.

  The user account configured for this service must be a member of the Local Administrators group on the server in which the service is being installed to. This account must have Local Administrator access to the Operations Master server share (\\Servername\slogic$ (file://servername/slogic$) in order to read the Register.ini file for licensing purposes, as well as for access to the Internet.

- **IIS Application Pool** – Desktop Authority's web based Console uses IIS to host the application. The IIS Application pool identity is used to allow IIS to host web applications/virtual folders as standalone processes to avoid application crashes. Port 443 is required for IIS.

  Domain user credentials are required so it can log information to the database. If Windows Authentication is chosen for the SQL database authentication, the account selected for the IIS Application pool will need to have login access to the database.

What Desktop Authority relies on/Windows Built-in

Desktop Authority makes use of HTTPS along with a digital certificate to ensure secure communication via the Console. During the DA installation, the DAInstaller has the option to create a new certificate or use an existing certificate. The certificate is used by IIS HTTPS to encrypt the data.

Service communication within Desktop Authority makes use of WCF (Windows Communication Foundation). This also makes use of the digital certificate for encryption of data.

Ports

Desktop Authority Manager relies on the following ports to be opened for inbound access.

1433 – Required by SQL Server to communicate over a firewall

443 – HTTPS port used by IIS

http://support.microsoft.com/kb/832017 Article discusses the ports, protocols and services used my MS client and server operating systems.

445 SMB over TCP for shared access to files, printers, serial ports and miscellaneous communication

137, 138, 139 NetBIOS over TCP/IP port

The ports mentioned above for CIFS/SMB are the underlying the protocol ports for Desktop Authority's services including DA Update Service and the DA Administrative service. The "File and printer sharing" Local Firewall Policy exception configured by the Desktop Authority Installer enables desired communication through the local firewall.

These ports may have been already been opened/configured by the Desktop Authority Installer so there will not be a need to open them explicitly unless these ports are intentionally blocked through other means.

Services

File and Printer Sharing

Active Directory

Computer Browser (requires firewall exception for File and Printer sharing service)

Event Log

Net Logon

WMI

RPC

12

File Paths

The following table describes the paths that Desktop Authority uses.

Desktop Authority upgrades from previous versions to 11.3.2 will use the existing installation paths.

> Important: PF stands for %programfiles% in an x86 environment and %programfiles(x86)% in a x64 environment

Server side

Location Install paths for upgrades from ver 9.x to 11.3.2	Install Path for ver 11.3.2
Group Policies Admx file location	
• x:\PF\ScriptLogic\Desktop Authority Manager\TemplateFiles	• x:\PF\Quest\Desktop Authority\Desktop Authority Manager\TemplateFiles
Remote Mgmt Alternate DesktopAuthority.exe default location (shared as SLDAClient$)	
• x:\Quest\Desktop Authority\Desktop Authority Manager\DesktopAuthority	• x:\Quest\Desktop Authority\Desktop Authority Manager\DesktopAuthority
Default MS SQL 2014 Server Express installation location	
• x:\PF\ScriptLogic\Desktop Authority Manager	• x:\PF\Quest\Desktop Authority\Desktop Authority Manager
Default MS SQL 2014 Server Express database location	
• x:\PF\ScriptLogic\Desktop Authority Manager\Database	• x:\PF\Quest\Desktop Authority\Desktop Authority Manager\Database
Website Configuration DA Virtual Directory	
• x:\PF\ScriptLogic\Desktop Authority Manager\DAConsole\	• x:\PF\Quest\Desktop Authority\Desktop Authority Manager\DAConsole\
Desktop Authority Manager location (shared as SLogic$)	

Location Install paths for upgrades from ver 9.x to 11.3.2	Install Path for ver 11.3.2
• x:\PF\ScriptLogic\Desktop Authority Manager	• x:\PF\Quest\Desktop Authority\Desktop Authority Manager
DA Manager ProgramData logs	
• x:\ProgramData\ScriptLogic\DAConsole	• x:\ProgramData\Quest\DAConsole
Website Configuration Web service Virtual Directory	
• x:\PF\ScriptLogic\Desktop Authority Manager\DAComponentWebServices	• x:\PF\Quest\Desktop Authority\Desktop Authority Manager\DAComponentWebServices
Default Update Service Download Cache	
• x:\PF\ScriptLogic\Update Service\Cache	• x:\PF\Quest\Desktop Authority\Update Service\Cache
Update Service Location	
• x:\PF\ScriptLogic\Update Service\Daupdsvc.exe	• x:\PF\Quest\Desktop Authority\Update Service\Daupdsvc.exe
Update Service Log File	
• x:\PF\ScriptLogic\Update Service\Daupdsvc0.log	• x:\PF\Quest\Desktop Authority\Update Service\Daupdsvc0.log
Update Service Status Reporter Log File	
• %temp%\DesktopAuthority\DAUpdtSvcStRep.log	• %temp%\DesktopAuthority\DAUpdtSvcStRep.log
ⓘ Note: In the temp directory of the Update Service user account.	
OpsMaster ETL Repository	
• x:\PF\ScriptLogic\Desktop Authority Manager\OpsMasterService\ETLFileRepository	• x:\PF\Quest\Desktop Authority\Desktop Authority Manager\OpsMasterService\ETLFileRepository
Signature Files	
• x:\PF\ScripLogic\Desktop Authority Manager\slsrvmgr.ske	• x:\PF\Quest\Desktop Authority\Desktop Authority Manager\slsrvmgr.ske
Admin Service XML file repository (shared as slETL$)	
• x:\PF\ScriptLogic\ETL Cache	• x:\PF\Quest\Desktop Authority\ETL Cache
Admin Service Log file	
• (32-bit) %SystemRoot%\System32\DAAdminSvc_%ComputerName%.log	• (32-bit) %SystemRoot%\System32\DAAdminSvc_%ComputerName%.log

Location Install paths for upgrades from ver 9.x to 11.3.2	Install Path for ver 11.3.2
• (32-bit) %SystemRoot%\System32\DAAdminSvcStRep.log • (64-bit) %SystemRoot%\SysWow64\DAAdminSvc_%ComputerName%.log • (64-bit) %SystemRoot%\SysWow64\DAAdminSvcStRep.log	• (32-bit) %SystemRoot%\System32\DAAdminSvcStRep.log • (64-bit) %SystemRoot%\SysWow64\DAAdminSvc_%ComputerName%.log • (64-bit) %SystemRoot%\SysWow64\DAAdminSvcStRep.log
Admin Service StatusGateway log	
• %temp%\DesktopAuthority\DAStatusGateway.log	• %temp%\DesktopAuthority\DAStatusGateway.log
ⓘ Note: In the temp directory of the Admin Service's user account.	
User Management Replication	
• Source: x:\PF\ScriptLogic\Desktop Authority Manager\scripts • Target: %windir%\SYSVOL\sysvol\DomainName\scripts	• Source: x:\PF\Quest\Desktop Authority\Desktop Authority Manager\scripts • Target: %windir%\SYSVOL\sysvol\DomainName\scripts
Computer Management Replication	
• Source: x:\PF\ScriptLogic\Desktop Authority Manager\Device Policy Master • Target: %windir%\SysVol\sysvol\DomainName\Policies\Desktop Authority\Device Policy Master	• Source: x:\PF\Quest\Desktop Authority\Desktop Authority Manager\Device Policy Master • Target: %windir%\SysVol\sysvol\DomainName\Policies\Desktop Authority\Device Policy Master
Replication Log	
• x:\PF\ScriptLogic\Desktop Authority Manager\SLRepl.log	• x:\PF\Quest\Desktop Authority\Desktop Authority Manager\SLRepl.log

Client side

Prior Paths USB/Port Security devices	New or 11.3.2 Version Paths
• x:\PF\ScriptLogic\Port Security	• x:\PF\Quest\Desktop Authority\PortSecurity • %windir%\system32

User Detailed Trace File

- %temp%\Desktop Authority

Computer verbose debug mode

- %windir%\Temp\Desktop Authority

Client Files and Agents

- x:\ScriptLogic
- x:\PF\ScriptLogic\Desktop Authority
- x:\PF\ScriptLogic\Common
- x:\PF\ScriptLogic\DA Update Client
- x:\PF\ScriptLogic\Desktop Authority\Client Files

Expert Assist

- x:\PF\DesktopAuthority

- %temp%\Desktop Authority
- %windir%\Temp\Desktop Authority
- x:\Desktop Authority
- x:\PF\Quest\Desktop Authority
- x:\PF\Quest\Desktop Authority\Common
- x:\PF\Quest\Desktop Authority\DA Update Client
- x:\PF\Quest\Desktop Authority\Client Files
- x:\PF\Quest\ExpertAssist

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

Tools

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Index

B

Backup 8

D

Desktop Authority Version Comparison 6

I

Installation 12

M

Making a backup 8

R

Register Desktop Authority 49
Registration 49

V

Version Comparison 6