Quest™

KACE® Desktop Authority 11.2

Administrator Guide

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

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

Patents

Trademarks

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 - Administrator Guide
Updated - October 2021
Version - 11.2

Contents

1

Concepts

What is Desktop Authority?

Quest® Desktop Authority®, the leading desktop management platform for Windows-based networks, significantly reduces total cost of desktop and application ownership by enabling administrators to proactively secure, manage, support and inventory desktops and applications from a central location. Desktop Authority centralizes control over desktop configurations, combining the functionality of logon scripting, group policies, user profiles and computer profiles into one comprehensive solution.

Desktop Authority is available 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, Custom Reporting and the Desktop Authority Remote Management tool.

Desktop Authority Standard is a version of Desktop Authority that is geared towards enterprises who already use KACE Systems Management Appliance (SMA, previously known as K1000) or Microsoft's System Center Configuration Manager (SCCM) or other similar management tools. Since they provide tools for Software Distribution and Asset Management, Desktop Authority does not include its own built-in Software Distribution or Asset Management capabilities.

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

This product includes a set of standard documents, such as the *Administrator Guide*, online help, *Release Notes*, and other manuals. For the latest version of the Desktop Authority documentation, visit the Technical Documentation page on the Quest Support Portal: https://support.quest.com/kace-desktop-authority/technical-documents.

Desktop configuration (user and computer management)

From a single server-based installation point, Desktop Authority assists administrators with the never-ending chore of configuring each desktop attached to the network. When a user logs on or off, their personalized configurations

are applied to their environment. The Operating System and applications get "fine-tuned" to the specific user. Best of all, Desktop Authority does this without requiring you to reduce overall security, without maintaining separate security policies and without the need for a network administrator to visit each computer.

Desktop Authority allows administrators to centrally manage over 30 different categories of desktop settings including drive mappings, search paths, printer deployment, Windows Firewall ports, Internet configuration & proxy settings, Microsoft Office paths, service pack, Group Policy Templates, Security Policies, desktop shortcuts, automatic mail profile creation for Outlook/Exchange, file operations, registry settings and more.

Desktop Authority also attends to each computer in the enterprise. Using a computer based agent, each computer can be configured and inventoried, independent of the users that log on to the computer.

Desktop Authority uses its patented Validation Logic technology to determine how each desktop will be configured. The Validation Logic technology is based on over 20 validation types including the class of computer (such as desktop or portable), client operating system, group membership, Active Directory sites, OUs, and registry and file properties. Selection can be enhanced further using AND/OR expressions to combine multiple Validation Logic rules. Custom validation types can also be defined to allow configuration by desktop attributes list, Asset Tags or hardware configuration.

Software Management

> Note: Not available in Desktop Authority Essentials.

MSI packages contain all necessary files an application needs in order for it to be installed using Microsoft's Windows Installer. Desktop Authority manages a repository of Microsoft Windows Installer (MSI) packages. Packages can be deployed to and/or removed from specified desktops based on User and/or Computer specifications.

USB/Port Security

> Note: Not available in Desktop Authority Essentials

The myriad of portable storage mediums today make it essential for corporations to prohibit or monitor the use of certain devices on the company network. These devices can be very harmful to a corporation. Confidential data can easily be copied to any portable device, viruses can be introduced to the network and spread corporate wide and illegal software can be copied to the company network.

Since most portable devices are small in size it is simple for any employee to use these devices regardless of a written or verbal company policy. The user's ability to use these devices and/or transfer data to and from these devices must be restricted. The USB/Port Security object will do just this.

Users and/or groups of users can be restricted from using certain types of removable storage devices. Desktop Authority's USB/Port Security object will protect the company network against unauthorized usage of devices such as MP3 players, PDAs, WiFi and more.

The USB/Port Security Option can help to free the enterprise of unwanted removable storage devices, easily and quickly.

Role Based Administration

In larger organizations there are typically multiple levels of administrators, with junior ones assigned to specific geographical locations or restricted administration tasks. Desktop Authority’s new architecture allows Super Users to restrict other administrators to only view, change, and add or delete a limited set of configuration objects. By defining roles and applying those roles to users or groups at the profile level, SuperUsers can ensure that administration of Desktop Authority follows enterprise security boundaries.

Hardware and Software Inventory and Custom Reporting

Note: Not available in Desktop Authority Essentials.

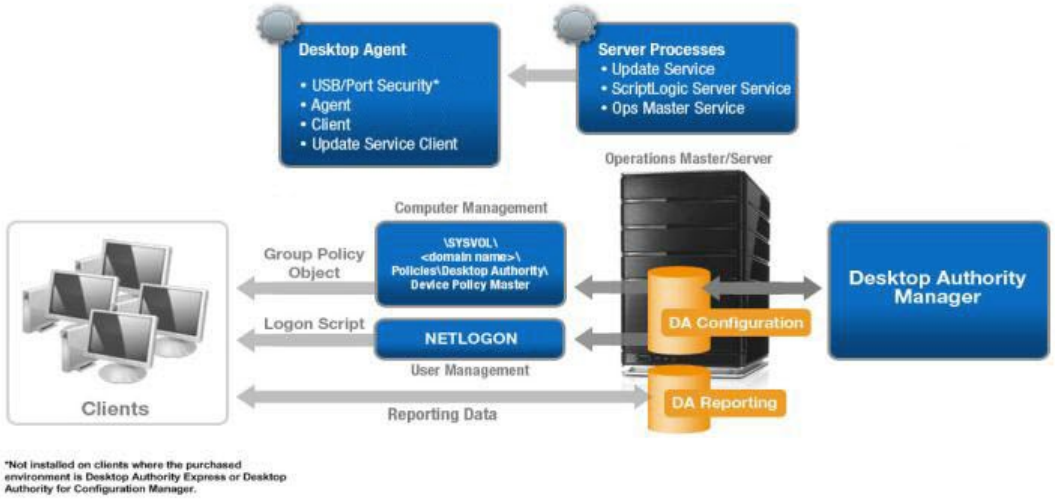
Desktop Authority profiles and their configurations are stored in an SQL database, along with information about the managed desktop. Built-in and custom reporting puts vital information at the fingertips of administrators, including reports on hardware and software inventory, and user activity.

Comprehensive Reporting includes built-in and custom reporting on Hardware/Software Inventory, User Activity and Desktop Authority configuration.

How does Desktop Authority work?

Desktop Authority uses several components to facilitate the configuration of desktops and servers. These components include the Desktop Authority Manager, Configuration and Reporting databases, Server Processes and the Desktop Agent. These components all work together to provide an efficient, scalable, and secure desktop management system.

Figure 1: Overview the Desktop Authority system



Desktop Authority Manager

The Desktop Authority Manager is the central console from which configuration profiles, services and reports are managed by the Network Administrator. The Manager also provides the ability to remotely manage client computers over the local area network or Internet.

Once configuration data is saved and ready to be configured on client computers, the data is published to the NETLOGON and the Device Policy Master shares. This is done using replication. The replication process updates the replication targets for all target servers specified in the Server Manager object. Data is extracted from the DACONFIGURATION database and written to configuration files in the replication shares. The data is used to configure user based settings when a user logs in to each client machine. Computer based settings are configured and executed on each client, by the local Computer Management agent. The agent is deployed to each client using Smart Client Provisioning (Logon and/or GPO Based deployment).

DA Manager Service

The Desktop Authority Manager Service is the business logic layer for the Manager. It manages communications between the Manager and the SQL databases, DACONFIGURATION and DAREPORTING.

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 insuring that the client configuration files are correctly signed.

Update Service

The Update Service is used for file distribution purposes by Desktop Authority, but is only needed when the Software Distribution feature is in use. The service can be installed on one or more servers within a domain.

Operations Service

Desktop Authority may be installed to a Domain Controller, however it is strongly suggested that Desktop Authority be installed to a Member Server. The installation server is known as the Operations Master. The Operations service is hosted on the Operations Master. This service manages and supports the ETLProcessor and ReportScheduler plugins. This service is installed once per domain on the Operations Master.

Configuration and Reporting Databases

Desktop Authority can install Microsoft SQL Server 2014 Express Edition on the Operations Master server or use an existing SQL Server 2008, 2008 R2, 2012, 2014, 2016, 2017 or 2019 instance. Within this SQL instance there are two databases created. They are DACONFIGURATION and DAREPORTING. The DACONFIGURATION database is used to store product configuration data. The DAREPORTING database stores a copy of the profile configuration data, hardware and software inventory, user activity and other essential data that is collected for reporting purposes (not available for Desktop Authority Essentials).

Smart Client Provisioning

There are two ways in which Desktop Authority can deploy the necessary client files to machines that will be managed by Desktop Authority. Desktop Authority uses Smart Client Provisioning which encompasses both GPO-based Deployment and Logon-based Deployment. Smart Client Provisioning dynamically chooses from the best of several deployment approaches at runtime. The specific technique used depends on the client environment, and the obstacles present in that environment. Click here for more detailed information on Smart Client Provisioning.

Computer Management

Computer Management objects are executed on each client by the Computer Management agent. The Computer Management agent is a service that is deployed to each client as a part of the Smart Client Provisioning process. The agent service interprets the Computer Management object settings and executes them at the appropriate startup, shutdown, refresh and scheduled events.

User Management (Logon Script)

As each user logs on to the network and is authenticated, the user's logon script is executed. Desktop Authority is launched via a logon script named SLOGIC. This script must be defined as the user’s logon script in order for a

client to execute Desktop Authority. The logon script performs initializations and launches the Desktop Authority engine. Desktop Authority User Management configurations can be executed at logon, refresh and logoff events.

Desktop Engine

Once the logon script performs its initial checks, the Desktop engine is launched. The engine will initiate the configuration of objects and elements. First, the Global Options are applied, user defined variables are processed and Pre-Engine custom scripts are executed. If configured, the USB/Port Security and MSI Packages components are launched on the client.

From here, clients are configured with the settings defined in the Manager. Once these settings are complete the engine will execute post-engine custom scripts. Finally, when the logon script completes, reporting data is collected, including hardware and software inventory, and the client desktop is loaded.

Upon logoff, the Desktop engine is again launched. This time any configuration elements found to validate for Logoff timing and for the user and/or computer, will execute. During logoff there is an optional visual indicator that can display to let the user know that something is happening.

What are dynamic variables?

A Dynamic Variable represents an area in memory that is reserved to hold a specific value. The value of the variable is dynamic in that the value will differ based on the current user. These variables are used to hold temporary values during the execution of a logon or custom script. All **Desktop Authority** dynamic variables are prefixed with a dollar ($) sign. The rules for defining new dynamic variables follow the KiXtart guidelines. More information on KiXtart can be found at www.kixtart.org/.

There are two categories of Dynamic Variables: Predefined and Custom. Predefined dynamic variables are ones that are defined by **Desktop Authority**. Custom Scripts may override the value of these variables. **Desktop Authority** can also make use of User Defined Custom dynamic variables.

Predefined dynamic variables

In the **Desktop Authority** Manager, predefined dynamic variables are used to aid in the creation of configuration elements. The great thing about these variables is that since their values change based on the current user/computer, a single configuration entry can be used for all users/computers. You can be assured that at runtime when the logon script is executed, the predefined dynamic variable will contain the documented value based on the current user/computer.

For example, the predefined dynamic variable $UserId can be used to denote the logon id of the current user. At runtime when the logon script is executed, the $UserId variable will contain the UserID of the user currently logging on to the network.

Dynamic variables can be used throughout the Manager by typing the name of the variable into the desired field or by pressing the F2 key when the cursor is in any entry box. Pressing F2 will display a dialog box similar to the following, allowing the selection of a predefined variable from a visual list.

To select a variable, select it in the list and click Insert or double-click the variable. The selected variable will be inserted into the field at the current cursor position. Click the Info link at the right side of the list to get more information about a dynamic variable.

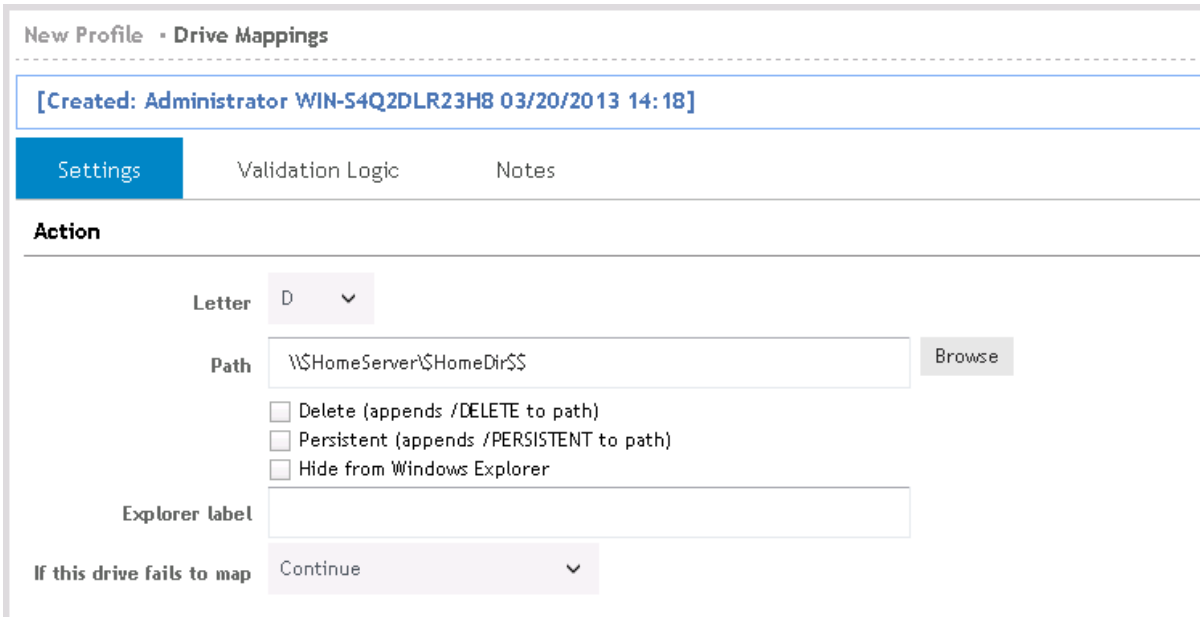
Dynamic variables can also be used in custom scripts. When writing a custom script there is no popup list of valid predefined dynamic variables.

Click here for a complete list of predefined variables.

Example usage:

One of the most commonly used places for using Predefined Dynamic Variables is in the Drive mappings object. Use the $HomeServer and $HomeDir variables to map a home drive for your users.

Figure 2: Example usage of Dynamic Variable



Custom dynamic variables

Custom Dynamic Variables can be pre-defined for use in the Manager as well as in Custom Scripts. To use your custom dynamic variables in the Manager, simply add the variable definition to the Definitions tab of either the Global Options or the Profile dialogs. Defining a variable within Global Options makes the variable available everywhere, regardless of which profiles are processed on the client. Variables defined in the profile's Definitions tab are available only if the profile in which the variable is defined is processed on the client. To add a custom variable, simply click **Edit** on the Definitions tab.

Example usage:

Instead of using the internal dynamic variable for the wallpaper file, a custom Dynamic Variable can be created. Modify either the Global Options or Profile Definitions file. Add a new custom variable called $customwallpaper. Other code can be wrapped around this definition to determine which group (department) the user belongs to. On the Display object, enter $customwallpaper in the Wallpaper file box. When the logon script is executed, the $customwallpaper variable is evaluated and set for each user.

2

User Interface

Overview

The Desktop Authority Manager is a web based application for Network Administrators to centrally manage client's user and computer configurations. All configurations are defined within the Desktop Authority Manager. The Manager is also used to replicate and deploy settings to the clients during the logon, logoff, startup, shutdown and other specified events. The Manager also provides other tools to allow the Administrator to access and configure Global, Profile, Remote Management and Reports.

The minimum screen resolution for the Desktop Authority web console is 1024 x 768.

Logging in to the Desktop Authority Manager

The Desktop Authority Manager is secured by user logins. Access to the different parts of the Manager is granted and/or denied based on the user's permissions granted in the Console Access Settings. This is granted based on roles, permissions and the user assigned to a role.

System settings

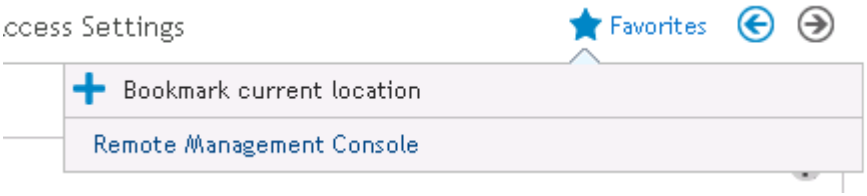
Logged in as

This is informational text that displays the username of the user who is currently logged into the system.

Bookmarks

Displays a list of favorite pages within the Manager. Pages are made a favorite by clicking on the *Bookmarks* link and then *Bookmark current location*.

Figure 3: Desktop Authority Bookmarks



Preferences

Click on Preferences to configure the Manager's global settings.

Help

Opens the help file. If Internet access is available, the online help file will be opened otherwise the help file stored locally will be opened.

Customer Feedback

Opens the online product feedback page. This page allows you to send feedback about your product experience. This is not the place to request technical support.

Logout

Click Logout to exit the Desktop Authority Manager.

Menu Bar

The menu bar provides access to the main areas of Desktop Authority. This includes Client Configuration, Deployment Settings, Remote Management, Reporting and Control Access Settings.

Client Configuration

Configure Computer and User profiles containing client configurations.

Deployment Settings

Configure the deployment of the Desktop Authority Client application, Software Distribution, Server Manager and System Configuration.

Remote Management

Configure and access Desktop Authority Remote Manager. Remote Management offers a simple way to remotely access multiple computers on the network for the purpose of remote control, restarting the computer or deploying or removing the Desktop Authority service.

Reporting

Provides access to the Reporting tool. This tool is downloaded and run locally outside of the web browser.

Console Access Settings

This is Desktop Authority's Role Based Administration area. Console Access Settings provides roles to which users are assigned to. This limits their access to the system, based on what options the roles allow them to access.

Navigation pane

The Navigation pane is available for several of the Menu bar options. For the Client Configuration object, the Navigation pane is used to select a specific Computer or User object to work with. The View pane changes based on the object selected in the Navigation pane.

The Navigation pane is also available for the Remote Management object. Here you will select the client computer to work with.

View pane

The View pane is used to set various configurations and is based on the currently selected object from the Menu bar and Submenu.

Status bar

The Status bar shows a few miscellaneous items including a link to the Replication options, Registration, Getting Started page and Product Resources.

Logging in to the Desktop Authority Manager

The Desktop Authority Manager is secured by user logins. Access to the different parts of the Manager is granted and/or denied based on the user's permissions granted in the Console Access Settings. This is granted based on roles, permissions and the user assigned to a role.

The User name/Password credentials used to login to the Manager are the user's Active Directory credentials.

Check the Use Windows Logon box to logon using current Windows session login credentials. Those are the credentials entered at the Window's logon prompt

Once logged in to the Manager, users will be limited to specific areas of the Manager based on their Roles defined in the Console Access Settings. There can be one or more Super Users defined for the system that has access to the entire console.

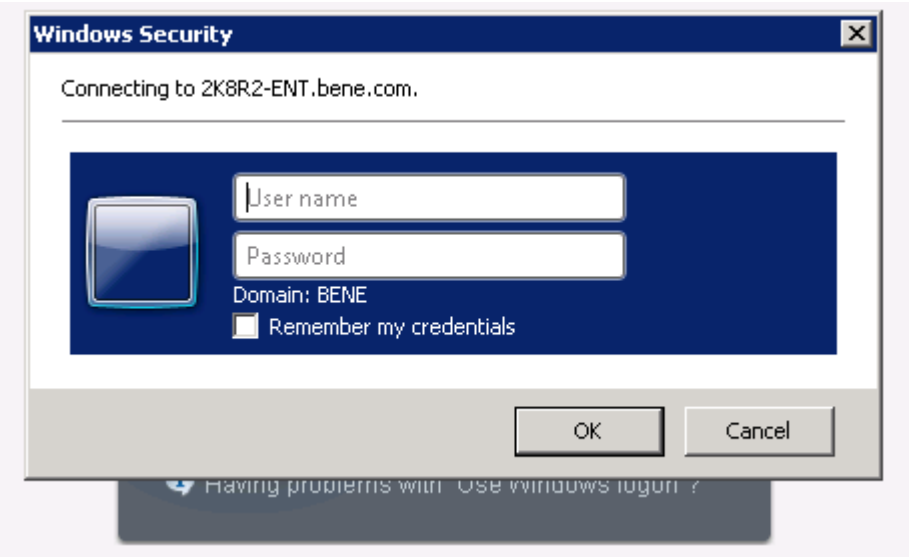
Having problems with Window's logon?

Internet Explorer

Selecting the option 'Use Windows logon" checkbox with the Internet Explorer web browser may cause a dialog box to be displayed requesting the user credentials regardless of the fact that you chose to logon using the current

Windows logon credentials.

Figure 4: Windows security credentials



Internet Explorer must be configured to trust the site. Once this is done, the user credentials will not be prompted for upon each logon.

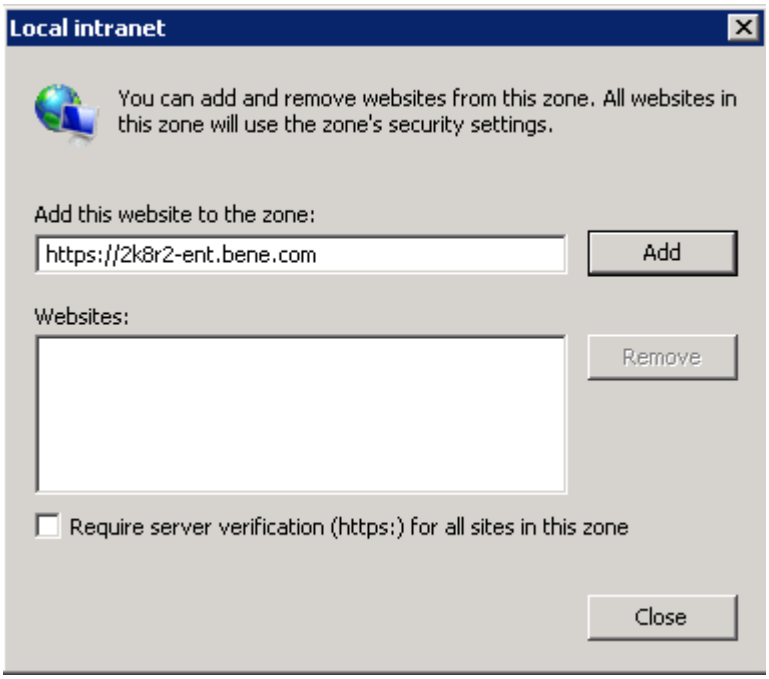
The following steps will help you to configure Internet Explorer.

1. From the Internet Explorer browser window, go to **Tools > Internet Options**.
2. Select the **Security** tab.
3. Select the Local Intranet zone and click on the **Sites** button.
4. Click the **Advanced** button.
5. In the entry field below **Add this website to the zone:** prompt, enter the following:

   https://[*servername*].[*domainname*].com

   For example: https://2k8r2-ent.bene.com

Figure 5: Adding a computer to the Local Intranet zone



6. Click the **Add** button to add it to the Websites list. Then click **Close**.
7. Click on the following 2 OK buttons to save the changes.
8. Restart the browser.

This configuration will add the trusted site to the local intranet zone. This must be done on every machine that will access the Desktop Authority Manager using the **Use Windows logon** option.

Firefox

Selecting the option "Use Windows logon" checkbox when using the Firefox web browser may cause a dialog box to be displayed requesting credentials to be entered each time a login is attempted. However, the correct credentials are not accepted.

The first thing to note is how to enter the credentials. The username must be entered using the format "*DomainName**Username*" (without quotes). If entering only the username, it will not be authenticated on the domain.

The Firefox web browser must be configured to allow NTLM authentication.

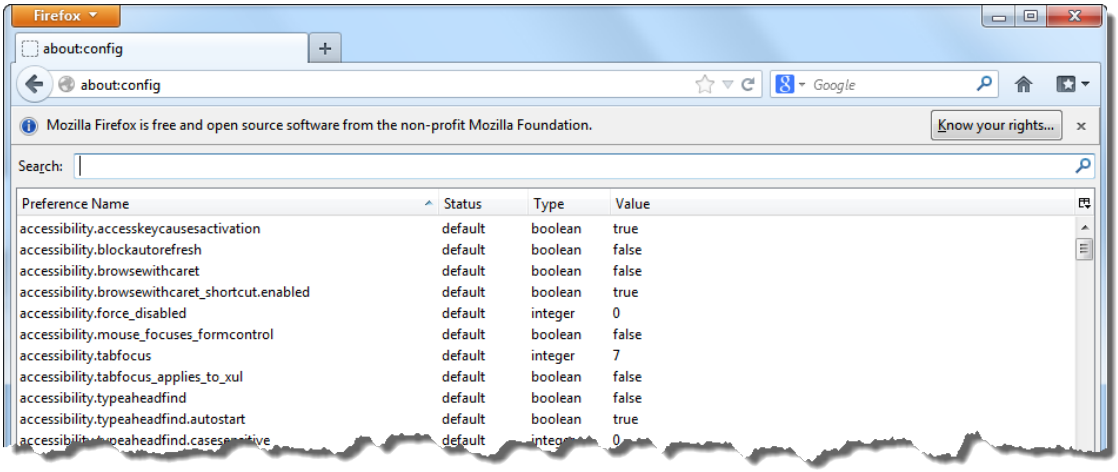
1. Load the web browser and type "about:config" (without quotes) in the address bar.

2. You will be prompted with the following warning:

Figure 6: Firefox configuration warning

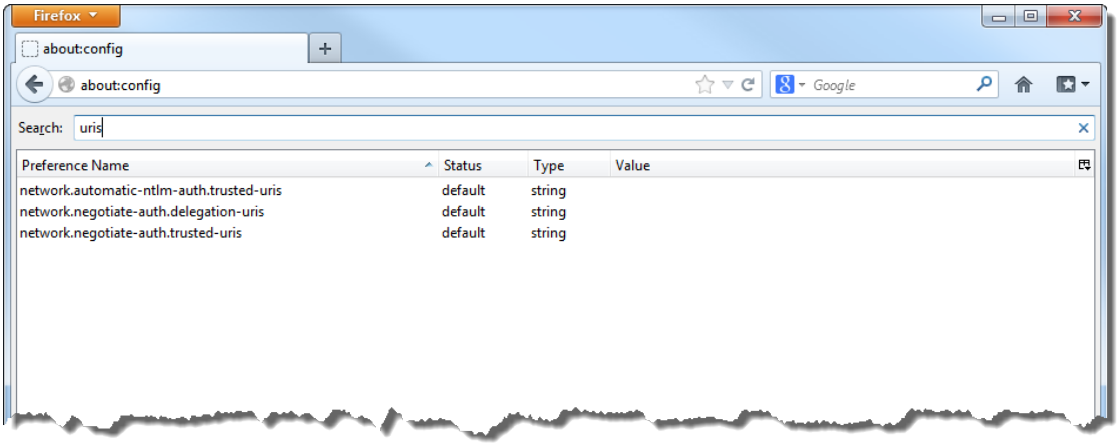
3. Click the "I'll be careful, I promise!" button.
4. You will then be presented with the advanced configuration dialog.

Figure 7: Firefox advanced configuration dialog



5. In the Search entry box, type "uris" (without quotes).
6. This will minimize the configuration list to the following 3 items.

Figure 8: Firefox filtered configuration list



7. Double click on each entry in the list and set the value to the fully qualified domain name (ex. *servername.domainname.local*) of the application to use NTLM authentication. However, if using Firefox with NTLM on the server where DA is installed, then the server name is only required to be entered. If any of the entries already have a value, you should use a comma (,) between each entry.
8. Restart the browser.

Menu bar

The Menu Bar provides access to the main functions of the Desktop Authority Manager. These include Client Configuration, Deployment Settings, Remote Management, Reporting and Console Access Settings.

Client Configuration

Client Configuration is the heart of Desktop Authority. This is where the Computer and User object settings are configured.

Deployment Settings

The Client Deployment object provides access to Assign Script and GPO Deployment, both of which arm the domain user and computer with configurations for Desktop Authority to execute during client logon process

Remote Management

Use the Remote Management menu to Remotely Manage the selected computer in the Remote Management tree of the Navigation Pane.

Reporting

The Reporting object provides predefined reports distributed with Desktop Authority as well as the ability to create custom reports. Reports can be run manually at any time or may be scheduled to run on a specific and/or recurring Date/Time.

Console Access Settings

Use the Console Access Settings menu to configure Super Users/Groups and define Global Roles that define the resource actions that are allowed by any member assigned under the role. Also, select to Change the Operations Master service Credentials from this menu.

Status bar

Replicate

Desktop Authority uses replication to provide a method of publishing Desktop Authority configurations to domain controllers. Desktop Authority does this with its own replication process from within the Server Manager. Server Manager sets the configuration of the replication process on the Server Properties tab within the Service Management dialog. Desktop Authority's replication can be used to replace Windows Directory Replication services or work in conjunction with it. Of course, if Desktop Authority is your only logon script, there is typically no need to add the overhead of Windows' replication process to your domain controllers. Each time changes are made to your

configuration using the Desktop Authority Manager, you will save the changes, replicate and then exit. By default, only the changed files will be replicated.

Desktop Authority can be replicated from any page of the Console. A selection box is available in the status bar of the console (bottom).

Choose to *Replicate changed files (default*, *Replicate all files* or perform a *Force an update of the Desktop Authority folder on clients*.

Replicate changed files - Select this option to replicate only those files that have a different date than those on the destination domain controller. If this check box is cleared, all files will be replicated.

Replicate all files- Select this option to replicate all files, regardless of date and time.

Force an update of the Desktop Authority folder on clients- There are various files that are distributed to each client when Desktop Authority is initially configured on each workstation. As time goes on some of these files may need to be updated. To force this update to occur on all clients, select this option.

The Replicate button contains a colored icon which indicates the status of the Manager's current configurations. This tells at a glance if the most recent configuration changes have been replicated.

The icons represent the following statuses:

 (Yellow) This status indicates that the configurations have been saved but have not yet been replicated.

 (Green) This status indicates all changes made within the Manager have been successfully saved and replicated.

Preferences

The Preferences dialog presents several options that are used to configure Desktop Authority Manager. Click Preferences on the Manager's System Menu.

General

User preferences

Language

Select the Language for the Desktop Authority Manager to use. Currently it is available in English and Russian.

Date/Time format

Select the format the system will use to display all date and time fields.

Session timeout

The Session timeout value represents the amount of time the Desktop Authority Console session can remain active while not in use. Once the selected timeout value is reached, the user logged into the console will automatically be logged out. Select a timeout value from the session timeout drop list.

Time zone

Select to display the server time or the local time in the console. Also select the default time zone for the Desktop Authority Manager. All times will be adjusted and shown in the selected zone.

Profile sort order

Select the sort order of the Client Configuration Computer and User profiles. Select from *by Category*, *Alphabetically*, or *by Execution Order*.

Theme

The Desktop Authority gives the option of being displayed with different themes.

Default description for new list elements

Each object configuration element has a description associated with it. Specify the default description for use on each new configuration element. Several predefined dynamic variables may be used in the description. They are currently limited to: *$USERID*, *$FULLNAME*, *$WKSTA*, *$DATE* and *$TIME*.

Entering **`Created by $Userid, $Date $Time`** provides a description of **`Created by Administrator, 5/10/2003 11:24`** when a new element is added.

The default description is applied to all future configuration elements added to any profile object. Existing elements are not updated. The description may be overridden for each configuration element.

By default, show hidden shares in resource browser

The Resource Browser displays a selection box of available shared, drives and/or folders. Select this box to set the default value for the *Show hidden shares* checkbox in the Resource Browser.

Show Active Directory in resource browser

Select this option to shows Domains, Users and Groups, Computers and Domain Controllers Active Directory objects in the Resource Browser.

By default, show confirmation when navigating off unsaved data page

When a user is editing an element within an object, there is the possibility to navigate away from the unsaved element dialog. Select this box to show a confirmation message that the unsaved data will be lost if you leave the page. Unselect this box so no confirmation message will appear when this scenario happens.

By default, show welcome screen upon startup

When starting the Desktop Authority manager after an upgrade, there is a dialog box that can be displayed which shows a features list for the newly installed version. This notification can be turned off by unselecting this checkbox as well as selecting the "Do not show on startup" checkbox on the upgrade notification dialog.

Show unused objects in profiles

Choose to show all objects within a profile or hide the unused objects, by default, within the profile.

> ⓘ Note: When unselected, a new profile will show only the Logging and Alerts profile objects. To see all of the objects for a profile, this box or the Profile Actions Show Unused must be selected .

Confirmations

Show confirm dialog when the following operations are attempted

Select the box next to each listed item if you want to see a confirmation dialog box when the specified task/action occurs. You will be given the option to continue with the operation or cancel it at that time. Unselecting the box on

this dialog means you will not be prompted for confirmation when these actions occur.

Resource browser

The Resource Browser dialog, most commonly used to configure validation logic, is used to select a specific object from the network resources. The selectable objects are file name, folder, servers and printers. The contents of the dialog are based on the object that the Resource Browser is called from.

Domains, Users and Groups, Computers and Domain Controllers Active Directory objects can also be optionally shown in the Resource Browser. This option is configured in the system preferences.

The **Browse** button is used to call the Resource Browser.

Profile Management

A Profile is a collection of elements that define a set of configurations and default profile settings, including log file definitions, default descriptions, default Validation Logic settings, alerts and custom scripts. Profiles are applied to a particular category of users or computers based on the validation logic defined in the profile settings.

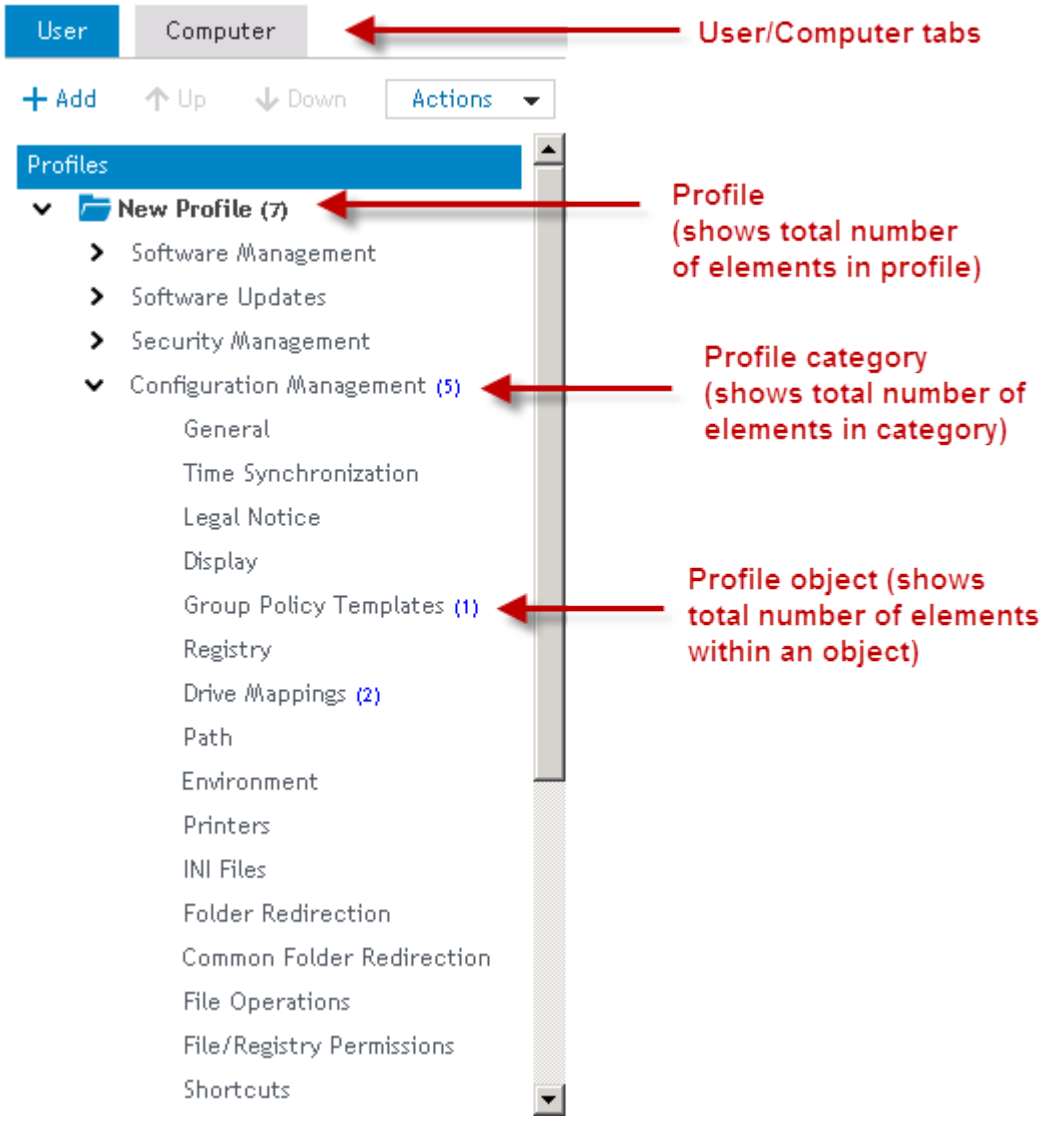
A profile may contain other profiles (children). This allows for greater flexibility and further granularity for its contained configuration elements.

User Profiles are evaluated and applied to the current user's working environment during the logon and/or logoff process or Refresh intervals. Computer Profiles are evaluated and applied to a computer during the Startup and/or Shutdown process, Refresh intervals or based on a defined Scheduled. Only profiles that pass the Validation Logic test will be executed at the specified time on the clients and/or computers.

Using profiles enables greater manageability and control over client configurations. Using profiles also offers the reward of faster logon script processing. Since profiles tend to break down a large number of configurations into smaller groups of configurations, not all settings are processed or 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.

The Manager displays profiles in the Profiles branch of the Navigation tree. There are separate tabs for User Profiles and Computer Profiles. Click ⊞/⊟ on a profile to expand or contract the objects and categories contained within the profile.

Figure 9: Overview of the parts on the navigation pane tree

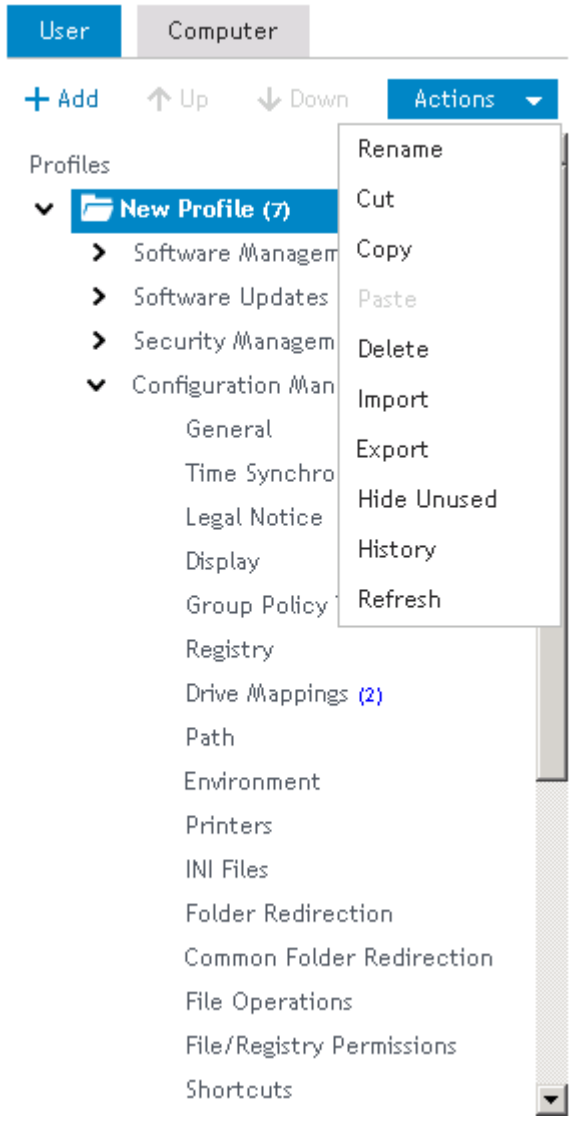


Within each part of the Profile tree, if there are elements within it (Profile, Category, Object) the number of total elements will be displayed within parentheses. Passing the cursor on top of the profile, category or object will display a tooltip with more information about the number of active and inactive elements within the section.

Profile actions

Profiles can be maintained by selecting an action from the Actions drop box. Click Add to create a new Profile. Prior to selecting an action, select either the Computer or User tab and then select either the Profile root or a specific profile to modify.

Figure 10: Select an action from the Actions list



Add

Select **Add** to create a new profile. The newly added profile will be added to the point in the tree that is highlighted. Select the Profiles root to add a new parent profile. Select an existing profile before the Add to make a new child profile.

Every newly created Parent or Child profile is automatically assigned a Profile Admin Role by default. The Profile Admin role by default has full access to Add, Change and Delete elements in all Profile objects as well as the ability to add, change and delete profiles.

Rename

Select **Rename** to modify the currently selected profile's name.

Delete

Select **Delete** to remove the currently selected profile. If the profile to be deleted contains any children, the child profiles will also be removed. Upon deletion, a confirmation dialog is presented, if selected in **Preferences > Confirmations**.

Select **Delete**, **Export and delete** or **Cancel** to continue the delete procedure. The Export and delete option will save the profile to a file in a user selected location. The profile could be imported at a later time using the **Import** action on the Profile Actions menu.

> ⓘ Note: History cannot undo the deletion of a profile. Please confirm the deletion of the profile before performing the action.

Cut/Copy/Paste

Profiles may be managed by using the standard Windows Cut/Copy/Paste actions to maneuver them into child profiles or parent profiles. Drag and Drop actions may also be used for this purpose.

Import

Profiles can be imported for the use of restoring a previously exported profile, or for importing it into another Desktop Authority Manager.

Export

Profiles can be exported for the use of a backup, or for importing it into another Desktop Authority Manager. The Export option copies the selected profile's configurations (profile.slc, profile.sld and profile.slp) to a selected location.

> ⓘ Note: When exporting profiles using Internet Explorer 9 with Enhanced security turned on, the *Do not save encrypted pages to disk* setting must be turned off in order for the file to be downloaded and saved.
> IE Enhanced security automatically turns this option on. Since Desktop Authority requires secure pages (https), the files cannot be saved while this option is turned on.

Hide/Show Unused

This option will Show or Hide unused profile elements. This action affects all profiles (parent and children).

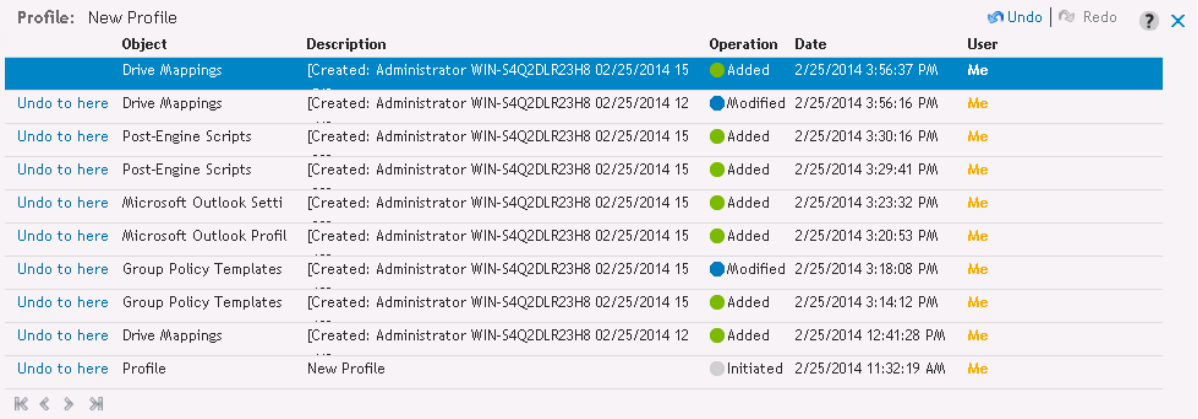
Move up/Move down

Profiles will be evaluated on a client in the order they appear in the Navigation tree. This order can be modified by using the Move Up and Move Down buttons. To move a profile, you must first select it, by clicking on it. Once it is selected (it will be highlighted), press the Move Up or Move Down button based on which way you want to move the profile.

History

The Desktop Authority Manager keeps track of actions taken during the current session with Desktop Authority.

Figure 11: Example History window



Click **History** to see the actions that have taken place. Click **Undo** to go back to a specific action or **Redo** to repeat and action that was previously Undone.

Operations may be undone by any user, regardless of who originally executed the action, as long as the user has the permission to perform the specific operation. If the user attempts to undo an action to which he does not have permission to, the undo operation will stop at the point where the permission does not exist.

NOTE: History cannot undo the deletion of a profile. Please confirm the deletion of the profile before performing the action.

Refresh

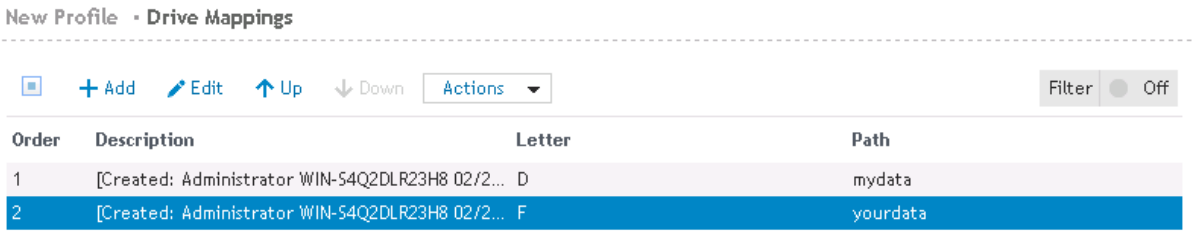
Update the Profile tree display.

Using and configuring profile objects

The View Pane for each object within a profile contains a list of the elements configured for the object.

Configuring elements

Figure 12: Configuring Profile elements

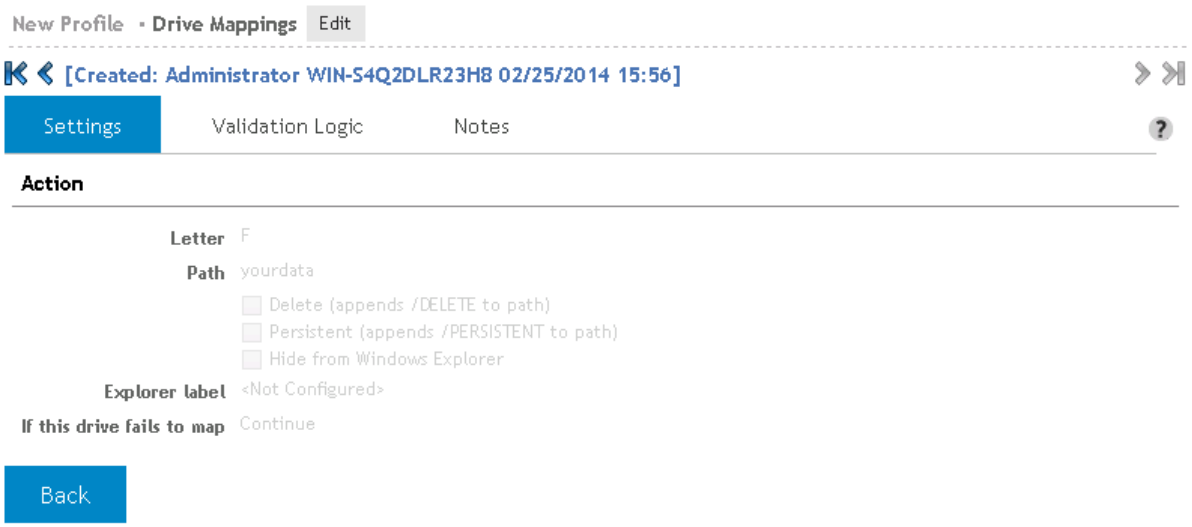


Read

Click Read to see the settings configured for the selected element. Edit the current element by clicking the **Edit** button.

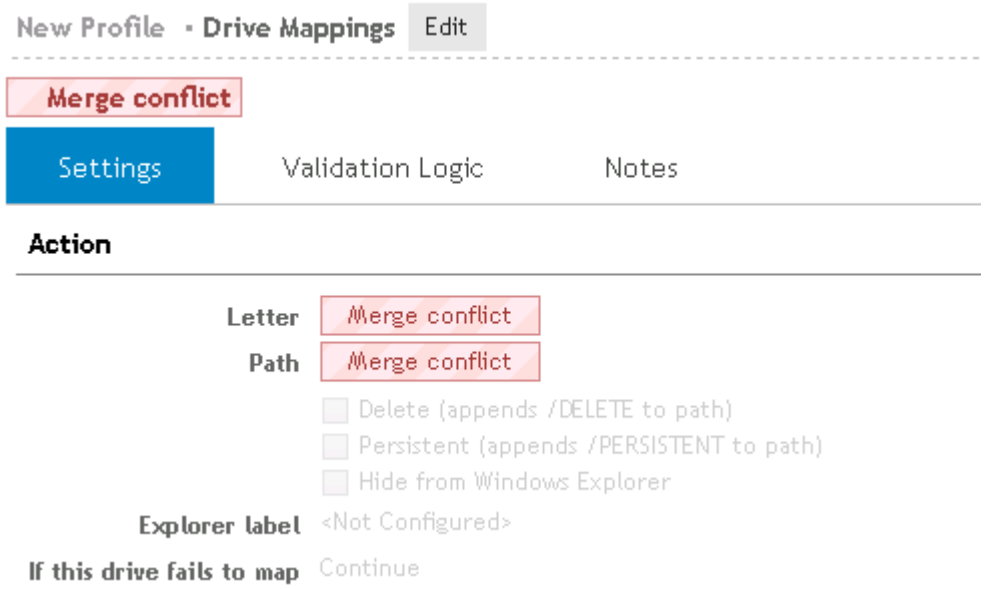
To the left and right of the element's description (above the tabs), click the arrow icons to move to the previous, next, first or last element configured for the profile object. Each element will be displayed in Read mode.

Figure 13: Profile element in read only mode



If multiple elements are selected, the fields that contain different data will display a red Merge Conflict warning. Click the Back button to return to the View pane.

Figure 14: Merge conflict warning



Add/Edit

Click Add to add a new element to the list or select one or more elements in the list and click Edit to modify. The Settings tab for the element will be displayed. Fill in the settings for the element and click Save to complete the element configuration.

ⓘ Note: Multiple elements may be modified at the same time. Any setting that appears in red denotes that the setting for that field differs among the selected elements.

Delete

Click Delete to remove a previously configured element from the object list.

Filter

The filter can be used to reduce the number of elements being displayed in the configuration list. One can use this to find a specific element in a large list of elements, analogous to finding a needle in a haystack. Another use might be to use it as a check to make sure all of the elements for a specific operating system are configured.

Column preferences

Click *Choose columns* to configure the display and order of the columns that are displayed in the element list.

Select the columns that should display in the list. When highlighted, a column can be moved up or down in the list by clicking the up and down arrow icons.

Click **Apply** to save the changes. Click **Default** to set the element list display back to its default settings.

Cut/Copy/Paste elements

Elements in the configuration list can be copied and pasted for duplication, or cut for removal from the list. Use the toolbar buttons above the list for these actions. Select the elements in the list prior to clicking the appropriate toolbar action. Multiple elements may be selected for these actions.

Changing the operation order of list elements

As Desktop Authority processes the configuration elements defined by the list, Validation Logic is applied to each element, beginning at the top of the list. Prioritize the list entries by clicking the Up/Down toolbar buttons to reorganize the list.

Multi-select box

The elements in the profile's list can be selected, edited and/or removed one at a time or several at one time. You can select more than one element in the list using the Shift or Ctrl key in combination with a mouse click. To select multiple elements, hold down the CTRL key while clicking the individual servers to select. Consecutive servers in the grid can be selected by clicking the first server to select and then, while holding down the SHIFT key, clicking the last server to select. To select the entire list of servers select the checkbox to the left of the column headers. This box will be empty if no elements are selected and will be filled with a square if some elements are selected. An element's selected status may be changed by clicking on it. If there is only one element in the list, it will always be selected.

Profile Tabs

Most often, the settings for an object consists of a Settings tab, Validation Logic tab, Description tab and a Notes tab.

Settings tab

The Settings tab contains the configurations options for the object. Some objects may contain other tabs which contain additional object settings.

Validation Logic tab

The Validation Logic tab contains the Validation settings for a configuration element.

The Validation Logic Rules list is not required to contain any rules. If no rules are specified, the element is automatically validated on the client based on the specified Class, Operating System, Connection Type and Timing.

Notes tab

The Notes tab provides an area to add any additional notes needed to document the use of the profile element.

Profile Configuration

Profiles have several configuration options. These include Validation Logic, Default Validation Logic, Default Timing, Permissions and Named Schedulers and are available as Tabs in the View Pane.

To modify any of the options on the profile configuration tabs, click on Edit. This will put the settings into edit mode with Save and Cancel at the bottom of the display. You must click either Save or Cancel to complete the edit.

Validation Logic

Validation Logic is used in conjunction with profiles to determine whether the configuration elements within a profile should be considered for processing on the client. Once the profile passes the validation test, each configuration element within the profile is processed. These entries are first verified by testing the validation logic defined for the entry. If the entry passes the validation logic test, it is executed on the client. If the validation logic for the profile does not meet the client specifications then no elements within the profile are processed.

It is important to keep in mind that not all configuration elements will be executed on a client just because a profile passes the validation logic test. This is due to the secondary validation logic provided for, on individual configuration element within the profile.

For detailed information about Validation Logic settings see the Validation Logic concepts help topic.

Only a Super User/Group has the ability to change the Validation Logic on a root level profile.

Default Validation Logic

Default Validation Logic is used to provide defaults to any new configuration element defined within the profile. Changing the Default Validation Logic for a profile will not change the validation logic defined for the profile or any existing configuration element.

For detailed information about Validation Logic settings see the Validation Logic concepts help topic.

Only a Super User/Group has the ability to change the Default Validation Logic on a root level profile.

Default Timing (available for Computer Management profiles only)

Default Timing is used to provide defaults to the timing tab for any new configuration element defined within Computer Management profiles. Changing the Default Timing for a profile will not change the Timing defined for the profile or any existing configuration element.

For detailed information about Timing settings see the Validation Logic Timing help topic.

Only a Super User/Group has the ability to change the Default Validation Logic on a root level profile.

Advanced

The Advanced tab contains specialized profile options.

Select the If this profile is validated during execution, do not process any subsequent profiles option, to stop processing all following profiles once this profile is validated and processed.

Keep in mind that profiles are process the order that they appear in the navigation pane. The order of the profiles may be rearranged by using any of the methods described in the Profile Management topic.

Only a Super User/Group has the ability to change the Advanced options on a root level profile.

Permissions

The Permissions tab is used to assign permissions to users by assigning a user to a role.

Roles are created from the Console Access Settings menu selection. Most often roles are established to represent a common job function that is performed by one or more employees. A role defines the functions that a member of the role will be able to perform.

For more detail on using Role Based Administration, see Role Based Administration Overview.
To update the members of a role, select the Role from the Roles list. Click Add Member or Delete Member to update the Members list.

Only a Super User/Group has the ability to change the Permissions on a root level profile.

Named Schedules (available for Computer Management profiles only)

The Named Schedules tab is used to create, modify or delete saved schedules. A Schedule is used as a Timing option. When applied to an element, it allows the element to be executed at a specified cycle and time period. Click Add, Delete or highlight a schedule to update.

A Schedule can be added to any Computer Management Profile element within the profile it was created in. Schedules are inherited by children profiles. Schedules created in one parent profile are not available in any other profile that is not related to the one it is created in.

Schedules can also be created within an element's Timing options window by choosing the Scheduled timing option on the element's timing tab.

Validation Logic

What is Validation Logic?

In order for the profiles and configuration elements to be processed for users or computers, Desktop Authority must qualify whether a setting should be applied to the client. To do this, a set of rules is created for every profile and configuration element within the Manager. This set of rules, which includes the definition of connection types, class types, operating systems and many other types, is called Validation Logic.

During the logon/logoff, startup/shutdown, refresh, or custom schedules, the Validation Logic of each profile is inspected. If the Validation Logic matches the client environment, the profile is marked for processing. Once each profile's Validation Logic is evaluated, the Validation Logic for all configuration elements in the marked profiles is evaluated. When complete, the resulting qualified configuration elements are executed on the client in the following order.

User Management Validation Logic includes settings for different Validation types, classes, operating systems, connection types, timing, virtualization, platform and network connection options.

Computer Management Validation Logic includes settings for different Validation types, classes, operating systems, timing, virtualization, architecture and network connection options.

It is important to keep in mind that not all configuration elements will be executed on a client just because its profile passes the validation test. This is due to the secondary validation logic that is provided on individual configuration elements. If a configuration element has no validation logic rules defined and its profile passes the validation test, the configuration element will automatically be processed on the client.

Use the boxes on the Validation Logic and Validation Logic Rules pages to define the specific rules, classes, operating systems and connection types (not applicable to Computer Management objects), timing (timing is on a separate tab for the Computer Management objects), virtualization, platform and network connection that the rules will apply to.

When the Validation Logic Rules list includes more than one rule, Boolean logic is used between each of the rules to obtain a result. Select either the AND or OR option below the validation logic rules list. The selected logic will apply to all rules defined in the list.

Disable this element regardless of validation

Select this check box to temporarily disable the selected configuration element from executing. Clearing the box will re-enable the configuration setting.

Operating system

7

Check this box to execute an element if the computer is running the Windows 7 operating system.

8.1

Check this box to execute an element if the computer is running the Windows 8.1 operating system.

10

Check this box to execute an element if the computer is running the Windows 10 operating system.

2008

Check this box to execute an element if the computer is running the Windows 2008 operating system.

2008 R2

Check this box to execute an element if the computer is running the Windows 2008 R2 operating system.

2012

Check this box to execute an element if the computer is running the Windows 2012 operating system.

2012 R2

Check this box to execute an element if the computer is running the Windows 2012 R2 operating system.

2016

Check this box to execute an element if the computer is running the Windows 2016 operating system.

2019

Check this box to execute an element if the computer is running the Windows 2019 operating system.

Connection type (User Management only)

LAN

Check this box to execute a script element if the computer is directly connected to the network.

Dial-up

Check this box to execute a script element if the computer is connected to the network via a dial-up connection. A dial-up connection includes RAS and VPN connections, provided the client used a dial-up networking session to make the connection.

To disable a specific script element from being processed, clear the Dial-up and LAN connection types. You will be warned that the entry will not execute without at least one of the connection types selected. The entry will appear in gray text to illustrate it has been disabled.

Class

Desktop*

Use the **Desktop** validation to execute a configuration element on all workstations determined to be a desktop computer.

Portable*

Use the **Portable** validation logic to execute a configuration element on all devices determined to be a portable device.

Tablet PC

Use the **Tablet PC** validation logic to execute a configuration element on a Tablet PC.

Embedded

Use the **Embedded** validation logic to execute a configuration element on a client with an embedded operating system.

Member Server

Use the **Member Server** validation logic to execute a configuration element on all member servers logging onto the network. A member server is any server on the network that does not authenticate logon requests.

Domain Controller

Use the **Domain Controller** validation logic to execute a configuration element on all computers that are considered to be a Domain Controller (PDC, BDC, or otherwise). A Domain Controller is any computer that has the ability to authenticate logon requests.

> ⓘ Note: A complex rule set is used to distinguish the class of a computer. This rule set involves the determination of CPU types, batteries and PCMCIA drivers. The methods used to determine the class of a computer is not foolproof.

Timing

Common (User/Computer)

Shut down

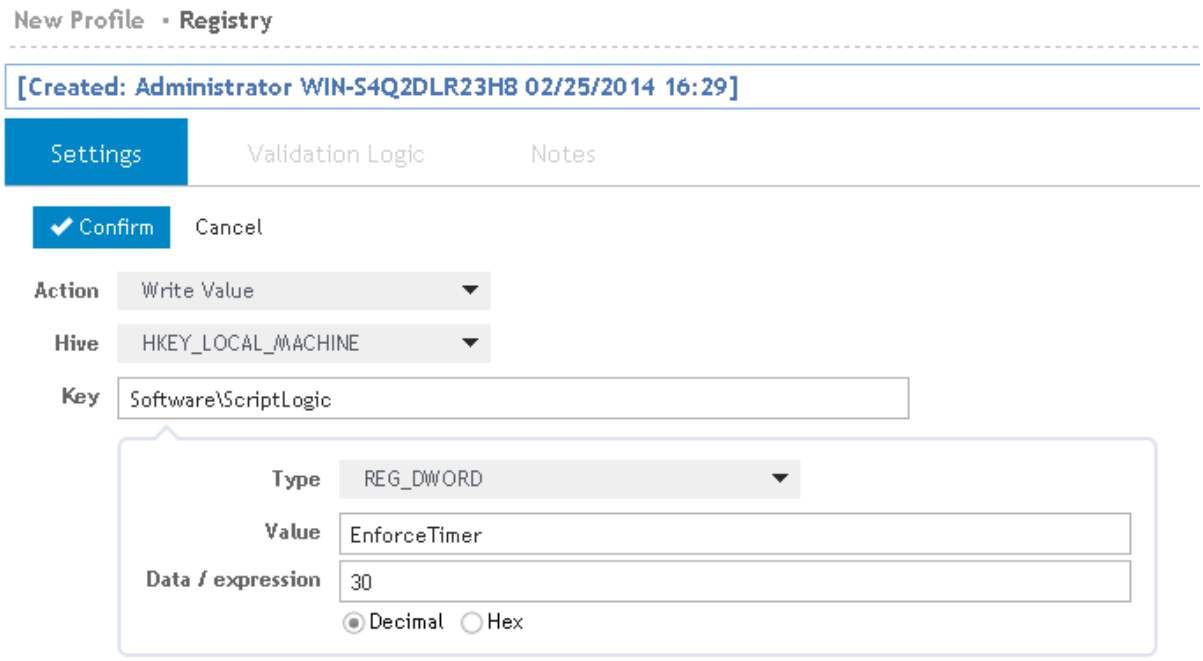
Check this box to execute an element when a client computer is shut down.

Refresh - User Management

Check this box to execute an element at a defined interval, following a client logon. The default refresh timer is set to every 60 minutes. The default refresh interval can be changed with the use of a registry setting. This can be automated by configuring a User Management Registry element. The User Management Refresh Timing interval is a separate timing interval from the Computer Management Refresh Timing interval.

To change this interval, create a new User Management Registry element. The interval is defined by specifying the number of minutes. The default value is 60. Entering 0 will disable the Refresh.

Figure 15: Optionally change Computer/User Timing value via Registry key



Refresh - Computer Management

Check this box to execute an element at a defined interval, following a client logon. The default refresh timer is set to every 60 minutes. The Computer Management Refresh Timing interval is a separate timing interval from the User Management Refresh Timing interval.

The Computer Management Refresh Timing interval can be changed using Computer Management Definitions. This can be access by going to Global Options > Computer Management Options > Definitions.

Within either the Global or Machine definitions section, click **Edit** and then **Add** to create a new definition. From the Name droplist, select Event_Refresh_Time and set the variable to the desired number of minutes. Refer to Computer Management Definitions for further detail about the various definitions that can be set.

User Management

Logon

Check this box to execute an element when a client logs on to the computer. The element will execute during the logon process.

The Logon timing event will be disabled if the parent profile does not have the Logon timing event box selected. This will make the Logon event unavailable for execution at logon.

Desktop

Check this box to execute an element when a client logs on to the computer. The element will execute after the logon process completes.

Logoff

Check this box to execute an element when a client logs off the computer.

The Logoff timing event will be disabled if the parent profile does not have the Logoff timing event box selected. This will make the Logoff event unavailable for execution at logoff.

At logoff, an optional progress bar can be displayed to let the user know that logoff operations are executing. The progress bar state can be set on the Global Options > Visual tab.

Computer Management

Startup

Check this box to execute an element when a client computer is started.

Scheduled

Scheduled timing allows a Computer Management element to be executed at a particular time or period. Check this box to execute an element, once, daily, weekly, or monthly at a specified timeframe.

Schedule options

Schedule Type

Select to use a Custom or Named schedule for this element. A Custom schedule allows the timing specifics to be specified by selecting a Cycle, Time and/or Date. A Custom schedule can be saved as a Named schedule for reuse with other elements. A Named schedule is simply a custom schedule that was previously created and saved.

Cycle

Select a time interval for which the element will execute. Choose from *Once*, *Daily*, *Weekly* or *Monthly*.

- Selecting *Once* as the cycle, will cause the element to be executed a single time on the specified time and date.
- Selecting *Daily* as the cycle, allows the element to execute at the specified time, each day. Configure the selected days to Everyday, Weekdays, Selected Days (select the specific days of the week) and Every Number of Days (execute this element every xx day(s)). The number of days is configured when Every number of days is selected.
- Selecting *Weekly* as the cycle allows the choice to execute the element on one or more days in the week, as well as the option to execute the element every xx weeks.
- Selecting *Monthly* as the cycle allows the selection of the month(s) to execute the element on, as well as the time, and day of week or month.

Advanced options

Do not execute if element has executed within the last xx hours

If a computer is not available at the time a scheduled event occurs, select this option to allow the event to execute for the computer if the event has last been executed within the specified number of hours.

If computer is unavailable at the scheduled time, run as soon as the computer becomes available

Select this box to execute the scheduled event for a computer that has missed a previously scheduled event. The event will be executed when the computer comes back online.

UID

The UID entry is used to make each scheduled element, a unique item. The data in this entry is automatically generated and should not be modified. However, if a scheduled element in the list is set to run only once and must be executed a second time, the UID can be changed by clicking **Generate New**.

Save as Named Schedule

Click this button to save the Scheduled Settings for use on other elements within the profile and its children.

> ⓘ Note: Each timing event is not necessarily available for all objects. Only the available timing events for each object will be enabled in the Timing validation box. Timing is not an available option for the Time Synchronization, Inactivity, and Mail Profile objects.

Validation Logic Architecture

Select Platform Type to enable validation checking based on the Operating System platform, **x32** or **x64** operating system. If the computer is running an operating system platform that matches one of the platforms selected, the configuration element will be processed.

Validation Logic Virtualization

Select Virtual Environment in order to execute a configuration element for the specific computer regardless of the user that logs onto the computer.

Non-virtual machines

Select **Non-virtual machines** to enable validation checking for all computers that are not considered to be virtual.

VMWare

Select **VMWare** to enable validation checking for a VMWare virtual machine. If the computer is running a VMWare session at the time of logon, the configuration element will be processed. The VMWare virtualization setting includes all VMWare platforms.

Microsoft Virtualization

Select **Microsoft Virtualization** to enable validation checking for Virtual PC, Virtual Server and Hyper-V virtual machines. If the computer is running a Microsoft virtual session at the time of logon, the configuration element will be processed. The Microsoft Virtualization setting includes all Microsoft Virtual servers and PC platforms.

Citrix Xen

Select **Citrix Xen** to enable validation checking for a Xen virtual solution. If the computer is running a Xen session at the time of logon, the configuration element will be processed. The Citrix Xen virtualization setting includes all Citrix Xen platforms.

Network Connection

Select a Network Connection type to enable validation checking based on the current connection to the network, **On-Network** or **Off-Network**. If the Network connection of the computer matches one of the connection types selected, the configuration element will be processed.

Desktop Authority can manage the computer and user's session when they are not connected to the corporate network. As an example, think of a laptop that is connected to the network at the office but when being used remotely it is disconnected from the company network. In this case the computer, when used remotely, would be considered Off-Network.

Select **On-Network** to validate when the computer is connected to the corporate network, because it is located physically in the corporate building or facility, or through a VPN. This means that the domain controller is reachable and therefore Windows Domain and Active Directory services are available.

Select **Off-Network** to validate when the computer is connected to a private or public network with internet access but the corporate environment is not available, i.e. the domain controllers are not pingable and Active Directory services, and network shares are not available.

It is assumed that a Desktop Authority managed computer has run Desktop Authority at least once while connected to the network, thus it has installed the client side files.

Off-Network support is configured on the **Deployment Settings >** **Off-Network Support** page.

The ability to execute elements Off-Network is not supported on with all profile objects. Therefore, the Network Connection Validation Logic section will only be visible for objects where Off-Network execution is supported.

Below is the list of objects that support Off-Network Execution:

Computer Management

- Application Launcher
- Data Collection
- Local Account Management
- MSI Packages
- Registry

User Management

- Application Launcher
- Pre-Engine Scripts
- Post-Engine Scripts
- General
- Legal Notice
- Display
- USB/Port Security
- Security Policies
- Group Policy Templates
- Registry
- Path
- Environment

- Application Launcher
- MSI Packages
- INI Files
- File Operations
- File/Registry Permissions
- Shortcuts
- Microsoft Office Settings
- Web Browser
- Microsoft Outlook Profiles
- Microsoft Outlook Settings
- OneDrive
- Inactivity
- Windows Firewall
- Power Schemes
- Message Boxes
- Data Collection

Validation type

Validation rules are created by selecting any of the various validation types along with providing a validation value. Together the validation type and value make a validation rule. Multiple validation rules can be added to the validation rule list. Press the Add button to add a new validation rule. Press the Modify button to change an existing validation rule. Press the Delete button to remove a validation rule from the list.

Validation rules support the asterisk (*) and question mark (?) wildcards in the validation value. This provides the ability to configure a setting for multiple instances of the selected Type. Use an asterisk to substitute a string of characters of any length. Use a question mark (?) to substitute a single character. One or more instances of each wildcard may be used in the comparison value.

Validation Logic rules use Boolean logic (AND or OR) to tie each rule together. Either AND or OR may be used on a set of validation rules, however, AND and OR may not be used together in the same validation rules list. Each validation rule may also use a Boolean NOT to negate the rule. Using a Boolean NOT in a rule will automatically use a Boolean AND to evaluate the combination of rules.

Validation Types are broken up into three sections in order to highlight the differences between User and Computer Management as well as the similarities.

Common Validation Logic Types include the available validation logic options for both User and Computer Management.

User Management Validation Logic Types lists the available validation logic options for User Management.

Computer Management Validation Logic Types lists the available validation logic options for Computer Management.

Common Management Validation Logic type

The following Validation Logic Types are available for use with Computer Management and User Management Profiles and Profile objects. Some Validation Logic Types allow the use of the * and ? wildcards.

The asterisk (*) wildcard means that at least one occurrence of the specified characters must exist in the entry field. When a profile or profile object element is being validated based on an entry field using the *, validation will return true and valid if the specified characters prior to the asterisk exist anywhere in the text field.

For example, if the specified Active Directory group is [*AC**], then any group that begins with AC, followed by any other characters will be valid for the validation.

The question mark (?) wildcard is used often used as a placeholder for unknown data. One or more ? may be used in a text field in conjunction with other characters. If the pattern of characters matches the field being validated, where a ? represents any other character, the validation will return true and valid.

For example, if a Computer Name is specified in the validation entry field as [*SHP??01*], then any computer with a name that starts with SHP and is then followed by any two characters plus 01. A computer name SHPAB10 would match and validate true for this example.

Network Membership

Computer Domain

> ⓘ Note: Validation Logic type allows use of wildcards.

Select Computer Domain to execute a configuration element for all computers that belong to the specified Domain. Find the Computer Domain Validation Logic type under the Network Membership category. In the Select Domain box, enter the name of the Domain. Optionally press the **Browse** button to locate the Domain. The supplied Computer Domain value is compared against the domain the client machine is a part of during the logon process and must match for the configuration element to be processed.

Examples:

BENE	Validates true for all computers in the BENE domain
BE*	Validates true for all computers in any domain beginning with the letters BE

Computer Group

> ⓘ Note: Validation Logic type does not allow the use of wildcards

Select Computer Group to execute a configuration element when the client computer is part of the specified Active Directory Group. Find the Computer Group Validation Logic type under the Network Membership category. In the Select Group box, enter the name of the Computer Group or press the **Browse** button to locate it. If the computer logging on is part of the supplied group, the configuration element and/or profile will be processed.

If *Include child groups* is selected, the configuration element will also execute when the client computer is in a group that is a member of the specified Active Directory Group. The domain must be configured with Windows 2008, Windows 2008 R2, Windows 2012, Windows 2012 R2, or Windows 2016 domain functional level.

Examples:

AdminGrp	Validates true for all computers in the AdminGrp.

OntarioGrp*	Validates true for any computer in the OntarioGrp including any nested groups of the OntarioGrp

OU (Computer)

Note: Validation Logic type allows use of wildcards

Select Organizational Unit (Computer) to execute a configuration element for all computers belonging to a specific OU. Find the OU (Computer) Validation Logic type under the Network Membership category. In the Select Organizational Unit box, enter the name of the OU or press the OU Browser button to locate it. The supplied OU value is compared against the OU the client machine is a part of during the logon process and must match for the configuration element to be processed.

Select the box **Include child OUs** to include all nested OUs of the selected parent in the validation logic rule.

Examples:

\Florida\Boca\Accounting	Validates true for any computer belonging to the \Florida\Boca\Accounting OU. Child OU's will be included if the "Include child OUs" box is selected.
OntarioGrp*	Validates true for any computer in the OntarioGrp including any nested OUs of the OntarioGrp
\Florida\Boca\Tech*	Validates true for any computers in any OU that begins with the letters Tech and also belong to the \Florida\Boca\ OU.

Site

Note: Validation Logic type allows use of wildcards

Select Site to execute a configuration element for all computers that belong to the specified Site. Find the Site Validation Logic type under the Network Membership category. In the Select Site box, enter the name of the Site. The supplied Site value is compared against the site the client machine is a part of during the logon process and must match for the configuration element to be processed.

Examples:

BENE	Validates true for any computer belonging to the BENE site.
BE*	Validates true for any computer in a site that begins with the letters BE.
ST??-01	Validates true for any computers in a site that begins with ST followed by any two characters and then a -01.

Computer Information

Computer Name

Note: Validation Logic type allows use of wildcards

Select Computer Name in order to execute a configuration element for a specific computer. Find the Computer Name Validation Logic type under the Computer Information category. In the Select Computer box, enter the Computer Name or press the **Browse** button to locate the computer name. The supplied Computer Name is

compared against the Computer Name of the client during the logon process and must match for the configuration element to be processed.

Examples:

PC221	Validates true for the desktop computer named PC221.
LAPTOP	Validates true for any desktop computer with LAPTOP in its name.
*221	Validates true for any desktop computer ending with 221 in its name.
PC*	Validates true for any desktop computer starting with PC as its name.
PC2??	Validates true for any desktop computer starting with PC2 in its name and is followed by two additional characters.
A??-PCxxx-ACCTG	Validates true for any desktop computer belonging to the ACCTG department, in building A, on any floor (??). This particular example denotes the granularity possible when used in conjunction with the corporate computer naming standards.

Host Address

Note: Validation Logic type allows use of wildcards

Select Host Address in order to execute a configuration element for the specific name. Find the Host Address Validation Logic type under the Computer Information category. In the Value box, enter the Host Address. The supplied Host Address is compared against the Host Address of the client during the logon process and must match for the configuration element to be processed.

The Host Address can identify a specific Host Address or a set of Host Addresses using wildcards.

For example, if a portion of the Host Address was used to distinguish between different office buildings, a wildcard can be used when validating the Host Address to deploy printers based upon in which building the computer is located.

Examples:

loc031-pc221.bldga.acme.com	Validates true for the specific computer whose Host Address is loc031-pc221.bldga.acme.com.
loc031-pc221.bldga.*	Validates true for the computer in building A, whose Host Address begins with loc031-pc221.bldga.
.bldga.	Validates true for any computers that are in Building A.
.bldga.acme.com	Validates true for any computers that are in Building A and part of the Domain Amoco

MAC Address

Note: Validation Logic type allows use of wildcards

Select MAC Address in order to execute a configuration element for a computer with a specific MAC Address. Find the MAC Address Validation Logic type under the Computer Information category. In the Value box, enter the MAC Address. The supplied MAC Address is compared against the MAC Address of the client during the logon process and must match for the configuration element to be processed.

This type of validation gives the ability to specify a specific computer on the network based on the MAC Address built in to the network adapter. This gives a simple way to address a specific machine regardless of the computer name (which is vulnerable to change). Validating on a MAC Address may also be useful if your network uses IPX/SPX as a protocol.

To determine the MAC Address for a computer's network adapter, run IPCONFIG /ALL. The MAC Address will be defined as the Physical Address for the network adapter.

Examples:

Mac Address	VL Mac Address Value
00-50-56-C0-00-10	005056C00010 (no hyphens)
00-50-56-*-*-*	Will validate for all MAC addresses that begin with 00-50-56

TCP/IP Address

Note: Validation Logic type allows use of wildcards

Select TCP/IP Address in order to execute a configuration element for the specific machine based on the TCP/IP address. Find the TCP/IP Address Validation Logic type under the Computer Information category. In the Value box, enter the TCP/IP address. The supplied TCP/IP address is compared against the TCP/IP address of the computer during the logon process and must match for the configuration element to be processed. The TCP/IP Address validation type will accept IPv4 and IPv6 addresses.

The asterisk (*) and question mark (?) wildcards may be used to match TCP/IP addresses. This wildcard technique and simplified string manipulation should be effective on most networks. Keep in mind that you are not required to specify complete octets. Specifying 192.168.1* would attempt to match the first two octets completely and the first character of the third octet to the client's TCP/IP address.

Examples:

192.168.100.5	Validates true for the computer whose TCP/IP address is 192.168.100.5.
192.168.100.*	Validates true for any computers whose TCP/IP address matches the first three octets.
192.168.*	Validates true for any computers whose TCP/IP address matches the first two octets.
192.168.1??.5	Validates true for any computers whose TCP/IP address matches 192.168.1xx.5, where xx is any number.
10::1	Validates true for the computer whose TCP/IP address is 10:0:0:0:0:0:0:1

True subnetting is supported in the TCP/IP Address value field. Use true subnetting values to selectively specify certain groups of IP addresses. Specify the IP address and subnet mask in the TCP/IP value entry. The subnet mask can be specified in either dotted decimal format or by specifying the number of mask bits.

Examples:

10.0.0.4/255.255.255.0	Validates true for the computers whose IP address is in the range or 10.0.0.1 - 10.0.0.254.
10.0.0.4/24	Validates true for the computers whose IP address is in the range or 10.0.0.1 - 10.0.0.254.

10.0.0.4/255.255.255.240	Validates true for the computers whose IP address is in the range or 10.0.0.1 - 10.0.0.14.
10.0.1.4/28	Validates true for the computers whose IP address is in the range or 10.0.1.1 - 10.0.1.14.
10.0.0.39/28	Validates true for the computers whose IP address is in the range or 10.0.0.33.

To determine the IP Address for a computer, run IPCONFIG.

File Exists

Note: Validation Logic type does not allow the use of wildcards

Select File Exists in order to execute a configuration element for a computer that has the existence of a specific file. Find the File Exists Validation Logic type under the Computer Information category.

In the Value box, enter the file name (including path) of the file to be checked. If the file exists in the path specified the configuration element will be processed.

File Version

Note: Validation Logic type does not allow the use of wildcards

Select File Version in order to execute a configuration element for a computer that has a specific file and version of that file (regardless of the user that logs on to the computer). Find the File Version Validation Logic type under the Computer Information category. The file's version information is normally embedded into the file and can be seen on the Version tab of the Properties for the file.

The File Version validation type requires three validation values to complete its configuration. The required values are File, Operator and Version. Enter the name of the file (including path) whose version will be compared against into the File box. Enter the comparison operator into the Operator box. Enter the comparison operator to be used in the compare operation. Enter the comparison value into the Version box.

The available compare operators for the Operator field are < (less than), <= (less than or equal to), <> (not equal to), = (equal to), > (greater than), >= (greater than or equal to).

The file's version is extracted and then compared against the information specified by the operator and comparison version. If the comparison (performed during the logon process) returns a TRUE result the configuration element will be processed.

Example:

File:	C:\Program Files\Microsoft Office\Office10\Winword.exe
Operator:	<=
Version:	10.0

If the version of the Winword.exe file is less than or equal to 10.0, the configuration element will be processed.

IPv4 Range

Note: Validation Logic type does not allow the use of wildcards

Select IPv4 Range in order to execute a configuration element for any computer with an IP address within the range specified. Find the IP Range Validation Logic type under the Computer Information category. In the Range boxes, enter the beginning and ending IP addresses. The supplied range of IP addresses is compared against the IP address of the computer during the logon process and must match for the configuration element to be processed.

Examples:

192.168.100.5 - 192.168.100.50	Validates true for the computer whose IP address is between 192.168.100.5 and 192.168.100.50, inclusive.

To determine the IP Address for a computer, run IPCONFIG.

IPv6 Range

> Note: Validation Logic type does not allow the use of wildcards

Select IPv6 Range in order to execute a configuration element for any computer with an IP address within the range specified. Find the IP Range Validation Logic type under the Computer Information category. In the Range boxes, enter the beginning and ending IP addresses. The supplied range of IP addresses is compared against the IP address of the computer during the logon process and must match for the configuration element to be processed.

Examples:

10::1 - 10::10	Validates true for the computer whose IP address is between 10:0:0:0:0:0:0:1 and 10:0:0:0:0:0:0:10, inclusive.

To determine the IP Address for a computer, run IPCONFIG.

Registry Key Exists

> Note: Validation Logic type does not allow the use of wildcards

Select Registry Key Exists in order to execute a configuration element for the specific computer if the specified Registry Key is found in the registry. Find the Registry Key Exists Validation Logic type under the Computer Information category.

In the Key box, enter the Registry Key name. If the Registry key exists, the configuration element will be processed.

Registry Value Exists

> Note: Validation Logic type does not allow the use of wildcards

Select Registry Value Exists in order to execute a configuration element for the specific computer if the specified Registry Key and Value is found in the registry. Find the Registry Value Exists Validation Logic type under the Computer Information category.

In the Key box, enter the Registry Key name. Enter the registry key value in the Value entry. If the Registry key and value combination exists the configuration element will be processed.

Registry Value

> Note: Validation Logic type does not allow the use of wildcards

Select Registry Value in order to execute a configuration element for a computer with a specific registry value. Find the Registry Value Validation Logic type under the Computer Information category.

The Registry Value validation type requires four validation values to complete its configuration. The required values are Key, Value, Operator and Data. Enter the registry hive and key to be checked into the Key box. Enter the name of the entry within the specified key to be checked into the Value box. Enter the operator to be used in the compare operation. Enter the data to be compared against into the Data box.

The available compare operators for the Operator field are < (less than), <= (less than or equal to), <> (not equal to), = (equal to), > (greater than), >= (greater than or equal to).

The supplied validation values (Value, Operator and Data) are used to form a condition that is applied to the specified Key. If the comparison (performed during the logon process) returns a TRUE result the configuration element will be processed.

Example:

Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX
Value:	Version
Operator:	<
Data:	9.0

If the installed version of DirectX is less than 9.0, the configuration element will be processed.

Virtual Environment

Select Virtual Environment in order to execute a configuration element on a client running a virtual environment. VMWare virtual machines are currently supported.

Select the VMWare virtual machine check box to execute a configuration element on a VMWare virtual environment.

Platform Type

Select Platform Type in order to execute a configuration element on a machine running a specific Operating System platform, **x32** or **x64** operating system. If the computer is running an operating system platform that matches one of the platforms selected, the configuration element will be processed.

Windows 10 Release ID

Select Windows 10 Release ID in order to execute a configuration element when a computer has or doesn't have a specific Release of Windows 10 installed..

In the Windows 10 Release ID column, select one or more Release Id's. If a Release ID is not specified, enter it into the Others box. Multiple Release ID's can be entered into the Others box delimited by commas.

User Management Validation Logic type

The following Validation Logic Types are available for use with User Management Profiles and Profile objects. Some Validation Logic Types allow the use of the * and ? wildcards.

The asterisk (*) wildcard means that at least one occurrence of the specified characters must exist in the entry field. When a profile or profile object element is being validated based on an entry field using the *, validation will return true and valid if the specified characters prior to the asterisk exist anywhere in the text field.

For example, if the specified Active Directory group is [*AC**], then any group that begins with AC, followed by any other characters will be valid for the validation.

The question mark (?) wildcard is used often used as a placeholder for unknown data. One or more ? may be used in a text field in conjunction with other characters. If the pattern of characters matches the field being validated, where a ? represents any other character, the validation will return true and valid.

For example, if a Computer Name is specified in the validation entry field as [*SHP??01*], then any computer with a name that starts with SHP and is then followed by any two characters plus 01. A computer name SHPAB10 would match and validate true for this example.

Network Membership

Authenticating Domain

> Note: Validation Logic type allows use of wildcards

Select Authenticating Domain to execute a configuration element for all computers that log on to the specified Domain. Find the Authenticating Domain Validation Logic type under the Network Membership category. In the Select Domain box, enter the name of the Domain. Optionally press the Resource Browser button to locate the Domain. The supplied Authenticating Domain value is compared against the domain the client machine is attempting to log on to and must match for the configuration element to be processed.

Examples:

BENE	Validates true for all computers authenticated in the BENE domain
BE*	Validates true for all computers authenticated in any domain beginning with the letters BE

OU (User)

> Note: Validation Logic type allows use of wildcards

Select Organizational Unit (User) to execute a configuration element for all users belonging to a specific OU. Find the OU (User) Validation Logic type under the Network Membership category. In the Select Organizational Unit box, enter the name of the OU or press the OU Browser button . The supplied OU value is compared against the OU the client machine is a part of during the logon process and must match for the configuration element to be processed.

Select the box Include child OUs to include all child OUs in the validation logic.

Examples:

\Florida\Boca\Accounting	Validates true for any computer belonging to the \Florida\Boca\Accounting OU. Child OU's will be included if the "Include child OUs" box is selected.
\Florida\Boca\Tech*	Validates true for any users in any OU that begins with the letters Tech and also belong to the \Florida\Boca\ OU.

Primary Group

> Note: Validation Logic type allows use of wildcards

Select Primary Group to execute a configuration element for all users of the specified Primary Group. Find the Primary Group Validation Logic type under the Network Membership category. In the Select Group box, enter the name of the Group or press the **Browse** button to locate it. The supplied Primary Group value is compared against the primary group of the user during the logon process and must match for the configuration element to be processed.

Example:

Sales	Validates true for all users that have Sales defined as their primary group
ST*	Validates true for all users that have a primary group of ST followed by any characters.

User Group

> Note: Validation Logic type does not allow the use of wildcards

Select User Group to execute a configuration element for all users belonging to a specific network group. Find the User Group Validation Logic type under the Network Membership category. In the Select Group box, enter the name of the Group or press the Resource Browser button to locate the group. The supplied group membership value is compared against the groups that the user is a part of during the logon process and must match for the configuration element to be processed.

Examples:

Marketing	Validates true for all users that are part of the Marketing group.
Sales	Validates true for all users that are part of the Sales group.
Marketing;Sales	Validates true for users of both the Marketing and Sales groups.
*	Validates true for all groups

User Group does not support the wildcards * (asterisk) and ? (question mark) with the exception of a single * meaning "all groups".

User Name

> Note: Validation Logic type allows use of wildcards

Select User Name to execute a configuration element for a specific User Name(s). Find the User Name Validation Logic type under the User Information category. In the Select User box, enter the name of the User(s) or press the **Browse** button. The supplied User Name value is compared against the User Name used during the logon process and must match for the configuration element to be processed.

Use the User Name validation type to execute a configuration element for a particular user regardless of the computer from which they log on to. For example, if the configuration element should execute any time Mary Jones (user name mjones) logs into the network, specify mjones as the user name.

Examples:

mjones	Validates true for user mjones only.
mjones; tsmith	Validates true for user mjones and tsmith.
*	Validates true for all users.

Timing and Events

Frequency

Note: Validation Logic type does not allow the use of wildcards

Select Frequency to validate a configuration element for users based on the specified timing. Find the Frequency Validation Logic type under the Timing and Events category. The specified Cycle and/or Frequency values are compared against the user, computer and UID. If the timing and UID conditions match, the configuration element will be processed.

UID

The UID entry is used to make each element that uses a Frequency Validation Logic type, a unique item, regardless of its configurations. This is helpful when the Frequency is set to Once Per Day or One Time. The data in the UID entry is automatically generated and should not be modified. However, if there is an element that is set to execute Once Per Day or One Time, and if it must execute a second time, the UID can manually be changed by clicking Generate New.

Frequency

Select a logon frequency from the list. Select from Every Time, Once Per Day (User), Once Per Day (Computer), One Time (User) and One Time (Computer).

Select a logon frequency from the list. Select from Every Time, Once Per Day (User) and One Time (User).

Every time is used to validate an element at the specified cycle, each time.

Select Once Per Day (User) to validate an element at the specified cycle, one time per day for the current user.

Select Once Per Day (Computer) to validate an element at the specified cycle, one time per day for the computer.

Select One Time (User) to validate an element at the specified cycle, a single time for the current user.

Select One Time (Computer) to validate an element at the specified cycle, a single time for the computer.

Cycle

Select a time interval for which the element will validate. Choose from Every time, Day of Week, Monthly (Day of Week), Monthly (Day of Month) and Specific Date

Selecting Every time as the cycle, will force the element to validate each day at the specified frequency.

Selecting Day of Week as the cycle, presents a new list allowing the selection of a day from Sunday to Saturday.

Selecting Monthly (Day of Week) as the cycle, presents a new list allowing the selection of a day in the month ranging from 1st Sunday, 1st Monday, ... to the last Saturday of the month.

Selecting Monthly (Day of Month) as the cycle, presents a new list allowing the selection of a date within the month.

Selecting Specific Date Range as the cycle presents a start date and end date in which the date range should be entered. Click the calendar icon to make your date selection from a popup calendar.

Time Range

Select Time Range to execute a configuration element if the current time is within the Time Range specified. Find the Time Range Validation Logic type under the Timing and Events category. Enter the beginning of the time range in the first box and the ending time range in the second box. The current time is compared to the time range values and must fall into the range for the configuration element to be processed.

Terminal Services

TS Application Name

> Note: Validation Logic type allows use of wildcards

Select TS Application Name in order to execute a configuration element based on the name of the Terminal Server (TS) published application that is currently in use. Find the TS Application Name Validation Logic type under the Terminal Services category. In the Value box, enter the TS Application Name. The supplied TS Application Name is compared against the running applications during the logon process and must be found for the configuration element to be processed.

Examples:

Outlook	Validates true for the published application Outlook
Outlook*	Validates true for any published application starting with the name Outlook. This may be used for different versions of the application.

Some Citrix environments precede the published application name with a # symbol. For example, if the application name is published as Outlook, the name on the client side may be represented as #Outlook. Therefore, the Validation Logic must be set to #Outlook (in this instance) for the element to validate properly.

#Outlook*	Validates true for any published application starting with the name Outlook. This may be used for different versions of the application.

To determine the actual published application name that is being used on the client, review the sltrace.htm log file.

NOTE: A value will not be returned for the Terminal Service Application Name on a Windows 2008/2008 R2/2012/2016/2019 server using RemoteApp. It will work, however, if Citrix Xen Server is installed on the 2012 server.

TS Client Name

> Note: Validation Logic type allows use of wildcards

Select TS Client Name in order to execute a configuration element based on the name of the TS Client. Find the TS Client Name Validation Logic type under the Terminal Services category. In the Value box, enter the TS Client Name. If the supplied name matches the name of the client logging onto the Terminal Server the configuration element is processed.

Examples:

PC221	Validates true for the client named PC221.
LAPTOP	Validates true for any client with LAPTOP in its name.
*221	Validates true for any client ending with 221 in its name.
PC*	Validates true for any client starting with PC as its name.
PC2??	Validates true for any client starting with PC2 in its name and is followed by two additional characters.

A??-PCxxx-ACCTG	Validates true for any client belonging to the ACCTG department, in building A, on any floor (??). This particular example denotes the granularity possible when used in conjunction with the corporate computer naming standards.

TS Client TCP/IP Address

Note: Validation Logic type allows use of wildcards

Select TS Client TCP/IP Address in order to execute a configuration element based on the IP Address of the client connecting to the Terminal Server (TS). Find the TS Client TCP/IP Address Validation Logic type under the Terminal Services category. Specify the TS Client TCP/IP Address by entering it into the Value entry. If both IP Addresses match the configuration element will be processed.

The asterisk (*) and question mark (?) wildcards may be used to match TCP/IP addresses. This wildcard technique and simplified string manipulation should be effective on most networks. Keep in mind that you are not required to specify complete octets. Specifying 192.168.1* would attempt to match the first two octets completely and the first character of the third octet to the client's TCP/IP address.

Examples:

192.168.100.5	Validates true for the client computer whose TCP/IP address is 192.168.100.5.
192.168.100.*	Validates true for any client computers whose TCP/IP address matches the first three octets.
192.168.*	Validates true for any client computers whose TCP/IP address matches the first two octets.
192.168.1??.5	Validates true for any client computers whose TCP/IP address matches 192.168.1xx.5, where xx is any number.
10::1	Validates true for the client computer whose TCP/IP address is 10:0:0:0:0:0:0:1.

True subnetting is supported. Use true subnetting values to selectively specify certain groups of IP addresses. Specify the IP address and subnet mask in the TCP/IP in the Value entry. The subnet mask can be specified in either dotted decimal format or by specifying the number of mask bits.

Examples:

10.0.0.4/255.255.255.0	Validates true for the client computers whose IP address is in the range of 10.0.0.1 - 10.0.0.254.
10.0.0.4/24	Validates true for the client computers whose IP address is in the range of 10.0.0.1 - 10.0.0.254.
10.0.0.4/255.255.255.240	Validates true for the client computers whose IP address is in the range of 10.0.0.1 - 10.0.0.14.
10.0.1.4/28	Validates true for the client computers whose IP address is in the range of 10.0.1.1 - 10.0.1.14.
10.0.0.39/28	Validates true for the client computers whose IP address is in the range of 10.0.0.33.

To determine the IP Address for a computer, run IPCONFIG.

TS Initial Program

Note: Validation Logic type allows use of wildcards

Select TS Initial Program in order to execute a configuration element based on the name of the Terminal Server (TS) Initial Program currently in use. Find the TS Initial Program Validation Logic type under the Terminal Services category. In the Value box, enter the TS Initial Program name. If the supplied TS Initial Program is running during the logon process, the configuration element is processed.

Examples:

appver71.exe	Validates true for the initial program appver71.exe only.
appver7?.exe	Validates true for any initial program name beginning with the characters appver7 followed by a single character and an .exe extension.

TS Session Name

Note: Validation Logic type allows use of wildcards

Select TS Session Name in order to execute a configuration element based on the connection name that is in use between the client and the Terminal Server (TS). The TS Session Name is made up of a combination of the Terminal Server Connection Name#Session Id. Find the TS Session Name Validation Logic type under the Terminal Services category. In the Value box, enter the TS Session Name. If a connection occurs on the supplied session, the configuration element will be processed.

Examples:

RDP-TCP#1	Validates true for the RDP-TCP#1 session.
RDP-TCP*	Validates true for any RDP-TCP session.
ICA-TCP*	Validates true for any ICA-TCP session.

Custom Validation

Custom Function

Note: Validation Logic type does not allow the use of wildcards

Select Custom Function in order to execute a configuration element based on the return value of the function. Find the Custom Function Validation Logic type under the Custom Validation category. Custom functions are defined in the Profile's Definitions tab. All custom functions must return a TRUE or FALSE value. Specify the Custom Variable by entering it into the Value entry. If the custom function returns TRUE (or any value other than 0), the configuration element will be processed. A FALSE return value will cause the configuration element to be unprocessed.

Example:

The function below is used to determine if the specified version ($version) of DirectX is greater, equal or less than ($operand) the currently installed version of DirectX. The function returns a value ($DXVersion) based on the parameters passed to the function. This function is defined in the Profile's Definitions tab.

```
; Custom Script File
; File Name: SLP00001.sld
; Description: SLP00001.sld
```

```
;
;-------------------------------------------------------
function DXVersion($operand, $version)
if slVersionCompare(ReadValue
('SOFTWARE\Microsoft\Directx','Version'),$operand,$version)
$DXVersion = 1
else
$DXVersion = 0
endif
endfunction
;-------------------------------------------------------
RETURN ; Must be last line of file. Do not remove this line
```

To use this function within the Validation Logic, select Custom Function from the Validation Logic dialog box. Specify the function name and parameters (if necessary) in the Value entry. In this example, an operand of '<' (less than) and a version of 7.0 is passed to the function. This is compared to the version of DirectX on the workstation. The return value is set accordingly. If the version of DirectX on the workstation is less than 7.0 than the script entry will be processed.

Desktop Authority provides no error control over custom functions. A syntax error in your custom function will cause Desktop Authority to unexpectedly terminate.

Custom Variable

> Note: Validation Logic type does not allow the use of wildcards

Select Custom Variable in order to execute a configuration element based on the value of the defined variable. Find the Custom Variable Validation Logic type under the Custom Validation category. Custom variables are defined in the profile's Definitions tab. All custom variables must evaluate to a TRUE or FALSE value. Specify the Custom Variable by entering it into the Value field. If the custom variable equals to TRUE (or any value other than 0), the configuration element will be processed. A FALSE value will cause the configuration element not to be processed.

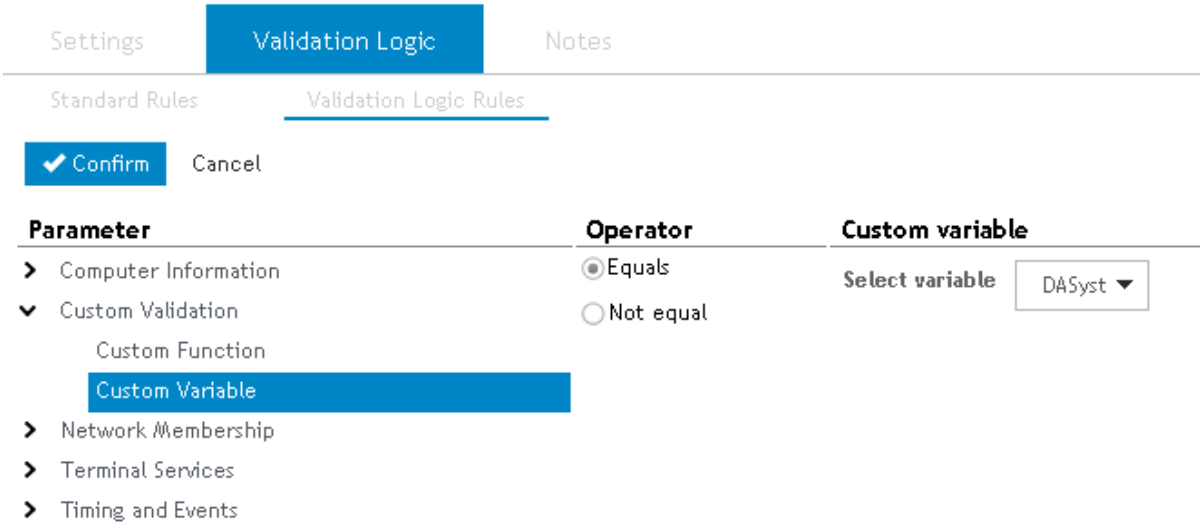
Example:

The value of the variable below ($DASystemTray) is evaluated with the code below. This variable is defined in the Profile's Definitions tab.

```
; Custom Script File
; File Name: SLP00001.sld
; Description: SLP00001.sld
;
;-------------------------------------------------------
$DASystemTray = ReadValue($DAKeyLM+'\v5\GUI\','EnableSystemTray')
;-------------------------------------------------------
RETURN ; Must be last line of file. Do not remove this line
```

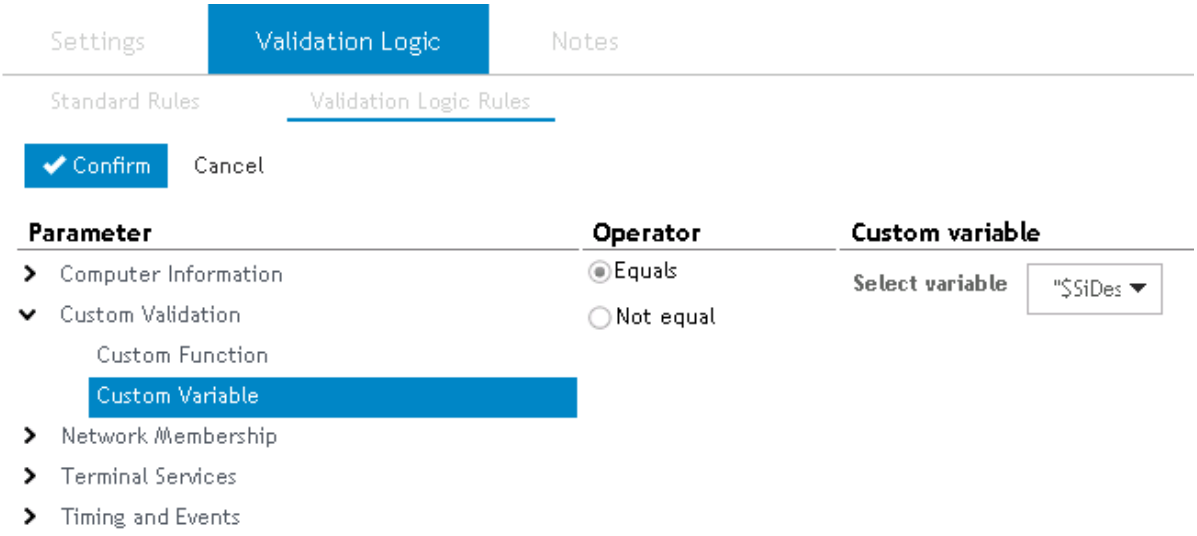
To use this variable within Validation Logic, select Custom Variable from the Validation Logic dialog box. Specify the variable name in the Value entry. In this example, the registry key can either equal a 1 or 0. When the registry key is read, the value is stored in the $DASystemTray variable. If the value of the variable is True (or any other non-zero value), the script element will be processed.

Figure 16: Using a custom variable within Validation Logic



If the variable does not result in a Boolean value and will be used as comparison to a string, the variable must be wrapped within quotes. In the following example, $SiDesktopSize, the variable results in the size of the computer desktop as a string. For example, "1024x768". This variable is expressed within quotes and compared to a string (within quotes) in the Validation Logic dialog.

Figure 17: Example of custom variable



Desktop Authority provides no error control over custom variables. A syntax error in your custom variable will cause Desktop Authority to unexpectedly terminate.

Computer Management Validation Logic type

The following Validation Logic Types are available for use with Computer Management Profiles and Profile objects. Some Validation Logic Types allow the use of the * and ? wildcards.

The asterisk (*) wildcard means that at least one occurrence of the specified characters must exist in the entry field. When a profile or profile object element is being validated based on an entry field using the *, validation will return true and valid if the specified characters prior to the asterisk exist anywhere in the text field.

For example, if the specified Active Directory group is [*AC**], then any group that begins with AC, followed by any other characters will be valid for the validation.

The question mark (?) wildcard is used often used as a placeholder for unknown data. One or more ? may be used in a text field in conjunction with other characters. If the pattern of characters matches the field being validated, where a ? represents any other character, the validation will return true and valid.

For example, if a Computer Name is specified in the validation entry field as [*SHP??01*], then any computer with a name that starts with SHP and is then followed by any two characters plus 01. A computer name SHPAB10 would match and validate true for this example.

Activity

Interactive User

> ⓘ Note: Validation Logic type does not allow the use of wildcards

The interactive user is the user that is logged on to the computer, i.e., the user who is physically at the computer. The Interactive User Validation Logic type allows an element to execute based on whether there is a user logged in to the computer or not. Find the Interactive User Validation Logic type under the Activity category.

Along with Interactive User, there is a Desktop Locked checkbox. This checkbox allows the validation logic to determine not only whether a user is logged on to the machine but if the machine is in a locked state or not.

Console Access Settings

What are Console Access Settings?

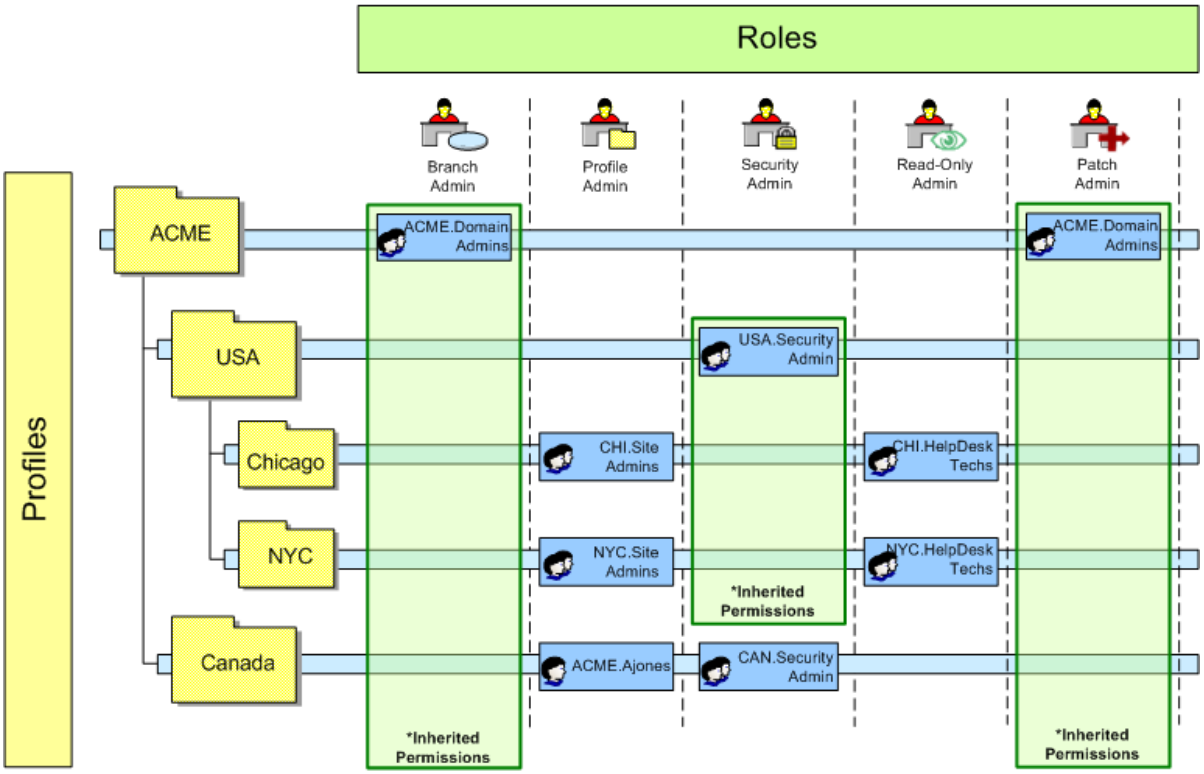
Console Access Settings implement the Desktop Authority's Role Based Administration (RBA) functionality which restricts access to profiles and the configuration elements contained within them. Access to profiles is limited to users and groups that have been granted specific permissions to them. Console Access settings can also limit Global System functionality to specific users.

Console Access Settings is comprised of maintaining System Roles, Super Users and Profile Roles.

A System Role is a container that defines permissions to specific parts of the Desktop Authority console.

A Profile Role is a container that defines the Permissions that are granted to any Member of that Role. A Role may be Global or Local. Global Roles are defined by the Super User and can be applied on any Profile in the system. Local Roles are defined per Profile and can be used to grant Permissions on a specific Profile and, optionally, its child Profiles. A Member is any user or group assigned to a Role. Members are assigned to Roles, Global and Local, at the Profile level. Even when a user or group is assigned to a Global Role, the membership applies at that Profile only. Resources are Profiles and Configuration Elements to which Permissions can be granted via Membership in a Role.

Figure 18: Example System roles



Permissions define the actions a member has to a specific resource. They are setup as part of the role creation process. Parent profiles define the base permissions and all child profiles inherit these permissions. Allowing for greater granularity, a child's inherited permissions may be altered at the child profile level.

Branch Admin

The ACME.Domain.Admins group is configured as a member of the Branch Admin role. This group is given permission to the ACME parent profile. The ACME.Domain.Admins group is also defined as a Super User/Group. This means the group will have unlimited access to all profiles and configuration elements, as well as global options, within the system. It is important to note that since this group is assigned permissions to the Branch Admin role at the parent profile level, these permissions are inherited on all child profiles within ACME Corporation. ACME.Domain.Admins also have unrestricted system access due to their Super User/Group status.

Profile Admin

The Profile Admin role is configured to have View, Change, Add/Delete permissions to all objects within a single branch of the profile tree. Child profiles are not included in the Profile Admin's permissions. The CHI.Site.Admins group are members of the Profile Admin role within the Chicago child profile only. The NYC.Site.Admins group are members of the Profile Admin role within the NYC child profile only. Note that user Ajones is assigned to the Profile Admin role within the CANADA profile.

Security Admin

The Security Admin role is assigned View, Change, Add/Delete permissions to several configuration objects within a profile. For instance, let's say the Security Admin is responsible for pushing out newly released service packs. The Security Admin role will be given permissions to the Registry, Application Launcher and Service Pack Deployment

objects. They will be given Deny access to all other configuration objects. Note in the illustrations above that the USA.Security.Admin group is assigned membership at the USA profile level. These permissions are inherited down to both the Chicago and NYC child profiles. The CAN.Security.Admin group is assigned membership to the Canada profile.

Read-Only Admin

The Read-Only Admin role is assigned View permissions only to all configuration objects within a profile. The Read-Only Admin role can be used for Users or Groups that will not have any ability to change elements within objects of a profile. In the illustration above, The NYC and CHI Helpdesk technicians are given the read-only permissions of the Read-Only Admin role. This way they can troubleshoot user issues and have an approved Administrator make the necessary changes to their profile. Note that the Canada profile does not have any User or Group assigned under the Read-Only Admin role. In this case, either the Branch Admin or Profile Admin have the necessary permissions to accomplish the same goal.

Super User management

What is a Super User?

A Super User is an attribute of a user or group that provides specialized system access. The Super User attribute is designed for privileged users who will have unrestricted access to the system. Regardless of the roles the users belong to, they will be able to view and update all objects in the system.

Default Super Users are added during the installation of Desktop Authority. Others may be added to the Super User list by an existing Super User.

To access the Super User Management dialog, select *Control Access Settings* from the menu bar and then *Super User Management* from the submenu.

Besides having full access to all profiles and objects, Super Users have other special system permissions.

Super Users can:

- create and manage Global Roles
- modify the Super Users list and attributes
- access all Global Options objects
- create, generate and schedule reports for delivery to other users/groups

Managing Super Users

To add a new user or group to the Super User list, click **Edit** to put the list in Edit mode. Then click **Add user** or select an existing user and click **Remove user**.

System roles

A System Role defines the areas of the Desktop Authority console that a member of the role will be able to access. Users are assigned to roles by selecting the Roles Assignment tab. The areas of the console that a System Role

can include are:

- Client Deployment
- Global Options
- Profiles
- Remote Management
- Reporting Tool
- Server Manager
- Software Distribution
- System Configuration

Managing system roles

Before assigning any users to a System Role, the system role must be created. System Roles are maintained in the **Console Access Settings > System Roles** tab.

Click the **Add role** button to create a new System Role. Enter the new role name in the entry below the Add role button. On the right side of the table, select the required areas of the console that the users of the role should have access to. Users assigned to this role will not be granted access to any unselected functions in this table.

Once you have selected permissions for the role, you need to assign one or more users to the System Role. Click on the Roles Assignment > **Add user**, or **Remove user** buttons to manage the users that are assigned to the System Role.

Be sure to click **Save** when the Role is finished being modified. To remove a role, click **Remove role** after selecting a single role in the table.

To edit an existing System Role, click the **Edit** button. This will put the currently selected System Role into edit mode. The currently selected System Role is the one with the yellow highlight.

Configuring roles

What is a role?

A role is a container that defines the actions that are permissible by members of the role.

Most often, roles are established to represent a common job function that is performed by one or more users (members). A role defines the functions that a member of the role will be able to perform. For example, as shown in the following table, there may be a Super User/Group who is responsible for defining profiles and maintaining the system for all sites (Domain Administrator), one or more users may be in charge of client configurations within their own site (Site Administrator), another group of users may be responsible for basic configurations and troubleshooting in their own site (Help desk), and so on.

There is several default roles included in the default setup of Desktop Authority.

Table 1: System default roles

Sample Role	Tasks	Required rights
Branch Admin	Oversee and configure profiles and clients,	Super User, All permissions
Profile Admin	Oversee and configure clients that belong to their own site.	Add, Change, Delete permissions to all objects within site's profiles. Does not include child profiles.
Security Admin	Responsible for keeping systems up to date and free of malware, secure desktops and run applications.	Add, Change, Delete permissions to Firewall, Security Policy, Group Policy Templates, Registry, Application Launcher, and other objects.
Read-Only Admin	Responsible for general help desk troubleshooting issues.	View only permission to all objects with a profile. Child profiles are not included.

Roles configure actions for all profile objects including the profile itself. The configurable actions of a role consist of View, Change, Add/Delete, and Deny permissions for each of the objects. The first step in configuring Role Based Administration is to create the roles that will be used to permit or deny access.

The above Roles are examples administrative roles that could be used. Role Based Administration allows the creation of as many custom roles as is needed.

Global role

A global role is a defined role that is available to all profiles.

Local role

A local role is defined at the profile level and is available only to the profile to which it is defined in.

By default, a new installation of Desktop Authority will create a Global Role named **Profile Admin**. The Profile Admin role by default has full access to Add, Change and Delete elements in all Profile objects as well as the ability to add, change and delete profiles. The permissions assigned to the profile admin may be modified within the Global Roles dialog.

Configuring global roles

Global Roles are created from the Manager's Console Access Settings menu. Select the **Global Profile Roles** menu item.

To create a new Role, click **Add role**. Enter the name for the new role. Once the new role is created, permissions must be assigned to it. Manipulate the View, Change, Add/Delete and Deny permissions for each profile object, or click on the **Grant all/Deny all** buttons. The profile objects are selectable by choosing Computer Management Object or User Management Objects from the drop down menu.

Be sure to click **Save** to save the role and its settings. Click the **Remove role** button to delete the selected Role. Click the **Edit** button to modify a roles assigned permissions and/or the role name.

Global roles may also be created from within a profile. On the Profile Permissions tab, click Add global role. Only Super Users/Groups can create global roles.

Configuring local roles

Local Roles are created from within a profile. Once the Profile is selected in the Navigation Pane, select the **Permissions** tab. In order to Add, Edit or Delete any roles on this dialog, you must press the **Edit** button at the top of the page.

Once in Edit mode, the Profile Roles tables will be able to be modified. To create a new Local Role, click **Add local role**. Modify a role by selecting a role from the table and clicking the **Edit** button. Click **Remove role** to delete the selected role from the list. A global role may be created from here by clicking the **Add global role** button. If the profile selected is a Computer Management profile, the table will display only the Computer Management objects. The same is true for User Management; if the profile selected is a User Management profile, the table will display only the User Management objects.

Once it Add or Edit mode, name or rename the role as well as select the appropriate profile object permissions by checking the View, Change, Add/Delete and Deny checkboxes. You may also click the Grant All/Deny All buttons to select or unselect all of the permissions. Be sure to click the Confirm or Cancel button to save any changes made to the permissions.

Object permissions

Read

Read permissions allow the object to be viewed only. No changes can be made to existing elements, nor can any elements be added or removed.

Modify

Modify permissions allow existing elements within the object to be updated only. Elements cannot be added or removed.

Add/Delete

Elements can be added to or removed from profile objects. Child profiles can be added or removed.

Deny

No access is permitted to the object selected in the permissions list. The object will not be visible in the navigation pane for any member that is a part of the role.

Deny access overrules all other permissions on an object.

Configuring profile permissions

The profile's Permissions tab is used to assign a user (member) to a role. Permissions are applied on a per profile basis. All child profiles inherit their parent's permissions. See the inheritance topic below for more information on how permissions are inherited.

To assign a user permissions to a profile, first select the Profile. Next, select the Permissions tab on the View pane.

Add local role

A local role is defined at the profile level and is available only to the profile in which it is defined. Click Add/Edit Local Roles to create or edit a role. The Local Roles dialog will open. For more information on Local Role configuration see the Configuring Roles topic.

Add global role

A global role is a defined role that is available to all profiles. To create a global Role, click Add/Edit Global Roles. The Global Roles dialog will open. For more information on Global Role configuration see the Configuring Roles topic.

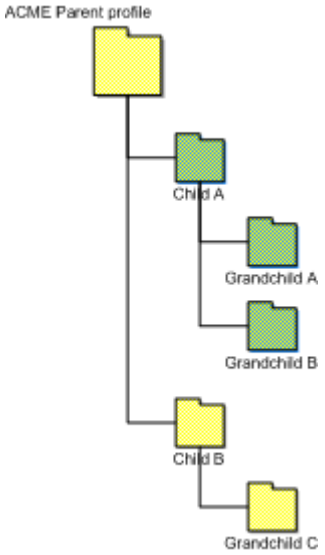
Add/Delete members to/from roles

To add a member to a role, select the role from the Roles list. Click Add Member.... Select a user or group from the resource browser and click OK. To remove a member from a role, select the Role and Member and then click Delete Member.

Permission inheritance

Profile permissions for all roles are inherited downward to all children profiles. Permissions do not inherit up the profile tree.

Figure 19: Permission inheritance



In the above illustration, Grandchild A and Grandchild B automatically inherit the permissions assigned to Child A. However, Grandchild C does not inherit any permissions from Child A. Grandchild C has the ability to inherit permissions from Child B which can inherit from the ACME Parent profile.

Figure 20: Explicitly deny permission inheritance

Permissions automatically are inherited by children profiles except in the case where the child profile explicitly denies the inheritance. In the above illustration, the role granted permission in profile Child B was explicitly given Deny permission in profile Grandchild C.

When creating a local role, the member cannot assign permissions to any object other than what they have access to. The permission level cannot be greater than the permissions that they have. For example, if a member of a role has View and Change permission to the printers object, they cannot assign another user Add/Delete permissions to the printer object.

Global Options

Global Options

The Global Options object provides the ability to define several settings which affect how Desktop Authority initiates for each client. These settings apply to all users, computers and profiles and include several objects. Global Options are broken up into three sub-components: Common Management Options, Computer Management Options, and User Management Options.

Global Options objects are available only to Super Users/Groups with the exception of Assign Script.

Common Management Options consists of Exception and Network Location Awareness options.

- Exceptions
  Exceptions are used to disable the ability to run Desktop Authority or allow an alternate logon script to run on any of the specified computers.
- Network Location Awareness (NLA)
  Network Location Awareness is used to configure NLA within the Desktop Authority Console. NLA. Desktop Authority uses Network Location Awareness to detect when a new network connection becomes available. Once the new connection is detected, Desktop Authority will be notified and can then determine whether it will execute for the user.

Computer Management Options consists of Definitions and Troubleshooting options.

- Definitions
  The Definitions object is used to define custom dynamic variables. These variables may be used within any profile as well as in any custom script.

- Troubleshooting
  The Troubleshooting object is used to define several settings that can help to troubleshoot problem clients. The most common setting on this object is the setting to create a detailed trace file for one or more specified users and/or computers.

User Management Options consists of Definitions, Visual, Desktop Agent and Troubleshooting options.

- Definitions
  The Definitions object is used to define custom dynamic variables. These variables may be used within any profile as well as in any custom script.
- Troubleshooting
  The Troubleshooting object is used to define several settings that can help to troubleshoot problem clients. The most common setting on this object is the setting to create a detailed trace file for one or more specified users and/or computers.
- Visual
  The Visual object is used to set the default graphical startup mode of Desktop Authority as it executes on the client during the logon process.
- Desktop Agent
  The Desktop Agent will launch specified programs as the client logs off or shuts down the computer. This object provides several default options for the Agent.

Common Management Options

Exceptions

The Exceptions tab is used to disable the ability to run Desktop Authority or allow an alternate logon script to run on any of the specified computers. Exceptions can only be modified by a Super User/Group. This object is applicable to both.

Do not execute Desktop Authority profiles or settings on:

Select the appropriate box for each computer class that should be excluded from running Desktop Authority. These selections may include any combination of the following computer classes: **Desktop computers**, **Portable**, **Tablet**, **Embedded**, **Terminal server clients**, **Member servers**, **Domain controllers**, **Clients connecting over dial-up**, **Citrix ICA published applications**, and **Specific computers**.

When excluding **Specific computers** from the execution of Desktop Authority, enter the computer names in the entry provided. Separate computer names using a semicolon (;). Wildcards may be used with the computer names.

Launch alternative script (bat/cmd)

Setting an alternate script only applies to user logins as the Login script is only executed when a user actually logs into the computer.

When a computer class is excluded from running Desktop Authority, an alternate batch or cmd file may be launched instead. Running an alternate batch file is useful if your users require only a few simple drive mappings and do not need the full configuration capabilities that Desktop Authority offers. Select the **Enable** box to designate the alternate selection. Manually type the name of the alternate file or click **Browse** to locate the file on the network. The file must have an extension of .BAT or .CMD in order for it to run as a logon script. Click **Browse** to locate the file will

automatically copy the file to the SLSCRIPTS share so that it may be replicated to the NETLOGON share on each domain controller.

Once a .BAT or .CMD file extension is entered into this field the Edit File link, is enabled. Click the Edit File link to edit an existing file or the creation of a new file if the file name is not found in the SLSCRIPTS share folder.

Do not perform User Management actions at logoff

Select this box to disable the ability to process User Management logoff actions. No logoff events will be processed, regardless of whether they are selected as part of a profile's or element's validation logic settings.

> Note: Selecting this check box will not remove the ability to select logoff or shutdown from the validation logic timing settings. However, the ability to execute a profile/element at logoff or shut down will be disabled.

Do not perform Computer Management actions at shutdown

Select this box to disable the ability to process Computer Management actions at shutdown. No events Computer Management events scheduled for shutdown will be processed, regardless of whether they are selected as part of a profile's or element's validation logic settings.

> Note: Selecting this check box will not remove the ability to select logoff or shutdown from the validation logic timing settings. However, the ability to execute a profile/element at logoff or shut down will be disabled.

Allow any client to selectively bypass Desktop Authority execution

Selecting this box allows certain computers to be excluded from ever executing Desktop Authority regardless of the options selected in the Desktop Authority Manager. This option requires the use of a special options file called SLBYPASS. If this file is present on the client, Desktop Authority will detect its presence and immediately exit before launching the main script engine and/or applying any configuration changes to the client.

> Note: For information on creating and using option files, see the Option Files topic.

Network Location Awareness

The Network Location Awareness (NLA) tab is used to configure the DA Client Service to automatically detect when an off-network computer (e.g. employee working remotely) establishes a new connection to the parent domain via a network change (e.g. using a VPN connection). Once the new connection has been detected, Desktop Authority will then immediately begin to execute all applicable validated settings.

Enable Network Location Awareness

Select this box to enable NLA and allow a managed DA computer to immediately run Desktop Authority when a new connection to the corporate network has been detected.

Enable DA script in case of network disconnections and reconnection

In addition to detecting a change in network, this setting allows for the detection of a disconnection and re-connection to the same corporate network. This would be used when a user disconnects from the direct connect LAN and then goes to wireless. This setting allows Desktop Authority to be able to immediately re-map printers, drives, etc.

Alternate logon script name

By default, NLA will verify if SLogic or SLogic.bat (default Desktop Authority logon script) is assigned to the user in Active Directory. If not, Desktop Authority will not be launched. This setting should be used to specify an alternative logon script name(s) currently associated with the execution of Desktop Authority. Multiple alternate logon scripts can be specified. Each filename must be separated by a comma.

Example: Login.bat,Login
Example: Login.bat,Login,Slogic.bat,Slogic

Path to UBM non-default logon script location

Specifies the location of where logon script resides. The batch file name does not need to be specified. The default location is %logonserver%\Netlogon". So if the Slogic.bat login script will be used from the Netlogon folder then nothing needs to be specified.

However, if Slogic.bat is being replicated to sub folder or different folder than Netlogon, like %logonserver%\Netlogon\DA, then the full UNC path needs to be specified.

Example: %LogonServer%\Netlogon\DA

Example: \\ServerName\FolderName\SubFolderName.

Type of event for DA script

Select the event when the logon script will be run. The default is set to Refresh.

When the Logon event is selected, the DA Client Splash screen will be displayed.

The DA Client Splash screen will not be displayed when the Refresh event is selected.

Minimum period between DA script executions

The amount of time needed before NLA will execute again. For example, if the period is set to "600" seconds (10 minutes) then when a user connects to VPN, NLA will detect this and kick off a refresh event (default). If the user disconnects and re-connects before 10 minutes, then NLA will not execute SLogic.bat again.

Computer Management Options

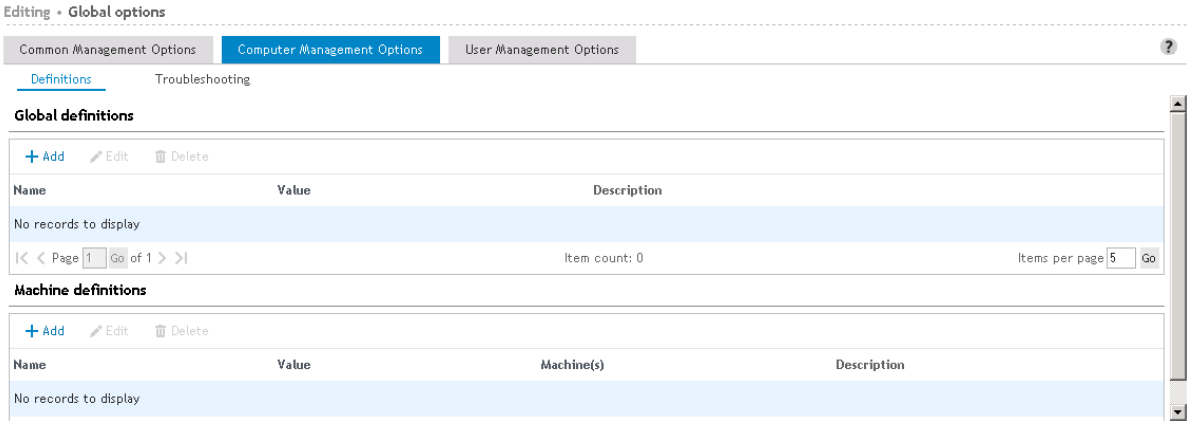
Definitions

> ⓘ Note: Computer Global Definitions can only be accessed by a Super User/Group.

Computer based definitions are variables that are defined for use in Computer Management profiles. These variables are for advanced and troubleshooting use.

Click **Add** to update the Global or Machine Definitions list with new definitions. Click **Edit** to modify an existing definition. Click **Delete** to remove a definition from the list. Once the list is in Add or Edit mode, select a Definition Name from the drop list and enter its corresponding value. Click **Save** when the definition is complete. Click **Cancel** to exit edit mode without saving the new Definition Name.

Figure 21: Global Options, Computer Management Options, Definitions dialog



The list of definition variables below is available for selection when configuring Global Definitions. A new variable many also be typed into this field.

Table 2: List of default computer definition variables

Name	Value
Event_Refresh_Time	Defines the time interval for the Computer Management refresh. The default refresh interval is 60 minutes. This value is specified in minutes.
ServicePackFreeSpaceNeededInMB	Defines the free space needed for Desktop Authority to install a Service Pack. The default free space needed is 1.4GB.This value is entered as megabytes.
Machine_Trace_Days_To_Retain	Defines the number of days to retain the Computer Management trace file. This can also be set on the Computer Troubleshooting tab, however in the Definitions object it can be set as a Machine definition for select machines. This setting will override the setting on the Computer Troubleshooting tab. Specify the number of days from 1 to 14.
Machine_Trace_File_Repository	By default, this variable is to set the network repository location for the Computer Management trace file. This can also be set on the Computer Troubleshooting tab, however in the Definitions object it can be set as a Machine definition for select machines. This setting will override the setting on the Computer Troubleshooting tab. Specify in the following format: \\ServerName\ShareName\FolderName
Machine_Trace_Level	Defines the level of logging to take place for Computer Management. This can also be set in the Computer Troubleshooting tab, however it can set it as a Machine definition for select machines. This setting will override the setting on the Computer Troubleshooting tab. Allowable values are: Verbose, Normal, Warning, Errors, None A Verbose trace contains all possible trace settings including Normal, Warnings and Errors. A Normal trace contains Normal, Warnings and Errors.

Name	Value
	A Warning trace contains all Warnings and Errors. An Error trace just contains Errors. Specify None for no trace.

For a list of special Global Variables that can be used, see the Global Variable Definitions List.

Computer Troubleshooting

The Troubleshooting tab is used to define several settings that are used to aid with tracing problems with objects/elements that are being applied on one or more client machines. The Troubleshooting object can only be modified by a Super User/Group.

The most common setting on this object is the ability to create a detailed trace file for one or more specified users and/or computers.

Delete client trace files older than xx days

Specify a number of days in which older Computer Management trace files should be removed from the system. This can be a number from 1 to 14. The default value is 7 days.

Upload a copy of each client's trace file to this network path

Manually enter a network path to which all Computer Management trace files will be copied to. Click **Browse** to locate the network location using the resource browser. The Computer trace 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 file is copied at the end of the day (midnight) if the computer is up or when the computer comes up and creates a new trace file for the day.

Click **View files** to view the trace file repository location as specified by the entry.

Enable verbose debug mode for these specific computers

By default, a simple Computer Management trace file is created for all computers. However, by selecting this box, a more detailed trace file can be created. This verbose trace file will detail and trace Computer Management profiles only. Since this trace file is extremely detailed, providing lots of information, it can grow quite large. For this reason, this option should not be enabled unless some specific debugging is necessary.

> Note: By default, log files will be stored in the *%windir%\Temp\Desktop Authority* folder. Please refer to the File Paths appendix for the correct path(s) based on the version of Desktop Authority you are using.

User Management Options

Definitions

> Note: User Global Definitions can only be accessed by a Super User/Group.

The **Definitions** tab is used to define User Management based custom dynamic variables. These variables may be used within any User Management profiles as well as in any custom script.

All definitions in the text block must contain valid KiXtart script code.

Definitions declared within the Global Definitions area are for use globally on all computers.

Desktop Agent

The **Desktop Agent** is an application that launches specified programs when the client logs off or shuts down the computer. There are several default options for the Desktop Agent.

NOTE: Desktop Agent options can only be modified by a Super User/Group.

Desktop options

Do not show Desktop Agent in system tray

Select this check box to hide the Desktop Agent icon in the system tray. Although the icon is hidden, the agent will still be active.

Always restart computer, even if shut down is selected (desktops only, excludes 64 bit platforms)

Select this check box to force the computer to Restart even if a Shutdown was selected. This option comes in handy when installing service packs or other applications that may need to complete after the system restarts.

Using this option sets the Agent to automatically launch regardless of any logoff/shut down events.

If logoff/shut down application does not complete

Wait before executing the next synchronous application

Specify the maximum number of seconds the computer will wait before running each successive synchronous logoff/shut down application. The timer default is 900 seconds (15 minutes); zero (0) will disable this timer. Disabling this timer will cause Desktop Authority to wait for the natural completion of each individual application. Each application must complete on its own before the next synchronous application will begin.

Wait after executing the last application before ending the Windows session

Specify the maximum number of seconds the computer will wait for all logoff/shut down applications to complete before performing the logoff or shut down of the computer. For asynchronous applications this timer starts after the last application is launched.

When synchronous applications are invoked, this timer begins after the completion of the final synchronous application. The timer default is 1,800 seconds (30 minutes); zero (0) will disable this timer. Disabling this timer will cause the Desktop Agent to wait for the natural completion of all applications (synchronous/asynchronous).

User Troubleshooting

The **Troubleshooting** tab is used to define several settings that are used to aid with tracing problems with objects/elements that are being applied on one or more client machines. These Troubleshooting settings will be in

effect for both Logon and Logoff timing events.

> Note: The Troubleshooting tab can only be modified by a Super User/Group.

The most common setting on this object is the ability to create a detailed trace file for one or more specified users and/or computers.

Do not hide windows during logon sequence

Select this check box to show all initialization windows during Desktop Authority startup. This option is useful when troubleshooting logon problems.

Force KiXtart to refresh its group token-cache during each logon attempt

Enumerated groups are cached to the local machine. To flush the local cache and rebuild it on the local machine select this check box. The cache will refresh during each logon attempt.

Create a detailed trace file on these specific computers and/or users:

Select this check box to enable a User trace file to be created for specific computers and/or users.

The sltrace.htm file is a color coded event log of actions taken during the logon process. Red text within the file indicates that some action may not have completed properly or may be taking longer than expected.

Specify a list of computer names and/or user names that a comprehensive trace file will be created for. This trace file describes the actions taken during the logon process. It is created in the client's %temp%\Desktop Authority folder and is called sltrace.htm.

Names must be delimited by a semicolon (;). The computer/user name supports the question mark (?) and asterisk (*) wildcards.

Example:

mjones;jsmith;PC221;PC3??;PC4*

Upload a copy of each client's trace file to this network path

Specify a network path to which all User trace files will be copied to, after each logon. The trace 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 User based log files are uploaded right after the event (Logon, Refresh, Logoff, or Shutdown) is complete.

Click **View files** to view the trace file repository as specified by the entry.

Enable debug mode for these specific computers and/or users:

Select this check box to allow Desktop Authority User Management to run in debug mode for the specified computers and/or users.

Specify multiple names by delimiting each by a semicolon (;). The computer/user name supports the question mark (?) and asterisk (*) wildcards.

To activate the debug session on the client, press any key upon Desktop Authority initialization. Debug mode runs the logon script, pausing after each entry is executed on the client machine. Press [Enter] to continue processing the next script entry. Press the letter [D] on the keyboard to continue processing the script to the end, without pausing. Press the letter [Q] on the keyboard to abort the script.

When the script if finished processing, you are prompted to apply the contents of the configuration profiles to the debug log. This will append the debug information generated from the client logon process to the sltrace.htm file.

You are then prompted to view the sltrace.htm file. This text file may be viewed at any time to further debug problems that may occur during logon for a client

Visual

The **Visual** tab is used to set the default graphical startup mode of Desktop Authority as it executes on the client during the logon and logoff process. One of three display types can be selected.

Note: The Visual object can only be modified by a Super User/Group.

During the logon sequence

Splash screen style

Select an option from the drop list to define how the Desktop Authority splash screen will be displayed on the client computer at logon.

Default graphic

Select this option to enable the default splash screen. This is a window that displays the logo along with a progress bar indicating the progress of the logon.

Displaying the default graphic during the logon process is the default option.

Custom graphic

Select this option to enable a custom graphic splash screen as the client logon request is processed.

This option requires clients to have Internet Explorer 4.0 or above. However, if Internet Explorer 4.0 has the Desktop Component Update (i.e. Active Desktop), only a progress bar will be displayed (no custom logo).

Logo filename

Enter the location of the custom graphic to be displayed on the client at logon. Click **Browse** to locate the image file. The following graphic formats are supported: bmp, rle, gif, png and jpg. Once an image is selected, it will be copied to the SLSCRIPTS$ share. Click **View** to preview the image that will be displayed.

Specifying *$weekday.ext* in the entry (where *ext* is the graphic file extension), will display the image associated to the current day of week. For example, if $weekeday.bmp is entered in the *Logo filename* entry, on Monday, Monday.bmp will be displayed. On Tuesday, Tuesday.bmp will be displayed, and so on for the rest of the days of the week. If no associated weekday image is found, the default Desktop Authority image will be used. $Weekday is the only variable that may be used in this field.

Progress dialog location

Select the location of the progress bar dialog box from the list. Valid choices are *Lower Right*, *Lower Left*, *Upper Right*, *Upper Left* and *Center*.

The following three options are available when either choosing to display the default or a custom graphic:

Allow any client to override this setting and always display the text screen

Select this check box to override the selected option and allow a client to use the text logon screen for troubleshooting purposes.

On each specific client that will use a text logon screen, create a file called *SLNOGUI.* (no file extension). The presence of this file notifies Desktop Authority to display a text logon screen during the logon process.

Display only the progress dialog when logging on from a Terminal Server session

Select this check box to display a small progress dialog for Desktop Authority execution on Terminal Server sessions. This minimizes the amount of data to be sent from the Terminal Server to the client.

Display only the progress dialog when logging on over a dial-up connection

Select this check box to display a small progress dialog for Desktop Authority execution on clients that connect to the network via a dial-up connection. This minimizes the amount of data to be passed over the line and will speed up the logon process.

Informational text screen

Select this option to enable a text splash screen as the client logon request is processed.

This display is a great tool for troubleshooting. It provides information regarding the user, the computer and functions that are being processed as the logon script runs.

End of script completion message

Enter static text to be used as a message in the text splash screen when the logon process is complete. Dynamic variables may be used in conjunction with any text entered. Desktop Authority's dynamic variable selection is available for this field by pressing the F2 key.

None

Select this option to disable all splash screens that would normally be displayed during the client logon process.

During the logoff sequence

Display progress graphic

Select this box to display a progress bar on the client during the logoff process. Clear this box to display no information on the client during the logoff process.

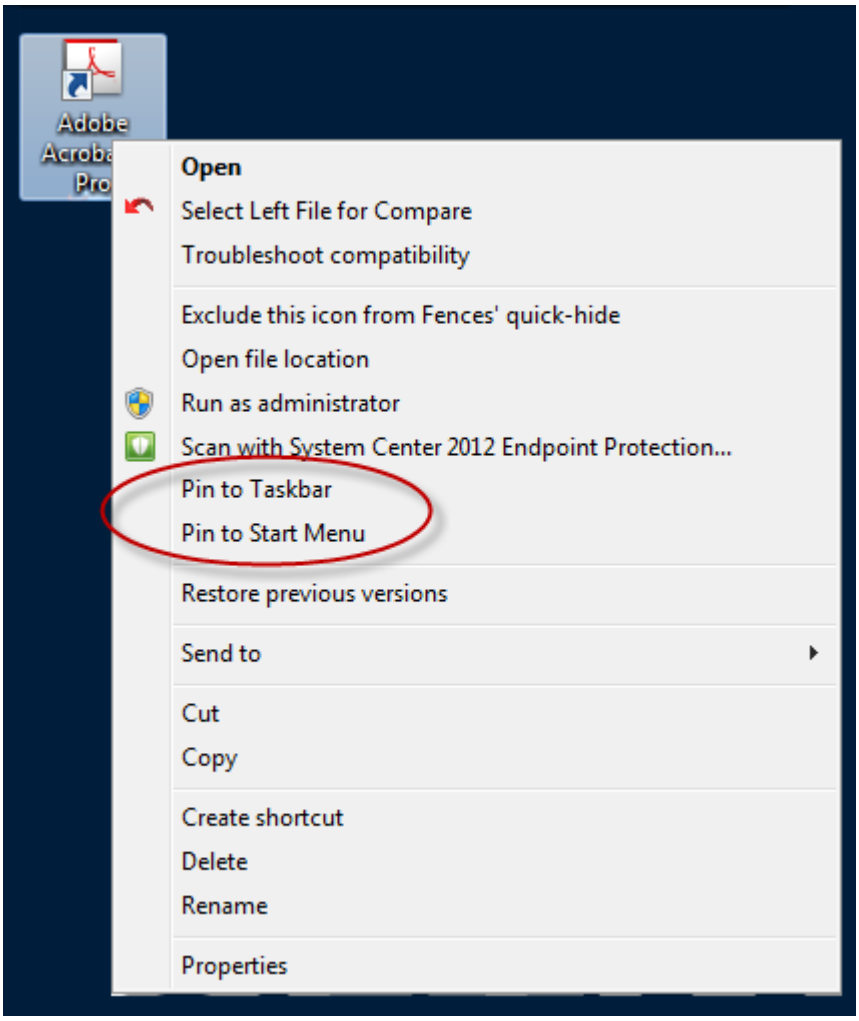
Global Definition variables list

User Management definitions

Shortcut profile object

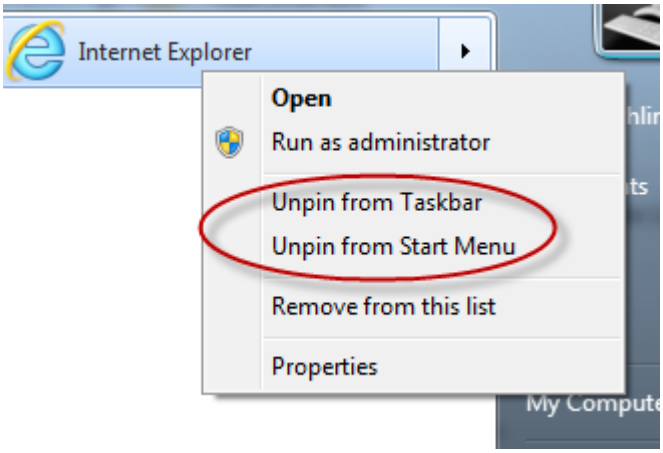
When selecting User Start Menu (Pin) or User Taskbar (Pin) with a non-English language workstation operating system, you must define a variable that defines the non-English verbiage to substitute in place of the English "Pin To..." verbiage. The value of these variables should match the "Pin to Taskbar" or "Pin to Start Menu" text on the popup menu of a program shortcut. The following variables can be defined as User Management Global Variables or as a Profile Definition Variable.

Figure 22: Example of "Pin to" options



For the Unpin variables, the value should match the "Unpin from Taskbar" or "Unpin from Start Menu" on the popup menu of a shortcut on the Start Menu or Taskbar.

Figure 23: Example of "Unpin from" options



$PinToTaskbarString

Defines the "Pin to Taskbar" verbiage on non-English client operating systems.

Example (German language operating system):

$PinToTaskbarString = "GermanLanguage"

where GermanLanguage will be replaced with the German language equivalent

$UnPinFromTaskbarString

Defines the "Unpin from Taskbar" verbiage on non-English client operating systems.

Example (German language operating system):

$UnPinFromTaskbarString = "GermanLanguage"

where GermanLanguage will be replaced with the German language equivalent

$PinToStartMenuString

Defines the "Pin to Start Menu" verbiage on non-English client operating systems.

Example (German language operating system):

$PinToStartMenuString = "GermanLanguage"

where GermanLanguage will be replaced with the German language equivalent

$UnPinFromStartMenuString

Defines the "Pin to Start Menu" verbiage on non-English client operating systems.

Example (German language operating system):

$UnPinFromStartMenuString = "GermanLanguage"

where GermanLanguage will be replaced with the German language equivalent

Web Browser profile object

The Web Browser object allows for the configuration of custom Firefox settings. If you wish to configure something in the Firefox browser that is not offered on the Web Browser object, it can be configured in the Global or Profile Definitions.

Use the following syntax for configuration:

AddCustomFirefoxPref('pref("Name", Value);')

This will set the named Firefox preference to the given value. This configuration can be accessed via the browser and changed by the user.

AddCustomFirefoxPref('lockPref("Name", Value);')

This will set the named Firefox preference to the given value. This configuration will not be able to be changed via the browser about:config dialog by the user.

"Name" is the name of the preference to be set.

Value is the boolean, string, or integer data for the preference.

Preferences and their settings can be seen in Firefox's about:config dialog.

NOTE: Custom Firefox preferences can be researched in this reference to the user preferences in the about:config,

Examples:

Bool Value: - value can be true or false

AddCustomFirefoxPref('pref("privacy.clearonshutdown.cache", true);')

String Value: - add double quotes around value

AddCustomFirefoxPref('pref("network.automatic-ntlm-auth.trusted-uris", "Http://www.google.com");')

Integer Value: - a numeric value

AddCustomFirefoxPref('pref("network.http.connection-retry-timeout", 500);')

Locked Integer Value: (to prevent a setting from being changed by the user, replace pref with lockpref)

AddCustomFirefoxPref('lockPref("network.http.connection-retry-timeout", 500);')

Computer Management definitions

Validation Logic

$VLCheckAllIPAddresses

This setting will enable Validation Logic to validate on any IP address defined for the client, instead of just the first one read. This variable can be defined as a User Management Global Variable or as a Profile Definition Variable.

Example:

$VLCheckAllIPAddresses = 1

Registry keys

sqlCommandTimeout

Sometimes, on large database transactions, the default SQL Command timeout value is not big enough to support the command, allowing the transaction to timeout and fail. Creating this new registry key allows this timeout value to be overridden and increased to alleviate a timeout problem.

Name	Type	Data
HKEY_LOCAL_MACHINE\SOFTWARE\ScriptLogic\SqlCommandTimeout	DWORD	specified in seconds

6

Deployment options

Deployment Settings

The Deployment Settings object provides the ability to configure settings for objects that will deploy options to the client.

Server Manager

The Server Manager object provides an interface to manage the DA Administrative service, the Update Service and the replication process.

Client Deployment

The Client Deployment object provides access to the Assign Script object and the GPO Deployment object, both of which arm the domain user and computer with configurations that allow Desktop Authority to execute for the User and on the Computer.

Software Distribution

ⓘ Note: not available for Desktop Authority Essentials

The Software Distribution object is used to import software packages into Desktop Authority for deployment.

System Configuration

The System Configuration object is used to retrieve resources from the network before they are actually needed so processing is faster.

Off-Network Support

The Off-Network Support object is used to configure devices to use Desktop Authority configurations when it is off-network.

RM Gateway Configuration

The RM Gateway Configuration object is used to configure Off-Network Remote Management.

Client Deployment

The Client Deployment object provides access to the Assign Script object and the GPO Deployment object, both of which arm the domain user and computer with configurations for Desktop Authority to execute during client logon process.

Assign Script

The **Assign Script** object is used to assign the SLOGIC logon script to domain user accounts for User Management profiles and objects.

GPO Deployment

The **GPO Deployment** object provides the ability to deploy Desktop Authority's SLagent technology to client workstations by using a GPO extension.

Client Provisioning

Client Provisioning encompasses both GPO Deployment and Logon-based Deployment and dynamically chooses from the best of several deployment approaches at runtime in order to deploy necessary files to the client computer.

Off-Network Client Provisioning (manual deployment)

Off-Network Support (ONS) allows computers to receive configuration updates over the internet without having an active connection to the parent domain. Off-Network Client Provisioning (ONCP) allows for the initial provisioning of new computers to occur off-network (i.e. while being disconnected from the parent domain). Once a new off-network computer has been provisioned using ONCP, it is immediately ready to begin retrieving Off-Network Desktop Authority settings (assuming an active internet connection and ONS being configured).

However, unlike the automated on-network provisioning process, ONCP deployment can only be done outside of the Desktop Authority framework. This means Admins attempting to utilize ONCP MUST first determine an efficient method to deploy and install the necessary files to their off-network computers that require Desktop Authority provisioning.

IMPORTANT: Microsoft .NET Framework 4.6 (or 4.5) must be installed and enabled on client computers prior to provisioning using ONCP. Desktop Authority will not function correctly on computers provisioned using ONCP without a supported version of .NET already installed and enabled. In the case of computers provisioned on-network, a supported version of .NET is automatically installed if needed.

Provisioning an Off-Network computer using ONCP

1. Once all latest changes have been saved and replicated within the DA Manager Console, copy both the **DAClientInstall.msi** and **DAClientInstall.ini** from the current User Management Replication share (**%logonserver%\Netlogon** by default).
2. Using the most efficient available method, copy both files down to each Off-network computer.

   NOTE: Both files MUST be located in the same folder prior to installation.
3. Install the DAClientInstall.msi file on each off-network computer. This can be done manually or automated using a custom script.
4. Once the installation has been completed, the newly provisioned computer(s) should immediately begin processing Desktop Authority settings. For off-network computers, this assumes there is an active connection to the internet and ONS was properly configured prior to copying the necessary files from the User Management Replication Share during Step 1.

Assign Script

The Assign Script dialog box provides the ability to assign a logon script to domain user accounts in order for the user to qualify for User Management settings. Computers that are **only** going to be configured with administrator settings from Computer Management profiles and objects are not required to have a logon script defined.

In addition to assigning a logon script to domain users, this tool can also be used to query which users in your domain currently have a specific logon script assigned to them. Any user who is a Domain Admin has the ability to update the assign/unassign logon scripts for users.

Select domain

On the left hand side of the Assign Script dialog, using the Active Directory OU and Groups tree, select the domain, group or organizational unit that will be used to locate users who will be assigned the Desktop Authority logon script.

Multi-select box 

The elements in the user list can be selected one at a time or several at one time. You can select more than one element in the list using the Shift or Ctrl key in combination with a mouse click. To select multiple users, hold down the CTRL key while clicking the individual users to select. Consecutive users in the grid can be selected by clicking the first user to select and then, while holding down the SHIFT key, clicking the last user to select. To select the entire list of users select the checkbox to the left of the column headers. This box will be empty if no users are selected and will be filled with a square if some users are selected. A user's selected status may be changed by clicking on it. If there is only one user in the list, it will always be selected.

Find users

Enter search criteria that will find matching Active Directory users. This is an inclusive search. Any user found with the search criteria in any part of the user name will be found as a match. Valid characters consist of [A-Z], [a-z] and [0-9].

Searching with a specific OU highlighted in the tree will search only that specific OU.

Assign script

Click **Assign script** to assign a logon script to all selected users in the list. In most cases, the script to assign will be SLOGIC. However, depending upon circumstances, this can be changed and the new script can be selected from the drop list to the left of the Assign script button.

Unassign script

Click **Unassign script** to unassign a logon script from all selected users in the list. The script may also be unassigned from a specific user by clicking the Unassign link in the Actions column. This link will only appear for users who already have an assigned logon script.

User list

The User list displays all users that have an established network account. Shown in this list are the User Name, Full Name, Description and associated logon script (if any).

GPO Deployment*

GPO Deployment will push out and install an MSI file to each computer in the targeted Domain or OU(s). The MSI file contains Desktop Authority's client files and must be installed to every computer that is to be managed by Desktop Authority.

The GPO is configured by selectively targeting the root of the domain or OUs (Active Directory Organizational Units) within the enterprise. 32-bit and 64-bit systems can also be selectively targeted. It is important to note that all computers within the selected domain or OU(s) will receive the client files unless a computer is defined as an exception.

Computer(s) to be excluded from the installation of the Desktop Authority client files are configured in the Global Common Management Exception Options. Excluded computers will not receive the necessary Desktop Authority client files that are necessary for the computer to be managed by Desktop Authority.

IMPORTANT: Client provisioning will determine the best way to install the client files to each workstation. This may include the use of GPO Deployment. Client provisioning provides a way to install the client files successfully on most computers in the network.

IMPORTANT: GPO Deployment requires the Authenticated Users group to have Read, Execute and List NTFS permissions on the %windir%\SYSVOL\sysvol\%DomainName%\Policies\Desktop Authority\Desktop Authority Agent 8.0 folder. If this requirement is not configured, Desktop Authority will automatically add the Authenticated Users group to this folder with the required permissions.

General

Preferred domain

Select a preferred domain from the drop list to be used as the default domain against which queries are run. This includes the types of queries where domain specific information, such as a list of domain controllers, is required.

Domain controller

If the client files location is set to SYSVOL, select a server from the drop list as the target for the client files.

WMI Filtering

Use WMI Filters

WMI Filters are used to fine tune the application of GPOs during a Group Policy refresh. A WMI Filter includes one or more WMI Query Language (WQL) queries. If any of these queries evaluate to True then the WMI filter is considered to evaluate to True and the GPO to which it is linked is applied. If the queries do not return anything in the resultant set then the GPO is not applied.

In most cases, this box should be selected. If however, WMI is posing a specific environment issue, unselect this option.

GPO Deployment List

The GPO Extension will be deployed to the selected domain or OUs in this list. The extension is set to either Install or Uninstall the MSI. Click on a column header to sort the list either ascending or descending by the selected column.

Organizational Unit

The Organizational Unit to which the extension will be installed to or removed from.

32-bit systems/64-bit systems

The selected install mode for 32-bit and 64-bit computers.

Add

Click **Add** to configure an OU for GPO deployment. The selected OU will be added to the GPO Deployment list.

GPO Deployment is supported on Windows 7 and above, Server 2008, Windows Server 2008 R2, Windows 2012, Windows 2012 R2, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8.1 and Windows 10. Windows Installer and .NET 4.6 are required on the target computers. Desktop Authority will install these software requirements, if necessary.

First, the OU must be selected. To do this, navigate to the OU on the left hand pane. As you click on the OU, the **Deploy DA Client to** in the right hand pane will be filled in with the selection from the left pane.

Next, select Install or Uninstall for 32-bit systems and 64-bit systems.

NOTE: Global Option Exceptions will be respected.

Confirm the selected settings and click **Save** to complete the GPO Deployment configuration for the selected OU.

Click **Cancel** to exit without saving any GPO Deployment configurations.

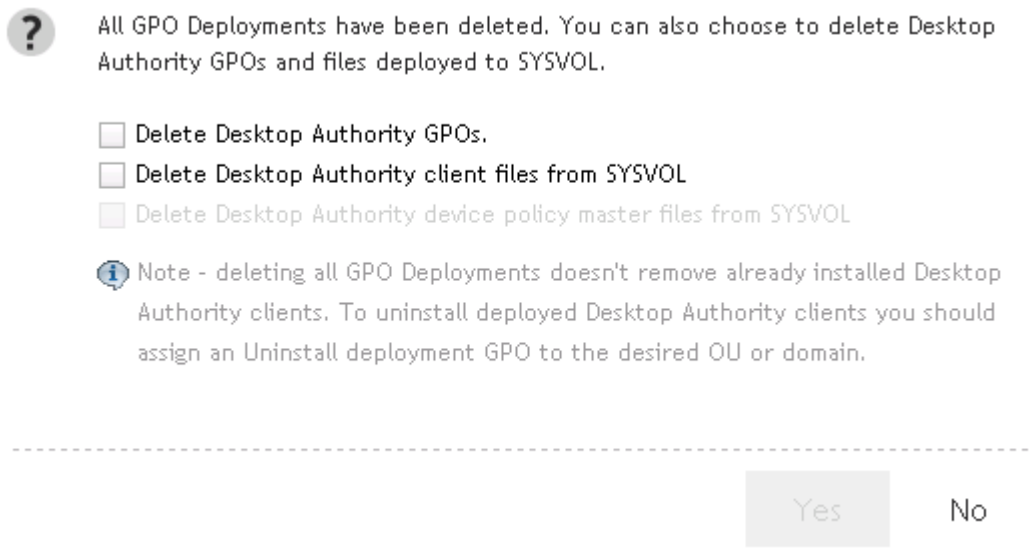
Remove

Click **Remove** to unlink the GPO from the OUs selected in the GPO Deployment list.

After unlinking the GPO, the following dialog provides the opportunity to remove the GPO and the associated files.

This dialog is only visible when the last GPO element is removed from the GPO Deployment list.

Figure 24: Delete GPO and associated files confirmation dialog



Delete Desktop Authority GPOs

Selecting this box will delete the GPOs and WMI filters.

Delete Desktop Authority Client files from SYSVOL

Selecting this box will remove the Desktop Authority Agent 8.0 folder under SYSVOL. The default path to this folder is C:\WINDOWS\SYSVOL\sysvol\[domain]\Policies\Desktop Authority\Desktop Authority Agent 8.0. This folder will be removed from one Domain Controller. During the course of normal replication on the domain, it will be removed from all other Domain Controllers.

Delete Desktop Authority device policy master files from SYSVOL

Selecting this box will remove the Device Policy Master folder under SYSVOL. The default path to this folder is C:\WINDOWS\SYSVOL\sysvol\[domain]\Policies\Desktop Authority\Device Policy Master. This folder will be removed from one Domain Controller. During the course of normal replication on the domain, it will be removed from all other Domain Controllers.

If both checkboxes, *Delete Desktop Authority Client Files from SYSVOL* and *Delete Desktop Authority Device Policy Master* files *from SYSVOL* are selected, the Desktop Authority folder under SYSVOL will be removed along with all the folders and files underneath it. The default path to this folder is C:\WINDOWS\SYSVOL\sysvol\[domain]\Policies\Desktop Authority.

Edit

Click to edit the selected OU settings. Change either the 32-bit or 64-bit install modes.

Verify GPOs

Click **Verify GPO's** to confirm that the Desktop Authority GPO extensions and WMI filters are up to date correctly configured.

Update GPOs

Click this button to increment the GPO extension internal version to the specified OUs. Once the version is incremented, the GPO will be recognized as a new version. It will be executed on any client whose version is different.

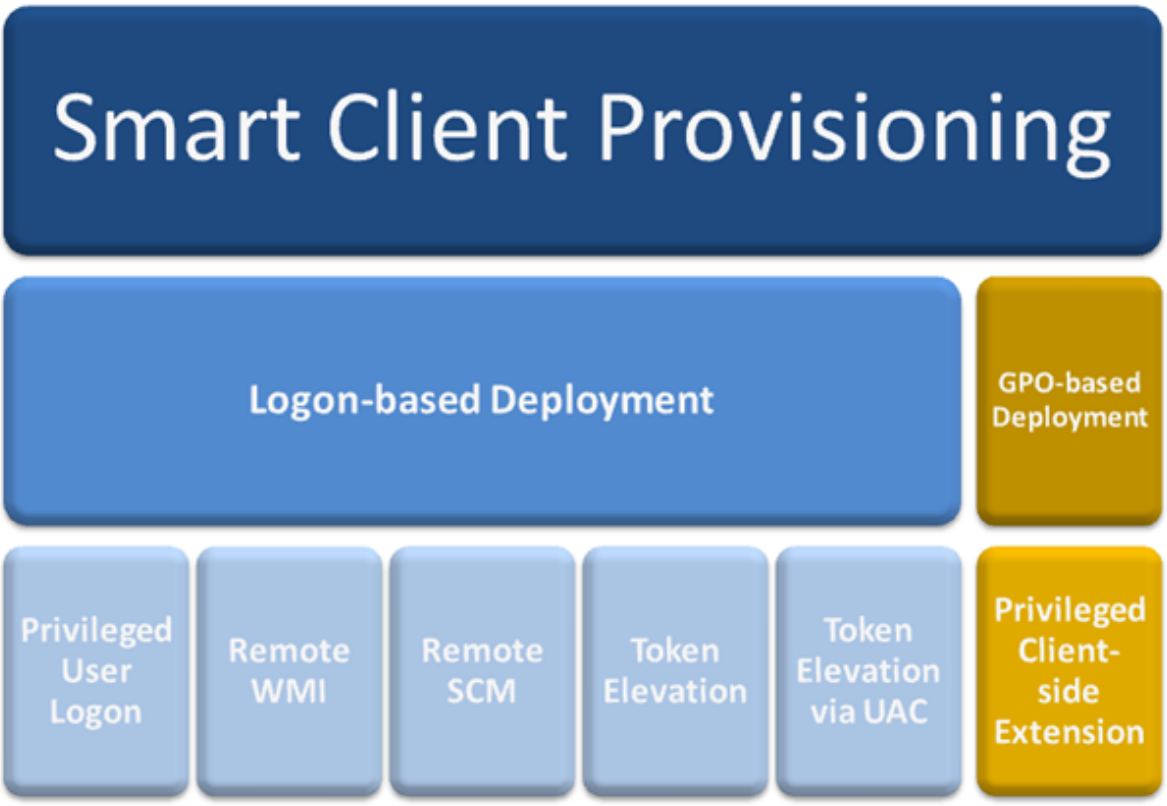
Refresh

Click **Refresh** to update the GPO Deployment list.

Client Provisioning

There are two ways in which Desktop Authority can deploy the necessary client files to machines that will be managed by Desktop Authority. Desktop Authority uses Client Provisioning which encompasses both GPO-based Deployment and Logon-based Deployment. Client Provisioning dynamically chooses from the best of several deployment approaches at runtime. The specific technique used depends on the client environment, and the obstacles present in that environment.

Figure 25: Client Provisioning overview



Desktop Authority GPO-based Deployment and Logon-based Deployment can both be used to deploy the Desktop Authority technology to client workstations and/or servers. They differ from each other in regard to the permission levels needed to accomplish the deployment. It is important to note that DA GPO does not require a user to login for the client files to be installed to the client, whereas the other methods used to deploy the client files will require a user logon. This is important to consider when provisioning workstations or servers.

Deploying the Privileged Client-side Extension with GPO-based Deployment 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 client file deployment without assistance from a Domain Admin, which defeats the purpose of having an OU Admin.

It is due to this privilege level issue, that Smart Client Provisioning has been implemented. Client Provisioning will go through the following series of steps to get the DAClientInstall.MSI deployed or installed on a machine.

1. Attempt to install the client files (DAClientInstall.MSI) with the user's credentials. This will be successful only if the user is a local admin.
2. If using the user credentials does not successfully install the client files, then an attempt to install the files using a process that is launched administratively via WMI. It is possible that a firewall may block WMI communications. TCP ports 135 or 445 may be opened to allow a remote WMI connect.
3. If using WMI does not successfully install the file, then an attempt is made to use a process installed as a service via SCM (Service Control Manager). It is possible that the firewall may block remote SCM calls.
4. If the above fails, an attempt to install the MSI will be made using a process, run administratively, that uses token elevation. This method may require an UAC prompt to the user.
5. If the above fails, then display the UAC prompt and install the MSI using a process, run administratively, using token elevation.
6. Otherwise, GPOs must be used to install the MSI. The use of GPO's is still required if you want no-touch provisioning of machines.

ⓘ Important: It is important to note that if WMI fails to allow a remote connection, TCP ports 135 or 445 may be opened to allow this connection to be successful and thereby allow the installation of the client files. Opening these ports may be easier to configure than to configure GPO deployment throughout the enterprise.

Client provisioning settings

Logon-based provisioning

Client files location

With Logon-based Deployment, client files can be delegated to client machines via NETLOGON, a custom NETLOGON or SYSVOL. This makes the Logon-based Deployment very flexible.

Select either NETLOGON or SYSVOL from the drop down menu. Client files will be replicated to the specified location and applied to each client computer when a user logs into the computer with the Desktop Authority logon-script (slogic.bat).

Select NETLOGON to use any NETLOGON share to store the client files. Using NETLOGON allows the NETLOGON share (or any custom share hosting the user files) to be used.

Selecting SYSVOL will allow client files to be stored in a single place, to be shared between GPO and logon-based provisioning.

ⓘ Note: When using both Logon-based Deployment and GPO-based Deployment, using the SYSVOL location is the most efficient. The file location is shared for both GPO-based and Logon-based Deployments. This is most useful in large environments. Using SYSVOL requires domain admin privileges.

Display error message if provisioning fails

Select this box to display an error message if the logon provisioning fails for some reason. This error will be displayed on the client.

Allow UAC dialog to be displayed if necessary

Select this box to ensure that the logon-based provisioning completes successfully on the client, if UAC is enabled on the computer. During the provisioning process, a Windows UAC dialog will be displayed, if necessary. This may be required if the client-side firewall is unusually restrictive. The user must accept the request. If the permission is not granted or this box is not selected, Desktop Authority may not be able to provision the computer properly.

Software Distribution*

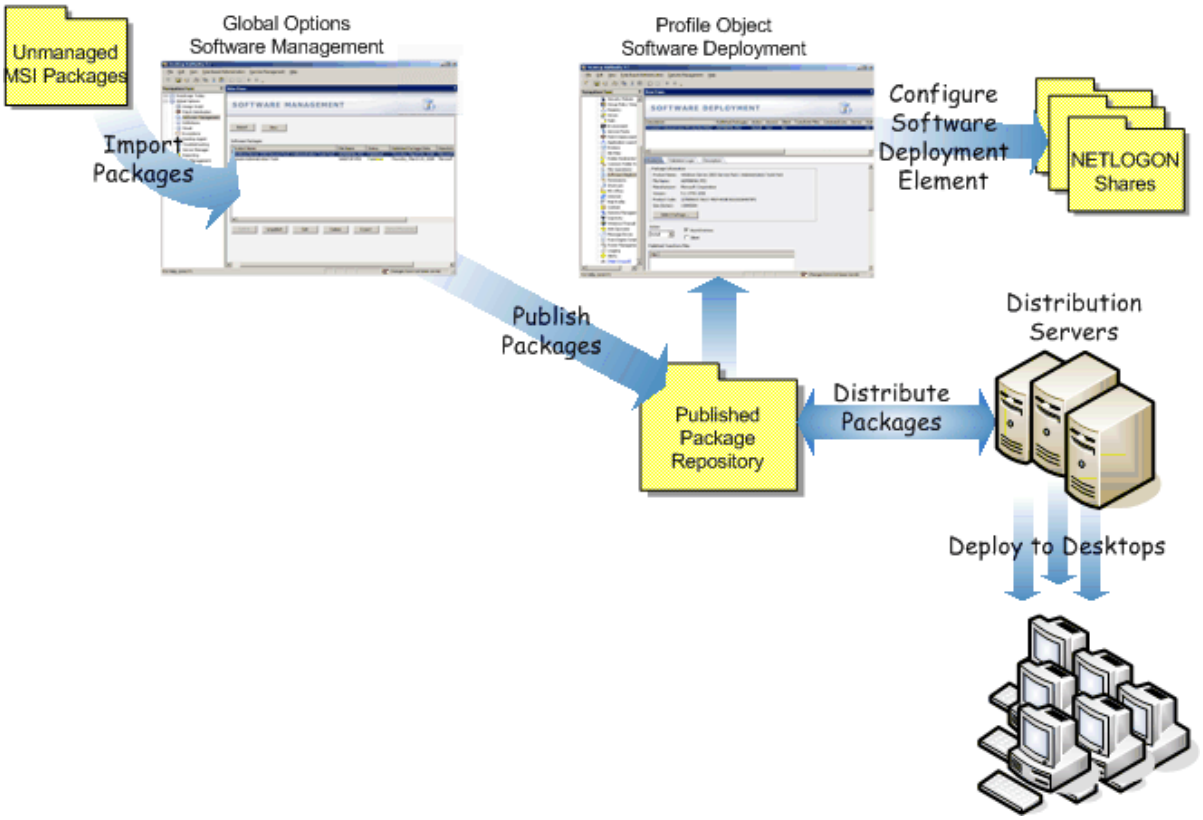
MSI packages contain all necessary files an application needs in order for it to be installed using Microsoft's Windows Installer. Windows Installer can install and/or uninstall MSI packages for any application regardless of the install package used by the manufacturer. Administrators can customize an MSI package by creating a transform (.MST) file. The transform can provide answers to Windows Installer when the MSI file calls for user input, such as choosing which options to install or the correct installation path. It can also remove unwanted features from the basic installation. MSP files are Microsoft Windows patch files that are updates to applications that have been previously installed with Windows Installer.

The Desktop Authority Software Distribution object is used to manage a repository of Microsoft Windows Installer (MSI, MST, MSP) packages.

The Software Distribution object provides the ability to:

- import packages into its repository.
- export packages from its repository.
- delete packages from the repository.
- publish packages for deployment using the Desktop Authority MSI Packages object.
- unpublish packages, i.e., remove them from use by the MSI Packages object.
- determine the differences between published and unpublished packages.

Figure 26: Software Distribution process overview



Desktop Authority accesses Windows Installer packages, providing the ability to Import, Export, Modify, Delete and Publish these packages.

Multi-select packages

One or more packages may be selected in the Software Distribution list by using the Shift or Ctrl key in combination with a mouse click. To select multiple packages, hold down the CTRL key while clicking the individual packages to select. Consecutive packages in the grid can be selected by clicking the first package to select and then, while holding down the SHIFT key, clicking the last package to select. To select the entire list of packages select the checkbox to the left of the column headers. This box will be empty if no packages are selected and will be filled with a square if some packages are selected. A package's selected status may be changed by clicking on it.

Import

Click Import to copy a Windows Installer package into the Desktop Authority repository. The Installer file must be an existing MSI, MST or MSP package.

Export

Click Export to copy a Windows Installer package from the Desktop Authority repository to another defined location.

Publish

Click Publish to make the selected packages available for install by Desktop Authority's MSI Packages object. The MSI package file is not initially copied to the server that the update service is installed to. However, when the client machine requests the package, the MSI package is copied to the server that the Update service is installed to. If a package is never requested by a client, it will not exist on the server.

For configuration information on the Update Service, see What is the Update Service?

Unpublish

Click Unpublish to remove Windows Installer packages from all distribution servers.

Delete

Click Delete to remove a Windows Installer package from the Desktop Authority repository.

Refresh

Click Refresh to freshen the Software Packages list.

Software packages list

The Software Packages list defines all Windows Installer packages that are available for deployment. This includes MSI, MST and MSP files. Packages must be imported into the Desktop Authority repository to show in this list. The following information is available about each package in the list: Product Name, File Name, Published Status, Published Date, Manufacturer, Type, Version, Product Code, and File Size.

Show differences

Click Show Differences between the published and unpublished versions of the selected package, if any differences exist.

This function is only available if the MSI is published and there are determined to be differences between the published and unpublished version of the package. If it is determined that there are no differences between the published and unpublished version of the package, this button will be disabled.

> ⓘ Note: This feature is not a standard part of Desktop Authority Essentials. To obtain this feature, Desktop Authority Essentials must be upgraded to the full version of Desktop Authority.

Server Manager

The Server Manager object is where the service, plugin and database configurations are configured. Only a Super User/Group will have access to Server Manager and its components.

Service Management

Service Management is a multi-threaded component that provides an interface to manage the DA Administrative Service, the Update Service and the replication process.

Plugins

The Plugins object is used to manage and configure plugins. Plugins are Desktop Authority provided objects that the Manager uses to perform specific operations. There are two default plugins that are necessary for Desktop Authority to collect data and report on it.

Replication options

Select the Replication Options tab to configure replication options and preferences.

Configure Site Map

Desktop Authority will attempt to connect to either the DA Administrative Service on the DA logon server (the server where slogic.bat is executed from, upon logon) or the Update service. If the requested service does not respond, or is not installed on that server, Desktop Authority will use a default site map to locate a server that has an active and responsive service. The default site map is created based on the information in the Server Manager list, and groups all servers to their respective site. The default site map will instruct Desktop Authority to attempt to connect with the service on one of the other server(s) that are listed in the same site as the workstation's site. Click on the Configure Site Map tab to configure a site map options or create a custom site map.

Plugins

The Operations Master service is used to manage and configure plugins. Plugins are Desktop Authority provided objects that the Manager uses to perform specific operations. There are a few default plugins that are necessary for Desktop Authority to collect data and report on it. The Operations Master service object is available exclusively to Super Users/Groups. Non-Super Users/Groups do not have the ability to open the Operations object.

The Operations Master service object list provides the ability to sort the list on any of the three columns, ascending or descending order. The order of the columns themselves can also be changed. Simply drag a column to its new desired location in the list.

Click on any plugin to select it. The Toolbar will become enabled with the necessary buttons.

Restart

Select this option from the toolbar to restart the selected service.

Edit

Click Edit to modify the selected plugins options.

Sync Reporting Data

Instead of waiting for the automatic Profile and RBA Audit data backup, click Synch Reporting Data to process reporting data right away. This button is only available when the ETLProcessor plugin is selected.

Refresh

Select refresh from the toolbar to update the plugins list.

Status legend

A green marker indicates that the plugin is currently running and there are no problems.

A yellow marker indicates that there is some problem with the plugin. The plugin may have either timed out or is not responding to requests. Select the problem plugin and click **Restart** to attempt to correct the issue with the plugin by reloading it.

A red marker indicates that this plugin is not currently running. Select the problem plugin and click **Restart** to start the plugin.

ETLProcessor

The ETL processor plugin manages the data collection processes. This plugin is a service that is installed and started when Desktop Authority is installed. This service should run regardless of whether the Manager is running or not. It helps to collect data as users' login and out of the network. Many other user operations are also logged.

User and Computer Data are collected by Desktop Authority's Operations Master service and the ETLProcessor plugin. Data Collection can be configured for both the User and Computer in their respective Data Collection objects. Computer Management Data Collection can be configured for hardware, software, and USB/Port Security. User based Data Collection can be configured for login/logoff and lock/unlock events.

There are several configuration parameters available for this plugin. Click Edit to modify the plugin details.

Collection thread sleep time

Specify the amount of time (in minutes) for the data collection and processing threads wait after they finish. The default sleep time is set to 15. Allowable values can be between 1 and 60 minutes.

Profile and role-based access audit data backup

Specify the time of day for the configuration data to be processed and moved to the Reporting database. Once the data resides in the Reporting database it can be reported on. Database maintenance is also performed at this time (removing old records), which is based on the *Retention period for database records* setting. The default time is set to 4:00 AM.

The Operations Service recycle time is automatically configured to be 15 minutes prior to the time specified here.

Purge malformed XML file imports

Specify the number of days in which malformed collection data files can be purged. The default value is set to 10 days but may be changed to any value between 0 and 30 days.

Retention period for database records

Certain configuration data tables grow at a very fast rate. This necessitates the ability to purge older data from the system. The default retention period is set to 180 days. This may however be set to any value between 0 and 360 days.

Save

Click Save to commit all changes to the ETLProcessor plugin configurations.

Cancel

Click Cancel to go back to the last saved values of all ETLProcessor plugin configurations.

Operations Master service

This service is a background service that is used to manage and configure Desktop Authority's plugins. These plugins are used to perform specific operations such as audit data collection and the execution of scheduled reports.

User and Computer Data is collected by Desktop Authority's Operations Master service and the ETLProcessor plugin.

Data Collection can be configured for both the User and Computer in their respective Data Collection objects. Computer Management Data Collection can be configured for hardware, software and USB/Port Security. User based Data Collection can be configured for login/logoff and lock/unlock events.

Select the Operations Master Service plugin by clicking on it. When selected, its color will be highlighted. Click **Edit** to change the service credentials for this plugin, Enter the User name and password credentials. The User name must be entered in the form of Domain\Username.

ⓘ Note: The Operations Master service requires a user account that belongs to the Domain Admins group.

ReportScheduler

The ReportScheduler plugin runs scheduled reports. This plugin runs every 10 minutes, by default, checking for reports to run. The timing interval may be changed in the Desktop Authority Setup tool.

Configure Site Map

Desktop Authority will attempt to connect to either the DA Administrative Service or the Update Service on the user's logon server (the server where slogic.bat is executed from, upon logon). If the requested service does not respond, or is not installed on that server, Desktop Authority will use a default site map to locate a server that has an active and responsive service. The default site map is created based on the information in the Server Manager list, and groups all servers to their respective site. The default site map will instruct Desktop Authority to attempt to connect with the service on one of the other server(s) that are listed in the same site as the workstation's site.

If for some reason, Server Manager does not include any servers within the workstation's defined site, or there is no available service to connect to in the list of servers on the site, Desktop Authority will then randomly select a server from the Server Manager list.

The default site map can be customized to utilize the enterprise's topology. Select **Custom** to customize the default site map settings.

DA Administrative Service/Update Service

Site map configuration

Automatic

Select this option to use the site map that is created by default by Desktop Authority. This option will try to locate a responsive service on the DA login server first, look to the default site map and check other servers on the same site as the workstation. As a last resort, Desktop Authority will randomly select a server from the Server Manager list.

Custom

Select this option to define a custom site map for specific to the enterprise's topology. Selecting this option will enable the Site Map grid and allow for changes to it. The default site map configuration will appear in the grid, before any changes are made.

Disable

Select this option to disable the site map functionality of Desktop Authority. When not using a site map, default or custom, Desktop Authority will first try to locate a responsive service on the DA login server. If the service does not respond, then a random server will be selected from the Server Manager list until a responsive service is found.

Client execution options

Check login server first (DA Administrative Service only)

This option is selected by default. This instructs Desktop Authority to check for a responsive DA Administrative Service on the login server first. The servers on the site of the workstation with the request will be recursed first.

Site recursion

This option will disregard any sites specified on a server entry. This will disable the ability to link the sites recursively.

Server caching

The use of server caching will force Desktop Authority to remember the last server where a responsive DA Administrative Service was found and to use that one for the next request, even if the next request is completed during another session. If this option is not selected, the cache will not be used. This will cause Desktop Authority to walk through the rules for finding a responsive service each time a request is made.

Server cache days

Enter the number of days the cache should be reset on. The default cache days are 5. This means, every 5 days, the cache will be reset (the servers will be walked through every 5 days). Enter 0 to disable the number cache days, and to always remember the last responsive server found.

Randomly failover if site server is not available

Select this box to have Desktop Authority randomly choose a server from the server manager list if all servers within the specific site fail to give a response to indicate that it is accessible.

Custom Site Map

Select **Custom** from the site map configuration options. This will present an editable grid, where you can build your custom site map.

Add/Edit/Delete site

Click **Add Site** to add a new site to the site map list. Select a known site from the drop list. Click **Edit Site** to edit the selected site. Click **Delete Site** to remove a site from the custom site map.

Select *DEFAULT from the drop down list to create a custom defined default site list. The custom defined default site list is one that is used as a catch all for any workstation that does not have a site defined for it. It is added to the custom site map with a site name of *DEFAULT.

When modifying the Site list (Add or Edit site mode), the Server/Site list will be available for modification. This is where the entries for the selected Site will be added.

Click **Add Server**, **Add Site**, and **Delete Entry** to update the entry list. An asterisk (*) will be automatically pre-pended to any site name in order to distinguish it from a server entry.

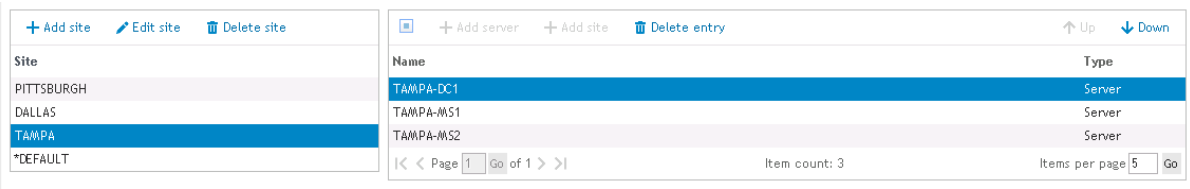
Click Save to save the Custom Map changes. Click Cancel to exit without saving changes.

Example Custom Site Map

Scenario 1

Let's assume first that Workstation124, in the Tampa site, makes a request of the DA Administrative Service. Since Workstation124 ran slogic.bat from server Tampa-MS1, DA will attempt to connect to the DA Administrative Service on Tampa-MS1.

Figure 27: Example site map



If the login server is unresponsive or the **Check login server first** option is unchecked, the site that the workstation belongs to will be discovered. The servers within the site will be checked in order until a responsive server is found. In this example, this means that the Tampa site will be discovered from the workstation. The next servers to be checked will be Tampa-DC1 and Tampa-MS2, respectively.

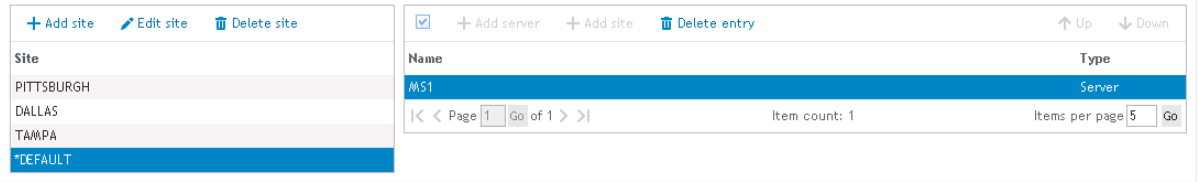
If all of the servers in the Tampa site fail, the example custom site map is configured to continue searching on the Dallas site. This is denoted with the Dallas site entry in the Tampa site map. However, if the Site recursion option is unchecked, the *Dallas entry in the site map will be disregarded.

If all sites and servers defined in the Tampa custom site map are exhausted, the default setting of the Randomly failover if site server is not available option (checked), takes over and servers listed in Server Manager will be randomly chosen until a responsive server if found. Keep in mind that no server will be checked more than once per request. If this option is not checked, a responsive server will not be found and the service request will fail.

Scenario 2

In this next example, Workstation1 makes a DA Administrative Service request. Workstation1 has no default site defined. Since Workstation1 ran slogic.bat from server MS3, DA will begin with an attempt to connect to the DA Administrative Service on the MS3 server. If the attempt fails, since there is no default site definition for the workstation, the servers specified for *DEFAULT will be used to look for a responsive service. Remember that the *Default site does not exist unless it was added to the custom site map by adding as a site.

Figure 28: Example site map



If the **Check login server first** is unchecked, the system will go right to the servers defined in the *DEFAULT section of the custom site map.

If the **Randomly failover if site server is not available** box is not selected, then the service request will immediately fail as the options do not allow the request to search for a responsive server.

Service Management

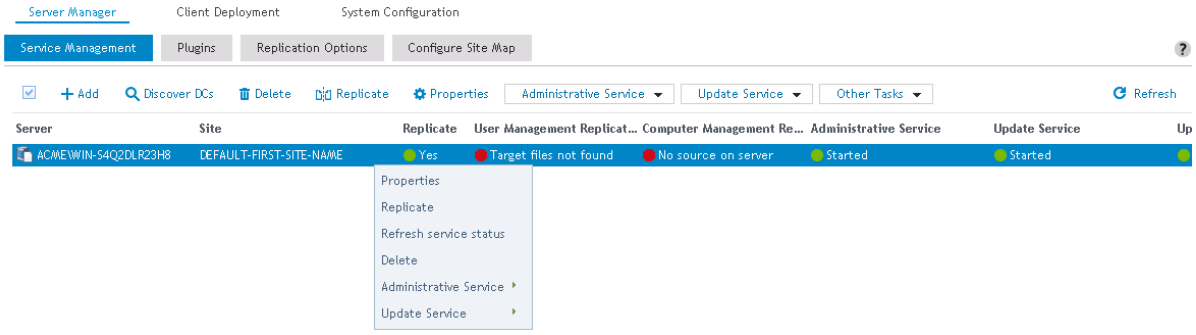
The Service Management object is a multi-threaded component that provides an interface to manage the Administrative Service, the replication process and the Update Service. Service Management is available exclusively to a Super User/Group. Non-Super Users/Groups do not have the ability to open the Service Management object.

Since the topology of each network is different it may be advantageous to execute Desktop Authority from locations other than your domain controllers. Server Manager implements a distributed management technology that allows you to delegate control of server configurations. One or more servers are assigned the responsibility of hosting the DA Administrative and Update services as well as acting as a replication partner for the published Desktop Authority configuration files.

Service Management grid

The Service Management grid details the status of each server utilized by Desktop Authority, including the status of the Administrative and Update Services and the replication status of configuration files. Using this grid, the status of service(s) and replication can be monitored for all servers at a quick glance. You can start, stop, configure, install and remove the Administrative and/or the Update Service on one or more servers from this single location. Replication is also be managed from this simple grid. One or more servers can be defined as a target for replication.

Figure 29: Service Management grid



Columns

Server

This is the server name. It is specified as Domain/Server Name.

Site

This column denotes the defined site name of the associated server. Workstation requests are directed to servers within the same site if possible. Using the Site helps to provide more efficient processing.

Replicate

User/Computer Management replication status

These two columns show the last time the User and/or Computer Management files were replicated. Information about Replication and its different status's is shown below.

Administrative/Update Service

These columns display the status of the service, whether it is started, stopped, installed or not installed. Click the respective toolbar button to configure each service.

Update Service connection status

This column provides the ability to view the Update Service log files.

Update Service type

This column displays how the Update service is being used on its respective server.

A server configured as a Distribution server is one that will receive MSI's. from a Distribution/Download server in order to deliver requested files to client computers.

A Distribution/Download server is one that will download MSI's. from the Internet and then deliver them to client computers.

User/Computer Management location

This column designates the replication folders. The folders will differ for User Management and Computer Management.

Download server

For a server that is configured as a Distribution server, this column displays the name of the preferred download server to get the MSI's from.

Service management toolbar

Add

All domain controllers should be listed in the Server Manager grid. If there are any missing from the list, click **Add** to update the list.

After choosing to add a server, traverse through the resource tree to locate the server to be added to Server Manager. Click  to expand or contract the server list. Highlight the server and click **Ok**.

Discover

Click **Discover** to force Server Manager to examine the network for existing domain controllers. Depending on the number of domain controllers and their geographic diversity over WAN links, this may take some time. Click **Add** to manually add a domain controller that is not automatically discovered.

Delete

Select one or more servers and click **Remove**. This is useful if a domain controller is removed from the network.

Replicate

Select one or more servers and click **Replicate**. This will publish the necessary files to selected servers.

Properties

Click **Properties** to configure one or more servers. Here you will be able to set the User/Computer replication target for the server. You will also be able to change the status of the Administrative service and the Update service.

Administrative Service

Clicking this button will drop down a list of actions that can be performed with respect to the Administrative service. This includes Start, Stop, Remove, Edit properties, Install or Restart the service. These actions will be performed on all of the selected servers. Selected servers are highlighted in a yellow color.

Update Service

Clicking this button will drop down a list of actions that can be performed with respect to the Update service. This includes Start, Stop, Remove, Edit properties, Install or Restart the service and Edit LAN settings as well as View Connection Status. These actions will be performed on all of the selected servers. Selected servers are highlighted in a yellow color.

More Operations

Select the More operations button provides access to the Test signature and View replication log action items.

Signatures validate the integrity of Desktop Authority definition and configuration files. **Test signature** is used to verify the various file signatures. It will first verify that the Signatures Public Key (stored in %Program Files%\Quest\Desktop Authority\Desktop Authority Manager\slsrvmgr.ske file) is the same on each server that has the DA Administrative Service installed. The signature is stored in the registry of each server as a hidden value.

Next, the signatures of the files in the NETLOGON share are check. This includes the .SLP, .SLD and .SL files. Following this, the Computer Management file signatures are tested. These files are found in the \SYSVOL\<domain name>\Policies\Desktop Authority\Device Policy Master folder.

Select **View replication log** to view the steps taken during the replication process.

Import servers from slsrvmgr.ini allows the Server Manger configuration from a backup on another server or a previous version to be imported into the current Server Manager. This serves as a way to automatically populate a large list of servers without having to do so manually.

Refresh

Click **Refresh** to update the status of each server in the server manager grid. Each server is inspected for services as well as the Desktop Authority configuration file. The grid is updated with the current status of each.

Managing servers

Servers can be added to or removed from the grid using the **Add**, **Discover** and **Remove** buttons.

To modify one or more servers in the grid, right-click on a single server or multi-select several servers and right-click to access a popup menu with common tasks to perform as shown below. The popup menu contains several actions that are also available on the Service Management toolbar.

Multi-select servers in the Server Manager grid by using the Shift or Ctrl key in combination with a mouse click. To select multiple elements, hold down the CTRL key while clicking the individual servers to select. Consecutive servers in the grid can be selected by clicking the first server to select and then, while holding down the SHIFT key, clicking the last server to select. To select the entire list of servers select the checkbox to the left of the Server column header. This box will be empty if no servers are selected and will be filled with a square if some servers are selected. A server's selected status may be changed by clicking on it.

Select **Refresh service status** to update the status of the services for each selected server in the server manager grid. Each selected server is inspected for services as well as the Desktop Authority configuration file. The grid is updated with the current status of each.

Managing services

The Administrative Service and Update Service menu items allow for the services to be managed. The same options are also available by right-clicking on the server and choosing the service menu item.

The service columns are color coded to show its current status.

Service status codes legend

 The service is installed, started and up to date on the server. *Started* will be displayed.

 The service is installed and started on the server but is not reporting its status to the server.

 The service is installed, started and outdated. *Service outdated* will be displayed. Server Manager will typically prompt you to update outdated services.

 The service is currently installed, stopped and up to date on the server. *Stopped* will be displayed.

 The service is not installed on the server. *Not Installed* will be displayed.

 The service has not reported its status to the server within an acceptable time frame and a manual refresh was not initiated. *Status Unknown* will be displayed.

 The service is currently being queried for its current status.

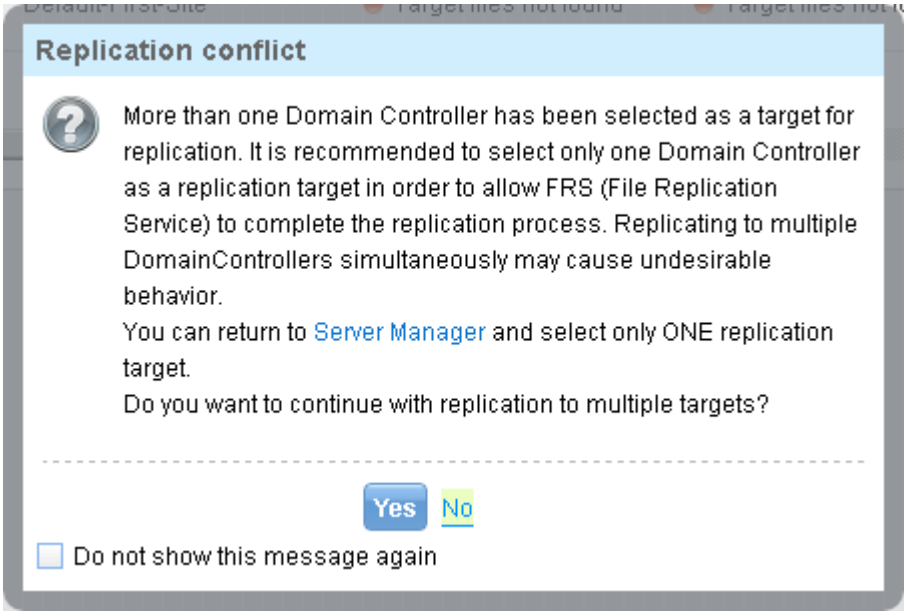
Replication

Desktop Authority uses replication to provide a method of publishing Desktop Authority configurations to domain controllers. Desktop Authority does this with its own replication process from within the Server Manager. Server Manager sets the configuration of the replication process on the Server Properties tab within the Service Management dialog. Desktop Authority's replication can be used to replace Windows Directory Replication services or work in conjunction with it. Of course, if Desktop Authority is your only logon script, there is typically no need to add the overhead of Windows' replication process to your domain controllers. Each time changes are made to your configuration using the Desktop Authority Manager, you will save the changes, replicate and then exit. By default, only the changed files will be replicated.

Clicking the **Replicate** button marks the target folder on a server as a location that will host Desktop Authority's configuration files when publishing. Normally the target path for replication is the NETLOGON share of your domain controllers but this can be changed in the *Server Properties* dialog. This is the path that Desktop Authority is executed from during logon. When you check the target box, Server Manager verifies that the target path exists; if not the directory will be automatically created.

It is recommended that only 1 domain controller be selected as a replication target. Desktop Authority will publish the necessary files to this DC. NTFRS will take care of replicating the changes to all other domain controllers. If more than 1 DC is chosen, it is possible that the replication by Desktop Authority and the NTFRS replication will collide resulting in morphed folders and other possible problems. Choosing 1 domain controller also allows for easier troubleshooting. Do not choose more than 1 server in order to speed up the replication process. If the process must be expedited, allow it to replicate to a single server and then force the NTFRS replication to occur within Active Directory. Choosing multiple replication targets will cause a warning message to be displayed upon replication.

Figure 30: Replication target warning dialog



This message will be displayed at the start of the replication process, if multiple domain controllers are selected as replication targets, for the user initiating the replication process. Click the **Do not show this warning again** to disable the message box from appearing again for the user and machine. This setting is saved in the HKEY_CURRENT_USER registry hive, so disabling the warning message on one computer will not disable it for all computers.

Select **No** to change the replication targets to a single one.

Select **Yes** to confirm that you wish to continue with the selection of multiple replication targets. This may cause folder-name conflicts during NTFRS replication.

Select **Do not show this warning again** to disable the message from appearing during subsequent replications for a given user.

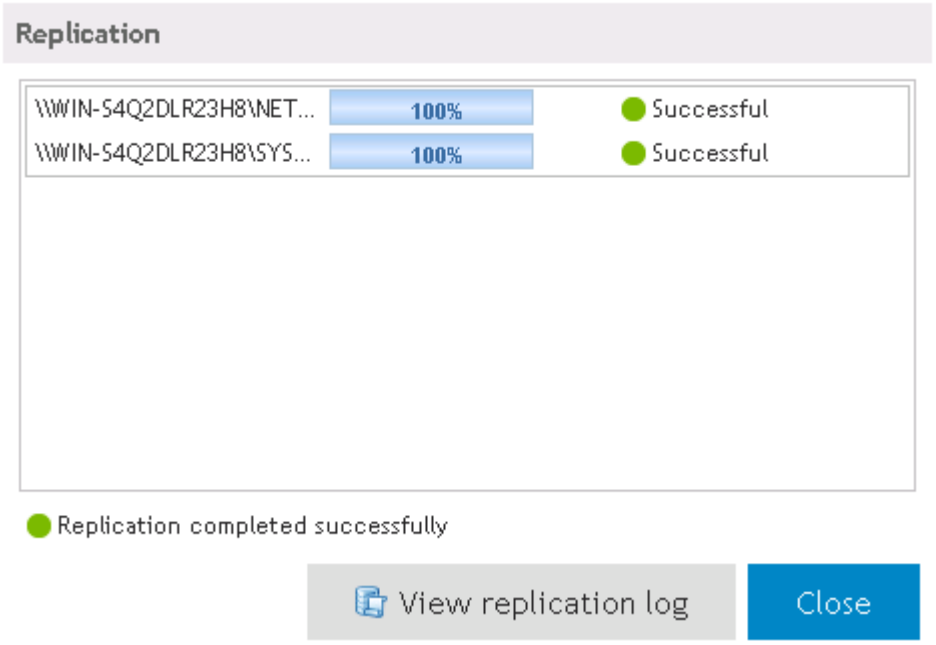
When you install Desktop Authority, a default source distribution system is created. The Domain Controller that you installed the program to (otherwise known as the Operations Master) holds the Desktop Authority Manager program files and acts as the source (or master) location for your script files.

The **Replication Status** column in the Server Manager grid is updated continually and shows when, or if, each server was last replicated to. The target path is first verified for existence and then queried to determine the date and time the Desktop Authority files were last updated.

Server Manager uses intuitive colored icons to represent the status of replication in the User Management Replication Status and the Computer Management Replication Status columns on each server.

When replication is complete, the replication status dialog will show a successful status for each target. A replication log is also available to view by clicking on the **View replication log** button. The replication process may be canceled during the process by clicking the **Cancel** button. Click the **Close** button to complete the replication process.

Figure 31: Replication status dialog



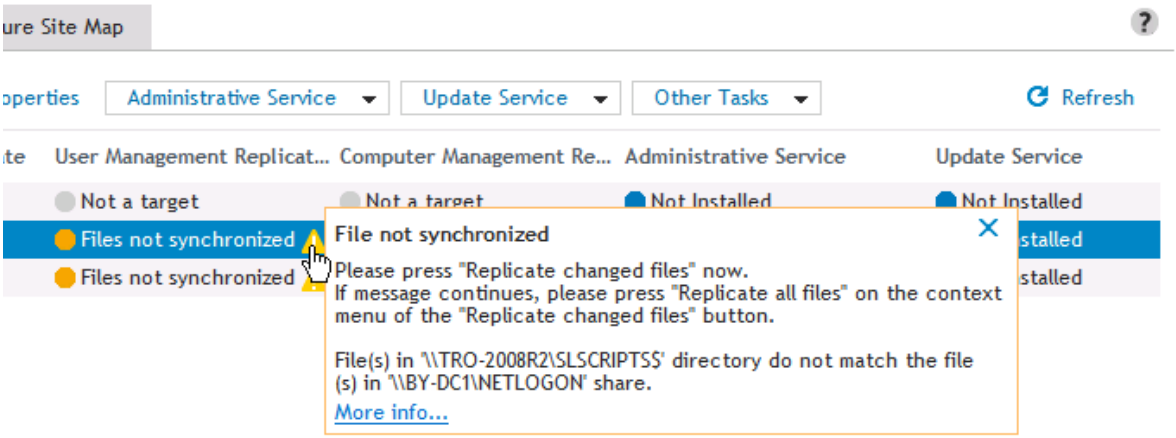
Replication status legend

A gray status indicates that the server is not configured to be a replication target or when there is not Administrator Service installed.

A green status indicates that the files in the target folder are in sync with the files in the Operations Master. All Desktop Authority configuration files on the server match the date and timestamp of the configuration files on the source domain controller. The date and time of the last replication is displayed.

A yellow status indicates that the files in the replication target folders are outdated. One or more files are missing from the target or different versions of these files exist on the Operations Master. Desktop Authority configuration files have been updated on the source domain controller, however, the changed files may not have been replicated to this server. The two folders being compared will be displayed when clicking on the warning icon.

Figure 32: Replication target folder outdated warning



A more detailed list of files can be displayed by clicking on the More Info link in the warning message.

A red status indicates that this server is a Target but no files are found in the target folder. Since this server is a Target, replication should occur for this server. The message "*Target files not found*" is indicated.

A blue status indicates that this server is currently in the process of replicating to its target. The message "Replication in progress" is indicated.

Replication options

The Replication Options dialog box provides several options and preferences.

Options

Source server

Specify the server that the Desktop Authority configurations are replicated from. By default, this is where the Manager is installed to.

User Management source folder

Specify the folder that User Management configurations are replicated from. By default, this is the NETLOGON location, shared by the installation as SLSCRIPTS$.

Computer Management source folder

Specify the folder that Computer Management configurations are replicated from. By default, this is the DADevicePolicyMaster$ share.

Include hidden and system files

Select this check box to include all hidden and system files that exist in the source folder in the replication copy. Clear this check box to leave all hidden and system files in the source folder.

Overwrite read-only files

Select this check box to overwrite any files marked as read-only in the destination folder with a new file from the source folder. Clear this check box to leave all original read-only files intact.

Include subdirectories

Select this check box to include all sub-folders found in the source folder in the replication copy. Clear this check box to suppress the copy of sub-folders.

Continue after errors

Select this check box to continue to replicate files even if an error occurs while copying files. Clear this check box to stop replicating files if an error occurs.

Preferences

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

Default User Management replication target location

Specify a folder that will hold the User Management replicated configurations. By default, this is the NETLOGON share.

Default Computer Management replication target location

Specify a folder that will hold the Computer Management replicated configurations. By default, this is the SYSVOL\[*Domain*]\Policies\Desktop Authority\Device Policy Master folder.

Server properties

Click **Properties** in the Server Manager grid to display the server properties. Once the Server properties are displayed, click **Edit properties** to modify them.

Status

User Management replication status

Displays the last date and time User Management files were replicated to the server.

Computer Management replication status

Displays the last date and time Computer Management files were replicated to the server.

Properties

User replication target

Select this box to make the server a User Management replication target. When User Management configurations are published, this server will host the Desktop Authority's configuration files.

User Management replication folder

Specify a folder that will hold the User Management replicated files.

Computer replication target

Select this box to make the server a Computer Management replication target. When Computer Management configurations are published, this server will host the Desktop Authority's configuration files.

Computer Management replication folder

Specify a folder that will hold the Computer Management replicated files.

Status refresh period

The amount of time each service will use to report back to Server Manager about its status. This time period is specified in seconds and defaults to 5 seconds.

Description

Enter a description to annotate the server. This may be the server location or any additional information you may need about this server.

DA Administrative Service

Select the DA Administrative Service tab to manage the service and change the log on credentials.

Update Service

Select the Update Service tab to manage the service and change the log on credentials.

Service options

Start

The Start Service action is available when at least one stopped service on one or more servers is selected. On the **Service** menu, click **Start** to start the service(s). Optionally, right-click on the selected cells in the server manager grid and select **Start** from the shortcut menu.

Stop

The Stop Service action is available when at least one started service on one or more servers is selected. On the **Service** menu, click **Stop** to stop the service(s). Optionally, right-click on the selected cells in the server manager grid and select **Stop** from the shortcut menu.

Restart

Restarting a service will simply stop and then start the selected service. This is available when a started service on one or more servers are selected. On the **Service** menu, click **Restart** to restart the service(s). Optionally, right-click on the selected cells in the server manager grid and select **Restart** from the shortcut menu.

Reinstall

Install performs the installation of the current version of the selected service. The DA Administrative service may be installed to multiple servers at the same time.

Install is available when a selected cell has a service that is *Not Installed*. On the **Service** menu, click **Install** to install the service(s). Optionally, right-click on the selected cells in the server manager grid and select **Install** from the shortcut menu.

Remove

Remove will remove the selected service from the server on which it is installed. The DA Administrative service may be removed from multiple servers at the same time.

Remove is available when one or more started or stopped services on one or more servers are selected. On the **Service** menu, click **Remove** to remove the service(s). Optionally, right-click on the selected cells in the server manager grid and select **Remove** from the shortcut menu.

Update Image

Update image performs the update of existing and currently running service(s) that are outdated. One or more services may be updated at the same time.

Update Image is available when a selected cell has an installed service that is either started or stopped and is outdated. On the **Service** menu, click **Update image** to update the service(s). Optionally, right-click on the selected cells in the server manager grid and select **Update image** from the shortcut menu.

Refresh

Refresh will update the service status based on a real-time inquiry to its status.

What is the DA Administrative Service?

Conventional scripts typically execute under the security context of the user logging on. Unless users are made administrators of their own machines, the ability to perform administrative tasks through a centralized logon script will be limited to each user's rights on their computer.

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 is used on each server 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.

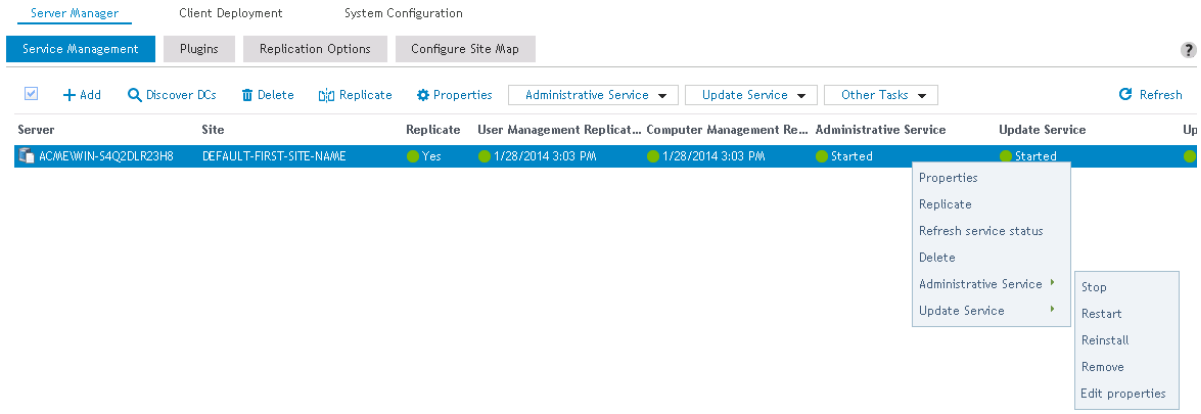
The Client User account (client side service) is used on each workstation to make registry changes, install software, add printers, synchronize time and perform any other task that may require elevated privileges during the logon, logoff or shutdown events. The Client user account should be a member of the Domain Users group.

Installing this service to all domain controllers is the preferred action for this service and provides the best configuration for load balancing.

Configuring the Administrative Service

To configure the Administrative service in the Server Manager grid, click **Properties** for the server that the service will be configured for. The service can also be managed by selecting **Properties** in the service drop list in the DA Administrative Service column.

Figure 33: Configure the Administrative Service



Administrative Service

Edit properties

Click **Edit properties** to edit the Service configuration and credentials.

Status

The status of the DA Administrative service can be managed by clicking the **Start**, **Stop**, **Restart**, **Reinstall** and **Remove** buttons. Click **Refresh** to update the Service status.

The DA Administrative Service requires two unique users accounts. Please provide one user account belonging to the Domain Admins group and one belonging to Domain Users group.

Service credentials

Log on as

Enter a Domain Admin account that the service will use to log on. This should be entered in the format of *Server\UserAccount*. Optionally, click **Browse** to select a user account.

Password

Enter the password associated with the selected log on account.

Note: The new logon credentials will not take effect until you restart the service.

Client service (domain user)

Log on as

Enter the Domain User account that the service will use to log on. This should be entered in the format of Server\UserAccount. Optionally, click **Browse** to select a user account.

Password

Enter the password associated with the selected user account.

Service configuration

Startup Type

Select from *Automatic*, *Disabled* or *Manual* from the Startup Type list.

Automatic will start the service immediately after it is installed.

Disable will stop the service if it is running and disable the service from being run in the future. To use this service at a later time, the Startup Type must be changed to either Automatic or Manual.

Manual will allow the service to be started at the administrators' discretion. The service will never be started automatically.

Log files repository

Specify a folder to hold intermediate data collected for reporting. Data is collected as users login and out of the network and includes user, hardware and software inventories and much more. During specific timed intervals, data is collected from this folder and parsed into the DAREPORTING database.

The default path is %programfiles%\Quest\Desktop Authority\ETL Cache\. Please refer to the File Paths appendix for the correct path(s) based on the version of Desktop Authority you are using.

The folder specified must be a folder on the server for which the service is being configured for. Click **Browse** to locate the folder.

Save/Save and restart/Cancel

Click **Save** to save the updated service credentials. The service must be restarted by clicking the Restart status button.

Click **Save and restart** to save the updated service credentials and automatically restart the service.

Click **Cancel** to reject the credential changes.

What is the Update Service?

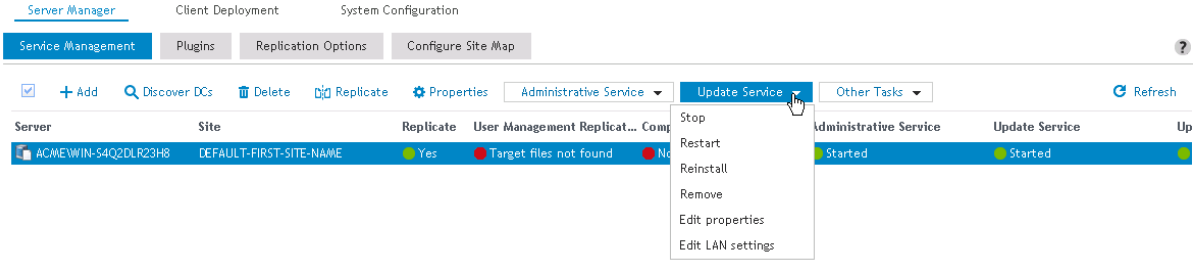
The Update Service is used by the USB/Port Security and Software Management objects. This service interfaces with Quest owned and third party websites in order to retrieve licensing information. The Update Service offers an encrypted and secure connection to the web site.

If a proxy is used to access the Internet, each server designated as an Update server must be configured to work with the proxy.

Configuring the Update Service

The Update Service is used by the USB/Port Security and Software Management objects. To configure the Update service in the Server Manager grid, first select the server that will be updated. Next click on the Update Service drop menu and then choose the selected action from the menu. The Update Service can also be managed by right-clicking on the server and choosing Update Service.

Figure 34: Configure the Update Service



Update Service

Status

The status of the Update service can be managed by clicking the **Start**, **Stop**, **Reinstall** and **Remove** buttons. Click **Refresh** to update the Update service status.

Edit properties

Click **Edit properties** to edit the Service configuration and credentials.

Import updates

Click the **Edit properties** button to edit the Service configuration and credentials.

Service credentials (domain admin)

Click the **Edit Properties** button to edit the Service configuration and credentials.

The Update Service is used by the USB/Port Security and Software Management objects.

Log on as

Enter a Domain Admin account that the service will use to log on. This should be entered in the format of `Server\UserAccount`. Optionally, click the Browse button to select a user account.

Password

Enter the password associated with the selected log on account.

Startup type

Select from *Automatic*, *Disabled*, or *Manual* from the Startup Type list.

Automatic will start the service immediately after it is installed.

Disable will stop the service if it is running and disable the service from being run in the future. To use this service at a later time, the Startup Type must be changed to either Automatic or Manual.

Manual will allow the service to be started at the administrator's discretion. The service will never be started automatically.

Add an exception in Windows Firewall for this service

If this service will be deployed to a server behind a firewall, select this box so an exception can be added in Windows Firewall for this service. This exception can be added manually as well.

Note: The new logon credentials will not take effect until you restart the service.

Updates cache

Download server

For servers that are not configured to download updates, specify the server where the update files will be located. Select Auto from the list to allow the update files to be located automatically when needed.

Allow this server to download updates

Select this check box to enable the Update Service to download selected updates to this server. Downloads will be stored in the specified download directory. Clear the box to prevent the service downloading updates to this server. This option is only available when the Update Service is installed on more than one server.

Download cache directory

Specify the directory to which all updates will be downloaded to. This directory specification is only available when one Update Service is installed or on servers which are configured as Download servers. The default download directory is `%Program Files%\Quest\Desktop Authority\Update Service\Cache`. Please refer to the File Paths appendix for the correct path(s) based on the version of Desktop Authority you are using.

Poll period (hours)

Specify how often the Update Service should look to Quest for updates.

Click **Save** to save the service properties. Click **Save and Restart** to save the server properties and restart the service with its new settings.

Local Area Network (LAN) settings

Note: Local Area Network settings are only available for the 'Started' service.

Click **Edit LAN Settings** to configure the use of proxy server settings. LAN Settings can only be configured when the Update service is installed and started. The settings are enforced on the server where the service is installed to, for the specific service account user.

Automatic configuration

Automatically detect settings

Check this box to automatically detect the proxy server settings at the time of connection.

Use automatic configuration script

Check this box to use a configuration script to configure the proxy settings.

Script location

Type an address (URL) or file name that will be used to configure the proxy settings for Internet Explorer.

Proxy server

Use a proxy server for this connection

Check this box to enable the use of a proxy server.

Use the same proxy for all protocols

Select this box to enable the use of a single proxy address for all server protocols (HTTP, Secure, FTP, Gopher, Soks)

Proxy address to use

Desktop Authority supports several protocols including HTTP, Secure, FTP, Gopher and Soks. If the server is using a proxy, these protocols can be configured to work with different proxy addresses if needed. Enter the specific proxy address (TCP/IP address or host name of the proxy server and port (TCP/IP port number) for each protocol. If a only one proxy address will be used, be sure to select the **Use the same proxy for all protocols**.

Bypass proxy for local addresses

Select this check box to ignore the proxy server for local addresses. Clear this check box to use the proxy server for all Internet addresses.

Exceptions

Enter any local addresses for which the proxy should not be bypassed.

Proxy credentials

Username

Enter the user name needed to access the proxy.

Password

Enter the password needed to access the proxy.

Confirm

Enter the password again to confirm its spelling.

Click **Save** to save the LAN Settings. Click **Cancel** to exit LAN Settings without changes.

System Configuration

The Preferences dialog presents several options that are used to configure the Manager’s settings. Select Preferences... from the File menu on the Manager's menu bar.

Domain Controller

Enumerate resources from this domain controller

This setting tells Desktop Authority to use a specific domain controller in order to enumerate Group and User information. Click **Edit** to modify the Domain Controller setting.

A Domain Controller may be selected by clicking **Browse**. Remove the selected server from the field to allow the network to decide which domain controller to query for necessary resources.

Click **Save** to confirm the updated setting. Click **Cancel** to abandon the changes.

Import custom options

Click **Browse** to import a custom INI file that will add new values to drop lists in the Alerts, Logging, MS Office, Common Folder Redirection, Security Policies, Service Packs, Folder Redirection and Shortcuts objects.

Off-Network Support

Off-Network Support (ONS) allows a computer previously provisioned with Desktop Authority to continue receiving configuration updates while off-network. A computer that is considered to be off-network may have an Internet connection but the company network is unreachable.

To use this feature, Off-Network Support must be configured in the Desktop Authority Manager.

Off-Network Support is accomplished by using Desktop Authority's Replication capabilities. Configuration and necessary files are replicated to a configured Internet cloud service; currently Desktop Authority supports Amazon Web Services (AWS) and Microsoft Azure.

IMPORTANT: Prior to configuring ONS (Off-Network Support) within the Desktop Authority Console, you will first need to access the web portal for your intended cloud storage provider (AWS or Azure) to create the appropriate storage container(s). Visit the video help link on the ONS configuration page to access a Knowledge base article containing information on the necessary pre-configuration steps for both AWS and Azure usage.

TIP: To prevent any unwanted dialogs or errors when off-network, the special SLBYPASS option file should be used. To configure this option refer to Special Option Files.

Off-Network support Configuration

Edit

Click **Edit** to manually configure or manage Off-Network support settings.

Check connection

Click Check Connection to confirm that Desktop Authority can connect to the selected Off Network Storage Provider.

Off-Network support

Select this Off-Network support box to enable and configure Off-Network support.

Off-Network provider

Select an Off-Network provider from the drop list. Currently Desktop Authority supports Amazon Web Services (AWS) and Microsoft Azure.

Amazon Web Services (AWS)

S3 Bucket Configuration

Auto Configure AWS

Click **Auto Configure AWS** to allow Desktop Authority to automatically configure the Off-Network support configurations.

Bucket Name

A Bucket is similar to a folder. This will be where the Desktop Authority files will be stored.

Region

Select the AWS geographic area.

Access Key for Manager Console/Clients

AccessKeyId

Access keys are assigned to your AWS account to allow programs to programmatically access your account. Amazon allows a maximum of 2 Active keys and recommends that they be changed every 90 days.

SecretAccessKeyId

Access keys are assigned to your AWS account to allow programs to programmatically access your account. Amazon allows a maximum of 2 Active keys and recommends that they be changed every 90 days.

Configuring AWS Off-Network Support

1. Click **Edit** and select Amazon Web Services (AWS) as the Off Network Provider.
2. Click **Auto Configure AWS** to automatically configure Off-Network Support or manually configure the settings.

   Using either the Autocreate or manual configuration options will require a copy/paste of the AccessKeyId and SecretAccessKeyId. The main difference in the operations is the Bucket.

   Autocreate will create a dedicated bucket for the Desktop Authority files. After the bucket is created, you MUST log in to AWS and define a region for it.

   When manually configuring Off-Network Support, a dedicated bucket must be created in AWS, with a region applied to it. It is recommended that this bucket be dedicated to Desktop Authority.
3. Enter the Access Keys for the Manager Console provided by AWS.
4. Enter the Access Key for Clients provided by AWS.

   NOTE: The Access keys will be used to access the Bucket.
5. Click **Save** if manually configuring ONS or Create if using the **Auto Configure AWS** option.

Microsoft Azure

Share Configuration

Share Name

The name of the storage folder within MS Azure where the replicated Desktop Authority configuration information will are stored.

NOTE: The configured share will automatically be created prior to replication, if it doesn't already exist.

Connection String for Manager Console

Connection string

The server-side connection string to connect to MS Azure storage. This connection should have Read/Write/List/Create/Delete access to the storage and is used by the DA Server Manager (server side).

Connection String for Clients

Connection string

The client-side connection string to connect to MS Azure storage. This connection should have Read/Write/Create access to the storage and is used by the DA Client (client side). This string can be the same as the connection string for the Manager Console.

Configuring Microsoft Azure Off-Network Support

1. Click **Edit** and select Microsoft Azure as the Off Network Provider.
2. Enter the name of the storage folder within MS Azure as the Share Name.

3. Copy and paste the Connection string from Microsoft Azure for the Manager Console. This must have Read/Write/List/Create/Delete access to the storage.
4. Copy and paste the Connection string from Microsoft Azure for the Clients. This must have Read/Write/Create access to the storage.
5. Click **Save**.

RM Gateway Configuration

The RM Gateway Configuration tab is used to configure the Off-Network Remote Management (ONRM) services which allow Desktop Authority to remotely control online computers that are currently disconnected from the corporate network. This feature extends the capabilities of the Desktop Authority Remote Management feature to support connecting to computers across networks.

NOTE: Desktop Authority's Off-Network Support (ONS) feature, used to push configuration updates to computers while they are remote and disconnected from the corporate network, is not required for the Off-Network Remote Management feature to work. However, having Off-Network Support enabled provides the added benefit of being able to deploy the Remote Management client (ExpertAssist) to both on and off-network computers that are joined to the corporate domain.

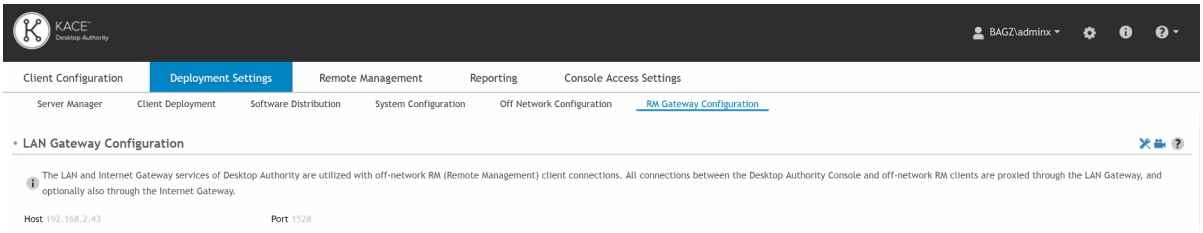
LAN Gateway Configuration

The LAN Gateway is used to transfer data between the Desktop Authority Console and Off-Network clients. The Host IP and Port specified here are read-only. They are the IP and Port that were specified during the installation of this feature through the Desktop Authority Installer or the DA Setup tool.

Internet Gateway Configuration

The Internet Gateway is a required component of the ONRM (Off-Network Remote Management) feature and is responsible for storing the external IP address and the port number used by remote RM clients while off-network. Optionally, the Internet Gateway can be installed on a machine with a public address and act as a proxy between the LAN Gateway and connections from external clients. However, for optimal performance, we strongly recommend the Internet Gateway be configured with the public/external IP address and Port of the network's router. From there, Port Forwarding can be used to route the associated traffic from RM clients directly to the LAN Gateway service (by-passing the Internet Gateway).

Enabling Off-Network Remote Management from the DA Setup Tool (or during Installation)

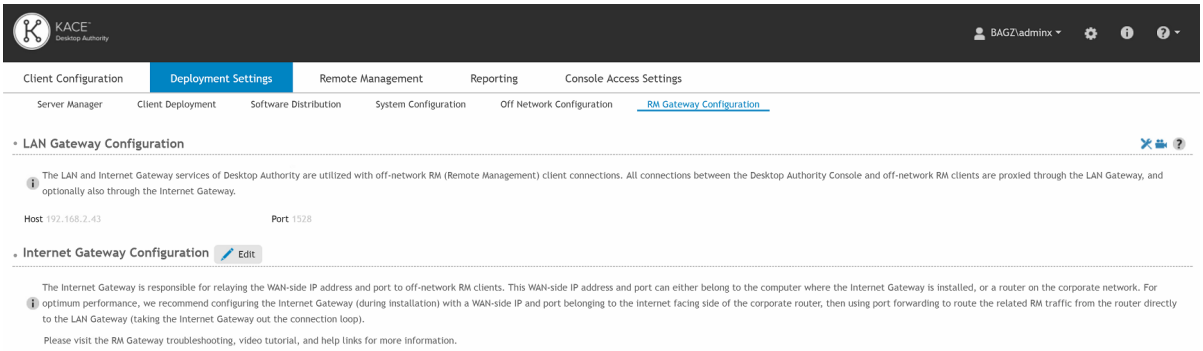


To configure the Internet Gateway click the **Edit** button. Enter the requested internal/private Host IP and listening Port. If you plan on installing the Internet Gateway on your Desktop Authority server, then just enter the IP for your Desktop Authority server and choose any open port.

The RM Gateway Configuration tab will only be visible in the Desktop Authority (DA) console if the Off-Network Remote Management feature was either enabled during the installation of Desktop Authority, or post-installation via the Desktop Authority Setup Tool.

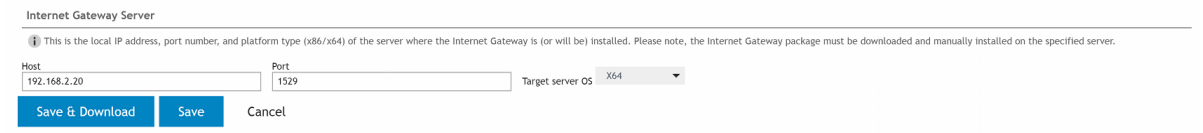
If the RM Gateway is not visible, please go to the ONRM tab of the DA Setup Tool and enable the feature.

Downloading the Internet Gateway installation package



In order to configure the Off-Network Remote Management feature, the Internet Gateway application needs to be downloaded and installed.

From the Internet Gateway section of RM Gateway Configuration tab, click the Edit button then enter the requested internal/private Host IP and listening Port.



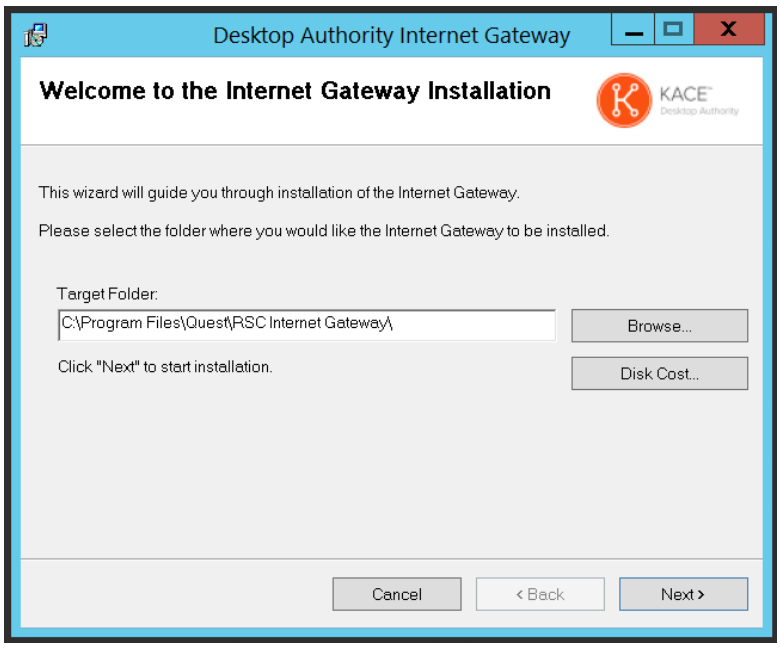
If you plan on installing the Internet Gateway on your Desktop Authority server, then just enter the IP for your Desktop Authority server and choose any open port.

Once the Internet Gateway's internally accessible IP/Port is configured, click the **Save & Download** button. You will be directed to download and install the Gateway via an installation wizard.

The Internet Gateway install will be downloaded to your machine. If you will be installing it on another computer simply copy this file over to the other computer. Otherwise, you can run the installation right away.

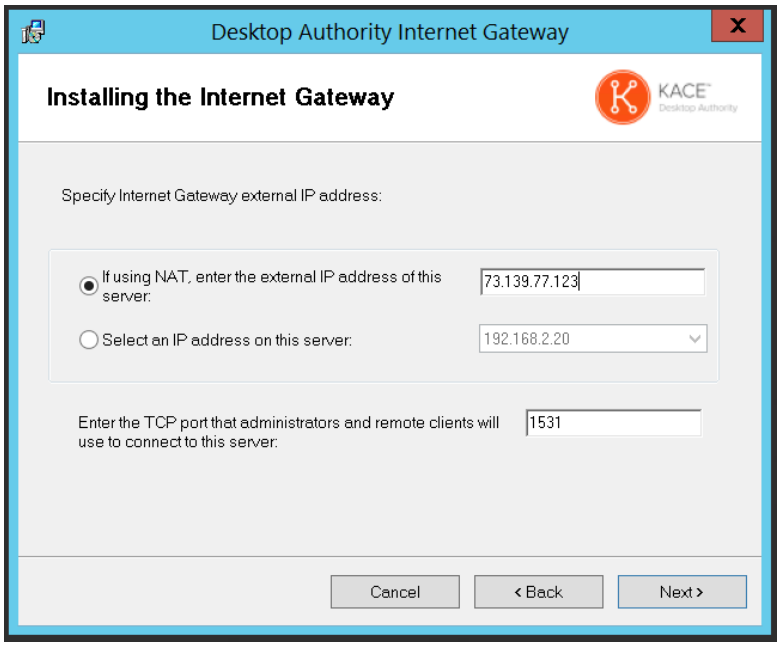
Installing the Internet Gateway

1. Launch the Gateway installer and enter the target installation folder.



   Click **Next** to continue.

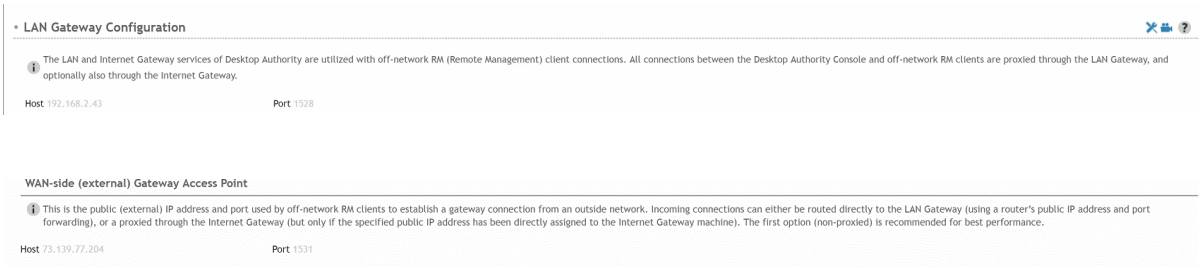
2. Next, a public, external facing IP address. This will be used when a remote client is connecting into the corporate network. If there is no external facing (public) IP address attached to a network adapter on the Internet Gateway server, then the NAT option must be used to specify the public IP address of your router (recommended for best performance).



3. Next, you must enter the TCP port that will be used by off-network RM clients when connecting back into the corporate network. Click **Next** to continue.
4. At this point you will be prompted to allow the Internet Gateway installer to create the necessary firewall entries for communication between the LAN and Internet Gateway services.
5. On the next page, click **Next** to confirm the installation. The installation will run and you will see an Installation Complete dialog when it is complete.
6. Once this process is complete, you **MUST save and replicate** these settings. Once the Gateway is installed you can come back to this tab to see the status of the Gateway.

Configuring Port Forwarding to the LAN Gateway

If the Internet Gateway was configured using the public address of a router, then the appropriate port forwarding must be created within the router's configuration in order for the Off-Network Remote Management feature to work properly. Specifically, any traffic being received on the configured Gateway Access Point Port (selected during the installation of the Internet Gateway) must be forwarded to the Host IP address and port of the LAN Gateway.



In the above example, 73.139.77.204 is the public IP address of the router and off-network RM clients will attempt to connect using port 1531 on that IP address. Therefore port 1531 will need to be forward to 192.168.2.43:1528 (LAN Gateway) within this router's configuration.

Internet Gateway Server

The Host IP address and Port shown here is the information about the server where the Internet Gateway is installed.

WAN-side (external) Gateway Access Point

The Host IP address and Port shown here is the information used by Off-Network clients to establish a connection from an outside network. This is the IP address and port used when installing the Internet Gateway.

NOTE: When using the Off-Network Remote Management (ONRM) feature it is highly recommended that you exclude all Quest installation folders from real-time AV/AM (Anti-virus/Anti-Malware) scans. Various AV/AM products have been known to drastically slow down and sometimes completely stop Desktop Authority processes (also potentially affecting the ExpertAssist remote management module).

Remote Management*

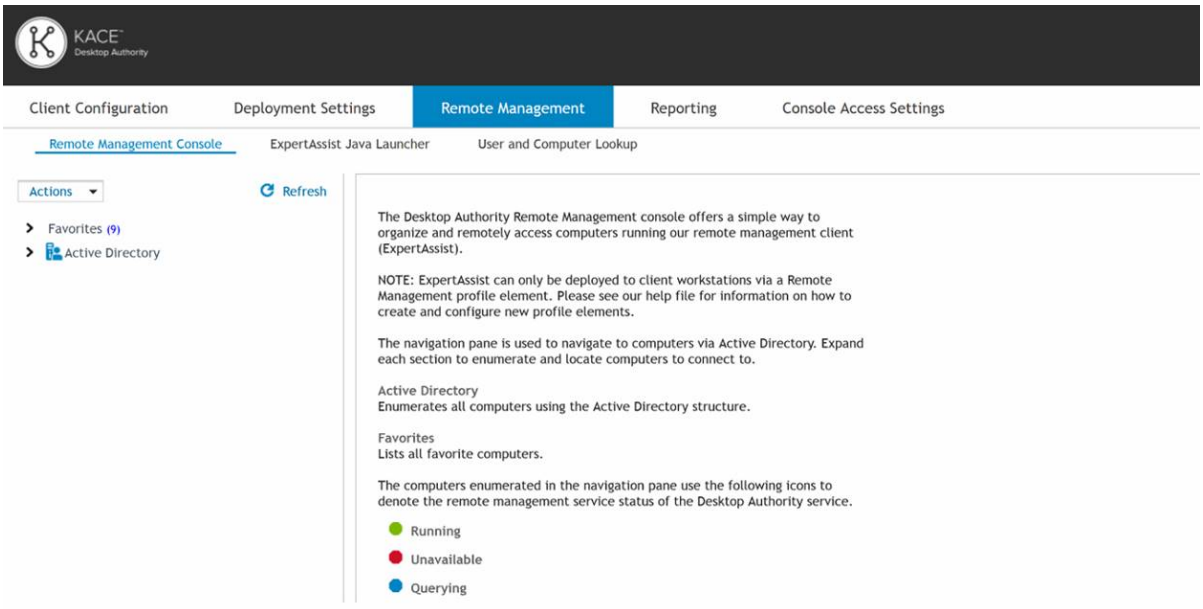
Desktop Authority Remote Management offers a simple way to remotely access multiple computers on the network for the purpose of remotely controlling and organizing computers running the Remote Management client (ExpertAssist).

Remote Management Console

Select this tab to remotely manage a computer running the Remote Management client.

Use the left side navigation pane to navigate through the Active Directory or Favorites and find the computer you will be connecting with. The right view pane provides the ability to establish a remote connection with a computer running the Remote Management client.

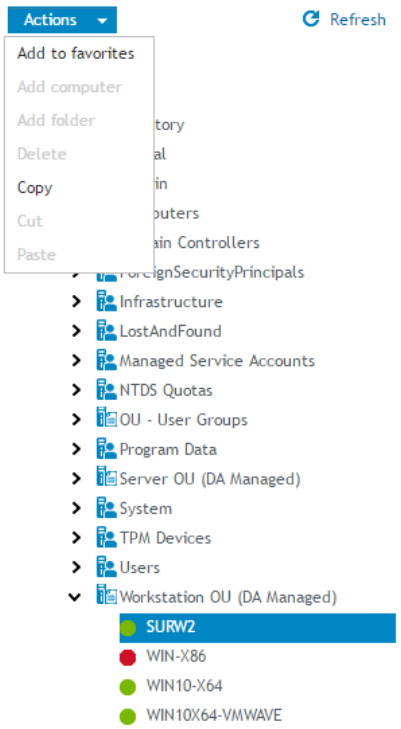
Figure 35: Navigation pane



The navigation pane displays a tree enabling a computer to be selected from Active Directory.

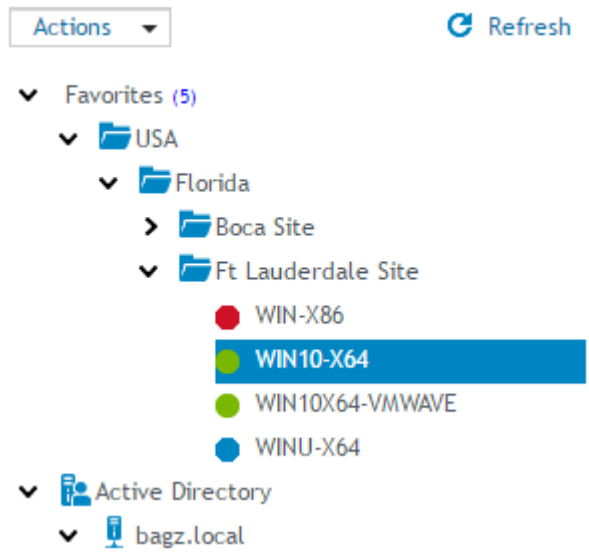
Once a computer is selected in the navigation pane, the Add To Favorites selection in the Favorites drop list is enabled. Click **Add To Favorites** to add the selected computer to the Favorites list. You can also add a computer to Favorites by utilizing the available drag/drop or copy/paste (right menu options) functionality. Use your Favorites for computers that are commonly accessed for Remote Management. **Add to Favorites** can also be selected by right-clicking on the computer in the navigation pane.

Figure 36: Manage Favorite computers



The favorites list displays computers that have been added to the favorites list from the Active Directory tree. The computers in the Favorites list lets you organize and quickly access the most frequently used computers. "Favorite" computers can be organized into folders by adding, moving, or deleting them.

Figure 37: Favorites list



The computers enumerated in the navigation pane use the following icons to denote the Remote Management service status.

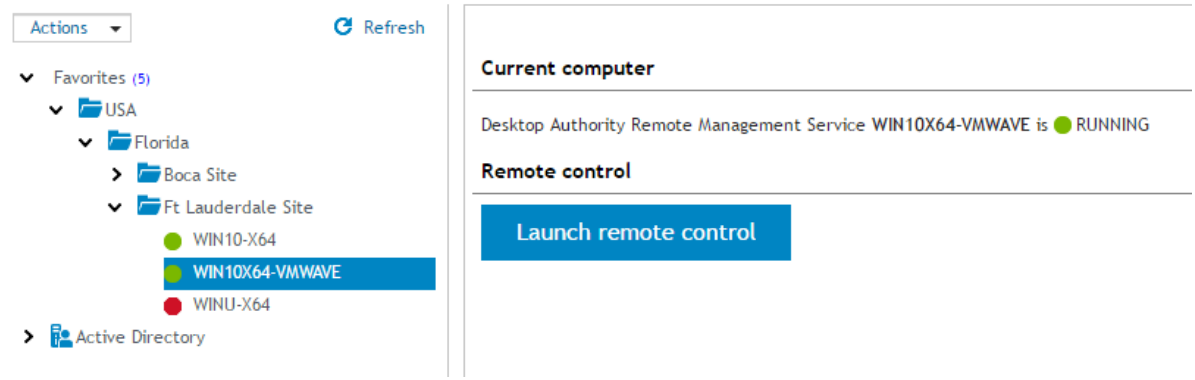
Table 3: navigation pane icons

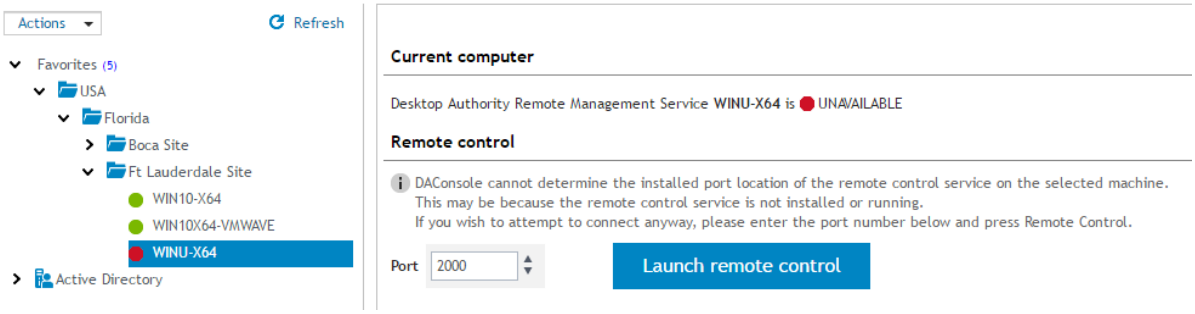
	Denotes the computer is running the Remote Management service.
	Denotes the computer is being queried regarding the status of the Remote Management service.
	Denotes the status of the Remote Management service on that computer cannot be determined.

NOTE: Network connectivity issues, target computer being offline, or the target computer's Remote Management Service not being started (or not installed), are a few possible causes of a status.

Once the computer is located, right-click on the computer name to access the available actions on the view pane.

Figure 38: Available actions for computer





Current computer

The Current computer section gives the status of the Remote Management service on the computer selected in the navigation pane.

Remote Control

Launch Remote Control

Once the Remote Management service is deployed to the client (via a Remote Management profile element), a computer status should be visible. You can then launch a remote control session using the **Launch remote control** button. When clicked, a new browser window will open with a logon to Expert Assist, the Remote Management client software.

*Note: This feature is not a standard part of Desktop Authority Essentials. To obtain this feature, Desktop Authority Essentials must be upgraded to the full version of Desktop Authority.

ExpertAssist Java Launcher

The Java Launcher provides an execution container for ExpertAssist's Java dependent functionality. Additionally, it is also responsible for automatically downloading and installing the OpenJDK version of Java if no supported Java version can be found on the host computer. Currently, both the Oracle JDK and OpenJDK version of Java are supported.

The Java Launcher must first be downloaded and installed in order to utilize any of the Java dependent features (e.g. Remove Control) of an ExpertAssist connection. Use the available **Download** link to download and install it.

User and Computer Lookup

Select this tab to quickly find a user or a computer to remotely manage. This tab provides shortcuts to the computer for easy access to remote management functionality.

The ExpertAssist Remote Management client MUST already be deployed (via a Remote Management element) to all computers being accessed via the User and Computer Lookup tab. Additionally, both User Data Collection (with "Collection logon and logoff session information" enabled) and Computer Data Collection (with Hardware, Software and Startup/Shutdown collection options enabled) must already be configured on these computers for the reporting component of the User & Computer Lookup feature to be fully functional.

To locate a recent session on a particular computer, enter the Computer Name and/or Username and click the **Lookup** button. Wildcards may also be used in the search field for either Computer Name or Username.

Examples of Search terms (Computer Name):

- IT* - All computers whose name begins with IT
- *ACCTG* - All computers whose name contains the string ACCTG

Examples of Search terms (Username):

- *SMITH - All users whose username ends with SMITH
- JBROWN - Only the user with the exact username of JBROWN will be displayed

To locate a computer or user using the Active Directory tree, click the **Browse** link under the entry field for Computer Name or Username.

The computers and/or users found via the lookup are displayed in the list below the search.

Shortcuts are provided for the following functionality:

- **Computer Information** - Click the Computer Name to view a report showing the latest hardware and software information collected for the associated computer.
- **Username information** - Click the Username to query Active Directory for the current user profile information for the associated user.
- **IP Info** - Displays the current IP address information for the associated computer.
- **Remote** - Initiate a remote control session to the associated computer.
- **Remote Management** - Initiate an ExpertAssist management session to the associated computer.
- **Remote Chat** - Initiate a remote chat session to the associated computer.
- **Remote Cmd** - Initiate a remote command line session to the associated computer.
- **SLTrace file** - Retrieve the latest SLTrace file from associated computer, for the associated user.
- **C: Drive** - Open a file browser session to the C Drive on the associated computer.
- **User Desktop** - Open a file browser session to the Desktop folder for the associated user, on the associated computer.
- **Registry Editor** - Open a registry editor session with the associated computer.
- **Services** - Open a services session with the associated computer.

By default, most User and Computer Lookup shortcuts require one login per machine (per session) to the ExpertAssist client running on the remote computer. However, for browsers that support automatic NTLM authentication for local sites, it is possible to avoid the need to enter credentials when using this feature.

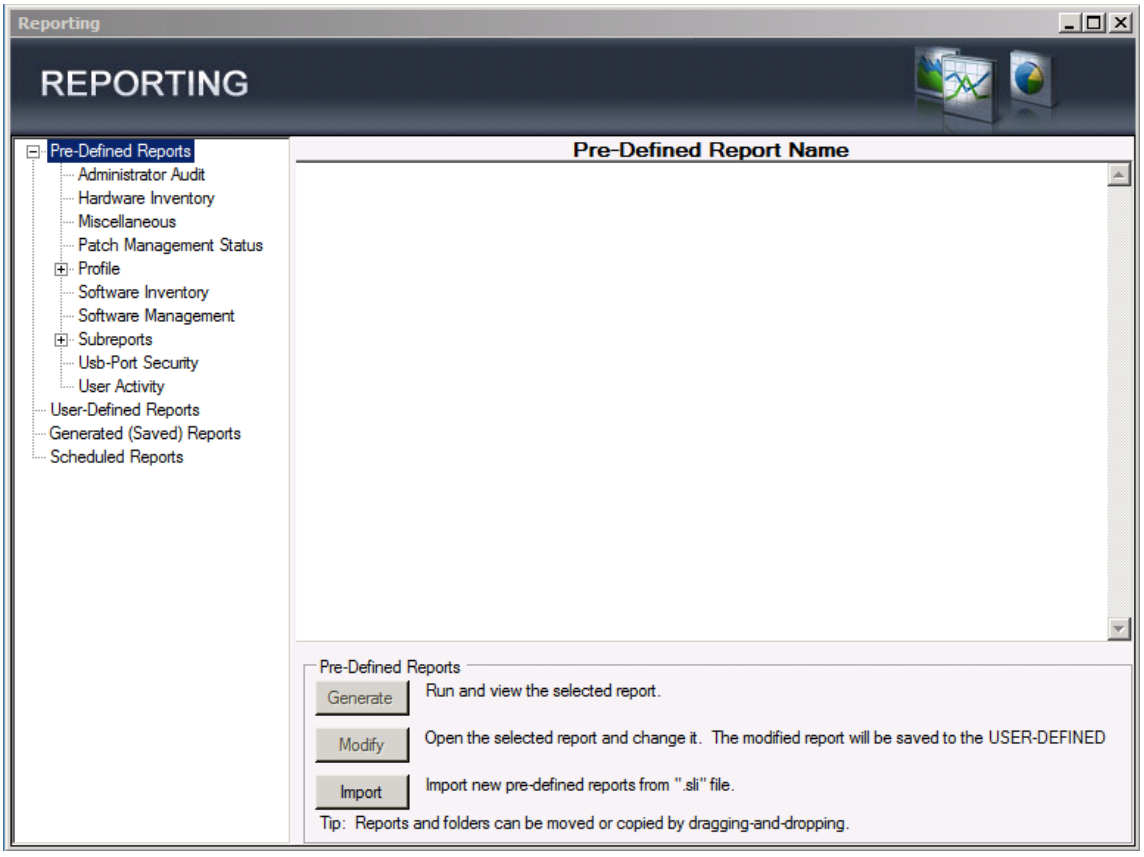
To do this you first need to enable NTLM for Remote Management (DA Setup Tool -> Remote Mgmt -> EA Connection Configuration -> Use the parameters in the URL -> Parameter string = /ntlm) and then configure your DA Console browser for automatic NTLM authentication. For example, in Firefox, the about:config setting network.automatic-ntlm-auth.allow-non-fqdn=True can be used to enable automatic NTLM authentication for all internal sites.

NOTE: Client computers must be turned on with network availability for all computer shortcuts to work.

Additionally, the ExpertAssist service must be up and running on the associated client computers. If this is not the case, some shortcut functionality will be disabled ("grayed out") and not available for use.

Reporting overview*

The Reporting object presents the opportunity to run predefined reports distributed with Desktop Authority™ or the ability to create custom reports. Reports can be run manually at any time or may be scheduled to run on a specific and/or recurring Date/Time.



Pre-defined reports

Select a report category from the Pre-Defined Reports tree. The Pre-Defined Reports object contains reports distributed with Desktop Authority. Click **Generate** or double-click a report in the report list to execute the selected report. Click **Import** to gather new report templates made available for Desktop Authority .

User-defined reports

Select User-defined Reports from the reporting tree. The User-defined Reports object lists reports that have been modified from the original supplied reports or newly created reports. Click **New** to create a new user-defined report or use the Wizard interface by clicking **Wizard**. Click **Modify** or double-click a report in the report list to open the selected report for changes. Click **Generate** to run and view the selected report. Click **Delete** to remove the selected report. Click **Import** to gather a user-defined .sli file into the user-defined report repository. Click **Export** to create a user-defined .sli file based on one or more reports in the user-defined report repository. User-defined reports can be categorized into separate folders. Click **New Folder** to create a new repository folder. Click **Delete Folder** to remove a repository folder. Rename an existing folder by clicking **Rename Folder**.

Generated (saved) reports

Select Generated (Saved) Reports from the reporting tree. Saved reports are reports that have been run as a Scheduled Report. Click **View** or double-click a report in the report list to display the selected report. Click **Delete** to remove the selected report.

Scheduled reports

Select Scheduled Reports from the reporting tree. The Scheduled Reports object defines a schedule for a selected report to be run automatically. Scheduled reports can accept parameters and can be defined to run one or more times. The schedule can also email the report to a destination once it is run. Click **New** to create a new schedule for a report. Click **Modify** or double-click a report in the report list to change the scheduled settings for a report. Click **Delete** to delete the selected scheduled report.

Scheduled reports are saved to the User-Defined report repository.

Enable/Disable report data collection

User and Computer Data is collected by Desktop Authority's Operations Master service and the ETLProcessor plugin. The ETLProcessor plugin is available in the Server Manager > Plugins tab for configuration.

Data Collection can be configured for both the User and Computer in their respective Data Collection profile objects. Computer Management Data Collection can be configured for hardware, software, Patch Management, USB/Port Security and Startup/Shutdown information. User based Data Collection can be configured for login/logoff and lock/unlock events.

ⓘ *Note: This feature is not a standard part of Desktop Authority Essentials. To obtain this feature, Desktop Authority Essentials must be upgraded to the full version of Desktop Authority..

Computer Management

What is Computer Management?

Computer Management allows computers in the enterprise to be configured whether or not a user is logged in to the system. Configurations that apply to the computer operating system, as well as configurations that apply to all users, can be configured.

Computer Management configurations are applied by the Computer Management Agent. This agent runs as a Windows service, starting when Windows is started and always available to apply configuration until Windows is shut down. The agent can apply configured settings at Windows Startup and Shutdown, at Refresh intervals, and at any scheduled time established by the admin. Desktop Authority uses patented Validation Logic for Computer Management so the admin can target computer specific settings based on a robust set of selection criteria.

Computer Management is especially helpful in configuring desktops during non-working hours and in configuring servers, where there may be no user logins to trigger configurations and where you want to manage the environment rather than the user's environment.

Application Launcher

The Application Launcher object allows you to define and launch applications on the client computer at Startup, Shutdown, defined Refresh intervals or based on customized Schedules.

In addition to launching standard applications, such as Internet Explorer or Outlook, the Application Launcher object is the perfect way to update your client's anti-virus signatures, using the update executable supplied by the vendor of your anti-virus software.

The Computer Management Application Launcher cannot be used to launch or execute anything that requires user interaction or shows a dialog box. This is because the Computer Management Service runs as a non-interactive service and cannot present anything to a user.

Learn more about the Configuration Element list

Settings

Application

File name including path

Enter the complete path and filename where the application's executable exists or click **Browse** to locate the executable's path. Desktop Authority's dynamic variable selection is available for this field by pressing F2.

Arguments

Enter any optional parameters (switches) to be passed to the launched application.

Launch asynchronously

Select this check box to run the application asynchronously. In asynchronous mode, the applications will run at the same time. If this check box is cleared, applications will run one after another. Each application must complete before the next one will begin.

Continue execution after xx hours, xx minutes, if the application has not closed

When launching an application, Desktop Authority may stop its processing if the application does not finish processing and close successfully. A machine reboot will allow Desktop Authority to complete. Select this checkbox to allow Desktop Authority to continue processing even if the Application launcher action does not complete. Enter the amount of time, in hours and minutes, for Desktop Authority to wait for the application completion.

If the application is still processing after the time has elapsed, Desktop Authority will execute the profile object element, leaving the current application process started.

Execution Options

Balloon

Show Balloon message to user before element executes

Check this box to show a pop up message from the system tray before each Desktop Authority element is executed on the computer. Enter the message text into the Text box.

Permission

Ask user's permission to execute element

Select this box to pause execution and request permission via a message box to execute an element on the desktop. Enter a message into the Text box. This text will be used on the on permission message box.

Text

Enter the text that will be displayed to the user to request permission to execute the application.

Message box will timeout after xx seconds

When permission is requested from the user, the message box will be displayed for the number of seconds specified here.

Default answer if message box times out

If there is no response during the timeout period, the message box will be accepted or dismissed based on the specified default answer.

Authorized by

Optionally enter then name of the person who authorized the specified configuration to take place.

Reboot

Reboot after element executes

Select this option to determine the timing in which a reboot will take place, if required, by the executed element.

Reboot type

Reboot immediately without user interaction

Allow the required reboot to happen immediately following the element configuration.

Reboot with count down (machine will reboot when count down dialog comes out, unless postponed)

The user will be provided a countdown timer before the reboot event occurs. Specify the number of seconds for the countdown in the **Seconds until reboot** box.

Remind user that a reboot is required (will not reboot unless user approves)

Select this option to delay the reboot to a time that the user deems acceptable.

Reboot timeout

Seconds until reboot

Enter the number of seconds to count down until reboot occurs.

Allow users to postpone reboot

Select this box to allow the user to postpone the impending reboot.

Timing

Select the Timing tab to configure when this element will be executed. Computer Management objects can execute at computer Startup, Shutdown, defined Refresh intervals or based on customized Schedules.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Local Account Management

The Local Account Management profile object provides the ability to manage the local built-in user accounts on client workstations. The local user accounts that can be managed are the Administrator and Guest local accounts. You can change the name of the account, change the password of the account, and disable either of these accounts. You can also remove local user profiles that have not been used for a specified period of time.

The Local Account Management profile object also provides the ability to manage local built-in groups on client workstations. It allows these built-in groups to be managed by adding and/or removing domain and local user and domain groups.

Users

Options for Built-in Users

Built-in User Account Name

Select a built-in user account from the drop down list. This is the account that the following options apply to.

Disable this account

Select this check box, ☑, to disable the selected built-in account. Clear the check box, ☐, to enable the selected built-in account. Gray the check box, ▣, to preserve the built-in account's current setting.

The default setting is to preserve the built-in account's current setting.

Account Settings

Change existing name

Select this option to change the name of the selected Built-in User Account.

Change existing password

Select this option to change the password of the selected Built-in User Account. Password strength is based on a level of 1 (weakest) to 5 (strongest). Take into account the following password guidelines for a strong password:

- Contains at least one lower case character
- Contains at least one upper case character
- Contains at least one numerical character
- Contains at least one special character
- Has at least 12 characters with no character repetition

Options for User profiles

Remove any Domain User Profiles not used in the last XX day(s)

User profiles are created and saved on the local workstation for every user that logs in. Select this option to remove any user profiles from the local computer when they have not been accessed (user has not logged in) for a certain amount of days. This can be any value from 30 and above. A profile will be removed only if it is stored on the local machine. Only domain user profiles will be removed. If any part of a profile is stored externally (outside of the profiles folder directory) will not be removed; this includes Roaming user profiles and Mandatory user profiles. The default value is 30 days.

Groups

Options for Built-in Groups

Select a built-in group to manage. Accounts may be added to or removed from this selected group.

Accounts to add or remove

Domain Accounts

From the drop down selection, choose either Add Domain Accounts or Remove Domain Accounts. From the popup resource browser, select one or more Domain Users, Domain Groups or Domain Computers to manage in the selected built-in group. Both of these selections will add an account to the Account list, each with the selected action, Add or Remove.

The Account list will show the desired Action (Add/Remove), Account Type (Domain/Local), Name (Domain/User Name), and Status. The status will confirm the users' or groups' SID was resolved or not. If the status is "Failed", it was not found (in Active Directory) and will not be able to be added to the built-in group. If the status is "Resolved", it was found (in Active Directory) in the Users/Groups SID and can be used.

To the right of each account in the Account list there will be an **Edit** link. Click the Edit link to modify the Action type. To remove one or more entries from the list, select each one and then click the **Remove** button.

Local Accounts

From the drop down selection, choose either Add Local User Accounts or Remove Local User Accounts. In the Account list, select the appropriate action and enter the local user name into the entry provided. Local accounts do not get resolved for a SID, therefore no status will be given in the status column. To the right of each account in the Account list there will be Edit and Remove options. Click the **Edit** link to modify the Action type. Click **Remove** to delete the account from the Account list.

Remove any domain users or domain groups from the local administrators group on the client that are not defined here

This setting is only available when the Administrators (built-in) group is the selected Built-in group list. It will be disabled for all other selected groups.

Select this option to remove all domain users and/or domain groups from the built-in local Administrators group unless the user or group is defined in the Account list.

Timing

Select the Timing tab to configure when this element will be executed. Computer Management objects can execute at computer Startup, Shutdown, defined Refresh intervals or based on customized Schedules.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

*This feature is not a standard part of Desktop Authority Essentials. To obtain this feature, Desktop Authority Essentials must be upgraded to the full version of Desktop Authority.

MSI Packages*

The MSI Packages object is used to configure the deployment of applications throughout the enterprise. The MSI Packages object supports the deployment of Windows Installer MSI, MST and MSP packages. Using a Windows Installer package ensures that applications are installed, updated and uninstalled in a consistent manner throughout the enterprise.

The MSI Packages settings tab provides the interface to select a previously published package and one or more transfer files, and add desired Windows Installer command line options. In addition, you can choose to distribution server that will serve the package to the desktops that validate for this configuration element.

Packages may be installed/uninstalled asynchronously or synchronously and they may be installed without user notification (silent), if desired.

> ⓘ Note: All MSI Packages are installed using the per-machine installation context. This makes the installed application available to all users of the computer and will be placed in the All Users Windows profile.

Settings

MSI Packages

Select Package

Click the **Select Package** button to select a package to install/uninstall on client computers within the enterprise. A package can be selected from a list of packages that are known and published by Desktop Authority within Software Distribution.

Once a package is selected, detailed information about the package will be displayed above the Select Package button. The detailed information includes the product name, file name, manufacturer, version, product code, file size and the published status of the package.

If a package is unpublished but is used in an existing MSI package element, click the **Publish** button to return it to published status.

Action

Select *Install* or *Uninstall* from the Action list to define the action for the MSI Packages element.

Asynchronous

Select this box to run the MSI installation asynchronously. In asynchronous mode, the installation will run at the same time as others. If this check box is cleared, applications will install one after another. Each installation must complete before the next one will begin.

> Note: The **"Reboot after element executes"** execution option will have no effect on the computer if the Asynchronous option is checked on.

Continue execution after xx hours, xx minutes, if the application has not closed

When launching an application, Desktop Authority may stop its processing if the application does not finish processing and close successfully. A machine reboot will allow Desktop Authority to complete. Select this checkbox to allow Desktop Authority to continue processing even if the Application launcher action does not complete. Enter the amount of time, in hours and minutes, for Desktop Authority to wait for the application completion.

If the application is still processing after the time has elapsed, Desktop Authority will execute the profile object element, leaving the current application process started.

Silent

All packages being installed from a Computer Management profile will automatically be installed silently, i.e. without displaying any user interface to the end user. This box will always be selected and cannot be unselected.

Packages

Published transform files

Transform files provide configuration settings to be used during the installation of a package. One use of a Transform file is to automatically provide responses to prompts during the installation, for example, to provide an installation path or serial number, so the end user does not have to.

To enable the use of Transform files, there must be at least one published MST. MST files are published within the Software Distribution global object. Both the Add and Delete buttons will be disabled if there are no published MST files in the software repository.

Click **Add Files** to select one or more transform files to add to the Transform Files list. Click **Delete** to remove selected transform files from the Transform Files list.

Additional command line options

MSIEXEC, the Windows Installer executable program installs packages and products, is called to deploy Windows Installer files. Based on the configurations for the MSI Packages object, specific command line options are passed to MSIEXEC. To use additional command line options, enter the switches in this box. For example, entering /norestart will not allow the computer to restart following the install/uninstall, even if the MSI calls for it. All switches entered into this box will be passed to MSIEXEC in addition to any command options that are part of the MSI Packages configurations.

Note: Using additional command line options will prevent reporting on the Installer file.

Distribution servers

Select **Automatic selection** to copy the Windows Installer packages to the client from an auto-selected server. Select **Use specific server** to define a specific server to copy the Windows Installer package file from. Separate multiple server names using a semicolon (;).

For configuration information on the Update Service, see What is the Update Service?

Execution Options

Balloon

Show Balloon message to users before element executes

Check this box to show a pop up message from the system tray before each Desktop Authority element is executed on the computer. Enter the message text into the Text box.

Permission

Ask user's permission to execute element

Select this box to pause execution and request permission via a message box to execute an element on the desktop. Enter a message into the Text box. This text will be used on the on permission message box.

Message box will timeout after xx seconds

When permission is requested from the user, the message box will be displayed for the number of seconds specified here.

Default answer if message box times out

If there is no response during the timeout period, the message box will be accepted or dismissed based on the specified default answer.

Authorized by

Optionally enter then name of the person who authorized the specified configuration to take place.

Reboot

Reboot after element executes

Select this option to determine the timing in which a reboot will take place, if required, by the executed element.

Note: This Reboot option will have no effect on the computer if used in conjunction with the Asynchronous option.

Reboot type

Reboot immediately without user interaction

Allow the required reboot to happen immediately following the element configuration.

Remind user that a reboot is required (will not reboot unless user approves)

Select this option to delay the reboot to a time that the user deems acceptable.

Reboot with count down (machine will reboot when countdown dialog comes out, unless postponed)

The user will be provided a countdown timer before the reboot event occurs. Specify the number of seconds for the countdown in the **Seconds until reboot** box.

Reboot timeout

Seconds until reboot

Enter the number of seconds to count down until reboot occurs.

Allow users to postpone reboot

Select this box to allow the user to postpone the impending reboot.

Timing

Select the Timing tab to configure when this element will be executed. Computer Management objects can execute at computer Startup, Shutdown, defined Refresh intervals or based on customized Schedules.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

> ⓘ Note: This feature is not a standard part of the Desktop Authority Essentials or Standard editions. This is only available to customers who use Desktop Authority Professional.

Registry

The **Registry** object provides a single point of control over changing values in the registry of a computer. This object will modify Windows 2008/7/8.1/10/2008 R2/2012/2012 R2/2016/2019 registry key/value under the context of the Local System account.

NOTE: The Registry object is extremely versatile and, if used improperly, can cause computers not to function properly. The Registry object is designed for use by experienced administrators only. Always use caution when manipulating the registry on any computer, and extreme caution when using a product such as Desktop Authority to make a network-wide change to a group of computers at once. It is highly recommended to first test any registry modification on a specific user or computer (using Validation Logic) prior to rolling the change out to an entire group, subnet or domain.

Settings

Registry action list

Instead of configuring a single registry setting per profile element, the Registry profile object lets you configure multiple registry actions within a single Registry profile element. Click Add from the Registry profile object to create a Registry profile element. This Registry implementation will save you time when implementing multiple registry settings. Group all registry settings together that will use the same Timing and Validation Logic settings. If you prefer, you can stick to the old way of doing things by adding one element to the Registry action list and create several Registry profile elements.

Desktop Authority **Report Date/Time:** 8/21/2016 9:34:30 AM

Profile Object - Registry

Report Date/Time: 8/21/2016 9:34 AM
Report Parameters: Profile Name: New Profile, Parent Profile Name: None

Profile Name: ***New Profile***
Parent Profile Name: ***None***
Child Profiles:
Profile Last Modified On: 8/21/2016 9:02:20 AM
Do Not Process Subsequent Profiles: False
Category: User

Profile Validation Logic
Enabled: True
Class: *
Timing: *
Virtualization: *
Network: ON_NETWORK OFF_NETWORK
Rules: Empty
Conn: LAN RAS
OS: *
Platform: *

Element Details

Registry

Element Validation Logic
Class: *
Timing: LOGON
Virtualization: *
Network: ON_NETWORK OFF_NETWORK
Rules: Empty
OS: *
Conn: LAN RAS
Platform: *

Priority: 0 **Enabled:** True **Created By:** SL\SLADMIN
Last Modified Date: 8/21/2016 8:48:10 AM **Last Modified By:** SL\SLADMIN
Description: [Created: sladmin WIN-9J2N40MA8S8 08/21/2016 08:48]

Notes:

Registry Item
Action:
Hive:
Key:
Type:
Value:
Data:
Recursive:

Add

Click **Add** to add a new entry to the Registry action list.

Import

Click **Import** to import existing registry (.reg) files.
Importing Registry Files

There are two ways to import an existing registry file:

- Import registry entries into a single Registry profile element
- Import registry entries into multiple Registry profile elements

Figure 39: Import registry entries into a single Registry profile element

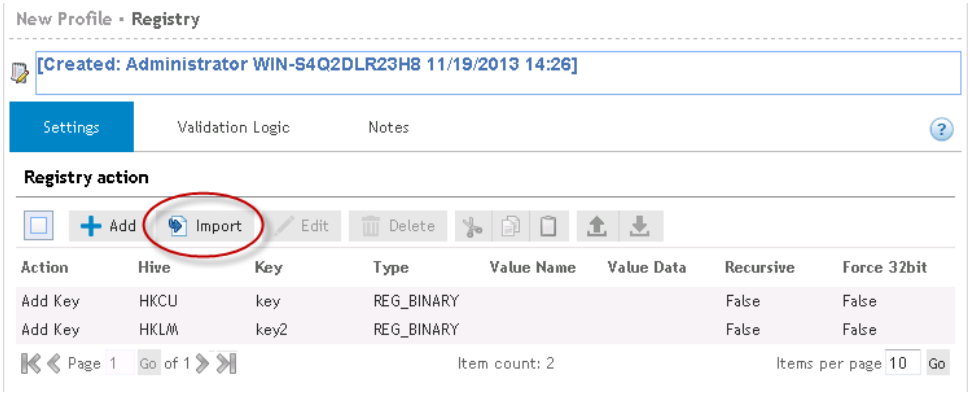


Figure 40: Import registry entries into multiple Registry profile elements

Clicking the **Import** button from the Registry profile object will import all entries within the selected .reg file as multiple elements in the Registry profile object. **This will result in *multiple* Registry profile elements.**

Edit

Select **Edit** to modify the currently selected registry action.

Delete

Select **Delete** to remove the currently selected registry action.

Cut/Copy/Paste

Registry actions can be managed by using the standard Windows Cut/Copy/Paste actions to maneuver them into child profiles or parent profiles. Drag and Drop actions may also be used for this purpose.

Move up/Move down

Registry actions will be evaluated on a client in the order they appear in the Registry action list, from the first Registry element to the last. The order of the Registry actions can be modified by using the Move Up and Move Down buttons. To move a registry action, you must first select it, by clicking on it. Once it is selected (it will be highlighted), press the Move Up or Move Down button based on which way you want to move the setting.

The order in which the Registry actions are displayed in the list is the order they will get processed in. For example, if there are 2 registry elements and they each have a registry action list, all actions for the first registry element will be processed and then all actions for the second registry actions list will be processed.

Configuring a registry action

Once you have configured the registry action, click **Confirm** to save the settings or **Cancel** to abort the setting changes.

Action

Select an action from the list to define how the registry setting is to be updated. Registry keys can be created and removed. Available actions are:

- **Write Value**
  Store the specified data to the specific Hive\Key\Value. If the key does not already exist, it will be created.
- **Delete Value**
  Remove the specified value from the specific hive\key.
- **Add Key**
  Create a key in the specified hive.
- **Delete Key**
  When the *Delete Key* is selected you have the option of deleting the key regardless of whether subkeys exist or not using the **Delete Key even if subkeys exist** option. Selection this option to delete the key and any associated subkeys. If this option is not selected, the key will not be deleted if any subkeys exist.

  This option cannot be performed on the *Software\Microsoft* or *Software\Classes* keys.

Hive

Select the hive on which to perform the action from the list. The following hives can be selected:

- **HKEY_LOCAL_MACHINE**
  Contains computer specific information about the type of hardware, software, and other preferences on a given PC.
- **HKEY_CLASSES_ROOT**
  Contains all file associations, OLE information and shortcut data.
- **HKEY_USERS/.DEFAULT**
  Contains default profile preferences.
- **HKEY_CURRENT_CONFIG**
  Represents the currently used computer hardware profile.

Key

Enter the specific key to be added or updated in the registry. Keys are subcomponents of the registry hives. Dynamic variables are available for use in defining the key.

Type

Select the value type to be stored in the registry key.

Valid types are:

- REG_BINARY
  The entry field for binary data is similar to the entry field in RegEdit. Use the actual hex values as entry.
- REG_DWORD
- REG_DWORD_BIG_ENDIAN
- REG_DWORD_LITTLE_ENDIAN
- REG_EXPAND_SZ
- REG_FULL_RESOURCE_DESCRIPTOR
- REG_MULTI_SZ
  Enter each piece of data or expression on a new line.
- REG_NONE
- REG_QWORD
  Select the type of data to be entered, Decimal or Hex.
- REG_RESOURCE_LIST
- REG_SZ

The Type list is not applicable when the Action field is set to either Add Key or Delete Key.

Value

Enter the name of the value for the registry key that will be written. Value is not applicable when the Action field is set to either *Add Key* or *Delete Key*.

A value is not required when the Action field is set to *Write Value*. If no value is specified, the data will be written to the key's default value.

Data/expression

Type the data you would like stored in the specified value. This field may contain static text, Desktop Authority Dynamic Variables, KiXtart macros or any combination of the three. Press the **F2** key to select a dynamic variable from the list.

If you want to create a new value with no data, or to erase an existing registry value’s data, leave this field blank. The value will be created with no data.

Force use of 32 bit registry locations on 64 bit operating systems

Check this box to force the 32 bit registry location to be used instead of the 64 bit location when executing on 64 bit operating systems.

Timing

Select the Timing tab to configure when this element will be executed. Computer Management objects can execute at computer Startup, Shutdown, defined Refresh intervals or based on customized Schedules.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Service Pack Deployment

The **Service Pack Deployment** object allows you to deploy service packs for all 7/2008/2008 R2 clients and servers (64-bit operating systems included).

A few items to note regarding service pack deployment:

- Computer Management Service Pack Deployment will only install service packs to 7/2008/2008 R2 clients and servers if connected over a LAN connection.
- Computer Management Service Pack Deployment will never downgrade the currently installed service pack on a computer.
- Computer Management Service Pack Deployment will only install the requested service pack if the client/server has an older or no service pack installed.
- Computer Management Service Pack Deployment will not attempt to install the requested service pack if the client/server does not have enough available disk space on the drive that hosts the %temp% folder. The engine determines the amount of available disk space before the service pack is installed. By default, 1.4G (1400mb) of disk space must be available to install any service pack. This default can be overridden by defining a value in the global or profile definition file.

The variable $ServicePackFreeSpaceNeededInMB is used to override the available disk space amount. Select Global Options > Definitions or select the Definitions tab on the profile's settings.

Example:

$ServicePackFreeSpaceNeededInMB="1000"

- Computer Management Service Pack Deployment will run all service packs in unattended mode, will force the computer to close other programs when it shuts down, and will not back up files for uninstall purposes.
- Computer Management Service Pack Deployment will not install service packs on any Windows Embedded operating system.

Desktop Authority can bypass the automatic installation of service packs on specific computers. If you have specific computers that you would never like **Desktop Authority** to install a service pack on (such as a development

station), create a file called *SLNOCSD* in the root directory of the System Drive. This allows you to generally apply service packs based on Validation Logic, while providing for special-case exemptions based on individual systems.

Settings

Service Packs settings

Operating system version

Select an Operating System version from the list. Valid selections are Windows 2008, Windows 2008 x64 and Windows 7.

Operating system language

Select a language from the list. This language should specify the dialect of the operating system installed on the client/server as well as the service pack. If the languages do not match, the service pack will not be installed.

Update to

From the list, select the service pack to be deployed. Service Packs displayed in the list are filtered based on the OS Version selected.

Location of Update.exe /Spinstall.exe

Enter the complete path and filename where the installation executable exists or click **Browse** to locate the executable's path. The installation executable may be called either spinstall.exe or update.exe based on the operating system being installed. The service pack install file is called spinstall.exe in Windows 2008.

Example:

\\server1\installs\W2KSP1\Update.exe

The executable file downloaded from Microsoft is an archive that must be extracted at a command line by using the *-x* switch. This will extract the service pack into multiple folders among which you will find the *update.exe or spinstall.exe* executable.

The following parameters are used when installing service packs from the Computer Management Service Pack object:

- Server 2008 = ' /quiet /norestart'
- Windows 7 and Server 2008R2 = ' /quiet /nodialog /norestart'

  For information about the Microsoft Service Pack command line parameters, refer to Microsoft's Command-line switches for Windows software update packages knowledge base article.

Execution Options

Balloon

Show Balloon message to users before element executes

Check this box to show a pop up message from the system tray before each Desktop Authority element is executed on the computer. Enter a message into the text box to be shown in the popup message.

Permission

Ask user's permission to execute element

Select this box to pause execution and request permission via a message box to execute an element on the desktop. Enter a message into the text box. This text will be used on the on permission message box.

Message box will timeout after xx seconds

When permission is requested from the user, the message box will be displayed for the number of seconds specified here.

Default answer if message box times out

If there is no response during the timeout period, the message box will be accepted or dismissed based on the specified default answer.

Authorized by

Optionally enter then name of the person who authorized the specified configuration to take place.

Reboot

Reboot after element executes

Select this option to determine the timing in which a reboot will take place, if required, by the executed element.

Reboot type

Reboot immediately without user interaction

Allow the required reboot to happen immediately following the element configuration.

Remind user that a reboot is required (will not reboot unless user approves)

Select this option to delay the reboot to a time that the user deems acceptable.

Reboot with count down (machine will reboot when countdown dialog comes out, unless postponed)

The user will be provided a countdown timer before the reboot event occurs. Specify the number of seconds for the countdown in the **Seconds until reboot** box.

Reboot timeout

Seconds until reboot

Enter the number of seconds to count down until reboot occurs.

Allow users to postpone reboot

Select this box to allow the user to postpone the impending reboot.

Timing

Select the Timing tab to configure when this element will be executed. Computer Management objects can execute at computer Startup, Shutdown, defined Refresh intervals or based on customized Schedules.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element. Service Packs may only be applied to computers classified as a Desktop, Portable Tablet PC, Member Server and Domain Controller. Operating System and Connection type are disabled.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Data Collection

The Data Collection object is used to configure which Computer data is collected from the client computers connected to the environment to which Desktop Authority is installed.

Data is collected by Desktop Authority's Operations service and the ETLProcessor plugin. These two plugins are available in the Server Manager > Operations Service tab for configuration.

Settings

Data to collect

Collect client hardware information

Select this box to allow Desktop Authority to keep track of hardware information for each computer in the enterprise.

> ⓘ Note: Collect client hardware information must be enabled in order for Wake On LAN Deployment to wake up targeted computers. This Data Collection option allows for the MAC addresses to be collected.

Collect installed software information

Select this box to allow Desktop Authority to keep track of the installed software on each computer in the enterprise.

Collect USB/Port Security information

Select this box to allow Desktop Authority to keep track of the devices plugged in to each computer in the enterprise. Detailed USB/Port Security data collection options can be set in the User Management USB/Port Security object.

Collect startup/shutdown information

Select this box to disable the collection of startup and shutdown events. Deselect this box to collect data about these events.

Collect machine heartbeat packets every xx hours

Select this box to specify how often the client computer will notify Desktop Authority that the computer is it still powered up. The default collection time period is every 6 hours. This allows for more accurate reporting.

Timing

Select the Timing tab to configure when this element will be executed. Computer Management objects can execute at computer Startup, Shutdown, defined Refresh intervals or based on customized Schedules.

Validation Logic

Select the Validation Logic tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Wake on LAN

Wake On LAN (WOL) is a computing standard by which computers that are asleep can be sent a message through the network to wake them up. Wake on LAN is supported on all Microsoft Windows operating systems. Machines can be awoken when in Sleep, Hibernate or Stand by modes.

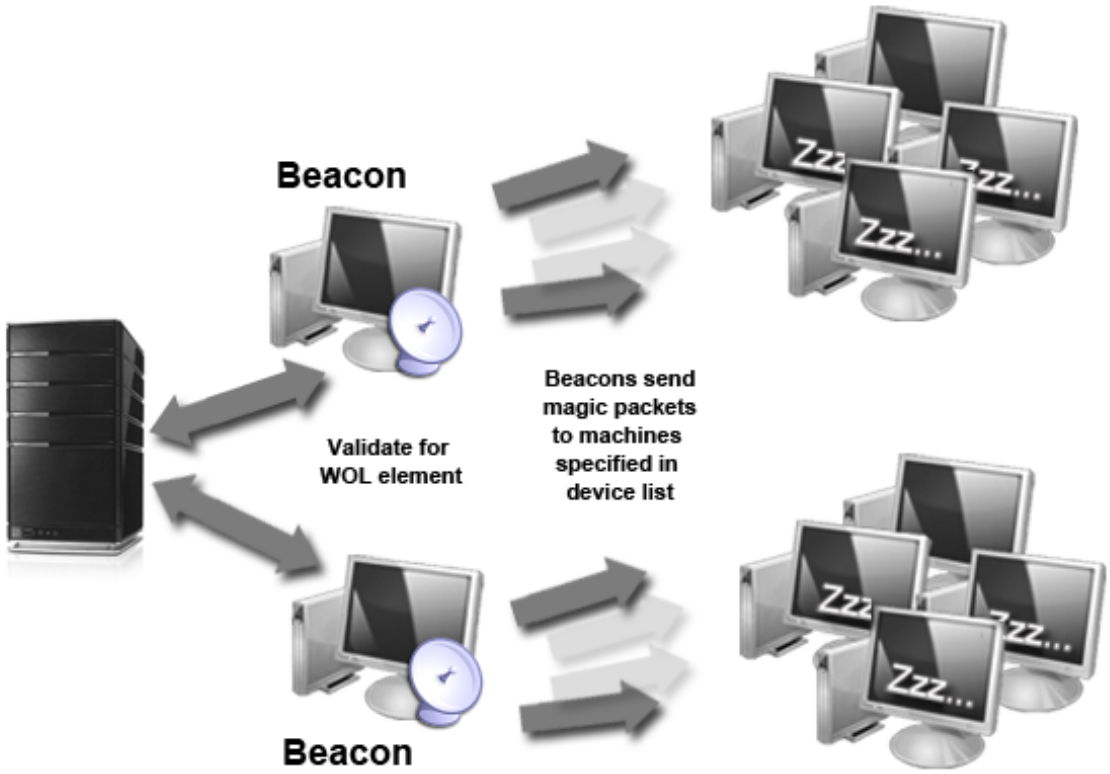
> ⓘ Note: Wake on LAN is only supported from Sleep or Hibernation states in Windows 8.1. Refer to Microsoft KB Article 2776718 for more information.

The only requirement for WOL is a computer with a NIC and Bios that supports WOL. There are usually 2 settings in the BIOS to support this. In the BIOS enable the PXE setting, and/or depending on the computer hardware in the BIOS - Power Management, enable Wake On LAN.

As well as turning on WOL in the BIOS, the OS must also be configured to support WOL. On client machines, go to the LAN Connection properties and click the Configure button. On the Power Management tab, enable the "Allow this device to wake the computer" (Windows 7).

Desktop Authority's implementation of WOL consists of beacon machines that are used to send out packets to wake specified computers. A beacon is defined as any computer managed by Desktop Authority that validates for a Wake on LAN element. Once a machine validates for a WOL element, it becomes a beacon and begins sending out packets to each computer specified in the WOL settings. Since a computer can only send out packets when it is powered on and awake, ensure that computers designated as beacons will be on at the time the WOL element is scheduled to execute.

Figure 41: Wake on LAN graphical overview



Once a beacon is determined by passing validation logic for a WOL element, the machine will send out special WOL "magic" packets to all machines specified in the WOL element's settings.

Settings

Wake Target configuration

New target to wake

Add a custom entry to the WOL List by Machine name, IP address, MAC address or by Excluded MAC address.

Add existing

Select a computer from a list of machines discovered by Data Collection. Computer can be selected by Machine names, IP addresses, MAC addresses or by Excluded MAC addresses. All available items in the system inventory will be listed and will be available for selection

Remove

Select one or more elements from the WOL list and click the **Remove** button.

Import

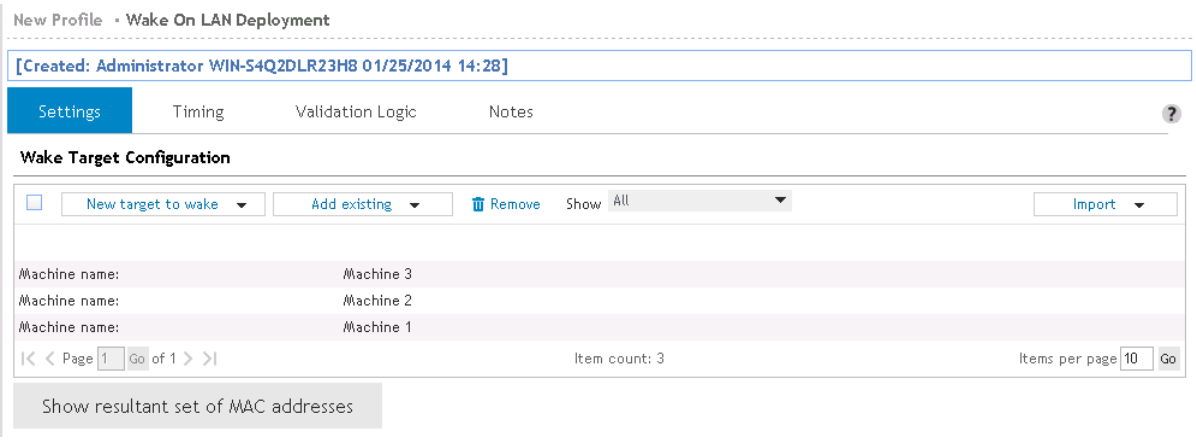
Click Import to import a list of Machine names, IP addresses, MAC addresses, or Excluded MAC addresses.

When importing, the import file must be a .CSV file containing one column of one or more Machine Names, IP Addresses, MAC Addresses, or Excluded MAC Addresses exclusively.

Example:

ACME.Machine1
ACME.Machine2
ACME.Machine3

The above example list provides the following result when imported:



Show resultant set of MAC addresses

Retrieve a complete list of all MAC addresses that this beacon will send the "magic" packet to. MAC addresses are retrieved from the Hardware inventory database. If a MAC address cannot be retrieved for a computer, it will not be woken up when the WOL element is executed.

> Note: Some routers and switches may filter out magic packets resulting in the inability to wake the target machines. Therefore, it is recommended to select a beacon that resides on the same subnet as the target machine(s).

Timing

Select the Timing tab to configure when this element will be executed. Computer Management objects can execute at computer Startup, Shutdown, defined Refresh intervals or based on customized Schedules.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

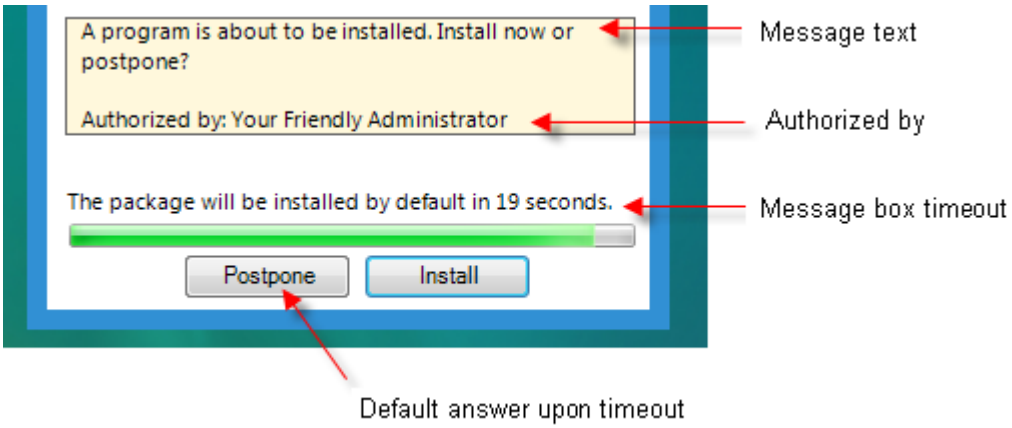
When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

User Experience - client side

Computer Management Application Launcher, MSI Packages and Service Pack Deployment have Execution Option settings which can optionally alert the user on the client, if any, that an element is about to execute.

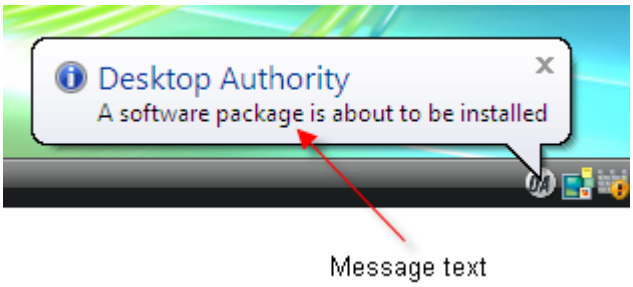
If the **Ask user's permission to execute element** option is selected, a message box similar to the one below, will be displayed on the desktop. The user will be notified before the element is executed and will be given an option to postpone the action.

Figure 42: Client side permission box



If the **Show Balloon message to users before element executes** option is selected, a balloon will be displayed in the system notification area.

Figure 43: Client side balloon notification



User Management

What is User Management?

Desktop Authority User Management features the application of settings that are specific to a Windows user environment. These configuration settings are applied at user Logon, Logoff and Desktop Authority Refresh intervals.

Alerts

The **Alerts** object allows for the custom configuration of warning and notification messages (events) that Desktop Authority may display during the logon process. The event message text may be customized and a notification may be posted to the client and/or designated Administrator via the event log, popup message box or email.

A list of all configured Alerts is displayed upon entry into the object. Click **Edit** on the entry that is to be modified.

Event configuration

Alert title

Type in static text or press F2 to select a dynamic variable. The window title is displayed at the top of an Alert's popup message box.

Alert type

Select a message box type from the list. Choose from *Information*, *Question*, *Warning*, or *Error*. Each type displays an icon to the left of the message. The types use the following icons in the message box:

 Information

 Question

 Warning

 Error

Alert text

Enter the text to be displayed in the message box. Dynamic variables can be used in conjunction with any other text or dynamic variable(s). Press the F2 key to select a dynamic variable.

Destination

Define the settings that configure the display of the event notification.

Display a pop-up message to the user logging on

Select this check box to enable a popup message box to display on the clients desktop. The message box will be displayed when the selected event occurs during the client logon process. Clear this check box to disable the popup alert.

Timeout (seconds)

Timeout is available when the Client Message Box notification destination is selected. Enter a numeric value representing the number of seconds the message box will display for. It will be displayed for the specified number of seconds unless the OK button is pressed before the timeout occurs.

Display a pop-up message to specific user(s) and/or computer(s)

Select this check box to enable a popup message box to the specified computers or user's desktop. The message box will be displayed when the selected event occurs regardless of the user logging on. Clear this check box to disable this message box notification.

Enter one or more computer names and/or user names that will receive visual notification of the selected event. Each computer/user should be delimited by a semicolon (;).

Write this alert to the client computer’s event log

Select this check box to enable event logging on the client computer. The event will be logged when the selected event occurs during the client logon process. Clear this check box to disable event logging for the selected event.

Write this alert to the event log on one or more specific computers

Select this check box to enable event logging to the specified computers or users. The event will be logged when the selected event occurs during any client logon process. Clear this check box to disable event logging for the selected event.

Enter one or more computer names and/or user names that will receive visual notification of the selected event. Each computer/user should be delimited by a semicolon (;).

E-mail this alert to specific address(es)

Select this check box to enable e-mail alerts. Notification of the alert will be e-mailed when the selected event occurs during any client logon process. Clear this check box to disable e-mail alerts for the selected event.

Enter one or more e-mail addresses to receive notification of the selected event. Each e-mail address should be delimited by a semicolon (;).

Reset to Default

Click this button to reset the event to its default settings.

Global alert settings

SMTP server

Enter the name of the SMTP server to be used to send e-mail alert(s).

Application Launcher

The Application Launcher object allows you to define and launch an application on the client's desktop after the logon script completes. This is equivalent to placing a shortcut in the client's Startup folder, however, Desktop Authority performs this in a centralized fashion so there is no need to visit each computer to set this up.

In addition to launching standard applications, such as Internet Explorer or Outlook, the Application Launcher object is the perfect way to update your client's anti-virus signatures, using the update executable supplied by the vendor of your anti-virus software.

The Desktop Authority Application Launcher queues programs for launching after the logon process is complete. However, if Desktop Authority detects the client is connecting over dial-up networking, the application is immediately launched while the script continues to execute.

Settings

Application

File name including path

Enter the complete path and filename where the application's executable exists or click **Browse** to locate the executable's path. Desktop Authority's dynamic variable selection is available for this field by pressing the F2 key.

Arguments

Enter any optional parameters (switches) to be passed to the launched application.

Miscellaneous options

Run as administrator

Select this check box to run the application with Administrator privileges. If the user logging on to the network does not normally have Administrator privileges, the application will be executed using Desktop Authority's RunAs Admin service.

If this check box is cleared and the user does not have rights to access or run the application, the application will not run.

Hide any screen output

Select this check box to hide any windows that would normally be displayed by the application.

Launch asynchronously

Select this check box to run the application asynchronously. In asynchronous mode, the applications will run at the same time. If this check box is cleared, applications will run one after another. Each application must complete before the next one will begin.

Message box settings

Show time-out message box prior to launching applications

Select this box to pop up a message box before the application is executed.

Window Title

Type in static text or press F2 to select a dynamic variable. The window title is displayed at the top of the popup window.

Message

Enter the text to be displayed in the message box. Dynamic variables can be used in conjunction with your text. Press F2 to select a dynamic variable.

Message box will time-out in xx seconds

Optionally, specify the number of seconds for the message box to be displayed. If there is no confirmation of the message box, the message box will be closed and the application will automatically be launched. Specifying 0 seconds will display the time-out message box, until it is confirmed.

Cycle schedule

Unique ID

The unique id entry is used to make each entry in the Application Launcher list a unique item, regardless of the application that is to be launched. This is helpful in the execution of an application when the Frequency is set to run Once Per Day or One Time. The data in this entry is automatically generated and should not be modified. However, if an entry in the list, that is set to run Once Per Day or One Time, must be executed a second time, the unique id can manually be changed by clicking the **Generate** button.

Frequency

Select a logon frequency from the list. Select from *Every Time, Once Per Day (User)*, *Once Per Day (Computer)*, *One Time (User) and One Time (Computer)*.

Select **Every Time** to launch the application every logon, logoff, refresh, shut down, desktop.

Select **Once Per Day (User)** to launch the application at the specified cycle, one time per day for the current user.

Select **Once Per Day (Computer)** to launch the application at the specified cycle, one time per day for the computer.

Select **One Time (User)** to launch the application at the specified cycle, a single time for the current user.

Select **One Time (Computer)** to launch the application at the specified cycle, a single time for the computer.

Example:

To launch Outlook each time your users log on, select Everyday from the first cycle prompt and Every Logon from the second. Anti-virus updates need only be launched once on the selected day. For this type of application, you would select Specific Date and set the logon frequency to Once per day.

Cycle

Select a time interval for which the application will run. Choose from *Every Time*, *Day of Week*, *Monthly (Day of Week)*, *Monthly (Day of Month) and Specific Date*.

Selecting **Every Time** as the cycle, will force the application to be run each day each logon, logoff, refresh, shut down, and desktop timing as specified in the Application Launcher validation logic.

Selecting **Day of Week** as the cycle, presents a new list allowing the selection of a day from Sunday to Saturday.

Selecting **Monthly (Day of Week)** as the cycle, presents a new list allowing the selection of a day in the month ranging from 1st Sunday, 1st Monday, ... to the last Saturday of the month.

Selecting **Monthly (Day of Month)** as the cycle, presents a new list allowing the selection of a date within the month.

Selecting **Specific Date** as the cycle, presents an entry to which the specific date should be entered. Press the arrow to make your date selection from any calendar day.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Common Folder Redirection

The **Common Folder Redirection** object allows you to change the location of where Windows 7/2008/2008 R2/2012/2012 R2/2016/2019 computers look for common specialized folders known as the *All Users Shell Folders*.

Common Shell Folders are folders that are shared by all users of the computer and include Common Desktop, Common Programs Group, Common Start Menu and the Common Startup Group.

By instructing the operating system to locate the Common Shell Folders on a network share (or mapped drive), rather than the computer's own local hard drive, you allow users to access the common portion of the Desktop, Start Menu and/or Program Group regardless of the computer from which they log on to.

In addition to Common Shell Folders, Windows 7/2008/2008 R2/2012/2012 R2/2016/2019 also includes an individual set of shell folders that are available to each user on each computer. Individual user shell folders can be configured by Desktop Authority using the **Folder Redirection** object.

Settings

Action

Shell folder

Select a shell folder from the Shell Folder list. Desktop Authority's dynamic variable selection is available for this field by pressing the F2 key.

Redirect to folder

Specify a path that the shell folder should be redirected to. The path may be in the form of a path, mapped drive or UNC. Click **Browse** to navigate to the path. Desktop Authority's dynamic variable selection is available for this field by pressing the F2 key.

Reset to default

Select this check box to restore the redirected folder to the operating system's default location.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Data Collection

The Data Collection object is used to configure which User data is collected from the client computers connected to the environment to which Desktop Authority is installed.

Data is collected by Desktop Authority's Operations service and the ETLProcessor plugin. These two plugins are available in the Server Manager > Operations Service tab for configuration.

Settings

Data to collect

The User Management Data Collection Settings can be configured to collect data when a user session is started and completed (logon/logoff) as well as when a user session is locked and unlocked. If this option is not selected, Desktop Authority will not keep track of any user specific events.

Collect logon and logoff session information (requires Logon and Logoff timing)

Select this box to allow Desktop Authority to keep track of every logon and logoff event during the user session. Use of this option requires that Logon and Logoff Validation Logic Timing be selected.

Collect lock and unlock information

Select this box to allow Desktop Authority to keep track of every lock/unlock event during the user session.

Collect user heartbeat packets every xx hours

Select this box to specify how often the client computer will notify Desktop Authority about user event information. The default collection time period is every hour. This allows for more accurate reporting.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Display

The **Display** object provides several options that control general operating system settings including the desktop and user interface.

Settings

Desktop and Explorer

Remove Windows Welcome

This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  .

Select this check box to remove the initial Welcome to Windows dialog box that appears when a user logs on to a computer for the first time. Clear this check box to display the Welcome dialog box to new users. Gray the check box to leave the client's setting untouched.

The default for this option is cleared.

Remove IntelliMouse tips

This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  .

Select this check box to remove the Microsoft IntelliMouse tips dialog box that appears when a user logs on to a computer for the first time. Clear this check box to display the Tips dialog box to new users. Gray the check box to leave the client's setting untouched.

The default for this option is cleared.

Remove "Shortcut to" prefix

This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  .

Select this check box to remove the text *Shortcut to* when a new desktop shortcut is created. Clear this check box to include the *Shortcut to* prefix when creating new desktop shortcuts. Gray the check box to leave the client's setting untouched.

The default for this option is cleared.

Remove Find Fast startup

This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  .

Select this check box to remove the Find Fast shortcut from the Startup folder. Clear this check box to leave the Find Fast shortcut in the Startup folder untouched. Gray the check box to leave the client's setting untouched.

The default for this option is cleared.

The Find Fast shortcut is created in the Startup folder, by default, with a complete installation of Microsoft Office. This utility builds indexes to documents and is stored on the local drive of the computer. It is used to speed up finding documents from any Office Open dialog box. In most networked environments, there is no need to index the documents on local hard drives since they are typically stored on network shares.

Enabling this option (to remove the shortcut) will not automatically delete the indexes that Find Fast may have already created, however it will prevent the excessive CPU utilization and disk activity that is caused by the execution of the Find Fast utility.

Remove MSN desktop icon

This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  .

Select this check box to remove the MSN icon from the desktop. Clear this check box to leave this default icon on the desktop. Gray the check box to leave the client's setting untouched.

The default for this option is cleared.

Remove online services desktop folder

This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  .

Select this check box to remove the Online Services desktop folder from the Windows desktop*. Clear this check box to leave this default folder on the desktop. Gray the check box to leave the client's setting untouched.

The default for this option is cleared.

Disable print popup

This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  .

Select this box to disable the popup from appearing when printing. Clear this box to leave this enable the print popup window. Gray the check box to leave the client's setting untouched.

The default for this option is to preserve the client setting.

Remove My Documents desktop icon

This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  .

Select this check box to remove the My Documents icon from the Windows desktop. Clear this check box to leave this default icon on the desktop. Gray the check box to leave the client's setting untouched.

The default for this option is cleared.

Context menu

Enable "Command Prompt Here" (not on Terminal Server client)

This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  .

Select this check box to have the Command Prompt Here shortcut on the context (shortcut) menu when in Windows Explorer. The Command Prompt Here shortcut opens a DOS command window defaulting to the directory that is clicked on in Explorer.

Enable remote control shell extensions (not on Terminal Server client) (not available in Desktop Authority Essentials)

This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  .

Select this check box to have a Remote Management shortcut on the context (shortcut) menu when in Windows explorer. The Remote Management shortcut provides the ability to jump directly to a Remote Management session on the workstation.

The default value for this setting is or grayed (preserve client setting)  .

Keyboard

Enable Num Lock on boot

This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  . Select this check box to turn on the Num Locks key. Clear this check box to turn off the Num Locks key. Gray the check box to leave the Num Locks key in its current state.

Additional settings

Wallpaper file

Specify an image file to use as wallpaper on all client desktops. The location of the image file may be specified in the form of a path, mapped drive or UNC. Press **Browse** to locate the image file (.jpg, .gif, .png). Other file types may manually be typed into the entry. Desktop Authority's dynamic variable selection is available for this field by pressing the F2 key. If specifying a UNC, the location and filename should be specified in the form of \\server\share\filename.bmp.

During the logon process the specified image is copied from the specified location to the client's %Windir% folder.

Leaving this field empty will allow all clients to select their own preferred wallpaper image.

Enter the word clear within parentheses ( ) to disable all clients from using wallpaper.

Example:

- Specify to use a custom logo image file.\\myserver\myshare\mylogo.bmp
- Specify to use Windows' setup.bmp as the custom image file, $windir\setup.bmp
- Specify to disable client's wallpaper (clear)

Use current location

Select **Use current location** to have each client to access the wallpaper image from the selected location.

NOTE: In order for to use this location all users must have *Read* access to the selected folder.

Copy file to new location

Select **Copy file to new location** to have the system copy the selected file to the NETLOGON share where all clients will automatically have access to it.

Registered owner (not on servers)

Enter a Registered Owner name to override the setting that was used during the install of the operating system. Desktop Authority's dynamic variable selection is available for this field by pressing the F2 key.

Example:

- Specify $FullName Mary Jones

Registered company (not on servers)

Enter a Registered Company name to override the setting that was used during the install of the operating system. Desktop Authority's dynamic variable selection is available for this field by pressing the F2 key.

Example:

- Specify ABC Incorporated

It is recommended to use static text instead of dynamic variables or macros when Desktop Authority is used on a multi-user environment such as Terminal Server and/or Citrix MetaFrame.

Rename "*My Computer*" to (not on servers)

Enter a name to use for the *MyComputer* desktop shortcut. This will override the operating system's default setting. Desktop Authority's dynamic variable selection is available for this field by pressing the F2 key.

Example:

- Specify *$userid ($wksta)mjones(PC-111)*

This setting has no effect on Terminal Server or Citrix Server sessions.

Rename "*Network Neighborhood*" to (not on servers)

Not available for Windows 7 and later.

Enter a name to use for the *Network Neighborhood* desktop shortcut. This will override the operating system's default setting. Desktop Authority's dynamic variable selection is available for this field by pressing the F2 key.

Example:

- Specify $Domain ABC

This setting has no effect on Terminal Server or Citrix Server sessions.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Drive Mappings

The **Drive Mappings** object configures network drive mappings. Drive Mappings redirect a local resource (drive letter) to a shared network resource (hard drive or folder on the network). Using mapped drives to access server-based information provides administrators with the ability to make changes faster and more transparently than using straight UNCs on each client.

For example, the *Groups* share is where all users store shared departmental documents and is mapped to drive G: on Server1. If Server1 begins to run low on disk space, simply stop sharing the *Groups* folder on Server1 and move the *Groups* folder structure to Server2 (where there is plenty of free disk space). Change the share to the *Groups* folder on Server2. Now simply change Desktop Authority's mapping for the G drive to the *Groups* share on Server2. A trip to each desktop is saved because the client applications did not need to be changed — they still reference the folder structure as drive letter G:.

Settings

Action

Letter

Click the Letter arrow to select a drive letter to map. A valid drive letter may also be entered into the field. Valid drive letters are any single letter from A to Z. The drive letter entered can be uppercase or lowercase.

Path

Enter the folder location that the selected drive letter will be mapped to. The folder location should be specified in the form of a proper UNC, **\\server\share**. Optionally, click **Browse** to navigate to the network share.

Desktop Authority's dynamic variable selection is available for this field by pressing F2.

Mapping drive H: to all users' home directories can be done in a single entry in the Drives list. This is done by using dynamic variables. Use \\$HomeServer\$HomeDir or \\$HomeServer\$HomeDir$$ (hidden share) as the path. At logon time, the dynamic variables are substituted by the correct values based on the user logging on to the network.

When mapping to a hidden share there must be two trailing dollar signs ($$) following the share name. By clicking **Browse** and selecting a share, Desktop Authority will automatically place the extra trailing dollar sign. If the share is manually typed into the Path entry, the extra dollar sign must manually be entered.

To hide a local drive, leave the Path entry blank. The drive specified in the Letter entry will be hidden from Windows Explorer and My Computer.

Delete (appends /DELETE to path)

Select this box to remove a persistent drive mapping from a workstation. This will append the text /DELETE following the path. /DELETE may also be manually typed in to the Path entry following the specific path. This will remove any persistent drive mappings to the drive letter specified in the Letter entry.

The /DELETE option does not need to be used prior to mapping a drive. Desktop Authority will automatically remove the persistent drive mapping on the workstation if it is in conflict with the driver letter to be mapped.

Persistent (appends /PERSISTENT to path)

Select this box to make a drive mapping persistent. This will append the text **/PERSISTENT** in the Path entry. /PERSISTENT may also be manually typed in to the Path entry following the specific path. The drive will later be mapped each time the user logs onto the network, even if Desktop Authority is not running.

Hide from Windows Explorer

Select this box to hide the mapped drive letter. Hiding a drive hides it from Windows Explorer and My Computer. Although the drive is hidden, it is still available for applications to use.

Hiding a drive from Windows Explorer is often beneficial in protecting your programs and data from accidental deletion or misuse. A good example would include a standard database application. Users need NTFS Full Control of the folder and files to effectively use the database, but don't need to actually see the folder when using Windows Explorer. In this example, there would most likely be a hidden the share also. Adding a trailing dollar sign ($) to the share name when sharing the folder would prevent this share from being visible.

Explorer label (Windows 2000 and newer)

Use this label to change the default drive label (name) as shown in Explorer. This label is only available on Microsoft 2000 operating systems and newer. Desktop Authority's dynamic variable selection is available for this field by pressing F2.

If this drive fails to map

Select *Continue*, *Alert and Continue*, or *Alert and Logoff* from the list. The selected action will occur if there is a problem when attempting to map to the specified drive. The *Alert and Continue* action will issue the *Error mapping drive* alert. The *Alert and Logoff* action will issue the *Error mapping mandatory drive* alert.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Environment

The **Environment** object allows environment variables to be centrally configured on the client using static text, Desktop Authority dynamic variables or KiXtart macros.

Settings

Environment settings

Variable

Enter the environment variable to be defined. Desktop Authority's dynamic variable selection is available for this field by pressing F2.

Value

Enter the data to be assigned to the environment variable. This can be static text, a Desktop Authority dynamic variable (**F2**) or a KiXtart macro.

Example:

Variable [User]
String [$FullName]

Desktop Authority includes a dynamic variable called $Initials. This variable is set by reading the user's Description field from User Manager for Domains. If a pound symbol (#) appears anywhere in the field, the following 3 characters are returned as $Initials. For example, if the user's Description field is set to [Chief Technology Officer #JJS], the value of the $Initials becomes JJS.

Variable Location

User

Select this option to set an environment variable for the currently logged on user. User Environment variables may differ depending on the user logged on.

Machine

Select this option to set a computer environment variable. Machine based environment variables are the same for all users who log on to the workstation.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

File Operations

The File Operations object provides the ability to Copy, Delete, Move and Rename files and folders. File Operations support Local, Mapped and network drive paths as well as a generous portion of operation options.

Settings

File operation

Operation

Select Copy, Move/Rename, Delete or Create Folder from the Operation list to specify the action to execute on the specified files.

Source folder

Specify the folder on which the selected Operation will act upon.

Source file(s)

Specify the files on which the selected Operation will act upon.

Destination folder

For Copy, Move/Rename or Create Folder operations, specify the folder to be used as the destination for the selected Operation.

Destination file(s)

For Copy or Move/Rename operations, specify the file names to be used for the destination of the selected Operation.

Options

Only files

Select this check box to enable extra File Operation options. When enabled, select changed before, changed after, changed between, changed on and older than from the list

- changed before

  Select changed before, for the selected operation to act on all files last modified prior to the specified date.

- changed after

  Select changed after, for the selected operation to act on all files last modified after the specified date.

- changed between

  Select changed between, for the selected operation to act on all files last modified between (and including) the specified dates.

- changed on

  Select changed on, for the selected operation to act on all files last modified on the specified date.

- older than

  Select older than, for the selected operation to act on all files older than the specified number of days.

- last accessed before

  Select last accessed before, for the selected operation to act on all files that were last accessed before the specified date.

- last accessed after

  Select last accessed after, for the selected operation to act on all files that were last accessed after the specified date.

- last accessed between

  Select last accessed between, for the selected operation to act on all files that were last accessed between the specified dates.

- last accessed on

  Select last accessed on, for the selected operation to act on all files that were last accessed on the specified date.

- last accessed more than X days

  Select last accessed more than X days, for the selected operation to act on all files that were last accessed more than the specified number of days ago.

Include subdirectories

Select this check box to include all subdirectories of the Source Folder in the selected Operation. Clear this check box to exclude all Source Folder subdirectories in the selected Operation.

Continue on error

Select this check box to continue performing the selected Operation regardless of any errors that occur during the execution of the action. Clear this check box to stop the selected Operation if an error occurs.

Include hidden/system files

Select this check box to include all hidden and system files in the selected Operation. Clear this check box to ignore all hidden and system files in the selected Operation.

Overwrite read-only files

Select this check box for the selected operation to overwrite or delete read-only files. Clear this check box for the selected operation to ignore all read-only files.

Overwrite existing files

For Copy or Move/Rename operations, select this check box for the operation to overwrite existing files. Clear the check box for the operation to ignore existing files.

Overwrite older files

For Copy or Move/Rename operations, select this check box for the operation to overwrite existing files if the destination file is older than the source file. Clear the check box for the overwrite operation to ignore overwriting destination files that are older than the source files.

Perform copy asynchronously

Select this box to perform the selected operation asynchronously. In asynchronous mode, the File Operations element will execute at the same time as other File Operations elements. If this check box is cleared, applications will run sequentially one after another. Each application must complete before the next one will begin.

Redirect to 32 bit folder on 64 bit operating systems

Select this box to force the operation to copy files to the corresponding 32-bit folder, when performing the operation on 64-bit operating systems.

Wipe disk area to DoD 3 spec

Available for Move/Rename and Delete operations, select this check box to securely remove files/folders from the specified source using the DoD 3 specification.

Show progress bar

Show the progress of the file operation.

Possible File Operations

Source Folder	Source File	Destination Folder	Destination File	Operation
X		X (non-existing)		**Rename** folder
X		X (existing)		**Move** folder
X	Single	X		**Move** file to different folder
X	Multiple	X		**Move** files to different folder

Source Folder	Source File	Destination Folder	Destination File	Operation
X	Single	X	Single	**Rename** file
X	Multiple	X	Single	**Not supported**
X	Single	X	Multiple	**Not Supported**
X	Multiple	X	Multiple	**Not supported**

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Folder Redirection

The **Folder Redirection** object provides the ability to change the Windows default location for specialized folders known as *Shell Folders*. Shell folders are folders that are specific to each authenticated user. They include the Contacts (Windows 7, Windows 8.1), Cookies (Windows 8.1), Desktop (Windows 8.1), Downloads (Windows 7, Windows 8.1), Favorites (IE Bookmarks)(Windows 8.1), History (Windows 8.1), My Music (Windows 8.1), My Pictures (Windows 8.1), My Videos (Windows 7, Windows 8.1), Personal (My Documents Folder)(Windows 7, Windows 8.1), Programs Group (Windows 7, Windows 8.1), Recent (Windows 7, Windows 8.1), Send To (Windows 7, Windows 8.1), Start Menu (Windows 7, Windows 8.1), Startup (Windows 7, Windows 8.1) and Temporary Internet Files (Windows 7, Windows 8.1).

Shell folders are located under the authenticated user's profile, C:\Documents and Settings*profilename*\.

By defaulting the location of these folders to a network share (or mapped drive), rather than the local computer, users are allowed to access their own desktop, bookmarks, recent document list, application settings, etc., regardless of the computer they log on to. This also enables the profile to be secured and backed up.

In addition to user-specific shell folders, Windows 2008/7/8.1/2008 R2/2012/2012 R2/2016/2019 also includes a common set of shell folders that are available to all users of the computer. This common set of shell folders is often referred to as the "All Users" profile or "Users Profiles".

Settings

Action

Shell folder

Select a shell folder from the Shell folder list.

> **NOTE:** Redirecting Temporary Internet Files to a network share is not supported with IE 8 and later.

Redirect to folder

Specify a folder that the shell folder should be redirected to. The folder designation may be in the form of a path, mapped drive or UNC. Click **Browse** to navigate to the path. Desktop Authority's dynamic variable selection is available for this field by pressing the F2 key.

> **NOTE:** Although a path in the form of C:\RedirectedFolder may be used, it is recommended that a fully qualified UNC be used instead. Note that UNC paths longer than 260 are truncated by the operating system. If this occurs, the folder redirection will not work.

Reset to default

Select this check box to restore the redirected folder to the operating system's default location.

Copy any files that exist in the original folder

Select this check box to copy files from the current folder to the redirected folder when it is redirected.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

General

The **General** object provides several miscellaneous settings including settings to purge the client TEMP files, password expiration warnings and others.

Settings

TEMP Files

Enable purge

Select this checkbox to enable purging of the client computer's %TEMP% folder.

Purge client %TEMP% files on the first Wednesday of every month

%TEMP% is an environment variable that defines the location of the User's temporary files folder. Desktop Authority can easily control the purging of this folder in order to keep the client's machine free of extraneous, unused files. The user will never have to remember (or forget, as is usually the case) to manually purge this folder.

Purging is completed on the first Wednesday of each month.

Select **Prompt** from the list to let the user decide whether to purge the **%TEMP%** folder.
Select **Always** from the list to purge the **%TEMP%** folder on the first Wednesday of each month.

Specify the file(s) to purge from the %temp% folder. Use wildcards to specify multiple files. A subfolder may also be specified.

The default is **[Prompt]** purge.

File mask

Specify a file mask that defines exactly what files to include in the purge operation.

The default is to purge all ***.tmp]** files.

Warnings

Password expiration

Enter a numeric value, or use the arrows, representing the number of days prior to expiration in which to enable a warning to the client that their password is about to expire. The warning will give the user an advanced reminder the specified number of days before the password will expire. If no number is entered, the warning is disabled.

Low disk space

Enter a numeric value, or use the arrows, representing the number of megabytes to enable a warning to the client if disk space falls below the specified size. If no number is entered, the warning is disabled.

Local admin password

To define local admin access for clients, enter the local admin username/password. After entering the local admin password, click OK. The password will be encrypted for display purposes in the Manager.

Set password

Select this box to use the currently logged on user credentials as the local admin password. Deselect this box to modify the credentials. Enter the Password twice to enter a new local admin password.

Network

Disconnect all existing network drives before mapping new ones

Select this check box to forcibly disconnect all existing network drive mappings before Desktop Authority drive mapping elements are executed. If Desktop Authority is executed and this check box is not selected, any persistent connections that the client may have defined for the same drive letter to be mapped by Desktop Authority will be overridden. Desktop Authority will not automatically remove all persistent connections on each client (unless this check box is selected) — only the ones that conflict with the mappings being applied by Desktop Authority during the logon process.

Disconnect all existing network printers before connecting new ones

This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  . Select this check box to forcibly remove all existing network printer mappings from the client before Desktop Authority printer mapping elements are executed. Clear this check box to leave the computers existing printer mappings as is. Gray the check box to leave the printer mappings set to what they have already been validated for.

Disconnect all existing IP printers before connecting new ones (excludes server operating systems)

This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  . Select this check box to forcibly remove all existing IP printer mappings from the client before Desktop Authority printer mapping elements are executed. Clear this check box to leave the computers existing printer mappings as is. Gray the check box to leave the printer mappings set to what they have already been validated for.

> Note: IP printers on servers will not be disconnected by this option.

Concurrent drive limit

Limit concurrent logons by monitoring the share mapped using drive

This option provides a mechanism by which the number of concurrent logons by a single user can be limited. Implementation of this feature requires a combined effort between Desktop Authority and the domain's servers where the shares reside.

Once configured, Desktop Authority will immediately log off any user that attempts to concurrently log on more sessions than they are allowed.

Additional

Don't display last user name

Use this setting to clear or set the previous user's logon name.

Set this check box to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  . Select this check box to clear the logon name of the previous user of the computer. The user name entry will be blank on the logon dialog box the next time a user logs onto the computer. Clear the check box to display the previous user's name. The user name will be shown in the logon dialog box each time a user logs on to the computer. Gray the check box to disable Desktop Authority's control of the user name.

Clear all existing security policies

Select this check box if you are using Desktop Authority's Security Policies **only**. This setting instructs Desktop Authority to remove all existing security policies prior to applying new ones. Removing a security policy removes the setting from the registry which in effect disables the policy from being applied to the workstation.

Clear this check box if you are using Microsoft's Policies in combination with Desktop Authority's Security Policies. Microsoft's Group Policies are applied to the computer before the logon script executes, this option will ensure that Desktop Authority does not "clear" the existing Microsoft Policies.

Graying this check box acts exactly as if the check box is cleared unless there are other elements that either Select or Clear this option. If there are other elements with a selected or cleared check box, this option will be ignored. The last setting processed, either selected or cleared will take precedence over all other settings.

Remove IE tour

Select this check box to remove the Internet Explorer Take a Tour splash screen. Once removed, it cannot be reactivated by Desktop Authority.

Remove Internet connection wizard

Select this check box to remove the Internet Connection Wizard and prevent it from launching the first time each user of the computer attempts to launch Internet Explorer. Once the Internet Connection Wizard is removed, it cannot be reactivated (added back to the desktop) by Desktop Authority.

Do not show Desktop Agent icon in system tray

This check box can be set to one of three (3) different states: on (enabled),  ,hide the Desktop Agent icon in the system tray, off (disabled),  , show the Desktop Agent icon in the system tray, or grayed,  , preserve Global Desktop Agent setting.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Group Policy Templates

Overview

Administrative Template files are used by the Group Policy Templates object to describe security policy settings and where they are stored in the registry. Administrative templates include a policy category, policy options and registry settings for each policy contained within the template. Group Policies are rules that administrators can employ to enforce a specific desktop environment. Policies can apply to the entire domain or an individual computer or user. They are made up of a combination of one or more Registry keys.

There are several standard administrative templates that are installed with Windows 2008, 7, 8.1, 10, 2008 R2 2012, 2012 R2, 2016, and 2019. Additional Administrative templates are available in several of Microsoft's Resource kits, service packs and the Microsoft Download center. Templates can also be created from scratch or customized to meet specific needs. Custom templates are also available online for download from various sources.

Although Microsoft has its own built-in Group Policy editor, Desktop Authority lets you use existing Administrative templates providing a simpler interface for configuring the Group Policies contained within them. Using Desktop Authority's patented Validation Logic allows a policy to be configured to a granular level including OS, Class, Connection Type and more.

All Group Policies that are a part of the selected ADM/ADMX templates will be displayed within their defined categories in the Administrative Templates tree on the Settings tab. ADM Templates are displayed in the Classic Administrative Templates tree and are valid for operating systems prior to Microsoft Windows 7. ADMX Templates are used by Microsoft Windows 7 operating system and above. ADMX Templates are displayed in the Administrative Templates tree. Select a Policy category from the template tree. Once selected, the Policies within the category will be displayed in the Policy list to the right of the tree. Once the policy to be configured is selected, the Policy Setting and Explanation will be displayed.

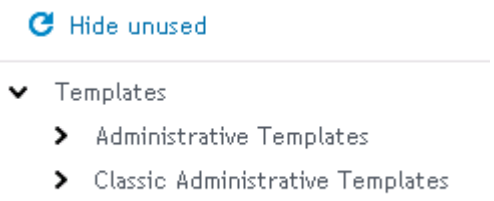
Configure the Policy on the Policy Setting tab. Once configured, click Apply Changes to accept the changes for the current Group Policy element. Click Discard changes to undo the latest changes. Review a description on the Policy Explanation tab. To save the Group Policy element, click the Save toolbar button.

Settings

Administrative templates tree

The Classic Administrative Templates tree displays the categories for all policies within the selected ADM template files. Policies within the ADMX template files are shown in the Administrative Templates tree. Each category displays the policies available for configuration in a list to the right of the category.

Figure 44: Administrative Template Tree



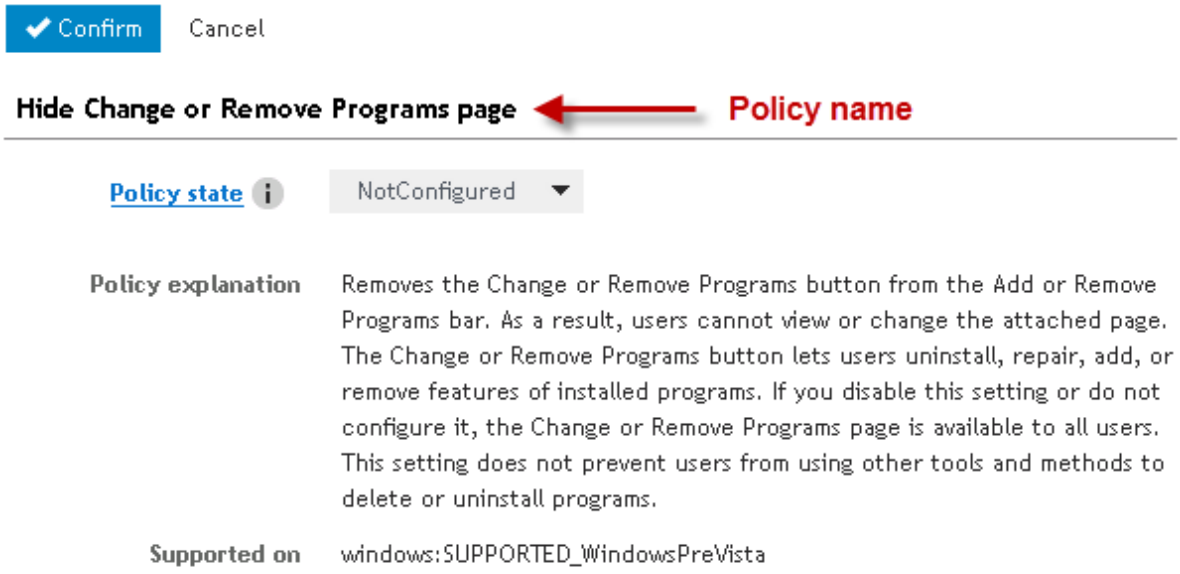
Click the **Hide Unused** button to hide policies in the list that are not yet configured. If policies are hidden, click **Show Unused** button to display all policies, configured or not.

Policy list

The Policy list displays all policies for the category selected in the Administrative Template tree. Click on a policy to select it. Press the **Edit** button to edit the policy settings.

Policy configuration

Figure 45: Policy configuration dialog



The Policy configuration tab is where each Policy is configured. The setting is displayed along with its configuration state and options. Once the policy's options are set, click **Confirm** to accept the changes for the current Group Policy element. Click **Cancel** to undo the most recent changes.

Policy Explanation

The Policy explanation provides a complete description of the policy and its settings.

Add/Remove ADM files

Desktop Authority's Group Policy Templates object provides the ability to import Classic Administrative templates and deploy the policy settings contained within them.

Once a Group Policy Template element is added to the configuration list, administrative template settings can be configured. This requires that Administrative templates be imported into the system. By default, the Operations Master's %windir%\inf folder is scanned for existing ADM files. All ADM files that are found are imported into Desktop Authority and copied to the Group Policy folder. By default, CONF.ADM, INETRES.ADM, and SYSTEM.ADM are selected for use in the Group Policy element.

To add a new ADM template to the list, click **Import template files**. Browse to the ADM template file and select it. Click Select to confirm the selection. The template file will be automatically be imported and added to the list. All policies within the template file are immediately available for use in a Group Policy Templates element.

Select the template file(s) that will be used with this Group Policy Templates element (☑). Once template files have been selected, select the Settings tab to configure them.

Add/Remove ADMX files

Desktop Authority's Group Policy Templates object also provides support to import ADMX Administrative templates and deploy the policy settings contained within them.

Once a Group Policy Template element is added to the configuration list, administrative template settings can be configured. This requires the Administrative templates be imported into the system.

ADMX file location

The ADMX file location defines where Desktop Authority will hold the ADMX file to be used by the system. Upon import, the system makes a copy of the file and places it in the selected file location.

Select Use default location, to use the Desktop Authority default path for ADMX files. This path is %program files%/Quest\Desktop Authority/Desktop Authority 9.0/TemplateFiles. To select a custom path, choose Global location. The Global location path is set on the Global Settings (Global_System_Settings.htm) dialog.

Available ADMX template files

Import template files

To add a new ADMX template to the list, click **Import template files**. Browse to the ADMX template file and select it (multiple ADMX files can be selected). Click Open to confirm the selection. The template file(s) will be automatically be imported and added to the list. All policies within the template file are immediately available for use in an Group Policy Templates element. Select the template file(s) that will be used with this Group Policy Templates element (☑). Once template files have been selected, select the Settings tab.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Inactivity

The **Inactivity** object allows automatic Logoff, Shut down, Restart, or Locking of a computer based on a period of inactivity occurring within a specified period of time. Inactivity detection time is set in half-hour increments. Inactivity settings are particularly useful in situations where you need users to logoff at the end of the day so appropriate updates are applied to all machines at logoff or the next logon. The Inactivity option of locking a computer when inactive is supported on 2008, 7, 8.1, 10, 2008 R2, 2012, 2012 R2, 2016, and 2019 operating systems only.

To select or clear an inactivity period, highlight a range of cells in the inactivity grid. Press **Unselect** to clear the cells. Press **Select** to select the cells. To select an entire day, double click the day of the week label to the left of the

grid. To select a specific half-hour increment for every day of the week, double click the blue box in the All row above the grid.

Multiple inactivity settings are supported per computer, if and only if, there are no overlapping inactivity monitoring times. If any part of the detection hours overlap between elements, only the first element will be processed.

For example, if element 1 is monitoring for inactivity between the hours of 5:00am - 7:30pm and element 2 is monitoring for inactivity between the hours of 6:00am - 5:30pm, there is a period of time between 6:00am and 5:30pm which are contained in both elements. In this case, only element 1 would be processed on each applicable client.

Settings

Action

Select Logoff, Always Shutdown, Shutdown, Restart, Standby, Hibernate or Lock from the Action list. This action will occur if the computer is considered inactive for the elapsed time specified.

Logoff— When the computer is considered inactive, log the user off.

Always Shutdown — When the computer is considered inactive, Shutdown the system regardless if any users are logged in.

Shutdown — When the computer is considered inactive, Shutdown the system only if there are no users logged in.

Restart — When the computer is considered inactive, Restart the system.

Standby — When the computer is considered inactive, put the system in Standby mode. Standby will turn off the monitor, stop the disk drives and save the current computer state into memory. At the touch of the mouse or keyboard your computer will wake up, and return to the state where you left it. In Standby mode, the computer is put into a low power state.

Hibernate — When the computer is considered inactive, put the system in Hibernation mode. In order for a computer to go into Hibernation, Hibernation mode must be enabled in the computer Power settings. If Hibernation is not enabled on the computer, selecting this option will put the computer in StandBy mode. Hibernate mode will turn off the monitor, stop the disk drives and save the current computer state into memory. The computer will then be turned off. When the computer is restarted it will return back to the state where you left it.

Lock — When the computer is considered inactive, Lock the system.

> **NOTE:** The Lock and Logoff actions only validate on Terminal Server clients, Member servers and Domain controllers.

Desktop user can delay inactivity for a maximum of xx hours

There are some cases when the computer may seem to be inactive but is actually in use. For example, the computer may be running a video or a large procedure that does not require user interaction. To give the user the opportunity to delay the inactivity action for a period of time, specify the number of hours inactivity may be delayed for.

Duration of inactivity before action (in minutes)

Specify a period of time in minutes for which the computer must be inactive before the *Action* takes place. A computer is considered inactive based on any keyboard and mouse activity.

User warning

Warn before taking action

Prior to the selected Action (Logoff, Always Shutdown, Shutdown, Restart, Standby, Hibernate, Lock) occurrence, a warning dialog may be displayed for a specified number of minutes. If the warning dialog is responded to, the Action will not take place. Once the warning box is displayed, keyboard and/or mouse activity will not abandon the desired action. The warning box must be responded to in order to cancel the Action.

Warning to display

Specify the text to display in the warning box.

Sound to play

Specify a sound file (.WAV) to play when the inactivity warning is displayed.

Duration of warning (in minutes)

Specify the number of minutes to display the warning dialog on the inactive computer.

Detection hours

Unselect

Click **Unselect** after selecting a set of cells in the grid to set the selected period of time as unmonitored time.

Select

Click **Select** after selecting a set of cells in the grid to set the selected period of time as monitored time. Monitored time periods will display as colored blocks.

Clear All

Click **Clear All** to remove any selections in the grid.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

INI Files

INI Files provide a means of configuration to many programs. The INI Files object provides a single point of control over changing values in an INI configuration file.

Settings

INI file action

Action

Select an action from the Action list to define how the INI file is to be updated. INI files can be updated by adding or deleting a Section, and/or adding or deleting a Value or Data/Expression within a specific section.

Available actions are:

- *Write Value*
  Store the data/expression along with the specified Value to the INI File's section. If the Section does not exist it will also be created. If the Value does not exist in the INI file, it will be created in the specified section.
- *Delete Value*
  Remove the specified value from the specified section in the INI file.
- *Delete Section*
  Delete the specified section in the INI file. If the Section already exists, it will be removed.

Filespec

Enter the name of the INI file to be updated. If no path is specified, Windows will try to locate the file in the Windows directory.

Section

Enter the name of the section that will be updated. If the Section does not exist in the INI file, it will be created. Section names are not case-sensitive; therefore, "ThisSection" is equivalent to "thissection".

Value

Enter the name of the value that will be updated in the INI file. If the Value does not exist in the specified section, it will be created. Value is not applicable when the Action is set to Delete Section.

Data/expression

Enter the data you would like stored in the specified Value. Data is not applicable when the Action is set to Delete Section or Delete Value.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Legal Notice

The **Legal Notice** object allows a company-wide logon banner or notice to be centrally configured. This notice must be acknowledged by pressing the **Ok** button. The legal notice is displayed on the client prior to actually logging on to the domain. The Legal Notice differs from *Message Boxes*, in that it is displayed **before** the user authenticates to the domain. This provides a way for the company to spell out or remind staff of company policies regarding use of the computer network, email, Internet access, etc.

Since displaying a legal notice would interfere with the automatic logon process, the Legal Notice will NOT be applied to any 2008//7/8.1/10/2008 R2/2012/2012 R2/2016/2019 computer if the computer has AutoAdminLogon enabled.

Settings

Legal notice

Clear Legal Notice

Select this check box to temporarily disable the Legal Notice from displaying on your clients. Clear this check box to configure a legal notice.

Window title

Enter a caption for the window frame in which the message text will be displayed. Static text or Desktop Authority Dynamic Variables can be used to configure the window title.

Example:

WARNING: Use of this computer is restricted and monitored!

Message

Enter the actual message text that will be displayed in the Legal Notice window.

Example:

Information contained within this computer system may be protected by the Privacy Act of 1974. All output, both visual and printed, must be marked appropriately and all precautions taken to prevent unauthorized use or disclosure. Do not discuss, enter, transfer, process, or transmit classified/sensitive national security information of greater sensitivity than that for which this system is authorized. This system is approved for SENSITIVE but UNCLASSIFIED information only. This is a Department of Defense (DoD) computer system. This computer system, including all related equipment, networks and network devices (specifically including Internet access), are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal

information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Logging

The Logging object maintains log files used to track information about users logging onto the network and the computer they are logging on from. Several customized fields of information may be stored in the log file. The first 17 fields are automatically configured by default. They may be changed, deleted, or added to, to meet specific needs.

Log files are Comma Separated Value (.CSV) formatted files. These files may be viewed by clicking View Logs. These files may also be viewed in any text editor, including notepad.

Log files use the profile name and current date for its file naming convention. The file name is in the format of *ProfileName_YYYYMMDD.CSV* and is stored in the LOGS$ share, by default. A single log file is created once per day per profile and contains all logon information for the day and profile.

Log file location

Path

Enter the location where the log files will be created or press **Browse** to select a folder. The location may be specified in the form of a path, mapped drive or UNC. Dynamic variables may be used as an aid in defining the location. Press F2 to select a dynamic variable from the popup list.

If specifying a UNC, the location should be specified in the form of **\\server\share**. Typically, the log file folder is a shared folder and is stored on a Domain Controller.

The default share name (unless modified during the install) is set to LOGS$.

Example:

\\pdcserver\LOGS$$ use LOGS$ share on pdcserver

To disable logging, clear the specified **Path**.

Variable list

Log file list

Log files can be configured with several fields of customized information. Log file elements within the list are processed in the order that they appear in the list.

Click **Add** to add a new element to the list. This will add the new element to the end of the list.

Click the **Edit** link to edit the existing highlighted element in the list. Enter static text into the variable field, select a variable from the drop down list and/or press F2 or the **Insert dynamic variable** link to use insert a dynamic variable.

Copy will duplicate the selected element. You are given the opportunity to modify the settings at the time of the copy.

Click **Delete** to remove the highlighted element from the list.

Use **Move Up** and **Move Down** to reorder the elements in the list by moving the selected element up or down.

The following variables are defaults in new profiles:

Variable	Description
$Date	Current date
$Time	Current time
$LogonServer	Authenticating Domain Controller
$ConnType	Connection method
$WrkSta	Computer Name
$SiComputerType	Computer Type
$IPaddr	TCP/IP address
$SiCpuType	CPU Type
$SiCpuSpeed	CPU Speed
$SiRamMb	Physical RAM (Mb)
$SystemDrive	System Drive
$VerboseOS	Verbose Operating System version
$OSCSDVersion	Current service pack
$HotFixes	Current Hot Fixes
$IeCurVer	Internet Explorer version
$OfficeCurVer	Microsoft Office version
$UserID	User ID
$FullName	User's full name
$Description	User account Description

View logs

Click the View Logs tab to open the Log File Viewer.

Available logs

Filter the available log files by Profile, Year and Month.

Purge old log files

Purge log files older than

Enter the age of log files to purge. Files must be older than the number of months specified. Click **Purge** to remove files.

Message Boxes

The Message Boxes object allows you to centrally manage and configure popup messages. This popup window is displayed on the client during the logon process after the user is authenticated. Message boxes can be used to notify users of scheduled downtime or upcoming company events.

Since displaying Message Boxes could interfere with the automatic logon process, Message Boxes will NOT be displayed on any computer if AutoAdminLogon is enabled.

Settings

Message box

Window title

Type in static text or press the F2 key to select a dynamic variable. The window title is displayed at the top of the popup window.

Message

Enter the text to be displayed in the message box. Dynamic variables can be used in conjunction with your text. Press the F2 key to select a dynamic variable.

Style

Select a message box style from the Style list. Choose from *Information*, *Warning*, or *Error*. Each style displays an icon to the left of the message. The styles make use of the following icons in the message box:

 Information (i)

 Warning (!)

 Error (x)

Timeout

Enter a numeric value representing the number of seconds the message box will be displayed for. It will be displayed for this number of seconds unless the OK button is pressed before the timeout occurs. Enter 0 to disable the timeout function.

Cycle

UID

The UID entry is used to make each element in the Message Box list, a unique item, regardless of the contents of the message box. The data in this entry is automatically generated and should not be modified. However, if an configuration element in the list is set to run *Once Per Day or One Time*, and must be executed a second time, the UID can be changed by clicking  .

Frequency

Select *One Time (Computer)*,*One Time (User)* ,*Once Per Day (Computer)* ,*Once Per Day (User), Every time* elect a logon frequency from the drop-down list. Select from

- Select *Every time* to display the Message Box at the specified cycle, every time the user logs on or off the network.
- Select *Once Per Day (User)* to display the Message Box at the specified cycle, one time per day for the current user.
- Select *Once Per Day (Computer)* to display the Message Box at the specified cycle, one time per day for the computer.
- Select *One Time (User)* to display the Message Box at the specified cycle, a single time for the current user.
- Select *One Time (Computer)* to display the Message Box at the specified cycle, a single time for the computer.

The Message Box is displayed at the specified cycle and frequency.

Cycle

Select a time interval for which your message box will display. Choose from *Everyday*, *Day of Week*, *Monthly (Day of Week)*, *Monthly (Day of Month)*, or *Specific Date*.

- Selecting *Every time* as the cycle, will force the Message Box to be displayed each logon, logoff and refresh as specified in the validation logic.
- Selecting *Day of Week* as the cycle presents a new Day of Week list allowing the selection of a day from Sunday to Saturday. The Message Box will be displayed on the specified day, every week, at the selected frequency.
- Selecting *Monthly (Day of Week)* as the cycle, presents a new Day of Month list allowing the selection of a day in the month ranging from 1st Sunday, 1st Monday, . . . to the last Saturday of the month. The Message Box will be displayed on the specified day, at the selected frequency.
- Selecting *Monthly (Day of Month)* as the cycle, presents a new Day of Month list allowing the selection of a day number of the month. The Message Box will be displayed on the specified day of the month, at the selected frequency.

- Selecting *Specific Date* as the cycle presents an entry to which the specific date should be entered. Press the Date arrow to make your date selection from any calendar day. The Message Box will be displayed on the specific day, at the selected frequency.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Microsoft Office Settings

The Microsoft Office object provides the ability to centrally configure default file locations for Microsoft Office.

By centrally configuring the paths used by Microsoft Office, it is ensured that user-created documents are stored to network servers rather than locally on the user's computer. This enables documents to be secured, backed up nightly, and made available to the user regardless of which computer the user logs on from.

ⓘ Note: Microsoft Office 2010 and 2016 are supported.

Settings

Application options

Application/suite

Select an application including the version from the list.

Option

Select an option from the list. The content of the list varies based on the Application/Suite chosen.

Path

Specify a path that the selected option should be redirected to. The path may be in the form of a path, mapped drive or UNC. Click **Browse** to navigate to the path. Optionally, press the F2 key to use a Desktop Authority dynamic variable.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Microsoft Outlook Profiles

The Microsoft Outlook Profiles object provides the ability to configure one or more client mail profiles. Mail profiles are part of the Windows Messaging system and are used to define the services and options needed to connect the Outlook client to your Microsoft Exchange server. An administrative template can be established that will automatically configure the most common services used by Outlook when your clients log on to the network.

Desktop Authority will automatically create mail profiles for a user on any computer that they log on to. With Desktop Authority performing this necessary administrative task, a visit to each desktop will be saved. Your users will benefit from increased productivity if they roam to different computers — no matter which computer they log on to. They will have access to their electronic mail instantly!

Mail Profile creation requires Internet Explorer 4.01 or greater to be installed on the client.

NOTE: Microsoft Outlook 2010, 2013, 2016,Exchange 2010, 2013, 2016 and Exchange Online are supported.

NOTE: Exchange Online support (Microsoft's cloud-based Exchange solution) is limited to the on-premise configuration of supported versions of Microsoft Outlook as an Exchange Online email client. It does not include support for configuring any cloud-based (off-premise) Exchange Online server or client properties.

Settings

Mail profile

If user has an existing profile, do not apply the settings below

Select this check box disable the creation of profiles for users that have existing profiles on the client they are logging in from. Clear this check box to enable the creation of mail profiles regardless of whether there are existing profiles for the user.

Delete all profiles except for user's default profile

Select this check box to delete all profiles for this user except the user's default profile.

Rename user's existing default profile if mail profile name is different

If the user mail profile name is different than what is specified as the Mailbox name, select this check box to rename the existing profile. Leave this check box clear to keep the existing profile name.

Delete all backup profiles created during configuration

Select this check box to remove all backup profiles.

Mail profile name

Enter the name to be used for the new profile creation. This can be static text, a Desktop Authority dynamic variable, or a combination of the two. Press the F2 key to select a dynamic variable.

The default value for the mail profile name is $FullName.

Mailbox name

Enter the name of the mailbox the user will be connected to on the Exchange Server. Press the F2 key to select a dynamic variable.

The Mailbox name must match the Display Name, Alias or Distinguished Object name defined for the user on the Exchange Server. To achieve this, use a dynamic variable. This may need to be used in combination with static text.

The default for this field is $UserID, which typically matches the user's Display Name defined in Exchange.

Exchange Mail server

Enter the name of the Exchange server to which the profile will be connected to. Type the server name into the field or click **Browse** to locate and select a server. Press the F2 key to select a dynamic variable.

Cached Mode

Select this check box,  , to configure Outlook to use its Cached Exchange Mode. Clear the check box,  , to remove the use of Cached Exchange Mode.

Connect to Microsoft Exchange using HTTP

Select this check box,  to configure Outlook to configure Outlook to Connect to Microsoft Exchange using HTTP. Clear the check box,  , to remove the use of this setting.

Exchange CAS (Proxy) server

Enter the name of the client access server or proxy server. Type the server name into the field or click **Browse** to locate and select a server. Press the F2 key to select a dynamic variable.

Connect using SSL only

Select this check box,  , to enforce that a Secure Sockets Layer protocol is used when data is transmitted over HTTP. Clear the check box,  , to remove the SSL protocol restriction.

On fast networks, connect using HTTP first, then connect using TCP/IP

Select this check box,  , on fast internet connections, such as DSL or Broadband, to connect to the Exchange server via HTTP first. If the connection is unsuccessful, TCP/IP will be used to connect to the Exchange server.

On slow networks, connect using HTTP first, then connect using TCP/IP

Select this check box,  , on slow internment connections, such as dial-up, to connect to the Exchange server via HTTP first. If the connection is unsuccessful, TCP/IP will be used to connect to the Exchange server.

Use this authentication when connecting to my proxy server for Exchange

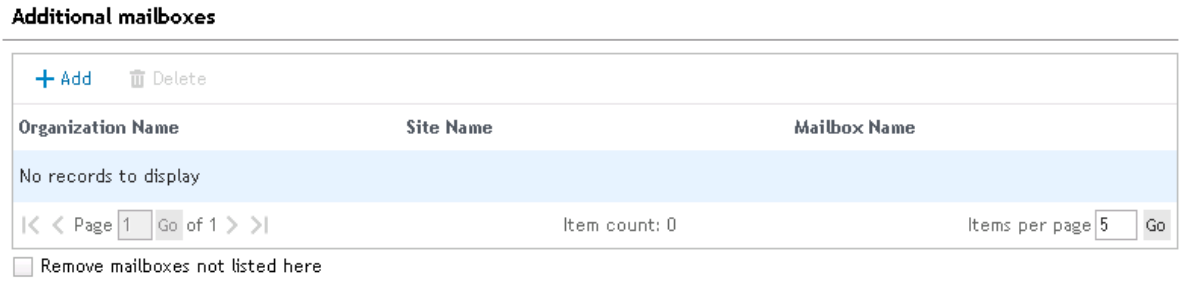
Open the drop down list and select the authentication method you want to use when connecting to your proxy server. Options include **Negotiate**, **Basic** and **NTLM Authentication**.

> Note: Please refer to your Exchange/Outlook version-specific documentation for more information regarding authentication.

Additional mailboxes

> Note: Please note that Microsoft Outlook must be opened once on individual client machines before Desktop Authority is able to configure additional mailboxes.

Many times it is necessary to assign a delegate to a mailbox. A delegate is someone who is given permission to view a mailbox other than their own. The mailbox will be added to the delegates profile and be visible to the user when Outlook opens. Click **Add** to add a mailbox to the Mailbox list. Specify the mailbox owner's UserName as the mailbox name. Click **Delete** to remove the selected mailbox from the mailbox list.



Additional mailboxes will be assigned to any user who validates for the configuration setting. In order for the user to have permission to view the additional mailbox, the delegate must be granted permission to view the nominated mailbox. Desktop Authority will take care of adding the additional mailboxes to the delegate's profile.

Remove mailboxes not listed here

Select this check box to remove any mailbox associated with the mail profile that is not explicitly defined in the Desktop Authority mailbox list.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Microsoft Outlook Settings

The Microsoft Outlook Settings object provides the ability to configure several Microsoft Outlook configurations. Outlook client settings are configured during the logon process. These settings are reconfigured each time a user logs on to the network.

NOTE: Microsoft Outlook 2010, 2013 and 2016 are supported for use with on-premise versions of Exchange

NOTE: Microsoft Outlook 2016 is currently the only version of Outlook supported for use with Exchange Online (Microsoft's cloud-based Exchange solution). Additionally, new Exchange Online users will need to re-login at least once (after they have launched Outlook and supplied their password) before their expected Outlook settings will be applied.

NOTE: Please note that Microsoft Outlook must be opened once on individual client machines before Desktop Authority is able to configure any of the following Outlook Settings.

General settings

General settings

View Outlook bar

Select this check box,  , to display the Outlook shortcut bar upon entry into Outlook. Clear the check box,  , to hide the Outlook shortcut bar. Gray the check box,  , to preserve the user's current Outlook setting.

The Outlook bar is available in versions of Outlook prior to 2003. This is not a feature in Outlook 2003.

View folder list

Select this check box,  , to display the folder list upon entry into Outlook. Clear the check box,  , to hide the folder list. Gray the check box,  , to preserve the user's current Outlook setting.

The folder List is available in versions of Outlook prior to 2003. This is not a supported in Outlook 2003.

Warn before permanently deleting items

Select this check box,  , if Outlook should warn the user before deleting entries from the Deleted Items folder upon exit. Clear the check box,  , to disable any warning that entries will be deleted from the Deleted Items folder. Gray the check box,  , to preserve the user's current Outlook setting.

Startup in this folder

Select an Outlook folder from the list. Choose from *Outlook Today*, *Inbox*, *Calendar*, *Contacts*, *Tasks*, *Journal* and *Notes*. The selected folder is the default folder that will be opened upon Outlook startup. Select *User-defined* from the list to use the folder as specified in the clients Outlook options.

Outlook Today is not supported in Outlook 97. If Desktop Authority detects Outlook 97, and the *Outlook Today* folder is selected, Desktop Authority will set the startup folder to the *Inbox*.

Empty Deleted Items folder on exit

Select a day of the week, *Everyday* or *Never* from the list. This selection controls when the entries in the Deleted Items folder will be permanently deleted. Select *User-defined* from the list to use the setting as specified in the

client's Outlook options.

New mail arrival

Display a notification

Select this check box,  , to enable a visual notification when new mail arrives to the inbox. Clear the box,  , to disable any visual notification of new email. Gray the check box,  , to preserve the user's current Outlook setting.

Play a sound

Select this check box,  , to play a sound when new mail is received. Clear the box,  , to provide no audio notification of new email. Gray the check box,  , to preserve the user's current Outlook setting.

AutoArchive

AutoArchive every xx days

Select this check box,  , to configure Outlook items for archival. Clear this check box,  , to disable the AutoArchiving of Outlook items. Gray the box,  , to preserve the user's current Outlook setting.

If AutoArchiving is activated, items will be archived every x number of days. The number of days must be between 1 and 60. If a value of 0 is entered, the client's current profile setting will be used.

Prompt to autoarchive

Select this check box,  , to prompt the user that autoarchiving is about to occur. This will give the user the ability to cancel the archival process. Clear this check box,  , to never prompt the user about the archival process. Gray the check box,  , to preserve the user's current Outlook setting.

Folder

Enter the folder where the archive files should be stored. Manually type the path or UNC into this field. Alternatively, click **Browse** to navigate to the folder.

If the specified folder does not exist, Desktop Authority will create it. If no folder is specified, Desktop Authority will use the client's current profile setting. This will allow each client to specify a location of their choice.

File name

Enter the name of the file to store archived items to. This file will be stored in the Folder specified in the **Folder** entry.

The default for this field, is $UserID.PST, which uses a dynamic variable to build the file name. To insert a dynamic variable, press the **F2** key to select it from the list. The dynamic variable will be inserted into the field at the cursor's current position.

If the specified file does not exist, Desktop Authority will create it. If no file is specified, Desktop Authority will preserver the user's current setting.

Delete expired items (email folder only)

Outlook items can be deleted instead of archived using the Delete expired items options. This option will delete old items instead of moving them to an archive file. Select this check box,  , to delete items instead of archiving them.

Clear this check box, ☐, to archive items instead of deleting them. Gray this check box, ▣, to preserve the user's current Outlook setting.

When sending a message

Allow comma as address separator

Select this check box, ☑, to allow the use of commas (,) as well as the standard semicolons (;) to separate names in the To, Cc and Bcc address lines. Clear this check box, ☐, to only allow the standard semicolon (;) separator. Gray this check box, ▣, to preserve the user's current Outlook setting.

Automatic name checking

Select this check box, ☑, to allow Outlook to check the names entered into the To, Cc and Bcc address lines. Names are checked against the address book. If the name is found, it is underlined. Clear this check box, ☐, to disable automatic name checking. Gray this box, ▣, to preserve the user's current Outlook setting.

Message format and handling

Message format

Select a message format from the list. Choose from *User-Defined*, *HTML*, *Rich Text* or *Plain Text*. When creating new messages this format will be used.
Choose *User-defined* to allow the user to control the message format.

Use Microsoft Word as editor

Select this check box, ☑, to tell Outlook to use Word when creating or editing messages. Clear this check box, ☐, to use Outlook's default editor. Gray this check box, ▣, to preserve the user's current Outlook setting.

Send pictures from the Internet

Select this check box, ☑, to send any pictures that are part of the message. Clear this check box, ☐, to disable the sending of attached pictures. Gray this check box, ▣, to preserve the user's current Outlook setting.

Save copies of mail in 'Sent Items' folder

Select this check box, ☑, to save a copy of each outgoing message in Outlook's Sent Items folder. Clear this check box, ☐, to disable the saving of a copy of each outgoing message. Gray this check box, ▣, to preserve the user's current Outlook setting.

Auto-save unsent messages every xx minutes

Select this check box, ☑, to allow Outlook to automatically save a copy of unsent messages to the Drafts folder. Messages will be saved every xx minutes. Specify the number of minutes in the entry box. Clear this check box, ☐, to prevent saving a copy of unsent messages. Gray this check box, ▣, to preserve the user's current Outlook setting.

Spelling

Always check spelling

Select this check box,  , to configure Outlook's spell check to always spell check a message before sending it. Clear this check box,  , to disable spell check on outgoing messages. Gray this check box,  , to preserve the user's current Outlook setting.

Always suggest replacements

Select this check box,  , to configure Outlook's spell check to always suggest word replacements for misspelled words. Clear this check box,  , to disable misspelled word replacement. Gray this check box,  , to preserve the user's current Outlook setting.

Ignore words in UPPERCASE

Select this check box,  , to configure Outlook's spell check to ignore all uppercase words during spell check of a message. Clear this check box,  , to include uppercase words during the spell check of a message. Gray this check box,  , to preserve the user's current Outlook setting.

Ignore words with numbers

Select this check box,  , to configure Outlook's spell check to ignore any words that contain numbers during spell check of a message. Clear this check box,  , to include words with numbers during the spell check of a message. Gray this check box,  , to preserve the user's current Outlook setting.

Ignore original message in replies

Select this check box,  , to configure Outlook's spell check to ignore the text of the original message during spell check of a message. Clear this check box,  , to include the text of the original message during the spell check of a message. Gray this check box,  , to preserve the user's current Outlook setting.

Ignore Internet and file addresses

Select this check box,  , to configure Outlook's spell check to ignore words that are Internet URLs, email addresses and file locations during spell check of a message. Clear this check box,  , to include the text of the original message during the spell check of a message. Gray this check box,  , to preserve the user's current Outlook setting.

The following are examples of some words that would be excluded from a spell check if this option is set:

- http://www.acme.com
- \\acme.wsh\public
- mailto:ceo@acme.com

Flag repeated words

Select this check box,  , to configure Outlook's spell check to ignore words that are repeated in succession during spell check of a message. Clear this check box,  , to include the text of the original message during the spell check of a message. Gray this check box,  , to preserve the user's current Outlook setting.

An example of repeated words that would be excluded from a spell check if this option is set:

- **The The** ACME sales department...
- Lunch was catered **from from** The Corner Deli.

Enforce accented uppercase in French

Select this check box,  , to configure Outlook's spell check to stop on French words that contain uppercase letters that are missing an accent mark during spell check of a message. Clear this check box,  , to include the text of the original message during the spell check of a message. Gray this check box,  , to preserve the user's current Outlook setting.

Suggest from main dictionary only

Select this check box,  , to configure Outlook's spell check to use the main dictionary only during spell check of a message. If this option is selected, words from custom dictionaries will not be in the suggested words list. Clear this check box,  , to include the text of the original message during the spell check of a message. Gray this check box,  , to preserve the user's current Outlook setting.

Microsoft Outlook Data Files

The Microsoft Outlook Data Files tab is used to enable/disable and set file locations for the Personal Address Book, Personal Folders, Offline Address Book and Offline Folders locations.

PAB and personal folder settings

(Personal Address Books are not supported on Outlook 2010 and above)

PAB configuration

Select a configuration option from the list to add the Personal Address Book service to the profile. Select from *Leave alone*, *Create if one does not exist, Create if one does not exist or modify existing*, Only modify existing or *Remove any existing* from the list.

PAB file name

Enter the file name to be used for the Personal Address Book. This file will be stored in the file and location specified by the **PAB file name and PAB folder** entries.

The default for this field, is $UserID.PAB, which uses a dynamic variable to build the file name. To insert a dynamic variable, press the F2 key and select it from this list. The dynamic variable will be inserted into the field at the cursor's current position.

PAB folder

Enter the folder to be used to store the Personal Address Book and Folder Settings. This can be entered in the form of a mapped drive, path or UNC.

Manually type the path or UNC into this field. Alternatively, click **Browse** to navigate to the folder if it is located on a network share. To insert a dynamic variable, press the F2 key and select it from this list. The dynamic variable will be inserted into the field at the cursor's current position. If the specified folder does not exist on the target drive, Desktop Authority will create it.

PST configuration

Select a configuration option from the list to add the Personal Folders service to the profile. Select from *Leave alone*, *Create if one does not exist, Create if one does not exist or modify existing*, Only modify existing or *Remove any existing* from the list.

PST file name

Enter the file name to be used for Personal Folders. This file will be stored in the location specified by the **Folder** entry.

The default for this field, is $UserID.PST, which uses a dynamic variable to build the file name. To insert a dynamic variable, press the F2 key and select it from the list. The dynamic variable will be inserted into the field at the cursor's current position.

PST folder

Enter the folder to be used to store the Personal Folder settings. This can be entered in the form of a mapped drive, path or UNC.

Manually type the path or UNC into this field. Alternatively, click **Browse** to navigate to the folder if it is located on a network share. To insert a dynamic variable, press the F2 key and select it from this list. The dynamic variable will be inserted into the field at the cursor's current position. If the specified folder does not exist on the target drive, Desktop Authority will create it.

New style PST file (if supported by Outlook)

Select this check box,  , to use Outlook 2003 style PST files when creating or modifying PST configuration files.

Clear the check box,  , to use the earlier version of Outlook PST files. Gray the check box,  , to use the user's current Outlook default. This box is only available when creating or modifying the PST configuration.

Offline access settings

OST configuration

Offline Folders (.ost) are used to keep a local copy of the client's Exchange mailbox local to the computer. The items in the .ost file are synchronized with the server when the connection is available. Using this option allows for the client to work productively from local files when the server is unavailable.

Select a configuration option from the list to enable Offline Files. Select from *Leave alone*, *Create if one does not exist, Create if one does not exist or modify existing*, *Only modify existing* or *Remove any existing* from the list. This also activates the use of automatic offline synchronization. The offline content is stored in the file and location specified by **OST File Name** and **OST Folder**.

> ⓘ Note: When Offline Use is enabled in Outlook, and the OST file is removed by Desktop Authority or by any other method, the OST file will be recreated the next time Outlook is started on the client. If Offline use is disabled and the OST file is removed, it will not be recreated the next time Outlook is started.

Offline Use can be enabled or disabled in Outlook by modifying the Offline Folder Files settings for the specific e-mail account.

OST file name

Enter the file name to be used for Offline folders. This file will be stored in the location specified by the **OST Folder** entry.

The default for this field, is $UserID.OST, which uses a dynamic variable to build the file name. To insert a dynamic variable, press the F2 key to select it from the list. The dynamic variable will be inserted into the field at the cursor's current position.

OST folder

Enter the physical path on the client machines where the Offline Folder (OST) files should be stored. Manually type the path or UNC into this field. Alternatively, click **Browse** to navigate to the folder. If the specified folder does not exist, Desktop Authority will create it. To insert a dynamic variable, press the F2 key to select it from the list. The dynamic variable will be inserted into the field at the cursor's current position.

OAB configuration

Along with enabling Offline Folders, the Personal Address Book can also be made available offline (OAB). Select a configuration option from the list to enable the use of the Offline Address Book service for the Mail Profile. Select from *Leave alone*, *Create if one does not exist, Create if one does not exist or modify existing*, Only modify existing or Remove any existing from the list.

The Offline Address Book does not include a file name. The OAB is comprised of a number of files which are automatically created and named by Outlook when first used.

OAB folder

Enter the physical path on the client machines where the Offline Address Book (OAB) should be stored. Manually type the path or UNC into this field. Alternatively, click **Browse** to navigate to the folder. If the specified folder does not exist, Desktop Authority will create it. To insert a dynamic variable, press the F2 key to select it from the list. The dynamic variable will be inserted into the field at the cursor's current position.

Cached Mode

The Microsoft Cached Mode tab is used to configure Outlook's Cached Exchange Mode and Outlook Anywhere settings. Outlook's Cached Exchange Mode allows Outlook to cache its mailbox data to the local drive. This allows access to Outlook data when the Exchange server is unavailable. When the Exchange server is available, Outlook will periodically connect and retrieve its data.

Microsoft Outlook can communicate with Exchange servers over the Internet via a browser based interface. Outlook Anywhere is used to allow remote users to access the Exchange server for email access through the company firewall without the necessity of using a VPN.

Exchange over the internet (Outlook Anywhere)

Connect to Exchange mailbox using HTTP

Select this check box,  , to configure Outlook to connect to the Exchange server using RPC over HTTP protocol. Clear the check box,  , to remove the use of RPC over HTTP communication protocol. Gray the check box,  , to preserve the user's current Outlook setting.

Connection Settings

Use this URL to connect to my proxy server for Exchange

Enter the Exchange server's fully qualified domain name.

Connect using SSL only

Select this check box,  , to enforce that a Secure Sockets Layer protocol is used when data is transmitted over HTTP. Clear the check box,  , to remove the SSL protocol restriction.

Mutually authenticate the session when connecting with SSL

Select this check box,  , to enable mutual authentication. Clear the check box,  , to disable the mutual authentication requirement.

Principal name for proxy server

Enter the proxy server's principal name. This is the server name used to mutually authenticate the session.

On fast networks, connect using HTTP first, then connect using TCP/IP

Select this check box,  , on fast internet connections, such as DSL or Broadband, to connect to the Exchange server via HTTP first. If the connection is unsuccessful, TCP/IP will be used to connect to the Exchange server.

On slow networks, connect using HTTP first, then connect using TCP/IP

Select this check box,  , on slow internment connections, such as dial-up, to connect to the Exchange server via HTTP first. If the connection is unsuccessful, TCP/IP will be used to connect to the Exchange server.

Proxy authentication settings

Use this authentication when connecting to my proxy server for Exchange

Select Basic Authentication or NTLM Authentication from the list. Basic Authentication will require the user to enter a password each time a connection is made to the Exchange server.

Cached Mode

Use Cached Exchange Mode

Select this check box,  , to configure Outlook to use its Cached Exchange Mode. Clear the check box,  , to remove the use of Cached Exchange Mode. Gray the check box,  , to preserve the user's current Outlook setting.

Signature

The Microsoft Outlook Signature tab is used to format a block of text and/or graphics to appear at the end of outgoing messages. Normally, signatures are used to identify the sender of the message, along with their contact information.

Signature

Name

Enter a name for the signature. This will be the name of the signature used in Outlook.

Select signature settings

Mail Profile creation and signature configuration cannot be configured during the same logon event. The Mail Profile must be instantiated before the signature can be configured within the profile. The signature configuration will require an extra logon event.

Select signature for new messages

Select this check box,  , to configure Outlook 2002 and above to use this signature at the bottom of every new message. Clear the check box,  , to remove the use of this signature at the bottom of every new message. Gray the check box,  , to preserve the user's current Outlook 2002 and above setting regarding the use of signatures at the end of every new message.

Select signature for replies and forwards

Select this check box,  , to configure Outlook 2002 and above to use this signature at the bottom of every message that is a reply or forward of a previous message. Clear the check box,  , to remove the use of this signature at the bottom of every message that is a reply or forward of a previous message. Gray the check box,  , to preserve the user's current Outlook 2002 and above setting regarding the use of signatures at the end of every message that is a reply or forward of a previous message.

Signature Code

Enter code into the WYSIWYG editor to be included in Outlook messages as the signature. Click **Confirm** to save the updated signature. Click **Cancel** to ignore the signature changes.

Insert dynamic variable

Click the Insert Dynamic Variable link to insert a variable that is based on the user/computer logging in to the network.

Insert Image

Click the Insert Image button to add an image to the signature file. The image can be added from a URL or uploaded.

Add Hyperlink

Click Add Hyperlink to include a clickable link in the signature file. This can be a URL or a mailto: link. First select the Link Type (URL or E-mail).

Adding a URL link

Select the Link Type **URL** to insert a link to a web site, file, or other resource. Select the Protocol that represents the type of data that will be linked to. In the URL prompt, specify the link, without entering the protocol, as shown below.

Adding an Email link

Select the Link Type **Email** to insert a link that will send an email when clicked. Enter the target Email address, message Subject and message text. When the Email link is clicked, the email will automatically fill in this information in the email window.

Default signature

Click the **Default signature** button to reset the signature to its default value:

$FullName
$adTitle,
$adEmail

$adCompany
$adAddress
$adCity, $adState $adZip
$adPhone Direct
$adFax Fax

www.typecomanynamehere.com

NOTICE: The information contained in this email and any document attached hereto is intended only for the named recipient(s). If you are not the intended recipient, nor the employee or agent responsible for delivering this message in confidence to the intended recipient(s), you are hereby notified that you have received this transmittal in error, and any review, dissemination, distribution or copying of this transmittal or its attachments is strictly prohibited. If you have received this transmittal and/or attachments in error, please notify me immediately by reply e-mail and then delete this message, including any attachments.

Junk E-mail

Select the Junk E-mail tab to configure how Outlook will handle incoming mail.

Options

Leave these settings unconfigured

Select this box to configure junk e-mail protection. Configuring this option will review incoming emails to determine if an email is a junk e-mail. Of course there is no way to exactly determine whether an e-mail is truly junk mail, but Outlook lets you configure an E-mail Filter defining the level of permissiveness from least to most aggressive. Messages determined to be junk e-mail are moved to the Junk E-mail folder.

Choose the level of junk e-mail protection you want

Select *Leave Alone* to use the setting that is currently set in Microsoft Outlook on the computer.

Select *No Automatic Filtering* to use no Junk e-mail filters. Only mail from users specified in the Blocked Senders list is moved to the Junk E-mail folder.

Selecting *Low* will move the most obvious junk e-mail to the Junk E-mail folder.

Selecting *High* will detect most junk e-mail, however some regular e-mail may caught as well. The Junk E-mail folder must be checked often to avoid missing emails that are detected incorrectly as junk.

Select *Safe Lists Only* to accept mail only from people or domains on your Safe Senders List or Safe Recipients List. All other e-mails will be moved automatically to the Junk email folder.

Additional Options

Permanently delete suspected junk e-mail instead of moving it to the junk e-mail folder

Select this option to immediately delete all e-mail determined to be junk e-mail instead of moving to the pre-defined Junk e-mail folder.

Disable links and other functionality in phishing messages (available on Outlook 2007 and above)

If Outlook determines that a message appears to be phishing, the message is delivered to the Inbox, but attachments and links in the message are blocked and the Reply and Reply All functions are disabled.

Warn me about suspicious domain names in e-mail addresses (recommended) (available on Outlook 2007 and above)

This option warns you when the sender's e-mail domain uses certain characters in an attempt to masquerade as a well-known, legitimate business. Leaving this functionality enabled protects you against phishing attacks using spoofed e-mail addresses.

When sending e-mail, postmark the message to help e-mail clients distinguish regular e-mail from junk e-mail (available on Outlook 2007 and above)

Before messages leave your Outbox, Outlook will stamp each message with an e-mail postmark. The postmark incorporates unique characteristics of the message, including the list of recipients and the time when the message was sent. As a result, the postmark is valid only for that e-mail message. It takes some extra computer processing time to construct the postmark.

When the recipient e-mail application receives a postmarked message (must support Outlook E-mail Postmarking), it will recognize the postmark. The postmark indicates to the recipient e-mail application that the message is not likely to be spam and is taken into account when the message is evaluated by the e-mail application's spam filter.

Safe Senders

The Safe Senders list contains e-mail addresses and domain names that are considered to be safe to receive e-mail from. All e-mails received from any e-mail or domain name on this list are never considered to be junk e-mail, regardless of the content of the message. If an e-mail address or domain name is accidentally considered junk e-mail, the sender may be added to the Safe Senders list so it is not mistakenly identified as junk e-mail the next time.

Remove any safe senders from the client that are not defined here

Select this box to clear out the Safe Senders list on the client. This option will remove any sender on the client's Safe Sender list that is not defined on the Safe Sender list within Desktop Authority.

Safe Sender List

Click **Add Sender** to add a new sender email address or domain to the list.

The Sender list has an action associated with each email address or domain name added to the list. The action will allow a sender to be added to the client safe sender list or removed from the client safe sender list. Select the appropriate action from the drop list and enter the sender email address or domain name. Click **Confirm** to save the entry or **Cancel** to quit updating the sender list.

Click the **Remove** button to remove selected entries in the list. Entries are selected by clicking the check box in the lefthand column.

To modify or delete a single entry in the list, click the **Edit** or **Remove** links to the right of the entry in the list.

Click the **Import** button to automatically add senders from a comma delimited text file.

Automatically trust e-mail from contacts in my Contacts list

Select this check box,  , to tell Outlook to treat emails from anyone on the client contact list as an email from a Safe Sender. Clear the check box,  , to tell Outlook to use the normal Safe Sender list rules to determine if an incoming e-mail is from a safe sender or not. Gray the check box,  , to preserve the user's current Outlook setting.

Automatically add e-mail recipients to the safe senders list

Select this check box,  , to tell Outlook to add contacts to the safe senders list when an email is sent to them.

Clear the check box,  , to tell Outlook to not add contacts to the safe senders list when an email is sent to them.

Gray the check box,  , to preserve the user's current Outlook setting.

Safe Recipients

Mailing lists or distribution lists often have a recipient name that is the name of the sender of the list. These list names can be added to the Safe Recipient list so that any message coming from these lists will not be treated as junk, regardless of the content of the message.

Remove any recipients from client are not defined here

Select this box to clear out the Safe Recipients list on the client. This option will remove any recipient on the client's Safe Recipient list that is not defined on the Safe Recipient list within Desktop Authority.

Safe Recipient List

Click **Add Recipient** to add a new email address or domain to the list.

The Recipient list has an action associated with each email address or domain name added to the list. The action will allow a recipient to be added to the client safe recipient list or removed from the client safe recipient list. Select the appropriate action from the drop list and enter the sender email address or domain name. Click **Confirm** to save the entry or **Cancel** to quit updating the sender list.

Click the **Remove** button to remove selected entries in the list. Entries are selected by clicking the check box in the lefthand column.

To modify or delete a single entry in the list, click the **Edit** or **Remove** links to the right of the entry in the list.

Click the **Import** button to automatically add senders from a comma delimited text file.

Blocked Senders

Messages from a specific sender can be blocked by adding their e-mail address or domain name to the Blocked Sender List.

Remove any blocked senders from the client that are not defined here

Select this box to clear out the Blocked Senders list on the client. This option will remove any sender on the client's Blocked Senders list that is not defined on the Blocked Senders list within Desktop Authority.

Blocked Senders List

Click **Add Sender** to add a new email address or domain to the list.

The Blocked Sender list has an action associated with each email address or domain name added to the list. The action will allow a sender to be added to the client blocked senders list or removed from the client blocked sender list. Select the appropriate action from the drop list and enter the sender email address or domain name. Click **Confirm** to save the entry or **Cancel** to quit updating the sender list.

Click the **Remove** button to remove selected entries in the list. Entries are selected by clicking the check box in the lefthand column.

To modify or delete a single entry in the list, click the **Edit** or **Remove** links to the right of the entry in the list.

Click the **Import** button to automatically add senders from a comma delimited text file.

Blocked Top-Level Domain List (available on Outlook 2007 and above)

The Blocked Top-Level Domain List provides the ability to block emails from certain countries by selecting the country code domain extension. As an example, selecting CA (.ca) would block all emails coming from a domain with a .ca domain extension.

Outlook will block emails from any domain that has the selected domain extensions in the list ().

Outlook will allow emails from any domain that has the selected domain extensions in the list ().

Domain extensions marked with the gray check box (), will use the clients current Outlook setting for the domain extension.

Select the **Select All** box to block, allow or disregard the entire list of domain extensions.

Blocked Encoding List (available on Outlook 2007 and above)

The Blocked Encoding List allows you to block email addresses that are formatted using a specific language endcoding.

Outlook will block emails from any domain that has the selected encodings in the list ().

Outlook will allow emails from any domain that has the selected encodings in the list ().

Encodings marked with the gray check box (), will use the clients current Outlook setting for the encoding.

Select the **Select All** box to block, allow or disregard the entire list of encodings.

Other

Reading pane options

Mark items as read when viewed in the reading pane

Select this check box,  , to configure Outlook to automatically mark emails as read when they are viewed in the reading pane. Clear the check box,  , to configure Outlook to not mark emails as read when viewed in the reading pane. Gray the check box,  , to preserve the user's current Outlook setting.

Wait xx seconds before marking item as read

If Outlook is configured to automatically mark emails as read when they are viewed in the reading pane, specify the number of seconds the client has to preview the message for before the email will be marked as read.

Mark item as read when the selection changes

Select this check box,  , to configure Outlook to automatically mark emails as read when the selected message changes. Clear the check box,  , to configure Outlook to not mark emails as read when the selected message changes. Gray the check box,  , to preserve the user's current Outlook setting.

Single key reading using space bar

Select this check box,  , to configure Outlook to use the spacebar to automatically scroll through each message in the reading pane. Clear the check box,  , to configure Outlook to not allow the use of the spacebar to scroll through messages in the reading pane. Gray the check box,  , to preserve the user's current Outlook setting.

Person Names

Display online status next to a person name

Select this check box,  , to configure Outlook to show the online status next to a persons name. Clear the check box,  , to configure Outlook to turn off the display of a person's online status. Gray the check box,  , to preserve the user's current Outlook setting.

Display online status in the To and Cc field only when mouse point rests on a person name

Select this check box,  , to configure Outlook to show the online status when the mouse pointer is over a persons name. Clear the check box,  , to configure Outlook to turn off the display of a person's online status when the mouse pointer is over their name. Gray the check box,  , to preserve the user's current Outlook setting.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

MSI Packages*

The MSI Packages object is used to configure the deployment of applications throughout the enterprise. The MSI Packages object supports the deployment of Windows Installer MSI, MST and MSP packages. Using a Windows

Installer package ensures that applications are installed, updated and uninstalled in a consistent manner throughout the enterprise.

The MSI Packages settings tab provides the interface to select a previously published package and one or more transfer files, and add desired Windows Installer command line options. In addition, you can choose to distribution server that will serve the package to the desktops that validate for this configuration element.

Packages may be installed/uninstalled asynchronously or synchronously and they may be installed without user notification (silent), if desired.

> ⓘ Note: All MSI Packages are installed using the per-machine installation context. This makes the installed application available to all users of the computer and will be placed in the All Users Windows profile.

Settings

MSI packages

Select Package

Click the **Select Package** button to select a previously published MSI package to install/uninstall on client computers.

Action

Select **Install** or **Uninstall** from the Action list to define the action for the MSI Packages element.

Asynchronous

Select this box to run the MSI installation asynchronously. In asynchronous mode, the installation will run at the same time as others. If this check box is cleared, applications will install one after another. Each installation must complete before the next one will begin.

Silent

Select this box to execute the desired action on the selected package without displaying any user interface to the end user. Clear the box to display the full user interface from the MSI to the end user.

Additional package options

Published transform files

Transform files provide configuration settings to be used during the installation of a package. One use of a Transform file is to automatically provide responses to prompts during the installation, for example, to provide an installation path or serial number, so the end user does not have to.

To enable the use of Transform files, there must be at least one published MST. MST files are published within the Software Management global object. Both the Add and Delete buttons will be disabled if there are no published MST files in the software repository.

Click Add Files to use one or more transform files to the Transform Files list. Click Delete to remove selected transform files from the Transform Files list.

Additional command line options

MSIEXEC, the Windows Installer executable program installs packages and products, is called to deploy Windows Installer files. Based on the configurations for the MSI Packages object, specific command line options are passed to MSIEXEC. To use additional command line options, enter the switches in this box. For example, entering /norestart will not allow the computer to restart following the install/uninstall, even if the MSI calls for it. All switches

entered into this box will be passed to MSIEXEC in addition to any command options that are part of the MSI Packages configurations.

Using additional command line options will prevent reporting on the Installer file.

Distribution servers

Select **Automatic selection** to copy the Windows Installer packages to the client from the auto-selected server. Select **Use specific server(s)** to define a specific server to copy the Windows Installer package file from. Separate multiple server names using a semicolon (;).

For configuration information on the Update Service, see What is the Update Service?

If requested packages are not available on the client machine, suspend the startup/shutdown process until they are downloaded

Select this box to copy the necessary file if it does not exist on the client. This request is sent to a server that is a designated download server. Once requested, the Installer file will be copied (if necessary) and duplicated on the distribution server.

Any client that requests the same Installer file from a distribution server following the duplication of the Installer file will receive the file for installation.

Clear this box to continue processing if the Installer file does not exist at the specified location. The client will check for the file during future logons until it can be installed successfully.

User options

User options

Hide all progress indicators

Select this box to hide the package deployment progress indicators. These include the machine assessment dialog as well as package download and install/uninstall dialogs.

Defer packages option

Allow user to defer packages

Select this box to allow the end user to defer the installation of a package to another session. The ability to Defer a Package only applies to synchronous installations only.

Number of times the user can defer package installation before the package is installed automatically

Enter the number of times a user can defer the package installation. Once the package has been deferred the selected number of times, the installation will no longer be allowed to be deferred and the package will automatically be installed.

Amount of time in seconds for the user to respond before the package is installed

Enter the number of seconds the user has to respond to the defer package installation dialog. If there is no response to the dialog and the number of seconds expires, the package will automatically be installed.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Note: This feature is not a standard part of the Desktop Authority Essentials or Standard editions. This is only available to customers who use Desktop Authority Professional.

OneDrive

The OneDrive object provides the ability to centrally configure Microsoft OneDrive for all users. Centrally configuring OneDrive ensures that it is set up and ready to synchronize the user's files.

Once the desired OneDrive settings are configured in the Manager Console, end users will then need to enter their associated OneDrive email address and password into the OneDrive client (build 18.0.0.0 or greater required). However, no password will be required if single sign-on is enabled for the associated OneDrive email account(s). Additionally, OneDrive settings must execute at least once on each client computer after the associated OneDrive account has been configured, in order for the configured settings to be fully propagated.

NOTE: All email accounts being used with OneDrive must already be associated with an instance of OneDrive within the Microsoft Cloud.

IMPORTANT: OneDrive works on any supported operating system having the latest release of the OneDrive client already installed. However, Windows 10 is recommended for the best user experience due to its built-in OneDrive integration.

Settings

OneDrive Email Account

Enter the user's email address. Optionally, press the F2 key to use a Desktop Authority dynamic variable to configure for multiple users.

Example:

$adEmail

Location on your PC

Enter the location of the OneDrive folder on the users computer. Optionally, press the F2 key to use a Desktop Authority dynamic variable. The Default OneDrive folder is C:\Users\[username]\OneDrive.

Auto sync Desktop

Select this check box,  , to automatically sync the user's Desktop with OneDrive. Clear the check box,  , to not sync the user's Desktop with OneDrive. Gray the check box,  , to preserve the user's current OneDrive setting.

Auto sync Pictures

Select this check box,  , to automatically sync the user's Pictures folder with OneDrive. Clear the check box,  , to not sync the user's Pictures folder with OneDrive. Gray the check box,  , to preserve the user's current OneDrive setting.

Auto sync Documents

Select this check box,  , to automatically sync the user's Documents folder with OneDrive. Clear the check box,  , to not sync the user's Documents folder with OneDrive. Gray the check box,  , to preserve the user's current OneDrive setting.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Path

The **Path** object configures client search paths to include local paths, network paths or UNCs. Entries made here will be appended to (placed at the end of) the client's existing path as set in the autoexec.bat in the User's Environment on Windows 2008/7/8.1/10/2008 R2/2012/2016/2019.

Settings

Search path addition

Path

Specify a new search path to be appended to the client's existing search path. The path may be in the form of a path, mapped drive or UNC. Click **Browse** to select an existing path. Optionally, press the F2 key to use a dynamic variable.

Examples:

C:\Batch
S:\Utilities
\\Server1\Tools

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

File/Registry Permissions

The File/Registry Permissions object provides the ability to modify NTFS File and Folder permissions or Registry permissions. Permissions are configurable for 2008, 7, 8.1,10, 2008 R2, 2012, 2012 R2, 2016, and 2019 systems only.

Settings

Action

Type

Select File/Folder or Registry from the Type list. The selected Type is the object that Permissions will be applied to.

Action

Select Append, Overwrite or Revoke from the Action list. This action defines how to apply the Permissions to the selected object.

- Append - Add permissions to list of existing permissions for the object.
- Overwrite - Replace existing permissions with permissions specified in this element for the object.
- Revoke - Remove permissions for the object from the specified user/group.

Path/hive/Key

For the File/Folder Type, enter the Path to the object that Permissions will be applied to. For the Registry Type, enter the Hive and Key that the Permissions will be applied to.

Force use of 32-bit registry locations on 64-bit operating systems

Check this box to force the 32 bit registry location to be used instead of the 64 bit location, when executing on 64 bit operating systems.

Inheritance

Select Do not modify this object's inheritance, Allow this object to inherit from parent, Do not allow this object to inherit from parent and discard inherited permissions, Do not allow this object to inherit from parent and copy inherited permissions from the Inheritance list. The Inheritance selection defines how or if permissions for the object will be inherited.

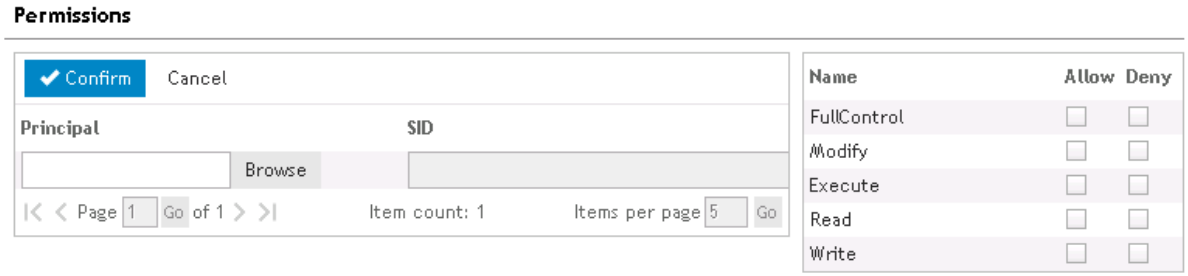
- Do not modify this object's inheritance - This object will not assume (inherit) permissions from any other object.
- Allow this object to inherit from parent - This object is allowed to assume permissions from its parent object.
- Do not allow this object to inherit from parent and discard inherited permissions - This object will not be allowed to assume permissions from its parent object. If the object already has inherited any parent permissions they will be removed.
- Do not allow this object to inherit from parent and copy inherited permissions - This object is not allowed to assume (inherit) permissions from its parent object, nor is it allowed to copy permissions from its parent.

Permissions

The Permissions list designates which users and/or groups will be given permissions to the selected object (File/Folder or Registry)

Press **Add** to define users and/or groups to which permissions will be given to the selected object. Press **Edit** to edit an entry in the Permissions list. Press **Delete** to remove an entry from the Permissions list.

Figure 46: Creating permission sets



Once in Add/Edit mode update the following entries:

Principal

Specify a user or group that will be assigned the designated permissions.

SID

The SID (Security Identifier) will be automatically populated once a Principal is selected.

Permissions

The permission boxes represent the standard permissions that can be allowed or denied for the specified Principal. Select Allow to permit access to the object. Select Deny to refuse access to the object. Selecting either Allow or Deny Full Control will automatically select the Read, Write, Execute and Modify permissions.

Propagation

Select Apply to this object only, Apply to this object and child objects one level deep, Apply to this object and allow all child objects to inherit, or Apply to this object and apply to all child objects from the Propagation list. The

propagation selection defines which components (Parent and/or Child) of the object are affected by the Permission change.

- Apply to this object only - Permissions are applied to the selected Path or registry Hive/Key only. No child objects are affected.
- Apply to this object and child objects one level deep - Permissions are applied to the selected Path or registry Hive/Key object and to any container immediately within this object.
- Apply to this object and allow all child objects to inherit - Permissions are applied to the selected Path or registry Hive/Key object. All child objects have the ability to inherit these permissions however the child objects are not given these permissions automatically.
- Apply to this object and apply to all child objects - Permissions are applied to the selected Path or registry Hive/Key object and to any all containers below this object.

Child object to include

Select Files, Folders, or Files and Folders from the list. The selected child object(s) will be included in the propagation of the applied permissions.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Power Schemes

The Power Schemes object is used to establish power settings in order to save energy and reduce costs and may possibly save some wear and tear on computer equipment by managing how certain devices use power settings.

Power Scheme settings can be configured to run on Windows 7, 8.1 and 10. Power Schemes cannot be configured to run on Terminal Servers, Member Servers or Domain Controllers and 2008, 2008 R2, 2012, 2012 R2, 2016, and 2019 operating systems.

To configure Power settings on Windows 7 machines and above, select the Power Plan Settings tab.

Power Plan Settings

Power plan

Action

Select *Create/Modify or Remove* from the Action list. The Create/Modify action will create a new Power plan if one does not already exist with the specified Power plan name or modify the existing Power plan if one already exists with the specified name. Remove will delete an existing Power plan if one exists with the specified Power plan name.

Power plan name

Select from existing Power plans Desktop Authority Power Plan, Balanced, Power Saver, and High performance pre-defined power plans. Enter a new Power plan name to define new configurations. Enter an existing power plan name to update an existing scheme.

Power plan based on

Select one of the existing power plans as the base of your new custom power plan.

Sleep and display settings

Turn off the display

Enter the amount of idle time that must elapse before Windows turns off the display. This time can be set independently for a computer running on battery and when it is plugged in.

Put the computer to sleep

Enter the amount of idle time that must elapse before Windows puts the computer into sleep mode. This time can be set independently for a computer running on battery and when it is plugged in.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Printers

The **Printers** object configures printer mappings. Printer mappings redirect local printer ports (LPTx) and printer resources to a shared network printer.

Settings

Printer

Printer type

Select either *Network Printer* or *IP Printer* from the Printer Type list.

Shared printer (Network Printer)

Enter the path of the network printer. The path should be specified in the form of **\\server\share**. Optionally, click **Browse** to navigate to the network printer. Press the F2 key to use a dynamic variable.

Specify **/DELETE** in the Shared Printer prompt to remove all persistent printer mappings that a user has created on their workstation that corresponds to the same port number specified for the shared printer configuration.

Printer share for driver installation (IP Printer)

IP Printer: Enter the path of the printer driver that will be installed to the client for the IP Printer.

Auto add/remove(printer)/remove(driver)

Select *Add*, *Remove*, *Remove Printer Driver* or "-" from the list. This allows you to choose from automatically adding or removing a printer or removing a printer driver on a client. This applies to clients with Microsoft Windows 2008//7/8.1/10/2008 R2/2012/2012 R2/2016/2019 operating systems.

Keep in mind that IP Printers are machine specific (local ports). Therefore, everyone connected to the machine will have access to the specified IP Printer.

Set as Default

Select this check box to set any Auto-Added printers as the default printer on the client.

For Desktop Authority to be able to set an auto-added printer as the client's default printer, the printer name must match the share name exactly. For example: On the server, if there is a printer called "HP4000 Accounting"; it must be shared as "HP4000 Accounting". Alternatively, the printer can be renamed to "HP4000AC" and shared as "HP4000AC".

Printer IP

Enter the TCP/IP address defined on the printer.

Advanced printer settings

Protocol (IP Printer)

Select the printer's supported printing protocol.

Port number (IP Printer)

Specify the printer's port number when the RAW protocol is selected. Specify the printers queue name if the LPR protocol is selected.

Printer name (IP Printer)

Specify the printer name.

Port name (IP Printer)

Specify the name that will appear in Windows Printer properties port list.

SNMP name (IP Printer)

Specify the community name used by the printer.

Capture LPT# (Network Printer)

Select a port number from the list or type a new LPT port. Valid LPT port numbers are 1 - 9.

Do not capture LPT1:, or set auto-added printer as default, if client has a local printer defined on LPT1: (Network Printer)

Select this check box for Desktop Authority to ignore any requests to redirect (capture) or set an auto-added printer as the default printer if the client already has a printer defined on LPT1. Clear this check box for Desktop Authority to redirect (capture) or set an auto-added printer as the default, regardless of whether or not the client has a local printer defined on LPT1.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Pre/Post Engine Scripts

Out of the box, Desktop Authority accommodates virtually every installation's requirements simply by filling in the blanks of the objects in the Desktop Authority Manager. While feature-rich and easy-to-use, the Manager may not provide all of the desired functionality out of the box. That's where custom scripting comes in.

Custom Scripting can be used for automated software deployment, locating and/or copying files, special-case drive mappings or to override the Manager settings.

Custom scripting is relatively easy and can be as simple or complex as necessary -- though it does require programming knowledge in KiXtart, PowerShell or VBScript and often requires a working knowledge of the Windows registry. Custom scripts contain scripting code and may launch additional executables, batch files, or scripts of any type using the "shell" or "run" commands.

> Note: Documentation about the KiXtart scripting language can be found at KiXtart.org, the official home of KiXtart.

Pre-engine custom scripts are launched after Desktop Authority's defined configuration settings are read into memory but before these configuration settings are applied. This allows you to "override" variables defined by Desktop Authority with your own custom settings.

Post-engine custom scripts are launched after the Desktop Authority Engine processes the Manager defined configuration settings. This allows you to use drive mappings and other configuration settings after Desktop Authority has applied them to the client.

Custom scripts

A custom script is an ASCII text file written using a scripting language. Desktop Authority supports KiXtart (.kix), PowerShell (.ps1) and VBScript (.vbs). A script may be created using Notepad or any other text editor. The script file may be created within or outside of the Manager.

To create a script from within the manager

1. Decide at which point the script should run, **Pre** or **Post** Engine. Create the element by clicking **Add** inside the element list on the Pre/Post-Engine Scripts object.
2. Specify a script file name on the Settings tab. The file name should end with a .kix, .ps1 or .vbs extension depending on the type of script being created. Once the extension is recognized by the Manager, the **Edit file** button will be enabled.
3. Click the **Edit file** button and the new script file will be created and opened within the custom script editor.

   > Note: If creating a .kix script, be sure to leave all of the default contents of the script file intact and enter your script code between the comment lines.

4. Click the **Save** button to save your changes or the **Cancel** button to abort your changes.

To modify an existing script from within the Manager

1. Select either the **Pre** or **Post** Engine Scripts object and then the element to be modified. Click the **Edit** button.
2. Once the element is open, click the **Edit file** button to open the custom script file in the editor. You may now make any necessary changes to the script.

   > Note: Keep in mind that the script file may also be edited in any other appropriate editor you see fit outside of the Desktop Authority Manager.

3. Click the **Save** button to save the changes or the **Cancel** button to abort the changes.

Using an existing script created outside of the manager

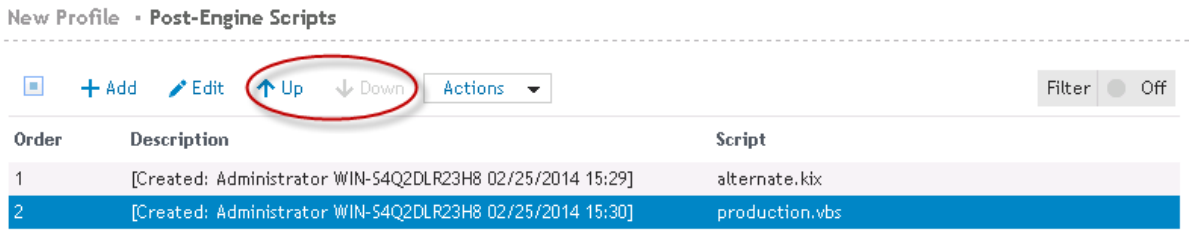
> Note: To create a script outside of the Manager, simply load any appropriate text editor and begin typing. Once the script is complete (and tested) it may be added to the Pre and/or Post-Engine object within the Manager.

1. Create or modify the Pre/Post-Engine script element.
2. Once the script element is open, click the **Browse** button to locate the file with the resource browser.
3. Click Open to select the file once it is located.
4. Click the **Save** button to save the changes or the **Cancel** button to abort the changes.

Custom Script execution

As Desktop Authority processes the custom script elements defined by the Pre and/or Post Engine Script list, Validation Logic is applied to each script, beginning with the element at the top of the list. Prioritize the list entries by selecting one or more entries and clicking the **Up** or **Down** buttons to reorganize the list.

Figure 47: Set the order of the script entries for execution



Settings

Pre/Post-engine scripts settings

File name

Enter the name of the custom script file. The script file name must have an extension of .kix, .ps1 or .vbs. Click **Browse** to locate and select an existing script file from a network share. If the file does not already exist, Desktop Authority allows the creation of scripts directly from this dialog box. Once a file name with a recognizable extension (.kix, .ps1, .vbs) is entered into the file name field the file may be edited. Click the **Edit file** button to edit it. The file will be created and/opened for edit in the system editor. If a new script is being created, some comments are automatically added to the file by Desktop Authority.

Dynamic Variables

Dynamic variables, environment variables or macros may be used as part of the custom script file name. These variables are translated during the client logon process.

Example:

File name: $UserId.kix

For the user Mary Jones, this will translate into mjones.kix when she logs on.

To insert a dynamic variable, press the **F2** key and select the variable from the popup list. The dynamic variable will be inserted into the field at the cursor's current position.

Dynamic variables may also be used as part of the content of a custom script. In order to use the Desktop Authority Dynamic variables within a PowerShell script, use $DA.davariablename. For example, if you wanted to enumerate the user's UserID, the dynamic variable is $UserID. You would format the variable as *$DA.UserID* in the PowerShell script.

In order to use dynamic variables in a VBScript use DA_davariablename. For example, if you wanted to enumerate the user's fullname, the dynamic variable is $FullName. You would format the variable as *DA_FullName* in the VBScript.

Administrative rights

Powershell and VBScripts may be run with Administrative rights by using the /admin switch following the file name.

> Important: The administrative rights switch (/admin) cannot be used with a KiXtart (.kix) script since Desktop Authority already provides API functions that are executed with admin rights. Standard KiXtart functions do not use administrative rights.

Example:

scriptname.ps1 /admin

scriptname.vbs /admin

\\servername\sharename\scriptname.ps1 /admin

\\servername\sharename\scriptname.vbs /admin

> IMPORTANT: When using the administrative rights switch (/admin) to execute a PowerShell or VBScript, the any Desktop Authority dynamic variables used will be evaluated based on the context of the user logging in. However, if PowerShell or VBScript variables are used within the script, they will be evaluated based on the context of the Desktop Authority Client Service user account.

There are not many rules about editing custom scripts, however, remember that each KiXtart script must end with a RETURN statement so that control is returned to the Desktop Authority Engine when the script is finished processing. This is not the case for Powershell and VBscripts.

Desktop Authority provides no error control over custom scripting. A syntax error in a custom script may cause Desktop Authority to unexpectedly terminate.

> Note: Quest does not offer support for writing, modifying or troubleshooting custom scripts.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Registry

The **Registry** object provides a single point of control over changing values in the registry of the user's computer. This object takes advantage of the DA Administrative Service, which allows Desktop Authority to modify any Windows 2008/7/8.1/10/2008 R2/2012/2012 R2/2016/2019 registry key/value, even if the user logging on does not have the necessary permissions to modify that particular key/value under their own security context.

NOTE: The Registry object is extremely versatile and, if used improperly, can cause computers not to function properly. The Registry object is designed for use by experienced administrators only. Always use caution when manipulating the registry on any computer, and extreme caution when using a product such as Desktop Authority to make a network-wide change to a group of computers at once. It is highly recommended to first test any registry modification on a specific user or computer (using Validation Logic) prior to rolling the change out to an entire group, subnet or domain.

Settings

Registry action list

Instead of configuring a single registry setting per profile element, the Registry profile object lets you configure multiple registry actions within a single Registry profile element. Click Add from the Registry profile object to create a Registry profile element. This Registry implementation will save you time when implementing multiple registry settings. Group all registry settings together that will use the same Timing and Validation Logic settings. If you prefer, you can stick to the old way of doing things by adding one element to the Registry action list and create several Registry profile elements.

Add

Click **Add** to add a new registry setting to the Registry action list.

Import

Click **Import** to import existing registry (.reg) files.
Importing Registry Files

There are two ways to import an existing registry file:

- Import registry entries into a single Registry profile element
- Import registry entries into multiple Registry profile elements

Figure 48: Import registry entries into a single Registry profile element

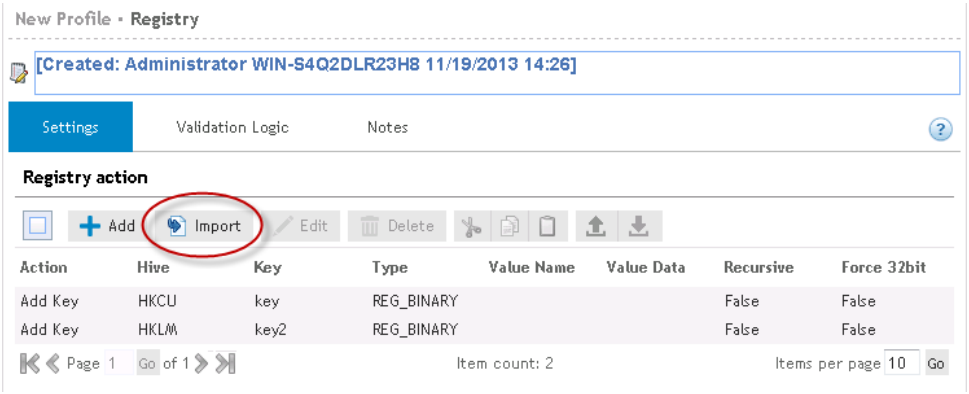
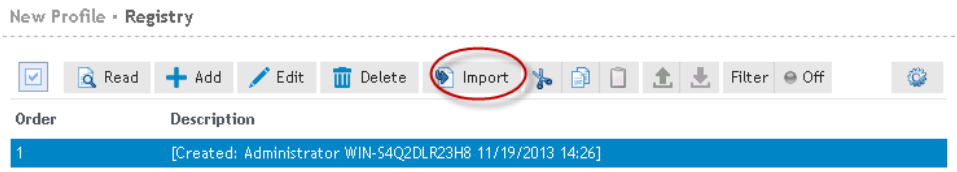


Figure 49: Import registry entries into multiple Registry profile elements



Clicking the **Import** button from the Registry profile object will import all entries within the selected .reg file as multiple elements in the Registry profile object. **This will result in *multiple* Registry profile elements.**

Edit

Select **Edit** to modify the currently selected registry action.

Delete

Select **Delete** to remove the currently selected registry action.

Cut/Copy/Paste

Registry actions can be managed by using the standard Windows Cut/Copy/Paste actions to maneuver them into child profiles or parent profiles. Drag and Drop actions may also be used for this purpose.

Move up/Move down

Registry actions will be evaluated on a client in the order they appear in the Registry action list, from the first Registry element to the last. The order of the Registry actions can be modified by using the Move Up and Move Down buttons. To move a registry action, you must first select it, by clicking on it. Once it is selected (it will be highlighted), press the Move Up or Move Down button based on which way you want to move the setting.

The order in which the Registry actions are displayed in the list is the order they will get processed in. For example, if there are 2 registry elements and they each have a registry action list, all actions for the first registry element will be processed and then all actions for the second registry actions list will be processed.

Configuring a registry action

Once you have configured the registry action, click **Confirm** to save the settings or **Cancel** to abort the setting changes.

Action

Select an action from the list to define how the registry setting is to be updated. Registry keys can be created and removed. Available actions are:

- **Write Value**
  Store the specified data to the specific Hive\Key\Value. If the key does not already exist, it will be created.
- **Delete Value**
  Remove the specified value from the specific hive\key.
- **Add Key**
  Create a key in the specified hive.

- **Delete Key**
  When the *Delete Key* is selected you have the option of deleting the key regardless of whether subkeys exist or not using the **Delete Key even if subkeys exist** option. Selection this option to delete the key and any associated subkeys. If this option is not selected, the key will not be deleted if any subkeys exist.

  This option cannot be performed on the *Software\Microsoft* or *Software\Classes* keys.

Hive

Select the hive on which to perform the action from the list. The following hives can be selected:

- **HKEY_CURRENT_USER**
  Contains preferences for the user currently logged in.
- **HKEY_LOCAL_MACHINE**
  Contains computer specific information about the type of hardware, software, and other preferences on a given PC.
- **HKEY_CLASSES_ROOT**
  Contains all file associations, OLE information and shortcut data.
- **HKEY_USERS/.DEFAULT**
  Contains default profile preferences.
- **HKEY_CURRENT_CONFIG**
  Represents the currently used computer hardware profile.

Key

Enter the specific key to be added or updated in the registry. Keys are subcomponents of the registry hives. Dynamic variables are available for use in defining the key.

Type

Select the value type to be stored in the registry key.

Valid types are:

- REG_BINARY
  The entry field for binary data is similar to the entry field in RegEdit. Use the actual hex values as entry.
- REG_DWORD
- REG_DWORD_BIG_ENDIAN
- REG_DWORD_LITTLE_ENDIAN
- REG_EXPAND_SZ
- REG_FULL_RESOURCE_DESCRIPTOR
- REG_LINK
- REG_MULTI_SZ
  Enter each piece of data or expression on a new line.
- REG_NONE
- REG_QWORD
  Select the type of data to be entered, Decimal or Hex.

- REG_RESOURCE_LIST
- REG_SZ

The Type list is not applicable when the Action field is set to either Add Key or Delete Key.

Value

Enter the name of the value for the registry key that will be written. Value is not applicable when the Action field is set to either *Add Key* or *Delete Key*.

A value is not required when the Action field is set to *Write Value*. If no value is specified, the data will be written to the key's default value.

Data/expression

Type the data you would like stored in the specified value. This field may contain static text, Desktop Authority Dynamic Variables, KiXtart macros or any combination of the three. Press the F2 key to select a dynamic variable from the list.

If you want to create a new value with no data, or to erase an existing registry value's data, leave this field blank. The value will be created with no data.

Force use of 32 bit registry locations of 64 bit operating systems

Check this box to force the 32 bit registry location to be used instead of the 64 bit location when executing on 64 bit operating systems.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Remote Management*

The **Remote Management** object provides the ability to install, configure or remove the Remote Management component to/from host computers.

Settings

Remote management options

Select to *Install* or *Remove* the Desktop Authority host software on client workstations.

Port

Specify a listening port that Desktop Authority will use to communicate with client workstations. By default the Desktop Authority host software is configured to use port 2000.

Display tray icon

Select this check box to display a system tray icon on the client workstation. This icon indicates that the Remote Management host software is installed on the client. Clicking on this icon provides a wealth of extra information, including a log of recent events and detailed performance data graphs.

Grant full control to administrators

Select this check box to allow all administrators access to start a remote management session. Clear this check box to disable administrators default access to remotely manage workstations. Explicit permissions must be granted to users who will have access to start a remote management session

Ask permission from the interactive user

Select this check box to enable the **Desktop Authority** system tray icon and request permission from the user at the workstation when a remote management session is to be started. Enabling the system tray icon also enables the ability to use the Chat function. If this box is cleared there will be no indication at a workstation when a remote control session is started. The Chat function will also be disabled.

Open port in Windows Firewall to allow remote management

Select this check box to open the port that allows a remote management connection.

Enable Remote Registry Service

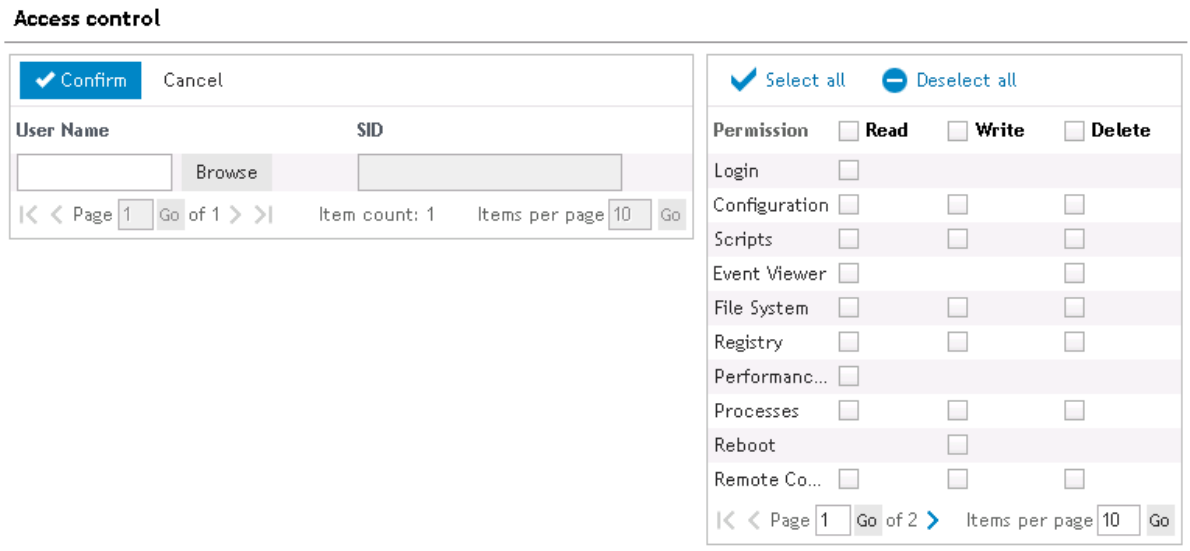
Select this box,  , to set the Remote Registry service startup type to automatic and start the service. Clear this box,  , to set the Remote Registry service startup type to manual and stop the service. Gray the check box,  , to leave the startup type and service status as is.

NOTE: Enabling the Remote Registry Service on client machines is no longer required for Remote Management functionality

Access control

The Access Control List allows permissions to be controlled for Remote Management sessions.

Figure 50: Configure Access Control List permissions



Login

Anyone with any sort of access to Desktop Authority is implicitly granted Login access. This allows for looking at the Info page, reading the Help file, chatting with the user in front of the computer, and logging out.

Configuration

Users with access to the Configuration module have access to all Basic permissions plus Computer Settings > Automatic Priorities, Server Functions > FTP capabilities, Performance Monitoring > Telnet/SSH Connections, Security > IP configurations and Preferences. Keep this in mind this grants users access to modifying Desktop Authority permissions.

Scripts

Users can execute, create, change or delete scripts.

Event Viewer

Allows the use of the Event Viewer module under Computer Management.

File System

Allows the use of the File Transfer module, Computer Management > File Manager and Security > **Desktop Authority** Logs.

Registry

Allows for editing and compacting of the registry under Computer Management.

Performance Data

Ability to view performance and system information data under Performance Monitoring. Processes Allows access to the Process List, and adds the ability to terminate processes and/or change their priorities. These items can be found under Computer Management.

Processes

Ability to view Processes data under Computer Management.

Reboot

Allows rebooting the computer and restarting the Desktop Authority service. This section can be found under Computer Management.

Remote Control

Allows use of both the screenshot-based and the Java-based Remote Control module.

User/Group Accounts

Allows the use of the User Manager module found under the Computer Management section.

System Configuration

Allows the user access to Computer Settings.

SSH Shell

Allows access to a command prompt on the host computer via the SSH protocol.

SSH Port Forward

Grants the user rights to use SSH Port Forwarding.

SSH Privileged Port Forward

Grants the user rights to use SSH Privileged Port Forwarding.

SCP

Grants the user rights to use SCP (Secure file Copy Protocol).

SFTP

Allows the user access to the file system of the host computer via the SFTP (Secure File Transfer Protocol).

Telnet (DA Client)

Allows the user to use the secured telnet client found in the browser under the Command Prompt item.

Telnet

Allows access to the machine via Telnet - either using the built-in telnet client or any standalone terminal emulator.

Click **Select All** to mark all permissions. Click **Deselect All** to clear all permissions.

Advanced

The Remote Management Advanced tab provides several advanced settings for Remote Management. The Advanced settings are comprised of several options pertaining to General, Interactive user's permission, Security, Audible notification, Logging, and IP Filtering settings.

General

Use mirror display driver

Desktop Authority provides a mirror display driver on the W2K platforms. This display driver provides a faster and less CPU-intensive remote control session. Select this check box to use the mirror display driver. Clear this check box to disable the use of the mirror driver.

Automatically disable wallpaper

Select this check box to disable the wallpaper (or background desktop image) on the host computer when a remote control session is started. Clear this check box to view the image during the remote session.

Clipboard transfer size

The Remote Management host software provides the ability to transfer clipboards between host and client machines, allowing the ability to copy from one machine and paste on the other.

Specify the maximum number of kilobytes (KB) that can be transferred between machines. The default size is 1024 KB. Transferring significantly larger amounts may cause slowdowns. The maximum limit is 8 MB in both directions. If the clipboard is larger than the maximum limit nothing will be transferred.

Idle time allowed

Specify the number of minutes a remote host may be inactive for. If a period of inactivity is determined, the client will automatically be disconnected from the remote session.

Screen shot updates per second

Specify the number of times the display is to be updated each second.

Enable remote printing

Select this check box to enable the ability to print remotely. Clear this check box to disable the ability to print remotely.

Interactive user's permission

Warning text

Enter the confirmation text to be presented to the host when a remote control session is about to begin. The string '%%user%%' will be substituted by the name of the user who is attempting the remote control operation.

Duration of warning in seconds

Specify the amount of time before the notification message to the host times out.

If warning times out, allow remote control anyway

Select this check box to allow remote control access to a host when the local user does not answer the query for access. Clear this check box to cancel the query for access to the host when the local user does not answer.

Display notification during remote control

When a remote session is in progress, a small window in the top right corner of the remote screen is displayed stating who is currently remotely connected to the machine. Select this check box to have this remote management

notification displayed during the remote session. Clear the check box to display no connection notification dialog during the remote session.

Do not ask permission if admin has full control

Select this check box to allow immediate remote control access without requesting permission from the host. This is only possible if the user requesting remote access has Full control permissions. Clear this check box to disable this ability.

Security

Disable host keyboard and mouse

Select this check box to disable the host's keyboard and mouse during the remote session. This will prevent the host user from using the keyboard or mouse while the remote control session is in progress. Clear this check box to enable the host's keyboard and mouse during the remote control session.

Lock console when connection broken

Select this check box to lock the console in order to protect open files, if, due to a network error, the Java remote control client loses its connection to the server. Clear this check box to leave console as is when the connection is broken.

Lock console when connection times out

Select this check box to lock the console in order to protect open files, if the connection times out. Clear this check box to leave client as is when the connection times out.

Always lock console when remote control disconnects

Select this check box to lock the console when the remote session ends. Clear this check box to leave client as is when the remote session ends.

Blank host screen

Select this check box to blank the display on the host computer during a remote control session. This is useful for preventing user interaction while remote work is in process.

Audible notification

Beep whenever a session begins or ends

Select this check box to have an audible beep on the host computer when a remote control session is initiated or ended.

Beep continuously during remote control

Select this check box to have a periodic audible beep on the host computer during the remote control session.

Beep interval in seconds

Specify an interval for the periodic beep during the remote control session. The beep interval is specified in seconds.

Logging

Keep logs for

Specify the number of days in which log files will be kept for. Set to zero to disallow the system from deleting any log files. Log files can be deleted manually from the specified log file location.

Log file location

Specify the folder where log files will be stored. Leaving the check box empty will cause the log files to be stored in the x:\Program Files\Desktop Authority folder on the host machine.

IP filtering

The Remote Management IP address filtering feature allows the configuration of exactly which computers are allowed to access the Remote Management system. Click Add to add a new IP Filter to the list. Click Modify to edit an existing IP Filter. Click Delete to remove an existing IP Filter from the list.

Allow/Deny

Select Allow or Deny from the type list. Allow specifies that access will be granted to the defined IP address. Deny will refuse access to the IP address specified.

IP/Subnet

Enter either a single IP address with no subnet mask, an IP address with a subnet mask, essentially granting or denying access for a whole network, or an IP address with wildcards and no subnet mask. Valid wildcards are an asterisk (*) that matches any number of characters, or a question mark (?), that matches a single character only.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

*Note: This feature is not a standard part of Desktop Authority Essentials. To obtain this feature, Desktop Authority Essentials must be upgraded to the Standard edition of Desktop Authority.

Security Policies

The **Security Policies** object allows user security settings to be centrally configured. Security policies can be set for individual users or computers.

User policies are registry entries stored to the [HKey_Current_User] registry hive. This registry hive is stored in the user's profile. On Windows 2008/7/8.1/10/2008 R2/2012/2012 R2/2016/2019 operating systems, each user has an individual user profile.

Computer-specific policies are registry entries stored to the [HKey_Local_Machine] registry hive. This type of policy will affect every person that uses the computer.

When a Policy is enabled, it remains in effect until you specifically disable it or select the Clear all existing policies first option. Once you configure the security policy to be disabled using either of these two methods, the user must log on one more time so that Desktop Authority may apply the "disabled" setting to the computer.

Security Policies are registry settings. Deleting a Policy entry from the list will leave the policy in effect whether it is enabled or disabled. To clear the policy setting, you must reset the policy in the list or check the Clear all existing policies first box.

Settings

Policy action

Enable/disable

Select Enable or Disable from the list to enable or disable a security policy.

Category

Select a specific policy area from the Category list for a security policy to be set. The available categories are: (All Policies), Computer, Explorer, Internet Explorer, Network, System and WinOldApp. (All Policies) will display policies for all categories. WinOldApp provides policy settings for MS-DOS apps.

Selecting a policy category will filter the policy selection list below the category.

Policy

Select a policy from the list. This list is filtered based on the policy category chosen. To see all policies, select the (All Policies) category.

User Account Control (UAC)

Select the User Account Control (UAC) tab for Security Policy settings pertaining to UAC on Windows 2008, Windows 7, Windows 8.1, Windows 10, Windows 2008 R2, Windows 2012, Windows 2012 R2, Windows 2016, and Windows 2019.

User Account Control (UAC) on Windows 7 and later

This setting determines the behavior of all UAC security policies on the target system. Select **Enable** from the drop list to use UAC policies throughout the target system. Select **Disable** from the drop list to disallow the use of UAC policies. Select **Leave Alone** to preserve the system's current UAC settings. By default, UAC policies are enabled on Windows 7 and later operating systems.

UAC changes on Windows Server 2008 machines require a reboot before the change will take effect.

Windows Security Center will notify the user that the overall security of the system has been compromised if UAC security policies are disabled.

User Account Control Polices

All individual UAC security policy settings are disabled for individualized configuration unless the User Account Control (UAC) on Windows 2008 server selection is enabled.

Admin approval mode for the built-in administrator account

By default the Built-in Administrator account will run all applications with full administrative privileges. Enable this option to prompt the Built-in Administrator with the consent dialog. From this dialog the administrator can then choose to permit or deny the action. **Disable** this option to allow the Built-in Administrator to run all applications with full administrative privileges. Select the Leave Alone option to preserve the system's current setting.

Behavior of the elevation prompt for administrators in admin approval mode

The elevation prompt is a dialog that is used to prompt the administrator for permission to continue, or to prompt the user for credentials in order for the requested elevation of permissions to continue. This option allows the behavior of the elevation prompt to be set for administrators. Select a setting, Leave Alone, Elevate without prompting, Prompt for credentials and Prompt for consent, from the drop list.

Select the Leave Alone option to preserve the system's current setting, which by default is Prompt for Consent.

The Elevate without prompting option will allow an operation that requires permission elevation to continue with prompting for consent or credentials.

The Prompt for credentials option prompts the administrator with the elevation prompt dialog. The user is required to enter their user name and password. The request will continue with the applicable privileges. When UAC is enabled, this is the default setting.

The Prompt for consent option forces the elevation prompt dialog to pop up when there is an attempt to perform an administrative task. This dialog consists of a Permit and Deny selection. Permit will allow the operation continues with the user's highest available privilege. The operation cannot continue if Deny is selected. This is the default selection when UAC is enabled.

The **Prompt for consent from non-windows binaries (Win 7)** option forces the elevation prompt dialog to pop up when there is an attempt to perform an operation for a non-Microsoft application. The user is prompted to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege. The operation cannot continue if Deny is selected.

Behavior of the elevation prompt for standard users

The elevation prompt is a dialog that is used to prompt the administrator for permission to continue, or to prompt the user for credentials in order for the requested elevation of permissions to continue. This option allows the behavior of the elevation prompt to be set for standard users. Select a setting, Leave Alone, Elevate without prompting, Prompt for credentials and Prompt for consent, from the drop list.

The Prompt for credentials option prompts the user with the elevation prompt dialog. The user is required to enter their user name and password. The request will continue with the applicable privileges.

The **Automatically deny elevation requests** option will return an access denied error message to the user when an operation is attempted that requires elevation of privileges.

Select the Leave Alone option to preserve the system's current setting.

Detect application installations and prompt for elevation

This setting determines the behavior of application installation. Select Enable from the drop list to pop up the elevation prompt dialog based on the configured elevation prompt behavior. Select Disable from the drop list to not trigger installer detection. Select Leave Alone to preserve the system's current settings.

Only elevate executables that are signed and validated

This setting will enforce PKI signature checks on any interactive application that requests elevation of privilege. Enterprise administrators can control the admin application allowed list through the population of certificates in the local computers Trusted Publisher Store. Select Enable to enforce the PKI certificate validation of an application

before it is allowed to run. Select Disable to not enforce PKI certificate chain validation before an application is allowed to run. Select Leave Alone to preserve the system's current settings.

Only elevate UIAccess applications that are installed in secure locations

This setting will enforce the requirement that applications that request execution with a User Interface Accessibility integrity level must reside in a secure location on the file system. Select Enable to launch the application only if it resides in a secure location. Select Disable to launch the application regardless of whether it resides in a secure location or not. Select **Leave Alone** to preserve the system's current settings.

Switch to the secure desktop when prompting for elevation

When prompting for elevation permissions, the system can process the request on the interactive user's desktop or on the Secure Desktop. Select Enable to process elevation requests on the secure desktop. Select Disable to process elevation requests on the interactive user's desktop. Select Leave Alone to preserve the system's current settings.

Allow UIAccess applications to prompt for elevation without using the secure desktop

This setting allows User Interface Accessibility programs to not automatically disable the secure desktop for elevation prompts. Instead, the prompts will appear on the interactive user's desktop instead of the secure desktop. By default, this setting is Disabled in Windows.

Virtualize file and registry write failures to per-user locations

This setting enables the redirection of legacy application write failures to defined locations in the registry and file system. Select Enable to facilitate the runtime redirection of application write failures to a specific user location. Select Disable to allow applications that write data to protected locations to fail as they did in prior versions of Windows. Select Leave Alone to preserve the system's current settings. This is the default setting.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Service Pack Deployment

The **Service Pack Deployment** object allows you to deploy service packs for all Windows 7 clients. A few items to note regarding service pack deployment:

- The User Management Service Pack Deployment will only install service packs to Windows 7 clients if connected over a LAN connection.
- The User Management Service Pack Deployment will never downgrade the currently installed service pack on a computer. Desktop Authority will only install the requested service pack if the client has an older or no service pack installed.
- The User Management Service Pack Deployment will not attempt to install the requested service pack if the client does not have enough available disk space on the drive that hosts the %TEMP% folder. The engine determines the amount of available disk space before the service pack is installed. By default, 1.4G (1400mb) of disk space must be available to install any service pack. This default can be overridden by defining a value in the global or profile definition file.

The variable $ServicePackFreeSpaceNeededInMB is used to override the available disk space amount. Select Global Options > Definitions or select the Definitions tab on the profile's settings.

Example:

$ServicePackFreeSpaceNeededInMB="1000"

- The User Management Service Pack Deployment will run all service packs in unattended mode, will force the computer to close other programs when it shuts down, and will not back up files for uninstall purposes.
- The User Management Service Pack Deployment will not install service packs to any Windows Embedded operating system.
- The User Management Service Pack Deployment will not install any service packs to a server.

Desktop Authority can bypass the automatic installation of service packs on specific computers. If you have specific computers that you would never like Desktop Authority to install a service pack on (such as a development station), create a file called *SLNOCSD* in the root directory of the System Drive. This allows you to generally apply service packs based on Validation Logic, while providing for special-case exemptions based on individual systems.

Settings

Service packs settings

Operating system version

Select a client Operating System version from the list.

Operating system language

Select a language from the list. This language should specify the dialect of the operating system installed on the client as well as the service pack. If the languages do not match, the service pack will not be installed.

Update to

From the list, select the service pack to be deployed. Service Packs displayed in the list are filtered based on the OS Version selected.

Location of SPInstall.exe

Enter the complete path and filename where the installation executable exists or click **Browse** to locate the executable's path. The installation executable may be called either spinstall.exe or update.exe based on the operating system being installed. The service pack install file is called spinstall.exe in Windows 2008.

Example:

\\server1\installs\W2KSP1\Update.exe

The executable file downloaded from Microsoft is an archive that must be extracted at a command line by using the *-x* switch. This will extract the service pack into multiple folders among which you will find *update.exe*.

The following parameters are used when installing service packs from the User Management Service Pack object:

- Windows 7 = ' /quiet /nodialog /forcerestart'

  For information about the Microsoft Service Pack command line parameters, refer to Microsoft's Command-line switches for Windows software update packages knowledge base article.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element. Service Packs may only be applied to computers classified as a Desktop or Portable. Operating System and Connection type are disabled.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Shortcuts

The Shortcuts object provides the ability to centrally define shortcuts to be used on the client's machine. A shortcut is a pointer to an application or folder. Once the shortcut is created, the user will never have to remember the details to access the referenced program or folder again. They simply run the shortcut.

Settings

Shortcut settings

Name

Enter a name for the shortcut. This name will appear below the icon for the shortcut. This field is required.

Location

Specify the folder where the shortcut will be created or removed from. Type a location or select one from the list. Available options to choose from are: All Users Desktop, All Users Programs Group, All Users Start Menu, All Users Startup Group, User Desktop, User Favorites (IE bookmarks), User Programs Group, User Quick Launch Bar, User Start Menu, User Startup Group, User Start Menu (Pin), User Taskbar (Pin).

A location may also be specified by a dynamic variable, environment variable or macro which is translated by Desktop Authority during the client logon process.

Example:

ShellProg\Shared Documents\Employee Manual

When Desktop Authority executes on the client, $ShellProg will be populated with the location of the user's Start Menu Programs folder, for example: C:\Windows\Start Menu\Programs or D:\WinNT\Profiles\bclinton\Start Menu\Programs.

If the specified folder for the shortcut does not exist when Desktop Authority attempts to create the shortcut, the folder will automatically be created during the client logon process.

ⓘ Note: User Start Menu (Pin) and Taskbar (Pin) locations are not supported in Windows 8.1.

NOTE: When selecting User Start Menu (Pin) or User Taskbar (Pin) with a non-English language workstation operating system, you must define a variable that defines the non-English verbiage to substitute in place of the English "Pin To..." verbiage. The value of these variables should match the "Pin to Taskbar" or "Pin to Start Menu" text on the popup menu of a program shortcut. The following variables can be defined as User Management Global Variables or as a Profile Definition Variable.:

- $PinToTaskbarString
- $UnPinFromTaskbarString
- $PinToStartMenuString
- $UnPinFromStartMenuString

The Value for each variable should match the operating system verbiage to the popup menu when a right-click is done on a Shortcut.

See the Global Definition Variables list for other variable that can be used to customize other configurations in Desktop Authority.

Action

Select *Create Shortcut* or *Remove Shortcut* from the Action list.

Overwrite

Select this check box to overwrite an existing shortcut if it exists in the same location with the same name. Clearing the check box will not overwrite the shortcut if it exists.

Target

Some programs need to reference other files in a specific folder. In order for the shortcut to find these files, the folder must be specified. Type the folder name or click the **Browse** button. In most cases this field will contain the path used in the Target field. This field is required.

Target arguments

Specify any optional command line parameters for the selected target program.

If you need to pass a reserved character (@, $, or %) to a program, you must double the reserved character within the Desktop Authority Manager. For example, if the program requires /@u-username as a command line argument, type /@@u-$UserID in the arguments field.

Start in

Some programs need to reference other files in a specific folder. In order for the shortcut to find these files, the folder must be specified. Type the folder name or click the **Browse** button. In most cases this field will contain the path

used in the Target field. This field is required.

Comment

Enter a text description for the shortcut. This is displayed on the shortcut properties dialog.

Icon file

Specify the icon file to display for the shortcut. An icon, icon library or program file may be specified. If there is more than one icon in the file specified, enter the icon number in the **Icon index** entry. An icon file may be selected by clicking the **Browse** button.

Key

Specify the keyboard combination that will be used to start or switch to the target application. Shortcut keys are always a combination of the CTRL key plus the ALT key and then one other key to add to the sequence.

For example, to specify a shortcut key of CTRL + ALT+ T, enter the letter T in the field. Set the field to *None* to disable the shortcut key by pressing the BACKSPACE key.

The ESC, Enter, TAB, Spacebar, Print Screen or Backspace keys are not allowed as shortcut keys. If this shortcut key conflicts with a keyboard shortcut in another Windows application, the keyboard shortcut in the other Windows application will not work.

Run Window

Select a window option from the list. This defines the style of the window the application will initially execute in. Select from *Normal*, *Minimized*, or *Maximized*.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Example

One way to make use of shortcuts is to create a shortcut in your user's Internet Explorer Favorites. This example demonstrates how to create the Favorites shortcut.

Time Synchronization

Keeping client workstation times synchronized is simple to configure using the Time Synchronization dialog box. This synchronizes each workstation's clock with a specified server. When the client logs on the network, the time is automatically adjusted to match the server's time.

Settings

Server

Time server

Enter the name of the Time Server which the client will by synchronized with. Type the server name or click **Browse** to locate and select a server.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

USB/Port Security*

The myriad of portable storage mediums today make it essential for corporations to prohibit or monitor the use of certain devices on the company network. These devices can be very harmful to a corporation. Confidential data can easily be copied to any portable device, viruses can be introduced to the network and spread corporate wide and illegal software can be copied to the company network.

NOTE: To use this feature, you must have Microsoft Visual C++ 2005 redistributable installed on your system. For more information on how to obtain and install this package, see your Microsoft documentation.

Since most portable devices are small in size it is simple for any employee to use these devices regardless of a written or verbal company policy. The users' ability to use these devices and/or transfer data to and from these devices must be restricted. The USB/Port Security object will do just this.

Users and/or groups of users can be restricted from using certain types of removable storage devices. Desktop Authority's USB/Port Security object will protect the company network against unauthorized usage of devices such as MP3 players, PDAs, WiFi and more. The list of devices includes USB, Firewire (1394), Serial, Parallel, Floppy disks, IR, Bluetooth, IDE, SCSI, PCMCIA, IoMega, Blackberry, Pocket PC devices, Pocket OS devices, Hard disk, DVD, CD ROM, Modem, Plug and Play Storage, Flash Memory, PDA, MP3 Player devices, USB Printers, USB Scanners, USB add-on WiFi Adapters. The comprehensive list of devices is displayed in the device configuration list when creating the USB/Port Security element.

The list below shows the hierarchy of the list of devices in the USB and Port Security option for Desktop Authority, and some of the management options available for them:

- Ports (if you shut off a port then all devices attached to it will be unavailable)
    - BlueTooth Controllers
    - FireWire (1394) Controllers
    - Infrared Ports
    - Modems
    - Parallel Ports
    - PCMCIA/Cardbus Controllers
    - Serial Ports
    - USB Ports
    - WiFi Devices
- Removable Storage – Read and/or Write
- CD/DVD Readers/Writers – Read and/or Write
- Firewire (1394) Storage – Read and/or Write
- Floppy Disks – Read and/or Write
- Hard Disk Drives ** – Read and/or Write
- IoMega devices (Zip/Jaz Drives) – Read and/or Write
- MP3 Players *
- USB Storage – Read and/or Write
- PDAs
    - BlackBerry Devices
    - PocketPC Devices
    - Palm Devices
- Imaging
- USB Printers
- USB Scanners
- Unclassified USB Devices include all other USB detected devices.

* Uses a database of well-known MP3 players supplied by Desktop Authority, which can be extended by altering the C:\Program Files\Quest\Desktop Authority\PortSecurity\EmbargoDeviceClasses.xml file on each desktop

** Does not include partitions containing virtual memory, boot files or Windows system files

Validation Logic is used to determine which desktop computers will be configured with a given Permission Set. The Permission Set defines a permanent access control list for all portable devices on those desktop computers that match the Validation Logic. The access control list is enforced for all users and groups in the enterprise, regardless of who logged in and caused the permission set to be applied. The access control list remains in effect until a different permission set is applied to the desktop computer. Best practices will use Validation Logic to apply a Permission Set per computer or group of computers rather than by user since the Permission Set is enforced for all users and groups that subsequently access the desktop computer.

Permission Sets are defined within the USB/Port Security object. A Permission Set is a container that defines a set of devices and the type of access that is allowed for each device. Once a Permission Set is created, Users/Groups are assigned to the Permission Set. By default, all device types are given full control permissions when the permission set is created.

An explicit deny for a device type within a Permission Set will always supersede an explicit allow within another Permission Set in the same element. If a user validates for an element (containing multiple Permission Sets) that both denies and grants him/her access to a certain type of device, he/she will be denied access to that type of device. If a Permission Set does not explicitly grant a user permission to access a type of device, that user will automatically be denied access to that device type.

*If a user validates for multiple USB/Port Security elements, only the last element will be applied. The permissions in all permission sets for the validated USB/Port Security elements are summed to produce a "most restrictive" access control list.

Settings

Desktop options

Select **Install** or **Remove** to update the client workstation. An Install action will update the client workstation with the processes necessary to poll, allow and deny access to the client ports. A Remove action will uninstall all USB/Port Security client-side files and permissions.

Settings

Show Desktop task bar icon

Select this check box to display an icon in the notification area, at the far right of the taskbar of the client workstation. The icon indicates that USB/Port Security is actively watching client devices. Learn more about USB/Port Security on the client.

Show balloons on desktop

Select this check box to enable pop up device alerts in the notification area, at the far right of the taskbar on the client workstation. Learn more about USB/Port Security on the client.

> ⓘ Note: When *Show Balloons on Desktop* is selected and *Show Desktop task bar icon* is not selected, the task bar icon will appear if and when there are device alerts to show via a balloon message. However, when the icon does appear the context menu will be disabled.

Permission set

A permission set is a container that defines a set of devices and the type of access that is allowed for each device. Permissions include View, Write, Full Control and Deny.

The Permission Set list shows all of the sets of rules which have been configured.

Add

Click **Add** to create a new Permission Set. By default, all devices in the permission set are given Full Control permissions.

Edit

Click **Edit** to modify the selected permission set including the Permission Set name as well as the permissions allowed for selected devices and users/groups.

Once the permission set is defined (Add or Edit mode), the permissions for necessary devices should be defined. Each device can have its own permissions, Read, Write, Full Control or Deny. Once the devices are configured, users who this permission set applies to should be defined. Users include both single users and/or groups. Click **Add** in the Users list to select a user/group to assign to the Permission Set. Select a user or group from the user list and click **Remove** to delete it.

Disable All USB devices (except HID)

Select this option, when adding or editing a permission set, to disable all USB devices except Human Interface Devices (HID). A HID is any device that takes input. Included in this category are devices such as Keyboard, Mouse, Trackball, Touchpad, Webcam, Headset and others.

Remove

Click **Remove** to remove the selected permission set.

Logging

The Logging tab provides Data Collection options for USB/Port Security. This is where you can select specific types of data to collect. Choose from the following statuses: File Access Success, File Access Failure, Device Access Success, Device Access Failure.

Data collection options

Log file access success

Select this box to include File Access Success events to the log file.

Log file access failure

Select this box to include File Access Failure events to the log file.

Log device access success

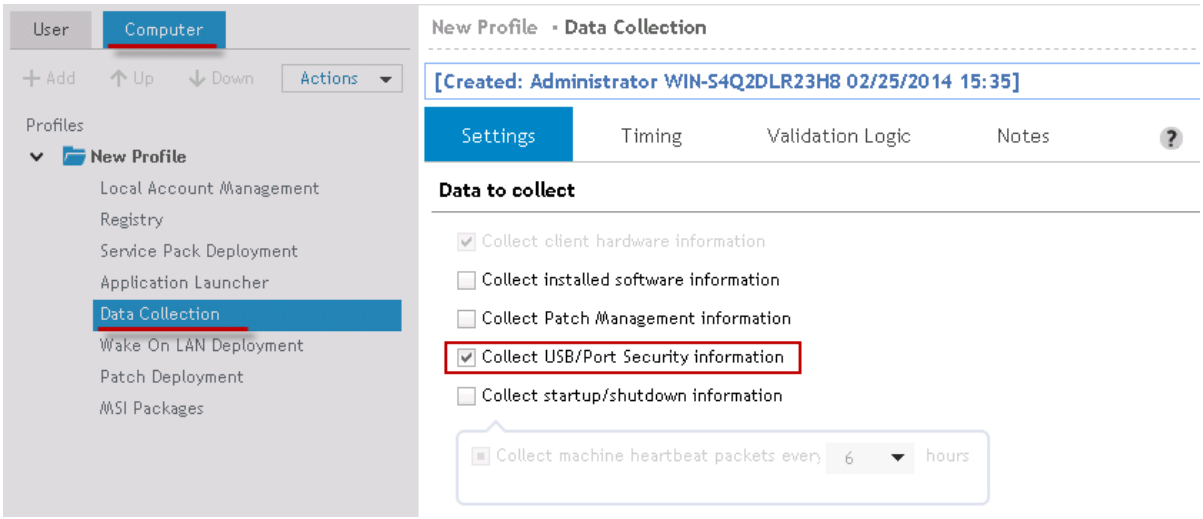
Select this box to include File Device Access Success events to the log file.

Log device access failure

Select this box to include File Device Access Failure events to the log file.

In order to collect USB/Port Security data, the Collect USB/Port Security Information box must be selected in the Computer Management Data Collection object.

Figure 51: Configure Data Collection to collect USB/Port Security data



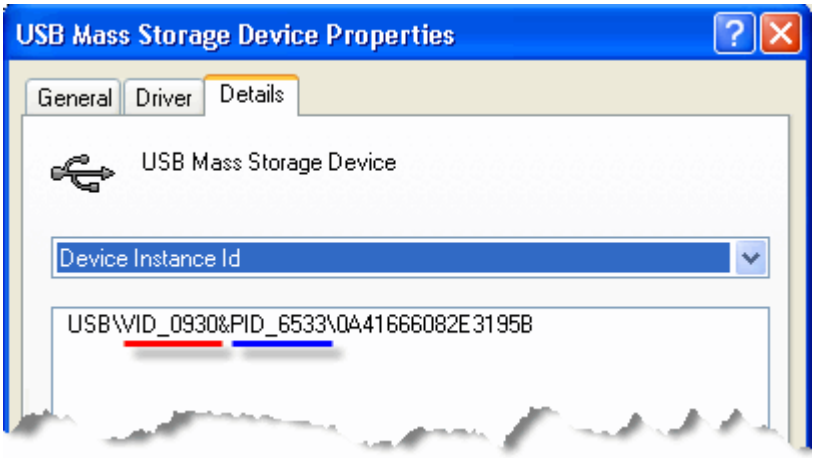
USB Device Exceptions

The USB/Port Security USB Device Exceptions tab provides a way to define a list of devices that are allowed/prohibited in to the Enterprise environment. Every USB device has a Vendor ID (VID) and Product ID (PID) to uniquely identify the device. These IDs are unique 16-bit numbers assigned to a specific vendor and product and are used for auto-detection, installation and configuration of the device to the machine.

Finding the VID/PID and Serial Number of a device

To look up the VID and PID of a device, go to the Device Manager. Locate the device in the list of components. Right-click on it and choose Properties. From the Properties dialog, select the Details tab.

Figure 52: Determine the VID and PID of a device



The VID and PID identifiers can be found within the Device Instance Id as shown above.

The Exceptions list is a list of devices that are either Allowed or Denied in the Enterprise's environment. Click **Add** to add a device to the list. Click **Edit** to update an existing device in the list. Click **Delete** to remove a device from the list.

Click **Add Existing** to add devices to the list that have been use in the enterprise environment.

Devices can be listed in a Comma-Separated file (CSV) with the VID, PID, Serial Number and Description. Click **Import** to read the file into the exception list. Click **Export** to write the devices in the list to a Comma-Separated file (CSV).

Select either Allow or Deny in the first column. Specify the VID and PID number for the specific device. The VID and PID numbers are required. Next enter a serial number and a description. The serial number and description fields are optional.

Administrative Override

Select the **USB/Port Security Administrative Override** tab to configure a password for the ability to temporarily override restricted device settings on the client computer.

Administrative password

Enable override

Select this box to set an administrative override password. This password can be used in the USB/Port Security service on the client computer.

On the client, right-click the USB/Port Security icon and select will give the user a new menu option to Disable Restrictions. If the correct password is entered, restrictions are lifted for the remainder of the user session.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

ⓘ *Note: This feature is not a standard part of Desktop Authority Essentials. To obtain this feature, Desktop Authority Essentials must be upgraded to the Standard edition of Desktop Authority.

USB/Port Security - client

Once a client validates for a USB/Port Security configuration, the USB/Port Security icon will be displayed in the client notification area.

Figure 53: USB/Port Security notification icon

USB/Port Security continually watches the system in order to secure the various devices/ports against the use of restricted devices on the company network. Clients can be notified via a popup warning upon the attempted use of a restricted device. If the system tray is not hidden from the client, permissions can be viewed via the system tray icon.

Configuring USB/Port Security on the client

To configure the client side of USB/Port Security, select the profile's USB/Port Security object.

Disable Popups

Select Disable Popups from the popup menu of the USB/Port Security system try icon to hide all system notifications from the client workspace.

Disable Restrictions

Select Disable Restrictions from the popup menu of the USB/Port Security system tray icon to override any security restrictions on your devices.

Enter the override password and click OK. You will be notified that the restrictions on the computer have been removed temporarily for the user's session on the computer.

See My Permissions

Select See My Permissions from the popup menu of the USB/Port Security system try icon to view access permissions to system devices/ports.

Figure 54: Viewing permissions set on computer

Web Browser

The Web Browser object provides the ability to configure Internet Explorer and Firefox settings as well as the operating system's Internet settings.

Common

General

Browsers

Apply element settings to these browsers

Select the appropriate web browsers to allow Desktop Authority to make changes to on the client.

Set default browser to

Desktop Authority can set the clients default web browser setting. Select the specific web browser from the drop list or select Leave alone to not change the default browser setting on the client.

> Note: This setting is supported in the OS versions up to Windows 7/2008.

Home page

The home page section handles whether Desktop Authority should be allowed to set the browser's home page setting on the client. There are three options to choose from.

Selecting **Leave alone** will tell Desktop Authority to ignore the home page setting. The home page setting on the client will not be touched. Select **Set home pages** to have Desktop Authority set the home page(s) to the specified URL. This option will not lock the user's ability to change this setting on the client. Select **Set home pages and prevent users from changing** to have Desktop Authority to set the home page(s) to the specified URL and lock the setting so the user cannot change it.

Enter the URL for the home page in the box below. You can set multiple home page tabs by specifying a home page link for each tab on its own line.

Downloads

The downloads section is where you will specify a file save location for files downloaded in the web browser on the client.

If the file location is not set, the browser's file download location will not be touched. Therefore, whatever option is set in the web browser's settings will be used.

Tabs

The Tabs section contains options that are related to using the browser with multiple tabs.

Show previews for individual tabs in the taskbar

Starting in Windows 7, you can quickly preview open windows that are in the taskbar. With the web browser that has multiple tabs open, you will also be able to preview the individual tabs when you hover the mouse over the browser icon in the taskbar. All tabs open in the browser will be displayed with a small preview above the taskbar.

Set this check box to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)

. Select this check box to enable the option to show previews of open tabs when the mouse hovers over the browser icon in the taskbar. Clear the check box to disable the option to show browser tab previews. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Warn me when closing multiple tabs

This option will save a user from accidentally closing the browser window if they only meant to close a single tab. Set this check box to one of three (3) different states: on (enabled) , off (disabled) , or grayed (preserve client setting) . Select this check box to enable the option to show a warning when closing a browser window with multiple tabs open. Clear the check box to disable the warning and just close the browser regardless of how many tabs are open. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Always switch to new tabs when they are created

The web browser has an option to control the active tab when a link is clicked that causes a page to be loaded in a new tab. Set this check box to one of three (3) different states: on (enabled) , off (disabled) , or grayed (preserve client setting) . Select this check box to enable the option and bring the new tab to the foreground. Clear the check box to disable the option and allow the new tab to stay in the background. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Enable quick tabs

Quick tabs is an Internet Explorer feature that allows you to see thumbnails of all open tabs in a single tab. Clicking on the thumbnail will activate the associated tab. In Firefox this feature is called All Tabs Preview, and is not enabled by default.

Set this check box to one of three (3) different states: on (enabled) , off (disabled) , or grayed (preserve client setting) . Select this check box to enable the option to show tab previews. Clear the check box to disable the option. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Always open links from other programs in a new tab in the current window

This option controls whether a new tab is created when a link is clicked or if the link is opened within the same tab. Set this check box to one of three (3) different states: on (enabled) , off (disabled) , or grayed (preserve client setting) . Select this check box to enable the option to open links in a new tab. Clear the check box to disable the option. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Miscellaneous

Remove "First Launch" setup screen (Internet Explorer only)

Set this check box to one of three (3) different states: on (enabled) , off (disabled) , or grayed (preserve client setting) . Select this check box to enable the First Run wizard. Clear the check box to disable the First Run

wizard. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Privacy tab

Pop-ups

The Pop-ups section is used to configure the browsers pop-up blocker as well as create a pop-up blocker exception list. Select one of four options from the drop list to configure the browsers pop-up blocker.

Select **Leave alone** to ignore this setting on the client's web browser. The option that is currently set on the client's web browser for the pop-up blocker will not be touched. **Select Turn on pop-up blocker** to enable the pop-up blocker and do not allow pop-up windows to open. Select **Turn off pop-up blocker** to disable the pop-up blocker and allow the browser to open all pop-ups. Select the **Turn on pop-up blocker and don't allow user to change it** option to enable the pop-up blocker option in the client browser and lock it so the option cannot be changed.

Selecting the option, **Turn on the pop-up blocker**, will enable the pop-up blocker exception list. The pop-up blocker allows for certain URLs to ignore the pop-up blocker.

Show Information Bar when pop-up is blocked

When a pop-up is blocked, the browser can inform you by displaying an Information Bar letting you know the pop-up window was blocked. This option controls whether the information bar is displayed or not. Set this check box to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  . Select this check box to enable the option and display an Information Bar when a pop-up is blocked. Clear the check box to disable the option of displaying an Information Bar. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Update the exception list by clicking the **Add** or **Remove** button. Click the **Import** button to import a list of URLs to the exception list.

When importing, the import file must be a tab delimited text file containing a Site Address and Action.

Example:

site1	add
site2	remove

Provides the following result when imported:

Figure 55: Results of imported exception list

Delete any exceptions from client that are not defined here

If selected, this option will delete all pop-up blocker exceptions that are defined on the client. If this option is not selected, the exceptions created on the client will be left alone.

History

Remember browsing history for at least xx days

Browsing history keeps track of the pages that have been visited in the web browser in the last xx days. Set this check box to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  . Select this check box to remember the web browser's browsing history for the specified number of days. Clear the check box to disable the browsing history option on the client. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Remember download history (Firefox only)

The download history window keeps track of files that are downloaded to the client, including files that are opened in the browser. When enabled, this option will tell the browser to keep track and remember the download history. Disabling this option will alert the browser to not bother keeping a history of downloaded files. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Clear history on Exit

When closing the web browser on the client, the history can be saved or not, depending on how the option is set in the browser. Set this check box to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  . Select this check box to clear the browser's history when it is closed. When selecting this option, you will be given a choice as to what history and files should be cleared. You can choose from Browsing history, Form history, Cookies, Cache, Saved passwords, Download history (Firefox only), Offline website data (Firefox only), Active logins (Firefox only), Site preferences (Firefox only), InPrivate filtering data (Internet Explorer only). All of these options also consist of a three state checkbox which allow you to clear the history, not clear the history or leave it alone, on the client.

Clear the check box to disable the browser's history on the client. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Auto complete

Another form of history that can be preserved on the web browser is AutoComplete history. This is where the browser will help you fill in or suggest to you what you may be typing if it is similar to something typed previously. In Firefox, this feature is called the Location bar.

There are options for the Form history, Browsing history, Favorites/bookmarks and Feeds (IE only). For each of these, select the check box to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  .

Cookies

A cookie contains information from a visited website and is stored on your computer. Most often they are used to remember certain settings for the site and are used for your return visit. Desktop Authority can configure the cookie settings for the web browser on the client.

A first-party cookie is a cookie that is issued by the web site that you are visiting.

A third-party cookie is issued by a site other than the one you are currently visiting.

Session cookies allow users to be recognized within a single website. Any page changes or item or data selection you do is remembered from page to page.

Select **Leave alone** to ignore the cookie settings on the client. Select **Don't accept cookies** to not allow cookies to be stored on the client at all. The other cookie options are **Accept session cookies only**, **Accept session and first party cookies**, and **Accept session, first party and third party cookies**.

There are always exceptions to the rule. You can create an exception list. This exception list will allow specific sites to handle cookies differently than the regular configuration. Click **Add** to add a site as an exception. Click **Remove** to remove a site from the list. Click the **Import** button to import a list of URLs to the exception list.

When importing, the import file must be a tab delimited text file containing an Site Address, Type and Action.

Example:

site1	block	add
site2	allow	remove

Provides the following result when imported:

Figure 56: Results of imported exception list

Delete any exceptions from client that are not defined here

If selected, this option will delete all cookie exceptions that are defined on the client. If this option is not selected, the exceptions created on the client will be left alone.

Security tab

Passwords

Allow browser to remember passwords

Both Internet Explorer and Firefox have the built-in ability to store passwords for future uses. In Firefox this is part of the Security options. In Internet Explorer it is part of the AutoComplete settings on the Content tab.

Set this check box to one of three (3) different states: on (enabled) , off (disabled) , or grayed (preserve client setting) . Select this check box to enable the browser to remember passwords. Clear the check box to disable the browser option to remember passwords. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Internet Explorer only

Phishing is a method that tricks you into divulging personal information by use of fake websites, email messages. Internet Explorer uses a Phishing filter and SmartScreen method to help combat these methods of gaining access to personal and/or sensitive information. They can also help by preventing the installation of malicious software or malware.

The **Phishing filter/SmartScreen** options can be configured by setting the Phishing filter/SmartScreen option. Set this check box to one of three (3) different states: on (enabled) , off (disabled) , or grayed (preserve client setting) . Select this check box to enable the Phishing filter and SmartScreen. Clear the check box to disable the Phishing filter and SmartScreen. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Firefox Only

Block reported attack sites

This Firefox option will check whether the site you are visiting may be an attempt to interfere with normal computer functions or send personal data about you to unauthorized parties.

Set this check box to one of three (3) different states: on (enabled) , off (disabled) , or grayed (preserve client setting) . Select this check box to enable the use of this option on the client. Clear the check box to disable this setting on the client. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Block reported web forgeries

This Firefox option will actively check whether the site you are visiting may be an attempt to mislead you into providing personal information (phishing).

Set this check box to one of three (3) different states: on (enabled) , off (disabled) , or grayed (preserve client setting) . Select this check box to enable the use of this option on the client. Clear the check box to disable this setting on the client. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Password exceptions

A password exception list can be created. This exception list will allow specific sites to handle remembering passwords differently than the regular configuration. Click **Add** to add a site as an exception. Click **Remove** to remove a site from the list. Click the **Import** button to import a list of exceptions to the list.

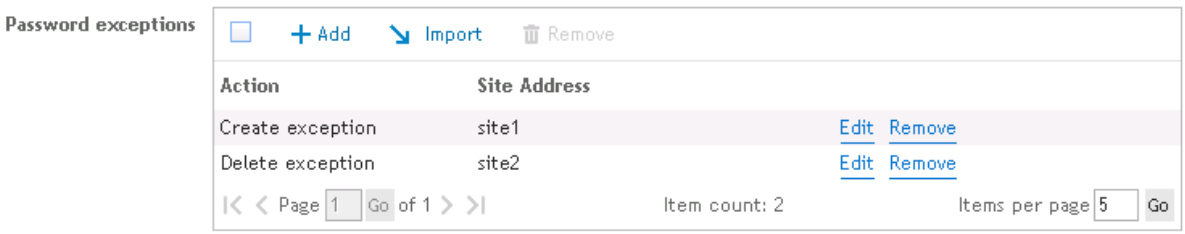
When importing, the import file must be a tab delimited text file containing a Site Address and Action.

Example:

site1	add
site2	remove

Provides the following result when imported:

Figure 57: Results of imported exception list



Delete any exceptions from the client that are not defined here

If selected, this option will delete all password exceptions that are defined on the client. If this option is not selected, the exceptions created on the client will be left alone.

Add-ons

Warn me when sites try to install add-ons

Firefox will warn you when a website tries to install an add-on and blocks the installation prompt.

Set this check box to one of three (3) different states: on (enabled) , off (disabled) , or grayed (preserve client setting) . Select this check box to enable this option on the client. Clear the check box to disable this setting on the client. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

To allow installations from a specific site, add an Exception to the exception list. The exception list will allow the installation of add-ons from specific sites differently than the regular configuration. Click **Add** to add a site as an exception. Click **Remove** to remove a site from the list. Click the **Import** button to import a list of exceptions to the list.

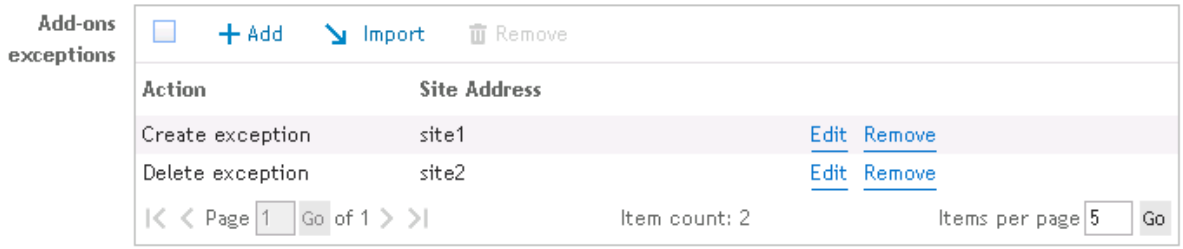
When importing, the import file must be a tab delimited text file containing a Site Address and Action.

Example:

site1	add
site2	remove

Provides the following result when imported:

Figure 58: Results of imported exception list



Delete any exceptions from the client that are not defined here

If selected, this option will delete all Add-on exceptions that are defined on the client. If this option is not selected, the exceptions created on the client will be left alone.

Prevent users from changing any settings on these pages

Each of these pages can be configured for the selected web browser(s) to be locked and unavailable to the user or unlocked and available for changes by the user. Access to the Internet Options pages include the General settings, Security settings, Content settings, Connection settings, Programs/Applications settings and the Advanced settings are controlled by this setting.

The check boxes can be set to one of three (3) different states: on (locked/unavailable for changes) , off (unlocked and available to the user) , or grayed (preserve the current client setting) . Select this check box to

enable the option on the client. Clear the check box to disable the setting on the client. Gray the check box to disable Desktop Authority's control of this option. In this case the option that is currently set on the client's web browser will not be touched when this is grayed.

> Note: In Firefox, there is a special circumstance that occurs with the Advanced and Connection settings dialog. This differs from Internet Explorer because the Connection settings dialog is tied to the Advanced settings tab.

If either the Connection page **OR** the Advanced page is set to be locked () within a Desktop Authority profile element, the Connection settings page will always be set to a locked state making it unavailable to the user.

If the Connection page and the Advanced page are set to locked () on one of them and Leave alone () on the other, then the Connection settings dialog will be left in its current state and not configured by Desktop Authority.

Windows Internet settings

Proxy options

> Note: Proxy Settings for Firefox are configured in the Windows system settings which can be verified in the Control Panel > Internet Options applet.

Automatic Configuration

Automatically detect settings

This setting will automatically detect the proxy settings for your network.

Set this option to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  . Select this check box to enable the option on the client. Clear the check box to disable the setting on the client. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Use automatic configuration script

Automatic configuration of the proxy uses a proxy auto-config (PAC) file to define how the web browsers are to automatically choose the proper proxy server.

Set this option to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  . Select this check box to enable the option on the client. Clear the check box to disable the setting on the client. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Automatic proxy configuration URL

Configuration URL

Type an address (URL) or file name that will be used for the automatic configuration script.

Manual configuration

Manually configuring the proxy server for your LAN connection requires you to specify the specific host and port for each web protocol.

Use a proxy server for your LAN connection (does not apply to dial-up or VPN connection)

Set this option to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  . Select this check box to enable the option on the client. Clear the check box to disable the setting on the client. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Manual proxy configuration

If **Use a proxy server for your LAN connection** is selected, you must enter the specific proxy information (host or ip, and port) for each protocol. Proxies can be set for HTTP, SSL, FTP, Gopher and SOCKS protocols. Once the HTTP Proxy is entered, you may elect to use these settings for all protocols.

Exceptions

Specify, if any, one or more sites or IP addresses to ignore proxy settings for. Separate each exception with a semicolon (;).

> Note: When adding a site to the exceptions list, it is preferred that an asterisk precede the site name. This is required for IE browsers, however FireFox will work without specifying the asterisk. The exception dialog box also allows a wildcard character (*) to be used in the place of zero or more characters in an ip address. For example, you can use "123.1*.66.*" to bypass addresses such as "123.144.66.12," "123.133.66.15," and "123.187.66.13."

Bypass proxy server for local addresses

Set this option to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  . Select this check box to set the option, to ignore the proxy server for local addresses, on the client. Clear the check box to set the option to use the proxy server for all Internet addresses on the client. Gray the check box to disable Desktop Authority's control of this option. The option that is currently set on the client's web browser will not be touched when this is grayed.

Prevent user from making changes to proxy setting

To lock the proxy settings so the user is not able to change the settings on the client, select this box. Clear this box to leave the proxy configuration open and available for change by the client.

Restricted sites

Restricted sites are web sites that you do not trust. Sites that are restricted are not able to be visited. Click **Add** to add a site to the restricted site list. Click **Remove** to remove the selected site. Click the **Import** button to import a list of restricted sites.

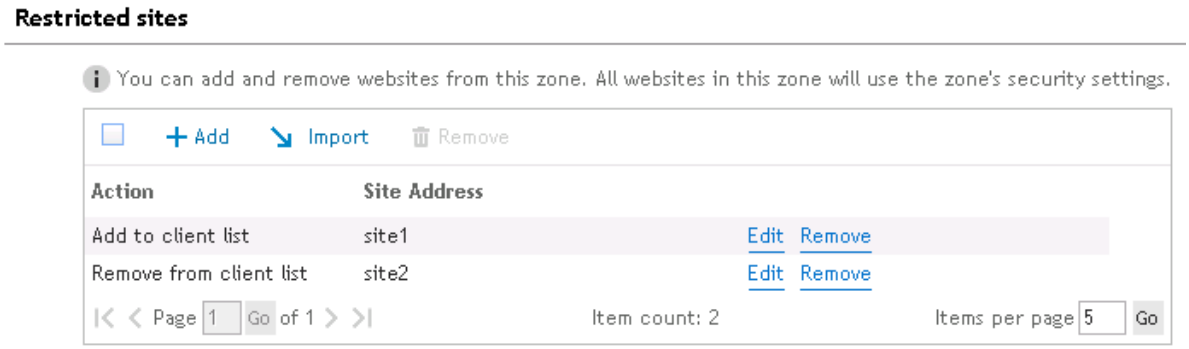
When importing, the import file must be a tab delimited text file containing a Site Address and Action.

Example:

site1	add
site2	remove

Provides the following result when imported:

Figure 59: Results of imported restricted sites



Remove any websites from the client that are not defined here

If selected, this option will delete all restricted sites that are defined on the client. If this option is not selected, the restricted sites on the client will be left alone.

Trusted sites

Trusted sites are web sites that you unconditionally trust. This can be in the form of a URL or IP address. Click **Add** to add a site to the trusted site list. Click **Remove** to remove the selected site. Click the **Import** button to import a list of trusted sites.\

> Note: When entering a URL the HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains key is updated. If an IP address is entered the Ranges key, HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Ranges is updated. Please refer to the Microsoft article: Internet Explorer security zones registry entries for advanced users (Article ID: 182569) for more details on the ZoneMap keys.

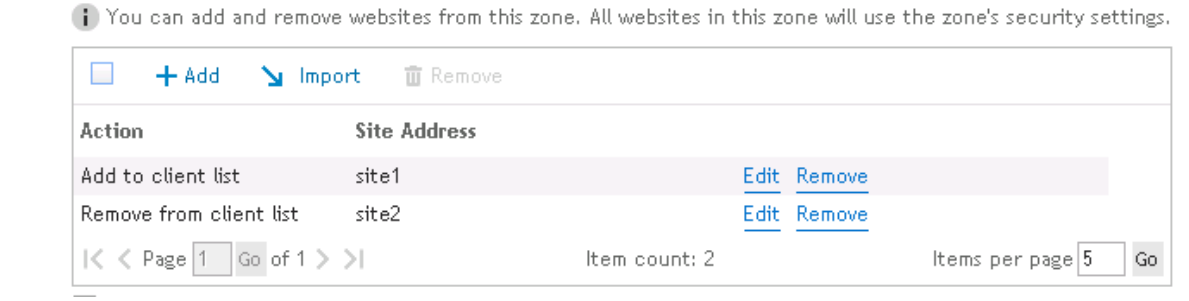
When importing, the import file must be a tab delimited text file containing Site Address and Action.

Example:

site1	add
site2	remove

Provides the following result when imported:

Figure 60: Results of imported trusted sites



Remove any websites from the client that are not defined here

If selected, this option will delete all trusted sites that are defined on the client. If this option is not selected, the restricted sites on the client will be left alone.

Require server verification (https:) for all sites in this zone

Select this option to allow only https: sites to be added to this zone. Unchecked, you will be able to add any site to this zone.

Local intranet sites

The Local Intranet zone contains all network connections that were established by using a Universal Naming Convention (UNC) path, and Web sites that bypass the proxy server or have names that do not include periods (for example, http://local), as long as they are not assigned to either the Restricted Sites or Trusted Sites zone.

Automatically detect intranet network

Select this box to allow Windows to automatically determine which sites are port of the Intranet. Unselect this box to detect which sites are deemed to be part of the Local intranet security zone.

Include all local (intranet) sites not listed in other zones

With the local intranet not being automatically detected, select this box to include all local sites in the intranet security zone, as long as they do not belong to any other zone.

Include all sites that bypass the proxy server

With the local intranet not being automatically detected, select this box to include all sites that bypass the organization's proxy server in the intranet security zone.

Include all network paths (UNCs)

With the local intranet not being automatically detected, select this box to include network paths in the intranet security zone.

Click **Add** to add a site to the trusted site list. Click **Remove** to remove the selected site. Click the **Import** button to import a list of trusted sites.

When importing, the import file must be a tab delimited text file a Site Address and Action.

Example:

site1	add
site2	remove

Provides the following result when imported:

Figure 61: Results of imported local intranet sites

Remove any websites from the client that are not defined here

If selected, this option will delete all local intranet sites that are defined on the client. If this option is not selected, the restricted sites on the client will be left alone.

Require server verification (https:) for all sites in this zone

Select this option to allow only https: sites to be added to this zone. Unchecked, you will be able to add any site to this zone.

Custom Settings

The Web Browser object allows for the configuration of custom Firefox settings. If you wish to configure something in the Firefox browser that is not offered on the Web Browser object, it can be configured in the Global or Profile Definitions. See AddCustomFirefoxPref for custom setting details.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Windows Firewall

The **Windows Firewall** object allows Microsoft's Windows Firewall to be enabled or disabled on any validated computer having the Windows XP x86 SP3 or Windows XP x64 SP2 operating system installed. The ability to specify certain port and program exceptions is also specified on this object's setting tab. Windows Firewall is only applicable on Windows XP x86 SP3 and Windows XP x64 SP2 or greater.

Settings

Windows Firewall

Select an action (Enable/Disable) to configure the Windows Firewall component on client computers.

Display a notification when Windows Firewall blocks a program

This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  .

Select this check box to display a visual notification to the user when the Firewall blocks a program from accepting an incoming request. The notification dialog box will allow the user to determine if the Windows Firewall should allow the program to keep blocking the program or to allow incoming requests to the program. Clear this check box for no visual notification or occur. Gray the box to leave the client's setting untouched.

Enable file and print sharing

This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  .

Select this check box to enable File and Print sharing on each validated client. Clear this box to disable File and Print sharing on each validated client. Gray the box to leave the client's setting untouched.

Don't allow exceptions (inbound firewall only)

This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  .

Select this box to disallow all excepted traffic specified in the exceptions list. Clear this box to allow traffic. Gray the box to leave the client's setting untouched.

Exceptions

The Exceptions list is a holding place for all Firewall port and program exceptions. Click **Add** to add an exception to the Exception list. Click **Edit** to edit an existing exception on the list. Click **Delete** to remove a configured port or program from the Exception list.

Action

Select *Open* or *Close* from the Action list. This will configure the specified port to be opened or closed for incoming traffic.

Type

Select *TCP*, *UDP* or *Program* from the Protocol list to specify the type of port or program to be configured.

Exception

When the Type is set to TCP or UDP, type the port number to be opened or closed into the Exception entry box. When the Type is set to Program, specify the path to the executable program into the Exception entry box.

Description

Type a meaningful description or reason for the exception in the Description box.

Scope

Select *Any Computer*, *My Network (subnet) only* or Custom List from the Scope list. *Any Computer* specifies that incoming traffic on the port is allowed regardless of where it is coming from. *My Network (subnet) only* specifies that incoming traffic on the specified port is allowed only if the request is coming from the local network. Custom List specifies that incoming traffic from any computer specified in the custom list is allowed. Delineate the custom list of IP addresses by commas.

Advanced

The Windows Firewall Advanced tab allows specific types of ICMP messages to be enabled or disabled. ICMP messages are used for diagnostics and troubleshooting. The requests listed below are types of requests that the computer may or may not need to respond to. Select each Internet request type that the computer will respond to. Clear each Internet request type that the computer will not respond to.

Default filters

Domain profile

A rule in the Domain profile applies when a computer is connected to a domain.

Allow inbound connections that do not match a rule

Check this box to allow an inbound connection request even if it does not match a Domain profile rule. This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  . Gray the check box to leave the client's setting untouched.

Allow outbound connections that do not match a rule

Check this box to allow an outbound connection request even if it does not match a Domain profile rule. This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  . Gray the check box to leave the client's setting untouched.

Private profile

A rule in the Private profile applies when a computer is connected to a private network location.

Allow inbound connections that do not match a rule

Check this box to allow an inbound connection request even if it does not match a Private profile rule. This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  . Gray the check box to leave the client's setting untouched.

Allow outbound connections that do not match a rule

Check this box to allow an outbound connection request even if it does not match a Private profile rule. This check box can be set to one of three (3) different states: on (enabled)  , off (disabled) , or grayed (preserve client setting) . Gray the check box to leave the client's setting untouched.

Public profile

A rule in the Public profile applies when a computer is connected to a public network location.

Allow inbound connections that do not match a rule

Check this box to allow an inbound connection request even if it does not match a Public profile rule. This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  . Gray the check box to leave the client's setting untouched.

Allow outbound connections that do not match a rule

Check this box to allow an outbound connection request even if it does not match a Public profile rule. This check box can be set to one of three (3) different states: on (enabled)  , off (disabled)  , or grayed (preserve client setting)  . Gray the check box to leave the client's setting untouched.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Notes

Select the **Notes** tab to create any additional notes needed to document the profile element.

Description

When adding or modifying a profile object element, the description appears above the settings tab. Enter a description to annotate the element. The default value for new profile elements can be changed by going to the system Preferences.

Desktop Authority reference

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	✓	✓

Feature	Professional/Standard	Essentials
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	✓	
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).

Files and logs locations

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

Replication

The Replication process logs the files and target folders that are copied during the replication process. The log file can be found in (32-bit OS) %Program Files%\Quest\Desktop Authority\Desktop Authority Manager\SLRepl.log or (64-bit OS) %Program Files (x86)%\Quest\Desktop Authority\Desktop Authority Manager\SLRepl.log.

User Management

During replication, user management files are published to the User Management target replication folder. By default, this folder is NETLOGON (*%windir%\SYSVOL\sysvol\DomainName\scripts* is shared as NETLOGON). The files are published from the SLscripts$ share (32-bit OS) - *%Program Files%\Quest\Desktop Authority\Desktop Authority Manager\Scripts* or 64-bit - *%Program Files (x86)%\Quest\Desktop Authority\Desktop Authority Manager\Scripts*).

Computer Management

Also during replication, computer management files are published to the Computer Management target replication folder. By default, this folder is located at *SYSVOL\[DomainName]\Policies\Desktop Authority\Device Policy Master*. The files are published from (32-bit OS) - *%Program Files%\Quest\Desktop Authority\Desktop Authority Manager\Device Policy Master* or (64-bit OS) - *%Program Files (x86)%\Quest\Desktop Authority\Desktop Authority Manager\Device Policy Master*.

Some files are published to the *\SYSVOL\[DomainName]\Policies\Desktop Authority\Desktop Authority Agent 8.0* folder.

DA Administrative Service

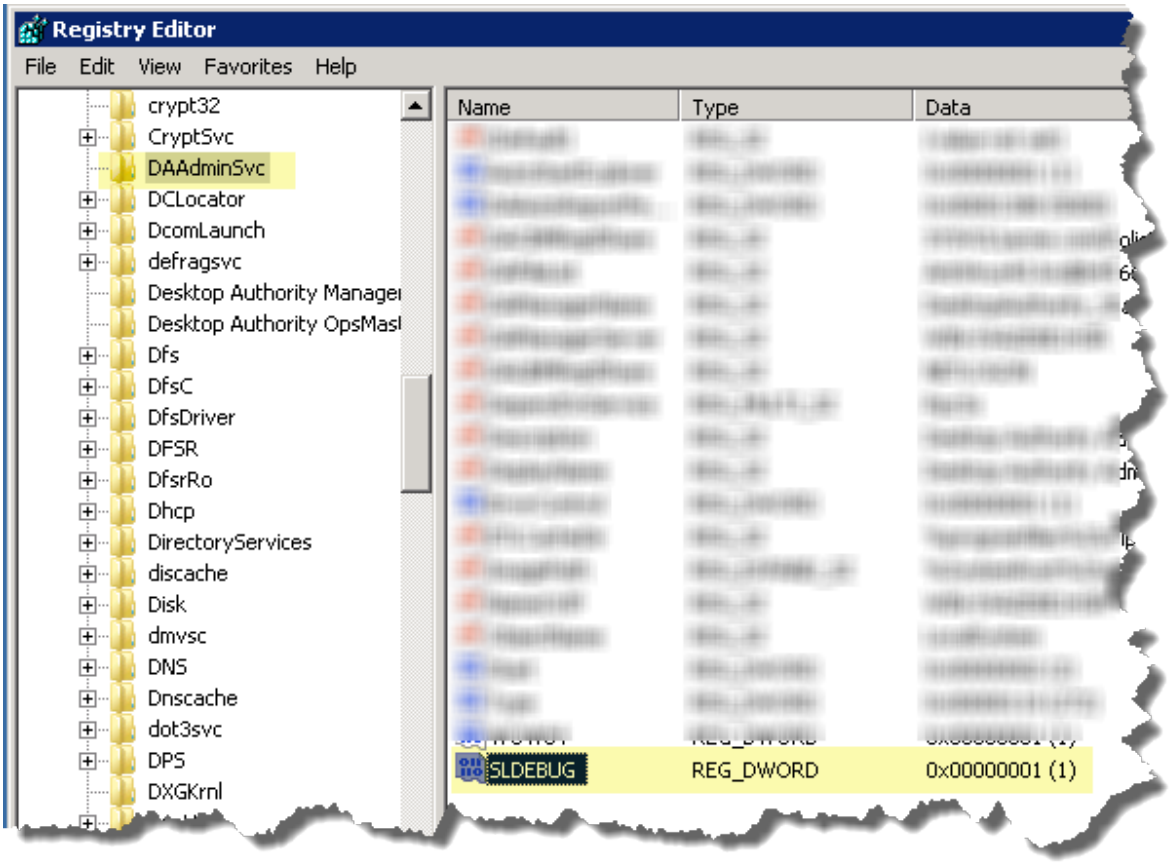
- The DA Administrative Service Data Collection XML file repository can be found at *%programfiles%\Quest\Desktop Authority\ETL Cache*.
- The DA Administrative Service log file repository can be found at (32-bit) *%SystemRoot%\System32* or (64-bit) *%SystemRoot%\SysWow64* The log file is named *DAAdminSvc_%ServerName%.log*.*
- The log file for the StatusGateway is located in the DA Administrative Service's account user profile *%temp%\DesktopAuthority\DAStatusGateway.log* on the server where the DA Administrative Service is installed.*

*Both the StatusGateway and Administrative Service log files can be enabled by setting or creating a registry key for the service.

Add or modify the SLDEBUG registry value in "HKLM\SYSTEM\CurrentControlSet\services\DAAdminSvc"

Set SLDEBUG to a DWORD whose value <>0 (1) to enable the log files.

Figure 62: Editing the DAAdminSvc in the Registry



Update Service

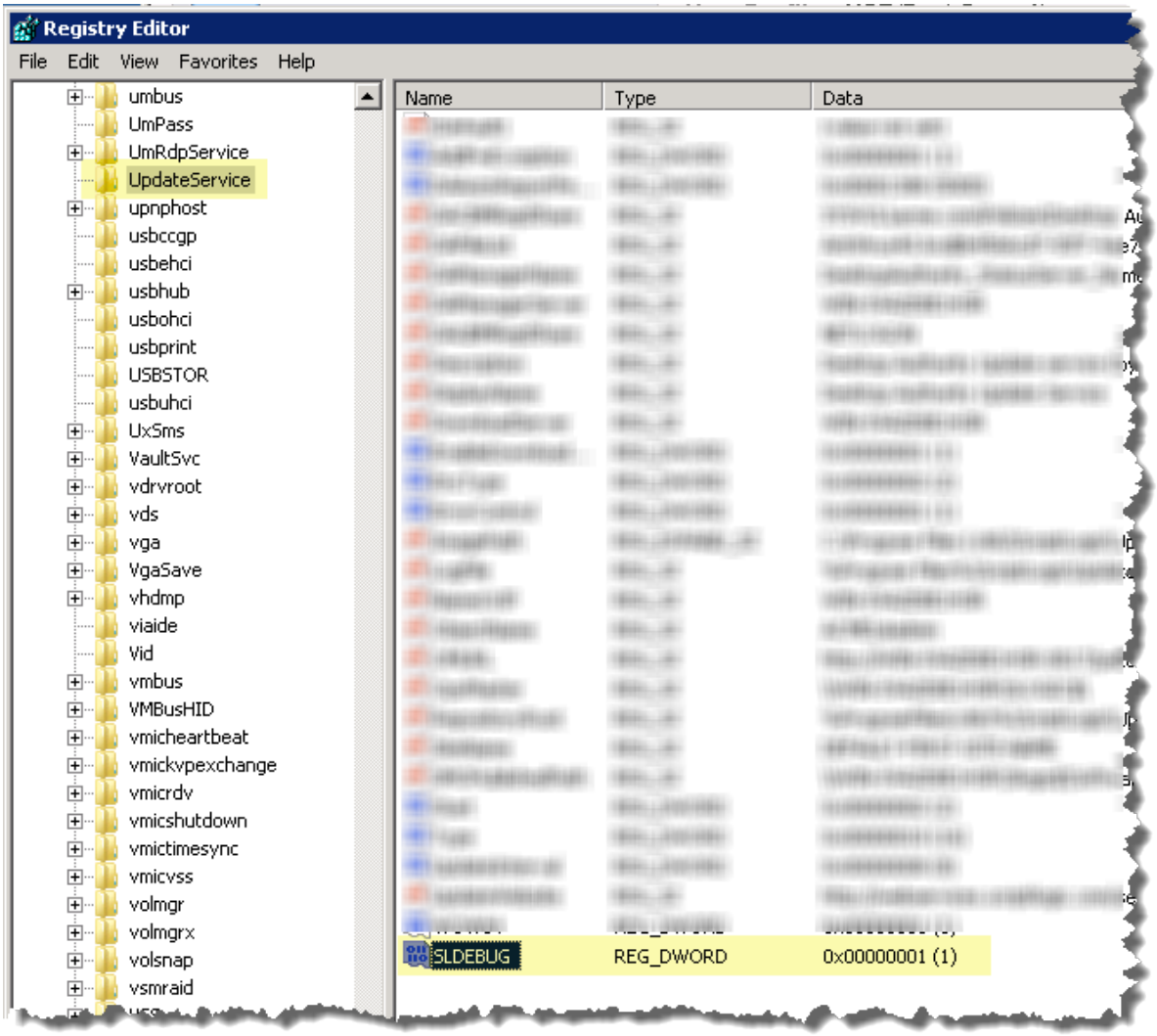
- The Update Service download cache can be found *%programfiles%\Quest\Desktop Authority\Update Service*. The files are named daupdsvc#.log.This repository containsSoftware Management catalog.
- The log file for the Update Service status reporter is located in the Update Service Account user profile *%temp%\DesktopAuthority\DAUpdtSvcStRep.log* where the Update Service has been installed.*

*Both log files can be enabled by setting or creating a registry key for the service.

Add or modify the SLDEBUG registry value in "HKLM\SYSTEM\CurrentControlSet\services\UpdateService"

Set SLDEBUG to a DWORD whose value <>0 (1) to enable the log files.

Figure 63: Editing the Update Service in the Registry



Log files

User

Desktop Authority uses the User's temp directory to store log files that pertain to the actual user events related to Desktop Authority. The users temp directory can be found in %TEMP%\ Desktop Authority.

Client configuration logs for the Web Browser and Folder Redirection profile objects

- SLTraceLogonCC.log
- SLTraceLogoffCC.log
- SLTraceRefreshCC.log
- SLTraceCC.log

SL Agent COM object is used for logging events (logon, logoff, inactivity and COM object registration) on the client

- SlagentÂ*.log

Detailed diagnostic log files for User based events. The log files are time stamped and record all User Management configuration settings applied to the client.

- SltraceÂ.htm - logon events
- SltracelogoffÂ.htm - logoff events
- SltraceenforceÂ.htm –refresh events

The SLTrace Update Service Locator logs entries showing the determination of which Update Service the client should use based on response time. Services are queried from a list servers provided by the Engine which are based on the computer's site.

- SLTraceUSLoc_*.htm

Other files may appear in the User's temp directory for more in-depth troubleshooting, if necessary.

Computer

Computer based log files will be stored on each individual client machine in the Windows temp directory, *%windir%\Temp\Desktop Authority*.

Detailed diagnostic log files for Computer based events. The log files are time stamped and record all Computer Management configuration settings applied to the client.

- ComputerManagementTrace*.htm

The SLTrace Update Service Locator logs entries showing the determination of which Update Service the client should use based on response time. Services are queried from a list servers provided by the Engine which are based on the computer's site.

- SLTraceUSLoc*.htm

Client files

Various files are stored on each client utilizing Desktop Authority. There are 3 folders that may be used depending on the Desktop Authority features used and the client platform. These folders are %SystemDrive%\Quest\Desktop Authority, %SystemDrive%\%Program Files%\Quest\Desktop Authority, %SystemDrive%\%Program Files (x86)%\Quest\Desktop Authority.

USB/Port Security client files are stored in the %Program Files%\Quest\Desktop Authority folder.

The following files are stored in %Program Files%\Quest\Desktop Authority or %Program Files (x86)%\Quest\Desktop Authority

- DA Update Client - Client side update service (used with Software Management)
- SLagent - Desktop client files used with the DA client service, if necessary
- DA client service - This service provides run as admin functionality
- Computer Management - Client Side service and configuration files

Replication files and their targets

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

Desktop Authority uses replication as a method of publishing Desktop Authority configurations to selected targets, which are usually Domain Controllers.

A log file is created during the replication process and lists each file that is published and to which folder. The log file is named SlRepl.txt.

This file can be located on the Operations Master in either (32-bit OS) - *%Program Files%\Quest\Desktop Authority\Desktop Authority Manager* or (64-bit OS) - *%Program Files (x86)%\Quest\Desktop Authority\Desktop Authority Manager*.

User Management

User Management files are published from the %Program Files%\Quest\Desktop Authority\Desktop Authority Manager\Scripts or %Program Files (x86)%\Quest\Desktop Authority\Desktop Authority Manager\Scripts, which is shared as SLscripts$.

User Management files are replicated to the User Management replication folder specified in Server Manager. This folder, by default, is \\server_name\NETLOGON (%windir%\SYSVOL\sysvol\[Domain Name]\scripts folder is shared as NETLOGON), but can be changed if necessary.

- DAClientInstall.msi
- DaLocMap.ini
- DASiteMap.ini
- daUpdateClient.exe
- DAUSLoc.dll
- DAUSLocCOM.dll
- {GUID}.sld
- {GUID}.slp
- dotnetfx.exe
- Interop.SLAgent.dll
- msvcp71.dll
- msvcr71.dll
- netfx64.exe
- NetOrder.exe
- profiles.sl
- psapi.dll
- ScriptLogic.MapiServer.exe
- ScriptLogic.MapiServer64.exe
- shfolder.dll
- slAgent.dll
- slAgent.exe
- slAPIEng90.dll
- slBoost.exe
- SLBoost.ini

- slDataCollection.dll
- slEngine.dll
- slInstall.exe
- SLogic.bat
- SLPdefault.SL
- SLPDefault.sld
- slSigs.ini
- slStart.exe
- SLStart.ini
- sqlite3.dll
- USBPort Security.exe
- usbps_x64.exe
- VarDefs.sl
- vcredist_x86.exe
- wKiX32.exe
- xdel.exe

Computer Management

Computer Management files are published from (32-bit OS) - %Program Files%\Quest\Desktop Authority\Desktop Authority Manager\Device Policy Master or (64-bit OS) - %Program Files (x86)%\Quest\Desktop Authority\Desktop Authority Manager\Device Policy Master.

This folder is shared as DADevicePolicyMaster$.

Computer Management files are replicated to the Computer Management replication folder specified in Server Manager. This folder, by default, is SYSVOL\[DomainName]\Policies\Desktop Authority\Device Policy Master, but can be changed if necessary.

- CBMConfig.xml.gzip
- ComputerConfiguration.ini
- DAClientInstall.msi
- dalocmap.ini
- dasitemap.ini
- daUpdateClient.exe
- DAUSLoc.dll
- DAUSLocCOM.dll
- dotnetfx.exe
- msvcp71.dll
- msvcr71.dll
- NetFx64.exe
- SLLicense.ini

- slsigs.ini
- slstart.ini

Desktop Authority API

The Desktop Authority API is a documented set of functions, variables and supplemental utility programs that allow you to fully harness the capabilities of Desktop Authority through custom scripting.

The Desktop Authority API can be broken down into four categories:

Functions: Wrap many lines of KiXtart code (and supplemental utilities) into a single line of code, for easy insertion into your custom scripts. Many of the Desktop Authority API functions are direct replacements for native KiXtart functions -- and they can overcome the security restrictions of the user logging on.

Dynamic Variables: Globally defined variables in the Desktop Authority engine. These variables are used by the engine itself and can be used in custom scripting.

Utility Programs have been developed to expand upon the built-in functionality of KiXtart. These tools are often wrapped by API Functions eliminating the need to execute them directly.

Desktop Authority API - Dynamic Variables

Predefined Dynamic Variables can be used to aid in the creation of configuration elements. These variables are globally defined and used by Desktop Authority during the client logon process. Using them is helpful, if not a necessity, when writing custom scripts.

Dynamic Variables can be used in virtually every field within the Desktop Authority manager, including those fields with built-in lists. Simply press the **F2** key to display a dialog that allows the selection of a predefined variable from a visual list. The dynamic variable will be inserted at the current position of the cursor.

These variables are available for a few different categories:

Applications Variables
Date and Time Variables
Folder and Disk Variables
Messaging System Variables
Network Variables
Operating System Variables
Security Variables
System Variables

$ConnType

Connection Type:

LAN - LAN or WAN connection

RAS - dial-up networking connection

$Date

Current date (e.g. "2000/04/01")

$Description

Description (from UMD)

$DllDir

Location of OS DLL's (e.g. Windows - "C:\Windows\System") (e.g. Win NT - "D:\WinNT\System32")

$Domain

Domain (or Workgroup) that computer belongs to.

$ExitFlag

If set to 1 in a custom script, Desktop Authority will immediately exit after pre or post-engine custom scripts complete.

$FreeSpace

Available disk space on $SystemDrive (in bytes)

$FreeSpaceMb

Available disk space on $SystemDrive (in Megabytes)

$GreetingTime

"morning", "afternoon" or "evening", based on time of day 00:00-11:59, 12:00-17:59, 18:00-23:59, respectively.

$HomeBase

Base sharename part of $HomePath. (e.g. "Users")

$HomeDir

'Long' name of the directory part of the home directory. (e.g. "bjohnson")

$HomePath

Complete home path, including the server, base share and home directory. (e.g. "\\Server1\Users\JohnSmith")

$HomeServer

Server-only part of $HomePath, without leading backslashes. (e.g. "MyServer")

$HomeShare

Server & base share parts of $HomePath. (e.g. "\\Server\Users")

$HostName

TCP/IP host name of the client.

$IeVersion

Internet Explorer Version

$IPAddr

IP address (First address detected)

$IPOct1

The first octet of $IPAddr

$IPOct2

The second octet of $IPAddr

$IPOct3

The third octet of $IPAddr

$IPOct4

The fourth octet of $IPAddr

$LogonServer

Authenticating Domain Controller - without leading backslashes. (Example: "server1')

$Lserver

Authenticating Domain Controller - with leading backslashes. (Example: "\\server1")

$MACaddr

Network MAC address (adapter 0)

$MapiDefProfile

Name of the default Windows Messaging System profile for the user logging on.

$NetLogon

location of Desktop Authority scripts on authenticating server in UNC form.
Example 1 - "\\server1\netlogon"
Example 2 - "\\server2\netlogon\site1"

$NtOsVerVal

Numeric value of the OS version, expressed as an integer (e.g. 40 or 50)

$NtType

a PDC, BDC or Member Server will return "Server"
an NT Workstation or Windows 2000 Professional will return "Workstation"

$OsBuildNumber

Operating System build number (e.g. 1381)

$OsCsdVersion

Operating System current service pack (e.g. Service Pack 4.0)

$OsType

Operating System type:
95 - Windows 95
98 - Windows 98
NT - All versions of NT/2000

$OsVersion

Operating System version (e.g. " NT Workstation 4.0")

$Priv

Privilege level of user on the domain: "User" or "Admin"

$ProgramFilesDir

Loc. of Program Files on the client (e.g. " C:\Program Files")

$PwDaysLeft

Number of days before password expiration.

$RestartFlag

If set to 1, user will be forced to logoff. A 2 will force the client to reboot.

$ShellAppData

Location of client's Application Data shell folder.

$ShellCache

Location of client's Temporary Internet Files shell folder.

$ShellCookies

Location of client's Cookies folder.

$ShellDesk

Location of client's Desktop shell folder

$ShellDeskCommon

Location of NT client's Common (All Users) Desktop shell folder.

$ShellFavorites

Location of client's Favorites shell folder (IE bookmarks).

$ShellFonts

Location of client's Fonts shell folder.

$ShellHistory

Location of client's History shell folder.

$ShellLocAppData

Location of client's Local Application Data shell folder.

$ShellMyPictures

Location of client's My Pictures shell folder.

$ShellNetHood

Location of client's Network Neighborhood shell folder.

$ShellPersonal

Location of client's Personal shell folder.

$ShellPrintHood

Location of client's Printer Neighborhood shell folder.

$ShellProg

Location of client's Start-Menu Programs shell folder.

$ShellProgCommon

Location of NT client's Common (All Users) Start-Menu Programs shell folder.

$ShellQLaunch

$ShellRecent

Location of client's Recent Documents shell folder.

$ShellSendTo

Location of client's Send To shell folder.

$ShellSMCommon

Location of NT client's Common (All Users) Start-Menu shell folder.

$ShellStartMenu

Location of client's Start-Menu shell folder

$ShellStartup

Location of client's Startup shell folder.

$ShellTemplates

Location of client's Templates shell folder.

$SiCpuSpeed

System Info: CPU #1 MHz (approx.)

$SiCpuType

System Info: CPU #1 Type

$SiCpuVendID

System Info: CPU #1 Vendor ID

$SID

Security Identifier (SID) of current user.

$SiDesktopSize

System Info: Size of desktop (Width x Height)

$SiHDiskSizeGb

System Info: Size of Hard Drive #1

$SiRamMb

System Info: Physical memory, in Mb

$SiSysBiosDate

System Info: System BIOS Date

$SiSysBiosName

System Info: System BIOS Mfg.

$SiVidBiosDate

System Info: Video BIOS Date

$SystemDrive

Drive where OS loaded from (e.g. "C:")

$TermServClient

0 = Non-Terminal Server Client
1 = Terminal Server Client

$Time

Current time (e.g. "14:10")

$TimeHour

Current 2-digit hour (e.g. "14")

$TimeMin

Current 2-digit minutes (e.g. "10")

$TSClient

0 = Non-Terminal Server Client

1 = Terminal Server Client

$UserID

Logon ID of the user.

$VerboseOs

Operating System version.build (e.g. " NT Workstation 4.0.1381")

$W9xPrfEnabled

For Windows 95 & 98 clients:

0 = User Profiles are not enabled.

1 = User Profiles are enabled.

Desktop Authority API - Functions

The Desktop Authority API functions are designed to streamline your custom scripts by reducing the amount of code you must write. They will also allow you to overcome security limitations of the user.

slAEnumKey

Enumerates registry keys into a single dimensional array.

Description:

Enumerates registry keys into a single dimensional array.

Syntax:

slAEnumKey("RegKey")

Parameters:

RegKey - String, Required

A string that specifies the name of the subkey you want to enumerate from

ReturnValue:

A single dimensional array containing one level of key names.

slAEnumValue

Enumerates registry value names into a single dimensional array.

Description:

Enumerates registry value names into a single dimensional array.

Syntax:

slAEnumValue("RegKey")

Parameters:

RegKey - String, Required

A string that specifies the name of the subkey you want to enumerate the values from.

ReturnValue:

A single dimensional array containing one level of value names.

slAlert

Generates alerts (pop-up messages / event log entries) to one or more destinations.

Description:

Generates alerts (pop-up messages / event log entries) to one or more destinations.

Remarks:

The SMTP e-mail (ToVal=16) is only supported with version 5.5 and newer.

Syntax:

slAlert("Type", "Title", "Text", Timeout, ToVal, "ToDestMsg", "ToDestLog", "ToDestEmail")

Parameters:

Type - String, Required

Type of messagebox to be displayed. Possible single-character types are:

"?"	Question
"i"	Informational
"!"	Warning
"X"	Error

Title - String, Required

Title of messagebox to be displayed (only applies to client message boxes).

Text - String, Required

Text included in the message/event.

Timeout - Integer, Optional

Timeout of the messagebox (only applies to client message boxes). If 0, there will be no timeout -- the user must press a button to continue.

ToVal - Integer, Optional

An integer representing one or more destinations

1	Display a pop-up message to the user logging on
2	Display a pop-up message to specific user(s) and/or computer(s)
4	Write this alert to the client computer's event log
8	Write this alert to the event log on one or more specific computers
16	E-mail this alert to specific address(es)

A combination of destinations can be used by passing the sum of all required destinations.

Example, to display a message to the user and send an email, use a value of 17

ToDestMsg - String, Optional

A string containing one or more destinations (NT-family computers), separated by semicolons {;}, to be used when the $ToVal destination will display a pop-up message to specific user(s) and/or computer(s)

ToDestLog - String, Optional

A string containing one or more destinations (NT-family computers), separated by semicolons {;}, to be used when the $ToVal destination will write an alert to the event log on one or more specific computers.

ToDestEmail - String, Optional

A string containing one or more SMTP E-mail address destinations, separated by semicolons {;}, to mail the alert to.

NOTE: you must use "@@" in place of a single "@" character within the e-mail address.

ReturnValue:

If the Type is ' ? ', this function returns a value of 6 for the Yes button and 7 for the No button. For all other types, this function returns nothing {0}.

slASort

Sorts the elements of an array.

Description:

Sorts the elements of an array.

Syntax:

slASort(array,[order])

Parameters:

Array - Array, Required

The array to perform the operation on.

Order - Boolean, Optional

0	ascending (default)
1	descending

ReturnValue:

An array or ordered elements.

slBinaryIP

Converts a dotted decimal IP address to binary string.

Description:

Converts a dotted decimal IP address to binary string.

Syntax:

slBinaryIP(IPaddr)

Parameters:

IPaddr - String, Required

IP address in dotted decimal form that you want to convert.

ReturnValue:

A string representing the IP address in binary form.

slCancelButton

Controls the behavior of the [Cancel] button of the active window.

Description:

Controls the behavior of the [Cancel] button of the active window.

Remarks:

Useful for some 'not so silent' unattended installations.

Syntax:

slCancelButton(Control)

Parameters:

Control - String, Required

Specifying "Hide" or "Disable" will deactivate the ability to press the Cancel button of the active Window.

Specifying "Show" or "Enable" will return the Cancel button to normal operation.

ReturnValue:

Nothing.

slClientAutoStartExplorer
Controls the SL/DA client service's built-in ability to auto-start Explorer upon initialization.

Description:

Controls the SL/DA client service's built-in ability to auto-start Explorer upon initialization.

Remarks:

The purpose of auto-starting a hidden instance of Explorer is to perform automatic completion of two-phase software installations, such as Internet Explorer upgrades.

Syntax:

slClientAutoStartExplorer(Control)

Parameters:

Control - String, Required

0	do not launch explorer when the SLclient service starts up
1	auto-start* explorer each and every time the SLclient service starts up
10	auto-start explorer the next time the SLclient service starts up (after that, revert back to 0)
20	force explorer to start the next time the SLclient service starts up (after that, revert back to 0)
21	force explorer to start the next time the SLclient service starts up (after that, revert back to 1)
*	"Auto-start" will trigger if more values/subkeys are found within HKLM\...\RunOnce or \RunOnceEx keys upon service startup.

slCnvtBase
Generalized base conversion

Description:

Generalized base conversion

Syntax:

slCnvtBase(number or array,oldbase,newbase,[NoHex])

Parameters:

Number or Array - Integer, Required

number (base 2-16 only) or array of digits w/MSD in element 0

oldbase - Integer, Required

integer specifying the base of the supplied number

newbase - Integer, Required

integer specifying the base to convert that number to

NoHex - Boolean, Optional

boolean true to use only characters 0-9 for return values

ForceSep - Boolean, Optional

boolean true to always separate digits with colons

ReturnValue:

A string. If highest digit > 9 (or F if HEX allowed), or ForceSep is true, the digits will be delimited with colons

slCompareIP

Compares two IP addresses to determine if they exist on the same network.

Description:

Compares two IP addresses to determine if they exist on the same network.

Syntax:

slCompareIP($IP1,$IP2,$BitMask)

Parameters:

IP1 - String Required

First IP address to compare

IP2 - String Required

Second IP address to compare

BitMask - Integer Required

BitMask to use in comparison

The subnet mask can be specified in either dotted decimal format or by specifying the number of mask bits. Example: 255.255.255.0 or 24

ReturnValue:

1	IP addresses exist on the same network.
0	IP addresses Do Not exist on the same network.

slComputerInGroup

Determine if the local computer is in a specific group

Description:

Determine if the local computer is in a specific group

Syntax:

slComputerInGroup($group, optional $DomainName)

Parameters:

group - String, Required

Name of group to check

DomainName - String, Optional

Name of the Domain that the group resides in.

ReturnValue:

1	Local computer is a member of group specified
0	Local computer is not a member of group specified

slCreateGUID

Create GUID

Description:

Create GUID

Syntax:

$NewGuid = slCreateGUID()

ReturnValue:

Returns a globally unique identifier

slCreateUniqueFile

Create Unique File)

Description:

Create Unique File

Syntax:

$RC = slCreateUniqueFile($Folder, $Extension)

Parameters:

Folder - String, Optional

Folder to create file in. Defaults to %TEMP%

Extension - String, Optional

Extension to use. Defaults to '.tmp'

ReturnValue:

Filespec of created file or empty string if no file was created.

slDebug

Write to the trace file

Description:

Write to the trace file

Remarks:

Writes a string to the sltrace.htm file.

Syntax:

slDebug($LogText, $FontColor)

Parameters:

LogText - String, Optional

String to write to trace file.

FontColor - String, Optional

Font color to use

slEndScript

Terminates the execution of Desktop Authority.

Description:

Terminates the execution of Desktop Authority.

Syntax:

slEndScript(NoExit)

Parameters:

NoExit - Integer, Optional

If specified as a positive integer, will instruct this function to perform all necessary clean-up procedures, but will not actually terminate Desktop Authority. This can be useful with performing a software installation, where the installation itself will perform a reboot upon completion.

ReturnValue:

Nothing.

Examples:

```
; Do not run SL on a specific computer.
```

```
; For use in a pre-engine custom script.
if @Wksta=' SpecialComputer '
$rc=slEndScript()
endif
```

slExec

Executes an application, batch or command file.

Description:

Executes an application, batch or command file.

Remarks:

Extremely powerful and versatile function for use in Custom Scripts.

Syntax:

slExec("program", "program arguments", "function flags")

Parameters:

Program - String, Required

Complete filespec of the Program, batch or command file to execute.

Program Arguments - String, Optional

Optional: Any command line arguments that need to be passed to the Program.

Function Flags - String, Required

Optional: Function Flags control when and how the Program is executed. There are (4) sets of flags that may be used. Choose (1) flag from each set and combine them into a single text string as the third parameter of this function. If the function flag from a given set is not supplied, the default (represented in the table below by an asterisk {*}) will be used. If no function flags are supplied, the program will be executed asynchronously; after the desktop loads; under the current user's security context, and visible. User* Admin Security context when launching the program. User = execute the program as the user logging on. Admin = execute the program with Administrative rights on the local computer. Visible* Hidden Hidden will mask all windows and output generated by the program. This is especially useful when executing console applications, batch or CMD files. During After* Logoff Shutdown When to execute the program: During the logon process, After the logon process completes.

ReturnValue:

Returns any error code generated by launching the program.

Examples:

```
; Custom Script to update recovery information
; on NT4/2000/XP systems, the first Wednesday of each month at logoff.
;
if @INWIN=1 and @Day='Wednesday' AND @MDAYNO<8
if $OS='NT' and $NtOsVerMajor=4 ; NT 4.0
$rc=slExec('rdisk','/S-','Admin Hidden Logoff')
else
; command line switches for ntbackup are documented in MSKB#Q300439
$rc=slExec('ntbackup','backup systemstate /f "$SystemDrive\SysState.bkf"','Admin Hidden Logoff')
endif
endif
```

slFileTimeCompare

Compare File Times

Description:

Compare File Times

Syntax:

slFileTimeCompare($File1, $Comparison, $File2, $Variance)

Parameters:

File1 - String, Required

File Name (including path) of first file

Comparison - String, Required

can be: '<', '<=', '=', '>=', '>', '<>'

File2 - String, Required

File Name (including path) of second file

Variance - String, Optional

Examples:

s3 = a three Second leniency

n5 = a five miNute leniency

h1 = a one Hour leniency

ReturnValue:

-3 = Neither file exists

-2 = $File2 does not exist

-1 = $File1 does not exist

0 = The expression is False

1 = The expression is True

slGetDefaultPrinter

Get Default Printer

Description:

Get Default Printer

Syntax:

$DP = slGetDefaultPrinter()

ReturnValue:

Name of clients default printer

slGetDriveList

List of drives

Description:

List of drives

Syntax:

$Drives = slGetDriveList()

ReturnValue:

returns a list of drives that the computer has

1 Removable

2 Fixed

3 CD/dvd

4 RamDisk

5 Networked drive

slGetDriveMap

The network resource name of the mapped drive or an empty string if not mapped

Description:

returns the network resource name of the mapped drive or an empty string if not mapped.

Syntax:

$UNC = slGetDriveMap('f')

Parameters:

$DriveLetter - String, Required

Mapped drive letter

ReturnValue:

Returns the network resource name of the mapped drive or an empty string if not mapped.

slGetFileExt

The file extension of a given file name

Description:

Returns the file extension of a given file name

Syntax:

$Ext = slGetFileExt('C:\boot.ini')

Parameters:

FileName - String, Required

Name of file

ReturnValue:

Returns the file extension of a given file name

slGetFileName

The filename from a complete path

Description:

Returns filename from a complete path

Syntax:

slGetFileName('FullPath')

Parameters:

FileSpec - String, Required

Complete path of file

ReturnValue:

Returns filename from a complete path

Examples:

$FileName = slGetFileName('c:\winnt\system32\kernel32.dll)

slGetFilePath

Extracts the path-only portion of a complete filespec

Description:

Extracts the path-only portion of a complete filespec

Syntax:

slGetFilePath('filespec')

Parameters:

FileSpec - String, Required

Full path of a file

ReturnValue:

Path-only portion of a complete filespec

slGetProcessID

Get process ID of specified process

Description:

Get process ID of specified process

Syntax:

slGetProcessID(ProcessName)

Parameters:

$ProcessName - String, Required

Process name to query

ReturnValue:

Returns the PID of the specified process, zero if not found

slGetProcessList

Get a list of all running processes

Description:

Get a list of all running processes

Syntax:

slGetProcessList(1)

Parameters:

$AllUsers - Boolean, Optional

Returns processes for all users rather the current user

ReturnValue:

Returns an array of all running processes for the current user (or all users if $AllUsers=1).

slGetSoftwareList

Get a list of software installed

Description:

Get a list of software installed

Syntax:

slGetSoftwareList(1)

Parameters:

$Sort - Boolean, Required

1 = return in sorted order

ReturnValue:

Returns an array of software currently installed (sorted if $Sort=1)

slIniEdit

Manipulate INI files

Description:

Manipulate INI files

Parameters:

$Action - String, Required

Possible Actions:

"Del" - Delete

"Write" - Write

$FileSpec - String, Required

Complete file path to INI

$Section - String, Required

Section name you wish to modify

$Value - String, Optional

Value name you wish to modify

$Data - String, Optional

The Data you wish to set to a given $Value

ReturnValue:

An error code if an error was encountered

slKillProcess

Kill a process

Description:

Kill a process

Syntax:

slKillProcess(ProcessName)

Parameters:

$ProcessNameOrID - String, Required

can be process name (string) or a process ID (int)

ReturnValue:

Returns 0 on success or a system error code on failure

slLogoff

Logoff the user

Description:

Logoff the user

Syntax:

$rc= slLogoff()

Parameters:

NoAlert - Integer, Optional

Suppress the alert associated with logoff.

ReturnValue:

0 = Success

or an error code

slMakeDir

Creates a folder (directory) and/or complete folder structure on disk.

Description:

Creates a folder (directory) and/or complete folder structure on disk.

Remarks:

Can be used to create folders on the local computer, mapped network path or UNC network path to a remote computer. When used to create a folder on the local computer, this function can overcome NTFS security restrictions (on the local computer) that

Syntax:

slMakeDir("Folder")

Parameters:

Folder - String, Required

Complete path of the folder to create.

ReturnValue:

Any error associated with performing the action. A return code of 0 (zero) indicates success.

Examples:

```
$rc=slMakeDir('%WinDir%\Web\Wallpaper')
$rc=slMakeDir('H:\Documents\Word\Backup')
$rc=slMakeDir('\\Server1\Users\'+$UserID+'\Docs')
```

slOccurs

Determine the number of times a string exists within a string or an array

Description:

Determine the number of times a string exists within a string or an array

Syntax:

$RC = slOccurs("abcabcabc","ab")

Parameters:

$ExpC1 - String, Required

a text string, array element or entire array to search

$Expc2 - String, Required

an expression we are attempting to find within the string or the elements of the array.

ReturnValue:

The total number of occurrences that $ExpC2 was found, or 0 if not found anywhere within the elements of the array.

slOrdinal

The ordinal string of a given number in string form

Description:

Returns the ordinal string of a given number in string form

Syntax:

slOrdinal("13")

Parameters:

$Expr - Integer, Required

Integer from which to generate the returned ordinal string.

ReturnValue:

returns the ordinal string of a given number in string form

Examples:

1=1st, 2=2nd, 3=3rd, 4=4th ... 110th

slPathCompare

Compare two paths

Description:

Compare two paths

Remarks:

Useful when you are given a mapped drive and a URL, or two shares that point to same physical path

Syntax:

$rc = slPathCompare("L:\Login","\\Server1\Logs\Login")

Parameters:

$Path1 - String, Required

First path to compare (local, mapped or UNC)

$Path2 - String, Required

Second path to compare (local, mapped or UNC)

ReturnValue:

1 if paths are same

0 if paths are different

slPathIsLocal

Determine if a path is local or mapped.

Description:

Determine if a path is local or mapped.

Parameters:

$Path - String, Required

Path to check

ReturnValue:

1 - If path resides on a local drive

0 - If path does not reside on a local drive

slPing

Ping a machine by Name or IP address

Description:

Ping a machine by Name or IP address

Syntax:

$rc = slPing("10.0.0.1")

Parameters:

$Host - String, Required

Machine name or IP address to ping

ReturnValue:

Returns the classic ping string or an empty string if other than successful.

slPlayWav

Play a wav file

Description:

Play a wav file

Syntax:

$rc = slPlayWav($Netlogon+"\GoodMorning.wav",1)

Parameters:

$Filespec - String, Required

File spec of wav file to play

$Sync - Integer, Required

0 - Runs aSynchronous

1 - Runs Synchronous

ReturnValue:

Returns 0 on success or a system error code on failure

slQueryHotFix

Query installed Hotfixes

Description:

Query installed Hotfixes

Remarks:

This function is only supported on the NT-family of products (NT4/2000/XP/etc.)

Syntax:

slQueryHotFix(OPTIONAL $HotFix, OPTIONAL $BCP)

Parameters:

$Hotfix - String, Optional

a specific hotfix to test for

ReturnValue:

If parameter is omitted, a string of all installed hotfixes is returned.

Alternatively, Parameter can be the name of a specific hotfix to test for

If the hotfix is installed, this function returns a numeric 1.

If the hotfix is not installed, this function returns a numeric 0.

slQueryIEHotFix

Query installed Internet Explorer hotfixes

Description:

Query installed Internet Explorer hotfixes

Syntax:

$rc = slQueryIEHotFix()

Parameters:

$HotFix - String, Required

Hotfix number to query

ReturnValue:

If parameter is omitted, a string of all installed IE hotfixes is returned.

Alternatively, Parameter can be the name of a specific IE hotfix to test for:

If the IE hotfix is installed, this function returns a numeric 1.

If the IE hotfix is not installed, this function returns a numeric 0.

slRegAddKey

Creates a registry key.

Description:

Creates a registry key.

Remarks:

The syntax and parameters are similar to KiXtart's built-in AddKey( ) function, with the following exceptions: A [sub]key can be created under any hive and/or key -- regardless of whether or not the user logging on has the privilege to add it.

Syntax:

slRegAddKey("hive\key")

Parameters:

Hive\Key - String, Required

Identifies the hive and [sub]key where you want to create the new key. When specifying the hive, you may use its 'short' or 'long' name: short long HKCU HKEY_CURRENT_USER HKDU HKEY_USERS\.DEFAULT HKLM HKEY_LOCAL_MACHINE HKCR HKEY_LOCAL_MACHINE\Software\Classes (a.k.a. HKEY_CLASSES_ROOT)

ReturnValue:

Any error associated with performing the action. A return code of 0 (zero) indicates success.

Examples:

$rc=slRegAddKey('HKLM\Software\MyKey')

slRegDelKey

Deletes a registry key.

Description:

Deletes a registry key.

Remarks:

A [sub]key can be deleted under any hive and/or key -- regardless of whether or not the user logging on has the privilege to delete it. If the key you are attempting to delete has subkeys beneath it, this function will fail and the keys will not be del

Syntax:

slRegDelKey("hive\key")

Parameters:

Hive\Key - String, Required

Identifies the hive and [sub]key where you want to delete the key. When specifying the hive, you may use its 'short' or 'long' name: short long HKCU HKEY_CURRENT_USER HKDU HKEY_USERS\.DEFAULT HKLM HKEY_LOCAL_MACHINE HKCR HKEY_LOCAL_MACHINE\Software\Classes (a.k.a. HKEY_CLASSES_ROOT)

ReturnValue:

Any error associated with performing the action. A return code of 0 (zero) indicates success.

Examples:

```
$rc=slRegDelKey($HKLM+'\Software\MyKey')
```

slRegDelTree

Deletes a registry key, including all subkeys.

Description:

Deletes a registry key, including all subkeys.

Remarks:

The keys can be deleted under any hive and/or key. This function should be used with extreme caution!

Syntax:

slRegDelTree("hive\key")

Parameters:

Hive\Key - String, Required

Identifies the hive and [sub]key where you want to delete the key. When specifying the hive, you may use its 'short' or 'long' name:

Short Long

HKCU HKEY_CURRENT_USER

HKDU HKEY_USERS\.DEFAULT

HKLM HKEY_LOCAL_MACHINE

HKCR HKEY_LOCAL_MACHINE\Software\Classes (a.k.a. HKEY_CLASSES_ROOT)

ReturnValue:

Any error associated with performing the action. A return code of 0 (zero) indicates success.

Examples:

$rc=slRegDelTree('HKLM\Software\America Online')

$rc=slRegDelTree('HKCU\Software\America Online')

slRegDelVal

Deletes a registry value.

Description:

Deletes a registry value.

Remarks:

The syntax and parameters are similar to KiXtart's built-in DelValue( ) function, with the following exceptions: Any value within any key can be deleted -- regardless of whether or not the user logging on has the privilege to delete it. To delete

Syntax:

slRegDelVal("hive\key", "value")

Parameters:

Hive\Key - String, Required

Identifies the hive and [sub]key where you want to delete the value.

When specifying the hive, you may use its 'short' or 'long' name:

short long

HKCU HKEY_CURRENT_USER

HKDU HKEY_USERS\.DEFAULT

HKLM HKEY_LOCAL_MACHINE

HKCR HKEY_LOCAL_MACHINE\Software\Classes

(a.k.a. HKEY_CLASSES_ROOT)

Value - String, Required

The name of the entry. To delete the default value of a key, specify "(default)".

ReturnValue:

Any error associated with performing the action. A return code of 0 (zero) indicates success.

Examples:

```
; Remove the "Copy To" context menu option:
$rc=slRegDelVal($HKCR+'\AllFileSystemObjects\shellex\ContextMenuHandlers\Copy To','
(default)')
```

slRegedit

A multipurpose function that handles all aspects of the registry.

Description:

A multipurpose function that handles all aspects of the registry.

Syntax:

slRegEdit(Action, Regkey, RegVal, RegExp, RegType, NoDebug)

Parameters:

Action - String, Required

Action to perform on registry. Possible values are:

AddKey

DeleteTree (Should be used with extreme caution!)

DeleteKey

DeleteValue

WriteValue

RegKey - String, Required

Identifies the hive and [sub]key where you want to perform action.

When specifying the hive, you may use its 'short' or 'long' name:

[Short] [Long]

HKCU HKEY_CURRENT_USER

HKDU HKEY_USERS\.DEFAULT

HKLM HKEY_LOCAL_MACHINE

HKCR HKEY_LOCAL_MACHINE\Software\Classes (a.k.a. HKEY_CLASSES_ROOT)

RegVal - String, Optional

The name of the value. To write/read the default value of a key, specify "(default)".

RegExp - String, Optional

The data to store to the value.

To write a blank or null string (effectively erasing the contents of the value), specify "(blank)".

To write a REG_MULTI_SZ data type, use the pipe symbol { | } to separate strings within the data. If the data contains the pipe symbol, represent it using double pipes { || }.

RegType - String, Optional

Type of expression to write.

Examples:

Reg_SZ

Reg_Expand_SZ

Reg_Multi_SZ

Reg_Binary

Reg_DWord

Reg_QWord

NoDebug - Boolean, Optional

0 - show entry in sltrace.htm

1 - do not show entry in sltrace.htm

ReturnValue:

Any error associated with performing the action. A return code of 0 (zero) indicates success.

Examples:

```
$RC = slRegedit("AddKey","HKLM\Software\Acme")
$RC = slRegedit("DeleteKey","HKLM\Software\Acme")
$RC = slRegedit("WriteValue","HKLM\Software\Acme","DataPath","C:\Acme\Data","Reg_SZ")
```

slRegReadValue

Read a registry value

Description:

Read a registry value

Remarks:

function slRegReadValue($RegKey,$RegVal)

$slRegReadValue=$SLcom.RegReadValue($RegKey,$RegVal)

endfunction

Syntax:

slRegReadValue(RegKey,RegVal)

Parameters:

$RegKey - String, Required

Key to read

$RegVal - String, Required

Value to read

ReturnValue:

Data of specified Value

slRegWriteVal

Assigns or changes a registry value.

Description:

Assigns or changes a registry value.

Remarks:

The syntax and parameters are similar to KiXtart's built-in WriteValue( ) function, with the following exceptions: The data of any value within any key can be changed -- regardless of whether or not the user logging on has the privilege to change it.

Syntax:

slRegWriteVal("hive\key", "value", "data", "data type")

Parameters:

Hive\Key - String, Required

Identifies the hive and [sub]key where you want to write the value. When specifying the hive, you may use its 'short' or 'long' name: short long HKCU HKEY_CURRENT_USER HKDU HKEY_USERS\.DEFAULT HKLM HKEY_ LOCAL_MACHINE HKCR HKEY_LOCAL_MACHINE\Software\Classes (a.k.a. HKEY_CLASSES_ROOT)

Value - String, Required

The name of the entry. To write to the default value of a key, specify "(default)".

Data - String, Required

The data to store to the value. To write a blank or null string (effectively erasing the contents of the value), specify " (blank)". To write a REG_MULTI_SZ data type, use the pipe symbol { | } to separate strings within the data. If the data contains the pipe symbol, represent it using double pipes { || }.

Data Type - String, Required

Identifies the data type of the entry. The following data types are supported: REG_NONE REG_SZ REG_EXPAND_ SZ REG_BINARY REG_DWORD REG_DWORD_LITTLE_ENDIAN REG_DWORD_BIG_ENDIAN REG_LINK REG_MULTI_SZ REG_RESOURCE_LIST REG_FULL_RESOURCE_DESCRIPTOR

ReturnValue:

Any error associated with performing the action. A return code of 0 (zero) indicates success.

Examples:

; change desktop background color at logon to Windows 2000 blue:

$rc=slRegWriteVal('HKDU\Control Panel\Colors','Background','58 110 165','REG_SZ')

; Create a "Copy To" context menu option:

$rc=slRegWriteVal('HKCR\AllFileSystemObjects\shellex\ContextMenuHandlers\Copy To','(default)','{c2fbb630-2971-11d1-a18c-00c04fd75d13}','REG_SZ')

slReplace

replaces a specified substring within a specified string with a new specified substring and returns the modified string

Description:

Replaces a specified substring within a specified string with a new specified substring and returns the modified string

Parameters:

String - String, Required

The string to be searched.

OldStr - String, Required

The substring you are searching for inside the string

NewStr - String, Optional

The new substring string that you wish to insert inside the string

ReturnValue:

Returns the modified string

slRestart

Logs the current user off -or- reboots the computer.

Description:

Logs the current user off -or- reboots the computer.

Remarks:

The reboot option is not allowed on servers or domain controllers.

Syntax:

slRestart(Option, NoAlert)

Parameters:

Option - Integer, Required

A numeric value of 1 or the text "Logoff" will logoff the current user. A numeric value of 2 or the text "Reboot" will reboot the computer.

NoAlert - Integer, Optional

Optional: A value of 1 will inhibit the standard Alert (messagebox, eventlog, or message) defined in the Desktop Authority Manager \ Profile Options \ Alerts screen associated with the logging off or rebooting of the computer.

ReturnValue:

Nothing.

Examples:

$rc=slRestart("Logoff",1)

slSendMail

Send an email

Description:

Send an email

Syntax:

slSendMail("SMTPServer", "SenderAddress", "RecipientAddress", "Subject", "Body")

Parameters:

SMTPServer - String, Required

SMTP server name to use

Sender - String, Required

A string containing an SMTP E-mail address of the sender.

NOTE: you must use "@@" in place of a single "@" character within the e-mail address.

Recipient - String, Required

A string containing one or more SMTP E-mail address destinations, separated by semicolons {;}

NOTE: you must use "@@" in place of a single "@" character within the e-mail address.

Subject - String, Required

A string containing the subject of the email.

Body - String, Required

A string containing the body of the email.

FileAttachment - String, Optional

A string containing the full path of to the file to attach to email.

RecipientCC - String, Optional

A string containing one or more SMTP E-mail address destinations to Carbon Copied, separated by semicolons {;}

NOTE: you must use "@@" in place of a single "@" character within the e-mail address.

RecipientBCC - String, Optional

A string containing one or more SMTP E-mail address destinations to blind carbon copy, separated by semicolons {;}

NOTE: you must use "@@" in place of a single "@" character within the e-mail address.

ReturnValue:

Returns a system return code. A return code of 0 indicates success.

slSerialDateTime

Serialize Date Time to perform simple math functions.

Description:

Serialize Date Time to perform simple math functions.

Remarks:

Integers can be used for general-purpose math computations on dates

Syntax:

slSerialDateTime($Exp)

Parameters:

$exp - String, Required

Must be a date (in the form of yyyy/mm/dd) or an integer previously derived by this function.

ReturnValue:

If passed a date, it returns an integer.

If passed an integer, it returns the date.

slSetGraphic

Changes the display state of the customer-supplied logon graphic.

Description:

Changes the display state of the customer-supplied logon graphic.

Remarks:

This function was designed for custom scripting, where a software deployment may not be completely scriptable in quite-mode. When Desktop Authority displays the customer-supplied logo, it is displayed "always on top." This could interfere with certain software

Syntax:

slSetGraphic("mode")

Parameters:

Mode - String, Required

String that specifies the new display state. There are two modes: "Hide" - Stop displaying the graphic. "Show" - Redisplay the graphic.

ReturnValue:

Nothing.

Examples:

```
$rc=slSetGraphic(' Hide ')
$rc=slSetGraphic(' Show ')
```

slSetM

Set local machine environment variables

Description:

Set local machine environment variables

Syntax:

$rc = slSetM("MyVar=Hello")

Parameters:

Definition - String, Required

Definition to set

ReturnValue:

Returns standard windows return code

slSetServiceStartup

Configure service startup

Description:

Configure service startup

Syntax:

slSetServiceStartup($shortname, $startup)

Parameters:

$shortname - String, Required

The short name of the service (same as the registry key)

$startup - Integer, Required

How to configure the service:

0 - Boot

1 - System

2 - Automatic

3 - Manual

4 - Disabled

slSetShellVars

Re-defines all Desktop Authority global dynamic variables relating to the location of Windows shell folders.

Description:

Re-defines all Desktop Authority global dynamic variables relating to the location of Windows shell folders.

Remarks:

When Desktop Authority initializes, global dynamic variables are defined. These variables point to the location of the various Windows shell folders

Syntax:

SlSetShellVars( )

Parameters:

New* - Variant, Required

ReturnValue:

Nothing.

Examples:

```
? 'Current user desktop folder: '+$ShellDesktop
$=writevalue('HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders','Desktop','H:\Desktop','REG_SZ')
$=slSetShellVars()
? 'new location of user desktop folder: '+$ShellDesktop
```

slShortcut

Creates or removes shortcuts.

Description:

Creates or removes shortcuts.

Remarks:

Like most Desktop Authority API functions, this function overcomes the normal user's NTFS security restrictions on the local machine - i.e. shortcuts can be created in any folder on the computer they are logging on to.

Syntax:

slShortcut("Action", "Folder", "Name", "Target", "Arguments", "StartIn", "Key", "RunWindow", "Comment", "IconFile", "IconIndex")

Parameters:

Action - String, Required

Create or Remove the shortcut. Only the first character is evaluated. Use the following table: Add Create Specifying "A", "Add", "C" or "Create" will create a shortcut. If a shortcut by the same name already exists, it will not be overwritten (the new shortcut will not be created). Overwrite Specifying "O" or "Overwrite" will create a shortcut, and will overwrite if necessary, any existing shortcut by the same name. Delete Remove Specifying "D", "Delete", "R" or "Remove" will delete an existing shortcut.

Folder - String, Required

The folder where the shortcut will be created. You can specify the folder as a static string, use a dynamic variable, or combine both. Desktop Authority will automatically create the folder if necessary.

Filename - String, Required

The name of the shortcut. It is not necessary to specify the extension, as this function will automatically assign the proper extension (lnk, pif, url, scf) when the shortcut is created.

Target - String, Optional

The name of the item (program, folder, URL, etc.) that the shortcut will launch. If the shortcut points to an executable file, and the file is not within the Windows search path, the full path to the file should be included, or the folder where the file resides should be specified in the StartIn field.

NOTE: this field is required when creating shortcuts, however, it is not used when removing shortcuts.

Arguments - String, Optional

The command-line parameters that should be passed to the Target application.

StartIn - String Optional

Specifies the folder that contains the original item or some related files. Sometimes, programs need to use files from other locations. You might need to specify the folder where these files are located so that the program can find them.

Key - String Optional

Specifies the keyboard shortcut that you want press to start or switch to a program. Shortcut keys automatically include CTRL+ALT. You cannot use ESC, ENTER, TAB, the SPACEBAR, PRINT SCREEN, DELETE or BACKSPACE.

RunWindow - String, Optional

Specifies how you want the window to display this item when you open the shortcut: in a standard window, in a full screen ("maximized"), or as a button on the taskbar ("minimized").

Comment - String, Optional

Displays the text description for this shortcut. For desktop shortcuts, the comment will appear in a box when you hover your mouse cursor over the shortcut.

IconFile - String, Optional

Specifies the name of the file that contains the icon for this shortcut. If not specified, the icon embedded within the Target application will be used.

IconIndex - String, Optional

Some files contain more than one icon, and this field allows you to select which icon from the application or icon library will be used. If this field is not specified, the first icon (location 0) will be used.

ReturnValue:

Nothing.

Examples:

```
$rc=slShortcut('Create', $ShellDesktop, 'My Stuff', 'Explorer.exe', '/e, /n, H:\Documents', '', '',
'Personal documents')
```

slShortcut

Creates or removes shortcuts.

Description:

Creates or removes shortcuts.

Remarks:

Like most API functions, this function overcomes the normal user's NTFS security restrictions on the local machine - i.e. shortcuts can be created in any folder on the computer they are logging on to.

Syntax:

slShortcut("Action", "Folder", "Name", "Target", "Arguments", "StartIn", "Key", "RunWindow", "Comment", "IconFile", "IconIndex")

Parameters:

Action - String, Required

Create or Remove the shortcut. Only the first character is evaluated. Use the following table: Add Create Specifying "A", "Add", "C" or "Create" will create a shortcut. If a shortcut by the same name already exists, it will not be

overwritten (the new shortcut will not be created). Overwrite Specifying "O" or "Overwrite" will create a shortcut, and will overwrite if necessary, any existing shortcut by the same name. Delete Remove Specifying "D", "Delete", "R" or "Remove" will delete an existing shortcut.

Folder - String, Required

The folder where the shortcut will be created. You can specify the folder as a static string, use a dynamic variable, or combine both. Desktop Authority will automatically create the folder if necessary.

Filename - String, Required

The name of the shortcut. It is not necessary to specify the extension, as this function will automatically assign the proper extension (lnk, pif, url, scf) when the shortcut is created.

Target (optional) - String, Optional

The name of the item (program, folder, URL, etc.) that the shortcut will launch. If the shortcut points to an executable file, and the file is not within the Windows search path, the full path to the file should be included, or the folder where the file resides should be specified in the StartIn field.

NOTE: this field is required when creating shortcuts, however, it is not used when removing shortcuts.

Arguments - String, Optional

The command-line parameters that should be passed to the Target application.

StartIn - String, Optional

Specifies the folder that contains the original item or some related files. Sometimes, programs need to use files from other locations. You might need to specify the folder where these files are located so that the program can find them.

Key - String, Optional

Specifies the keyboard shortcut that you want press to start or switch to a program. Shortcut keys automatically include CTRL+ALT. You cannot use ESC, ENTER, TAB, the SPACEBAR, PRINT SCREEN, DELETE or BACKSPACE.

RunWindow - String, Optional

Specifies how you want the window to display this item when you open the shortcut: in a standard window, in a full screen ("maximized"), or as a button on the taskbar ("minimized").

Comment - String, Optional

Displays the text description for this shortcut. For desktop shortcuts, the comment will appear in a box when you hover your mouse cursor over the shortcut.

IconFile - String, Optional

Specifies the name of the file that contains the icon for this shortcut. If not specified, the icon embedded within the Target application will be used.

IconIndex - String, Optional

Some files contain more than one icon, and this field allows you to select which icon from the application or icon library will be used. If this field is not specified, the first icon (location 0) will be used.

ReturnValue:

Nothing.

Examples:

$rc=slShortcut('Create', $ShellDesktop, 'My Stuff', 'Explorer.exe', '/e, /n, H:\Documents', '', '', 'Personal documents')

slStartButton

Hide/Show the Start Button

Description:

Hide/Show the Start Button

Syntax:

slStartButton($Control)

Parameters:

$Control - String, Required

"Hide" - Hides the start button

"Show" - Shows the start button

"Remove" - Removes the start button (Remove is permanent unless Explorer restarted)

ReturnValue:

a windows return code

slTimeSync

Synchronizes the system clock of the local computer with the system clock of the specified server.

Description:

Synchronizes the system clock of the local computer with the system clock of the specified server.

Remarks:

Like most API functions, this function overcomes the normal user's security restrictions - the user does not need the "Change System Time" privilege on the local computer for this function to succeed. When synchronizing time with a Windows NT

Syntax:

slTimeSync("Server")

Parameters:

Server - String, Required

The server you wish to synchronize the client' s clock to, specified in UNC form.

ReturnValue:

Nothing.

Examples:

```
$rc=slTimeSync('\\MyServer')
$rc=slTimeSync('\\'+$LogonServer)
$rc=slTimeSync('\\192.168.100.11')
```

slVersionCompare

Compare version numbers

Description:

Compare version numbers

Remarks:

If either Ver1 or Ver2 is blank, then it will converted to '0.0.0.0'

Syntax:

$rc = slVersionCompare("4.0.1.1","<","5.1.0.0")

Parameters:

Ver1 - String, Required

First version string to compare

Comparison - String, Required

can be: '<', '<=', '=', '>=', '>', '<>'

Ver2 - String, Required

Second version string to compare

Limit - String, Optional

Limits the number of segments to perform comparison on

If omitted, all segments (up to 4) will be compared

ReturnValue:

1 - comparison evaluates true

0 - comparison evaluates false

'' - not all arguments were properly supplied

slWinFirewallClosePort

Close an open Windows Firewall port (Windows 7 or greater)

Description:

Close an open Windows Firewall port (Windows 7 or greater)

Syntax:

slWinFirewallClosePort(PortNumber, IPProtocol)

Parameters:

$PortNumber - Integer, Required

Port number to close

$IPProtocol - String, Required

Specify what protocol "TCP" or "UDP"

Examples:

```
$rc = slWinFirewallClosePort( 80, "TCP")
```

slWinFirewallEnable

Enables Windows Firewall (Windows 7 or greater)

Description:

Enables Windows Firewall (Windows 7 or greater)

Syntax:

slFirewallEnable(enable)

Parameters:

$enable - Boolean, Required

1= enable Windows Firewall

0= disable Windows Firewall

Examples:

```
$rc = slWinFirewallEnable(1)
$rc = slWinFirewallEnable(0)
```

slWinFirewallOpenPort

Opens a port in Windows Firewall (Windows 7 or greater)

Description:

Opens a port in Windows Firewall (Windows 7 or greater)

Syntax:

slWinFirewallOpenPort(Name, PortNumber, LanOnly, IPProtocol, OnlyIfFirewallEnabled)

Parameters:

$Name - String, Required

Name to assign to open port

$PortNumber - Integer, Required

Port number to open

$LanOnly - Boolean, Required

Specifies the scope of the port opening

1= LAN Only

0= Full Network

$IPProtocol - String, Required

Protocol

"TCP"

"UDP"

$OnlyIfFirewallEnabled - Boolean, Required

Opens specified port only if the Windows Firewall is enabled

Examples:

```
$rc = slWinFirewallOpenPort( "Http", 80, 1, "TCP",0)
```

slWMIQuery

Queries WMI information

Description:

Queries WMI information

Syntax:

slWMIQUery($What,$From,$Computer,$Where,$x)

Parameters:

$what - String, Required

What it is you wish to query

$from - String, Required

Win32 Collection

$computer - String, Optional

defaults to local PC

$where - String, Optional

additional parameter for a 'WHERE' clause. Used with $x

$x - String, Optional

additional parameter for a 'WHERE' clause. Used with $Where

ReturnValue:

Array or @error 1 = Cannot create COM object on target PC

Examples:

```
$make = WMIQuery("Manufacturer","Win32_ComputerSystem")[0]
$modem = WMIQuery("Description","Win32_POTSModem",$remotePC,"Status","OK")[0]
for each $stick in WMIQuery("Capacity","Win32_PhysicalMemory")
? val($stick) / 1048576
next
```

slWriteLine

Write ASCII data to log files (Uses the DA Administrative service)

Description:

Write ASCII data to log files (Uses the DA Administrative service)

Syntax:

$rc= slWriteLine(LogFileSpec, LogData)

Parameters:

LogFilespec - String, Required

The full UNC to the file to APPEND the data to

LogData - String, Required

The ASCII data you want appended to the file

FunctionFlags - String, Optional

can contain:

'Async' - Desktop Authority will not wait for the write operation to complete before continuing

'NoCrLf' - A CRLF will not be automatically appended to the data written

ReturnValue:

Nothing

Examples:

```
$rc= slWriteLine("\\Server\Shr\File.log","Hello world")
```

Desktop Authority for VPN Clients

When remote users login to their machines (using cached credentials) and establish a VPN connection to the network, Desktop Authority will not run. Desktop Authority can be configured to fire an event when a network connection (VPN) is established.

Desktop Authority uses Network Location Awareness to detect when a new network connection becomes available. Once the new connection is detected, Desktop Authority will be notified and can then determine whether it will execute for the user.

Configuration settings

Configuring Desktop Authority for VPN Clients requires a few simple registry settings.

> IMPORTANT: Always use caution when manipulating the registry on any computer. Changes made to the registry happen immediately, and no backup is automatically made. Make sure to back up or export the registry key or subkey before making your changes.

VPN Client configuration settings are made on the client machine to the following registry hive/key depending on the computer's architecture.

- 32-bit: HKEY_LOCAL_MACHINE\SOFTWARE\ScriptLogic
- 64-bit: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ScriptLogic

Enable Desktop Authority for VPN Clients

Purpose: Enables or disables the VPN Client feature in Desktop Authority.

Applies to: User Management, Computer Management

Value name: EnableNLA

Value type: REG_DWORD

Value data: 1 (Enable), 2 (Disable - Default)

Login script validation

Purpose: Desktop Authority for VPN Clients will verify that the user has been assigned SLogic or SLogic.bat as their logon script. Desktop Authority will validate and execute for any user that has SLogic or SLogic.bat configured as their logon script in Active Directory.

If the company implementation of Desktop Authority does not assign Slogic or Slogic.bat as their user's logon script, an alternate script name can be defined using the **NLAAltScript** value. The specified script is used to validate that the user logged into the computer is a Desktop Authority user.

> Note: Multiple alternate script file names may be specified. Delimit each file name with a comma.

Applies to: User Management, Computer Management

Value name: NLAAltScript

Value type: REG_SZ

Value data: The name of the alternate login script file

Examples:

Login.bat

Login.bat,Login,Slogic.bat,Slogic

Connection time interval

Purpose: Desktop Authority will execute when a new network connection is detected and the user's assigned logon script has been validated. If the connection is dropped and then reestablished within 30 minutes, the default, Desktop Authority will not execute again. In order to change the time interval, use the **NLAperiod** value.

Applies to: User Management, Computer Management

Value name: NLAperiod

Value type: REG_DWORD

Value data: 0 (No Restriction/Disabled), 1 - 86400 (in seconds, default -1800 seconds/30 minutes)

User Management event type

Purpose: When a new network connection is detected and the user's assigned logon script is validated, a Refresh event will be triggered. To override the event that occurs when Desktop Authority executes use the **NLAUBMEvent** value.

Applies to: User Management

Value name: NLAUBMEvent

Value type: REG_SZ

Value data: Logon or Refresh or Logoff (Default - Refresh)

> Note: If Logon is specified, the Desktop Authority client splash screen will be displayed. However, the client splash screen is not displayed during a Refresh or Logoff event.

Alternate script location

Purpose: When Desktop Authority is executed, the SLogic.bat file is executed from the NETLOGON shared folder, by default. To instruct Desktop Authority to look in a different location for Slogic.bat use the **NLAUBMLocation** value. The full UNC path must be entered.

Applies to: User Management

Value name: NLAUBMLocation

Value type: REG_SZ

Value data: path of the logon script (Default - %Logonserver%\Netlogon)

> Note: If the location of the login script is %Logonserver%\Netlogon, the default, then the NLAUBMLocation does not need to be specified.

Example:

%logonserver%\\Netlogon\DA

\\ServerName\FolderName\SubFolderName

Hide command prompt

Purpose: The main purpose of this registry setting is to allow for troubleshooting in the case where Desktop Authority is not being executed properly.

By default, when Desktop Authority is executed, the command prompt window for SLogic.bat will be hidden. To display the SLogic.bat command prompt window when Desktop Authority is executed, configure the **NLAShowWindow** value to 1.

Applies to: User Management

Value name: NLAShowWindow

Value type: REG_DWORD

Value data: 0 (Disable– Default), 1 (Enable)

Limit concurrent logons

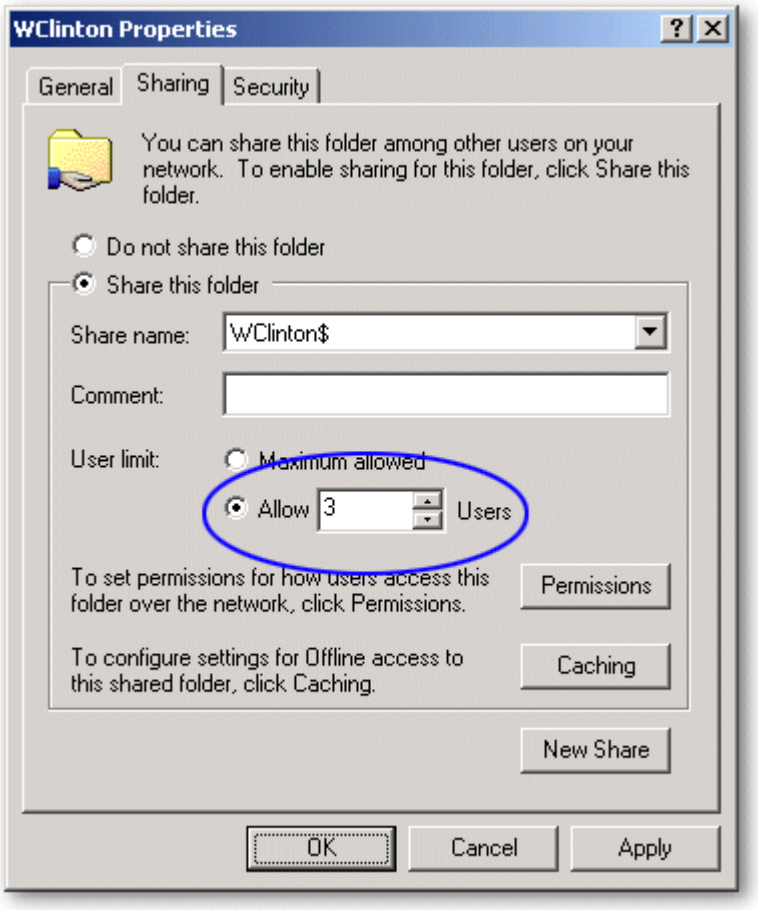
Since Desktop Authority executes during the logon process, which is before the user has control of their desktop, you have the ability to forcibly log off the user if you detect they have logged on too many times.

To Limit Concurrent Logons, you must:

- Share each user's home directory.
- Configure user logon maximums.

Since the Concurrent User Limit is applied individually to each user's share, you can configure your users to have different concurrent logon maximums while other users (such as Administrators) have no limit. This is done by setting the maximum number of connections in the properties dialog box for the share of the individual's user folder.

Figure 64: Set the maximum number of logons allowed by setting allowed user logons



Provide a drive mapping in Desktop Authority.

Using the Drive Mappings object within the Manager, map a drive to each user's Home Directory.

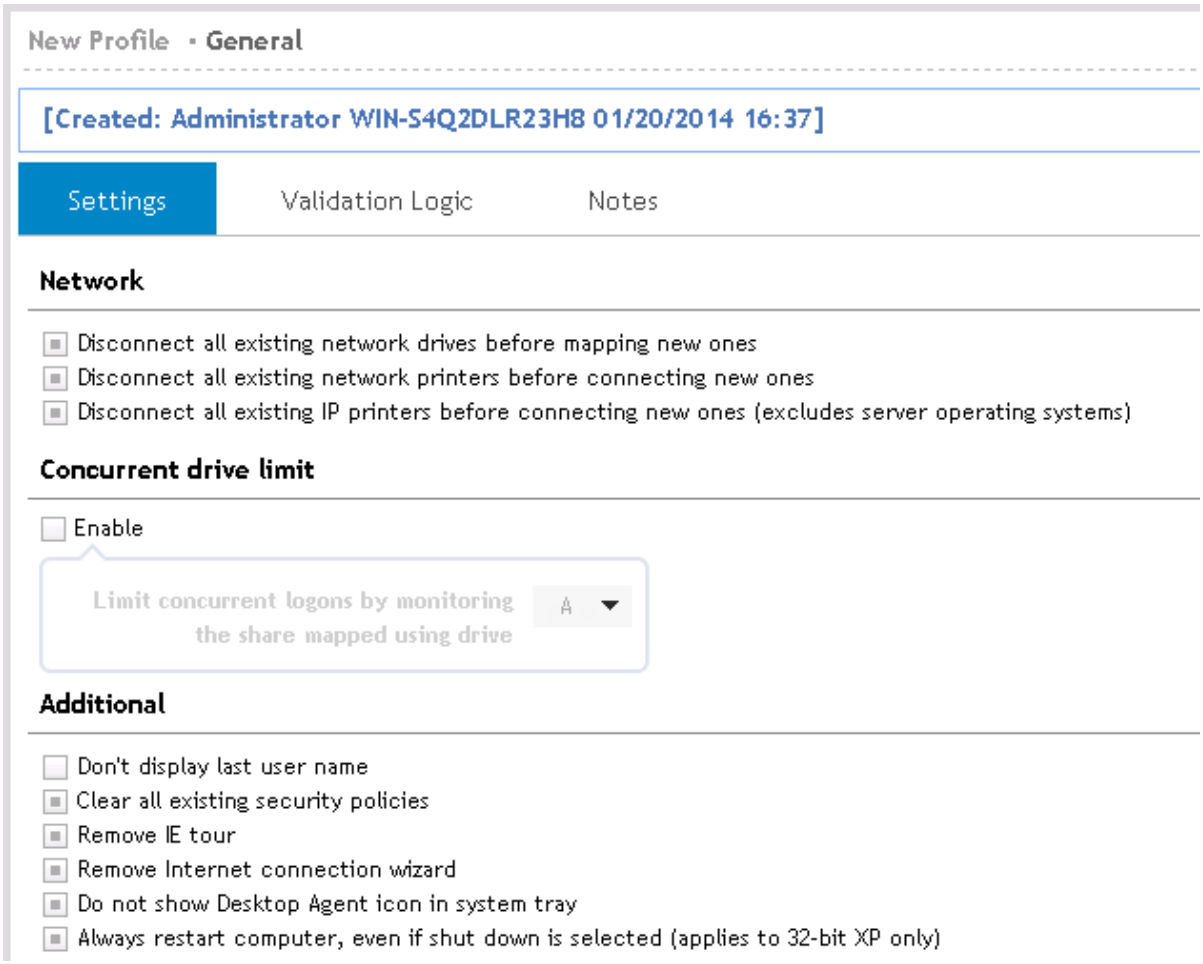
Example:

Map drive **H:** to the shared folder **\\$HomeServer\$HomeDir**

Set the concurrent logons limit.

Tell Desktop Authority what drive letter you are mapping to the user's share. Do this by selecting the **Limit concurrent logons by monitoring the share mapped using drive** check box on the General object.

Figure 65: Set the drive to monitor for concurrent logons



Once configured, Desktop Authority will immediately log off any user that attempts to concurrently log on more times than they are allowed.

Root Mapping home directories

Root Mapping, step-by-step

The Root Mapping concept originates from the Novell Netware operating system. It allows a drive to be mapped to a directory that looks and acts like a root directory instead of a subdirectory.

Root Mapping to the user's home directory provides a simple path to the directory. Since all other users' home directories on the drive are invisible to the user, there is no confusion as to where the directory is. The user does not have to scroll through a list of folders to search for their own folder. This makes it faster to find what they are looking for.

For example, using Desktop Authority, you can "root map" drive letter H: to each user's home directory and then have Microsoft Office open/save paths default to H:\Documents; you can redirect Internet Explorer's bookmarks to H:\Bookmarks; you can create Outlook/Exchange mail profiles on-the-fly and store the personal address book and/or personal folders on H:\Exchange; and you can redirect all your shell folder pointers to H:\ShellFolders.

Simply put, you end up with the ability for any user to logon to any machine and retrieve all their settings -- without a visit from the network administrator and without using Roaming Profiles!

1. Create a base share point for your user's home directories.
2. Open Windows Explorer on the server to house home directories. Create a folder called "Users".
3. Right click the Users folder you just created and select the Sharing tab. Share this folder as "Users".

   > ⓘ Note: You may elect to have multiple base share points spread across one or many servers. Since Desktop Authority can use dynamic variables when mapping drives, you will only need a single entry on the Drive Mappings object to accommodate any configuration you wish. If you have hundreds or thousands of users, you may want to create a more complex "user tree". For example: You may create a "users" folder. Under the users folder, you create "faculty" and "students". Under the students folder, you create "sophomores", "freshmen", "juniors" and "seniors" folders. In this more complex example, the (4) sub-folders of "students" would be the base share points.Replace this text with a description of a feature that is noteworthy.

4. Create your users with User Manager for Domains (UMD) or Active Directory.

   When creating users with UMD, the key element to root mapping home directories is how you populate the fields of the Profile page for each user.

   If your ultimate goal is to map drive letter H: to each user's home directory, choose a different letter here in UMD.

5. Now specify the path to the user's home directory. Note that there are three logical pieces to the user's home path (\\server1\users\%username%), each separated by a backslash.

   The Desktop Authority dynamic variable for this entire home share string is **$HomePath**. Separating this path into three logical pieces, the first piece "\\server" is the name of the server that contains the base share point we created in step 1 (The Desktop Authority dynamic variable, less the leading backslashes is **$HomeServer**). The second piece "users" is the base share point (Desktop Authority dynamic variable: **$HomeBase**). The last piece is the actual home directory for the user (Desktop Authority dynamic variable: **$HomeDir**). UMD will automatically translate the %username% environment variable to the user's logon name when you press OK to exit this screen.

   When you press OK and save the user, User Manager for Domains will automatically create the user's home directory based on the information entered in this dialog.

6. You must grant NTFS permissions to an administrative group so that you can share the user's home directory, and allow your third-party backup program to read any documents stored in this directory.

   After you grant Full Control NTFS permissions to each users home directory for your administrative group, you can then share each user's home directory.

7. Apply NTFS permissions and share each user's home directory.

   Launch Windows Explorer and expand the Users folder to show the users home directories beneath it. Right click on each user home directory and select Properties. Then select the Security tab.

8. Add your administrative group (e.g. Domain Admins) to the list with Full Control rights.
9. Click Apply and then select the Sharing tab.
10. For security, it is recommended that when you create shares for each user's home directory, you make them hidden shares. A hidden share does not show up when your clients browse the network using Windows Explorer and/or Network Neighborhood. A hidden share has a dollar sign appended to the end of the actual share name. Ex. WClint$

Now you can configure Desktop Authority's Drive Mapping object.

Now that the user and their home directory have been created, secured and shared, we can configure Desktop Authority to map a drive letter to the "root" of their home directory.

1. Launch the Desktop Authority Manager, from Profiles, select the profile and then the Drive Mappings object. Insert a new configuration element.
2. Specify drive H for the drive letter and a shared folder of \\$HomeServer\$HomeDir$$.

   Notice how we can leverage the use of Desktop Authority's dynamic variables so that a single entry to the Drive Mappings object will accommodate mapping a drive letter to each user's home directory no matter how many servers and/or base share points exist on your network.

   Also, note the use of the trailing double dollar sign. This is due to the way in which the KiXtart engine interprets strings during execution. Since dynamic variables begin with a {$}, we enter a double dollar sign {$$} so that KiXtart knows we don't want to insert a variable at this point -- we simply want a dollar sign appended to the share (i.e. hidden share).
3. Save the changes, replicate and exit. Logon from a client to verify your home mapping works as expected.

Implementing a Poor Mans Proxy

The ability of Desktop Authority to control proxy settings can even be beneficial even if you don't have a proxy server on your network. With a little creativity, you can create a "Low Budget" proxy which prevents users belonging to a specific group from browsing the Internet.

Implementing this is a simple process. Follow these steps:

1. Create two domain groups. Call them **InternetAccess** and **NoInternetAccess**.
2. Select the **Internet Explorer Settings** object. Insert a new configuration element and configure the proxy settings for the **NoInternetAccess** domain group. Enable the use of a proxy server by selecting the **Use a proxy server** check box. Enter an invalid TCP/IP address (or the address of your Intranet server) as the Proxy Server address.

   By selecting the **Bypass proxy server for local addresses** check box, you could allow access to a small list of company/business related sites.

   Set the **Validation Logic Type** to *Group Membership* with a **Value** of the *NoInternetAccess* domain group.
3. From the **Internet Explorer Settings** object, highlight the newly created element and copy it (CTRL+C). This will create a new Internet configuration element and select it for edits. Clear the **Use a proxy server** check box.

   Set the validation logic type to *Group Membership* with a value of the *InternetAccess* domain group.
4. The final step is to define a security policy that will disallow a user from changing the proxy server configuration.

   Select the **Security Policy** object. Insert a new configuration element and configure the *Internet Explorer: Disable changing proxy settings* policy.

   Select *Enable* from the **Enable/Disable** list.

   Select *Internet Explorer* from the **Category** list.

Select the *Internet Explorer: Disable changing proxy settings* from the **Policy** list.

Modify the default **Validation Logic** to apply this policy for Group Membership, NoInternetAccess.

Desktop Agent

What is the Desktop Agent?

Desktop Authority provides the ability to execute programs when Windows shuts down, restarts or logs off. This happens with the help of the Desktop Agent. The Agent is a program that sits idle in the system tray until a shut down, restart or log off event occurs. When one of these events are triggered, the Agent will seamlessly invoke any queued applications, shell scripts, or service pack installations. Custom Scripts may also be executed at this time providing an unlimited array of functionality.

Configuring the Desktop Agent

To configure the Desktop Agent, select the **Desktop Agent** object under **Global Options**.

Desktop Agent client

The Desktop Agent client is an application used to launch specified programs when the client logs off or shuts down the computer. The client side of the Agent also provides several options to control the workstation. The user may Shut down, Restart, Logoff or Lock the workstation if the agents icon is displayed in the system tray. Simply right-click on the icon for the shortcut menu.

About

Select **About** from the shortcut menu to see version and copyright information regarding the Agent.

Shutdown

Select **Shut down** from the shortcut menu to shut down the workstation.

Restart

Select **Restart** from the shortcut menu to restart the workstation.

Logoff

Select **Logoff** from the shortcut menu to log the current user off of the workstation.

Lock Workstation

Select **Lock Workstation** from the shortcut menu to lock the workstation. Pressing **CTRL-ALT-DEL** will allow the user to unlock the workstation.

Special Options

Option files

There are several ways to control the mode in which **Desktop Authority** executes on the client workstation. This is done with the use of option files that may exist on workstation.

What is an option file?

An option file is simply an ASCII file created using any text editor, including Microsoft's Notepad. The file has no contents and the filename has no extension.

Creating an option file

The easiest way to create a special option file is using Windows Explorer. Right-click in the appropriate folder. Choose **New** and select **Text Document** from the shortcut menu.

When using Windows Explorer (New / Text Document) to create a Special Option File, make sure you deselect the *Hide file extensions for known file types* option under Folder Settings. This will allow you to create the file without the ".txt" extension.

Security concerns

To tighten overall security and prevent users/students, etc. from using these special option files to change the behavior of **Desktop Authority**, you can disable them in the **Desktop Authority** Manager. This is done in the Global Options Visual, Exceptions and Troubleshooting objects. Clearing the check box disables **Desktop Authority** from determining if the corresponding option file exists.

SLNOGUI

The presence of this file, (**SLNOGUI**., no file extension) specifies the selected visual startup option displayed during the logon process is overridden with a textual version of the logon window. If there are problems with any **Desktop Authority** client configurations, use this option file to figure out what in the logon process is problematic. The use of this file requires the **Allow any client to override this setting and always display the text logon screen** option to be set. This is done on the **Visual** object within **Global Options**.

To turn the SLNOGUI mode on for all clients without the use of this file, select the **Display Text Logon** check box on the **Visual** object within **Global Options**. Setting this global option provides the text dialog for all workstations.

This feature can be enabled for either a specific user or a specific workstation by using this special option file. To enable this feature for all users logging in from a specific workstation, place this file in the root directory of the workstation's hard drive. To enable this feature for a specific user regardless of which machine they logon from, place this file in the user's home directory.

SLBYPASS

The presence of this file, (**SLBYPASS**., no file extension) allows you to exclude certain computers from ever executing **Desktop Authority** regardless of the options selected in the **Desktop Authority** Manager.

The use of this file requires the **Allow any client to selectively bypass Desktop Authority execution** option to be set. This is done on the **Exceptions** object of **Global Options**. If this file is present on the client, the **Desktop Authority** Pre-Flight-Check (*SLOGIC.BAT*), will detect its presence and immediately exit before launching the main script engine and/or applying any configuration changes to the client.

To enable this feature for all users logging in from a specific workstation, place this file in the root directory of the workstation's hard drive.

SLNOCSD

The presence of this file, (**SLNOCSD**., no file extension) allows you to exclude certain computers from automated Service Pack installations, regardless of the Validation Logic applied to the Service Pack configurations by the **Desktop Authority** Manager.

If this file is present on the client, **Desktop Authority** will **NOT** install the Service Pack to the client, regardless of whether or not the user/computer satisfies the criteria specified by the Validation Logic settings for the Service Pack.

To enable this feature for all users logging in from a specific workstation, place this file in the root directory of the workstation's hard drive.

Other Special options

Force Refresh after desktop has been loaded and logon script has finished executing

This option can be used by admins to delay the initial execution of user elements (eg. printers, drive mappings etc). In some cases, this will help to avoid login delays and potentially resolve timing conflicts. However for this option to be utilized, the applicable user object element MUST be set to be executed at Refresh. This option is configured in the Registry profile object.

Configure the Registry element as follows:

1. Click on the User Management Registry object.
2. Click **Add**.
3. Optionally, enter a Profile element description at the top of the element.
4. Under the Registry Action, click **Add**.
5. Set the **Action** to *Write Value*.
6. Set the **Hive** to *HKEY_CURRENT_USER*.
7. Set the **Key** to *Software\scriptlogic\slagent*.
8. Set the **Type** to *REG_DWORD*.
9. Set the **Value** to *LaunchFirstRefreshAtDesktop*.
10. By default the Data/express is 0, which means, do no launch the refresh event when desktop loads. Setting this Data/expression to 1 (or anything else) means to launch the refresh event once the desktop loads and script finishes. Set this **Data/expression** to *1* to turn the immediate refresh event on. Select the *Decimal* data type.
11. Click **Confirm**.
12. Select the Validation Logic tab.
13. Select the Refresh box in the Timing section. This must be set for this option to work.
14. Click Save to save the new Registry element.

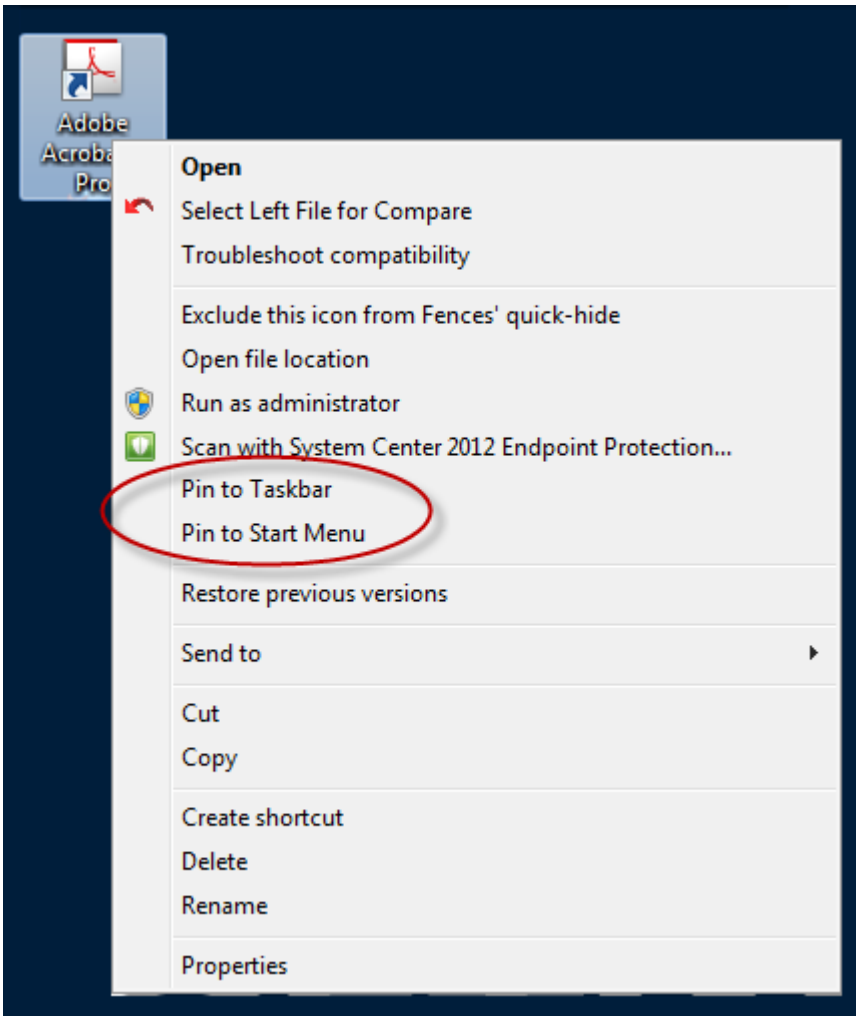
Global Definition variables list

User Management definitions

Shortcut profile object

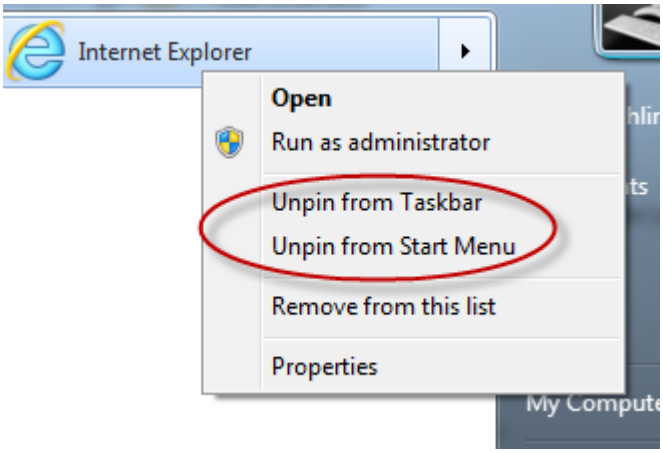
When selecting User Start Menu (Pin) or User Taskbar (Pin) with a non-English language workstation operating system, you must define a variable that defines the non-English verbiage to substitute in place of the English "Pin To..." verbiage. The value of these variables should match the "Pin to Taskbar" or "Pin to Start Menu" text on the popup menu of a program shortcut. The following variables can be defined as User Management Global Variables or as a Profile Definition Variable.

Figure 66: Example of "Pin to" options



For the Unpin variables, the value should match the "Unpin from Taskbar" or "Unpin from Start Menu" on the popup menu of a shortcut on the Start Menu or Taskbar.

Figure 67: Example of "Unpin from" options



$PinToTaskbarString

Defines the "Pin to Taskbar" verbiage on non-English client operating systems.

Example (German language operating system):

$PinToTaskbarString = "GermanLanguage"

where GermanLanguage will be replaced with the German language equivalent

$UnPinFromTaskbarString

Defines the "Unpin from Taskbar" verbiage on non-English client operating systems.

Example (German language operating system):

$UnPinFromTaskbarString = "GermanLanguage"

where GermanLanguage will be replaced with the German language equivalent

$PinToStartMenuString

Defines the "Pin to Start Menu" verbiage on non-English client operating systems.

Example (German language operating system):

$PinToStartMenuString = "GermanLanguage"

where GermanLanguage will be replaced with the German language equivalent

$UnPinFromStartMenuString

Defines the "Pin to Start Menu" verbiage on non-English client operating systems.

Example (German language operating system):

$UnPinFromStartMenuString = "GermanLanguage"

where GermanLanguage will be replaced with the German language equivalent

Web Browser profile object

The Web Browser object allows for the configuration of custom Firefox settings. If you wish to configure something in the Firefox browser that is not offered on the Web Browser object, it can be configured in the Global or Profile Definitions.

Use the following syntax for configuration:

AddCustomFirefoxPref('pref("Name", Value);')

This will set the named Firefox preference to the given value. This configuration can be accessed via the browser and changed by the user.

AddCustomFirefoxPref('lockPref("Name", Value);')

This will set the named Firefox preference to the given value. This configuration will not be able to be changed via the browser about:config dialog by the user.

"Name" is the name of the preference to be set.

Value is the boolean, string, or integer data for the preference.

Preferences and their settings can be seen in Firefox's about:config dialog.

NOTE: Custom Firefox preferences can be researched in this reference to the user preferences in the about:config,

Examples:

Bool Value: - value can be true or false

AddCustomFirefoxPref('pref("privacy.clearonshutdown.cache", true);')

String Value: - add double quotes around value

AddCustomFirefoxPref('pref("network.automatic-ntlm-auth.trusted-uris", "Http://www.google.com");')

Integer Value: - a numeric value

AddCustomFirefoxPref('pref("network.http.connection-retry-timeout", 500);')

Locked Integer Value: (to prevent a setting from being changed by the user, replace pref with lockpref)

AddCustomFirefoxPref('lockPref("network.http.connection-retry-timeout", 500);')

Computer Management definitions

Validation Logic

$VLCheckAllIPAddresses

This setting will enable Validation Logic to validate on any IP address defined for the client, instead of just the first one read. This variable can be defined as a User Management Global Variable or as a Profile Definition Variable.

Example:

$VLCheckAllIPAddresses = 1

Registry keys

sqlCommandTimeout

Sometimes, on large database transactions, the default SQL Command timeout value is not big enough to support the command, allowing the transaction to timeout and fail. Creating this new registry key allows this timeout value to be overridden and increased to alleviate a timeout problem.

Name	Type	Data
HKEY_LOCAL_MACHINE\SOFTWARE\ScriptLogic\SqlCommandTimeout	DWORD	specified in seconds

A

File Paths

The following table describes the paths that Desktop Authority uses.

Desktop Authority upgrades from previous versions to 11.2 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 11.2	Install Path for ver 11.2
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 11.2	Install Path for ver 11.2
• 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 11.2	Install Path for ver 11.2
• (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 11.2 Version Paths
• x:\PF\ScriptLogic\Port Security	• x:\PF\Quest\Desktop Authority\PortSecurity • %windir%\system32

User Detailed Trace File

- %temp%\Desktop Authority
- %temp%\Desktop Authority

Computer verbose debug mode

- %windir%\Temp\Desktop Authority
- %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

- 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

Expert Assist

- x:\PF\DesktopAuthority
- x:\PF\Quest\ExpertAssist

Product Improvement Program

To assist in the development of new features, as well as drive future improvements, we have implemented a Product Improvement Program. Feedback from this program provides product management with valuable insight into how our products are being used. This information is essential to help the R&D team prioritize existing enhancement requests within the roadmap of the each product. Participation is voluntary, and no personal contact information is ever collected.

How do I participate in the Product Improvement Program? What if I change my mind?

There is an option within the Desktop Authority Setup Tool (Product Improvement section) that can be used to verify or change your participation at any time.

How will the collected information be used?

Information collected will be used to develop new features and improve Desktop Authority.

Where is the data being stored?

The data is stored on a secure server within the USA and will be accessed only be the members of the Desktop Authority R&D team.

What information is collected?

- Desktop Authority features usage data such as console configuration settings
- System information such as operating system, processor, and memory installed
- Domain information such as number of users, servers, and workstations being managed
- Browser type and version
- Product information such as version
- License information such as type and number of seats

How does the Product Improvement Program work?

You choose to participate and allow Desktop Authority to send usage data, associated with an anonymous user ID from your computer. If you are offline at any time, the data will be sent the next time an Internet connection is available.

How long will collected data be stored?

We will store the collected data on our secure server for as long as the Product Improvement Program is in place.

Will I receive spam if I participate in the Product Improvement Program?

You will not receive any e-mail regarding the Product Improvement Program, regardless of whether you participate. We do not collect personally identifiable information.

Do I need an Internet connection?

An Internet connection is required for participation. However, it can be an intermittent connection. When an Internet connection becomes available, the information is automatically transmitted with minimal impact to your system.

Can I see the data that is collected before it is transmitted?

No, the information cannot be displayed on the customer side. The collection of the desired data occurs seamlessly in the background without affecting the product. Additionally, all formatting and processing of the collected data are done post transmission.

How long will my participation in the program last?

Information is actively collected as long as you use the product version for which you have agreed to participate or until you decide to end your participation.

How is my privacy protected?

We take many precautions in protecting the information that is collected and transmitted. You can learn more about how we handle user information by reviewing our Privacy Policy.

Since no personally identifiable information is collected, the anonymous data will not be meaningful to anyone outside of our company.

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.

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

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W