KACE® Desktop Authority 11.3.2

# Getting Started 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 - Getting Started Guide
Updated - October 2025
Version - 11.3.2

# Contents


**About this guide** ..... **4**

**Starting Desktop Authority for the first time** ..... **5**

**Registering Desktop Authority** ..... **7**

**Where do I begin?** ..... **8**

**Configure required services** ..... **10**
DA Administrative Service ..... 10
Update Service ..... 11

**User/Computer Management** ..... **12**
What's the difference? ..... 12
How do I know which to use? ..... 12

**Profile objects and profile elements** ..... **15**
Validation Logic ..... 15
Timing events ..... 16
Profile creation strategy ..... 17
Why do we want more than one profile? ..... 17
Some common ways to organize your profiles ..... 17
Creating profiles ..... 18
Configuring profile elements ..... 18

**Data Collection and Reporting** ..... **21**

**Are you on the right track? Validate your configurations** ..... **22**

**Client Provisioning** ..... **23**
Configure Off-Network Support (Optional) ..... 24

**Assigning the Logon Script** ..... **25**

**Saving and replicating configurations** ..... **26**

**File Paths** ..... **27**
Server side ..... 27
Client side ..... 29

**About us** ..... **31**
Technical support resources ..... 31
Tools ..... 31

# About this guide

Welcome to the Quest™ Desktop Authority™ Getting Started Guide. This manual is intended to instruct the new Desktop Authority Administrator on how to use the browser based console “Desktop Authority Manager” to configure, manage and secure computers.

This manual covers information regarding the use and configuration of Desktop Authority following its installation. For further information on using this product you may refer to the online help by pressing the help button ( ) within the Manager. There are also PDF manuals available for download from the Support Portal.

***All manuals available for download include:***

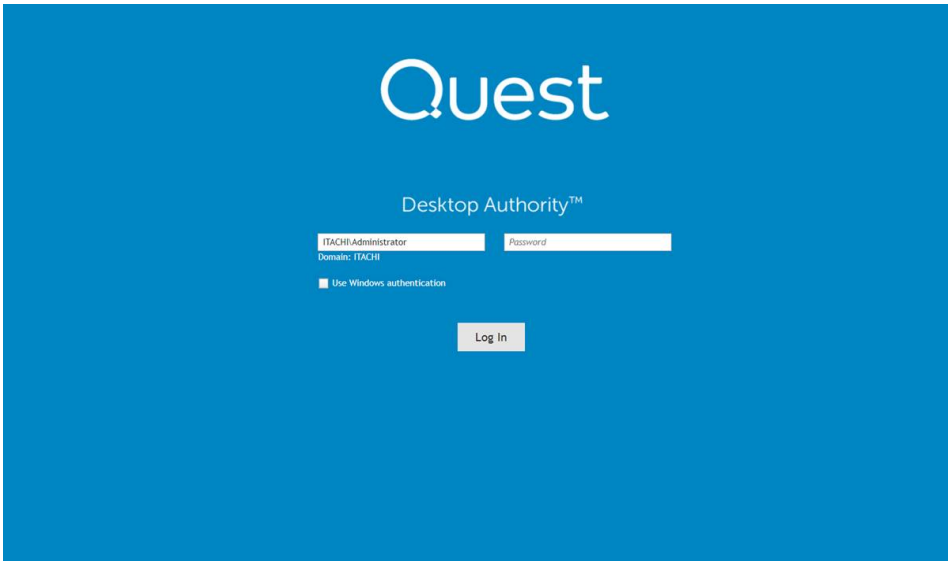
- Installation and Upgrade Guide
- Getting Started Guide
- Administrator Guide
- Reporting Guide
- Data Dictionary
- Database Diagram
- Release Notes

# Starting Desktop Authority for the first time

Once Desktop Authority is installed, based on the options selected during the installation, Desktop Authority will be automatically started. If it does not automatically start, you can run it from the Start menu.

Click Start > All Programs > Quest > Desktop Authority Manager > Desktop Authority Manager, to start the Desktop Authority Manager. You will be presented with the Manager and logon dialog within your default web browser.

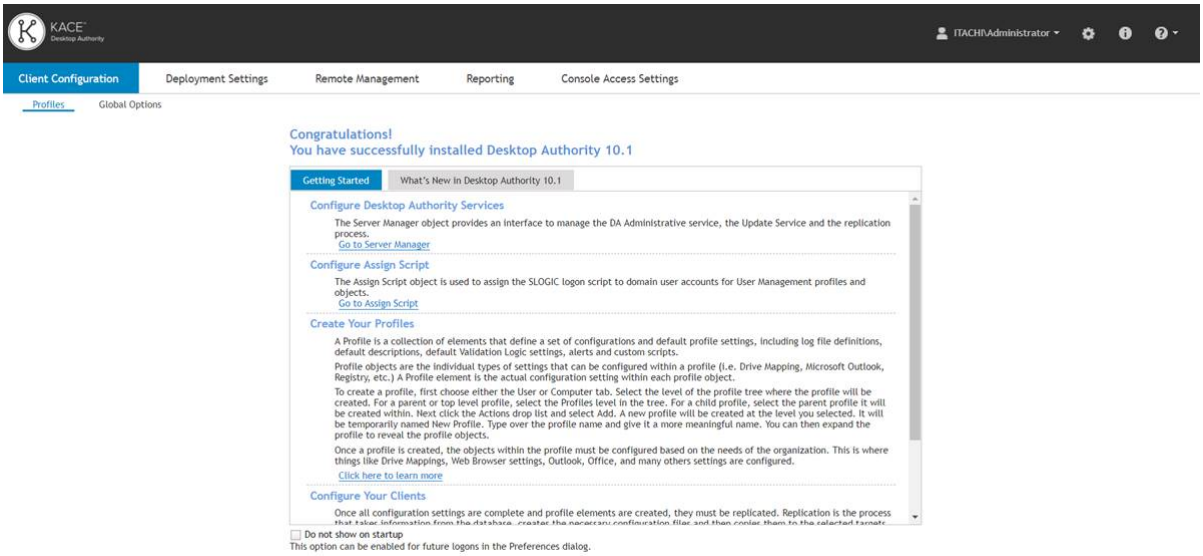
**Figure 1: Login to the KACE® Desktop Authority Manager**




Enter your User name and Password. Be sure to include the domain with your user name. Optionally you may choose to logon by using your current Windows logon credentials. To do this select the *Use Windows authentication* box.

Once you are logged in, you will see the Desktop Authority Dashboard. Here you will be instructed on how to proceed to get started. There is also a tab which shows new product features.

**Figure 2: KACE® Desktop Authority Dashboard**




The dashboard will be te first dialog to show when logging into the Desktop Authority Manager. If you prefer not to see this each time you log in, check the **Do not show on startup** box. You can re-enable this setting in the Preferences dialog at any time.

The dashboard is your guide to getting started with Desktop Authority. It will remind you of the specific things that need to be done to properly configure the Manager for use. These configurations will be discussed further along in this guide.

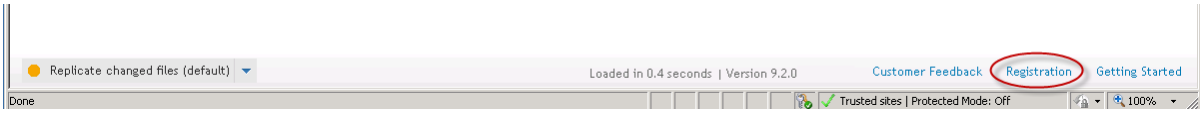
# Registering Desktop Authority

If you are evaluating Desktop Authority there is no registration necessary.

Once a Desktop Authority license are purchased, you must register the software. Registering the software will remove the evaluation time period shown on the Desktop Authority client side splash screen and in the Desktop Authority Manager.

To register your Desktop Authority licenses, click the Registration link at the bottom of the Manager.

**Figure 3: Click Registration to register your licenses of Desktop Authority**




Once on the registration dialog, click the “Add New License” button and enter the required Key. Click Register when finished. Once the registration information is saved, be sure to logout of the Manager and then back in to see the newly licensed features.

# Where do I begin?

There are numerous settings and configurations in Desktop Authority. These settings can be divided into two groups, 1) settings that are available to configure the inner workings of the Manager and backend services and 2) configurations that an administrator creates to provide desktop configuration, management and security for computers in the organization.

The following sections of the Getting Started manual are devoted to creating the settings that will help configure, manage and secure the computers in your organization.

- Configure required services — There are several services that are used by the Manager and must be configured for the system to operate correctly. These services include the Desktop Authority Administrative Service and the Update Service.
- User/Computer Management — All configurations that will be used to configure your organizations computers fall into either User or Computer Management. Here we will define what the difference is and how you should determine which one to use.
- Profile objects and profile elements — In this section we will discuss the basics of creating profiles (a container for common configurations) and the actual elements contained within them.
- Validation Logic — Desktop Authority's patented Validation Logic is used to establish which desktops and/or users will receive a particular configuration. In this section we will discuss how to use Validation Logic to provide granular control to the defined profiles and profile elements.
- Data Collection and Reporting — Here you will learn about the settings that must be configured in order to run the pre-defined and custom reports. Reports include just about all of the necessary data you need to know to manage your organizations computers.
- Are you on the right track? Validate your configurations — In this section we show you how turn on Desktop Authority Trace Files to verify configurations are applied correctly to the right set of computers/users. This technique is also used to troubleshoot configurations that are not working correctly.
- Client Provisioning — Client provisioning is used to deploy necessary files to client computers. These files are necessary to support the DA Administrative Client service, Desktop Agent and the Computer Management service. This section will detail how the client provisioning process works.
- Assigning the Logon Script — The logon script is the key to deploying user based settings. The KACE® Desktop Authoritylogon script must be assigned to any Active Directory user who is to receive configurations from Desktop Authority. This section will discuss how to assign the logon script.

- Saving and replicating configurations — The act of replication is how the Desktop Authority configurations are deployed to the computers within the organization. The settings are made available to users who log in to the network and computers that are part of the organization. Here we discuss how the replication process works.

The configurations that support the administration of the Desktop Authority Manager and its back end services are discussed in full detail in the Administrators Guide and the online help.

# Configure required services

In this section we will cover the installation/configuration of the different services that should be installed following a new installation or system update. These services include the Desktop Authority Administrative Service and the Update Service and will be explained below.

# DA Administrative Service

The DA Administrative service enables Desktop Authority to perform tasks that require administrative rights. This service helps Desktop Authority perform these 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.

To install or update this service, proceed to the Server Manager. Server Manager is a multi-threaded component that provides an interface to manage the DA Administrative Service, the replication process and the Update Service.

The first thing you will need to do is to load Server Manager with the servers that will be used by Desktop Authority. Click on the Go to Server Manager link on the Getting Started tab or click on Deployment Settings in the top menu.

Click the **Discover** button to have Server Manager automatically find existing Domain Controllers on the network. You can also manually add servers using the **Add** button. You will want to add servers/domain controllers that will be used for replication and hosting of the DA Administrative Service and Update Service.

Once the appropriate servers are added to the Server Manager grid, you will need to configure the DA Administrative Service. You will see a column in the grid for this service. Click on a server in the grid to add this service to. Once selected, click on the **Administrative Service** button and choose Install from the drop down menu. This will bring you to the service settings.

Provide two sets of credentials for the service. This service requires two unique user accounts. The Server user account (domain admin) is used on each Domain Controller to remotely install the Desktop Authority Administrative Client Service on each workstation. Therefore, 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 should be a member of the Domain Users group.

Click **Install** once the account credentials are entered. You will see the progress of the service installation. Once complete, click the Back link to go back to the Server Manager grid.

# Update Service

The Update Service is only used for MSI Packages and is installed in the Server Manager. If you have not done so yet, you will need to load Server Manager with the servers that will be used by Desktop Authority. Click the **Discover** button to have Server Manager automatically find existing Domain Controllers on the network. You can also manually add servers using the **Add** button. You will want to add servers/domain controllers that will be used for replication and hosting of the DA Administrative Service and Update Service.

Once the appropriate servers are added to the Server Manager grid, you will need to configure the Update Service. You will see a column in the grid for this service. Click on a server in the grid to add this service to. Once selected, click on the **Update Service** button and choose Install from the drop down menu. This will bring you to the service settings.

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, as well as access to the Internet.

Click **Install** once the account credentials are entered. You will see the progress of the service installation. Once complete, click the Back link to go back to the Server Manager grid.

# User/Computer Management

In this section we will cover the difference between User and Computer Management. We will also discuss how to decide if a specific configuration belongs in a User Management profile or a Computer Management profile.

## What's the difference?

Computer Management supports configurations of the computer operating system and options that apply to all users of the machine. These settings are configured whether there is a user logged on the system or not. Computer Management settings are applied during a workstations Startup, Shutdown, Refresh, and/or Scheduled events.

User Management objects are used to apply settings that are specific to the User environment and occur only when a user is logged on to the computer. These settings are applied at user Logon, Logoff and Refresh intervals. Note: The Computer and User Refresh intervals are separate from each other (two separate timers).

## How do I know which to use?

The User and Computer Management containers each have their own set of profile objects.

**Table 1: User and Computer Management profile objects**

| Computer Management | User Management |
|---|---|
| • Application Launcher | • Application Launcher |
| • MSI Packages | • MSI Packages |
| • Service Pack Deployment | • Service Pack Deployment |
| • Registry | • Security Policies |
| • Wake On LAN Deployment | • USB/Port Security |
| • Data Collection | • Windows Firewall |

| Computer Management | User Management |
| --- | --- |
| | • Alerts |
| | • Common Folder Redirection |
| | • Display |
| | • Drive Mappings |
| | • Environment |
| | • File Operations |
| | • File/Registry Permissions |
| | • Folder Redirection |
| | • General |
| | • Group Policy Templates |
| | • INI Files |
| | • Legal Notice |
| | • Logging |
| | • Message Boxes |
| | • Microsoft Office Settings |
| | • Microsoft Outlook Profiles |
| | • Microsoft Outlook Settings<br>• OneDrive |
| | • Path |
| | • Printers |
| | • Registry |
| | • Remote Management |
| | • Shortcuts |
| | • Time Synchronization |
| | • Web Browser |
| | • Inactivity |
| | • Power Schemes |
| | • Post-Engine Scripts |
| | • Pre-Engine Scripts |
| | • Data Collection |

You will notice by looking at these categories, most of them are under either User Management **or** Computer Management. However, for a few of them, they appear in both User **and** Computer Management.

First determine if the setting to be configured belongs to User, Computer or both. If it only belongs to one of them, then the decision is easy. When the setting belongs to both User and Computer Management you must use further deduction to determine the correct placement.

### *You must now ask yourself a few questions:*

1. Is this setting for one or more specific users? If so, then it belongs under User Management.
2. Is this setting for a specific Operating System? If so, then it belongs to Computer Management.
3. Does this setting pertain to a server (not terminal server)? If so, then it belongs to Computer Management.
4. Is this a setting that can be configured under both, User or Computer Management, opt for Computer Management. This may reduce the user's logon/logoff time.

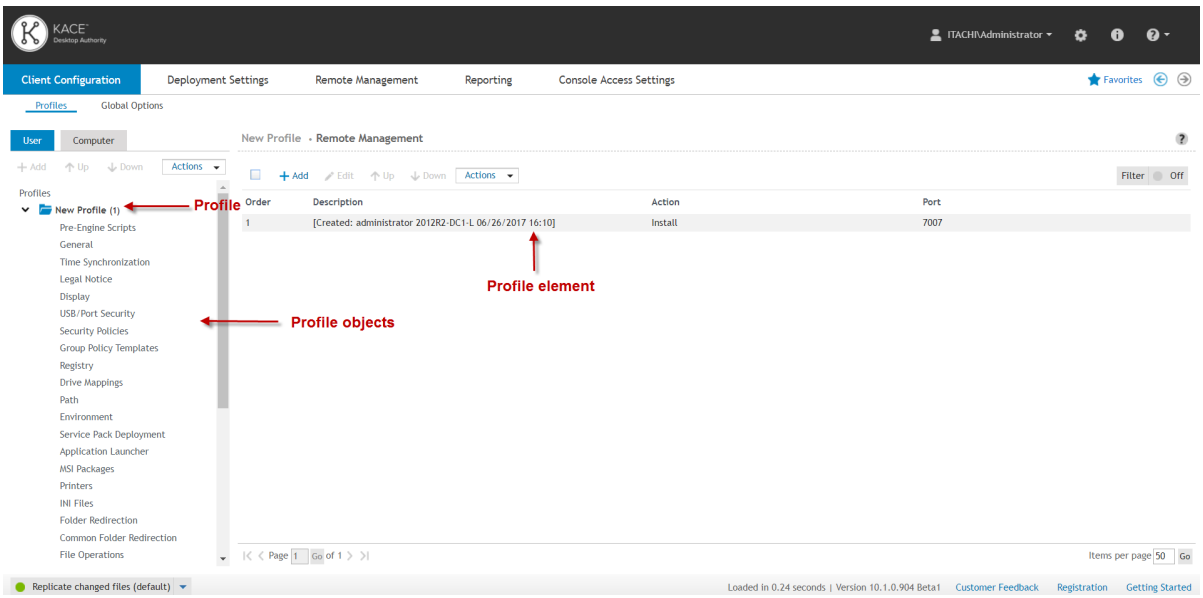
As with most things, since Desktop Authority is such a flexible tool, there will be some configurations that can be configured in more than one way. If you are not exactly sure how to configure a setting, use common sense and test the setting with a test user first.

# Profile objects and profile elements

A Profile is a collection of elements that define a set of configurations and default profile settings, including definitions (used to create custom variables), default descriptions, Validation Logic, default Validation Logic settings (default Validation Logic settings are used when new profile elements are created).

Profile objects are the individual types of settings that can be configured within a profile (i.e. Drive Mappings, Microsoft Outlook, Registry, Printers, etc.) A Profile element is the actual configuration setting within each profile object.

**Figure 4: Detailed view of Profiles, Profile objects and Profile elements**




# Validation Logic

In order for profiles and configuration elements to be processed for users or on computers, Desktop Authority must qualify whether a profile or a profile element should be applied to a workstation and/or user. Validation Logic is used to determine this. A set of rules is created for every profile and profile element setting within the Manager. This set of

rules includes the definition of connection types, class types, operating systems, virtual environment and many other types.

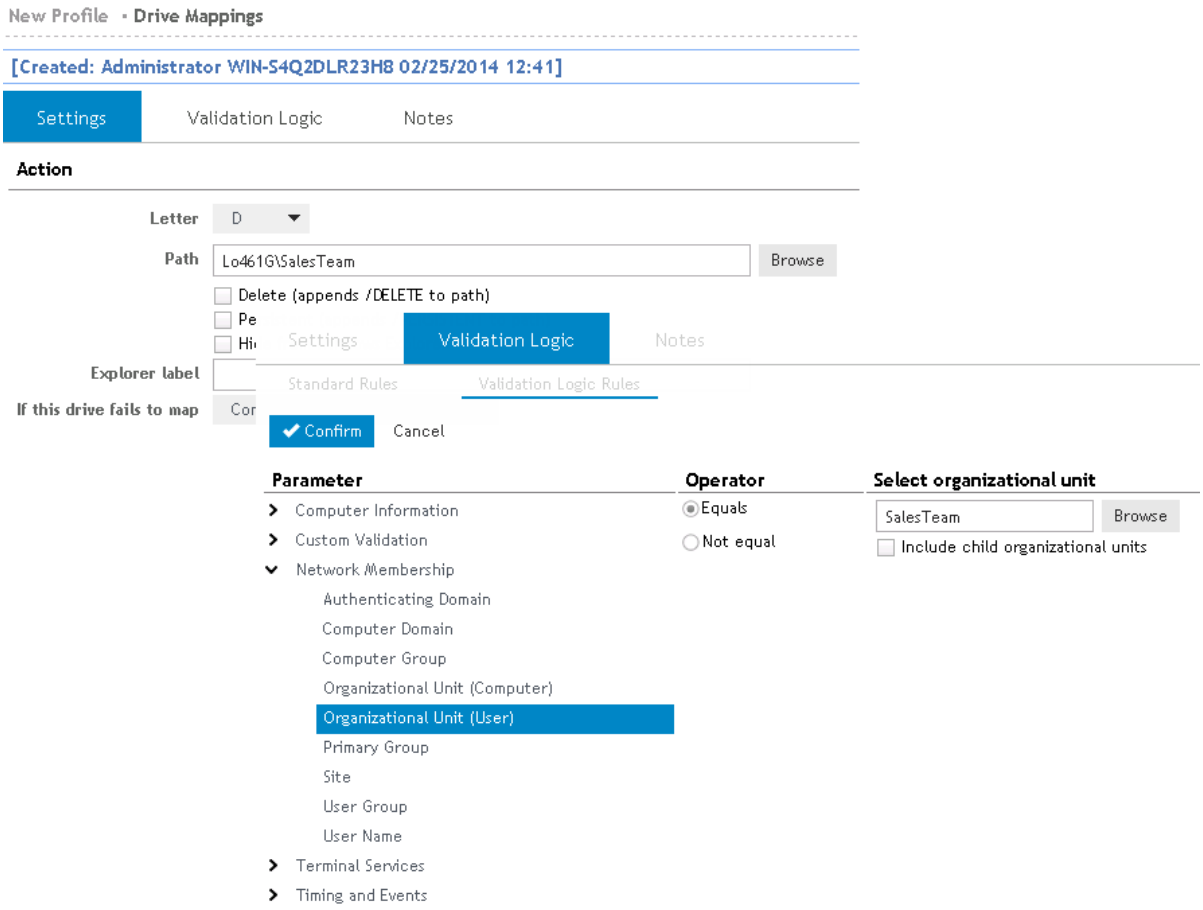
For every profile and profile element setting there is a Validation Logic tab. Select this tab and configure who or what type of computer the profile and/or setting should be applied to.

> Note: User based Validation Logic type rules are not available for use within Computer Management Validation Logic.

Here is an example of how validation logic might be used:

Let's say there is a share that you want to configure for the Sales department and you want to use Drive F:\. Using the Drive Mappings profile object, you will create an element and use Validation Logic to determine who is in the Sales department and therefore who will validate for this drive mapping. The Validation Logic for this element can use either Organizational Unit or User Group validation logic type, depending upon the OU and User setup in Active Directory.

**Figure 5: Example of Validation Logic usage**




# Timing events

Desktop Authority elements are configured to be applied to the User and/or Computer at specific times during the logon, logoff process of the user or startup and/or shutdown process of the computer. Timing allows elements to be applied at the appropriate event.

Computer Management elements can be set to configure during a computer startup event, computer shutdown event, refresh interval or based on a specific schedule. Refresh is an event that occurs every 60 minutes following the computers startup event. A scheduled event can be set to occur one time, daily, weekly or monthly.

User Management elements can be configured to be applied to the User environment on a computer during the client logon process and client logoff process and/or refresh interval. A refresh event occurs every 60 minutes following a client logon.

> ⓘ Note: A User Management refresh interval is entirely different from the Computer Management refresh timing interval. They are two separately timed events. The Computer Refresh timer begins following the computer startup. The User Refresh timer begins immediately following a user logon.

# Profile creation strategy

There are a million and one ways that profiles can be created and used within Desktop Authority. There is not really a right or wrong way, and it will vary based on the organization's needs. Most often, you will want to use more than one profile to hold all of the organization's configurations.

A smaller organization might not have as many Profiles as a larger one, but this still varies based on the company's needs.

## Why do we want more than one profile?

Using more than one profile enables greater manageability and control over client configurations. Using multiple profiles also allows the individual profiles to process faster. Multiple profiles will break down a large number of configurations into smaller groups of configurations, where not all settings will need to be validated at logon time. If a profile is deemed to be invalid for the client, all elements in the profile are bypassed thus saving the processing time it would have normally taken to validate each of the elements separately.

It also makes management of the profiles easier. For instance, if there is a specific profile for the Sales department, you know that when making any changes, it is the only profile that must be touched.

User Management and Computer Management are two separate entities in the Profile tree. They each have their own parent profiles, child profiles, profile objects and profile elements. Keep this in mind when determining how to setup your profiles.

## Some common ways to organize your profiles

- Group (User or Computer Group)
- Site
- Location (by IP Address or possibly Computer Name if the naming convention is location based.)
- Desktop, Laptop, Terminal Servers, Member servers, Virtual Environment.
- Timing (Logon, Logoff, Refresh)

Be sure to give your profiles meaningful names. You may want to draw up a profile map so anyone using the manager will know where to find particular types of elements..

Example profile map:

User Management

Profiles

ACME – Main company profile (all common settings here)

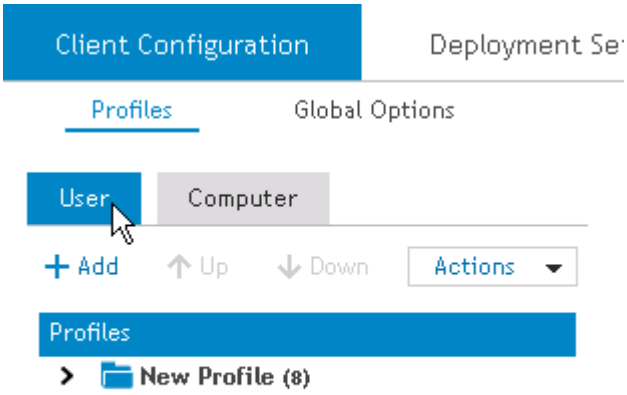
- ACME.STL – Child profile – Seattle office (settings specific to Seattle office)
    - Profile validation logic: SITE = ACME.STL
- ACME.NY – Child profile – NY division (settings specific to NY office)
    - Profile validation logic: SITE = ACME.NY
- ACME.SALES – Child profile – Sales dept settings, all offices
    - Profile validation logic: COMPUTER/USER GROUP = SALES

Once you have decided how your profiles will be mapped, go into the Manager and create each parent and child profile.

# Creating profiles

To create a profile, first choose either the User or Computer tab. Select the level of the profile tree where the profile will be created. For a parent or top level profile, select the Profiles level in the tree. For a child profile, select the parent profile it will be created within. Next click the **Actions** drop list and select Add. A new profile will be created at the level you selected. It will be temporarily named New Profile. Type over the profile name and give it a more meaningful name. You can then expand the profile to reveal the profile objects.

**Figure 6: Creating a profile**




When a profile is created, don't forget to update the Validation Logic. The profile validation logic will affect all elements within the profile. If the workstation validates for the profile, then the elements defined within it will also go through their own validation process. However if the workstation does not validate for the profile, then NONE of the profile elements will be inspected for validity with that computer/user.

# Configuring profile elements

Within each profile there are profile objects. Profile elements are created within profile objects. Let's walk through the creation of a few different types of profile elements.

The Drive Mappings object is one of the most often used profile objects. It is used to map a drive letter to a shared network resource.

***Let's first create the Drive Mapping element. It can be found within the User Management profile objects.***

1. Expand the profile's categories.
2. Expand the Configuration Management category and click on the Drive Mappings object.
3. Once the object is selected, it is displayed in the right hand pane of the console.
4. Click the **Add** button. The Drive Mappings Settings tab will be displayed. This is where you configurations will be made.
5. Choose a drive letter to use for the mapped drive.
6. Next choose the network location that the drive will be mapped to. Click the resource browser to locate it or enter the path manually.
7. Now we will fill in the Validation Logic. Click on the Validation Logic tab.
8. Select the specific Class, OS, Connection Type, Timing, Virtualization and Platform this element will apply to.
9. The last part of this element will define the specific validation rules. Select the Validation Logic Rules tab. If the drive mapping will apply to all users, there is no need to define any rules. However, let's pretend that the mapping we are defining will need to be applied to all users in the HR department, regardless of what computer they logon from. This rule can be created a few different ways depending on how the users are defined in Active Directory. For this example we will say that the HR users all belong to an Organizational Unit called HR_DEPT. Let's select the Organizational Unit (User) parameter. We will select the Equals Operator and select the Active Directory Organizational Unit or HR_DEPT. Click on the resource browser button to locate it in AD. Click Confirm to save the Validation Logic Rule.
10. This element is now complete. Click the **Save** button to save the element.

Let's configure another element. This time we will configure a Registry setting. Before jumping in and creating the element. We must give this one some thought.

This new Registry setting will override the default computer refresh interval.

The Registry profile object is one of the few objects that can be configured in both the User Management and Computer Management profile object trees. It is based on the context of the registry setting. Is it user based or computer based?

***Since it is the computer refresh interval we will be working with, we will use the Computer Management Registry object. Select the Computer tab in the profile tree.***

1. Expand the profile's categories.
2. Expand the Configuration Management category and click on the Registry object.
3. Once the object is selected, it is displayed in the right hand pane of the console.
4. Click the **Add** button. You will be redirected to the Registry Settings tab. This is where you configurations will be made.

5. We will configure the following settings:
    - Action: Write Value
    - Hive: HKEY_LOCAL_MACHINE
    - Key: \Software\ScriptLogic\Device Agent\Global Settings\
    - Type: REG_SZ
    - Value: Event_Refresh_Time
    - Data / Expression: 120
6. This setting will be in effect for all computers. In this case, a validation logic rule does not need to be defined. However, click on the Validation Logic tab and confirm the standard rules are all set.
7. Click **Confirm** to save the Validation Logic.
8. Click **Save** to save the profile element.

# Data Collection and Reporting

While setting up Desktop Authority profiles and profile elements it is essential to think about Data Collection. Data Collection refers to the data that Desktop Authority can optionally collect about client computers and users.

**Table 2: Data Collection collects the following types of data**

| Computer Management | User Management |
|---|---|
| Installed hardware | Computer Startup and Shutdown events |
| Installed software | User Logon and Logoff events |
| Computer heartbeats | User session Lock and Unlock events |
| Port Security | User session heartbeats |

Data Collection is configured as a profile object in both the User and Computer Management tree. As always, validation logic can be applied to the data collection elements, allowing the administrator to collect the data as granularly as necessary.

The collected data is stored in the SQL database called DAREPORTING. It can be reported on using the Desktop Authority Reporting tool. This is a tool that can be installed to an administrator's computer so they may run the necessary reports when needed. Reports can also be scheduled to run at certain times with the results emailed to selected recipients.

Desktop Authority provides a multitude of reports for the admin to manage the computers and users on the network. However, if there is some facet that must be reported on differently, the admin may modify a pre-defined report or create a custom report to suit their needs.

By default the reporting tool is installed to the server where Desktop Authority is installed to. However, it can be downloaded and installed to another computer in the network by selecting the Reporting tab from the menu bar within the Desktop Authority Manager.

More information on using the Desktop Authority Reporting tool can be found in the Reporting Guide which is available for download from the Support Portal.

# Are you on the right track? Validate your configurations

To ensure the configurations are set on the client as you wanted, you may turn on trace file logging to check out what was set. Logging will collect specific information from the client machine as well as user information based on Active Directory, which Desktop Authority uses to determine whether or not a Profile or a Profile element validates. Logging can also be used to troubleshoot any future problems you may encounter.

The log creates a timed stamped log of each action that Desktop Authority takes based on the Profile and Profile elements created in DA Manager.

There are two places where logging should be configured. They are both found within the Global Options. Computer Management logging is always on by default. The files it creates can be found on each client computer in the "%windir%\temp\Desktop Authority" folder. However these client files can be uploaded to a central repository on the network and the file is renamed with the date, time, and computer name for uniqueness. Configure the network location by selecting Global Options > Computer Management Options > Troubleshooting.

For User Management logging, select Global Options > User Management Options > Troubleshooting. Select the "Create a detailed trace file for these specific computers and/or users" and specify the computers and/or users that you would like to create a trace file for. Wildcards can be used here to enable logging for multiple computers, for example use "*" to validate for all computers and/or users. Again, you have the option of uploading the trace files to a central folder on the network. This makes for easier access to these files if you need to do some troubleshooting. The Computer and User based log files are uploaded to the central repository using the DA Administrative User account. This account must have appropriate permissions to the central repository location so the files can be copied. The Computer based log files are uploaded to the central repository at the end of the day and user based log files are uploaded right after the event (Logon, Refresh, Logoff, or Shutdown) is complete.

# Client Provisioning

Desktop Authority must deploy certain files to client machines. These client files are used to support the DA Administrative Client service, Desktop Agent and the Computer Management service.

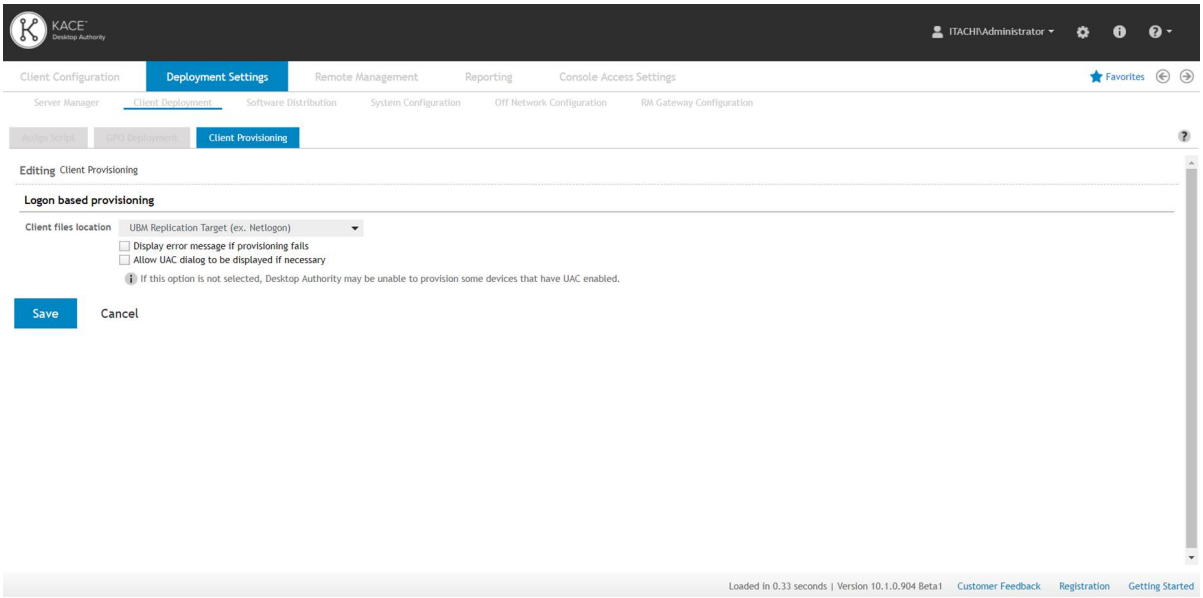
The client files are deployed using Smart Client Provisioning. Smart Client Provisioning dynamically chooses from the best of several deployment approaches at runtime to determine which method will work on the client. Once a deployment option is found the files are deployed to the machine. The specific technique that is chosen to deploy the client files depends on the client environment and the obstacles present in that environment.

The client files may be deployed using the DA GPO client side extension. However configuring this requires higher permission levels than non-domain admins, such as an OU Admin, would typically have. Therefore, in some cases, an OU Admin would not be able to configure the files for deployment to clients without assistance from a Domain Admin. Having to request a Domain Admin to help configure this, defeats the purpose of having an OU Admin, who should be able to configure and deploy files to the clients under the OU they are in charge of.

It is due to this privilege level issue and other circumstances, that Smart Client Provisioning has been implemented. Smart Client Provisioning will go through a series of steps to get the client files deployed to or installed on client machines.

Client Provisioning is configured by selecting **Deployment Settings > Client Deployment > Client Provisioning**. Click the Edit button and configure Logon-based provisioning by specifying a preferred domain, domain controller and the client files location. Desktop Authority will do the rest of the work for you.

**Figure 7: Configuring Client Provisioning**




Note: For more information on Smart Client Provisioning, please review the documentation provided in the Administrator's Guide, Online Help, or the Smart Client Provisioning article.

# Configure Off-Network Support (Optional)

For customers with a desire to configure remote machines while they are disconnected from the corporate network, Desktop Authority offers an off-network support feature. Once properly configured, remote users and computers will continue to receive the most applicable configuration updates as long as an active internet connection is maintained. Please see the Desktop Authority Administration Guide for more information on configuring Off-Network Support.

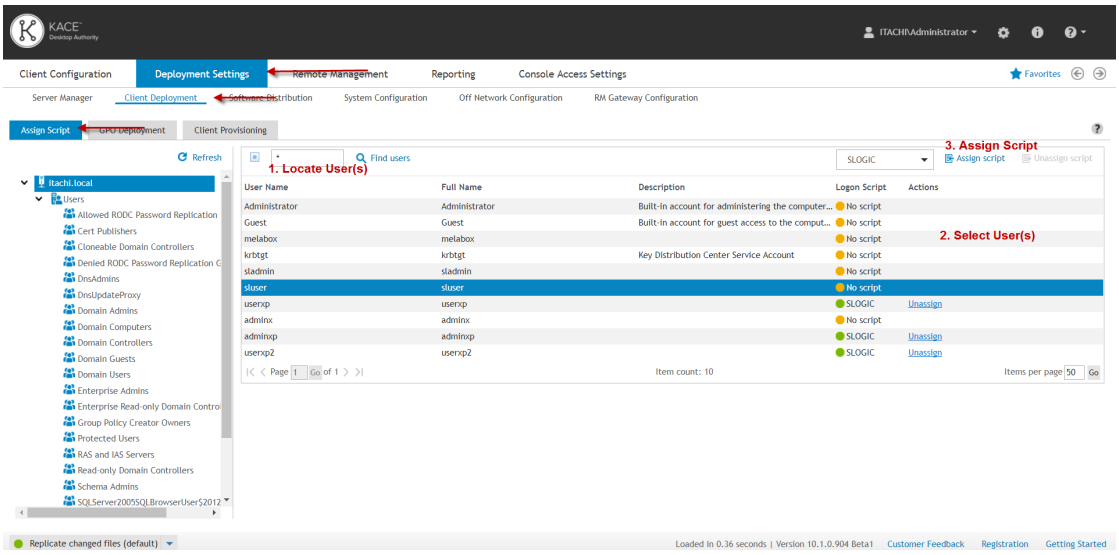
# Assigning the Logon Script

Desktop Authority User Management settings are configured on client computers when a user logs on to the machine. During the logon process, the user is authenticated by a Domain Controller. Desktop Authority is launched by a logon script that is specified in Active Directory for the user. Desktop Authority's logon script is SLOGIC.bat. This logon script can be assigned to users in Active Directory within the Desktop Authority Manager.

The Assign Script dialog can be found within the Deployment Settings tab. Go to **Deployment Settings > Client Deployment > Assign Script**.

Once on the Assign Script object you must locate one or more users to whom the logon script will be assigned. You may enter a search term to find a user1, and/or choose the Domain or an OU and click on the Find User button. Look through the returned list of users to locate the ones who will have the script assigned to them. Select the user(s) by clicking the checkbox to the left of the User Name2. Once all necessary users are selected, click the Assign script button. You will see the SLOGIC script get assigned to the selected user(s) in the Logon Script column.

**Figure 8: How to use the Assign Script dialog**




Note: The Active Directory script assignment is performed on a single Domain Controller, the same as when a script is assigned within Active Directory. This change will be replicated to all other Domain controllers by NTFRS.

# Saving and replicating configurations

Once all configuration settings are complete and profile elements created they must be replicated. Replication takes the information from the database, creates the necessary configuration files and then copies them to the selected targets as specified in Server Manager target folders. (Details about Server Manager can be found in the Desktop Authority online help or Administrator's Guide.) In a typical environment, the replication targets are subdirectories under Sysvol on the Domain Controllers. It is recommended to populate Server Manager with all of the Domain Controllers with the DA Administrative service installed to them. However, it is highly recommended to only select one of your Domain Controllers as a target for replication.

The replication process uses the account specified for the DA Manager (Console) service, which requires access to the Domain Controllers. By default, the Computer Management target folder is located at "C:\Windows\SYSVOL\sysvol\Domain.Name\Policies\Desktop Authority\Device Policy Master". The default User Management target folder is "C:\Windows\SYSVOL\sysvol\Domain.Name\scripts", which is shared as NETLOGON. These folders may be changed in Server Manager, if necessary. Please refer to the File Paths appendix for the correct path(s) based on the version of Desktop Authority you are using.

If your service account does not have access to the Domain Controllers, then DA can be configured to use member servers. Please contact Technical Support for further assistance working within a Member Server configuration.

At the bottom right-side of the Manager, there is a Replication status indicator. The status indicator will show as green or yellow. A green status means that all configurations have been saved and replicated to the target. Please allow NTFRS to replicate the configuration settings to the rest of the Domain Controllers in your environment. Yellow status means that the configurations must be replicated. Simply click on the Replication button to begin the process.

Once the settings are replicated you are ready for the computer and user settings to be configured on the client workstations.

For further details on using Desktop Authority, please reference the Administrator's Guide, Installation and Upgrade Guide, Reporting Guide and/or the built-in online help when running the Manager.

# A

# 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<br>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<br>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<br>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<br>• (64-bit) %SystemRoot%\SysWow64\DAAdminSvc_%ComputerName%.log<br>• (64-bit) %SystemRoot%\SysWow64\DAAdminSvcStRep.log | • (32-bit) %SystemRoot%\System32\DAAdminSvcStRep.log<br>• (64-bit) %SystemRoot%\SysWow64\DAAdminSvc_%ComputerName%.log<br>• (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<br>• Target: %windir%\SYSVOL\sysvol\DomainName\scripts | • Source: x:\PF\Quest\Desktop Authority\Desktop Authority Manager\scripts<br>• Target: %windir%\SYSVOL\sysvol\DomainName\scripts |
| **Computer Management Replication** | |
| • Source: x:\PF\ScriptLogic\Desktop Authority Manager\Device Policy Master<br>• Target: %windir%\SysVol\sysvol\DomainName\Policies\Desktop Authority\Device Policy Master | • Source: x:\PF\Quest\Desktop Authority\Desktop Authority Manager\Device Policy Master<br>• 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<br>USB/Port Security devices | New or 11.3.2 Version Paths |
|---|---|
| • x:\PF\ScriptLogic\Port Security | • x:\PF\Quest\Desktop Authority\PortSecurity<br>• %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