DESKTOP AUTHORITY®
VERSION 8

Desktop Authority 8
Administrator's Guide

SCRIPTLOGIC

This publication supports Desktop Authority 8. It is possible that it may contain technical or typographical errors. ScriptLogic Corporation provides this publication “as is,” without warranty of any kind, either expressed or implied.

ScriptLogic Corporation
6000 Broken Sound Parkway NW
Boca Raton, Florida 33487-2742

1.561.886.2400
www.scriptlogic.com

Documentation Conventions

Typeface Conventions

Bold Indicates a button, menu selection, tab, dialog box title, text to type, selections from drop-down lists, or prompts on a dialog box.

Contacting ScriptLogic

ScriptLogic may be contacted about any questions, problems or concerns you might have at:

ScriptLogic Corporation
6000 Broken Sound Parkway NW
Boca Raton, Florida 33487-2742

561.886.2400 Sales and General Inquiries
561.886.2450 Technical Support

561.886.2499 Fax

www.scriptlogic.com

ScriptLogic on the Web

ScriptLogic can be found on the web at www.scriptlogic.com. Our web site offers customers a variety of information:

- Download product updates, patches and/or evaluation products.
- Locate product information and technical details.
- Find out about Product Pricing.
- Search the Knowledge Base for Technical Notes containing an extensive collection of technical articles, troubleshooting tips and white papers.
- Search Frequently Asked Questions, for the answers to the most common non-technical issues.
- Participate in Discussion Forums to discuss problems or ideas with other users and ScriptLogic representatives.

TABLE OF CONTENTS

CONCEPTS

WHAT IS DESKTOP AUTHORITY?

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, Desktop Authority Express and Desktop Authority for Configuration Manager. Desktop Authority Express is a scaled down version of Desktop Authority. It does not include the following standard features included by default in the full version -- Patch Management, Software Management, Anti-Spyware, USB/Port Security, Hardware and Software Inventory and Custom Reporting and the Desktop Authority Remote Management tool.

Desktop Authority for Configuration Manager is a version of Desktop Authority that is geared towards enterprises who already use Microsoft's System Center Configuration Manager (SCCM) or other similar management tools. Since SCCM provides tools for Software Distribution and Asset Management, Desktop Authority does not include its own built-in Software Distribution or Asset Management capabilities.

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 and patch deployment, Group Policy Templates, Anti-Spyware detection, 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, inventoried and patched, 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

(not available in Desktop Authority Express and Desktop Authority for Configuration Manager)

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

(not available in Desktop Authority Express)

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

Patch Management

(not available in Desktop Authority Express)

The time taken for attackers to develop an exploit when a patch is released from Microsoft is decreasing. In the case of the Zotob worm, it was only 5 days from the release of the MS05-039 patch until attackers were able to take advantage of unpatched desktop computers. Administrators cannot simply rely on network perimeter security, since desktop users download files directly from the Internet and use their laptops on unsecured networks when traveling or at home.

Inherently, Desktop Authority includes the ability to scan desktops for missing patches and download them from Microsoft. Low severity patches can then be installed. Desktop Authority’s Patch Deployment for Desktops Option builds on the base Desktop Authority platform to dramatically simplify the task of installing any Microsoft Operating System or application patches onto desktops across the enterprise, and shut the door on attacks that exploit unpatched systems.

The Patch Deployment for Desktops Option takes the tasks of downloading patches from Microsoft, distributing them to deployment servers, selecting appropriate patches, selecting clients and deploying patches, and wraps them all up into the easy-to-use Desktop Authority Manager console, minimizing the amount of time required by administrators to manage patch deployment, while maximizing control over the patch management process.

Anti-Spyware

(not available in Desktop Authority Express)

One of today's fastest-growing threats to enterprise security is spyware. From simple annoying ad pop-ups, to identity-stealing key loggers and all the different types of software that snoops-on and threatens your network in between, spyware is potentially more dangerous and destructive to your business than any computer virus. Desktop Authority's enterprise-class Spyware Detection and Removal (SDR) option gives administrators the ability to centrally secure and protect desktops across the enterprise against spyware, together with centralized control and reporting.

Out of the box, Desktop Authority offers the ability to download spyware definition updates and detect spyware on desktops. In other words, without purchasing the Spyware Removal option, administrators can find out exactly how much spyware is currently residing on desktops across the network. Once the Spyware Removal option is enabled, quarantining and removal options are available to rid client machines of unwanted spyware. In the event that SDR reports that an application is classified as spyware even though it is known to be benign or an acceptable risk, SDR can be configured to exclude that application from detection.

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, super-users can ensure that administration of Desktop Authority follows enterprise security boundaries.

Hardware and Software Inventory and Custom Reporting

(not available in Desktop Authority Express and Desktop Authority for Configuration Manager)

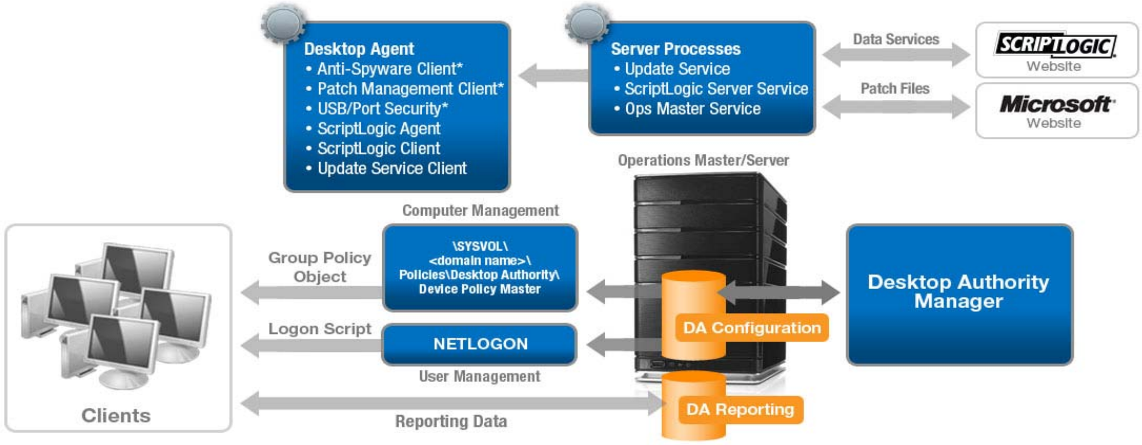
Desktop Authority profiles and their configurations are stored in an SQL database, along with information about the managed desktop. Built-in and custom reporting puts vital information at the fingertips of administrators, including reports on hardware and software inventory, user activity, patch deployment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

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

HOW DOES DESKTOP AUTHORITY WORK?

Desktop Authority uses several components to facilitate configuration 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.

An overview the Desktop Authority system is shown below.



*Not installed on clients where the purchased environment is Desktop Authority Express or Desktop Authority for Configuration Manager.

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 moved 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 tool. Data is extracted from the DACONFIGURATION database and written to configuration files, in the replication shares, which are used to configure user based settings when a user logs in to the computer. Computer based settings are configured and executed on each client based on the Computer Management agent that runs on the client. The agent is deployed to each client with Group Policy extensions.

Configuration and Reporting Databases

Desktop Authority can install Microsoft SQL Server 2005 Express Edition on the Operations Master or use an existing SQL Server. Within this database instance there are two databases created. They are DACONFIGURATION and DAREPORTING. The DACONFIGURATION database is used to store product configuration data. The DAREPORTING database holds hardware and software inventory, user activity and other essential data that is collected for reporting purposes (not available for Desktop Authority Express).

ScriptLogic Service

The ScriptLogic 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 ScriptLogic service to each client in order to temporarily elevate administrative rights. The ScriptLogic service is installed to one or more servers within the domain.

Update Service

The Update Service is used for software and data update services. This service is required for the Patch Management, Anti-Spyware, Software Management and Portable Device Control features of Desktop Authority.

This service interfaces with www.scriptlogic.com and www.microsoft.com in order to download Microsoft patches, anti-spyware definition updates and Patch Management updates. The Update Service offers an encrypted and secure connection to the ScriptLogic web site. This service is installed to one or more servers within the domain.

OpsMaster Service

Desktop Authority may be installed to a Domain Controller or Member Server. The installation server is known as the Operations Master. The OpsMaster service is hosted on the Operations Master server. This service manages communications among the Desktop Authority Manager, databases, services, and logs. This service is installed once per domain on the Operations Master server.

Group Policy Object (User and 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 by Group Policy extensions. The agent service interprets the Computer Management object settings and executes them at the appropriate startup, shutdown, refresh and scheduled events.

Logon Script (User Management)

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 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 Anti-Spyware and Patch Management components are launched on the client. The client is scanned for Anti-Spyware and missing patches.

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.scriptlogic.com/kixtart.

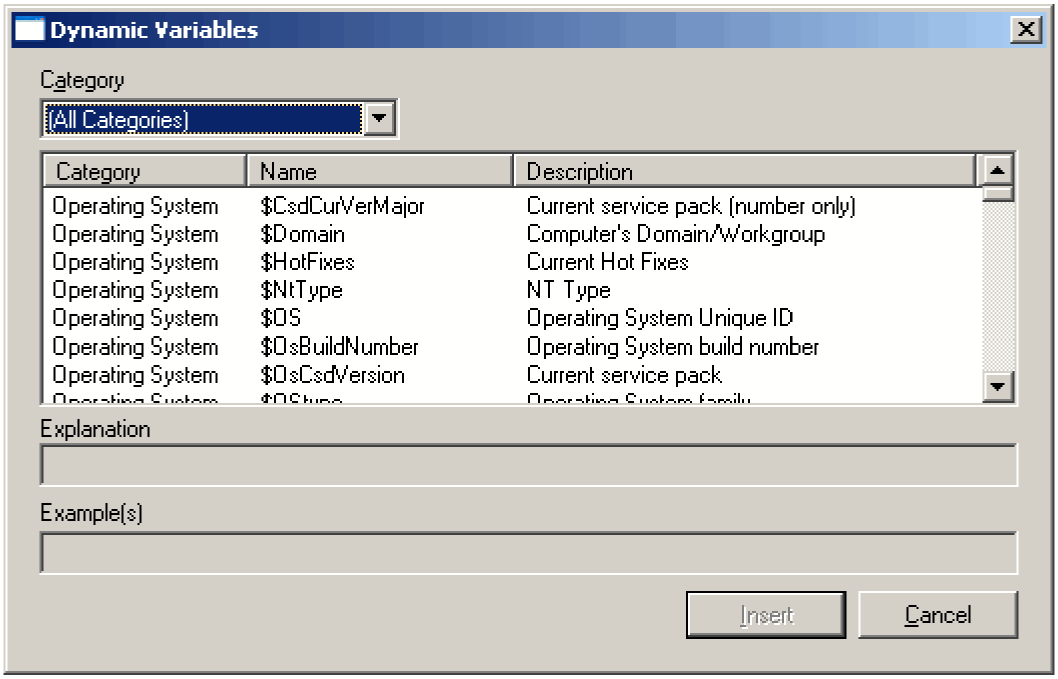
There are two categories of Dynamic Variables: Predefined and Custom. Predefined dynamic variables are ones that are defined by **Desktop Authority**. Custom Scripts may override the value of these variables. **Desktop Authority** can also make use of User Defined Custom dynamic variables.

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.



Category	Name	Description
Operating System	$CsdCurVerMajor	Current service pack (number only)
Operating System	$Domain	Computer's Domain/Workgroup
Operating System	$HotFixes	Current Hot Fixes
Operating System	$NtType	NT Type
Operating System	$OS	Operating System Unique ID
Operating System	$OsBuildNumber	Operating System build number
Operating System	$OsCsdVersion	Current service pack
Operating System	$OStype	Operating System family

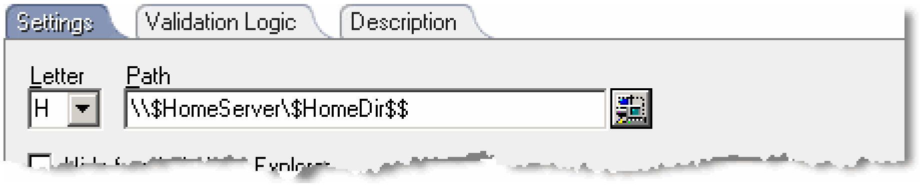
To select a variable, select it in the list and click Insert or double-click the variable. The selected variable will be inserted into the field at the current cursor position.

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

A complete list of predefined variables can be found on the ScriptLogic web site.

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.



Letter: H

Path: \\$HomeServer\$HomeDir$$

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.

User Interface

Overview

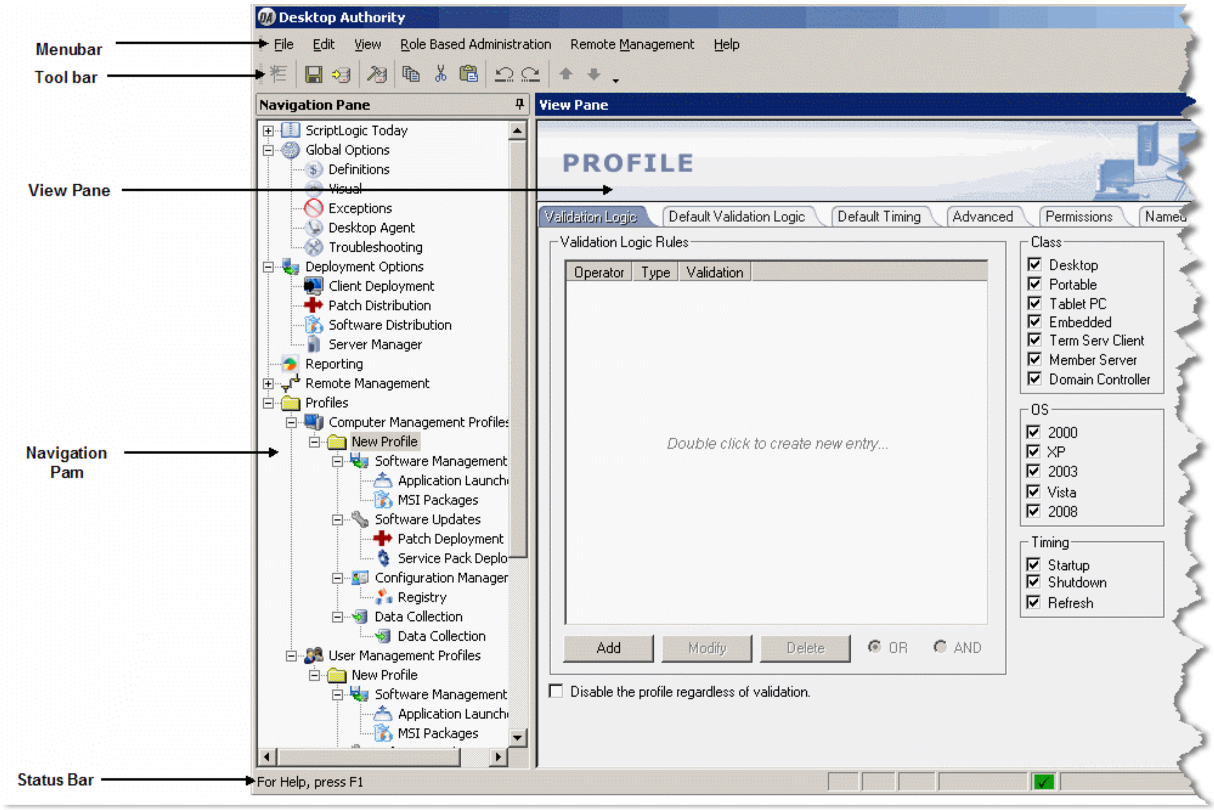
The Desktop Authority Manager is the Administrator's tool to centrally manage profiles and client configurations. All Desktop Authority configurations are defined within the manager. The manager is also used to replicate and deploy settings to clients during the logon process. It also provides access to configure Global, Profile, and Remote Management settings. Server Manager and Report Generator are also accessed from within the manager.

The Desktop Authority Manager is comprised of the following sections:

- Menu Bar
- Toolbar
- Navigation pane
- View pane
- Status Bar

The Manager requires Internet Explorer version 4.01 or greater to be installed. If Patch Management or Anti-Spyware are deployed, Internet Explorer version 4.10 SP2 or greater is required.

The figure below shows the location of each section in the manager.



Menu Bar

The menu bar provides pull-down menus that save and replicate the Manager's changes, maintain and/or update profiles in the navigation tree, customize the look of the manager, provide access to Server Manager, Report Generator and Remote Management. Help is also available from the menu bar. These menu items are also available in their respective part of the Navigation pane.

Some selections on the menu bar may be unavailable (disabled) depending on the currently selected functionality.

Toolbar

The Toolbar provides icons for fast and easy access to commonly used functions. The available toolbar icons are New (Profile and Configuration Element), Save changes, Replicate changes, Server Manager, Report Generator, Cut, Copy, Paste, Undo, Redo, Print, About, Move up and Move down.

Navigation Pane

The Navigation pane is used to select an object to work with. The View pane changes based on the object selected in the Navigation pane.

View Pane

The View pane is used to set configurations for the currently selected object in the Navigation pane.

Status Bar

The status bar shows the current status of manager. It can be either Red (not saved), Yellow (saved, not replicated) or Green (saved and replicated).

MENU BAR

The Menu Bar provides five menus used to perform operations on the various elements in the Navigation pane. Menu items are enabled or disabled according to the selected item in the Navigation pane. Disabled menu items appear on the menu but are grayed out and will not perform any action if clicked on.

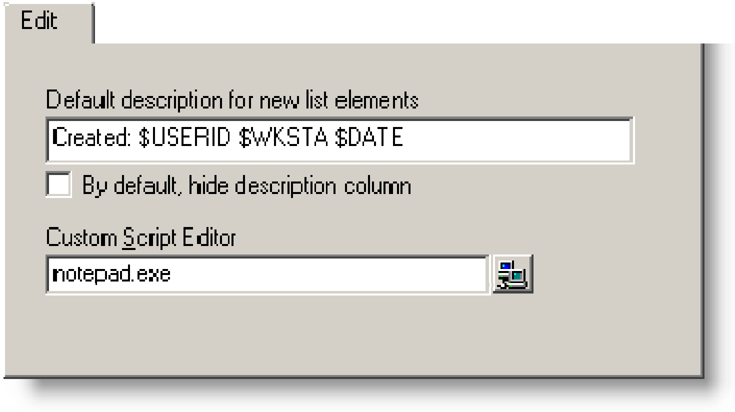
Menu	Description
File	Use the File menu to Save and Replicate changes. You can also Queue an Update of Client files, Import and Export profiles, set program Preferences, Create program shortcuts , Launch System Readiness Wizard and set Global System settings.
Edit	Use the Edit menu to add new profiles and update configuration entriesin existing profiles. This menu includes items for New Element, Undo, Redo, Cut, Copy, Paste, Delete and New Profile.
View	Use the View menu to change the appearance of the Manager. This includes managing the Manager's toolbars, Status bar, Shortcut Pane, Toolbar themes, Pane themes, and sorting of profile objects. Server Manager can also be run from the View menu. Select Reset to Default to set the Manager's orientation back to its default view which includes the Navigation Pane, Shortcut Pane and View Pane.
Role Based Administration	Use the Role Based Administration 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.
Remote Management (not available for Desktop Authority Express)	Use the Remote Management menu to Remotely Manage the highlighted computer in the Remote Management tree of the Navigation Pane.
Help	Use the Help menu to display Help on the selected item. The Help menu also displays information about the Manager.

PREFERENCES

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.

Edit tab

The Edit tab provides several options that configure the way each object configuration list works. These options set up an optional confirmation when deleting list elements, as wells as default description options for list elements.



Edit

Default description for new list elements

Created: $USERID $WKSTA $DATE

□ By default, hide description column

Custom Script Editor

notepad.exe

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*.

The description may be overridden for each configuration element.

By default, hide description column

Select this box to hide the description column in the object configuration lists. Clear this check box to display the description column in the object configuration lists. Press F3 to toggle the Description column, on and off, within the list.

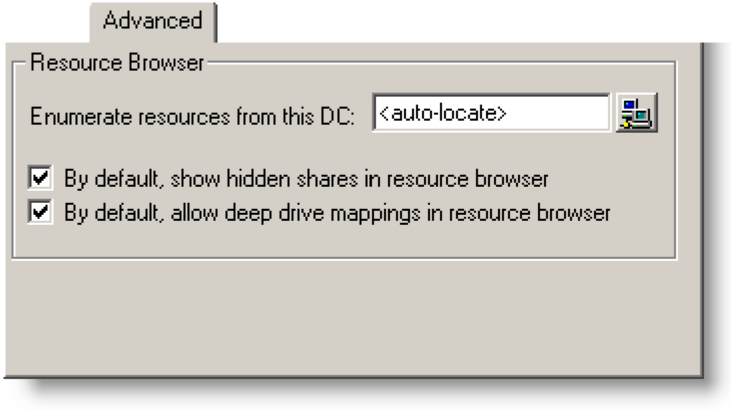
Custom Script Editor

Define the program to execute when creating or modifying custom scripts. Any ASCII editor may be used. There are several third-party specialized KiXtart-aware editors available.

Click to find the program location. The default Custom Script Editor is Notepad.exe.

Advanced tab

The Advanced tab provides several advanced options that the Desktop Authority Manager uses at startup. These options include Resource Browser options and Deep Drive Mapping options.



Advanced

Resource Browser

Enumerate resources from this DC: <auto-locate>

☑ By default, show hidden shares in resource browser

☑ By default, allow deep drive mappings in resource browser

Enumerate resources from this DC:

Tell Desktop Authority to use a specific domain controller in order to enumerate Group and User information. A Domain Controller may be manually typed into the field or selected by pressing the Select Server, , button. Leave blank to allow the network to decide which DC to query for necessary resources.

By default, show hidden shares in resource browser Select or clear this check box to control the default value of the Show Hidden option on the Desktop Authority resource browser. The Resource Browser is the file browser that is called when is clicked.

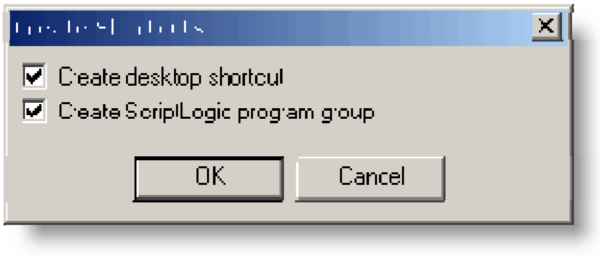
By default, allow deep drive mappings in resource browser

Deep Drive Mappings provide the ability to allow drive mappings to a subfolder inside a network share as opposed to solely the network share.

Select or Clear this check box to control the default value of the Deep Mapping option on the Desktop Authority resource browser. The Resource Browser is the file browser that is called when is clicked.

CREATE PROGRAM SHORTCUTS

The Create program shortcuts menu selection will easily create Desktop Authority shortcuts in the Start menu Programs group and on the desktop.



☑ Create desktop shortcut

☑ Create ScriptLogic program group

Click **Ok** to proceed with shortcut creation.

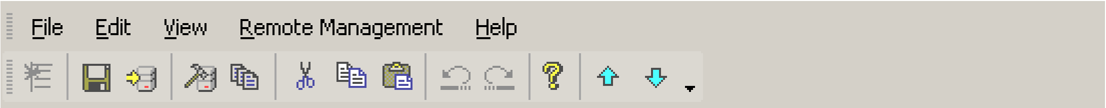
Click **Cancel** to return to the manager without creating shortcuts.

THEMES

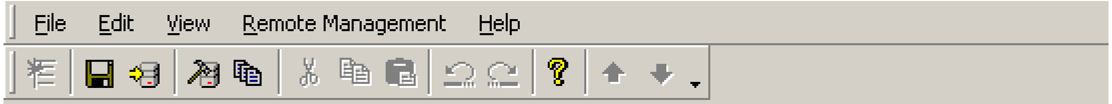
The **Desktop Authority** Manager supports various Themes that each provides for a different look to the Toolbars and Panes of the manager.

Toolbar Themes

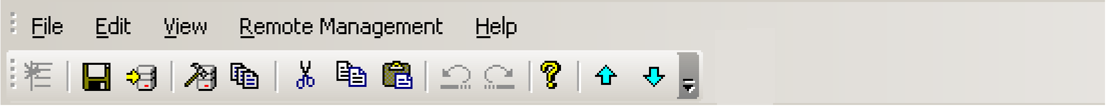
Office XP



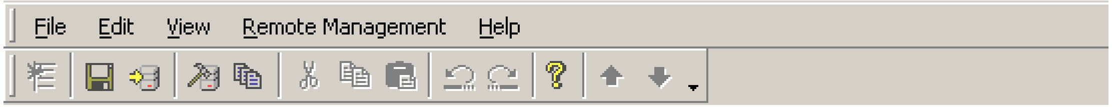
Office 2000



Office 2003

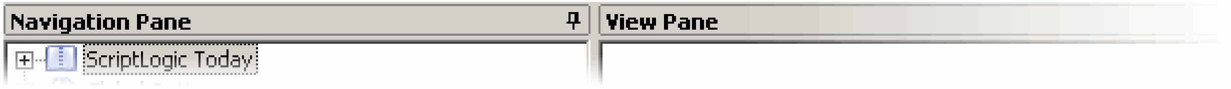


Windows XP

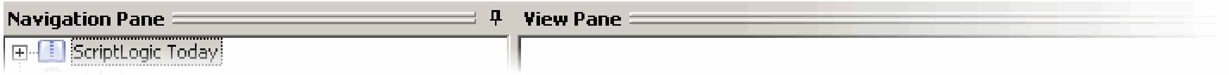


Pane Themes

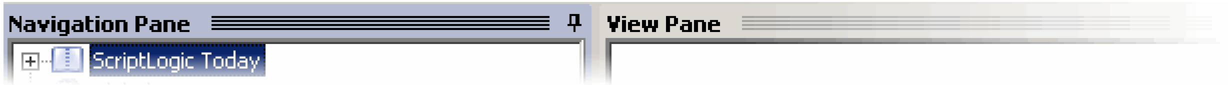
Office



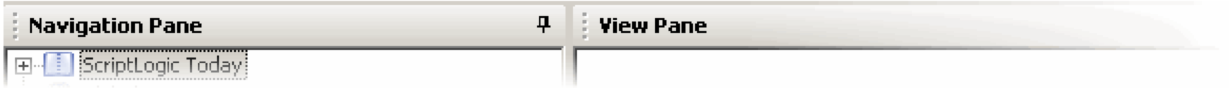
Grippered



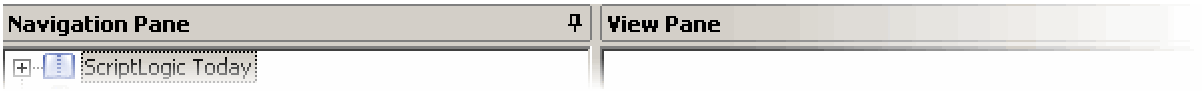
Visio



Office 2003



Windows XP

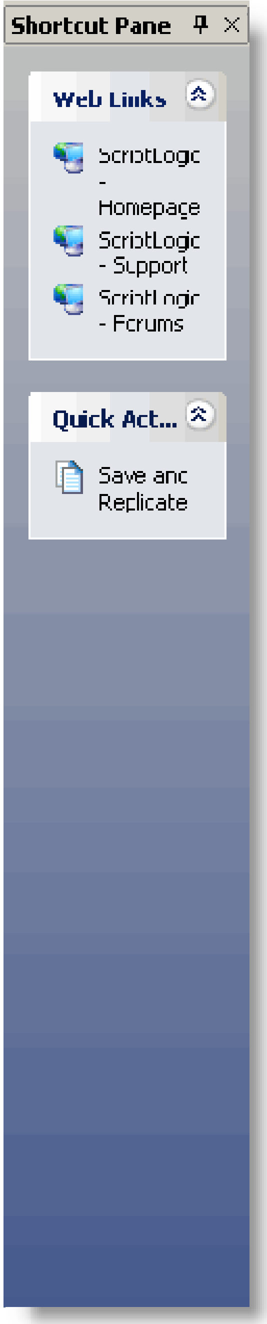


TOOLBAR

The toolbar provides icons that provide access to the most commonly used Manager functions. Access to each item is based on the object selected in the Navigation pane. If an icon on the toolbar does not apply to the selected object in the Navigation pane, it is disabled. Disabled icons appear on the toolbar but are grayed out and will not perform any action if clicked on. Move the mouse cursor over any available icon to view a description of it use.

Button	Name	Function
	New	New configuration entry or new profile.
💾	Save	Save all changes
	Replicate	Replicate changes.
	Server Manager	Run Server Manager
	Report Generator	Run Report Generator
✂	Cut	Cut selected text
⎘	Copy	Copy selected text
📋	Paste	Paste selected text
↶	Undo	Undo action
↷	Redo	Redo action
?	About	About
⇧	Move Up	Move configuration element or profile up.
⇩	Move Down	Move configuration element or profile down.

SHORTCUT PANE



The Shortcut pane is used to provide links to commonly used functions of the program. Upon entry into the manager, the shortcut pane is closed. It can be shown by selecting **Shortcut Pane** from the **View** menu. Close the Pane by again selecting Shortcut Pane from the View menu or by clicking ✕ on the top right of the pane. The Shortcut Pane is broken up into two groups, Web links and Quick Actions.

The Web Links section of the Shortcut Pane provides links to the ScriptLogic web site, home page, support and discussion forums pages.

The Quick Actions section provides links to Save and Replicate changes in the Manager.

Navigation Pane

The Navigation pane contains a hierarchical tree that displays the available objects in the Manager. The manager tree features functionality for

- System Dashboard
- Global Options
- Deployment Options
- Remote Management (not available for Desktop Authority Express)
- Profile Configurations

Click ⊞/⊟ to expand or contract each object on the manager's tree. Double-clicking will also expand or contract the tree objects. Upon selecting an object from the navigation tree the View pane will change to reflect the specific settings for that object.

View Pane

The View pane contains all content for the selected object on the Navigation pane. For most objects the View pane contains a list to the top of the pane and configuration tabs below the list.

Shortcuts

All configuration lists use a common shortcut key of CTRL-A to Select all items in the list.

Drag and Drop

Elements in the Configuration lists may be prioritized by clicking **Move Up (⇧)** and **Move Down (⇩)** on the toolbar or by Selecting specific elements and drag them to a new location in the list.

Toggle Description Column

The Description column in the Configuration list may be toggled to be displayed or hidden by pressing the F3 key.

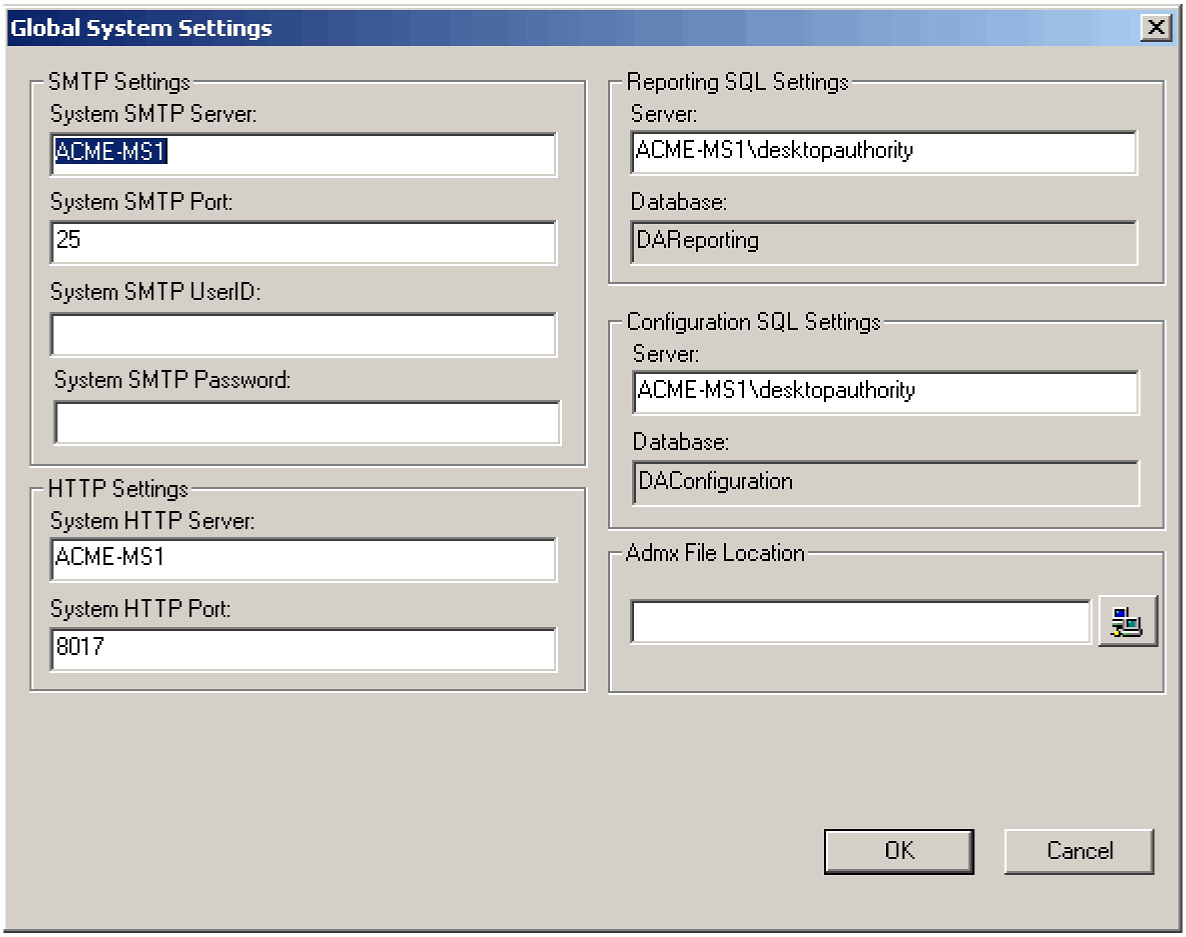
STATUS BAR

The Desktop Authority Manager contains a status bar which displays a colored LED. This LED indicates the status of the Manager's current configurations. This tells at a glance if the most recent configuration changes have been saved and/or replicated.

The LEDs represent the following statuses:

- ☒ (Red) This status indicates that the updated configurations have not been saved or replicated.
- ⚠ (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.

GLOBAL SYSTEM SETTINGS



SMTP Settings

System SMTP Server: ACME-MS1

System SMTP Port: 25

System SMTP UserID:

System SMTP Password:

HTTP Settings

System HTTP Server: ACME-MS1

System HTTP Port: 8017

Reporting SQL Settings

Server: ACME-MS1\desktopauthority

Database: DAReporting

Configuration SQL Settings

Server: ACME-MS1\desktopauthority

Database: DAConfiguration

Admx File Location

SMTP Settings

The Reporting object includes a report scheduler and can email reports to specific users or a distribution list.

System SMTP Server

The name of the SMTP server that email will be sent through.

System SMTP Port

The SMTP port that the server is listening on.

System SMTP UserID

Some SMTP servers require a userid and password in order to send mail. Enter the SMTP UserID here.

System SMTP Password

Some SMTP servers require a userid and password in order to send mail. Enter the SMTP Password here.

HTTP Settings

The Desktop Authority OpsMaster service runs Web Services and uses the following options to communicate

System HTTP Server

The server that the OpsMaster service is running on.

System HTTP Port

The port that the OpsMaster is listening on.

Reporting SQL Settings

Server

The database server where the Reporting database is held.

Database

The name of the reporting database, by default this is DAREPORTING.

Configuration SQL Settings

The Configuration database holds all data that the Manager uses to configure profiles.

Server

The database server where the Configuration database is held..

Database

The name of the configuration database, by default this is DACONFIGURATION.

ADMX File Location

Enter the path where ADMX files will be copied to when imported into Desktop Authority. This is the folder DA will use to manage all imported ADMX files. Click to browse to the path.

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 domain, group, OU, user, computer name, file name, folder, servers and printers. The contents of the dialog are based on the object that the Resource Browser is called from.

The icon 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 within the Profiles branch of the Navigation tree. Click ⊞/⊟ on a profile to expand or contract the objects contained within the profile. Double-clicking the profile name will also expand or contract the contained objects. The order of the profiles may be rearranged by clicking the ⇧ and ⇩ toolbar buttons. Profile ordering can also be rearranged by using a drag-and-drop operation.

Creating Parent (top level) Profiles

To create a new parent or top level profile,

1. Right-click on the Profiles branch of the navigation tree.
2. Select New Profile from the shortcut menu.
3. The new profile is added as the last profile in the Profiles list.
4. Enter the new profile's name.

Every newly created 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.

Creating Child Profiles

Profiles may contain child (sub) profiles. A child profile is a profile that is contained within another profile. The child profile will be evaluated for execution if and only if the validation logic for the profile above it is true.

To create a child profile,

1. Right-click on the parent profile to which the child profile will be added under.
2. Select New Child Profile from the shortcut menu.
3. The new profile will be added as the last child profile within it's parent.
4. Enter the new child profile's name.

Every newly created 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.

Deleting Profiles

To delete a profile,

1. Right-click on the profile to be deleted.
2. Select Delete Profile from the shortcut menu.
3. On the deletion confirmation dialog, click Yes to remove the selected profile along with any child profile within it. Click No to cancel the deletion.
4. If the deletion if confirmed, click Yes on the subsequent dialog to permanently remove the physical file that contains the profiles configurations. Click No to leave the configuration file in the SLSCRIPTS share. Leaving the file in the share provides the opportunity to recreate the profile by importing the file in the future.

Copying Profiles

To copy a profile,

1. Right-click on the profile to be copied.
2. Select Copy from the shortcut menu.
3. The profile is copied to the clipboard. It is now available to paste from the clipboard to another location
4. To paste this profile as a child profile, right-click on a Profile name and select Paste from the shortcut menu. To paste this profile as a parent (top level) profile, right-click on Profiles and select Paste from the shortcut menu.

Moving Profiles

Profiles can be moved within a parent profile to change the order in which it is evaluated, they can be moved into another profile or they can be moved to a parent (top) level profile.

To move a profile,

1. Select the profile to move by clicking on it. Holding the left mouse button down, drag the profile to the location it will be moved to and drop it by releasing the left mouse button. A profile cannot be moved to a child profile within itself.

or

1. Placement of a profile can also be changed by clicking or on the toolbar. This will move a child profile up one or down one within its parent, or a parent (top) level profile up or down one within the parent profile processing order.

Import Profiles

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

To import a profile,

1. Right-click on the profile to be imported.
2. Select Import from the shortcut menu.

Export Profiles

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

To export a profile,

1. Right-click on the profile to be exported.
2. Select Export from the shortcut menu.
3. Select a destination folder.

Exporting a profile does not include any child profiles. They must be exported separately.

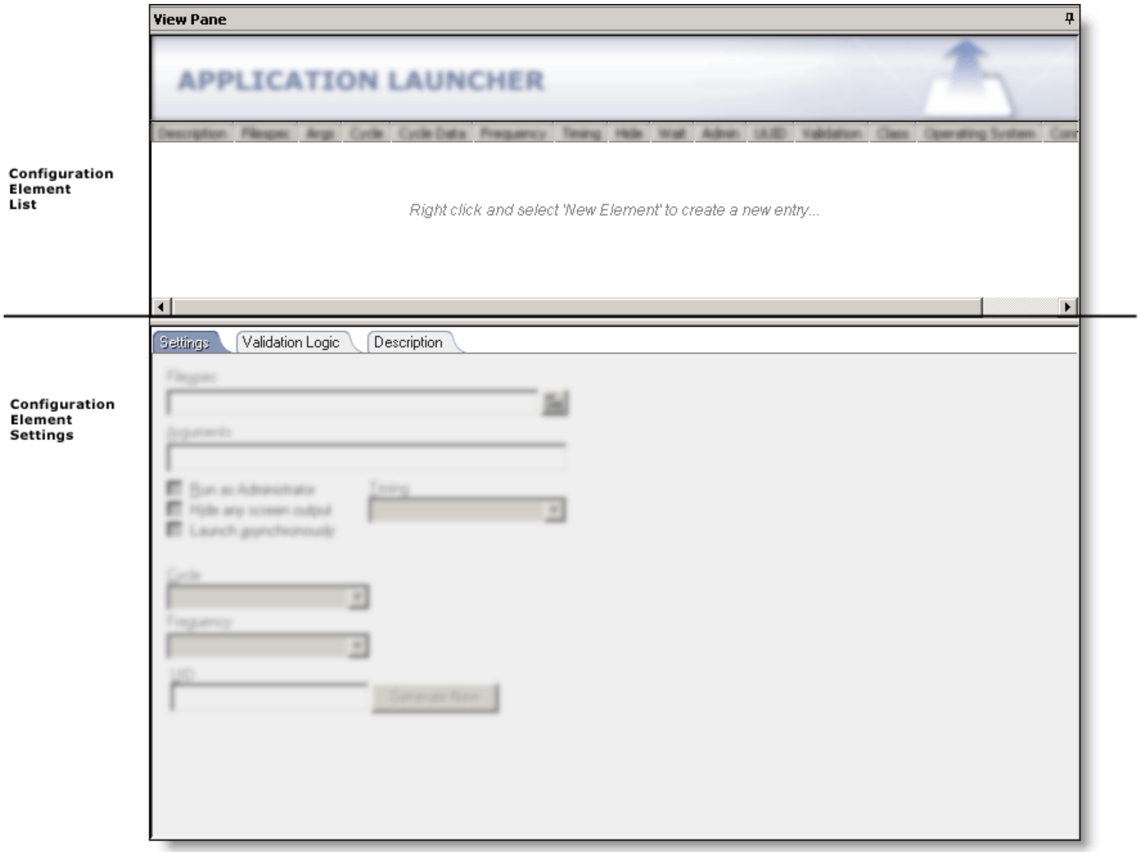
USING AND CONFIGURING PROFILE OBJECTS

The View Pane for each object within a profile is divided into two sections. The Configuration Element List and the Configuration Element Settings.

The Configuration list is where all settings for the object are held. As Desktop Authority processes the configuration elements defined by the configuration list, Validation Logic is applied to each element, beginning with the top of the list. Prioritize the list entries by clicking **Move Up (⇧)** and **Move Down (⇩)** to reorganize the list.

Click ↶ and/or ↷ from the tool bar to undo or redo a configuration element setting.

The bottom half of the object's View Pane contains the settings for individual configuration elements for the object.



Right click and select 'New Element' to create a new entry...

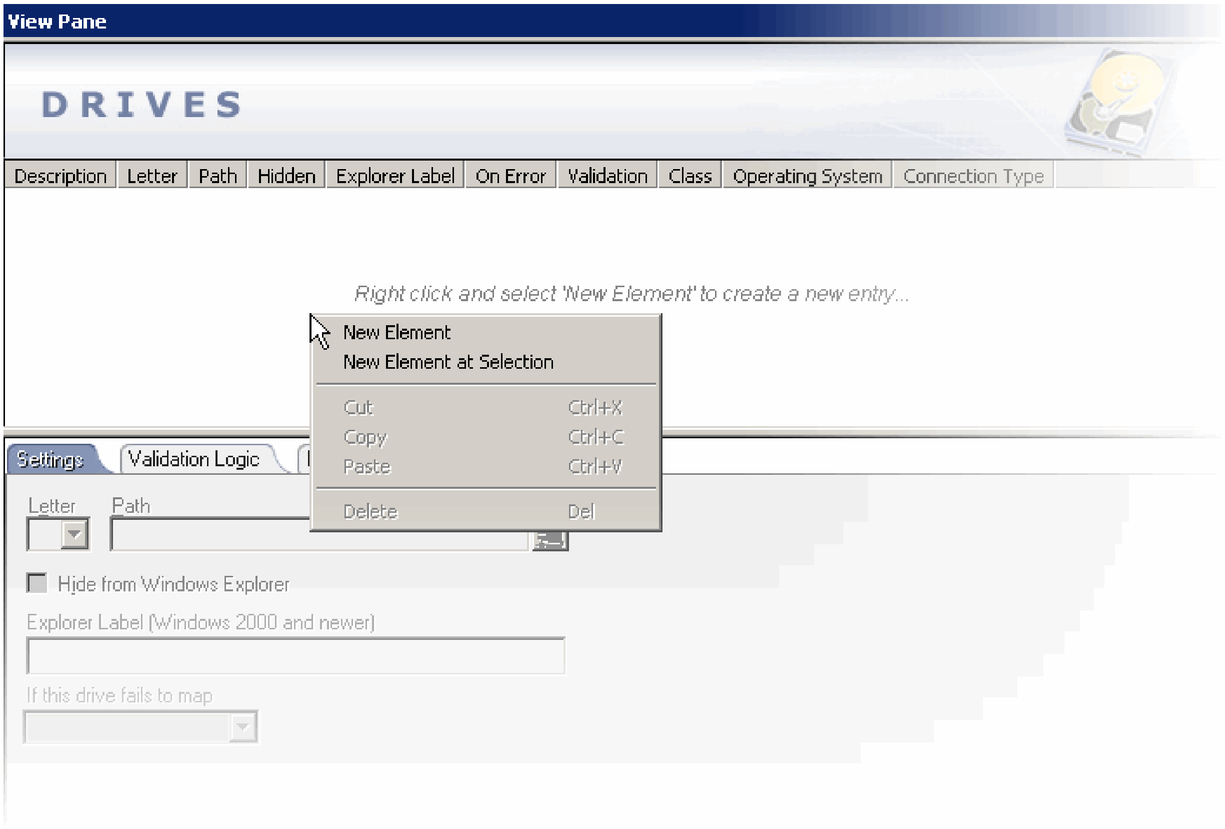
Configuation Object

Using the Configuration Element List

Creating Configuration Elements

To create a new configuration element,

1. Right-click on the configuration list.



2. Select either New Element or New Element at Selection from the shortcut menu.

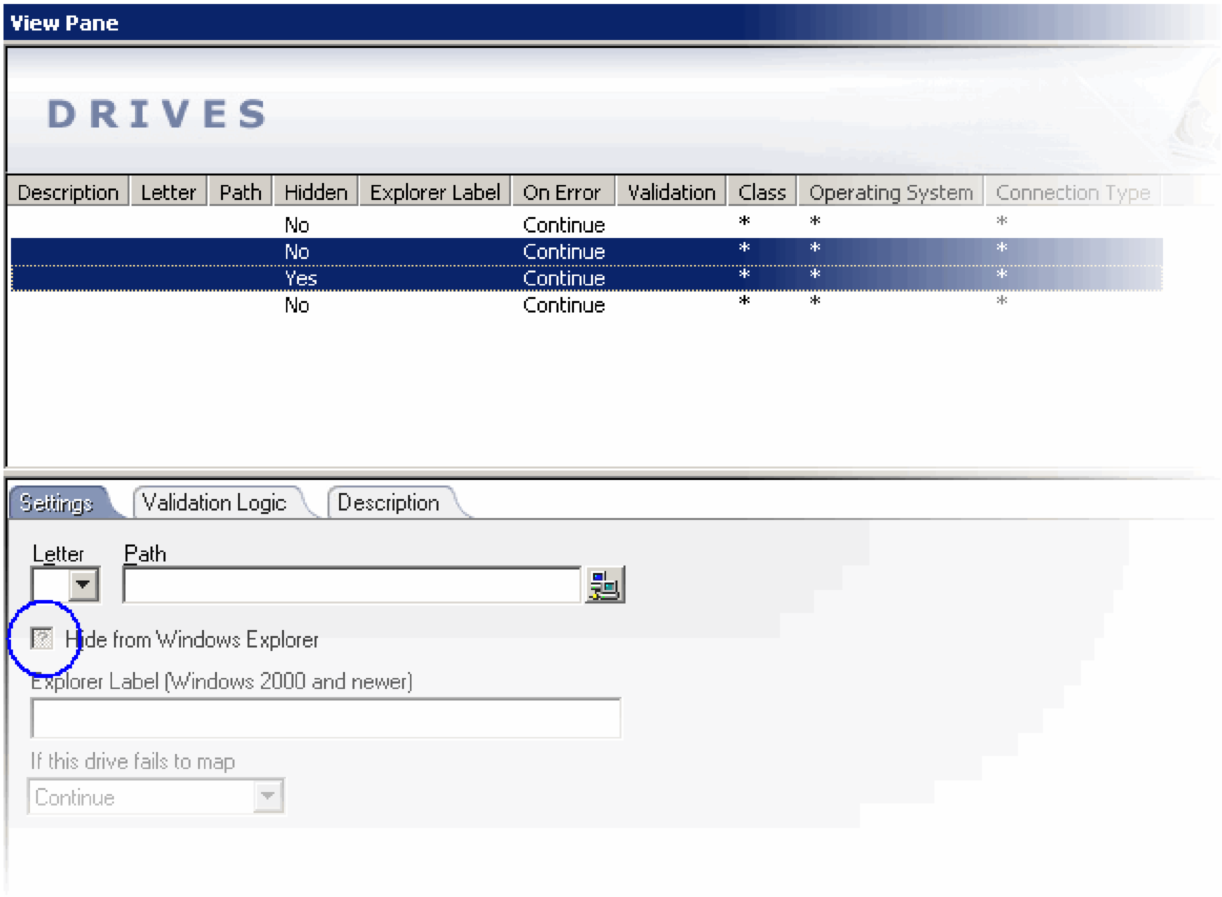
   New Element will insert a new configuration element at the bottom of the list. New Element at Selection will insert a new configuration element above the currently selected element in the list.

   A configuration element may also be added to the list by selecting New Element from the Edit menu.

Modifying Configuration Elements

Modifying a configuration element is simple. Once the element is selected in the configuration list, the Settings tab will automatically display the settings for the element. Change as needed.

Multiple elements may be modified together. Select multiple elements using the standard Windows techniques. Select all elements in a list by pressing CTRL-A or by selecting Select All from the Edit menu. Once the elements are selected, their settings will be shown on the Settings tab. Any control on the settings tab that have different values for all selected elements will clear the value from display. Check boxes with different values will display ▨.



Description	Letter	Path	Hidden	Explorer Label	On Error	Validation	Class	Operating System	Connection Type
			No		Continue		*	*	*
			No		Continue		*	*	*
			Yes		Continue		*	*	*
			No		Continue		*	*	*

Letter

Path

▨ Hide from Windows Explorer

Explorer Label (Windows 2000 and newer)

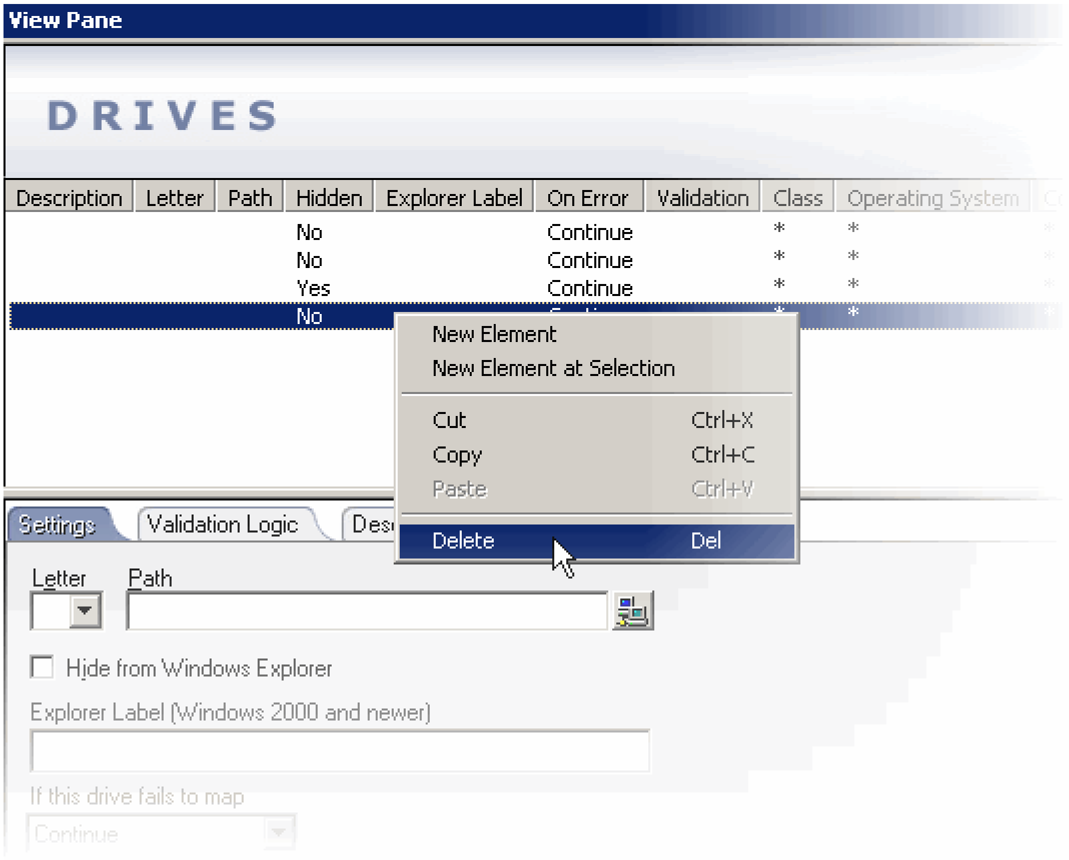
If this drive fails to map

Continue

Deleting Configuration Elements

To delete a configuration element,

1. Right-click on an element in the configuration list.
2. Select Delete from the shortcut menu.



Description	Letter	Path	Hidden	Explorer Label	On Error	Validation	Class	Operating System
			No		Continue		*	*
			No		Continue		*	*
			Yes		Continue		*	*
			No				*	*

Letter

Path

□ Hide from Windows Explorer

Explorer Label (Windows 2000 and newer)

If this drive fails to map

Continue

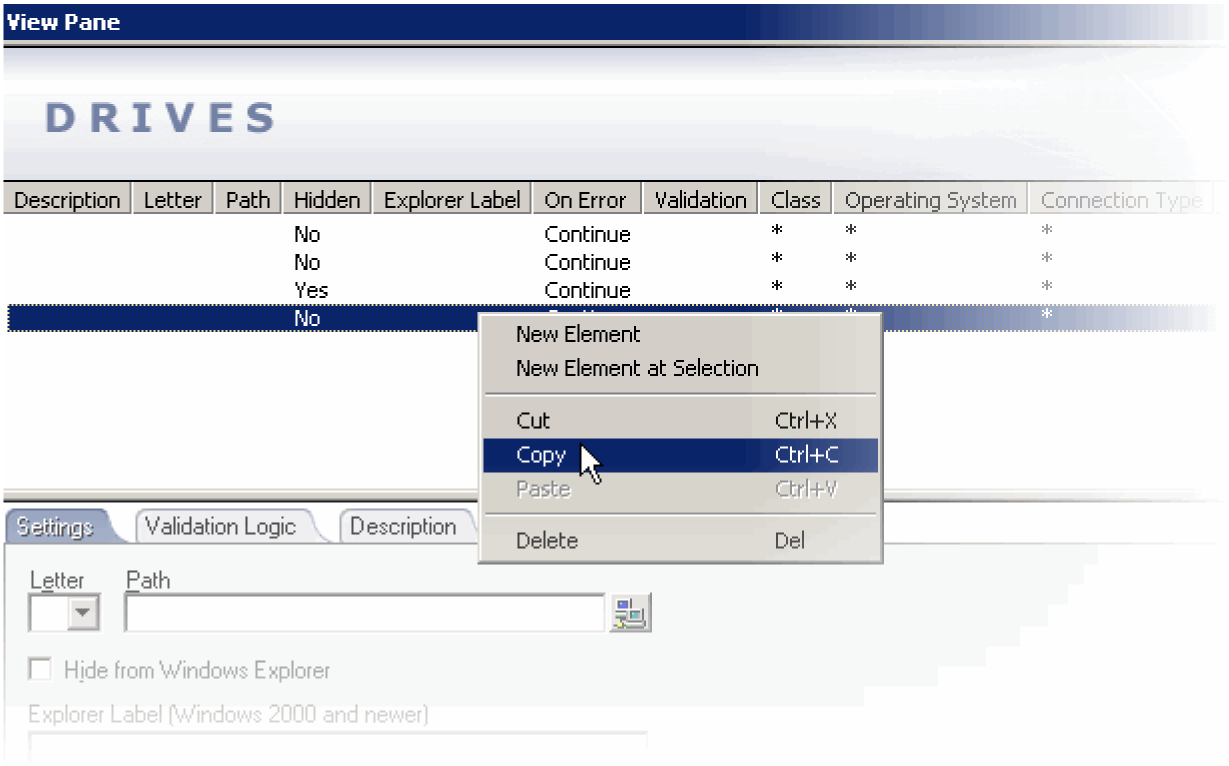
The element is immediately removed from the list.

Configuration elements may also be deleted by pressing the DEL key after selecting the element or by selecting Delete from the Edit menu. Select multiple elements for deletion using the standard Windows techniques. Select all elements in a list by pressing CTRL-A or by selecting Select All from the Edit menu.

Copying Configuration Elements

To copy a configuration element,

1. Right-click on an element in the configuration list.
2. Select Copy from the shortcut menu.



Description	Letter	Path	Hidden	Explorer Label	On Error	Validation	Class	Operating System	Connection Type
			No		Continue		*	*	*
			No		Continue		*	*	*
			Yes		Continue		*	*	*
			No						*

Letter Path

☐ Hide from Windows Explorer

Explorer Label (Windows 2000 and newer)

3. Paste the element into a new position in the list by right-clicking in the configuration list. Select Paste from the shortcut menu.

   A configuration element may also be copied by selecting the element in the configuration and choosing Copy and Paste from the Edit menu or by pressing CTRL-C and CTRL-P. One or more configuration elements may be copied and pasted into a configuration list. Select multiple configuration elements using the standard Windows techniques. Select all elements in a list by pressing CTRL-A or by selecting Select All from the Edit menu. Copied element(s) may be pasted into any other profile and must be pasted into the same object type.

Moving Configuration Elements

Elements within the configuration list are processed in the order they appear in the list. To change the order of any elements in the list,

Select the element to move by clicking on it. Holding the left mouse button down, drag the element to the location it will be moved to and drop it by releasing the left mouse button.

or

Placement of a configuration element can also be changed by clicking or on the toolbar. This will move an element up one or down one in the configuration list.

Configuring Elements

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

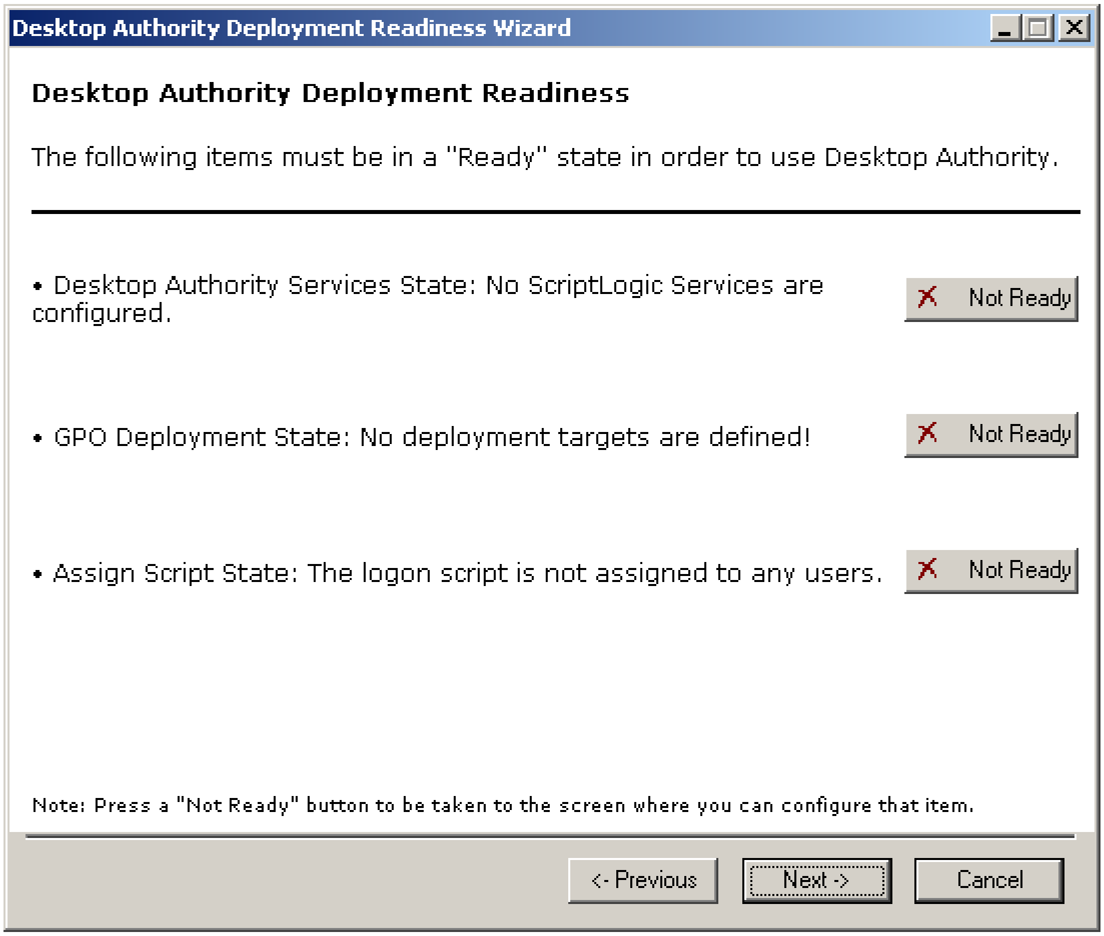
Description tab

Enter text on the Description tab to be used as an explanation for the configuration entry. The description defaults to the Default Description defined in Preferences on the Edit tab.

System Readiness Wizard

The Desktop Authority System Readiness Wizard helps to determine the ready state of Desktop Authority. This wizard will determine if the Desktop Authority Services are configured, check for GPO Deployment, Logon Scripts, Computer Exceptions, Troubleshooting options and Data Collection configurations.

The Readiness Wizard will automatically start the first time the Manager is run, following installation. It can be restarted at any time by selecting **Launch Readiness Wizard** from the File menu.



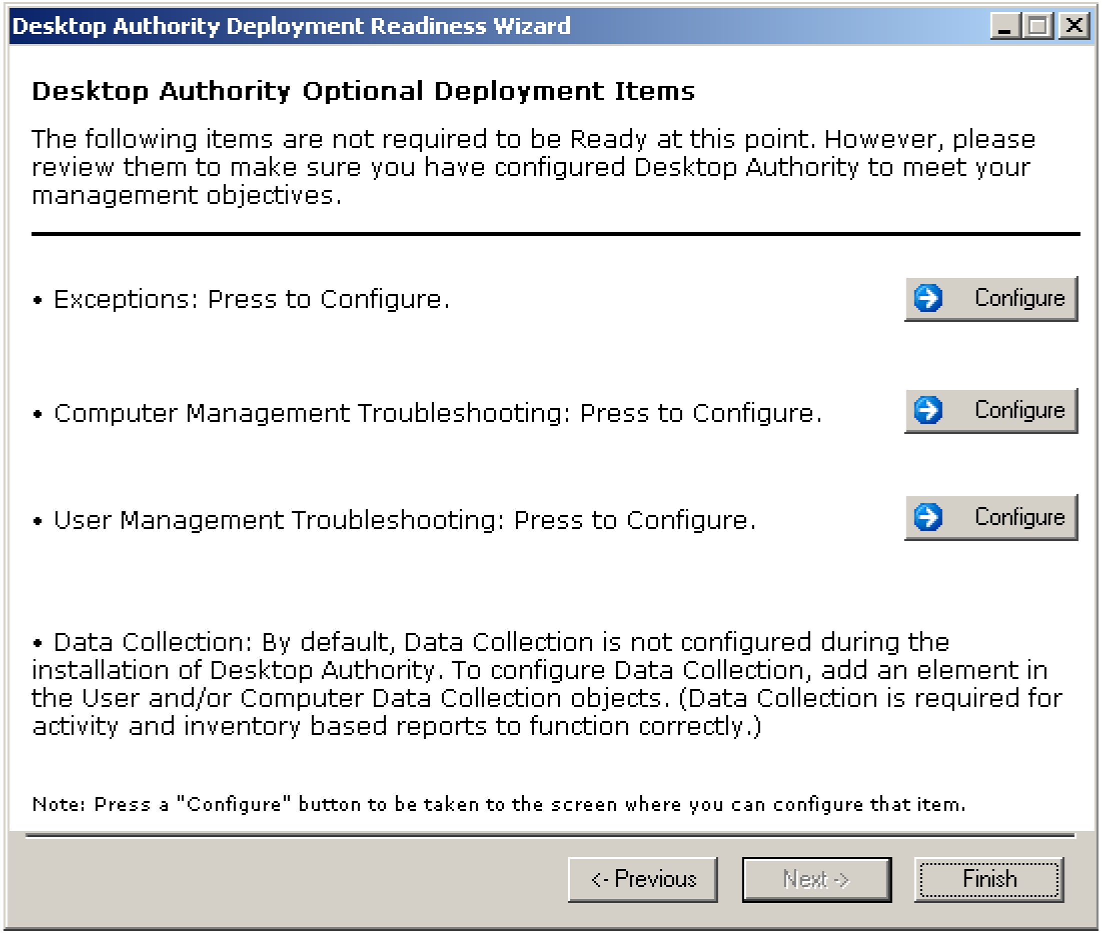
Desktop Authority Deployment Readiness

The following items must be in a "Ready" state in order to use Desktop Authority.

- Desktop Authority Services State: No ScriptLogic Services are configured. ✗ Not Ready
- GPO Deployment State: No deployment targets are defined! ✗ Not Ready
- Assign Script State: The logon script is not assigned to any users. ✗ Not Ready

Note: Press a "Not Ready" button to be taken to the screen where you can configure that item.

System Readiness Wizard Page 1



Desktop Authority Deployment Readiness Wizard

Desktop Authority Optional Deployment Items

The following items are not required to be Ready at this point. However, please review them to make sure you have configured Desktop Authority to meet your management objectives.

- Exceptions: Press to Configure.
- Computer Management Troubleshooting: Press to Configure.
- User Management Troubleshooting: Press to Configure.
- Data Collection: By default, Data Collection is not configured during the installation of Desktop Authority. To configure Data Collection, add an element in the User and/or Computer Data Collection objects. (Data Collection is required for activity and inventory based reports to function correctly.)

Note: Press a "Configure" button to be taken to the screen where you can configure that item.

System Readiness Wizard Page 2

The Readiness Wizard will determine the state of each component and allow you to click a button which directs you to the specific Desktop Authority dialog in which to configure the component.

Desktop Authority Services — This configuration check determines:

- There is at least one up to date ScriptLogic service, installed and configured within the enterprise.
- The existing configured Update service(s) are up to date and running.
- There is at least one valid User Management replication target.
- There is at least one valid Computer Management replication target.

GPO Deployment State — This configuration check determines:

- There is at least 1 GPO deployment target defined.

Assign Script State — This configuration check determines:

- There are no SLOGIC logon scripts assigned to any users in the domain.

Exceptions State — Defining computer exceptions is an optional part of the Desktop Authority deployment.

Computer Management Troubleshooting — Computer Management Troubleshooting is an optional part of the Desktop Authority deployment. It is used to troubleshoot problems arising from objects/elements that are being applied on client machines. When configured, verbose trace files will be written to each client's %windir%\Temp\Desktop Authority folder, by default. This folder can be changed to another location within the Troubleshooting tab.

User Management Troubleshooting — User Management Troubleshooting is an optional part of the Desktop Authority deployment. It is used to troubleshoot problems arising from objects/elements that are being applied on client machines. When configured, verbose trace files will be written to each client's %temp%\Desktop Authority temp folder, by default. This folder can be changed to another location within the Troubleshooting tab.

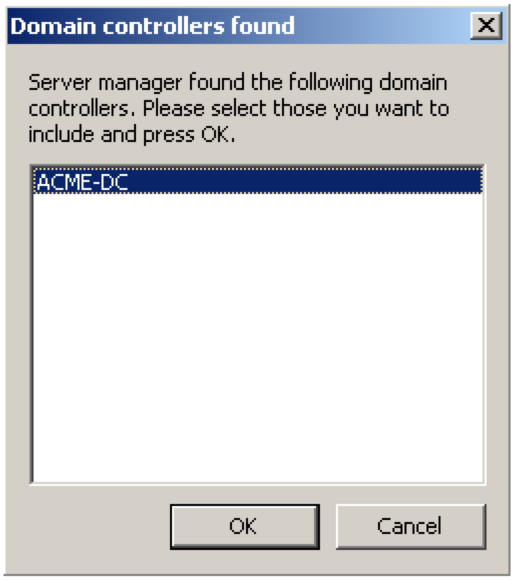
Data Collection — By default, Data Collection is not enabled. It can easily be enabled by adding a Data Collection element to any profile. Add a Computer Management Data Collection element to track Hardware, Software, Patch Management, Anti-Spyware and USB/Port Security information. Add a User Management Data Collection element to track user session (logon, logoff, lock and unlock) information.

Desktop Authority Readiness Wizard - Configure the Desktop Authority Services

Configuring the ScriptLogic Service

The configuration of the ScriptLogic service is required in order to use Desktop Authority.

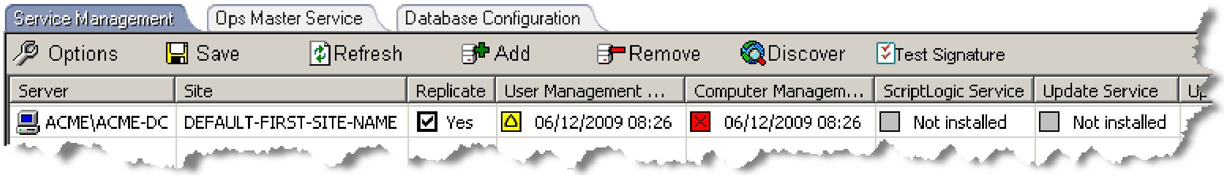
Click the Not Ready button to configure the necessary Desktop Authority services. The Server Manager dialog will be opened within the Desktop Authority Manager. The network will automatically be searched for available domain controllers. They will be presented, if found in a box similar to the one below.



Server manager found the following domain controllers. Please select those you want to include and press OK.

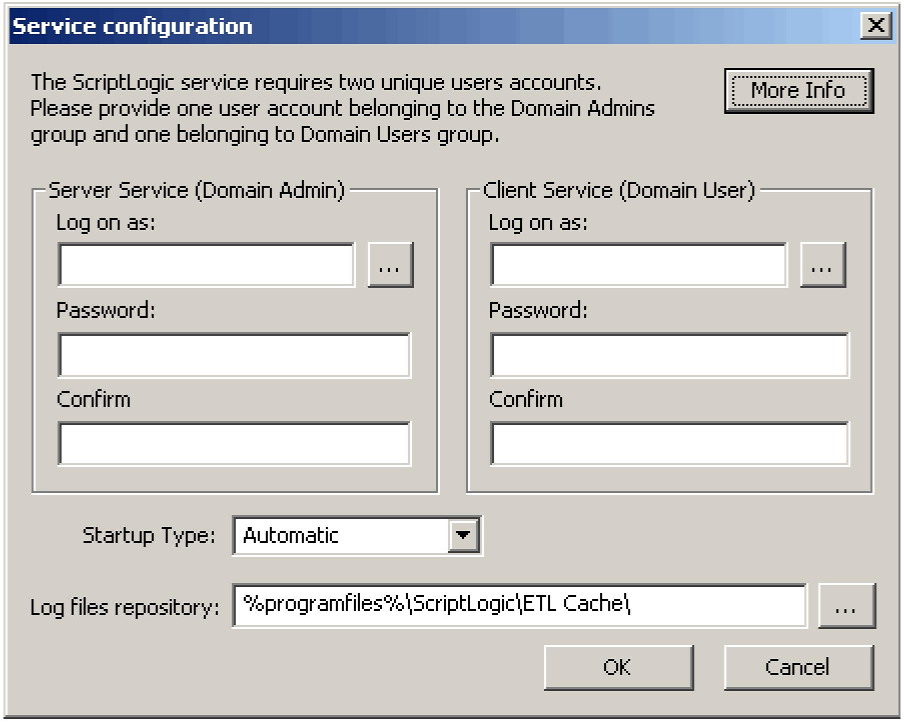
ACME-DC

Click **OK** to add the selected Domain Controllers to Server Manager.



Server	Site	Replicate	User Management ...	Computer Managem...	ScriptLogic Service	Update Service	Up
ACME\ACME-DC	DEFAULT-FIRST-SITE-NAME	☑ Yes	⚠ 06/12/2009 08:26	☒ 06/12/2009 08:26	□ Not installed	□ Not installed	

Right-click on a ScriptLogic Service cell to configure the service for a single domain controller installation. Click on the column header to select all domain controllers in the list, then right-click in the column to install the service for all selected domain controllers. Select Install from the pop-up menu. The ScriptLogic Service configuration dialog appears.



Service configuration

The ScriptLogic service requires two unique users accounts. Please provide one user account belonging to the Domain Admins group and one belonging to Domain Users group.

Startup Type: Automatic

Log files repository: %programfiles%\ScriptLogic\ETL Cache\

Two unique sets of user credentials must be supplied on the service configuration dialog. The Server Service account must have local administrative rights on each workstation. By default, the Domain Admins group is a member of the local Administrators group on each 2000/XP/2003/Vista workstation, so selecting a user account that belongs to the Domain Admins group would satisfy this requirement. This account will be used by the ScriptLogic service on each server to remotely install the ScriptLogic service on each workstation.

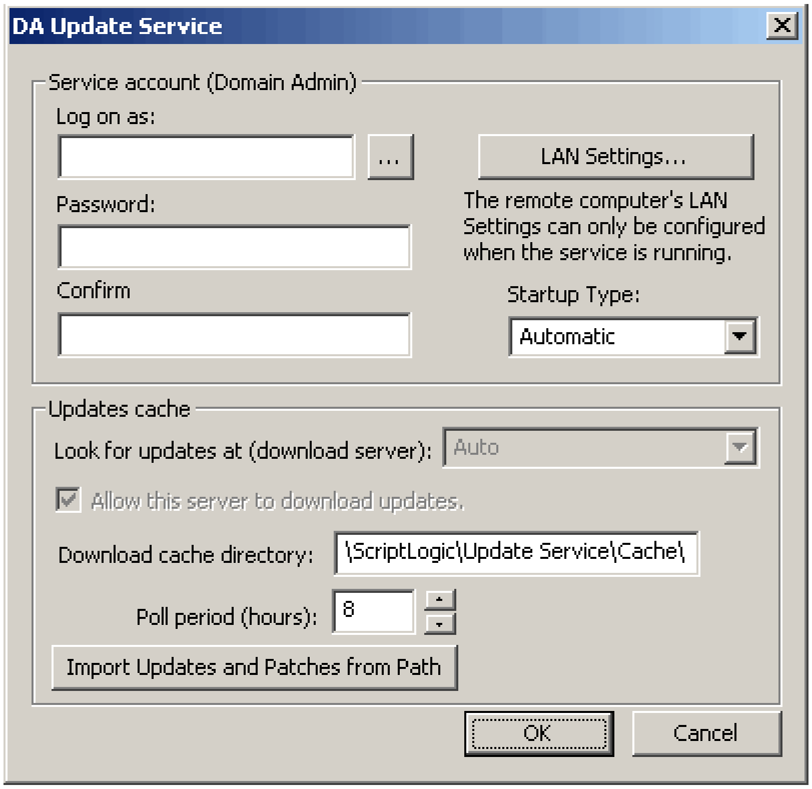
The Client Service account will be used by the ScriptLogic Client service on each workstation to perform the actual tasks that require the elevated administrative rights. This user account only needs to be a member of the Domain Users group. Installing this service to all domain controllers is the preferred action for this service and provides the best configuration for load balancing.

Once the user accounts are defined, click OK to start the service. You will see it in the Server Manager grid with a yellow then green icon next to it. A green icon indicates the service is installed and running.

Configuring the Update Service

The next service to configure is the **Update Service**. This is only required if your enterprise requires the use of USB/Port Security, Software Management, Patch Management or Anti-Spyware. If this functionality will not be used, the Update service is not required to be installed.

Right-click on a Update Service cell to configure the service for a single domain controller installation. Click on the column header to select all domain controllers in the list, then right-click in the column to install the service for all selected domain controllers. Select Install from the pop-up menu. The Update Service configuration dialog appears.



The remote computer's LAN Settings can only be configured when the service is running.

Startup Type: Automatic

Look for updates at (download server): Auto

☑ Allow this server to download updates.

Download cache directory: \ScriptLogic\Update Service\Cache\

Poll period (hours): 8

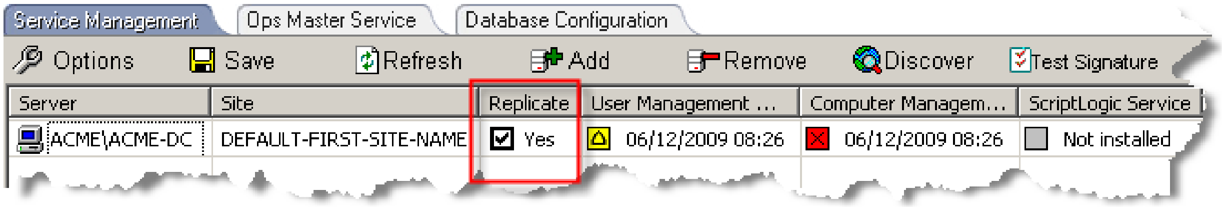
The Update service requires the use of a single user account. This user account must be a Local Administrator on the server where the Update service is being installed to.

The most important item to know about the Update service is that it can act as a Download server and/or a Distribution point. If there is only a single server configured in Server Manager, the deployed Update server must act as both the Download and Distribution server. However, if there are multiple servers, it must be decided which servers will act as Download servers and which as Distribution servers. Please note that the Download Cache Directory could point to some other server, thus the user account requires Local Admin rights on that server also.

Best practices for configuring the Update service for your Enterprises configuration, locate the Update Service Best Practices topic in the Administrators Guide. The Administrators Guide is available for download on the ScriptLogic website.

Replication Targets

Replication is the act of publishing the configurations made in the Manager out to the network and available to the clients, users and computers, when necessary. By default, User Management configurations are pushed out to the NETLOGON share on specified domain controllers. Computer Management configurations are pushed out to the SYSVOL\%domain%Policies\Desktop Authority\Device Policy Master folder. There must be at least one domain controller configured as a replication target on the domain. To configure choose one or more domain controllers to act as replication targets by selecting the Replicate checkbox in Server Manager.



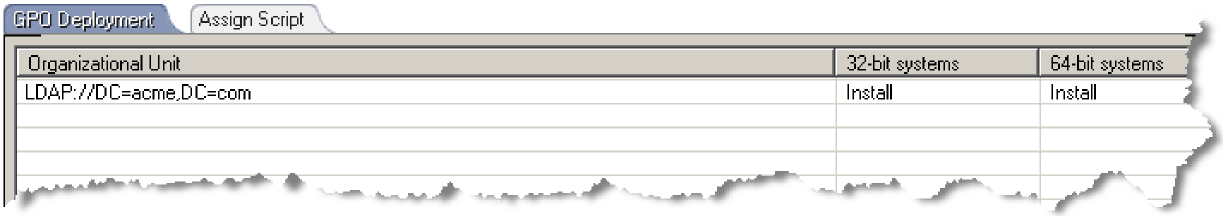
Server	Site	Replicate	User Management ...	Computer Managem...	ScriptLogic Service
ACME\ACME-DC	DEFAULT-FIRST-SITE-NAME	☑ Yes	⚠ 06/12/2009 08:26	☒ 06/12/2009 08:26	□ Not installed

Desktop Authority Readiness Wizard - Configure GPO Deployment

GPO Deployment is a required part of the Desktop Authority installation and is used to deploy the necessary client files to the computers that will be managed by Desktop Authority.

GPO Deployment is configured by specifying target OUs that contain the machines to be managed by Desktop Authority. Any computer that is not contained in the target OUs will not be able to be managed by Desktop Authority. GPO Deployment will push out and install an MSI file to each computer in the targeted OU(s). The MSI file contains Desktop Authority's User and Computer Management components and must be installed to every computer that is to be managed by Desktop Authority.

If GPO Deployment status in the Readiness Wizard is Not Ready, click the button to configure it. The GPO Deployment tab will be displayed in the Manager.



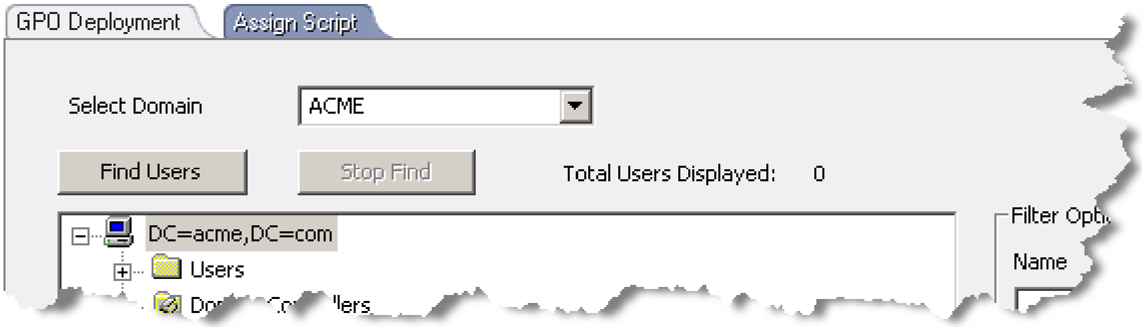
Organizational Unit	32-bit systems	64-bit systems
LDAP://DC=acme,DC=com	Install	Install

Click **Add** to run the GPO Deployment Wizard and select the OU(s) to deploy the client components to. All computers within the selected OUs will receive the client files.

Desktop Authority Readiness Wizard - Configure Assign Script state

Assigning Scripts 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 settings from Computer Management profiles and objects are not required to have a logon script defined.

If the organization will be using User Management configurations, click on the Not Ready button to configure the Assign Script State. The Assign Script tab will be displayed in the Manager.



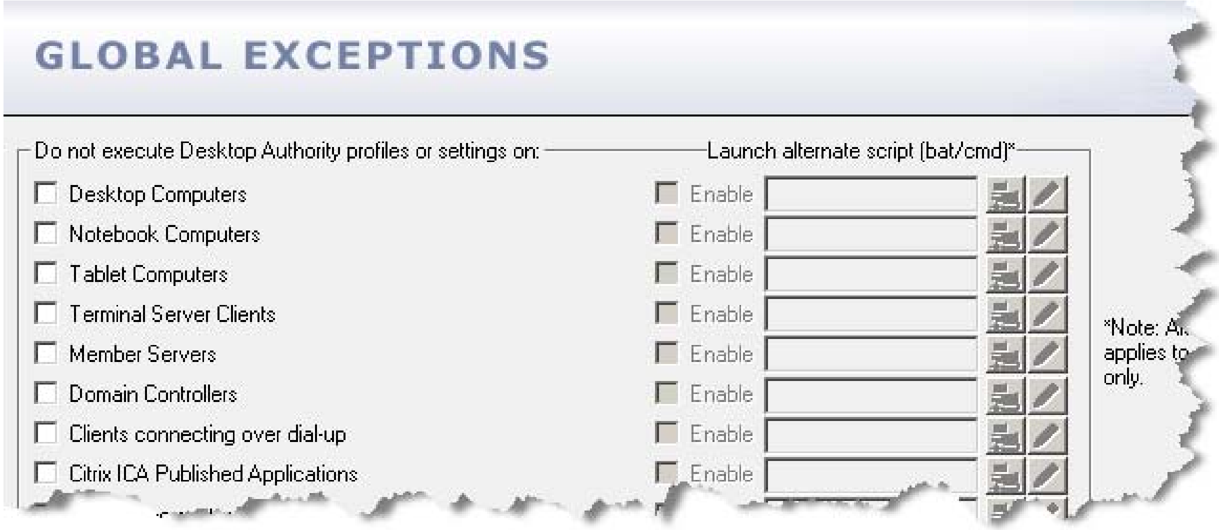
Select Domain: ACME

Total Users Displayed: 0

First the users must be found in the User List. Users may be searched by using the filter options to the right of the User List. Users will appear in the list on the bottom half of the Assign Script dialog. Select each user and click the **Assign Script** button.

Desktop Authority Readiness Wizard - Configure Exceptions

By default, Desktop Authority will be deployed to all computers in the targeted OU for GPO Deployment. Exceptions are used to exclude specific computers from being managed by Desktop Authority. This exclusion will specifically stop any Desktop Authority files from being installed to the specified computer. Click the **Configure** button to create exceptions. The Global Exceptions dialog will be displayed in the Manager.



GLOBAL EXCEPTIONS

Do not execute Desktop Authority profiles or settings on:

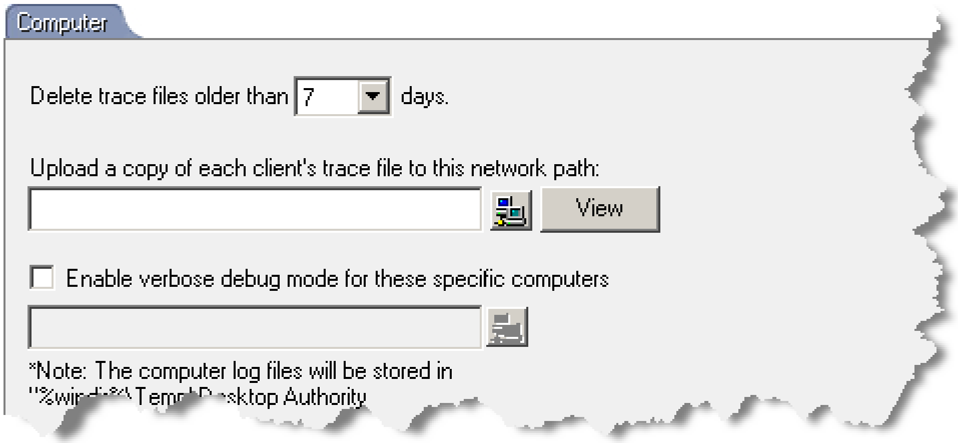
- ☐ Desktop Computers — Launch alternate script (bat/cmd)*: ☐ Enable
- ☐ Notebook Computers — ☐ Enable
- ☐ Tablet Computers — ☐ Enable
- ☐ Terminal Server Clients — ☐ Enable
- ☐ Member Servers — ☐ Enable
- ☐ Domain Controllers — ☐ Enable
- ☐ Clients connecting over dial-up — ☐ Enable
- ☐ Citrix ICA Published Applications — ☐ Enable

*Note: A... applies to... only.

Exceptions can be chosen by the class of computer (Desktop, Notebook, Domain Controller, etc.) as well as by specific computer name. To name specific computers, select Specific Computers and list each computer name delimited by a semicolon (;). Wildcards may also be used.

Desktop Authority Readiness Wizard - Configure Computer Management Troubleshooting

Computer Management Troubleshooting State is an optional configuration which is used to define several settings that are used to troubleshoot problems with objects/elements that are being applied on one or more client machines. 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. Click the **Configure** button on the Readiness Wizard to configure Computer Management Troubleshooting settings.



Delete trace files older than 7 days.

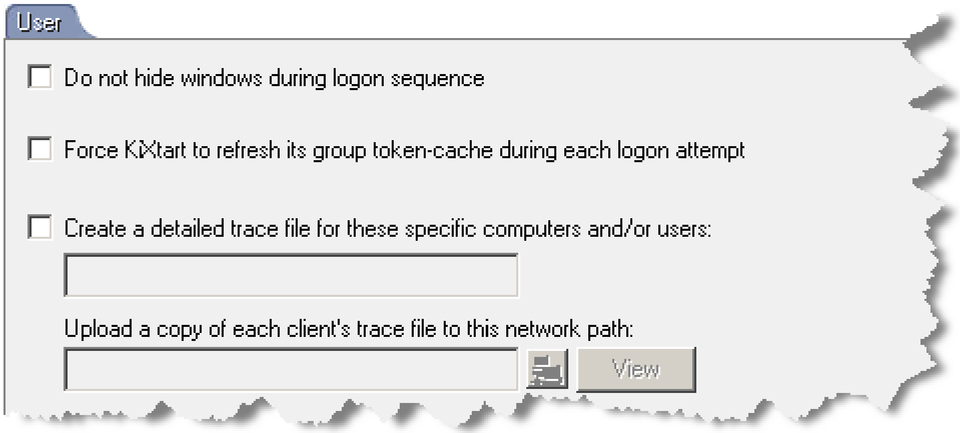
Upload a copy of each client's trace file to this network path:

□ Enable verbose debug mode for these specific computers

*Note: The computer log files will be stored in "%windir%\Temp\Desktop Authority

Desktop Authority Readiness Wizard - Configure User Management Troubleshooting

User Management Troubleshooting State is an optional configuration which is used to define several settings that are used to troubleshoot problems with objects/elements that are being applied on one or more client machines. 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. Click the **Configure** button on the Readiness Wizard to configure User Management Troubleshooting settings.



□ Do not hide windows during logon sequence

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

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

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

The last step in the Desktop Authority Readiness Wizard is the configuration of Data Collection.

By default, the installation of Desktop Authority does not configure any Data Collection settings. If the enterprise will be collecting and making use of this type of data for reports, it should be configured.

Desktop Authority can be configured to collect computer specific data including hardware and software inventory data, Patch Management, Anti-Spyware and USB/Port Security data from the computers and users that it manages. Data is also collected about user sessions, including session start and end and session lock and unlock.

All of this data is consumed by the Reporting module and puts this vital information at the administrator’s fingertips.

Data collection is configured at both the Computer and User management profile level. It can be configured to collect data virtually any way the administrator wants. Simply add one or more elements to either the Computer Management profiles, User Management profiles or both.

Once Desktop Authority publishes these settings, data will begin to be collected for the specified events and will be available to the Reporting module.

Click **Finish** to complete the Readiness Wizard and begin exploring the Desktop Authority Manager.

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.

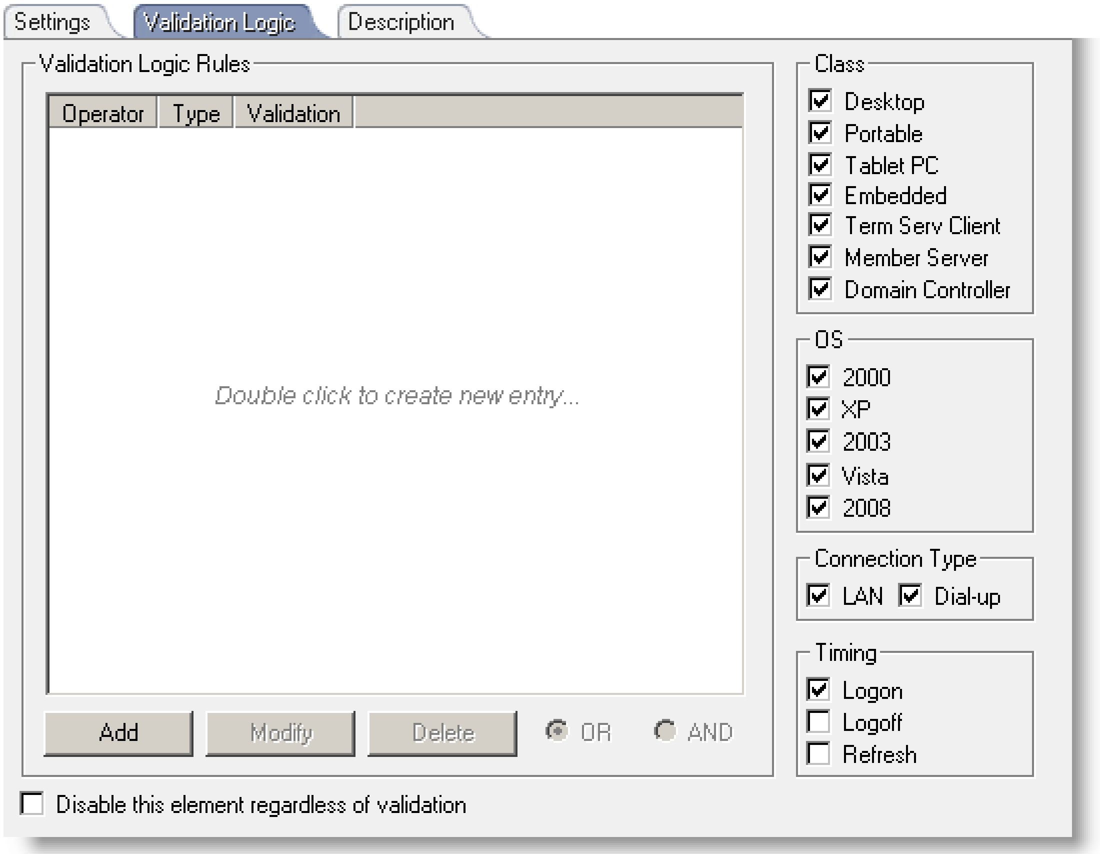
User Management Validation Logic includes settings for different Validation types, classes, operating systems, connection types, and timing options for Logon, Logoff, Refresh, Shut down and Desktop timing.

Computer Management Validation Logic includes settings for different Validation types, classes, operating systems and timing options for Startup, Shutdown, Refresh, and Scheduled intervals.

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.

The figure below is a snapshot of the dialog used to define validation logic for a profile or configuration element. Use the boxes to the right of the Validation Logic Rules list to define the specific classes, operating systems and connection types (not applicable to Computer Management objects) and timing (timing is on a separate tab for the Computer Management objects) that the rules will apply to. Double click on the validation logic rules list or press one of the buttons below it to add, change or delete rules to/from the list.

When the Validation Logic 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.



● OR ○ AND

Class
☑ Desktop
☑ Portable
☑ Tablet PC
☑ Embedded
☑ Term Serv Client
☑ Member Server
☑ Domain Controller

OS
☑ 2000
☑ XP
☑ 2003
☑ Vista
☑ 2008

Connection Type
☑ LAN ☑ Dial-up

Timing
☑ Logon
□ Logoff
□ Refresh

□ Disable this element regardless of validation

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.

USER MANAGEMENT VALIDATION LOGIC

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.

Listed below are the validation logic types that can be selected in the validation logic box.

Network Membership

Authenticating Domain

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.

Computer Domain

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 Resource Browser 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.

Computer Group

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 Resource Browser button, , to locate it. If the computer logging on is part of the supplied group, the configuration element and/or profile will be processed.

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

Examples:

Floor2Group	Validates true for all computers in the Floor2Group (all computers on the second floor).
PC2*	Validates true for all computers in any group starting with a PC2 prefix.
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)

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 groups of the OntarioGrp

OU (User)

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.

Primary Group

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 Resource Browser 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.

Site

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.

User Group

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

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 Resource Browser 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.

Computer Information

Computer Name

Select Computer Name in order to execute a configuration element for the specific computer regardless of the user that logs onto that 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 Resource Browser 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

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 acme.com.

MAC Address

Select MAC Address in order to execute a configuration element for a specific computer regardless of the user that logs onto that computer. 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 user that logs onto the machine or 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)

TCP/IP Address

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.

File Exists

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

Select File Version in order to execute a configuration element for the specific computer regardless of the user that logs onto that 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 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

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 between192.168.100.5 and 192.168.100.50, inclusive.

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

IPv6 Range

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 between10:0:0:0:0:0:0:1 and 10:0:0:0:0:0:0:10, inclusive.

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

Registry Key Exists

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.
10::1/112	

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

Registry Value Exists

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

Select Registry Value in order to execute a configuration element for the specific computer regardless of the user that logs onto that computer. 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 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 for the specific computer regardless of the user that logs onto that computer. Find the Virtual Environment Validation Logic type under the Computer Information category.

Select VMWare Virtual Machine 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.

Platform Type

Select Platform Type in order to execute a configuration element for the specific computer regardless of the user that logs onto that computer. Find the Platform Type Validation Logic type under the Computer Information category.

Select Platform Type to enable validation checking based on the Operating System platform, 32 or 64 bit operating system. If the computer is running an operating system platform that matches one of the platforms selected, the configuration element will be processed.

Terminal Services

TS Application Name

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.

Note: 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.

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

TS Client Name

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.

TS Client TCP/IP Address

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.

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 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 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 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 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 computers whose IP address is in the range of 10.0.0.33.

TS Initial Program

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.

TS Session Name

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.

Custom Validation

Custom Function

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.

```
; ScriptLogic 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

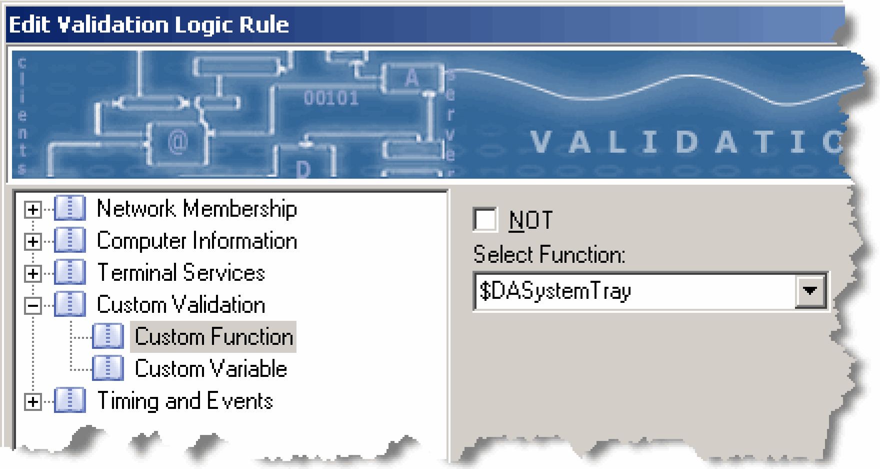
Select Custom Variable in order to execute a configuration element based on the value of the defined variable. Find the Custom Variable Validation Logic type under the Custom Validation category. Custom variables are defined in the profile's Definitions tab. All custom variables must evaluate to a TRUE 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.

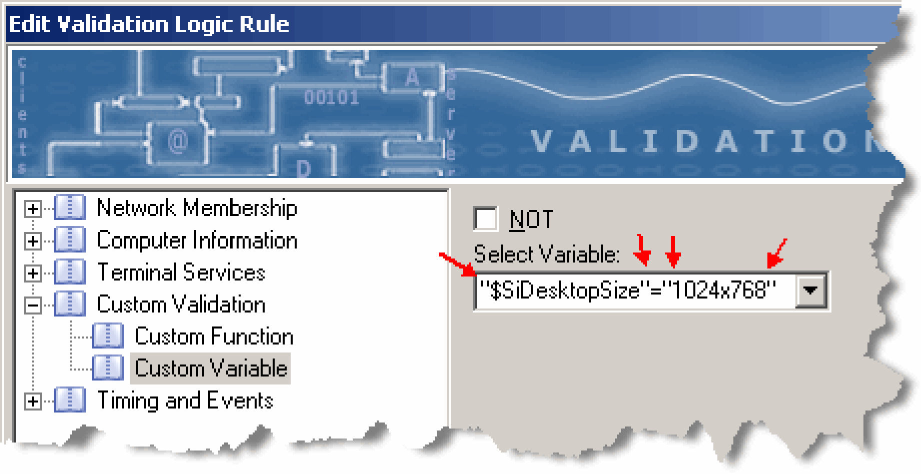
```
; ScriptLogic Custom Script File

; 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.



Select Function: $DASystemTray

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.



Select Variable: "$SiDesktopSize"="1024x768"

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

Timing and Events

Frequency

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.

Cycle

Select a time interval for which the element will validate. Choose from Everyday, 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 5th 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.

Frequency

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

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**.

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.

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. Tablet PCs run the Windows XP Tablet PC operating system.

Embedded

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

Term Serv Client

Use the **Term Serv Client** validation logic to execute a configuration element on a Terminal Server Client connection.

A resource is considered a Terminal Server Client if the operating system is Windows Server with Terminal Services installed and running in Application Server Mode.

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.

*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. There are two instances where the class of the computer may be incorrectly determined.

Operating System

2000

Check this box to execute an element if the computer is running the Windows 2000 operating system.

XP

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

2003

Check this box to execute an element if the computer is running the Windows 2003 operating system.

Vista

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

2008

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

Connection Type

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.

Timing

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.

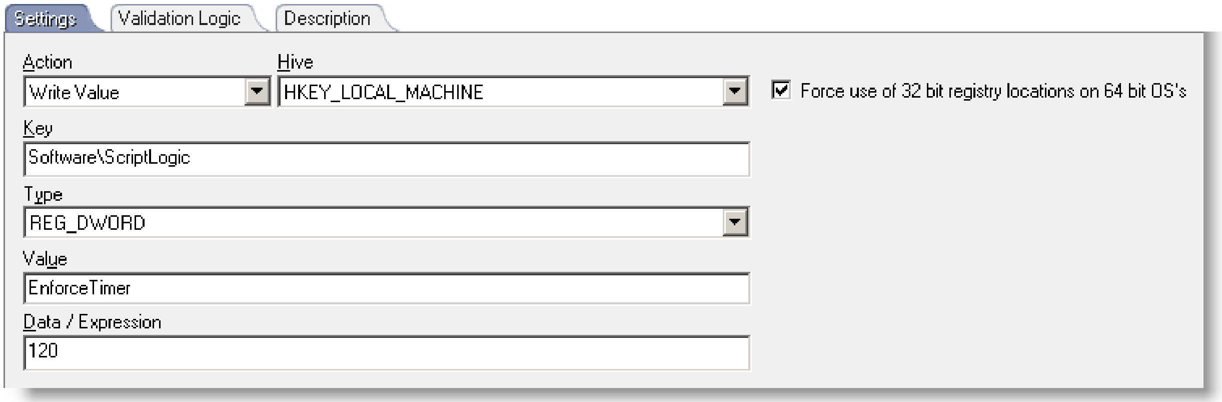
Shut down

Check this box to execute an element when the operating system is exited on a client computer.

Refresh

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 separate 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.



Action: Write Value

Hive: HKEY_LOCAL_MACHINE

☑ Force use of 32 bit registry locations on 64 bit OS's

Key: Software\ScriptLogic

Type: REG_DWORD

Value: EnforceTimer

Data / Expression: 120

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.

COMPUTER MANAGEMENT VALIDATION LOGIC

Timing

Startup

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

Shut down

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

Refresh

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. This can be changed, if needed, in the Computer Definitions object. The Computer Management Refresh Timing interval is separate from the User Management Refresh Timing interval.

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.

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.

Listed below are the validation logic types that can be selected in the validation logic box.

Network Membership

Computer Domain

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 Resource Browser 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.

Computer Group

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 Resource Browser button, , to locate it. If the computer logging on is part of the supplied group, the configuration element and/or profile will be processed.

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

Examples:

Floor2Group	Validates true for all computers in the Floor2Group (all computers on the second floor).
PC2*	Validates true for all computers in any group starting with a PC2 prefix.
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)

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 groups of the OntarioGrp

Site

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.

Computer Information

Computer Name

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 Resource Browser 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

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

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)

TCP/IP Address

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.

File Exists

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

Select File Version in order to execute a configuration element for a computer that has a specific file and version of that file. 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 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

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

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

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.
10::1/112	

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

Registry Value Exists

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

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 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 for the specific computer. Find the Virtual Environment Validation Logic type under the Computer Information category. Select VMWare Virtual Machine 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.

Platform Type

Select Platform Type in order to execute a configuration element for the specific computer. Find the Platform Type Validation Logic type under the Computer Information category.

Select Platform Type to enable validation checking based on the Operating System platform, 32 or 64 bit operating system. If the computer is running an operating system platform that matches one of the platforms selected, the configuration element will be processed.

Activity

Interactive User

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.

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. Tablet PCs run the Windows XP Tablet PC operating system.

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.

*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.

Operating System

2000

Check this box to execute an element if the computer is running the Windows 2000 operating system.

XP

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

2003

Check this box to execute an element if the computer is running the Windows 2003 operating system.

Vista

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

2008

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

Configuration

ScriptLogic Today

ScriptLogic Today provides product evaluation and registration information as well as links to the ScriptLogic web site. Within the ScriptLogic Today object links are provided to specific pages on the ScriptLogic web site, Home, Support, Knowledge base Articles, Custom Scripting, and the API Library.

These areas of the ScriptLogic web site provide access to technical information and help about ScriptLogic's products.

Home

The ScriptLogic web site's home page.

Support

The ScriptLogic web site's technical support page.

Knowledge base Articles

The ScriptLogic Knowledge base provides articles regarding common questions and issues. Search by article number, product or keywords to find information to help diagnose and solve product questions.

Custom Scripting

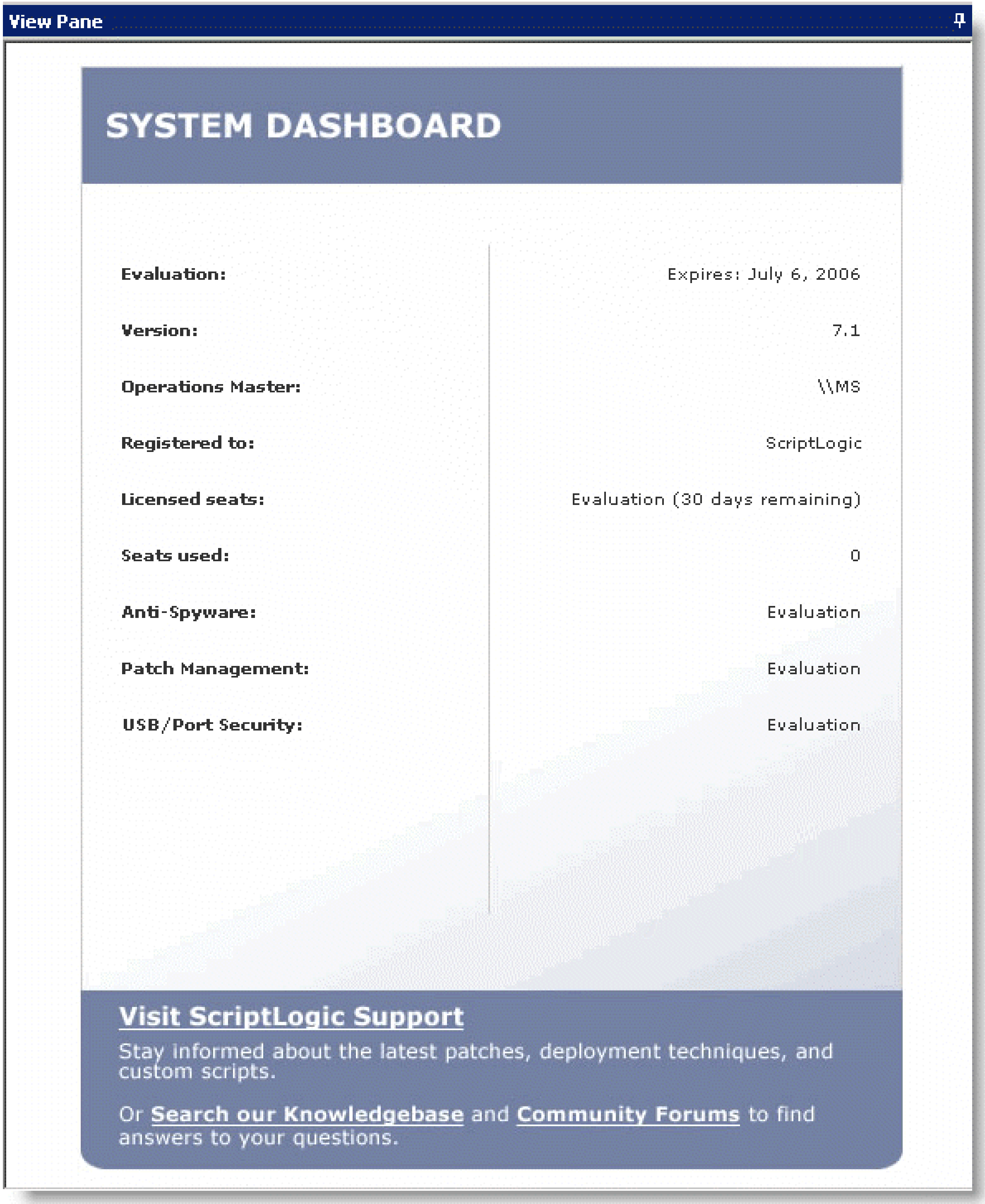
Although Desktop Authority provides virtually all core requirements right out of the box, it may be necessary to add additional functionality using custom scripts. Custom Scripts are written using the KiXtart scripting language. The Custom Scripting library provides many ready-to-use scripts that have been contributed by customers, certified partners and the ScriptLogic technical support team. Take a look through the library to see if a script has already been written to solve your needs.

API Library

An extensive API library is available for use in Desktop Authority. The API library includes an array of functions and variables that are ready to use with our solutions. Use API variables and functions in Custom Scripts, Global Definitions, Profile Definitions and within virtually every profile object.

System Dashboard

The System Dashboard provides product information including version and registration information. The Dashboard also provides links to the ScriptLogic web site.



SYSTEM DASHBOARD

Evaluation:	Expires: July 6, 2006
Version:	7.1
Operations Master:	\\MS
Registered to:	ScriptLogic
Licensed seats:	Evaluation (30 days remaining)
Seats used:	0
Anti-Spyware:	Evaluation
Patch Management:	Evaluation
USB/Port Security:	Evaluation

Visit ScriptLogic Support

Stay informed about the latest patches, deployment techniques, and custom scripts.

Or Search our Knowledgebase and Community Forums to find answers to your questions.

Product Name

The name of the installed product.

Version

The version of the installed product.

Evaluation/Maintenance

If evaluating the product, this is the date the evaluation version will expire. The evaluation is valid for 30 days from the installation date. If the product, along with maintenance has been purchased, this is the date the current maintenance will expire.

Operations Master

The Operations Master designates where Desktop Authority is installed to.

Registered To

The name of the company the product is registered to.

Licensed Seats

Displays the number of seats purchased.

Registered Users

The number of users the product is registered for. In evaluation mode, this will display the number of days remaining in the evaluation period.

Seats Used

Displays the number of seats used.

Anti-Spyware (not available for licensing with Desktop Authority Express)

The license period is shown. If evaluating Desktop Authority or the Anti-Spyware component, this will be set to Evaluation. When running a licensed Desktop Authority Express, this will be set to Not Licensed.

Patch Management (not available for licensing with Desktop Authority Express)

The license period is shown. If evaluating Desktop Authority or the Patch Management component, this will be set to Evaluation. When running a licensed Desktop Authority Express, this will be set to Not Licensed.

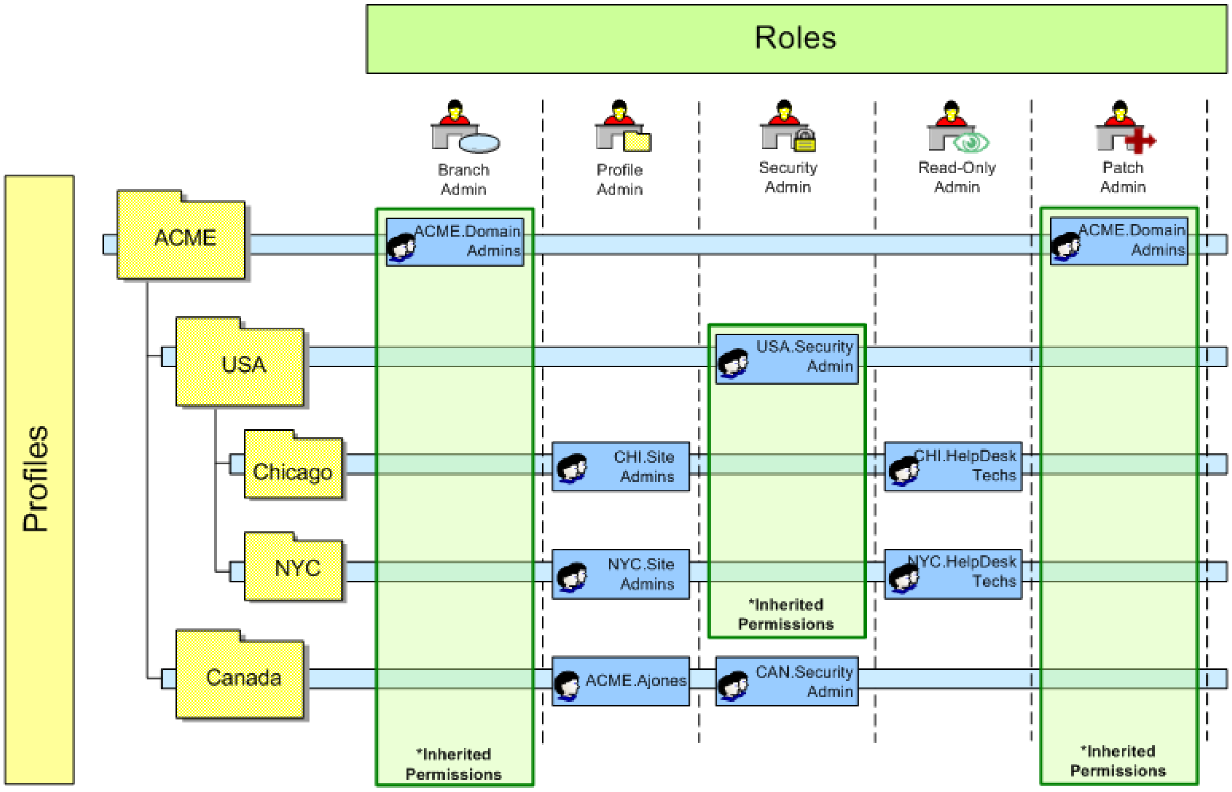
USB/Port Security (not available for licensing with Desktop Authority Express)

The license period is shown. If evaluating Desktop Authority or the USB/Port Security component, this will be set to Evaluation. When running a licensed Desktop Authority Express, this will be set to Not Licensed.

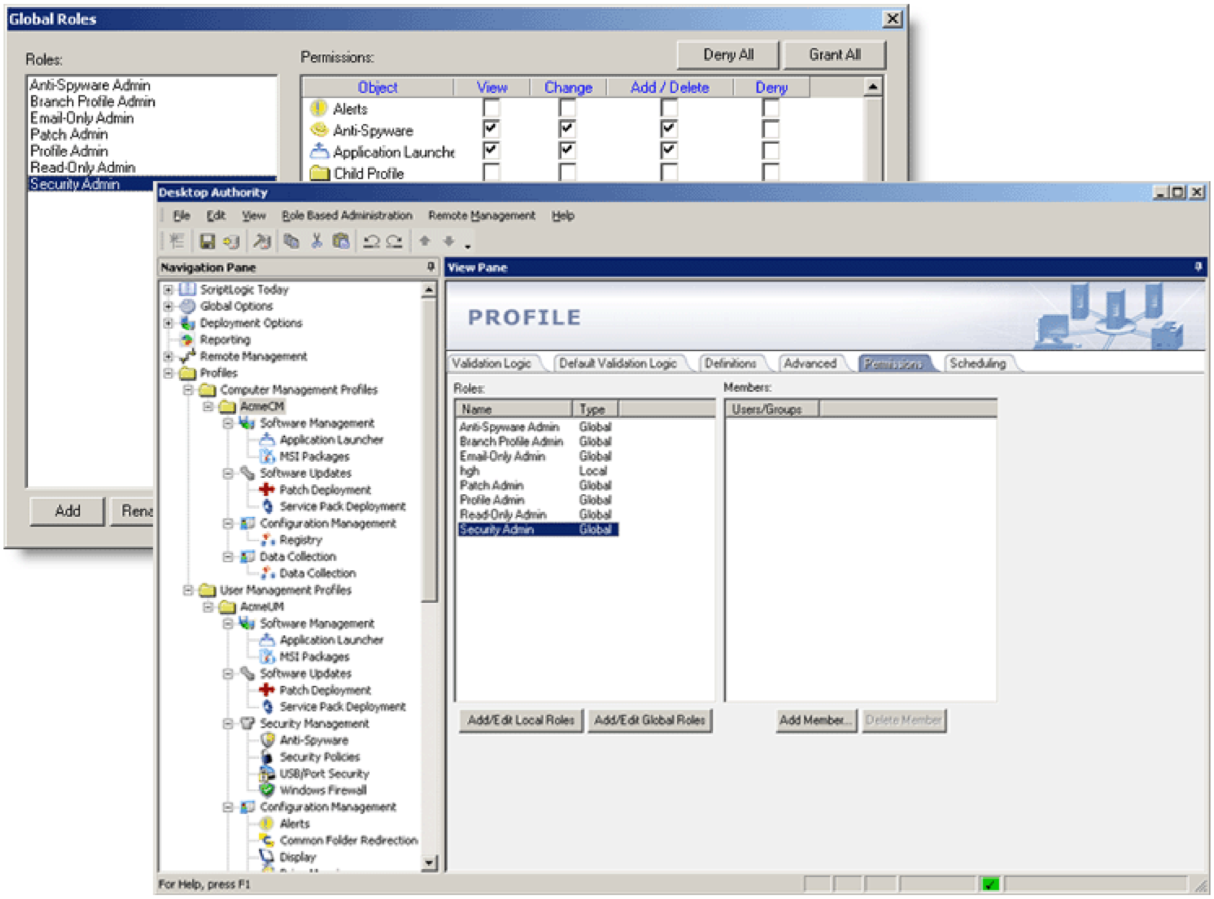
WHAT IS ROLE BASED ADMINISTRATION?

Role Based Administration (RBA) restricts Administrator 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.

A 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.



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.



Roles:

- Anti-Spyware Admin
- Branch Profile Admin
- Email-Only Admin
- Patch Admin
- Profile Admin
- Read-Only Admin
- Security Admin

Permissions:

Object	View	Change	Add / Delete	Deny
Alerts	□	□	□	□
Anti-Spyware	☑	☑	☑	□
Application Launche	☑	☑	☑	□
Child Profile	□	□	□	□

Roles:

Name	Type
Anti-Spyware Admin	Global
Branch Profile Admin	Global
Email-Only Admin	Global
hgh	Local
Patch Admin	Global
Profile Admin	Global
Read-Only Admin	Global
Security Admin	Global

Members:

Users/Groups

The illustrations above depict four default roles (created during installation of Desktop Authority) within the ACME Corporation. The default roles are Branch Admin, Profile Admin, Security Admin, Read-Only Admin and Patch Admin. Of course, this is just one small example. There are an endless number of ways RBA can be configured to suit an enterprise's administrative hierarchy, workflow, and segmentation of functional responsibilities.

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, lets say the Security Admin is responsible for pushing out newly released patches and is also responsible for maintaining current virus definition files as well as keeping an eye on various spyware attacks. The Security Admin role will be given permissions to the Patch Deployment, Registry, Application Launcher, Anti-Spyware 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.

Patch Admin

The Patch Admin role will be used for Users/Group who are responsible for testing and deploying new patches. In the ACME illustration above, the ACME.Domain.Admins are assigned to this role. Any Domain Admin in the domain can apply patches via Desktop Authority to any profile available in the domain.

Note: Permissions are cumulative at a given profile. This means then permissions of all roles which a user/group is a member are summed to define that user/groups total permissions on that profile, including permissions inherited from above. A user/group can be denied permission on a resource, irrespective of their cumulative inherited permissions, by assigning them to a role that grants Deny on that resource.

In some enterprises, the use of Role Based Administration may not be necessary. In this case, each user and/or group that will use Desktop Authority can just be added to the Super User/Group role.

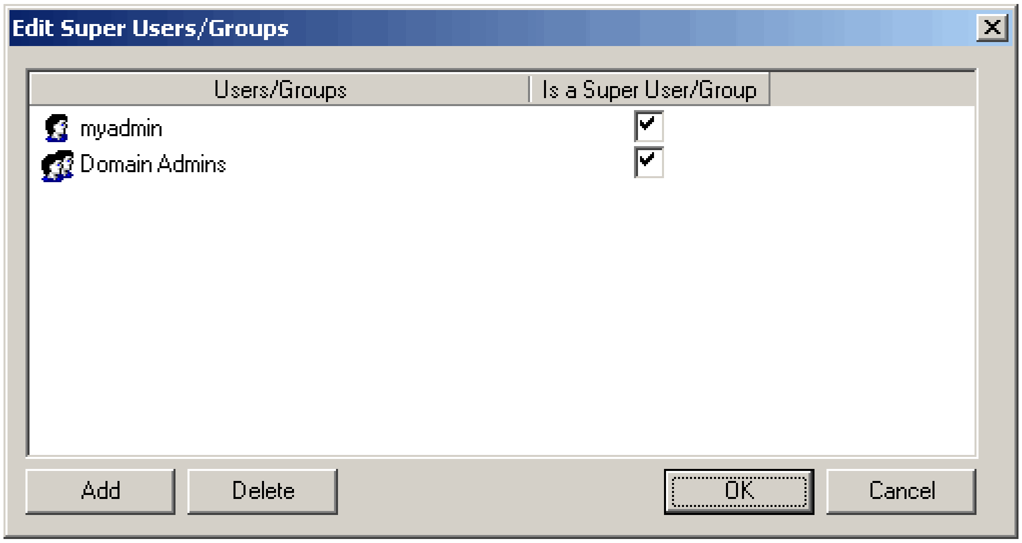
Configuring Super Users/Groups Accounts

What is a Super User/Group?

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

A default Super User/Group is added during the installation of Desktop Authority. Others may be added to the Super User/Group list by a Super User/Group.

To access the Super Users/Groups dialog, select Edit Super Users/Groups... from the Role Based Administration menu.



Users/Groups	Is a Super User/Group
myadmin	☑
Domain Admins	☑

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

Super Users/Groups can:

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

Creating a Super User/Group

To add a new user/group to the user list, click Add and select a user/group from the popup Resource Browser dialog.

Select a user/group from the list and click Delete to remove it.

To apply the Super User/Group attribute to a user account or group, access the Super User/Group dialog by selecting Edit Super Users/Groups... from the Role Based Administration menu. If the user/group that will be crowned Super User/Group exists in the list, simply select the Is a Super User/Group box for them. If the user or group is not yet in the Users/Groups list, add them. After adding the user, select the Is a Super User box for the user.

To remove the Super User/Group attribute from a user, simply clear the Is a Super User/Group box.

Click OK to save the changes made to the Super User/Group accounts. Click Cancel to exit the Super User/Group dialog without saving changes.

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.

Sample Role	Tasks	Required rights
Branch Admin	Oversee and configure profiles and clients,	SuperUser, 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 spyware, secure desktops and run applications.	Add, Change, Delete permissions to Anti-spyware, 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.
Patch Admin	Responsible for testing and deploying patches.	Add, Change, Delete permissions to Patch Deployment object.

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

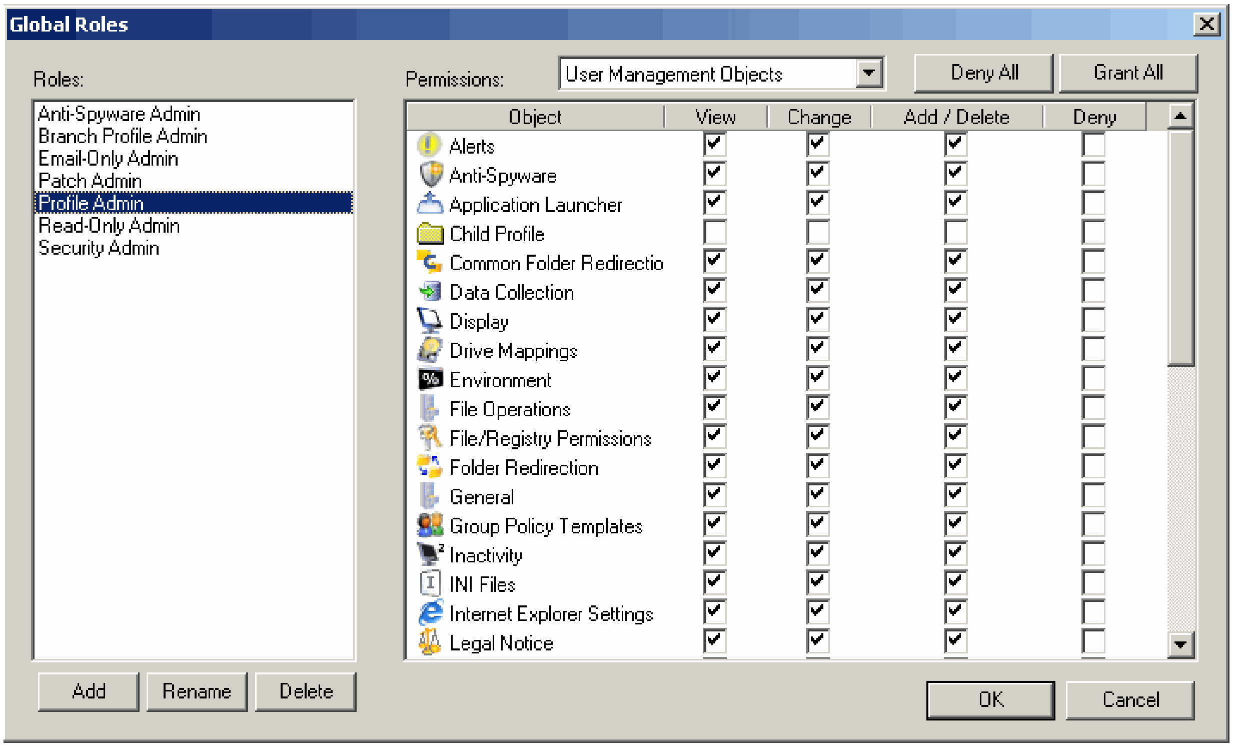
A local role is defined at the profile level and is available only to the profile to which it is defined in.

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 Role Based Administration menu selection. Select the Edit Global Roles menu item.

To create a new Role, click Add. Enter the name for the new role and click OK. Click Rename to change a role's name. Click Delete to remove an existing role. Once the new role is created, permissions must be assigned to it. View, Change, Add/Delete and Deny permissions can be configured for each profile object as well as profile configuration. Select User Management Objects or Computer Management Objects from the drop down box to give permissions to User and/or Computer based objects.



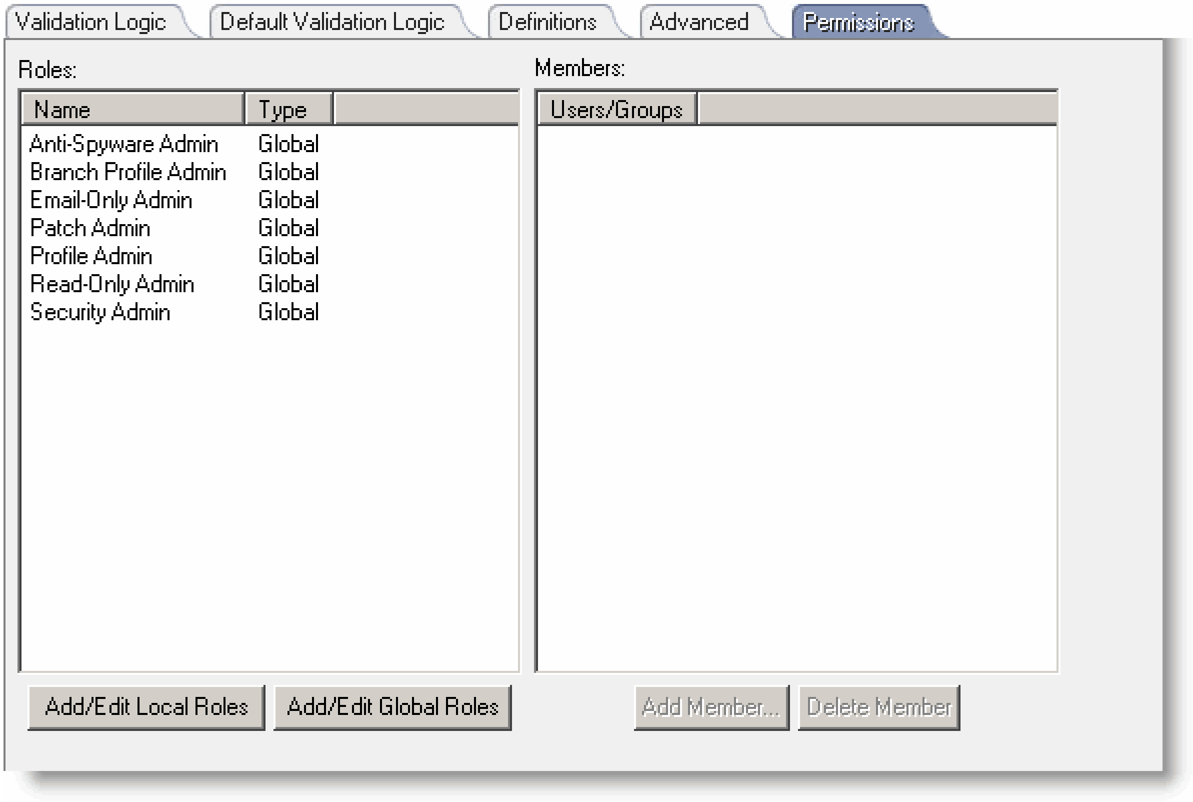
Roles:

- Anti-Spyware Admin
- Branch Profile Admin
- Email-Only Admin
- Patch Admin
- Profile Admin
- Read-Only Admin
- Security Admin

Permissions: User Management Objects

Object	View	Change	Add / Delete	Deny
Alerts	☑	☑	☑	□
Anti-Spyware	☑	☑	☑	□
Application Launcher	☑	☑	☑	□
Child Profile	□	□	□	□
Common Folder Redirectio	☑	☑	☑	□
Data Collection	☑	☑	☑	□
Display	☑	☑	☑	□
Drive Mappings	☑	☑	☑	□
Environment	☑	☑	☑	□
File Operations	☑	☑	☑	□
File/Registry Permissions	☑	☑	☑	□
Folder Redirection	☑	☑	☑	□
General	☑	☑	☑	□
Group Policy Templates	☑	☑	☑	□
Inactivity	☑	☑	☑	□
INI Files	☑	☑	☑	□
Internet Explorer Settings	☑	☑	☑	□
Legal Notice	☑	☑	☑	□

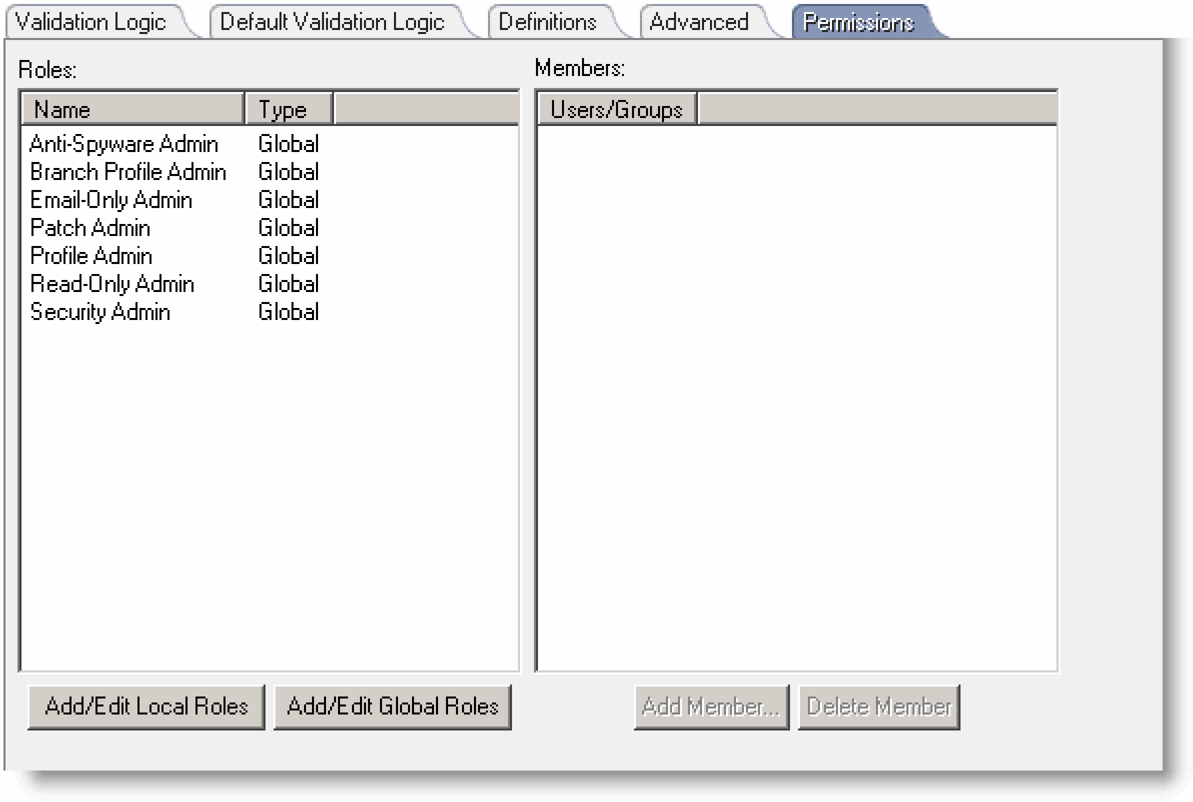
Global roles may also be created from within a profile. On the Permissions tab, click Add/Edit Global Roles. Only Super Users/Groups can create Global Roles.



Name	Type
Anti-Spyware Admin	Global
Branch Profile Admin	Global
Email-Only Admin	Global
Patch Admin	Global
Profile Admin	Global
Read-Only Admin	Global
Security Admin	Global

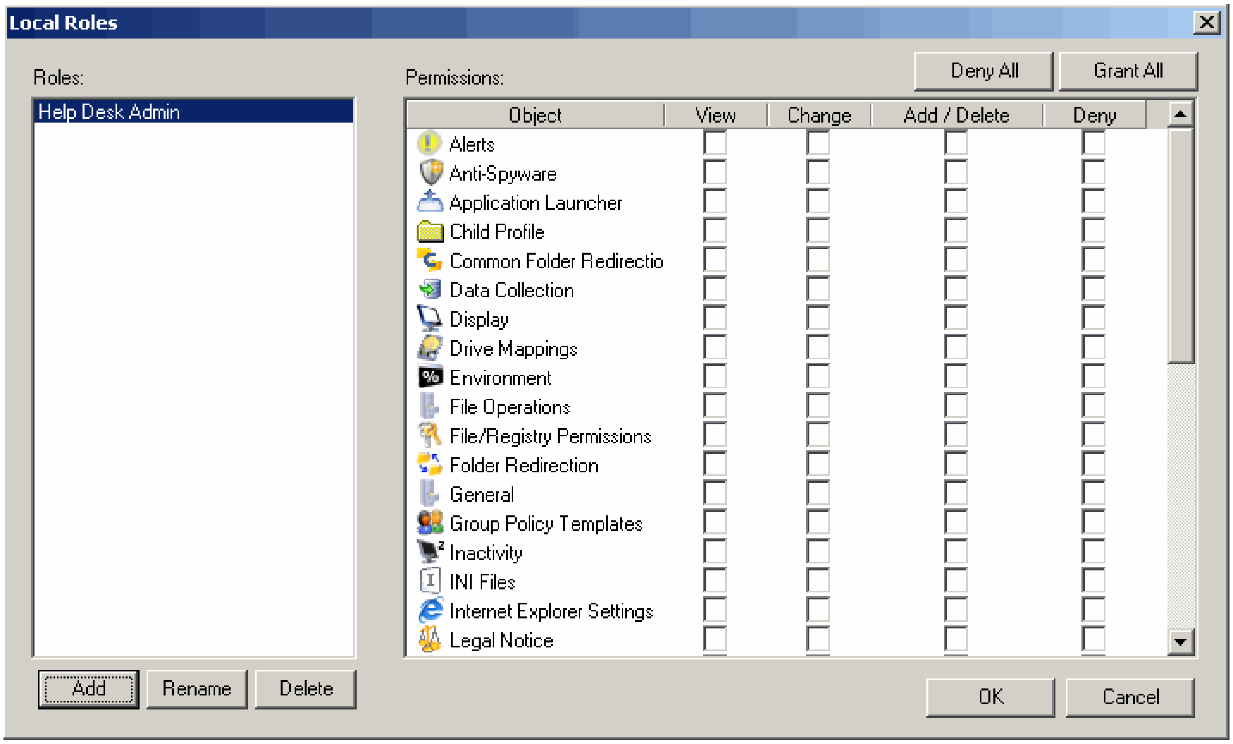
Configuring Local Roles

Local Roles are created from within a profile. Once the Profile is selected in the Navigation Pane, select the Permissions tab.



Name	Type
Anti-Spyware Admin	Global
Branch Profile Admin	Global
Email-Only Admin	Global
Patch Admin	Global
Profile Admin	Global
Read-Only Admin	Global
Security Admin	Global

To create a new Local Role, click Add/Edit Local Roles. If the profile selected is a Computer Management profile, the Local Roles dialog will display only the Computer Management objects. The same is true for User Management; if the profile selected is a User Management profile, the Local Roles dialog will display only the User Management objects.



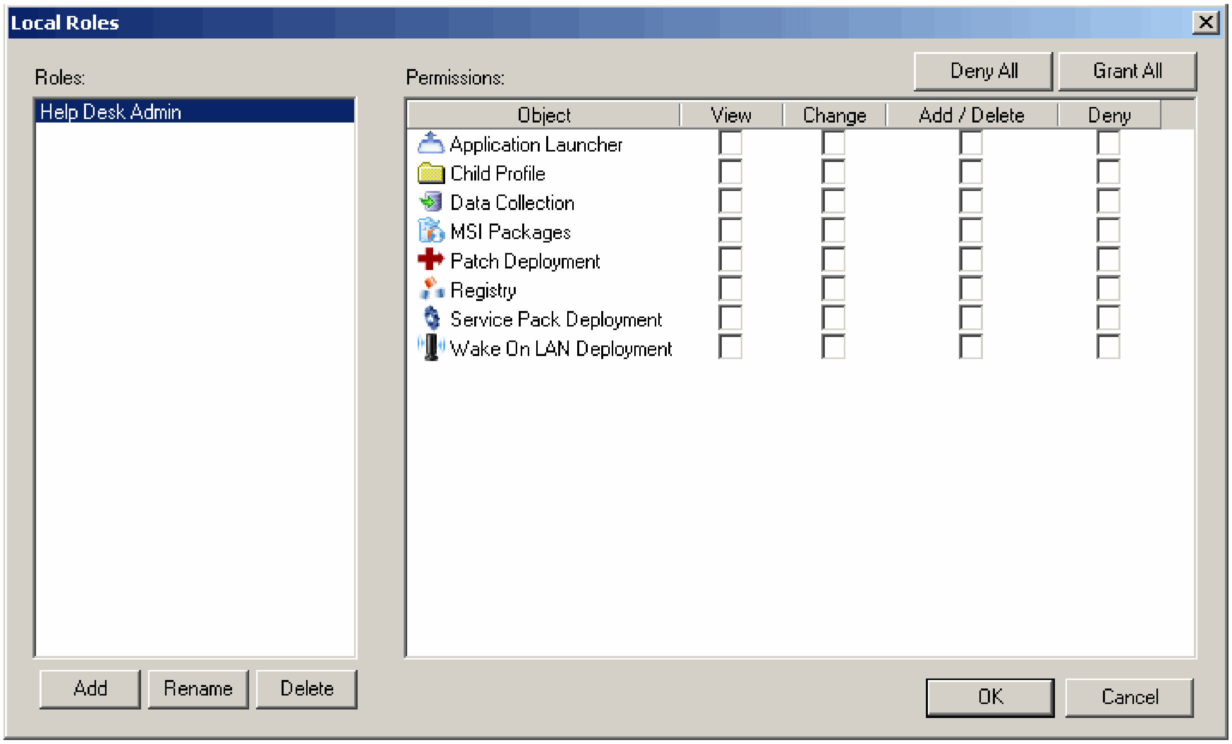
Roles:

Help Desk Admin

Permissions:

Object	View	Change	Add / Delete	Deny
Alerts	□	□	□	□
Anti-Spyware	□	□	□	□
Application Launcher	□	□	□	□
Child Profile	□	□	□	□
Common Folder Redirectio	□	□	□	□
Data Collection	□	□	□	□
Display	□	□	□	□
Drive Mappings	□	□	□	□
Environment	□	□	□	□
File Operations	□	□	□	□
File/Registry Permissions	□	□	□	□
Folder Redirection	□	□	□	□
General	□	□	□	□
Group Policy Templates	□	□	□	□
Inactivity	□	□	□	□
INI Files	□	□	□	□
Internet Explorer Settings	□	□	□	□
Legal Notice	□	□	□	□

Example of a Local Role for a User Management Profile



Roles:

Help Desk Admin

Permissions:

Object	View	Change	Add / Delete	Deny
Application Launcher	□	□	□	□
Child Profile	□	□	□	□
Data Collection	□	□	□	□
MSI Packages	□	□	□	□
Patch Deployment	□	□	□	□
Registry	□	□	□	□
Service Pack Deployment	□	□	□	□
Wake On LAN Deployment	□	□	□	□

Example of a Local Role for a Computer Management Profile

Click Add on the Local Roles dialog. Enter the name for the new role and click OK. To create a new Role, click Add. Enter the name for the new role and click OK. Click Rename to change a role's name. Click Delete to remove an existing role. Once the new role is created, permissions must be assigned to it. View, Change, Add/Delete and Deny permissions can be configured for each profile object as well as profile configuration.

Object Permissions

View

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

Change

Change 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

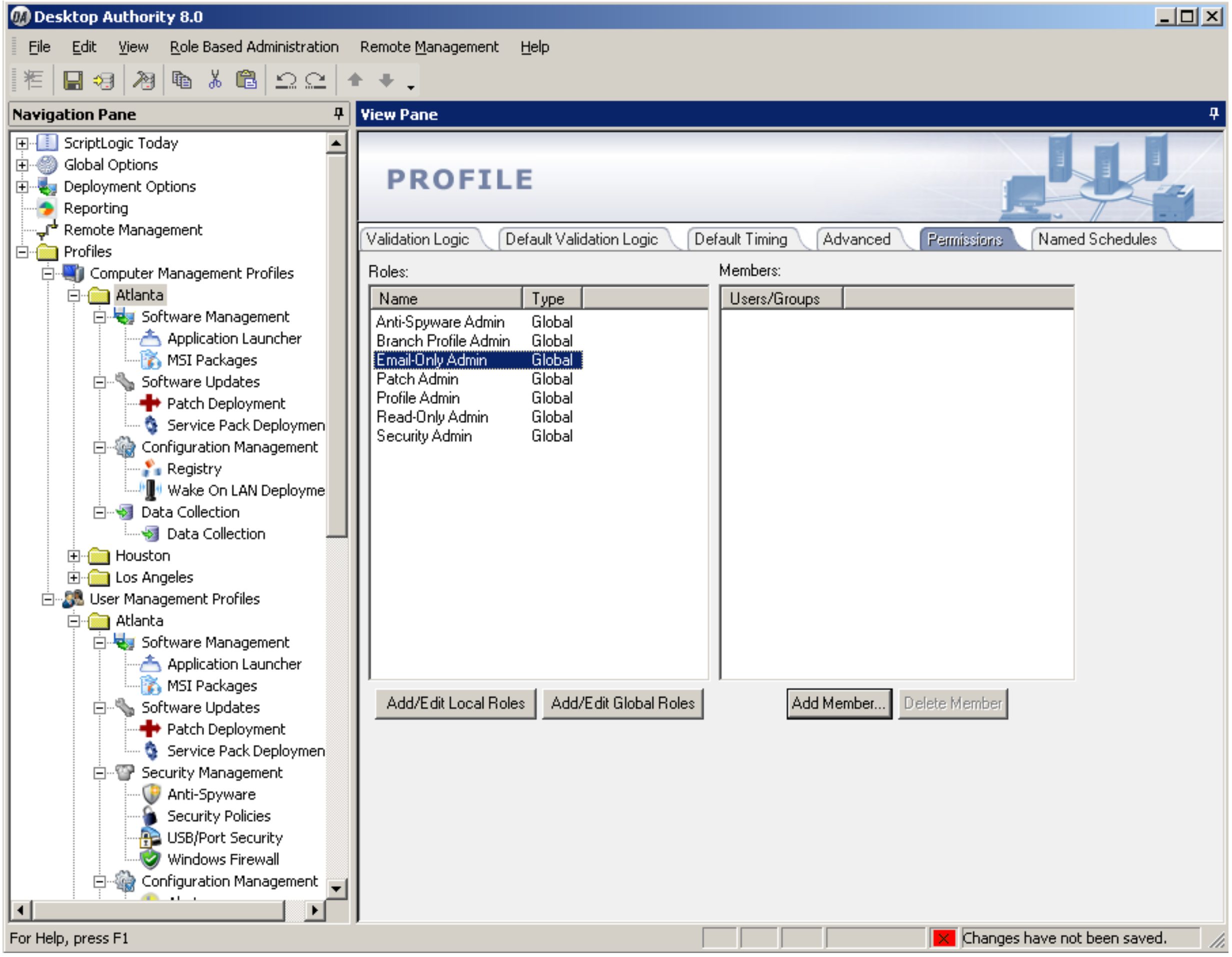
No access is permitted to the object selected in the permissions list. The object will not be visible in the navigation pane for any member that is a part of the role.

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



Name	Type
Anti-Spyware Admin	Global
Branch Profile Admin	Global
Email-Only Admin	Global
Patch Admin	Global
Profile Admin	Global
Read-Only Admin	Global
Security Admin	Global

Changes have not been saved.

Add/Edit Local Roles

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/Edit Global Roles

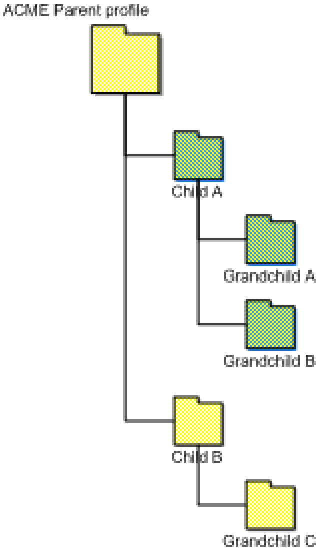
A global role is a defined role that is available to all profiles. To create a global Role, click Add/Edit Global Roles. The Global Roles dialog will open. For more information on Global Role configuration see the Configuring Roles topic.

Add/Delete members to/from roles

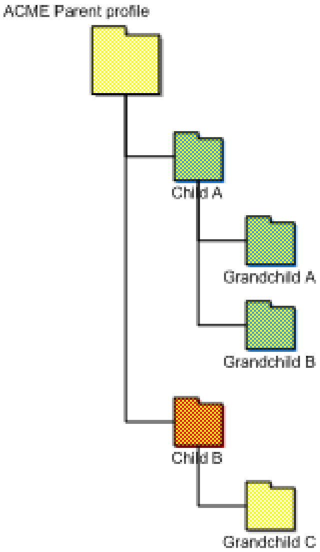
To add a member to a role, select the role from the Roles list. Click Add Member.... Select a user or group from the resource browser and click OK. To remove a member from a role, select the Role and Member and then click Delete Member.

Permission Inheritance

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



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.



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 options. 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.

Computer Management Options consists of Definitions and Troubleshooting options.

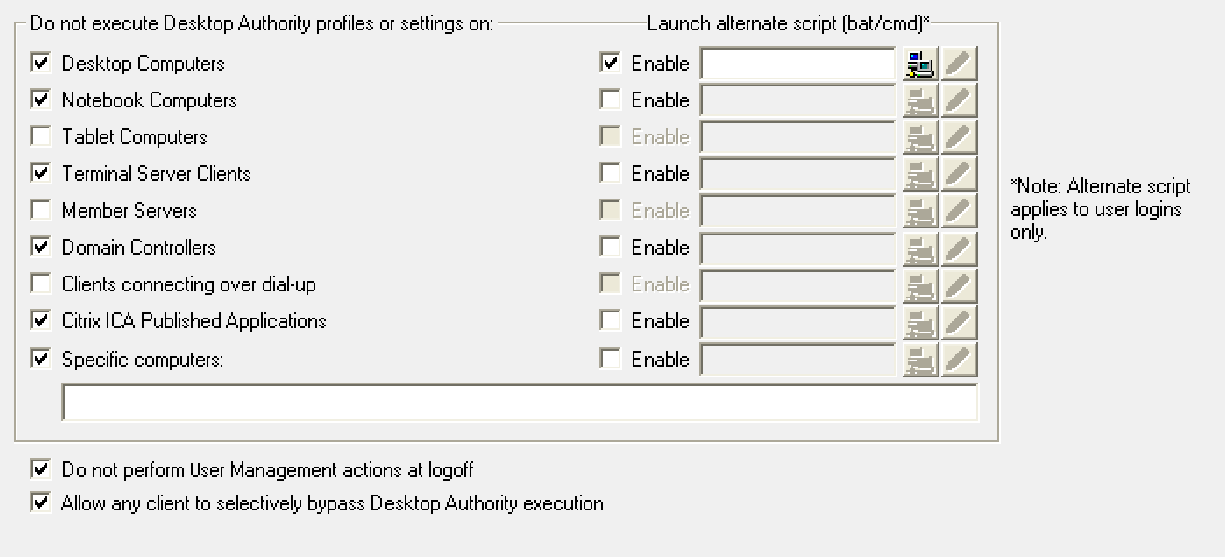
- **Definitions** The Definitions object is used to define custom dynamic variables. These variables may be used within any profile as well as in any custom script.
- **Troubleshooting** The Troubleshooting object is used to define several settings that can help to troubleshoot problem clients. The most 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.

EXCEPTIONS

The Exceptions object 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:	Launch alternate script (bat/cmd)*
☑ Desktop Computers	☑ Enable
☑ Notebook Computers	□ Enable
□ Tablet Computers	□ Enable
☑ Terminal Server Clients	□ Enable
□ Member Servers	□ Enable
☑ Domain Controllers	□ Enable
□ Clients connecting over dial-up	□ Enable
☑ Citrix ICA Published Applications	□ Enable
☑ Specific computers:	□ Enable

*Note: Alternate script applies to user logins only.

☑ Do not perform User Management actions at logoff

☑ Allow any client to selectively bypass Desktop Authority execution

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**, **Notebook Computers**, **Tablet Computers**, **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 multiple computer names using a semicolon (;). Wildcards may be used with the computer names.

Launch alternate script (bat/cmd)

Setting Alternate scripts 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 ▦ 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.

Using ▦ 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, ✎ is enabled. Clicking ✎ will allow editing of 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 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 timing validation logic settings. Only the ability to execute the profile/element at logoff or shut down will be disabled.

Allow any client to selectively bypass Desktop Authority execution

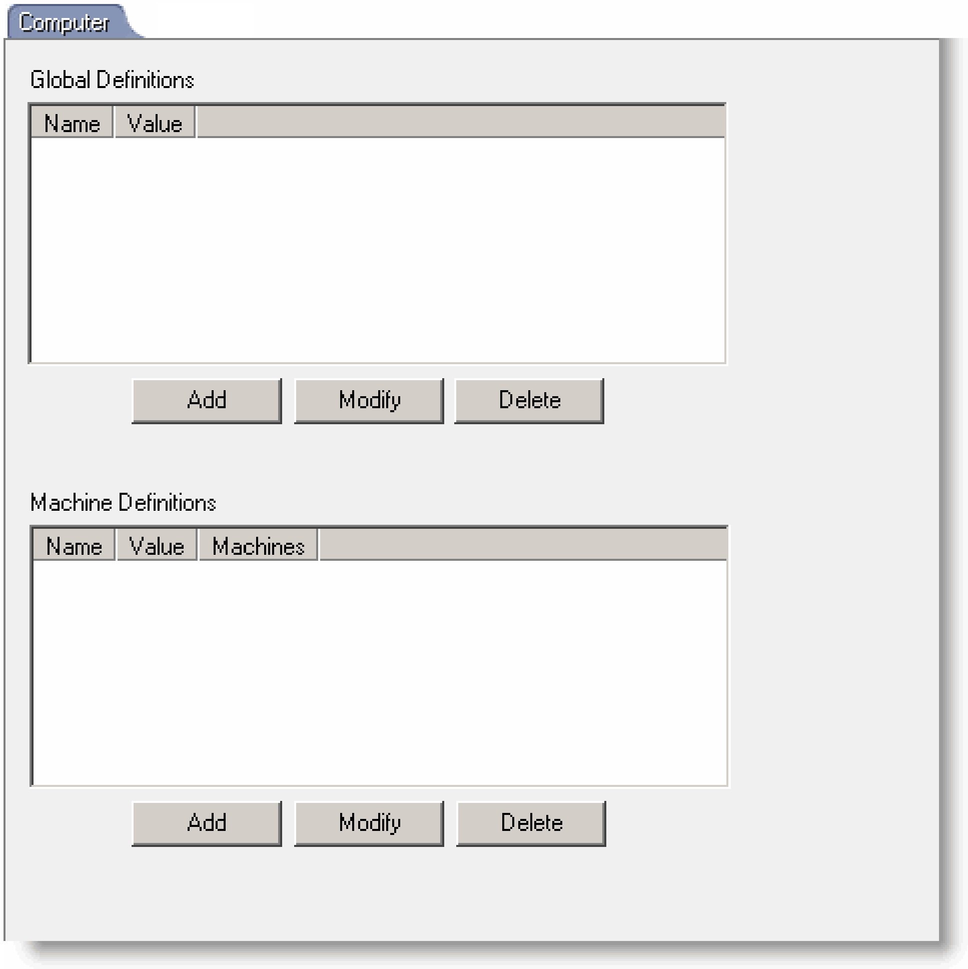
Selecting this box allows certain computers to be excluded from ever executing Desktop Authority regardless of the options selected in the Desktop Authority Manager. This option requires the use of a special options file called SLBYPASS. If this file is present on the client, Desktop Authority will detect 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.

DEFINITIONS

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. The following definitions are available for selection to be added to the lists. Click **Modify** to edit an existing definition. Click **Delete** to remove a definition from the list.

Event_Refresh_Time Defines the time interval for the Computer Management refresh. The default refresh interval is 60 minutes.

HotfixFreeSpaceNeedediNMB Defines the free space needed for Desktop Authority to install a Patch or update. The default free space needed is 1.4GB.

Machine_Trace_Days_To_Retain Defines the number of day 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.

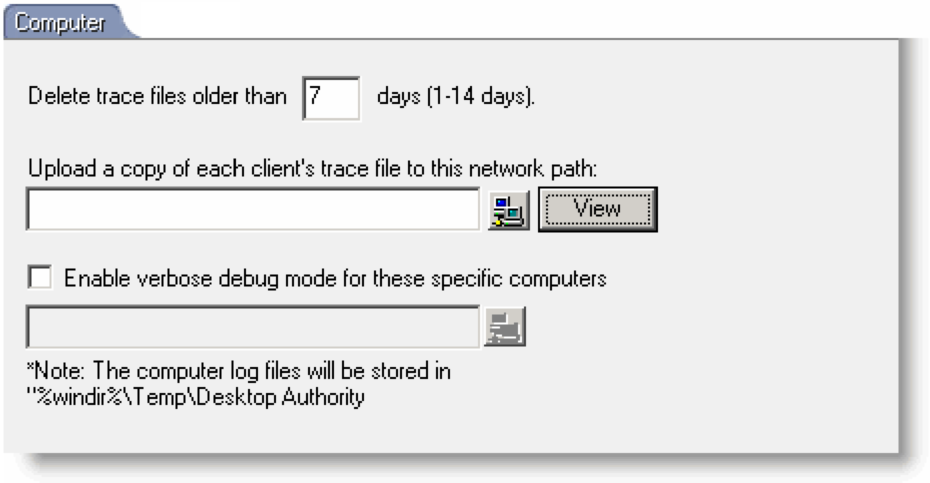
Machine_Trace_File_Repository By default, this variable is to set the network repository location for the Computer Management trace file. This can also be set on the Computer Troubleshooting tab, however in the Definitions object it can be set as a Machine definition for select machines. This setting will override the setting on the Computer Troubleshooting tab.

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.

TROUBLESHOOTING

The Troubleshooting object 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 trace files older than 7 days (1-14 days).

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

□ Enable verbose debug mode for these specific computers

*Note: The computer log files will be stored in "%windir%\Temp\Desktop Authority

Delete 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 clients trace file to this network path

Specify a network path to which all Computer Management trace files will be copied to. 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** to view the trace file repository as specified by the entry.

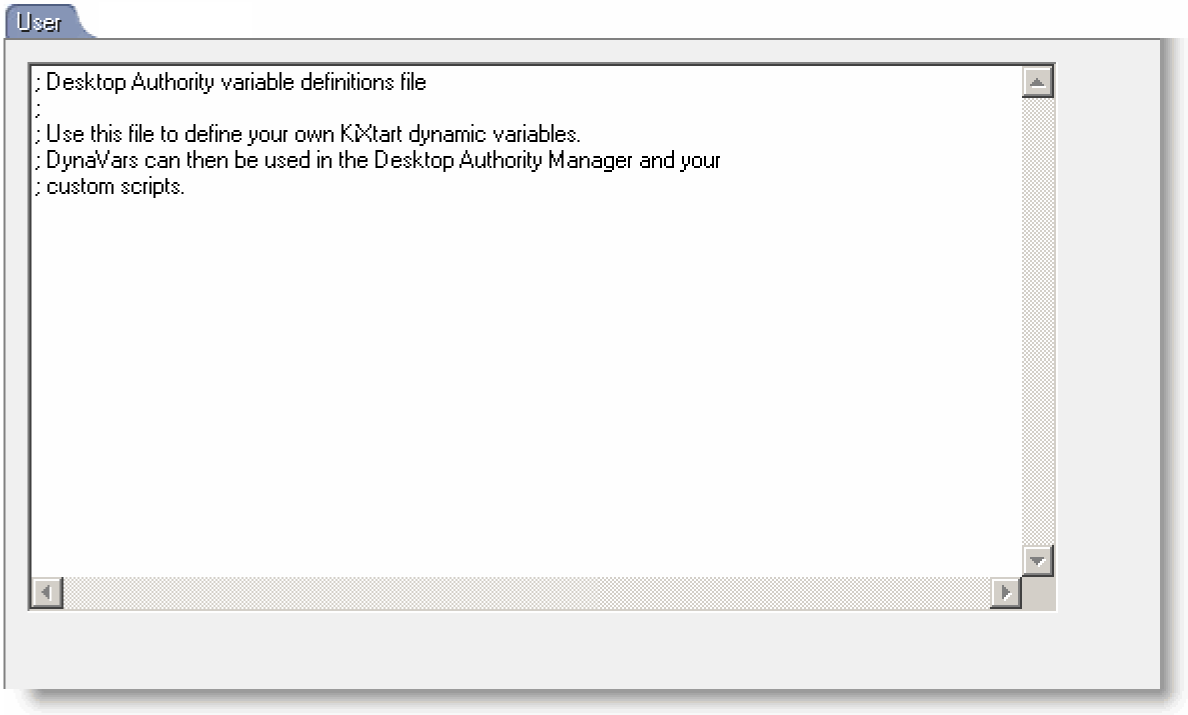
Enable verbose debug mode for these specific computers

By default a simple a 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.

DEFINITIONS

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

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



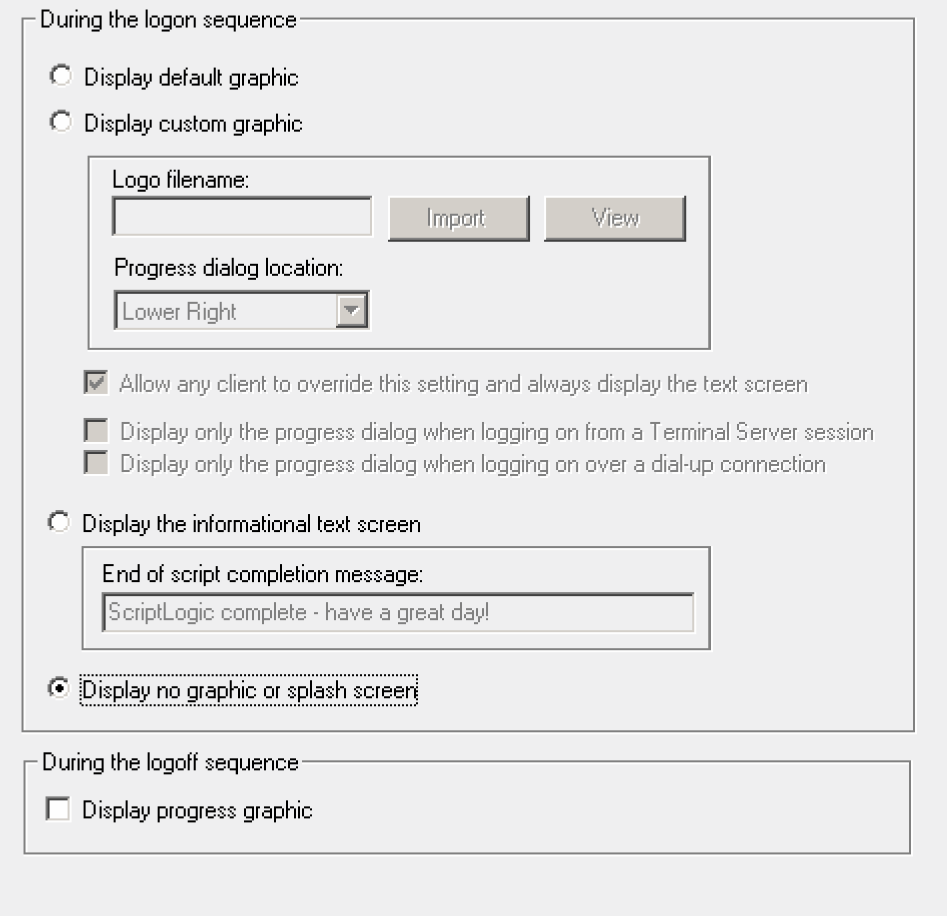
```
; Desktop Authority variable definitions file
;
; Use this file to define your own KiXtart dynamic variables.
; DynaVars can then be used in the Desktop Authority Manager and your
; custom scripts.
```

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

Definitions defined within the Global Definitions area are for use globally on all 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. One of three display types can be selected. Also on the Visual tab is a logoff visual option. The Visual object can only be modified by a Super User/Group.



During the logon sequence

○ Display default graphic

○ Display custom graphic

Logo filename: [ ] Import View

Progress dialog location: Lower Right

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

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

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

○ Display the informational text screen

End of script completion message: ScriptLogic complete - have a great day!

● Display no graphic or splash screen

During the logoff sequence

□ Display progress graphic

During the Logon sequence

Display 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.

Display 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

Click Import or type an image name into the *Logo filename* entry, to specify a custom image that will display during the logon process. The following graphic formats are supported: bmp, rle, gif 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*.

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.

Display the 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.

Display no graphic or splash screen

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

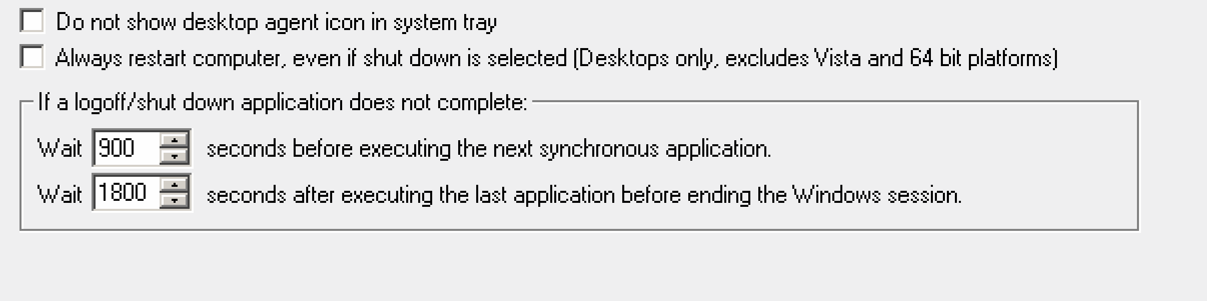
During the Logoff Sequence

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.

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



□ Do not show desktop agent icon in system tray

□ Always restart computer, even if shut down is selected (Desktops only, excludes Vista and 64 bit platforms)

If a logoff/shut down application does not complete:

Wait 900 seconds before executing the next synchronous application.

Wait 1800 seconds after executing the last application before ending the Windows session.

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 Vista and 64 bit platforms)

Select this check box to force the computer to Restart even if a Shut down 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.

Wait seconds 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 seconds after executing the last application before ending the Windows session.

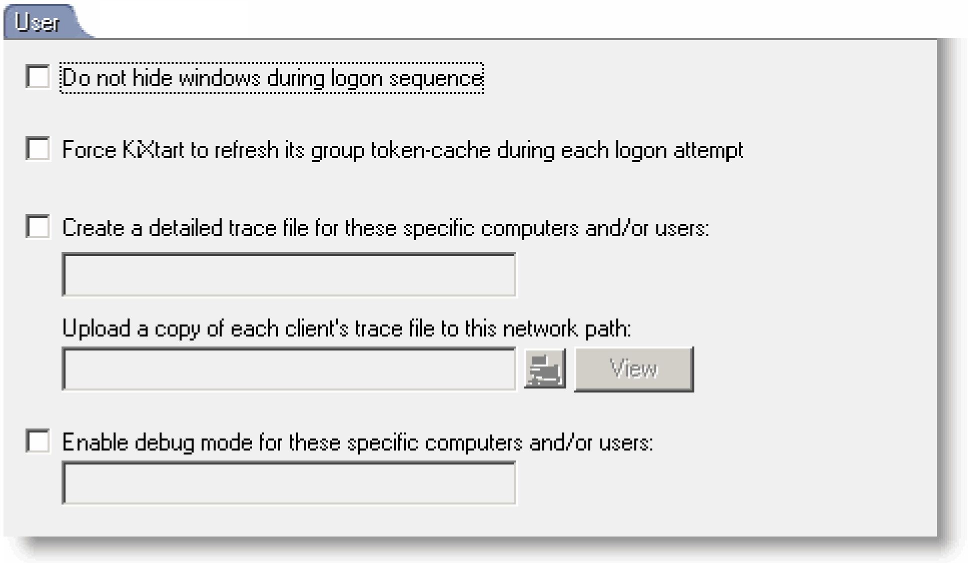
Specify the maximum number of seconds the computer will wait for all logoff/shut down applications to complete before performing the logoff or shut down of the computer. For asynchronous applications this timer starts after the last application is launched.

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).

TROUBLESHOOTING

The Troubleshooting object 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. 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.


User

□ Do not hide windows during logon sequence

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

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

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

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

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 clients trace file to this network path

Specify a network path to which all User trace files will be copied to, after each logon.

Click **View** 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

Deployment Options

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

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.

GPO Deployment

The GPO Deployment object provides the ability to deploy Desktop Authority's SLagent technology to client workstations by using a GPO extension. This is used by the Computer Management profiles to access and configure the computer regardless of whether there is a user logged on to the computer or now.

Assign Script

The Assign Script object is used to assign the SLOGIC logon script to domain user accounts. User Management profiles use this to configure Users.

Patch Distribution (not available for Desktop Authority Express and Desktop Authority for Configuration Manager)

The Patch Distribution object is used to help in researching and/or downloading new patches available from Microsoft. Use this tool to filter the available patch list based on severity and/or product.

Software Distribution (not available for Desktop Authority Express)

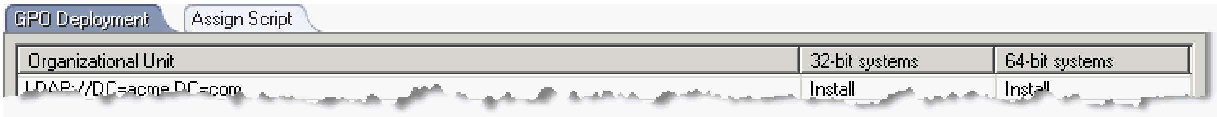
The Software Distribution object is used to import software packages into Desktop Authority for deployment as well as interface with Desktop Authority MSI Studio, if purchased, to create and update software packages.

Server Manager

The Server Manager object provides an interface to manage the ScriptLogic 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 for Desktop Authority to execute during client logon process.



Organizational Unit	32-bit systems	64-bit systems
LDAP://DC=acme,DC=com	Install	Install

GPO Deployment

The GPO Deployment object provides the ability to deploy Desktop Authority's SLagent technology to client workstations by using a GPO extension. Deployment of the Agent is necessary for all computers that will be configured with Computer Management objects.

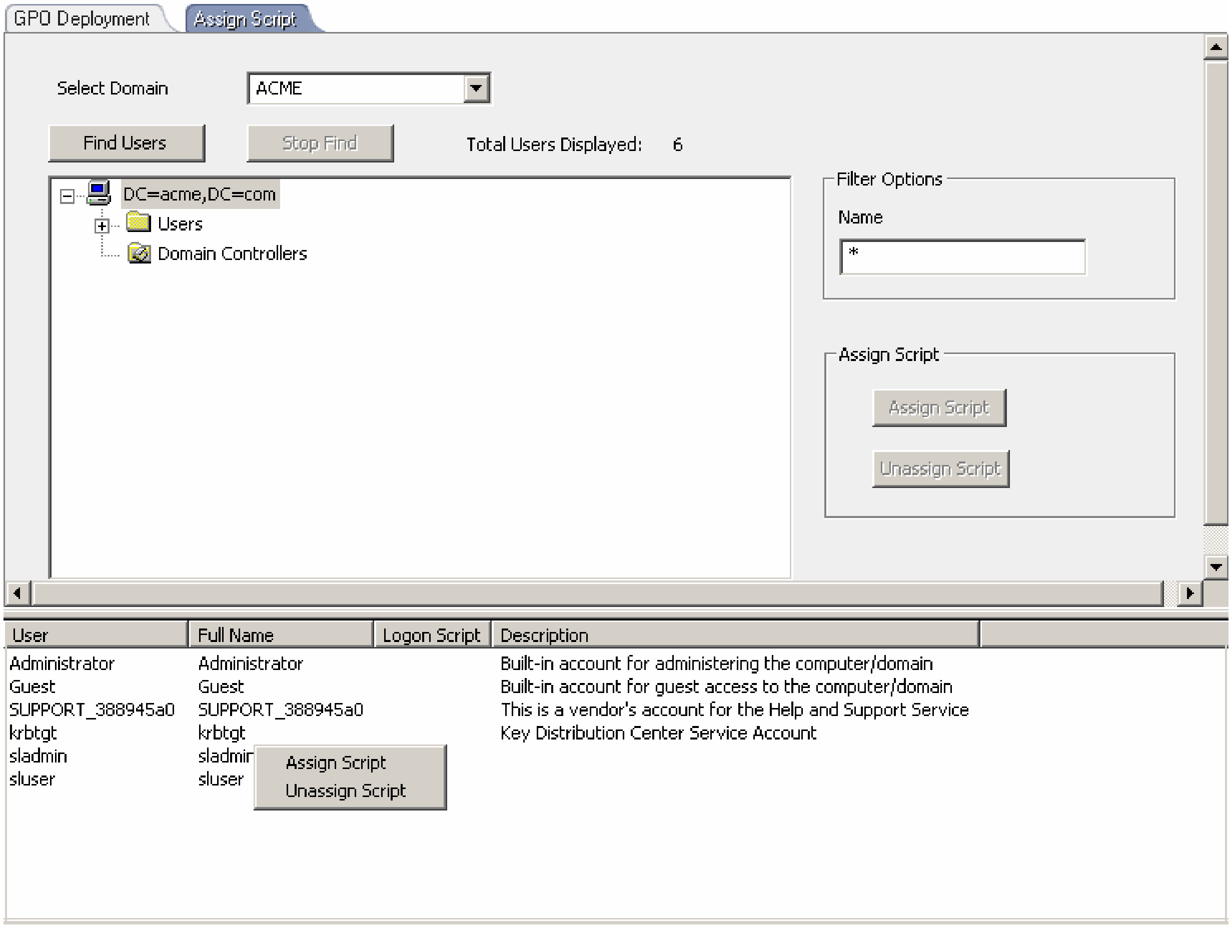
Assign Script

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

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 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: ACME

Total Users Displayed: 6

- DC=acme,DC=com
  - Users
  - Domain Controllers

Filter Options — Name: *

User	Full Name	Logon Script	Description
Administrator	Administrator		Built-in account for administering the computer/domain
Guest	Guest		Built-in account for guest access to the computer/domain
SUPPORT_388945a0	SUPPORT_388945a0		This is a vendor's account for the Help and Support Service
krbtgt	krbtgt		Key Distribution Center Service Account
sladmin	sladmir		
sluser	sluser		

Select Domain

Select the domain that will be used to search for users and assign logon scripts to them.

Active Directory OU and Groups Tree

The Active Directory OU and Groups Tree displays the Active Directory OUs and Groups in which users can be searched.

Filter Options

Username

Enter search criteria that will find matching Active Directory users. Searching with a specific OU highlighted in the tree will search only that specific OU. Search criteria can be entered in the following forms.

Enter an * wildcard to list all Active Directory users.

Ex. [*   ]

Enter one or more characters with a trailing * to find all users whose username begins with the specified characters.

Ex. [br*   ]

Leave the Username entry blank to get a list of all Active Directory users.

Ex. [   ]

Assign Script

Assign Script

Click Assign Script or right-click and select **Assign Script** from the shortcut menu to assign a logon script to all selected users in the list. Once the menu selection is chosen you will be prompted to name the script to assign to the user.

Unassign Script

Click Unassign Script or right-click and select **Unassign Script** from the shortcut menu to unassign a logon script from all selected users in the list. Once the menu selection is chosen you will be prompted to confirm your selection.

User List

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

Select a user by highlighting the user account in the list. To select multiple consecutive users from the list, click on the first one. While holding down the SHIFT key, select the last consecutive user. Multiple non-consecutive users may be selected from the list by pressing the CTRL key while selecting each individual user.

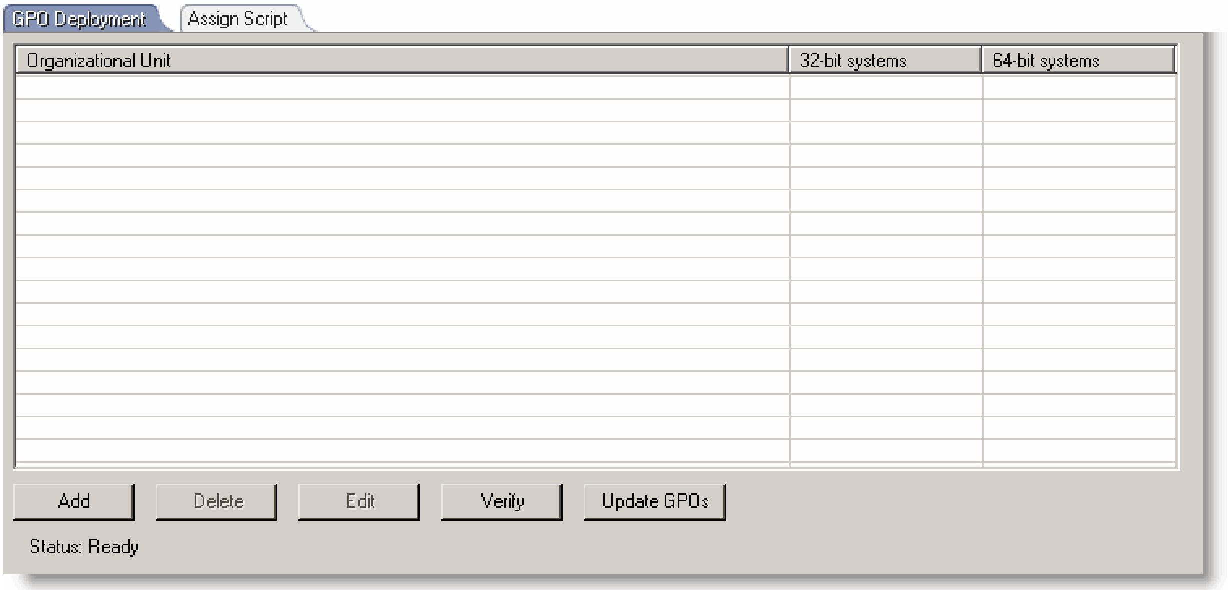
GPO DEPLOYMENT*

GPO Deployment will push out and install an MSI file to each computer in the targeted 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 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 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.

Desktop Authority 8.0 uses Active Directory and Group Policy for secure, consistent deployment of its management agent to all versions of Windows. Previous versions of Desktop Authority only required GPO Deployment for Microsoft Vista and Windows Server 2008 clients that had User Account Control (UAC) enabled. However, Desktop Authority 8.0 requires GPO Deployment for all clients that will be managed by Desktop Authority.



GPO Deployment requires the *Authenticated Users* group to have *Read*, *Execute* and *List* NTFS permissions on the *%windir%\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.

GPO Deployment List

The GPO Deployment list contains a list of OUs that the GPO Extension will be installed to or removed from. 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.

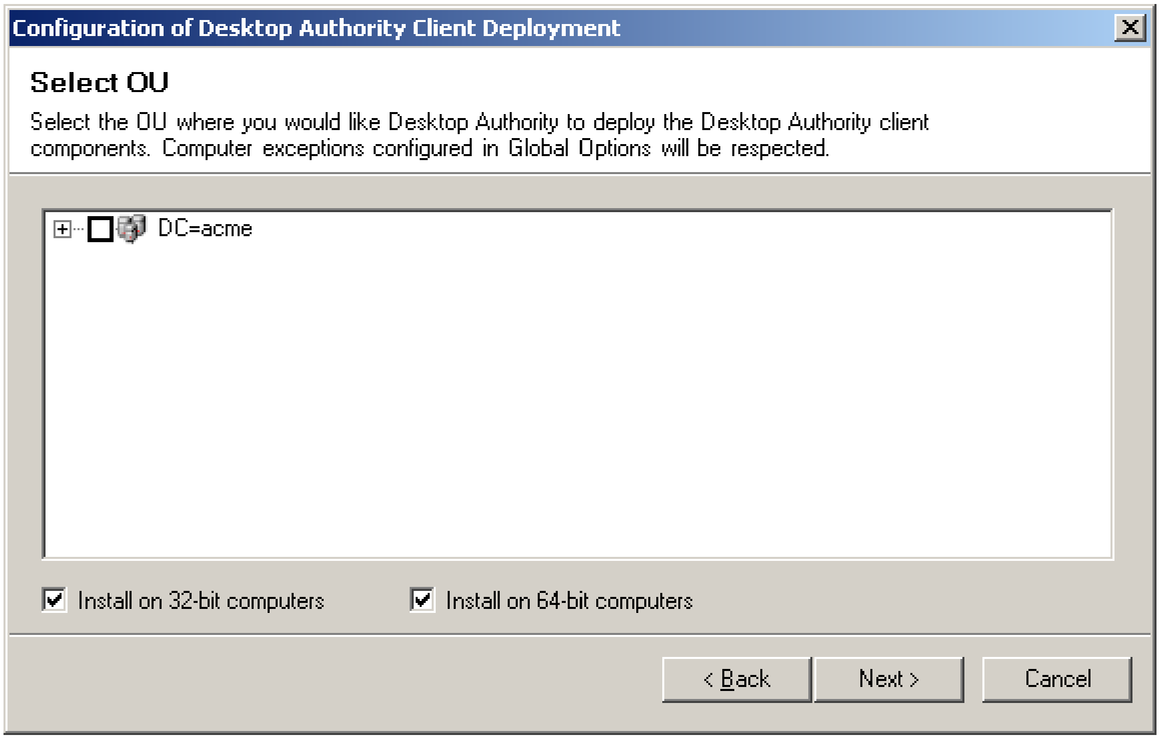
Add

Click **Add** to configure an OU for GPO deployment. The selected OU will be added to the GPO Deployment list. A simple wizard will guide you through the settings that must be completed.

The first page of the GPO Deployment Configuration Wizard is the Welcome. Click **Next** to continue. Click **Cancel** to exit the wizard.

Next the GPO Deployment requirements are listed. GPO Deployment is supported on Windows 2000 SP 3 and above, Windows Server 2003 and above, Windows XP SP 2 and above, Windows Vista SP1 and above and Windows Server 2008. Windows Installer 3.1 and .NET 2.0 are required on the target computers. Desktop Authority will install these software requirements, if necessary. Click **Next** to continue. Click **Cancel** to exit the wizard.

The next dialog is where the OU selection takes place.



Configuration of Desktop Authority Client Deployment

Select OU

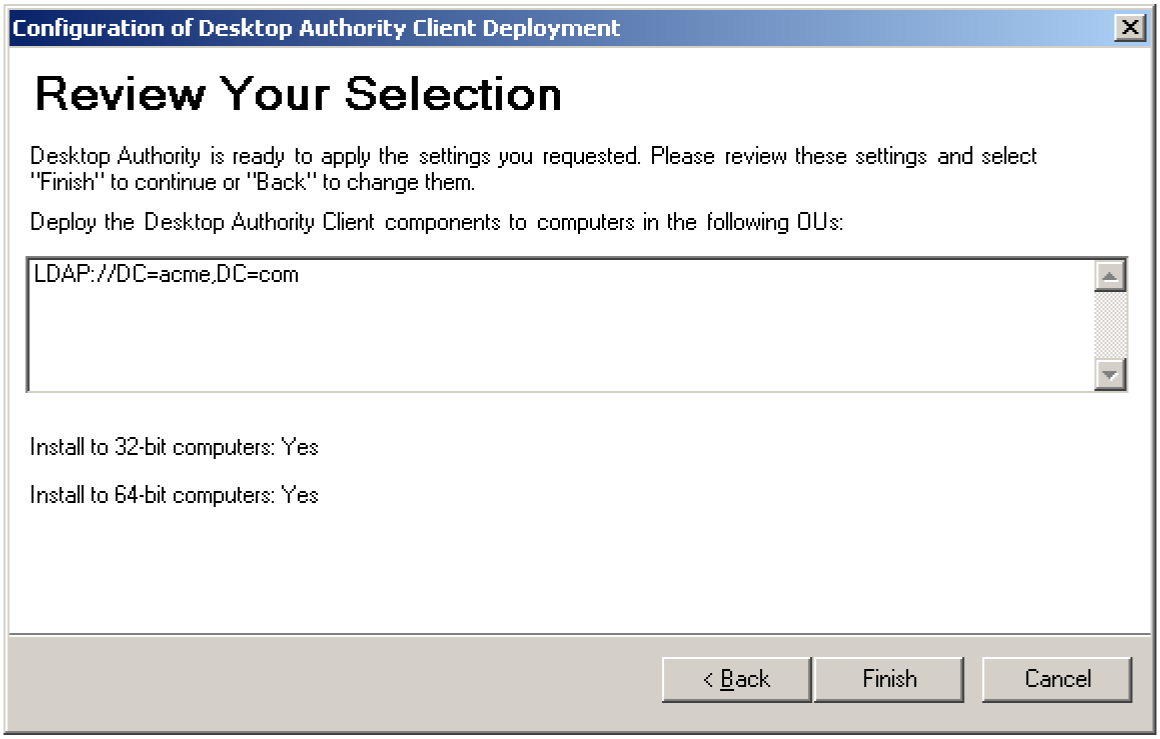
Select the OU where you would like Desktop Authority to deploy the Desktop Authority client components. Computer exceptions configured in Global Options will be respected.

⊞ □ DC=acme

☑ Install on 32-bit computers ☑ Install on 64-bit computers

Drill down to the OU where you would like Desktop Authority to deploy the Desktop Authority client components. Select the necessary checkboxes, Install on 32-bit computers/Install on 64-bit computers. Note that any defined Global Option Exceptions will be respected. Click **Next** to continue. Click **Cancel** to exit the wizard.

Now, confirm the selected settings and click Finish to complete the GPO Deployment configuration for the selected OU.



Review Your Selection

Desktop Authority is ready to apply the settings you requested. Please review these settings and select "Finish" to continue or "Back" to change them.

Deploy the Desktop Authority Client components to computers in the following OUs:

LDAP://DC=acme,DC=com

Install to 32-bit computers: Yes

Install to 64-bit computers: Yes

Click **Back** to modify any settings before clicking **Finish** to complete the GPO Deployment configuration. Click **Cancel** to exit the wizard without saving any GPO Deployment configurations.

Delete

Click to remove the selected OU from the GPO Deployment list.

Edit

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

Verify

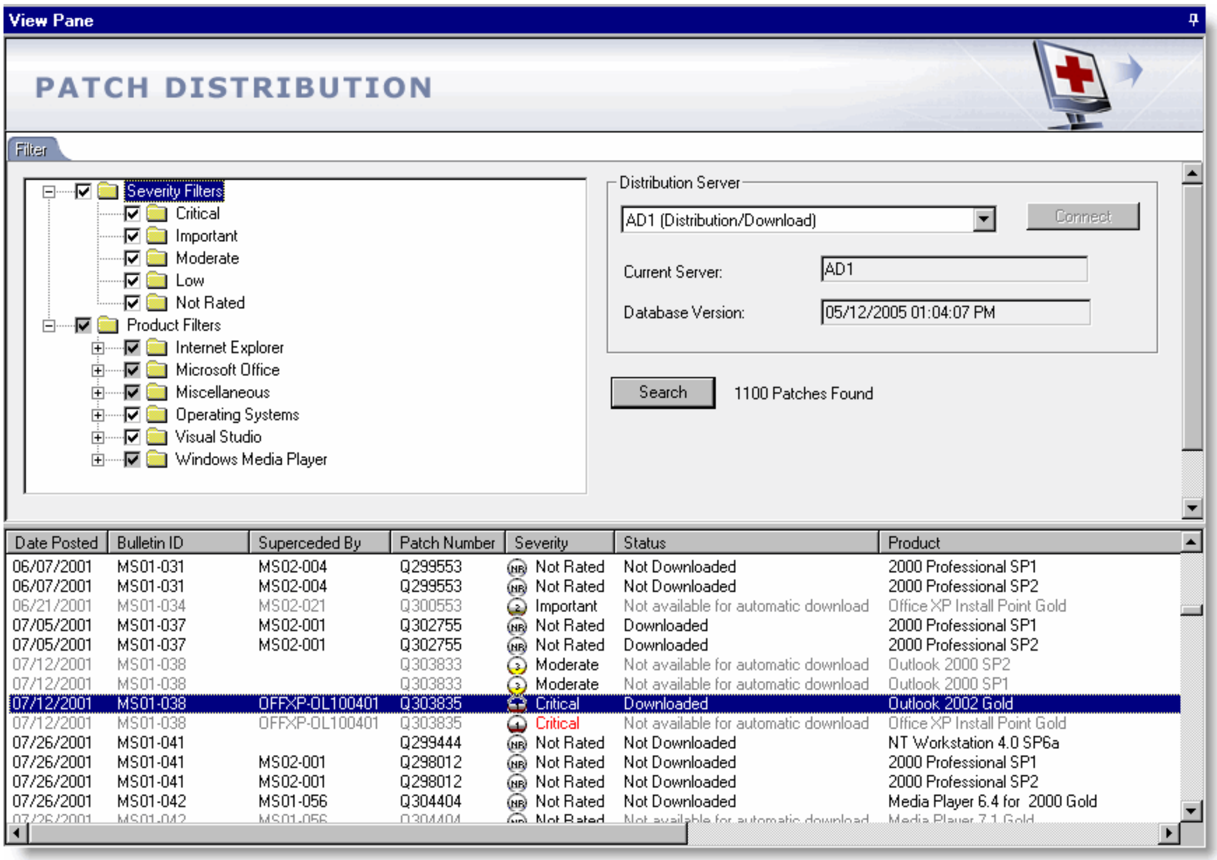
Click **Verify** to confirm that the GPO is up to date and intact.

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.

✚ PATCH DISTRIBUTION*

The Patch Distribution object is used to help in researching and/or downloading patches for Microsoft applications as well as Adobe Acrobat, Adobe Acrobat Reader and Firefox and others. The object's dialog is divided in half, displaying filter criteria on the top and a list of filtered patches on the bottom. The patch list can be filtered on severity and product to help find the patches needed. The Patch Distribution object can only be modified by a Super User/Group.



- ☑ Severity Filters
  - ☑ Critical
  - ☑ Important
  - ☑ Moderate
  - ☑ Low
  - ☑ Not Rated
- ☑ Product Filters
  - ☑ Internet Explorer
  - ☑ Microsoft Office
  - ☑ Miscellaneous
  - ☑ Operating Systems
  - ☑ Visual Studio
  - ☑ Windows Media Player

Distribution Server

AD1 (Distribution/Download) ▼ Connect

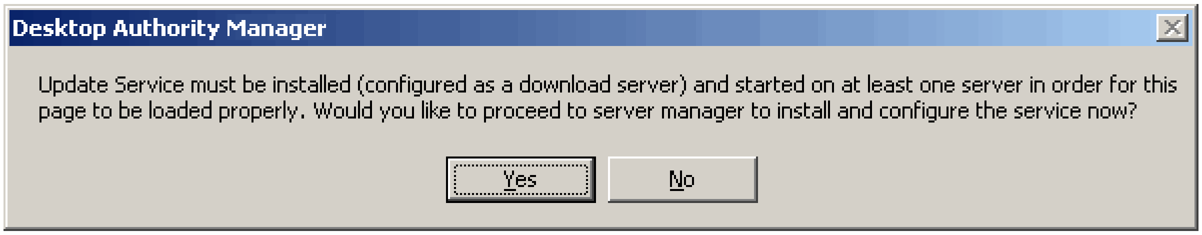
Current Server: AD1

Database Version: 05/12/2005 01:04:07 PM

Search 1100 Patches Found

Date Posted	Bulletin ID	Superceded By	Patch Number	Severity	Status	Product
06/07/2001	MS01-031	MS02-004	Q299553	Not Rated	Not Downloaded	2000 Professional SP1
06/07/2001	MS01-031	MS02-004	Q299553	Not Rated	Not Downloaded	2000 Professional SP2
06/21/2001	MS01-034	MS02-021	Q300553	Important	Not available for automatic download	Office XP Install Point Gold
07/05/2001	MS01-037	MS02-001	Q302755	Not Rated	Downloaded	2000 Professional SP1
07/05/2001	MS01-037	MS02-001	Q302755	Not Rated	Downloaded	2000 Professional SP2
07/12/2001	MS01-038		Q303833	Moderate	Not available for automatic download	Outlook 2000 SP2
07/12/2001	MS01-038		Q303833	Moderate	Not available for automatic download	Outlook 2000 SP1
07/12/2001	MS01-038	OFFXP-OL100401	Q303835	Critical	Downloaded	Outlook 2002 Gold
07/12/2001	MS01-038	OFFXP-OL100401	Q303835	Critical	Not available for automatic download	Office XP Install Point Gold
07/26/2001	MS01-041		Q299444	Not Rated	Not Downloaded	NT Workstation 4.0 SP6a
07/26/2001	MS01-041	MS02-001	Q298012	Not Rated	Not Downloaded	2000 Professional SP1
07/26/2001	MS01-041	MS02-001	Q298012	Not Rated	Not Downloaded	2000 Professional SP2
07/26/2001	MS01-042	MS01-056	Q304404	Not Rated	Not Downloaded	Media Player 6.4 for 2000 Gold
07/26/2001	MS01-042	MS01-056	Q304404	Not Rated	Not available for automatic download	Media Player 7.1 Gold

The Update Service must be installed and configured in order for Desktop Authority to retrieve the latest patch listings and files. If it is not configured at the time the Patch Distribution object is selected in the Navigation Pane, a message will be displayed with an opportunity to install and configure the service.



Update Service must be installed (configured as a download server) and started on at least one server in order for this page to be loaded properly. Would you like to proceed to server manager to install and configure the service now?

Once configured, the download servers will query scriptlogic.com to determine the product mode and download updated patch file listings, when available. For more information on the Update Service, see What is the Update Service?

Note: If the server does not have Internet access, the Desktop Authority Updates and Patch Download Service (DAUPDS) can be used to provide the Enterprise the ability to download patches and updates for Desktop Authority Servers that may not or can not have Internet access. This tool will download the updates and patches which can be imported into Desktop Authority for consumption by the Update Service. For more information on this tool, go to the Desktop Authority support page on the ScriptLogic website.

Filter

Use the Filter tool to minimize the available patch list based on severity and/or product. Select the Severity Filters check box to automatically select each severity listed below it or select individual severities below the Severity Filters check box. Clear the Severity Filters check box to clear all selected severities.

Select the Product Filters check box to automatically select all products listed below it or select individual products below the Product Filters check box. Clear the Product Filters check box to clear all selected products.

Distribution Server

Select a server from the list and click Connect to select a new Distribution server.

Current Server

The Current Server designates the server that is Update Service is currently connected to. This is the server that patch files will be downloaded to if Download File is selected from the shortcut menu in the Patch List.

Database Version

The Database Version specifies the date and time stamp of the Patch File which contains the list of patches available for download.

Search/Cancel

Click Search to filter the patch list based on the selected Severity and Product filters. A count of selected patches will be displayed following the search.

Once clicked, the Search button will turn into a Cancel button. Click Cancel to abort the current search.

Patch List

The Patch list displays all filtered patches. Information regarding each patch includes the date the patch was posted, Bulletin ID, Superceded By patches, Patch number, Severity, patch status, the product(s) the patch pertains to, patch title, and patch description. The patch list is sortable by any one of the columns available in the list. Sort the list by clicking on a column header.

Select a patch for download by highlighting it in the patch list. To select multiple consecutive patches from the list, click on the first one. While holding down the SHIFT key, select the last consecutive patch. Multiple non-consecutive patches may be selected from the list by pressing the CTRL key while selecting each individual patch.

The status column within the patch list describes whether the patch file has been downloaded or not. Periodically there will be a status for some patch files that says Not available for automatic download. This status may occur for various reasons. It may be a patch that is no longer supported or available for download or does not have a silent install. Silent installs are necessary for Patch Management.

Right-click on a patch in the patch list for further options.

Download Patches

Select Download Patches from the shortcut menu to start the download process. The selected patch(s) will be downloaded from Microsoft to the selected destination for each server running the Update Service. The Update Service is configured in Server Manager.

On a network with a single download server and multiple distribution servers, the downloaded patches are not automatically distributed to the distribution servers. For details on how patch files are distributed throughout the network, see the Best Practices using the Update Service topic.

Refresh

Select Refresh from the shortcut menu to refresh the filtered patch list.

More Info...

Select More Info... from the shortcut menu to read more detailed information about the patch. This will open Microsoft's Tech Net Bulletin for the selected patch. When multiple patches are selected, this option is not available.

*This feature is not a standard part of Desktop Authority Express. To obtain this feature, Desktop Authority Express must be upgraded to the full version of Desktop Authority.

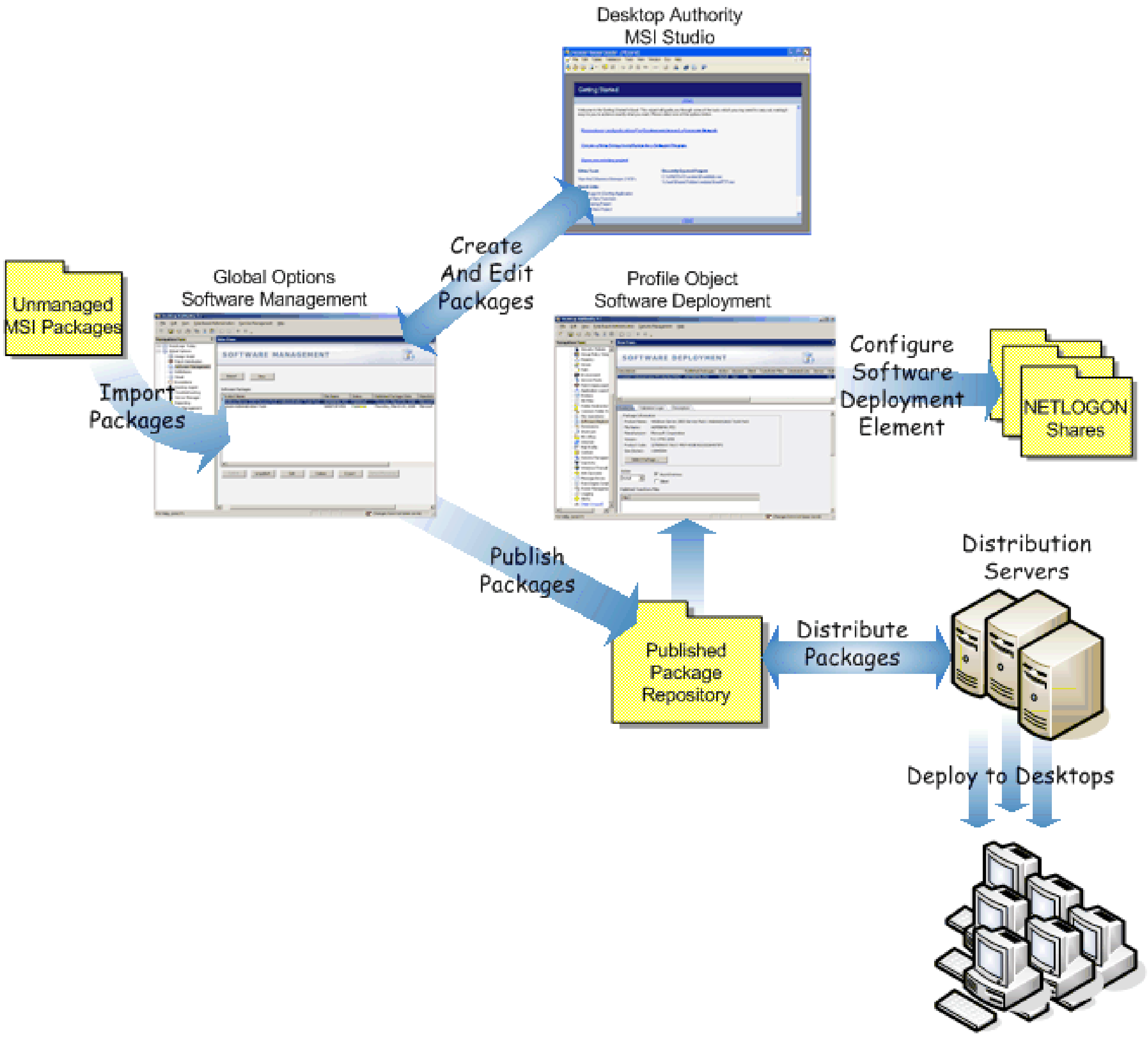
SOFTWARE DISTRIBUTION*

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.

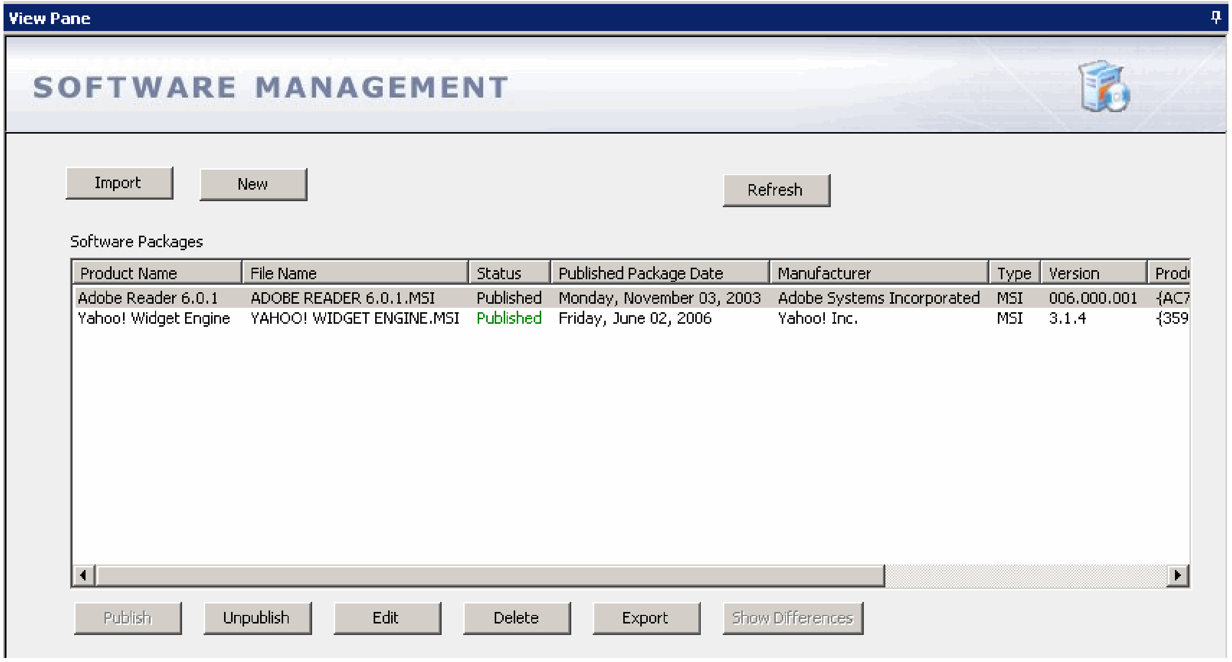
The Desktop Authority Software Distribution object is used to manage a repository of Microsoft Windows Installer (MSI, MST, MSP) packages. Desktop Authority provides access to Desktop Authority MSI Studio. MSI Studio is a complete application software packaging solution used to create new Windows Installer files and modify existing ones.

The Software Distribution object provides the ability to:

- import packages into its repository.
- export packages from its repository.
- create and modify packages using Desktop Authority MSI Studio.
- 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.



Desktop Authority accesses Windows Installer packages, providing the ability to Import, Export, Modify (by calling MSI Studio), Delete and Publish these packages.



Product Name	File Name	Status	Published Package Date	Manufacturer	Type	Version	Prod
Adobe Reader 6.0.1	ADOBE READER 6.0.1.MSI	Published	Monday, November 03, 2003	Adobe Systems Incorporated	MSI	006.000.001	{AC7
Yahoo! Widget Engine	YAHOO! WIDGET ENGINE.MSI	Published	Friday, June 02, 2006	Yahoo! Inc.	MSI	3.1.4	{359

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.

New

Click Edit to call Desktop Authority MSI Studio to package a new solution. This option is only available if MSI Studio is a licensed product.

Refresh

Click Refresh to freshen the Software Packages list.

Software Packages

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.

Publish

Click Publish to move the selected Windows Installer packages to the Update Service's distribution servers. Distribution servers are a defined part of the Update Service and are configured within Server Manager.

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.

Edit

Click Edit to call MSI Studio to modify an existing solution. This option is only available if MSI Studio is a licensed product.

Delete

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

Export

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

Show Differences

Click Show Differences between the published and unpublished versions of the selected package, if any differences exist. Differences will be displayed within MSI Studio.

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.

*This feature is not a standard part of Desktop Authority Express. To obtain this feature, Desktop Authority Express 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 ScriptLogic service, the Update Service and the replication process.

OpsMaster Service

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

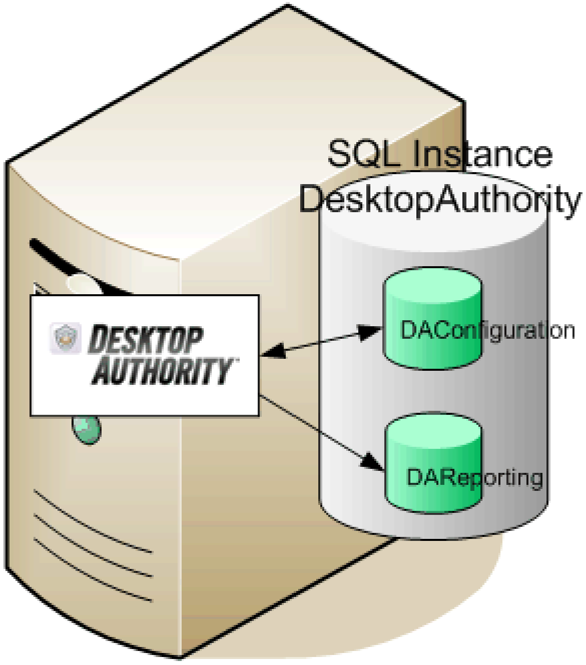
Database Configuration

The Database Configuration tool provides the ability to perform maintenance operations on Desktop Authority's back end SQL databases. The supporter operations include: backup/restore the database, shrink/increase the allocated database size, and maintenance operations such as rebuilding indexes and database consistency checks.

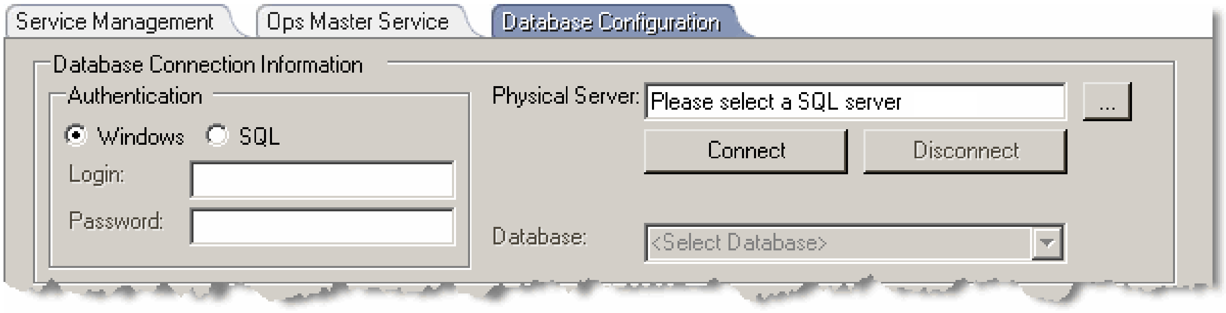
DATABASE CONFIGURATION

The Database Configuration tool provides the ability to perform maintenance operations on Desktop Authority's back end SQL databases. The supported operations include: backup/restore the database, shrink/increase the allocated database size, and maintenance operations such as rebuilding indexes and database consistency checks. The Database Configuration object is available exclusively to a Super User/Group. Non-Super Users/Groups do not have the ability to open the Database Configuration object.

The Database Configuration tool is broken up into two sections; Database Connection and Database Operations. Before any operations can be performed a connection to the database must be established. During installation, Desktop Authority creates a single named instance of the Microsoft SQL Server 2005 Express Edition. The named databases created within this SQL instance are DACONFIGURATION and DAREPORTING. The DACONFIGURATION database is where all of the Desktop Authority configuration data is stored. The DAREPORTING database is where the reporting data is stored.



Database Connection Information



Authentication

● Windows ○ SQL

Login:

Password:

Physical Server: Please select a SQL server

Database: <Select Database>

A connection to either database can be made using Windows Authentication mode or SQL Server Authentication mode.

Windows

Select Windows to connect to SQL using a Microsoft Windows user account.

SQL/MSDE

Select SQL/MSDE to connect to the database using Mixed Mode Authentication (Windows Authentication and SQL Server Authentication).

Login

Enter the SQL login name.

Password

Enter the SQL login password.

Physical Server

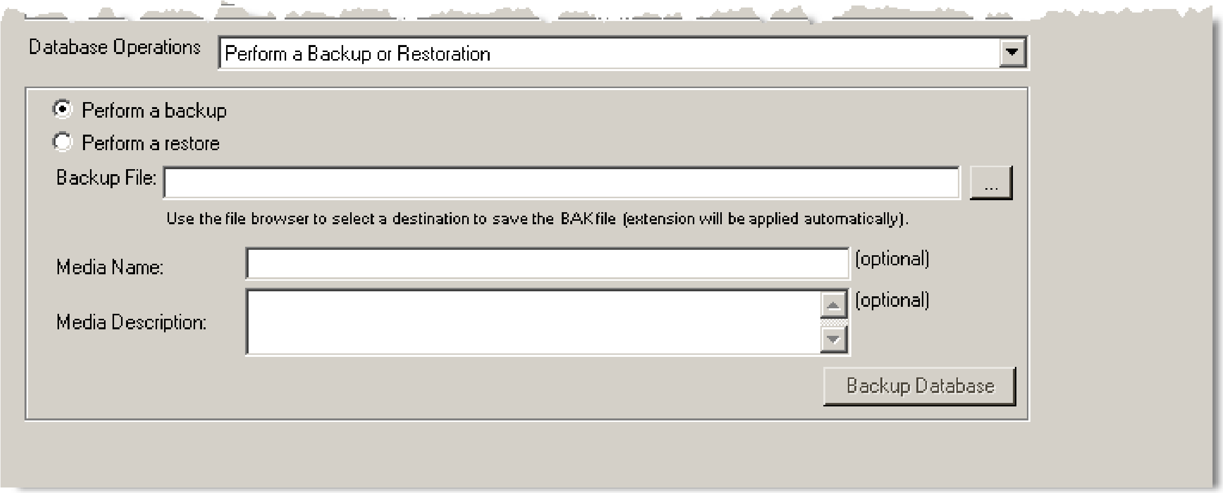
Enter the server or instance name containing the database to connect to. Click ... to select a database from the list of all named-instances found on the network. Click Connect to establish a connection to the desired server. Click Disconnect to remove the database connection to the server.

Database

Once the server is connected to, all of the databases on the server are made available to the database list. Select the desired database from this list.

Database Operations

Perform a Backup or Restoration



Database Operations: Perform a Backup or Restoration

● Perform a backup

○ Perform a restore

Use the file browser to select a destination to save the BAK file (extension will be applied automatically).

Perform a backup

Create a complete backup copy of the selected database. This copy is stored in a separate location that is protected from the potential problems on the server. If the MSDE/SQL server fails, or the database is damaged, the backup can be used to restore the database.

Perform a restore

Perform a restore operation on a previously backed up database.

Backup/Restore File

For a backup operation, specify the backup filename. For a restore operation, select the file to be restored. Specify a local file path or a UNC path.

Media Name

Provide informational text to aid in the identification of a backup set.

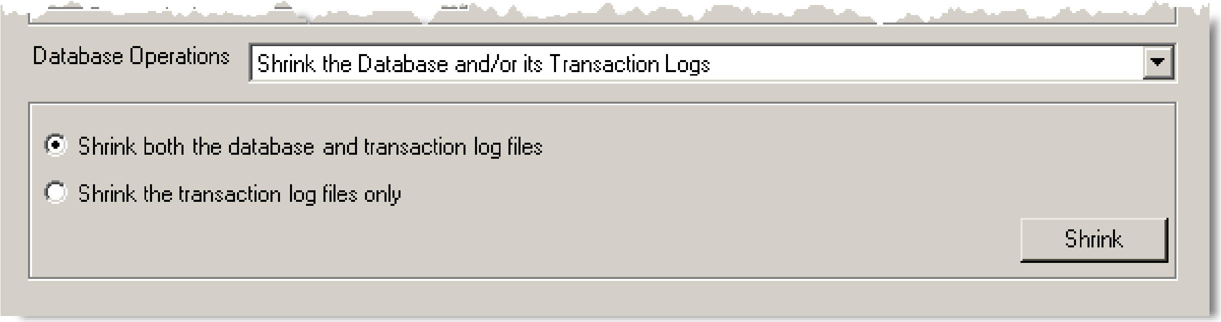
Media Description

Provide informational text to aid in the identification of a backup set.

Backup/Restore Database

Click Backup/Restore Database to start the selected operation.

Shrink the Database and/or its Transaction Logs



Database Operations: Shrink the Database and/or its Transaction Logs

● Shrink both the database and transaction log files

○ Shrink the transaction log files only

Shrink both the database and transaction log files

Reduce the size of all files in the database. File(s) are truncated to reflect freed space.

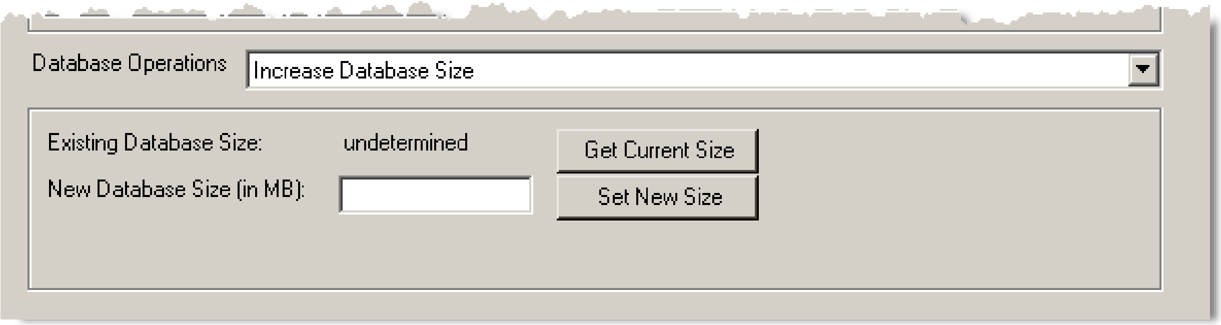
Shrink the transaction log files only

Reduce the size of the database's transaction log files only. File(s) are truncated to reflect freed space.

Shrink

Click Shrink to begin the selected shrink operation.

Increase Database Size



Database Operations: Increase Database Size

Existing Database Size: undetermined

New Database Size (in MB):

Existing Database Size

Displays the current size of the selected database in megabytes. The size includes data and transaction log files.

Get Current Size

Click Get Current Size to retrieve the database size information.

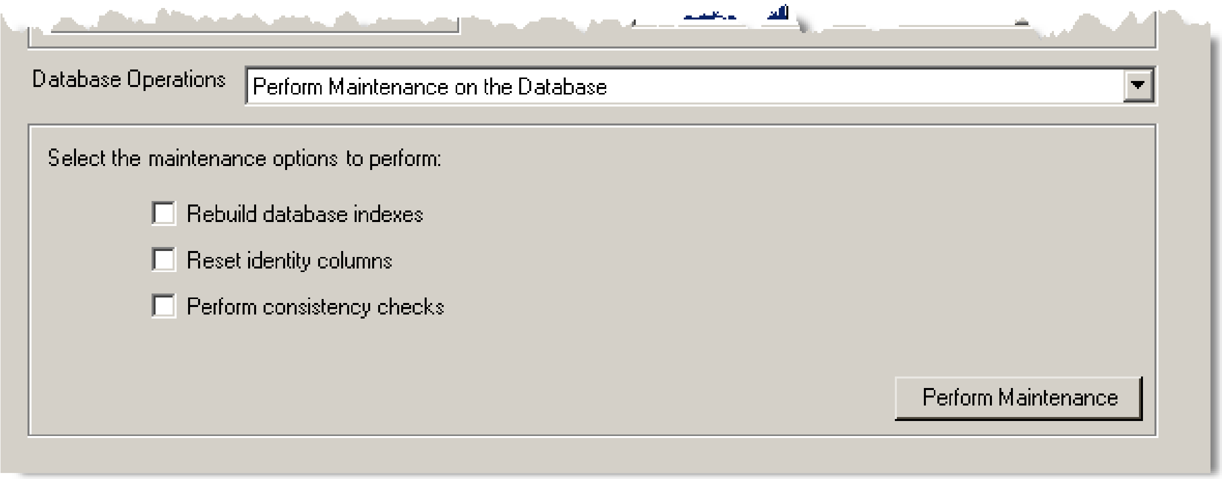
New Database Size (in MB)

Specify a new database size in megabytes.

Set New Size

Click Set New Size to increase the size of the database.

Perform Maintenance on the Database



Database Operations: Perform Maintenance on the Database

Select the maintenance options to perform:

- □ Rebuild database indexes
- □ Reset identity columns
- □ Perform consistency checks

Rebuild database indexes

Rebuilding indexes reorganizes the storage of the index data to remove fragmentation. This can improve disk performance by reducing the number of page reads required to obtain the requested data. Check this box to rebuild the database indexes.

Reset identity columns

Check this box to renumber the identity columns for all tables within the database.

Perform consistency checks

Check this box to check the consistency of the database and its indexes. If necessary this operation will rebuild the indexes and update the index statistics.

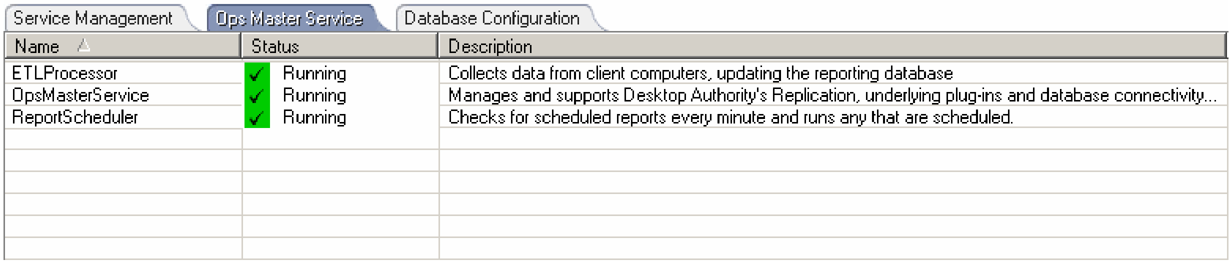
Perform Maintenance

Click Perform Maintenance to perform the selected maintenance operations.

OpsMaster Service

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

The OpsMaster 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 be changed. Simply drag a column to its new desired location in the list.



Name	Status	Description
ETLProcessor	✓ Running	Collects data from client computers, updating the reporting database
OpsMasterService	✓ Running	Manages and supports Desktop Authority's Replication, underlying plug-ins and database connectivity...
ReportScheduler	✓ Running	Checks for scheduled reports every minute and runs any that are scheduled.

Right-clicking on either plugin displays a shortcut menu. The two options on this menu include Restart Selected Plugin and Reload Plugins List.

Restart Selected Plugin

Select this option from the shortcut menu to restart the selected service.

Reload Plugins List

Select this option from the shortcut menu to refresh 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 or right-click and select Restart this plugin from the shortcut menu 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 or right-click and select Restart this plugin from the shortcut menu to start the plugin.

ETLProcessor

The ETL processor plugin manages 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.

There are several configuration parameters available for this plugin.

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 60. Allowable values can be between 1 and 36399 minutes.

Profile and RBA 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. The default backup time is set to 1:00AM.

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 365 days. This may however be set to any value between 0 and 7300 (20 years).

Synch Reporting Data

In opposition to the automatic Profile and RBA Audit data backup, click Synch Reporting Data to process reporting data right away.

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.

User and Computer Data is collected by Desktop Authority's OpsMaster service and the ETLProcessor plugin. These two plugins are available in the Server Manager > Ops Master Service tab for configuration.

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, Patch Management, Anti-spyware and USB/Port Security. User based Data Collection con be configured for login/logoff and lock/unlock events.

OpsMasterService

The OpsMasterService manages and supports Desktop Authority's replication, underlying plug-ins and database connectivity. There are no configuration options for this plugin.

To change the service credentials for this backbone plugin, select Change Operations Master Service Credentials... from the Role Based Administration menu.

ReportScheduler

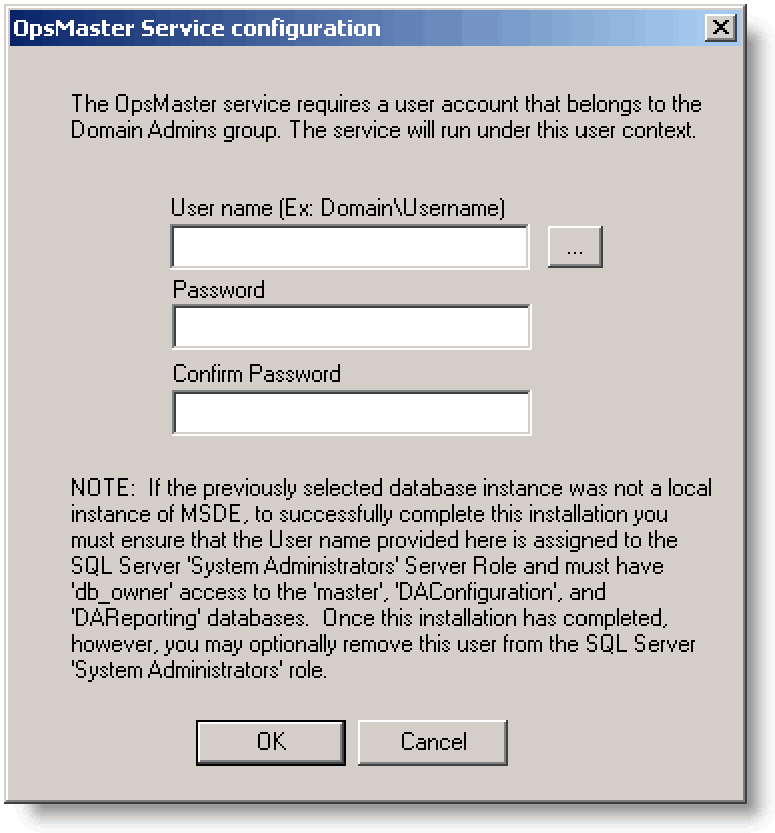
The ReportScheduler plugin that runs scheduled reports. This plugin runs every minute checking for reports to run. There are no configuration options for this plugin.

Restart

Click **Restart** to restart the selected service.

CONFIGURING THE OPSMASTER SERVICE

To change the service credentials for this backbone plugin, select Change Operations Master Service Credentials... from the Role Based Administration menu.



OpsMaster Service configuration

The OpsMaster service requires a user account that belongs to the Domain Admins group. The service will run under this user context.

User name (Ex: Domain\Username)

Password

Confirm Password

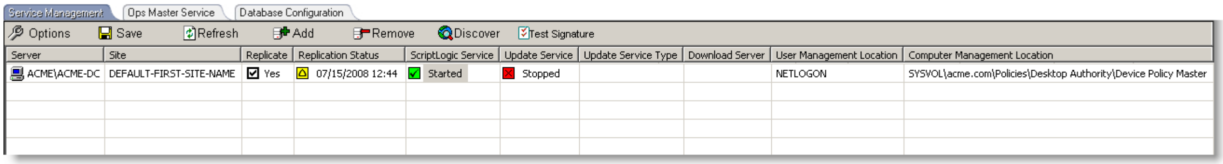
NOTE: If the previously selected database instance was not a local instance of MSDE, to successfully complete this installation you must ensure that the User name provided here is assigned to the SQL Server 'System Administrators' Server Role and must have 'db_owner' access to the 'master', 'DAConfiguration', and 'DAReporting' databases. Once this installation has completed, however, you may optionally remove this user from the SQL Server 'System Administrators' role.

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. Enter the User name and Password for a user account that belongs to the Domain Admins group. The user name should be entered in the form of Domain\Username. Click [...] to use the Resource Browser to browse the network and select an appropriate user.

SERVICE MANAGEMENT

The Service Management object is a multi-threaded component that provides an interface to manage the ScriptLogic 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.

The Service Management grid details the status of each server utilized by Desktop Authority, including the status of the ScriptLogic 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 ScriptLogic and/or the Update Service on one or more servers from this single location. Replication can also be managed from this simple grid. One or more servers can be defined as a target for replication and replicate the configuration files.



Server	Site	Replicate	Replication Status	ScriptLogic Service	Update Service	Update Service Type	Download Server	User Management Location	Computer Management Location
ACME\ACME-DC	DEFAULT-FIRST-SITE-NAME	☑ Yes	07/15/2008 12:44	✓ Started	☒ Stopped			NETLOGON	SYSVOL\acme.com\Policies\Desktop Authority\Device Policy Master

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 ScriptLogic and Update services as well as acting as a replication partner for the published Desktop Authority configuration files.

To configure servers for Server Manager, click the Discover button on the toolbar to tell Server Manager to examine the network for existing domain controllers and add them to the list. Right-click on one or more existing server(s) in the grid for several server properties.

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

Selecting the Target box 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 may 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.

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 Replication Options tab of the Server Manager Options dialog and the Server Properties menu. 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.

When you install Desktop Authority, a default 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 LEDs to represent the status of replication and the ScriptLogic service on each server.

Replication Status legend:

- ✅ A green marker 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 marker indicates that the files in the target folder are outdated. 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 date and time of the last replication is displayed.
- ❎ A red marker 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 "*Files not found*" is indicated in this cell.
- ⬜ A gray marker indicates that this server is not a Target and the configuration files do not exist in the Target folder. The message "Not a target" is indicated in this cell.

The ScriptLogic Service column shows the current state of the service on each server.

The Update Service column shows the current state of the Update Service on each server. The Update service type column designates how the Update server is configured. The Update server can be configured as a Distribution or Distribution/Download server. A server configured as a Distribution server is one that will deliver patch files to client computers. A Distribution/Download server is one that will download patch files as well as deliver them to client computers. The Update service type is defined by the Update Service configuration option to Allow this server to download patches. If this box is selected the Update service type is defined as Distribution/Download. A server type is defined as Distribution if the service is not configured to download patches.

Service Status Codes legend:

- ✅ The service is started on the server.
- ⚠ The service is out of date. Server Manager will typically prompt you to update outdated services.
- ❎ The service is currently stopped on the server.
- ⬜ The service is not installed on the server.

Right-click on one or more cells in either the ScriptLogic or Update service columns to Start, Stop, Restart, Configure, Install, Remove or Update the service image. For more information on these options refer to Service options.

The last two columns are User Management location and Computer Management location, which show the replication target locations.

Server Manager Toolbar

Options

Click Options to define replication options and Server Manager Preferences.

Save

Click **Save** to save any changes made in the Server Manager list.

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.

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. Alternatively, right-click on one or more servers in the **Server** column and select **Add Server** from the shortcut menu, click **Add server**.

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

Remove

Select one or more servers and click **Remove.** Alternatively, right-click on one or more servers in the **Server** column and select Remove **Server** from the shortcut menu. This is useful if a domain controller is removed from the network.

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.

Test Signature

Signatures validate the integrity of Desktop Authority definition and configuration files. Test Signature is used to verify the varoious file signatures. It will first verify that the Signatures Public Key (stored in %Program Files%\ScriptLogic Manager\slsrvmgr.ske file) is the same on each server that has the ScriptLogic 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.

OPTIONS

The Options dialog box provides several Replication options and Preferences.

Replication 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.

NT 4.0 Directory Replication

Publish an additional copy of the configuration files to:

Select this check box if Microsoft replication is being used in conjunction with Desktop Authority. Enter the additional path where the Desktop Authority configuration files should be published to. Click ... to locate the additional folder.

Options

Include hidden & 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.

Update only changed files

Select this check box 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.

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

Refresh timer

The Server Manager dialog box is constantly being refreshed in order to display the most accurate status information. Enter a number (in seconds) to represent how often Server Manager should verify and update its statuses.

Background threads

Specify the number of Server Manager threads that can be run concurrently for refreshing the service status', replication status, etc. The minimum value that can be specified is 2 and the maximum is 40. The default value is 10.

Disable the built-in KXRPC service on all servers

Select this check box to disable Desktop Authority's built-in KXRPC service. Click **Ok** to accept the updated preferences. Click **Cancel** to exit without saving any changes.

Default User Management replication target location

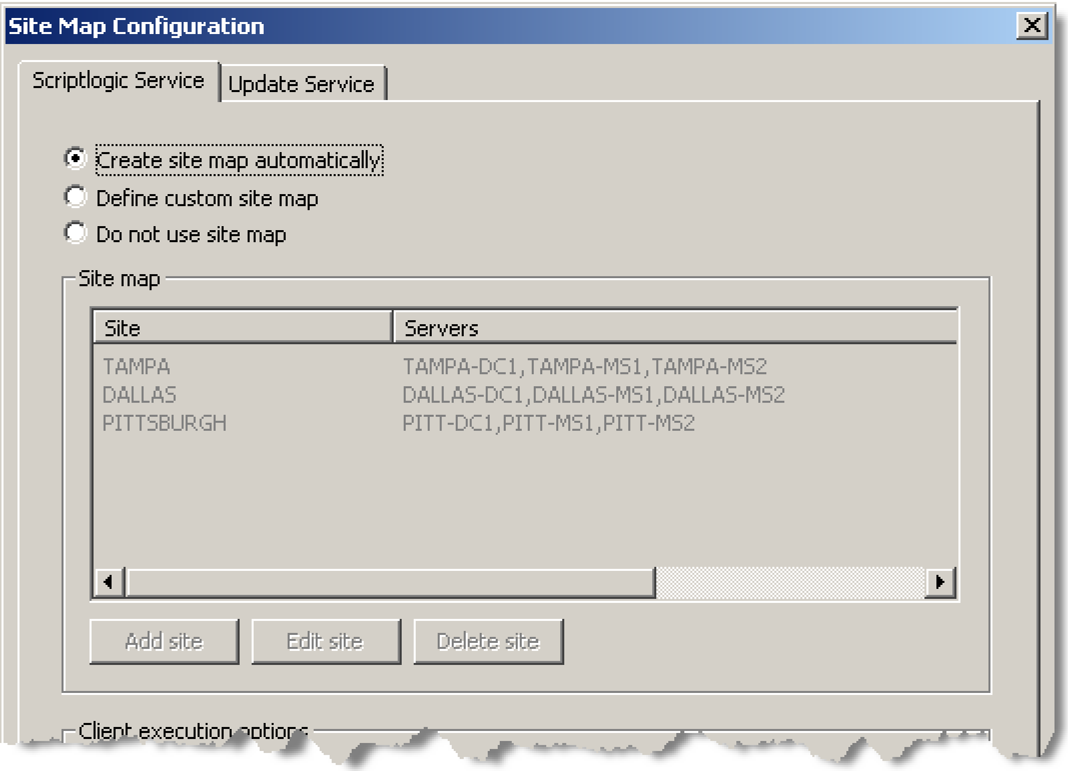
Specify a folder that will hold the User Management replicated configurations. By default, this is the NETLOGON share.

Default Computer Management replication target location

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

Configure Site Map...

Desktop Authority will attempt to connect to either the ScriptLogic 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.



● Create site map automatically
○ Define custom site map
○ Do not use site map

Site map

Site	Servers
TAMPA	TAMPA-DC1,TAMPA-MS1,TAMPA-MS2
DALLAS	DALLAS-DC1,DALLAS-MS1,DALLAS-MS2
PITTSBURGH	PITT-DC1,PITT-MS1,PITT-MS2

Client execution options

If for some reason, Server Manager does not include any servers within the workstations 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. Click **Define custom site map** to customize the default site map settings.

ScriptLogic Service / Update Service tabs

Create site map automatically

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.

Define custom site map

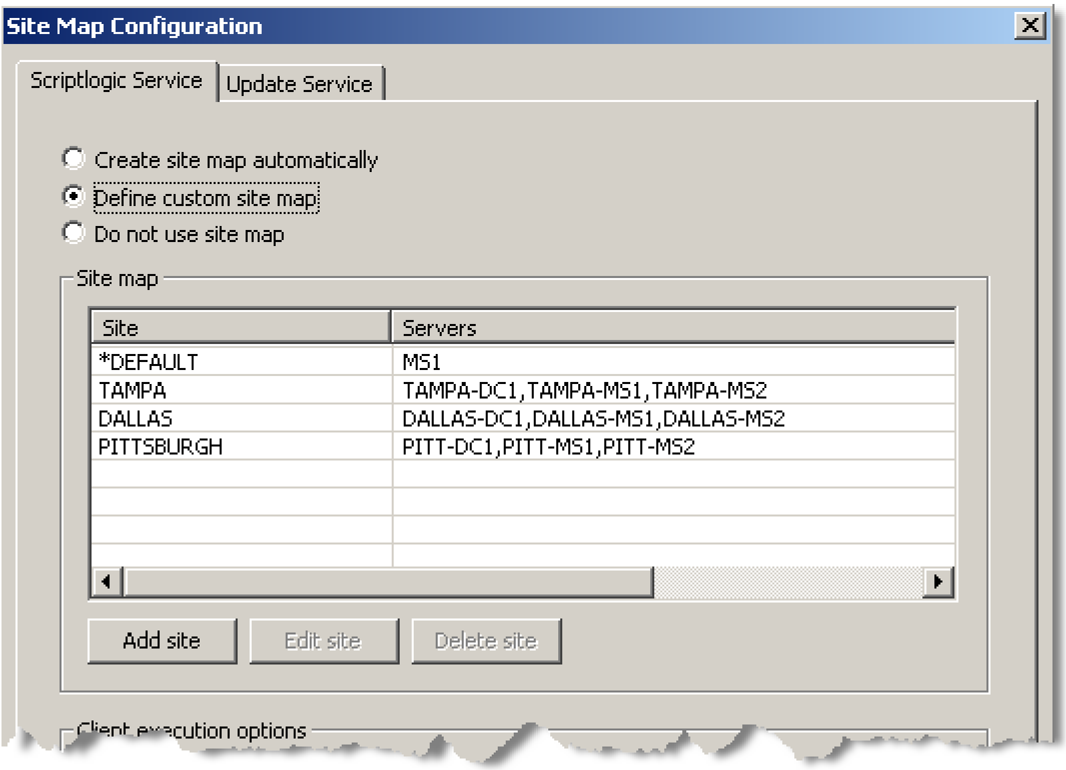
Select this option to define a custom site map for specific to the enterprise's topology. Selecting this option will enable the Site Map grid and allow for changes to it. The default site map configuration will appear in the grid, before any changes are made.

Do not use site map

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.

Configuring a custom site map

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



Site Map Configuration

○ Create site map automatically
● Define custom site map
○ Do not use site map

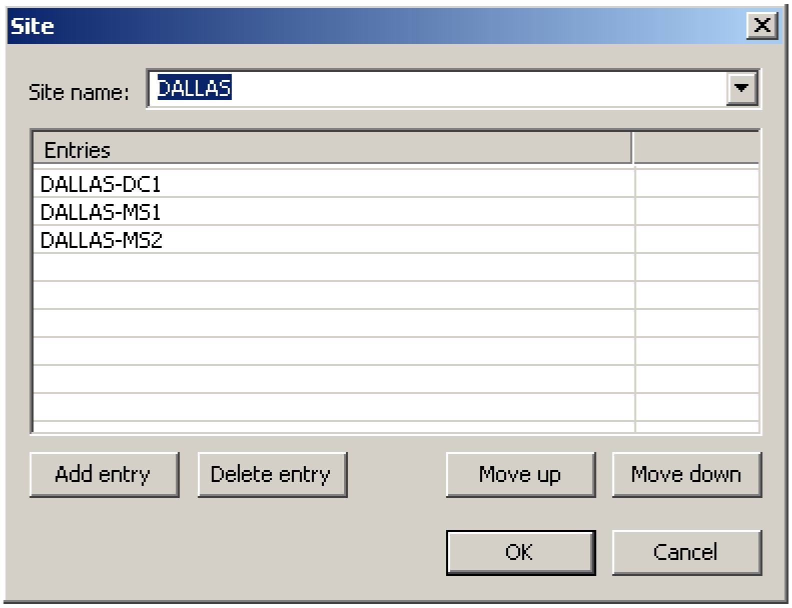
Site map

Site	Servers
*DEFAULT	MS1
TAMPA	TAMPA-DC1,TAMPA-MS1,TAMPA-MS2
DALLAS	DALLAS-DC1,DALLAS-MS1,DALLAS-MS2
PITTSBURGH	PITT-DC1,PITT-MS1,PITT-MS2

Add site

Click **Add site** to add a new site to the site map list. Select a known site from the drop down list, or click **Add entry** and type in a site name.

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.

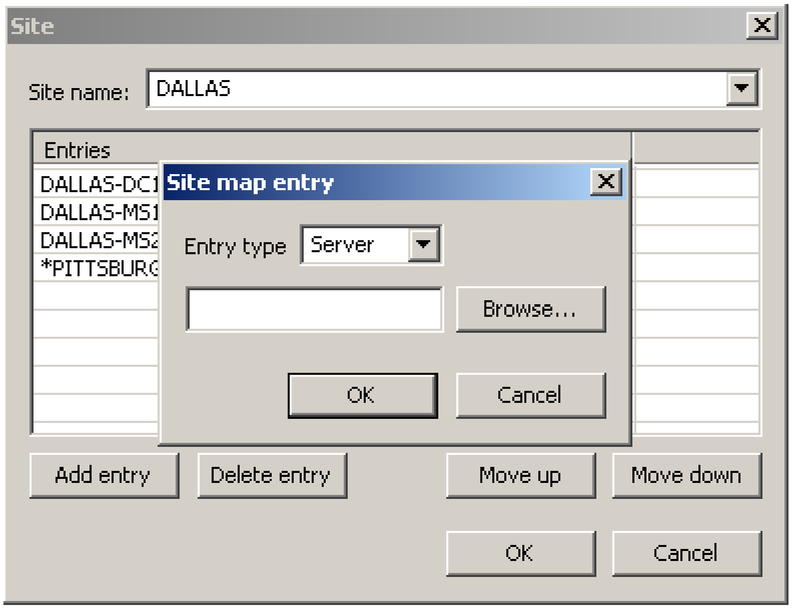


Site

Site name: DALLAS

Entries	
DALLAS-DC1	
DALLAS-MS1	
DALLAS-MS2	

From this site configuration window, the entries for each site will be entered. An entry can be either a server or a site.



Site name: DALLAS

Entries

DALLAS-DC1
DALLAS-MS1
DALLAS-MS2
*PITTSBURG

Entry type: Server

Select Server or Site from the Entry type drop down list. Click **Browse** to select a server or site from the servers and sites that Server Manager knows about or type in the name of any other server or site that should be used. An asterisk (*) will be automatically prepended to any site name in order to distinguish it from a server entry.

Click **Delete entry** to remove a server/site entry from the site map entry. Click **Move up/Move down** to change the order of the server and/or site entries.

Click **OK** to save the Site changes. Click **Cancel** to go back to the prior window without saving changes.

Edit site

Click **Edit site** to modify a site that is already on the site map list.

Delete site

Click **Delete site** to remove a site from the site map list.

Client execution options

Check login server first (ScriptLogic Service tab only)

This option is selected by default. This instructs Desktop Authority to check for a responsive ScriptLogic 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 ScriptLogic 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.

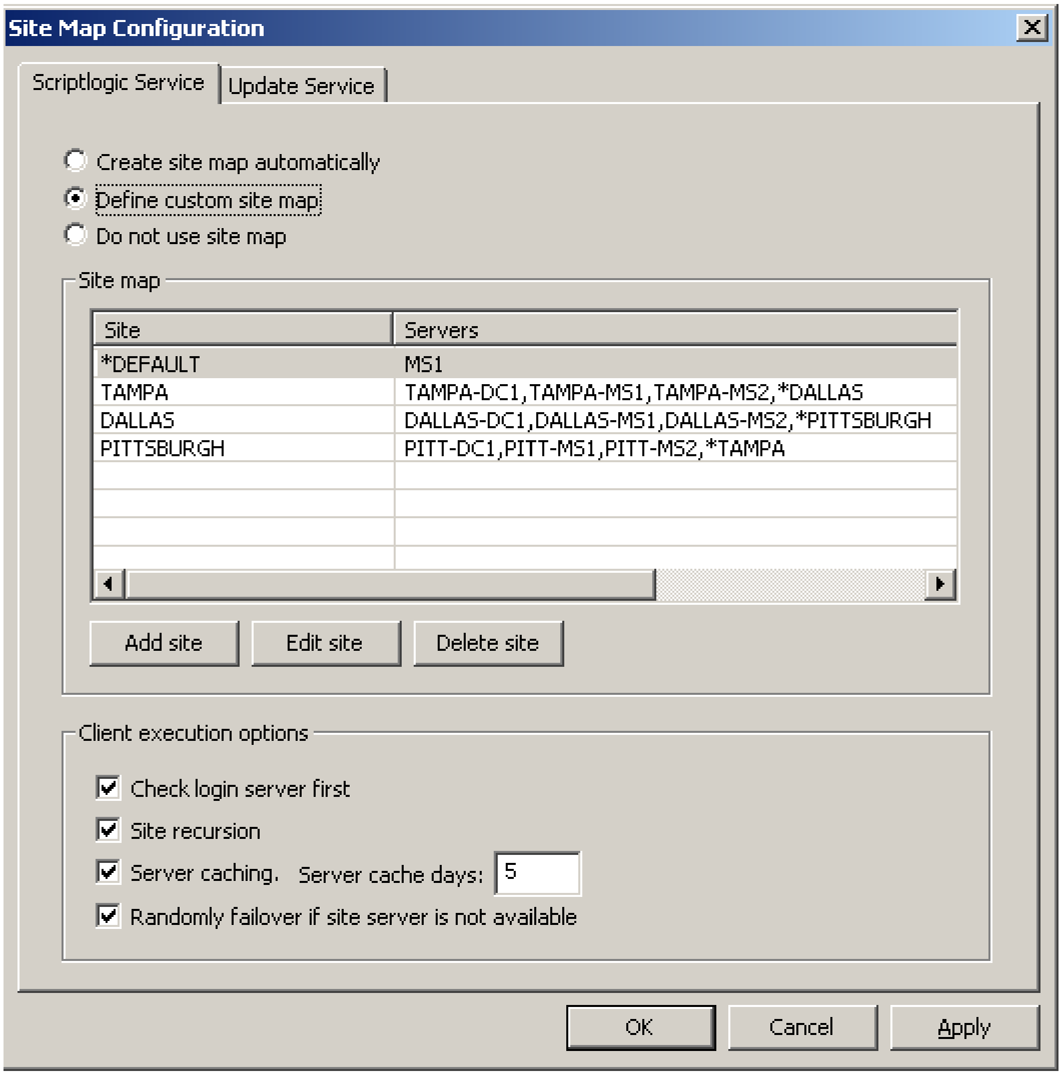
Server cache days

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.

Example Custom Site Map



Site Map Configuration

○ Create site map automatically
● Define custom site map
○ Do not use site map

Site map

Site	Servers
*DEFAULT	MS1
TAMPA	TAMPA-DC1,TAMPA-MS1,TAMPA-MS2,*DALLAS
DALLAS	DALLAS-DC1,DALLAS-MS1,DALLAS-MS2,*PITTSBURGH
PITTSBURGH	PITT-DC1,PITT-MS1,PITT-MS2,*TAMPA

Client execution options

☑ Check login server first
☑ Site recursion
☑ Server caching. Server cache days: 5
☑ Randomly failover if site server is not available

Scenario 1

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

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 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

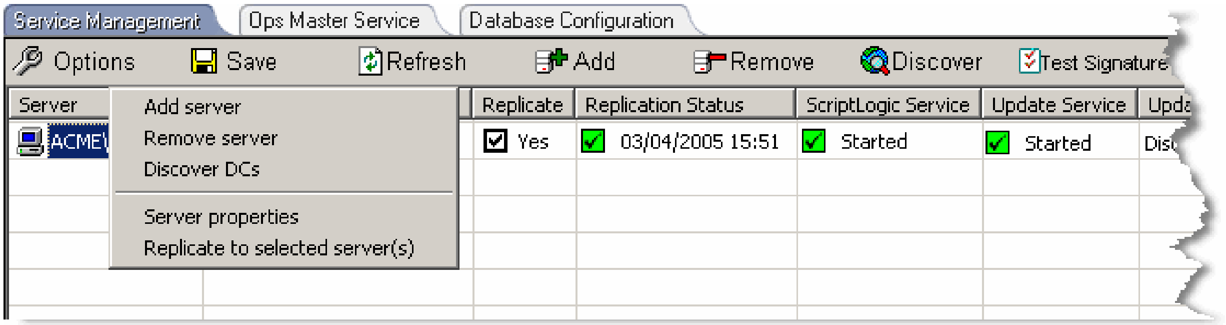
In this next example, Workstation1 makes a ScriptLogic service request. Workstation1 has no default site defined. Since Workstation1 ran slogic.bat from server MS3, DA will begin with an attempt to connect to the ScriptLogic service on the MS3 server. If the attempt fails, since there is no default site 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.

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* then the service request will immediately fail as the options do not allow the request to search for a responsive server.

SERVER PROPERTIES

Right-click on one or more existing server(s) in the grid for several server properties.



Server	Replicate	Replication Status	ScriptLogic Service	Update Service	Upda
ACME\	☑ Yes	✓ 03/04/2005 15:51	✓ Started	✓ Started	Disc

Add server

Select Add server to add a new server to the Server Manager grid.

Remove Server

Select Remove server to remove the selected server from the Server Manager grid.

Discover DCs

Select **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.

Server Properties

Server Name

This is a display only field. It represents the server that is being currently being configured.

Repl. Folder

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

CM Folder

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

SERVICE OPTIONS

Service

Services may be configured by selecting the specific server(s) and/or service(s) in the Server Manager grid. To select a service, click on a cell in the service column. To select multiple service cells from the grid, hold down the CTRL key and click on each individual cell.

The Server Manager grid also allows column and row selections. Click the Server or Service column header to select an entire column. Click > to select a row.

Once the selections are made, select the appropriate menu item or right-click the selected items to select an action from the shortcut menu.

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.

Configure

Configure allows the logon accounts and service start type to be configured. The startup type can be set to Automatic, Disabled, or Manual. The default startup type is set to Automatic. It is recommended to use the Automatic startup type unless troubleshooting service operations.

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

Install

Install performs the installation of the current version of the selected service. The ScriptLogic 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 ScriptLogic 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.

WHAT IS THE SCRIPTLOGIC SERVICE?

Conventional scripts typically execute under the security context of the user logging on. Unless users are made administrators of their own 2000/XP/2003/Vista machines, the ability to perform administrative tasks through a centralized logon script will be limited to each user's rights on their computer.

One of the key advantages offered by Desktop Authority is the ability to perform tasks that require administrative rights without sacrificing user-level security at the workstation. By using a specialized service, Desktop Authority is able to make changes to the registry, install software, add printers, synchronize time and perform any other tasks that require elevated rights during the logon, logoff or shut down sequences.

To install the ScriptLogic service, two unique sets of user credentials must be supplied. One user account must have local administrative rights on each workstation. By default, the Domain Admins group is a member of the local Administrators group on each 2000/XP/2003/Vista workstation, so selecting a user account that belongs to the Domain Admins group would satisfy this requirement. This account will be used by the ScriptLogic service on each server to remotely install the ScriptLogic service on each workstation.

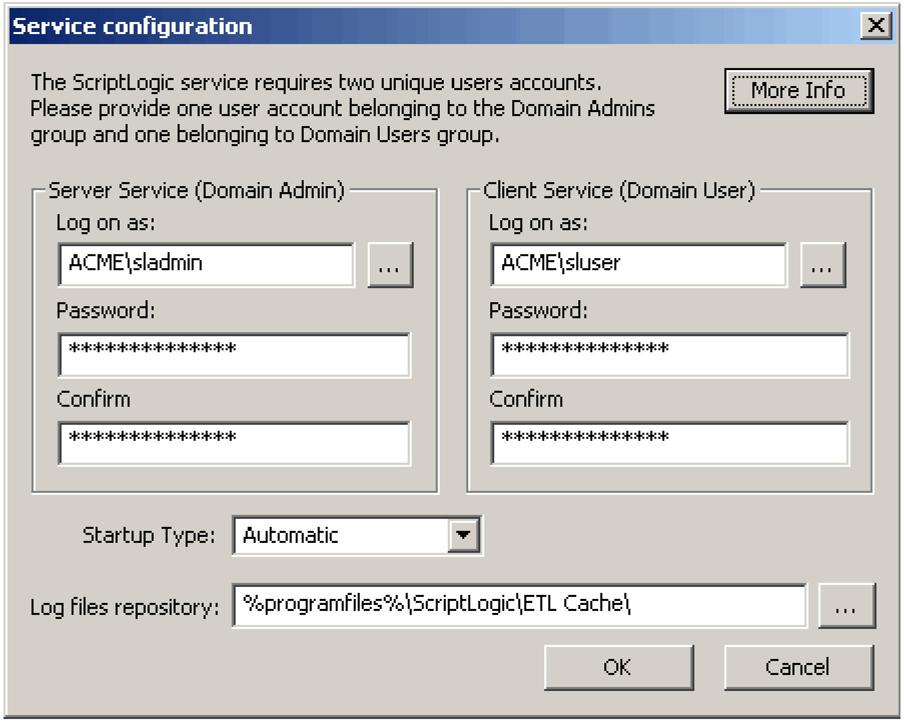
The second user account will be used by the ScriptLogic service on each workstation to perform the actual tasks that require the elevated administrative rights. This user account only needs to be a member of the Domain Users group.

Installing this service to all domain controllers is the preferred action for this service and provides the best configuration for load balancing.

CONFIGURING THE SCRIPTLOGIC SERVICE

To configure a *started* or *stopped* service in the Server Manager grid, right-click on a cell in the service column and select Configure Service from the shortcut menu.

The following Service configuration dialog will appear:



Service configuration

The ScriptLogic service requires two unique users accounts. Please provide one user account belonging to the Domain Admins group and one belonging to Domain Users group.

Server Service (Domain Admin)

Log on as: ACME\sladmin

Password: **************

Confirm **************

Client Service (Domain User)

Log on as: ACME\sluser

Password: **************

Confirm **************

Startup Type: Automatic

Log files repository: %programfiles%\ScriptLogic\ETL Cache\

Server Service (Domain Admin)

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 ... to select a user account.

Password

Enter the password associated with the selected log on account.

Confirm Password

Confirm the password for the selected log on account.

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 ... to select a user account.

Password

Enter the password associated with the selected user account.

Confirm Password

Confirm the password for the selected user 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 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 as well as patch data, spyware data and much more. During specific timed intervals, data is collected from this folder and parsed into the DAREPORTING database.

The default path is %programfiles%\ScriptLogic\ETL Cache\.

The folder specified must be a folder on the server for which the service is being configured for.

WHAT IS THE UPDATE SERVICE?

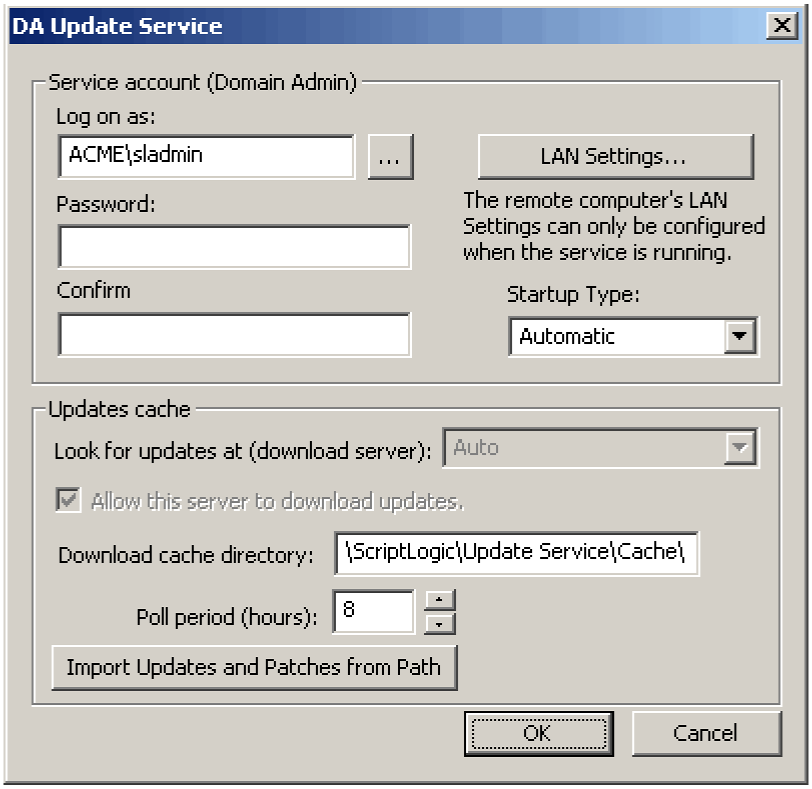
The Update Service is used by the USB/Port Security, Software Management, Patch Management and Anti-Spyware objects This service interfaces with www.scriptlogic.com and www.microsoft.com in order to retrieve licensing information as well as download patches, anti-spyware definition updates and ScriptLogic Patch Management updates. The Update Service offers an encrypted and secure connection to the ScriptLogic web site.

If a proxy is used to access the Internet, each server designated as a Update server must be configured to work with the proxy.

CONFIGURING THE UPDATE SERVICE

To configure a *started* or *stopped* Update Service in the Server Manager grid, right-click on a cell in the service column and select a configuration option from the shortcut menu.

When installing or configuring the service the following Update Service configuration dialog will appear:


DA Update Service
Service account (Domain Admin)
...
LAN Settings...
Updates cache
Import Updates and Patches from Path
OK
Cancel

Log on as: ACME\sladmin

Password:

Confirm

The remote computer's LAN Settings can only be configured when the service is running.

Startup Type: Automatic

Look for updates at (download server): Auto

☑ Allow this server to download updates.

Download cache directory: \ScriptLogic\Update Service\Cache\

Poll period (hours): 8

Service account (Domain Admin)

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 ... to select a user account.

Password

Enter the password associated with the selected log on account.

Confirm

Confirm the password for the selected log on account.

LAN Settings...

Click LAN Settings to configure the use of proxy server settings. LAN Settings can only be configured when the DA 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.

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.

Look for updates at (download server)

For servers that are not configured to download updates, specify the server where the update files will be made available from. 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 Updates 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%\ScriptLogic\Update Service\Cache.

Poll period (hours)

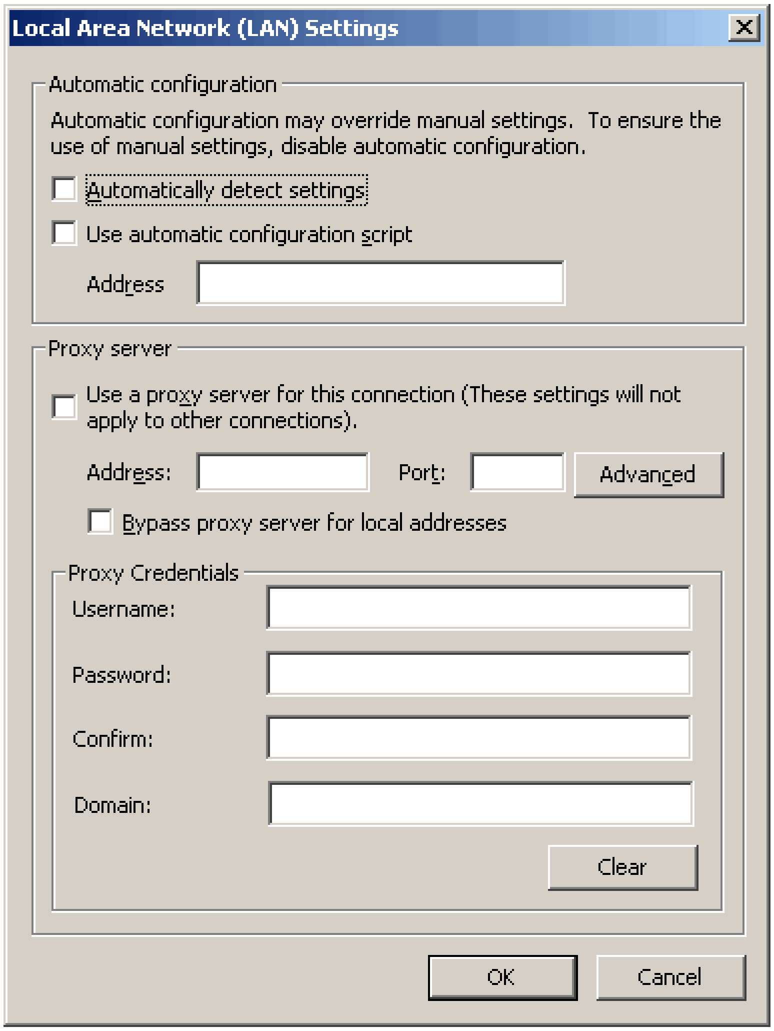
Specify how often the Update Service should look to ScriptLogic for updates.

Import Updates and Patches from Path

Click Import Updates and Patches from Path to import the update and patch data downloaded with the Desktop Authority Update and Patch Download Service (DAUPDS) applet. Once clicked, specify the location of the downloaded files. Click Import to start the process.

LAN Settings

Use this dialog to configure proxy server settings for the Update service.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

□ Use a proxy server for this connection (These settings will not apply to other connections).

Address: Port: Advanced

□ Bypass proxy server for local addresses

Proxy Credentials

Username:

Password:

Confirm:

Domain:

Clear

OK Cancel

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.

Address

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.

Address

Enter the name or TCP/IP address or host name of your network's proxy server.

Example:

```
192.168.100.205
```

If your organization has different proxy servers for different protocols, you may use the **Address** field for all applications. Create a single string in the **Address** field and leave the **Port** field blank.

Example:

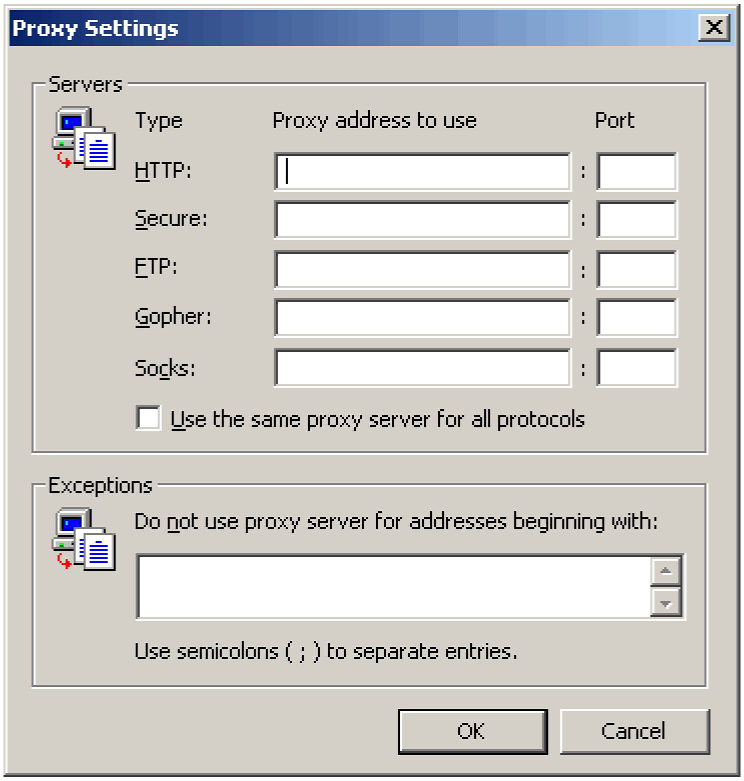
```
http=10.0.0.5:80;https=10.0.0.7:443;ftp=10.0.0.9:21
```

Port

Enter the TCP/IP port number of your network's proxy server.

Advanced

Click Advanced to configure advanced proxy server configurations.



Proxy Settings

Servers

Type	Proxy address to use		Port
HTTP:		:	
Secure:		:	
FTP:		:	
Gopher:		:	
Socks:		:	

□ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.

Servers

Proxy address to use

For each type of proxy server in use, enter the TCP/IP address or host name of the proxy server.

Port

Enter the corresponding TCP/IP port number for each of the proxy servers.

Use the same proxy server for all protocols

Check this box to use a single proxy address and port for all types of proxy servers.

Exceptions

Do not use proxy server for addresses beginning with

Enter addresses that the proxy server should not be used with. Separate multiple addresses with a semicolon (;).

Bypass proxy server 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.

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.

Domain

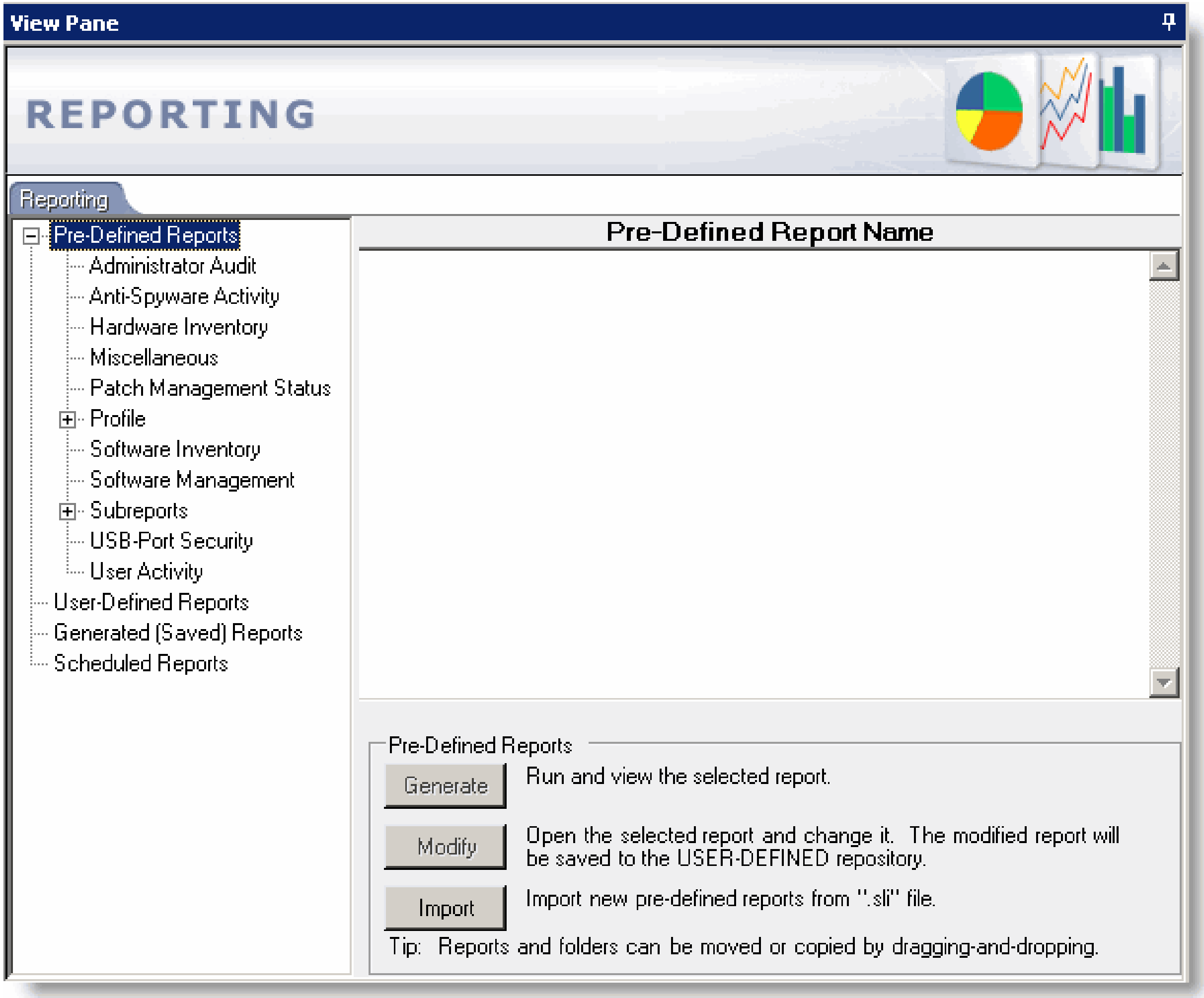
Enter the Domain name to which the proxy server belongs to.

Clear

Click Clear to remove the entered Proxy Server credentials.

REPORTING OVERVIEW*

The Reporting object presents the opportunity to run predefined reports distributed by ScriptLogic 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.



Generate: Run and view the selected report.

Modify: Open the selected report and change it. The modified report will be saved to the USER-DEFINED repository.

Import: Import new pre-defined reports from "*.sli" file.

Tip: Reports and folders can be moved or copied by dragging-and-dropping.

Pre-Defined Reports

Select a report category from the Pre-Defined Reports tree. The Pre-Defined Reports object contains reports created by ScriptLogic. 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 by ScriptLogic.

User-Defined Reports

Select User-defined Reports from the reporting tree. The User-defined Reports object lists reports available for modification or generation. 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 due to 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 OpsMaster service and the ETLProcessor plugin. These two plugins are available in the Server Manager > Ops Master Service tab for configuration.

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, Patch Management, Anti-spyware and USB/Port Security. User based _Ref-498741220Data Collection can be configured for login/logoff and lock/unlock events.

*This feature is not a standard part of Desktop Authority Express. To obtain this feature, Desktop Authority Express must be upgraded to the full version of Desktop Authority.

REMOTE MANAGEMENT*

The Desktop Authority Remote Management Console 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.

The Navigation Pane is used to navigate to computers via Microsoft Windows Network connections or Active Directory. Expand each section to enumerate and locate computers to connect to.

My Network - Enumerates all computers for each network protocol available.
My Active Directory - Enumerates all computers using the Active Directory structure.
Custom Servers- Lists all *Favorite* computers.

The computers enumerated in the navigation pane use the following icons to denote the Remote Management service status.

- ✓ Denotes the computer is running the Desktop Authority service.
- ✗ Denotes the computer is not running the Desktop Authority service.
- ? Denotes the computer is being queried regarding the status of the Desktop Authority service.

Once a computer is located, right-click on the computer name to access the available actions to take on the computer. The popup window allows the following actions:

Remote Control

Select **Remote Control** from the popup menu to automatically connect to the selected computer.

Restart

Select **Restart** from the popup menu to restart the selected computer.

Refresh

Select **Refresh** from the popup menu to Refresh the status of the selected computer and whether the Desktop Authority service is started or stopped.

Deploy Service

Select **Deploy Service** from the popup menu to deploy the Desktop Authority service to the selected computer.

Remove Service

Select **Remove Service** from the popup menu to remove the Desktop Authority service from the selected computer.

A**dd to Custom Servers**

Select **Add to Custom Servers** to add the selected computer to a saved list of favorite computers. Use this list for computers that are commonly accessed for Remote Management.

By default, the View pane provides quick access to the Desktop Authority Dashboard. Once a computer is chosen for remote control access, the remote control session will be displayed in the display pane.

Selecting a computer in the Navigation pane does not automatically refresh the View pane. To refresh the pane, select an item on the shortcut menu.

*This feature is not a standard part of Desktop Authority Express. To obtain this feature, Desktop Authority Express must be upgraded to the full version of Desktop Authority.

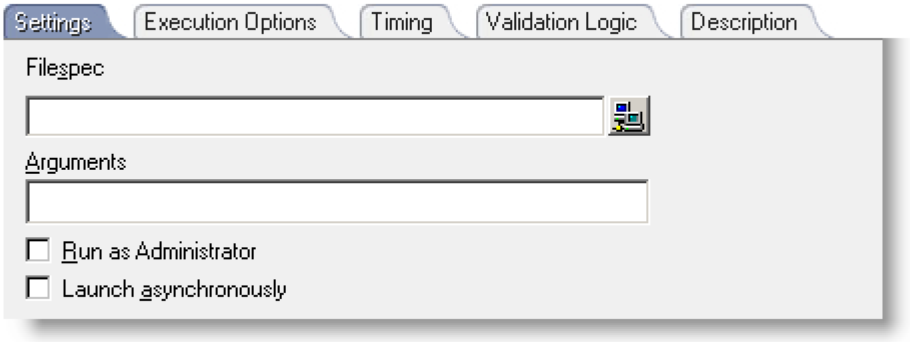
COMPUTER MANAGEMENT

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.



Settings

Filespec

Enter the complete path and filename where the application's executable exists or click 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.

Run as Administrator

Select this check box to run the application with Administrator privileges. The application will be executed using Desktop Authority's RunAs Admin service.

If this check box is cleared and the application requires administrator privileges, the application will not run.

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.

Execution Options

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 a message into the text box to be shown in the popup message.

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 after element executes

Select this option to determine the timing in which a reboot will take place, if required, by the executed element.

Reboot immediately

Allow the required reboot to happen immediately following the element configuration.

Reboot with count down

xx seconds until reboot

Warn the end user of an impending reboot operation. The warning dialog will be displayed for the number of seconds specified.

Allow users to postpone reboot

Select this box to allow the user to postpone the impending reboot.

Reboot later

Select this option to delay the reboot to a time that the user deems acceptable.

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.

Description

Select the **Description** tab to set the description for this element.

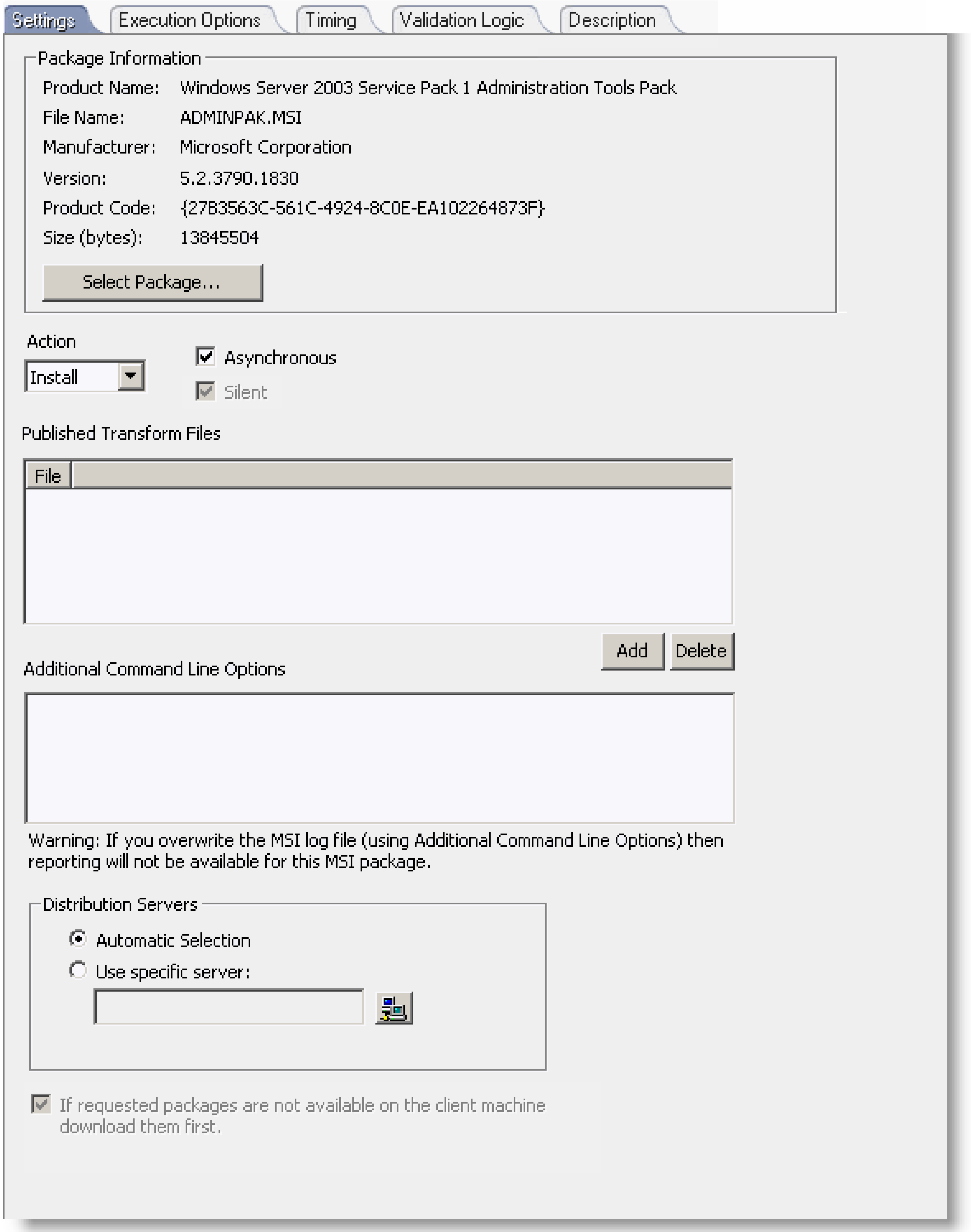
MSI PACKAGES*

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.

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.



Package Information

Product Name: Windows Server 2003 Service Pack 1 Administration Tools Pack

File Name: ADMINPAK.MSI

Manufacturer: Microsoft Corporation

Version: 5.2.3790.1830

Product Code: {27B3563C-561C-4924-8C0E-EA102264873F}

Size (bytes): 13845504

Action: Install

☑ Asynchronous

☑ Silent

Published Transform Files

Additional Command Line Options

Warning: If you overwrite the MSI log file (using Additional Command Line Options) then reporting will not be available for this MSI package.

Distribution Servers

● Automatic Selection

○ Use specific server:

☑ If requested packages are not available on the client machine download them first.

Settings

Package Information

The package information box displays information regarding the selected package. Product Name, File Name, Manufacturer, Version, Product Code and File Size information are displayed.

Select Package

Click Select Package to choose a package from a list of published packages. When clicked, a popup list is displayed with packages available for selection.

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

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.

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 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.

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 the 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?

If requested packages are not available on the client machine, download them first.

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.

Execution Options

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 a message into the text box to be shown in the popup message.

Ask users 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 after element executes

Select this option to determine the timing in which a reboot will take place, if required, by the executed element.

Reboot immediately

Allow the required reboot to happen immediately following the element configuration.

Reboot with count down

xx seconds until reboot

Warn the end user of an impending reboot operation. The warning dialog will be displayed for the number of seconds specified.

Allow users to postpone reboot

Select this box to allow the user to postpone the impending reboot.

Reboot later

Select this option to delay the reboot to a time that the user deems acceptable.

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.

Description

Select the **Description** tab to set the description for this element.

*This feature is not a standard part of Desktop Authority Express. To obtain this feature, Desktop Authority Express must be upgraded to the full version of Desktop Authority.

✚ Patch Deployment *

Desktop Authority's Patch Distribution and Deployment feature ensures that your Microsoft desktop Operating Systems and applications are kept up-to-date with the latest patches from Microsoft. Patches can be deployed to Microsoft Windows 2000 Professional and Server, Microsoft Windows 2003, Microsoft Windows 2008, Microsoft Windows XP and Microsoft Windows Vista, both 32- and 64-bit operating systems.

The Patch Deployment object provides the ability to deploy patches on clients during system Startup, Shutdown, Refresh intervals, or Scheduled intervals, based on the specified Validation Logic. Before a patch is installed, several checks are completed to ensure that the Operating System, product, version, language, and etc. match the intended recipient's configuration. Patches may also be uninstalled from a client machine if the patch contains uninstall capabilities.

Desktop Authority will not attempt to install patches if the client does not have enough available disk space. The engine determines the amount of available disk space before the patch is installed. By default, 200 mb of disk space must be available to install any patch. This default can be overridden by defining a value in the global or profile definition file.

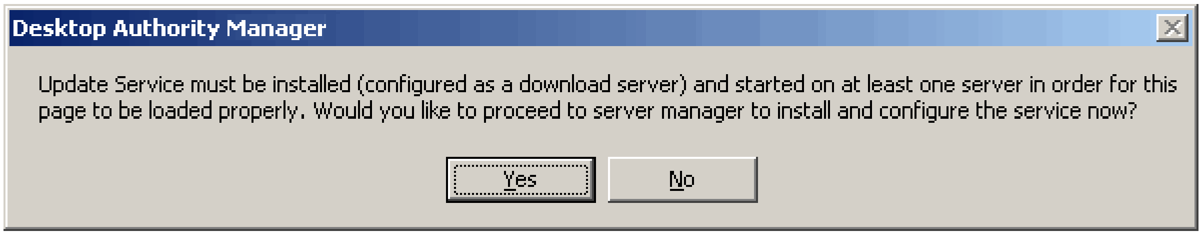
The variable #HotFixFreeSpaceNeededInMB is used to override the available disk space amount. Select Global Options > Definitions or select the Definitions tab on the profile's settings.

Example:

```
#HotFixFreeSpaceNeededInMB="100"
```

Patch Deployment, in evaluation mode, allows patches to be downloaded from Microsoft. However, only Low severity patches can be installed via desktop Authority in this evaluation mode.

Once the Patch Deployment Subscription service is purchased, all patch file(s) available from Microsoft can be downloaded and installed/uninstalled centrally with Desktop Authority. The Update Service must be installed and configured in order for Desktop Authority to retrieve the latest patch listings and files. If it is not configured at the time the Patch Deployment object is selected in the Navigation Pane, a message will be displayed with an opportunity to install and configure the service.



Desktop Authority Manager

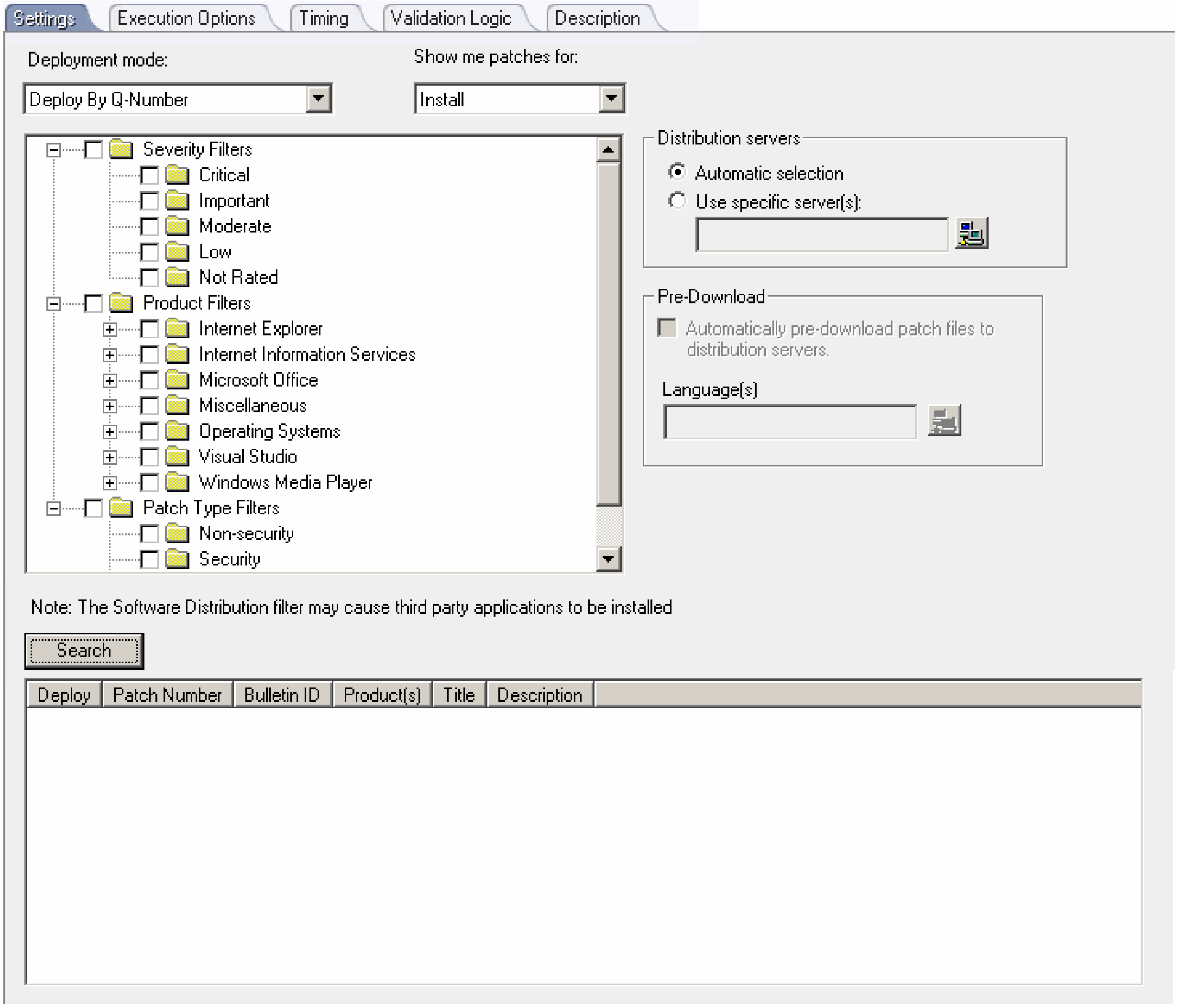
Update Service must be installed (configured as a download server) and started on at least one server in order for this page to be loaded properly. Would you like to proceed to server manager to install and configure the service now?

Once configured, the download servers will query scriptlogic.com to determine the product mode and download updated patch file listings, when available, and requested patch files. For more information on the Update Service, see What is the Update Service?

Timely installation of patches is essential to the security of the enterprise network. Following the recommended configurations will help to administer, distribute and install Microsoft operating system and product patches in a timely manner, without compromise to the security of the network.

Note: If the server does not have Internet access, the Desktop Authority Updates and Patch Download Service (DAUPDS) can be used to provide the Enterprise the ability to download patches and updates for Desktop Authority Servers that may not or can not have Internet access. This tool will download the updates and patches which can be imported into Desktop Authority for consumption by the Update Service. For more information on this tool, go to the Desktop Authority support page on the ScriptLogic website.

Settings



Deployment mode: Deploy By Q-Number

Show me patches for: Install

- □ Severity Filters
  - □ Critical
  - □ Important
  - □ Moderate
  - □ Low
  - □ Not Rated
- □ Product Filters
  - □ Internet Explorer
  - □ Internet Information Services
  - □ Microsoft Office
  - □ Miscellaneous
  - □ Operating Systems
  - □ Visual Studio
  - □ Windows Media Player
- □ Patch Type Filters
  - □ Non-security
  - □ Security

Distribution servers

● Automatic selection

○ Use specific server(s):

Pre-Download

□ Automatically pre-download patch files to distribution servers.

Language(s)

Note: The Software Distribution filter may cause third party applications to be installed

Deploy	Patch Number	Bulletin ID	Product(s)	Title	Description

The Software Distribution list may contain third party applications such as Firefox, Adobe Reader, etc. and may be chosen to be deployed to client machines.

Deploy by Q-Number/Deploy by Criteria/Deploy by Individual Patch

Deploy by Individual Patch allows one or more individual patches to be selected for deployment. Patches that are available for more than one installation platform are selected only once based on the actual patch number or bulletin id. The patch will be installed for all target installation platforms that the patch supports. Use the Filter criteria to locate and select the necessary patch files. When a client logs on and validates for the patch, the selected patch files will be installed.

Deploy by Criteria allows all patches with specific severities and products to be installed. Simply select the severities and products in the Filter criteria box. When a client logs on and validates for the patch deployment element, all patch files for the selected severities and products will be installed.

Deploy by Q-Number allows one or more individual patches to be selected for deployment. Patches that are available for more than one installation platform are selected based on the actual installation platform. A single patch number or bulletin id may be selected more than once in order to patch the selected target platforms. Use the Filter criteria to locate and select the necessary patch files. When a client logs on and validates for the patch, the specified patch files will be installed.

Show me patches for

Select from Install/Rollback (Uninstall) from the drop list. Selecting Install will show all patches that can be chosen for installation on target machines. Selecting Rollback will show all patches that contain an Uninstall procedure. Any patch selected with this option will be removed from target machines it if exists.

Filter

Use the Filter tool to minimize the available patch list based on severity and/or product. Select the Severity Filters box to automatically select each severity listed below it or select individual severities below the Severity Filters box. Clear the Severity Filters check box to clear all selected severities.

Select the Product Filters box to automatically select all products listed below it or select individual products below the Product Filters box. Clear the Product Filters box to clear all selected products.

Search

Click Search to filter the patch list based on the Severity and Product filters chosen in the Filter list. A count of selected patches will be displayed following the search.

Patch List

The Patch list is available when the Deploy by Individual Patch or Deploy by Q-Number option is selected. This list displays all patches matching the filter criteria. Information regarding each patch includes the Patch number and Affected Products. The patch list is sortable by any one of the columns available in the list. Sort the list by clicking on a column header.

Select a patch to deploy by selecting the Deploy box. To deploy multiple consecutive patches from the list, click on the first one. While holding down the SHIFT key, select the last consecutive patch, and then select the Deploy box. Multiple non-consecutive patches may be selected from the list by pressing the CTRL key while selecting each individual patch and then selecting the Deploy box.

Distribution servers

Select Automatic selection to copy the patch file(s) to the client from the selected server. Select Use specific servers to define a specific server(s) to copy the patch file(s) from. Separate multiple server names using a semicolon (;).

Pre-Download

Automatically pre-download patch files to distribution servers. (Available for Deploy by criteria only)

Select this box to allow the Update Service to automatically download new patches when there are any that match the specified Products and Severities.

Languages

Click to select one or more languages for the automatic pre-download patch files to download. Select from German, English, French and/or Spanish.

Execution Options

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 a message into the text box to be shown in the popup message.

Ask users 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 after element executes

Select this option to determine the timing in which a reboot will take place, if required, by the executed element.

Reboot immediately

Allow the required reboot to happen immediately following the element configuration.

Reboot with count down

xx seconds until reboot

Warn the end user of an impending reboot operation. The warning dialog will be displayed for the number of seconds specified.

Allow users to postpone reboot

Select this box to allow the user to postpone the impending reboot.

Reboot later

Select this option to delay the reboot to a time that the user deems acceptable.

Note: Opting to delay a reboot after patches are installed is not recommended as the installation of many patches do not complete until after a reboot has occurred.

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.

Installing patches during Refresh Validation Logic Timing is not recommended. Each time a patch installation is requested, the patch assessment process will run. Setting the installation to execute at Refresh will cause the patch assessment process to execute at this time as well (every hour) on all target machines. The patch assessment process could turn into a CPU intensive procedure.

Description

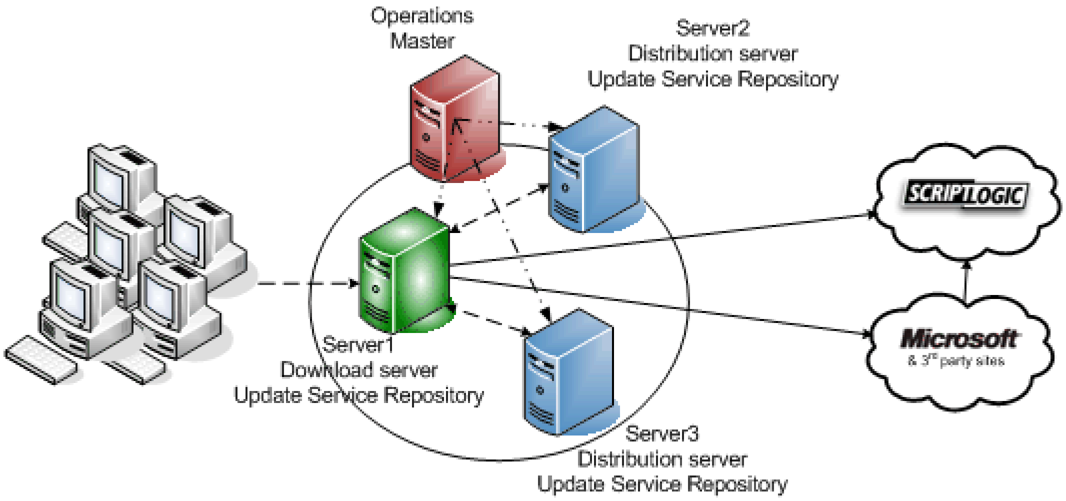
Select the **Description** tab to set the description for this element.

*This feature is not a standard part of Desktop Authority Express. To obtain this feature, Desktop Authority Express must be upgraded to the full version of Desktop Authority.

UPDATE SERVICE BEST PRACTICES

Timely installation of updates and patches are essential to the security of the enterprise network. Following the recommended configurations below will help to administer, distribute and install Microsoft operating system and product patches and updates in a timely manner, without compromise to the security of the network.

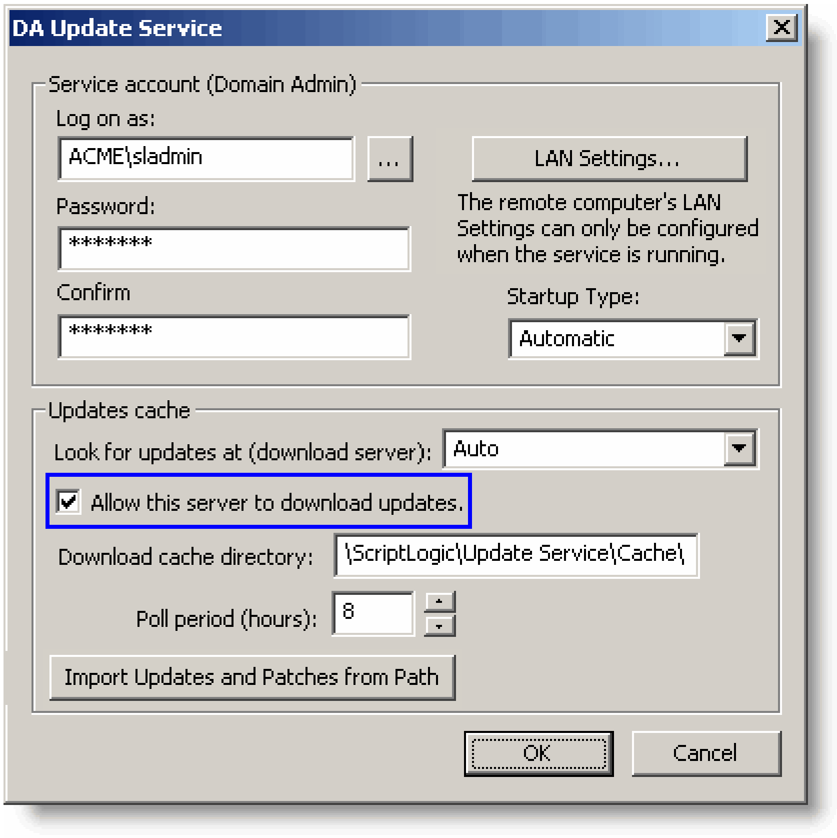
Single Site LAN



The installation of the Update Service is required in order to use Software Management, USB/Port Security, Patch Management and/or Anti-Spyware objects. The Update Service is installed within the Server Manager.

The MSI Packages object publishes packages to each server that has the Update Service installed.

To best configure the Update Service for a single site network, there should be one server that is designated as the download server. A server is configured to be a download server in the Update Service configuration dialog.



DA Update Service

Service account (Domain Admin)

Log on as: ACME\sladmin

Password: *******

Confirm: *******

The remote computer's LAN Settings can only be configured when the service is running.

Startup Type: Automatic

Updates cache

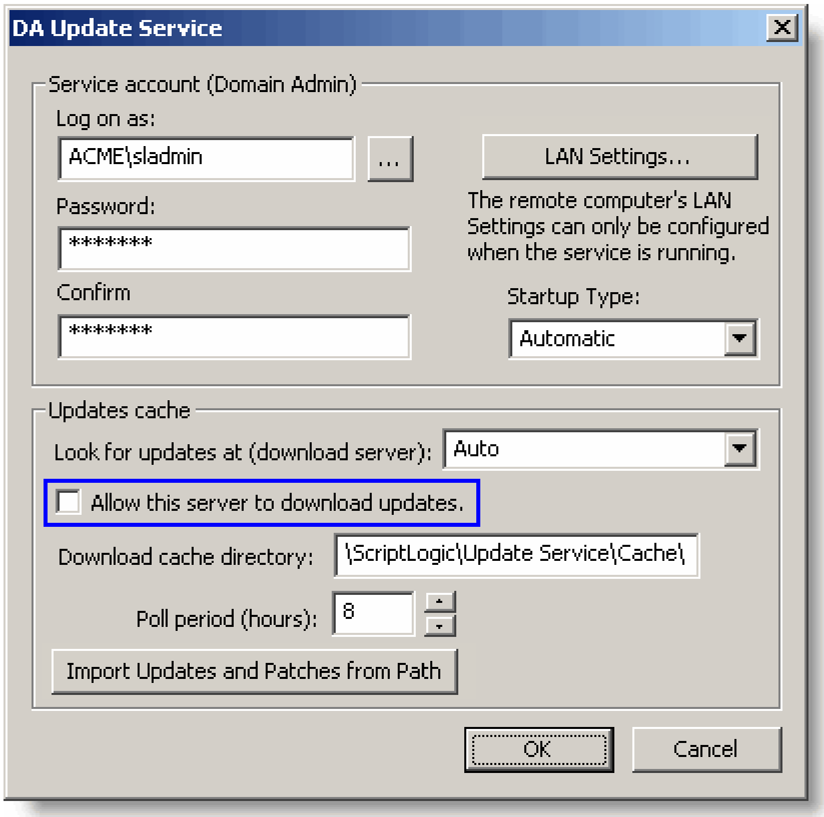
Look for updates at (download server): Auto

☑ Allow this server to download updates.

Download cache directory: \ScriptLogic\Update Service\Cache\

Poll period (hours): 8

Download Server configuration



DA Update Service

Service account (Domain Admin)

Log on as: ACME\sladmin

Password: *******

Confirm: *******

The remote computer's LAN Settings can only be configured when the service is running.

Startup Type: Automatic

Updates cache

Look for updates at (download server): Auto

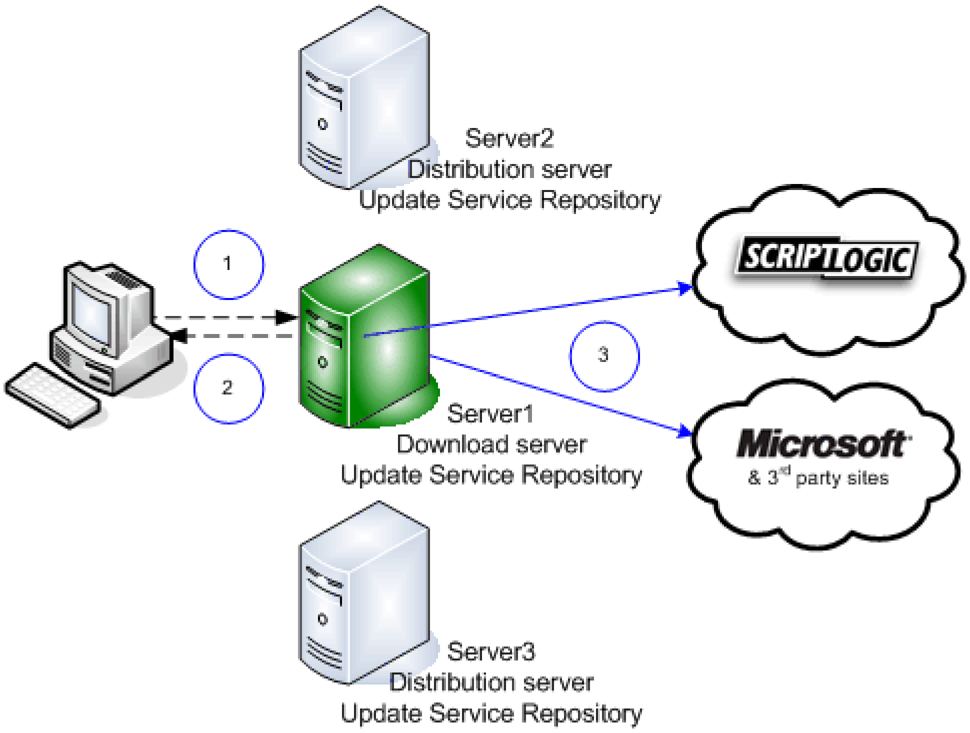
□ Allow this server to download updates.

Download cache directory: \ScriptLogic\Update Service\Cache\

Poll period (hours): 8

Distribution server configuration

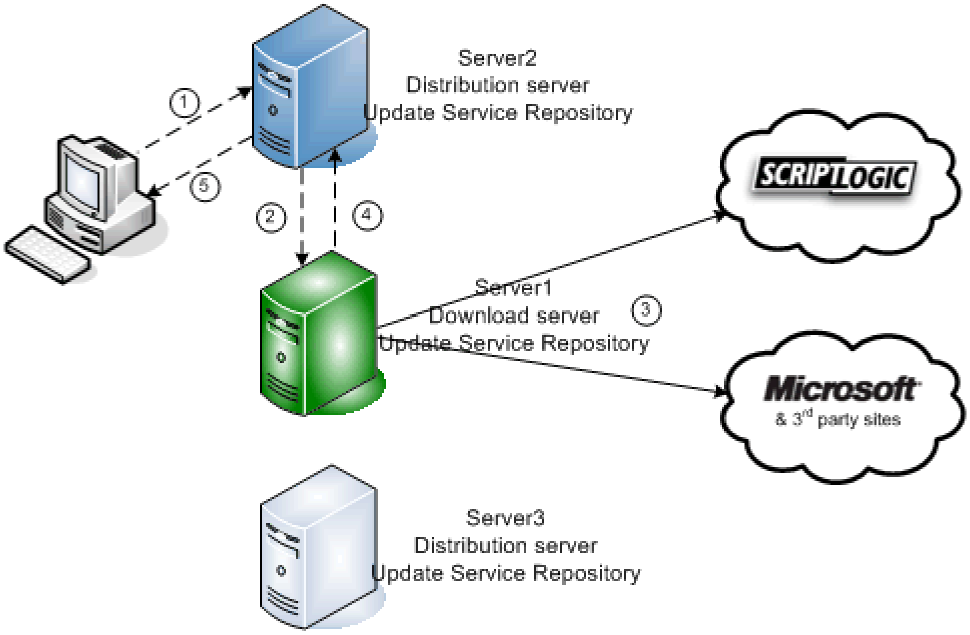
The download server pulls patch files from Microsoft. The downloaded patch files are stored in the directory specified in the Update Service configuration dialog. This directory by default is %Program Files%/ScriptLogic/Update Service/Cache. The download server also connects with ScriptLogic to pull down licenses information, anti-spyware definition updates, patch database updates and ScriptLogic Patch Management updates. The connection to the ScriptLogic web site is a secure connection.



In the illustration above, a client logs on to the network and is connected to Server11 via a random selection by the Desktop Authority engine. In this scenario, Server1 is configured as the download server. If the patch exists on the server, it is distributed to the client as requested, based on the validation logic specified for the patch file(s).

If the patch file has not yet been downloaded by the server, a request is sent via the Update Service to Microsoft and the patch file(s) is downloaded3. In this case, one of two scenarios will occur on the client. Depending on the configuration of the "If patch is not available, do not continue" prompt on the Patch Deployment element, either Desktop Authority will continue to process on the client without installing the patch, or it will pause and wait for the patch to download and install before going any further. If the prompt is selected (checked on), the client will wait for the patch to download and install. If the prompt is cleared (checked off), the client will attempt to install the patch during the next logon attempt.

In this scenario, Server2 and Server3 are designated as distribution servers. This means that these servers will never directly request a patch file from Microsoft. Instead, these servers will send a request to the networks download server for the patch file. At this time, the patch file will be delivered to the distribution server that requested it.

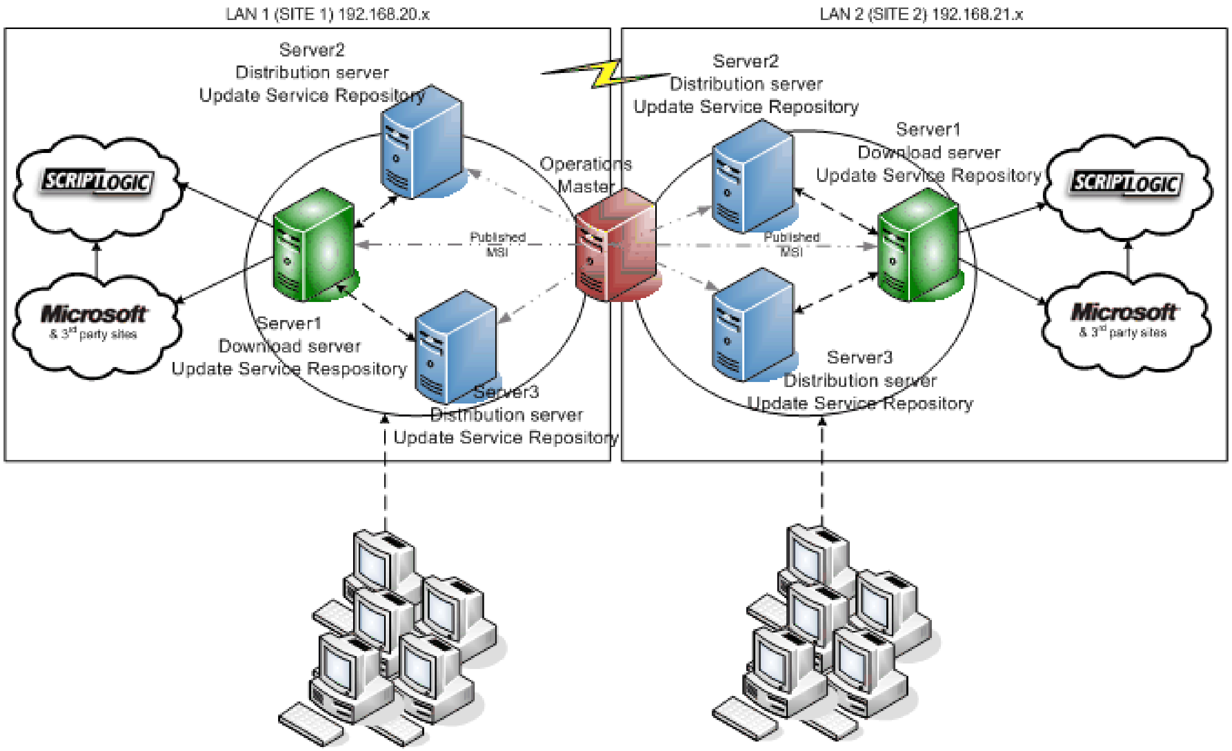


When a client logs onto the network and is connected to a distribution server1, a request is sent from the distribution server to the download server for the patch file (if it does not already exist on the distribution server)2. If the patch file does not already exist on the download server, it is downloaded by the Update Service3. The patch file is then distributed to the distribution server4 and then deployed to the client5.

Again, one of two scenarios will occur on the client when connected to a distribution server. Depending on the configuration of the "If patch is not available, do not continue" prompt on the Patch Deployment element, either Desktop Authority will continue to process on the client without installing the patch, or it will pause and wait for the patch to download and install before going any further. If the prompt is selected (checked on), the client will wait for the patch to download and install. If the prompt is cleared (checked off), the client will attempt the patch installation the on the next logon attempt.

Multiple Site LAN

On a network configured with multiple sites, the Patch Deployment process is similar as discussed above. However, there are some differences which are explained below.



In the above illustration, the network consists of two sites. Each site should have its own single download server. All other servers on the site should be set up as distribution servers. The Operations Master publishes all packages for the MSI Packages object to all servers (on all sites) that have a running Update Service.

Upon logon, a client is connected to a server within the site the client exists in. Upon a patch deployment request, a server within its own site is randomly chosen by the Desktop Authority engine. If the download server is chosen, the necessary patches are deployed to the client as requested.

If the patch file has not yet been downloaded by the server, a request is sent via the Update Service to Microsoft and the patch file(s) is downloaded. In this case, one of two scenarios will occur on the client. Depending on the configuration of the "If patch is not available, do not continue" prompt on the Patch Deployment element, either Desktop Authority will continue to process on the client without installing the patch, or it will pause and wait for the patch to download and install before going any further. If the prompt is selected (checked on), the client will wait for the patch to download and install. If the prompt is cleared (checked off), the client will attempt the patch installation the on the next logon attempt.

If a distribution server is selected via the Desktop Authority engine and the patch is available it is automatically deployed to the client.

If the patch file is not yet available on the distribution server, a request will be sent to the download server. The patch will be downloaded from Microsoft (if necessary) moved to the distribution server and then deployed to the client. Again, at this time, one of two scenarios will occur on the client when authenticated by the distribution server. Depending on the configuration of the "If patch is not available, do not continue" prompt on the Patch Deployment element, either Desktop Authority will continue to process on the client without installing the patch, or it will pause and wait for the patch to download and install before going any further. If the prompt is selected (checked on), the client will wait for the patch to download and install. If the prompt is cleared (checked off), the client will attempt the patch installation the on the next logon attempt.

It is important to note that depending upon the speed of the link between the sites in this type of configuration versus the speed of the Internet connection, it may be faster to manually copy the download cache between sites versus allowing the patch files to propagate through the system as they are needed.

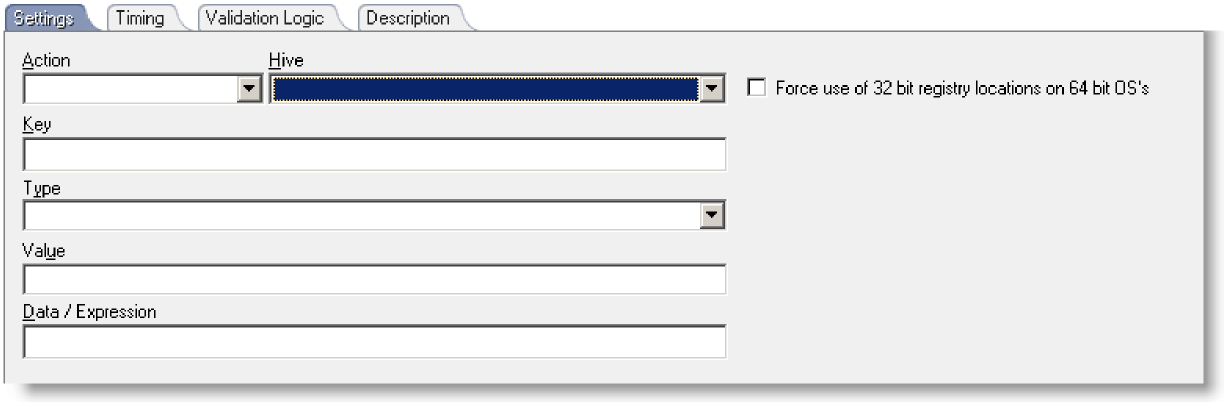
Miscellaneous Notes

- Although the Service Pack Deployment and Patch Deployment objects seem very similar, use the Service Pack Deployment object to install full service packs offered by Microsoft. A patch is an interim update which fixes one or more specific problems. A service pack is a cumulative update to fix multiple bugs and may include product enhancements. A service pack includes many patches bundled into a single service pack update.
- Prior to deploying a patch to the enterprise, use Desktop Authority's Validation Logic to target specific users or groups of users and/or specific computers or groups of computers for testing of patch installations.
- Since some patch installations may take considerable time to complete, It is recommended to target significant patches to occur at logoff time rather than logon.
- Patches for Office applications may require access to the original media (CD or DVD). To support Office patches without prompting the user to insert any form of media, the original product media should be made available on a CD/DVD drive that is accessible to all over the network.
- The Update Service requires Internet access to www.scriptlogic.com and www.microsoft.com. If a proxy is used to access the Internet, the download server must be configured to work with the proxy.

REGISTRY

The **Registry** object provides a single point of control over changing values in the registry of a computer. This object will modify Windows 2000/XP/2003/2008/Vista registry key/value under the context of the Local System account.

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

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.
- Delete Key
  Remove the specified key from the hive. For safety reasons, DeleteKey will only delete a single key. DeleteKey will not delete a key if there are subkeys beneath it.
- *Add Key*
  Create a key in the specified hive.

Hive

Select the hive on which to perform the action from the list. The following hives can be selected:

- HKEY_CLASSES_ROOT
Contains all file associations, OLE information and shortcut data.
- HKEY_LOCAL_MACHINE
Contains computer specific information about the type of hardware, software, and other preferences on a given PC.
- HKEY_USERS/.DEFAULT
Contains default profile preferences.
- HKEY_CURRENT_CONFIG
Represents the currently used computer hardware profile.

Force use of 32 bit registry locations of 64 bit OS's

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.

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
- REG_DWORD
- REG_DWORD_BIG_ENDIAN
- REG_DWORD_LITTLE_ENDIAN
- REG_EXPAND_SZ
- REG_FULL_RESOURCE_DESCRIPTOR
- REG_MULTI_SZ
- REG_NONE
- 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*.

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, enter the word clear surrounded by parentheses.

Example:

```
(clear)
```

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.

Description

Select the **Description** tab to set the description for this element.

SERVICE PACK DEPLOYMENT

The **Service Pack Deployment** object allows you to deploy service packs for all 2000/XP/2003/2008/Vista clients and servers (64-bit operating systems included).

A few items to note regarding service pack deployment:

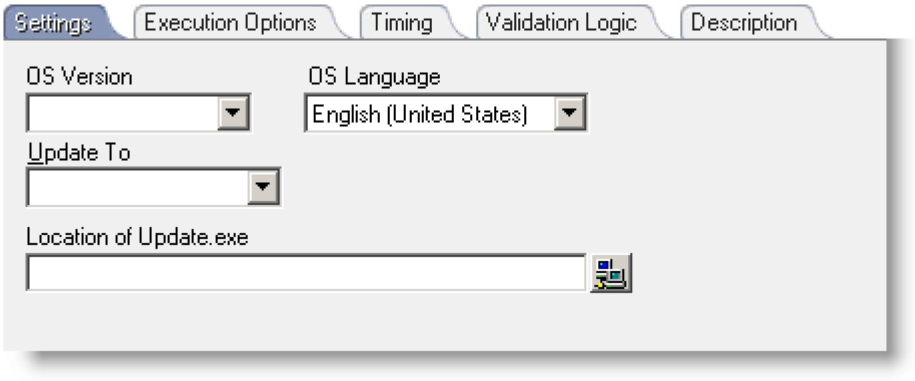
- Computer Management Service Pack Deployment will only install service packs to 2000/XP/2003/Vista clients/servers if connected over a LAN connection.
- Computer Management Service Pack Deployment will never downgrade the currently installed service pack on a computer.
- Computer Management Service 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, 1.5G (1500mb) 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.



OS Language: English (United States)

Settings

OS Version

Select an Operating System version from the list. Valid selections are Windows 2000, 2003, 2008, Windows Vista, Windows XP and Windows XP64 clients and servers.

OS 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

Enter the complete path and filename where the Update.exe executable exists or click to locate the executable's path.

Windows Vista and 2008 use spinstall.exe, not update.exe for the service pack install executable.

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*.

Execution Options

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 a message into the text box to be shown in the popup message.

Ask users 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 after element executes

Select this option to determine the timing in which a reboot will take place, if required, by the executed element.

Reboot immediately

Allow the required reboot to happen immediately following the element configuration.

Reboot with count down

xx seconds until reboot

Warn the end user of an impending reboot operation. The warning dialog will be displayed for the number of seconds specified.

Allow users to postpone reboot

Select this box to allow the user to postpone the impending reboot.

Reboot later

Select this option to delay the reboot to a time that the user deems acceptable.

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.

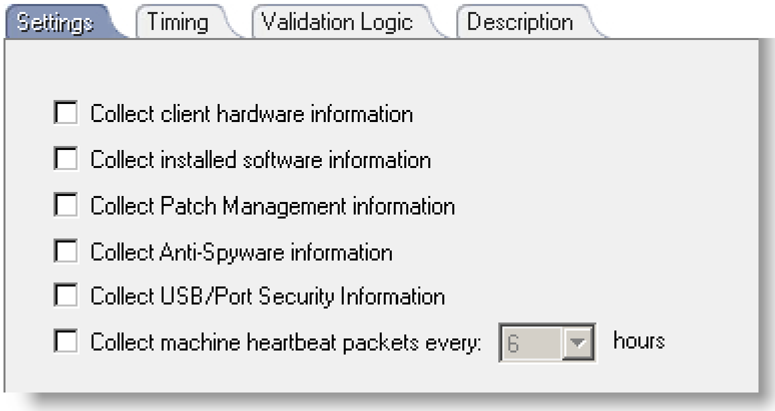
Description

Select the **Description** tab to set the description for this element.

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 OpsMaster service and the ETLProcessor plugin. These two plugins are available in the Server Manager > Ops Master Service tab for configuration.



□ Collect client hardware information

□ Collect installed software information

□ Collect Patch Management information

□ Collect Anti-Spyware information

□ Collect USB/Port Security Information

□ Collect machine heartbeat packets every: 6 hours

Collect client hardware information

Select this box to allow Desktop Authority to keep track of hardware information for each computer in the enterprise.

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 Patch Management information

Select this box to allow Desktop Authority to keep track of patches installed on each computer in the enterprise.

Collect Anti-Spyware information

Select this box to allow Desktop Authority to keep track of the Anti-spyware activity on each computer in the enterprise. This includes the Anti-spyware variants found on each computer and the action taken to rectify the infection.

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 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 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.

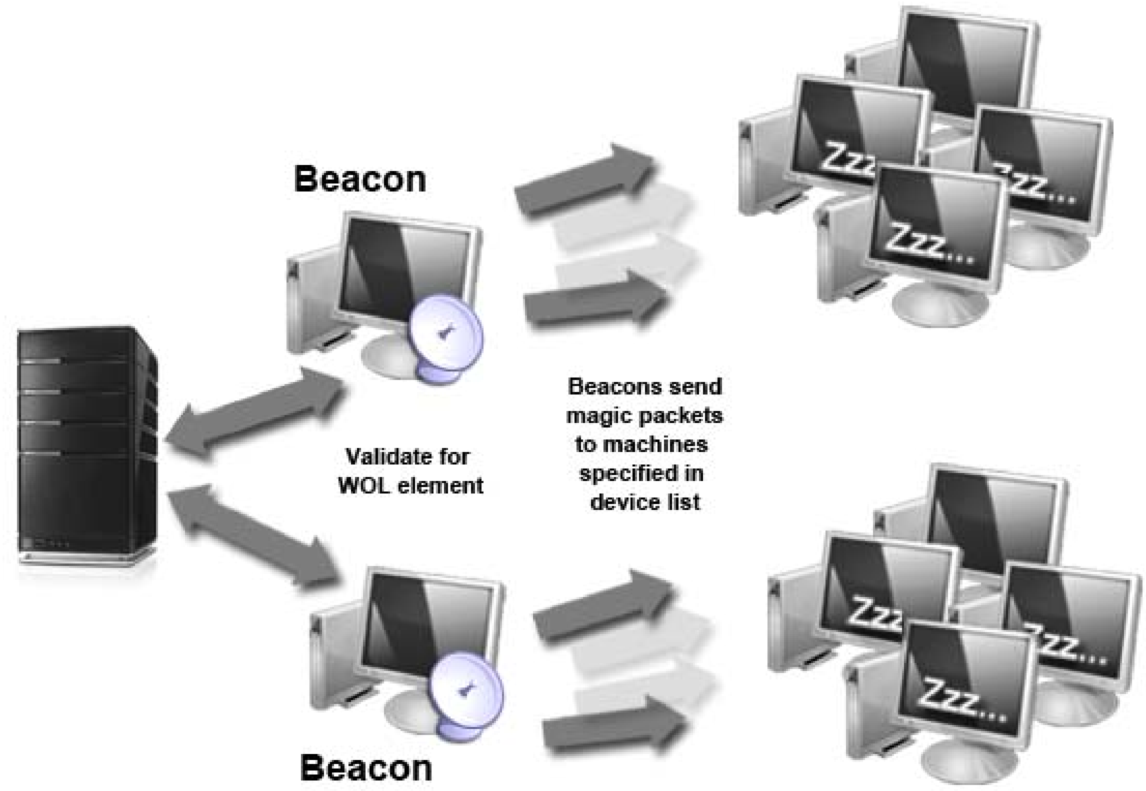
Description

Select the Description tab to set the description for this element.

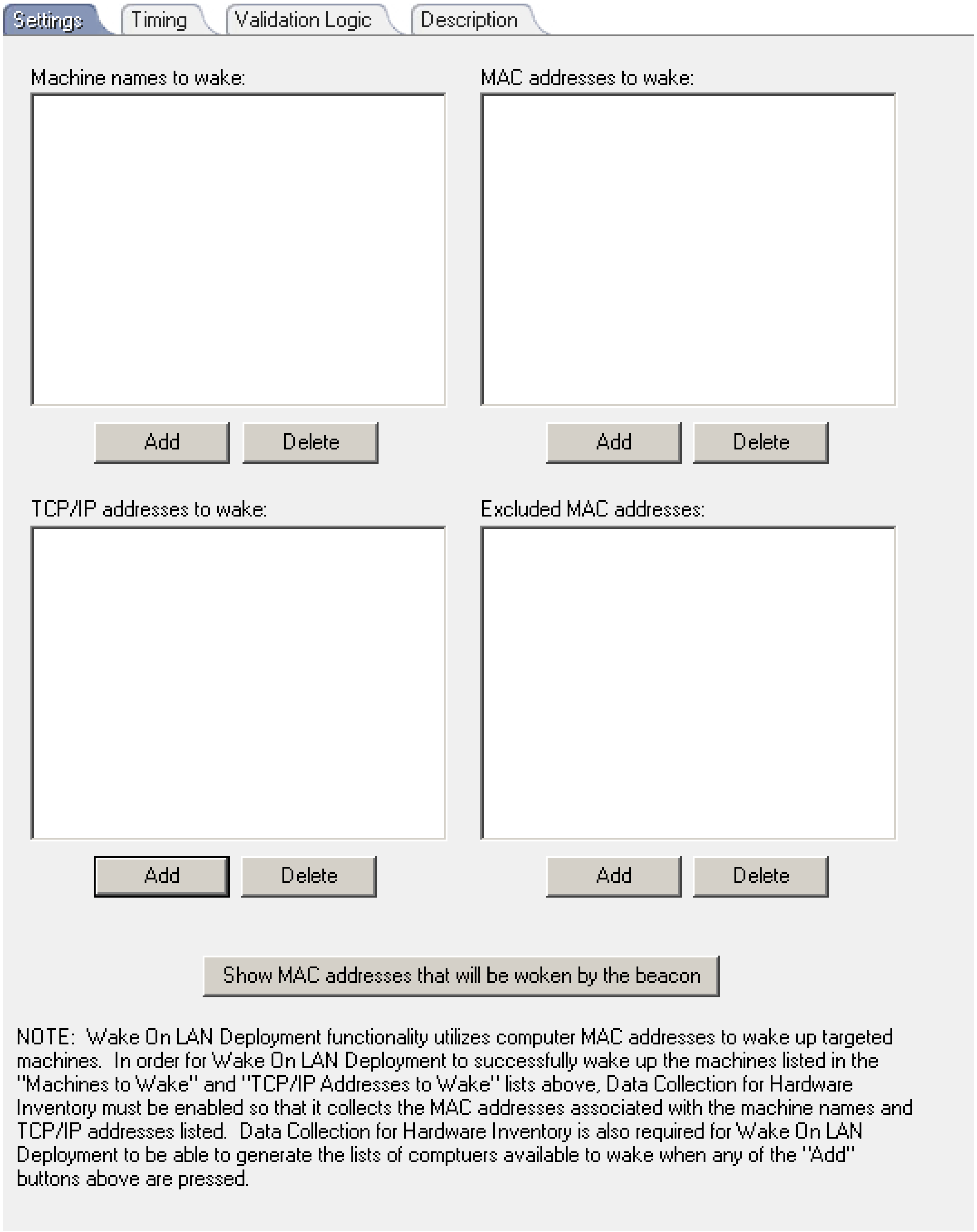
WAKE ON LAN

Wake On LAN (WOL) is a computing standard by which computers that are asleep (shutdown or hibernate state) can be sent a message through the network to wake them up. Wake on LAN is supported on all Microsoft Windows operating systems. The only requirement is a computer with a NIC and Bios that support WOL.

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 targeted as beacons will be on at the time the WOL element is scheduled to execute.



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.



NOTE: Wake On LAN Deployment functionality utilizes computer MAC addresses to wake up targeted machines. In order for Wake On LAN Deployment to successfully wake up the machines listed in the "Machines to Wake" and "TCP/IP Addresses to Wake" lists above, Data Collection for Hardware Inventory must be enabled so that it collects the MAC addresses associated with the machine names and TCP/IP addresses listed. Data Collection for Hardware Inventory is also required for Wake On LAN Deployment to be able to generate the lists of comptuers available to wake when any of the "Add" buttons above are pressed.

Settings

Machine names to wake

Create a list of computers, by Computer Name, to wake at the time this WOL element is validated by a beacon computer.

MAC addresses to wake

Create a list of computers, by MAC address, to wake at the time this WOL element is validated by a beacon computer.

TCP/IP addresses to wake

Create a list of computers, by TCP/IP address, to wake at the time this WOL element is validated by a beacon computer.

Excluded MAC addresses

Create a list of computers to exclude from WOL actions.

Click Add or Delete under any of the four lists specified above to update the list. When in Add mode, all available items in the system inventory will be listed and will be available for selection. A custom entry can be manually added to the list by clicking the Add Custom... button. Clicking Import CSV... will allow a comma delimited list to be imported into the list.

Show MAC addresses that will be woken by the beacon

Click this button to retrieve a complete list of all computers 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.

Wake On LAN Deployment uses MAC addresses to wake up targeted computers. In order for a machine to be woken up, Data Collection for Hardware Inventory must be enabled. With Hardware Inventory Data Collection enabled, MAC addresses are collected and associated with machine names and TCP/IP addresses. This is also required for Wake On LAN to generate the list of computers available to wake when the Add button is pressed.

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.

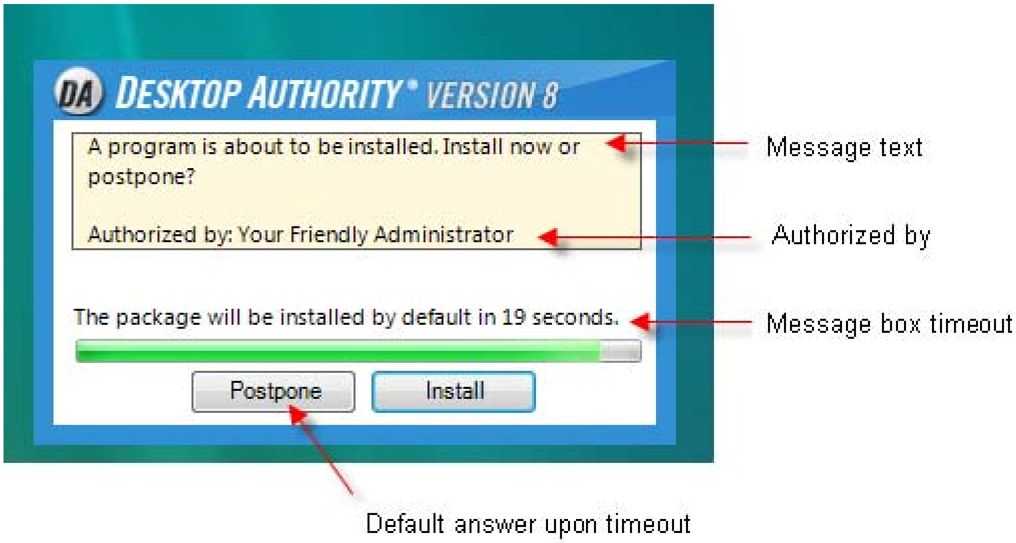
Description

Select the **Description** tab to set the description for this element.

USER EXPERIENCE - CLIENT SIDE

Computer Management Application Launcher, MSI Packages, Patch Deployment 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 users 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.



A program is about to be installed. Install now or postpone?

Authorized by: Your Friendly Administrator

The package will be installed by default in 19 seconds.

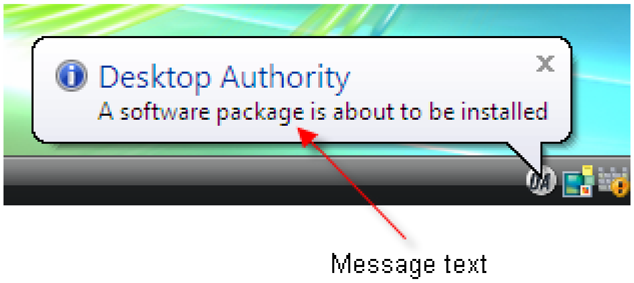
Message text

Authorized by

Message box timeout

Default answer upon timeout

If the **Show Balloon message to users before element executes** option is selected, a balloon will be displayed in the system notification area.



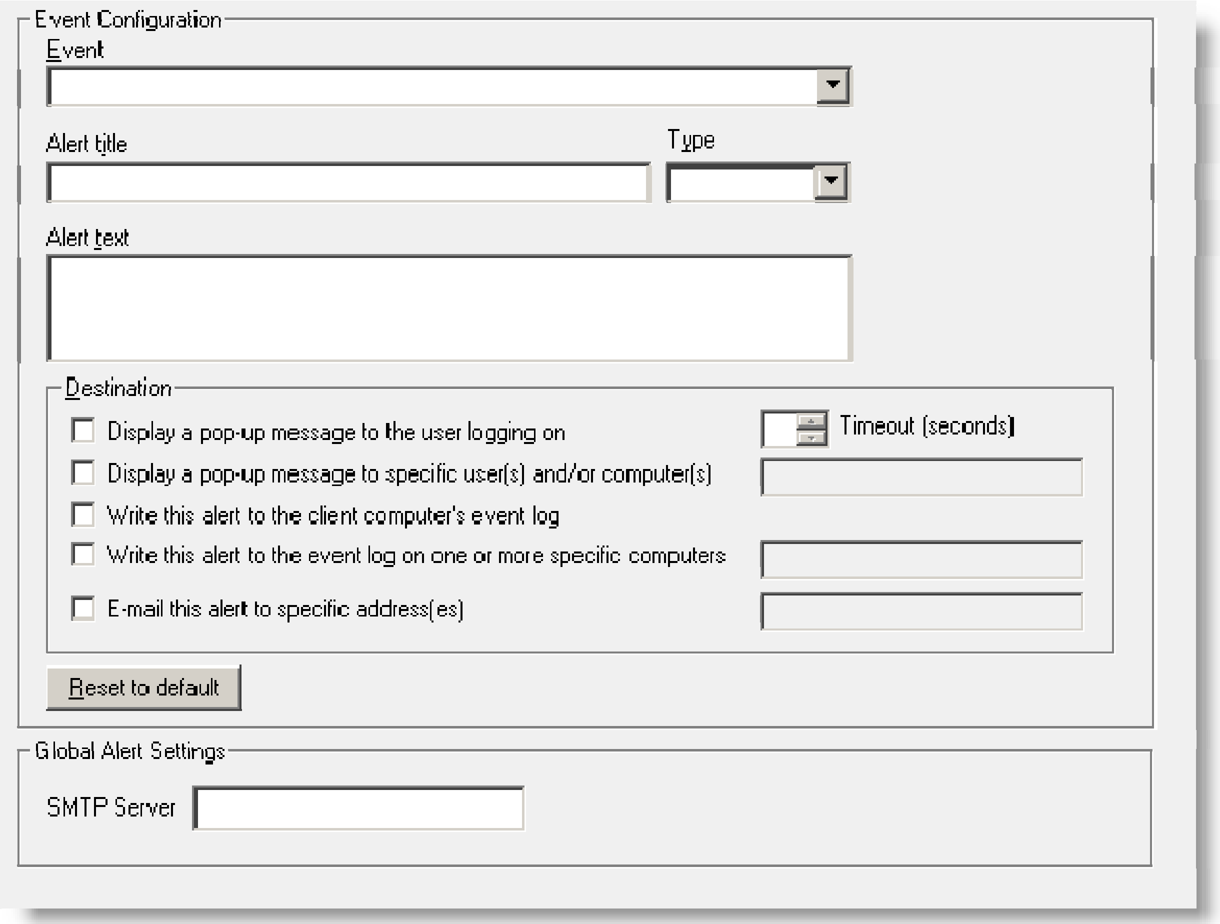
A software package is about to be installed

Message text

User Management

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.


Event Configuration
Event
Alert title
Type
Alert text
Destination
□ Display a pop-up message to the user logging on
Timeout (seconds)
□ Display a pop-up message to specific user(s) and/or computer(s)
□ Write this alert to the client computer's event log
□ Write this alert to the event log on one or more specific computers
□ E-mail this alert to specific address(es)
Reset to default
Global Alert Settings
SMTP Server

Event Configuration

Event

Select the event to customize from the Event list. Once the event is selected all options on the dialog box reflect the settings for that event.

Click the **Reset to Default** button to reset the options for the selected event to the system defaults.

Alert Title

Type in static text or press the F2 key to select a dynamic variable. The window title is displayed at the top of an Alert's popup message box.

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:

ℹ 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

Select a destination for the event notification. Leave all destinations cleared to disable the event notification.

Display a popup 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 popup message to specific user(s) and/or computer(s)

Select this check box to enable a popup message box to the specified computers or users 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 (;).

Global Alert Settings

SMTP Server

Enter the name of the SMTP server to be used to send e-mail alert(s).

ANTI-SPYWARE*

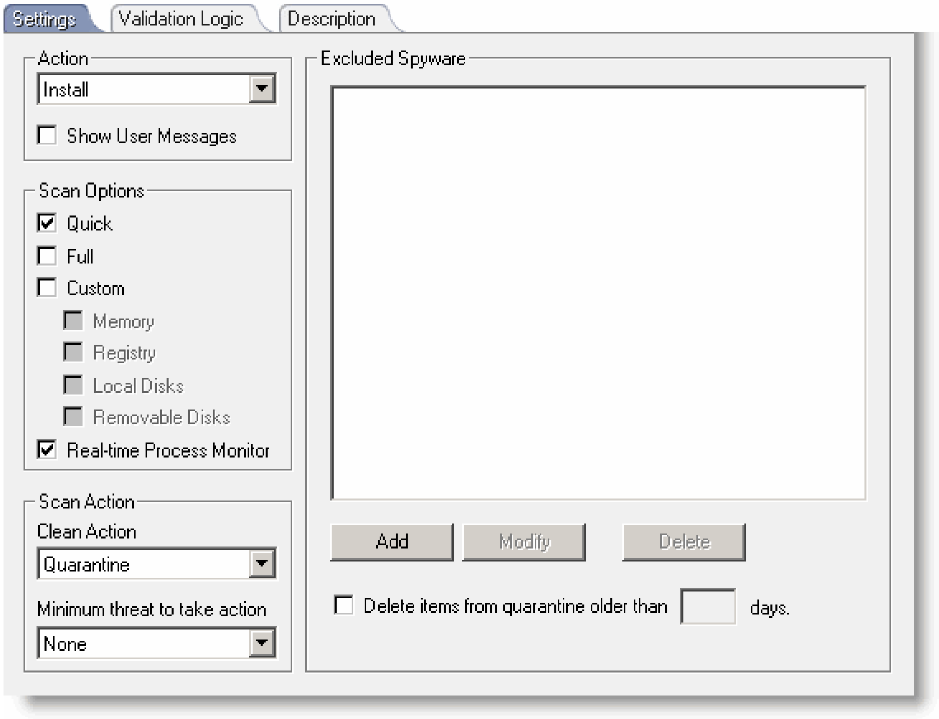
Spyware is software that gathers information from a computer without the knowledge or consent of the computer's user. A large amount of these spyware programs are malicious, gathering private and personal information. These days, spyware is difficult to avoid and also difficult to detect and remove. Desktop Authority's Anti-Spyware object provides the ability to scan clients, detect unwanted spyware and report on it. With the optional subscription service, Desktop Authority will remove or quarantine suspected spyware. Desktop Authority's spyware detection and removal capability is based on the detection and removal engine from Sunbelt Software.

The Anti-Spyware detection object cannot be configured to run on Tablet PCs, Embedded PCs, Terminal Servers, Member Servers or Domain Controllers (Windows 2000 Server, 2003 and 2008).

Anti-Spyware has the ability to scan client computers and report on suspected spyware. The Anti-Spyware object does not allow suspected spyware to be removed or quarantined from the system unless the Anti-Spyware Subscription service is purchased. When the Update Service is installed, the configured download servers will query scriptlogic.com to determine the product mode and download updated anti-spyware definition files when available.

Each scan on a client computer will create a log file named SpywareItems.log. This log file is created on each client in the \Program Files\ScriptLogic\Anti-Spyware folder. The log file should be looked over to determine that all programs deemed to be spyware are potential spyware programs. If a program is mistakenly believed to be spyware it should be added to the Exclude list so it is not reported on each time the scan is run. The next time a scan is run on the client the program will be restored.

Periodically, an updated anti-spyware definition file will be retrieved from the ScriptLogic web site. The definition file will contain the latest known spyware agents. Getting Spyware definition updates requires the use of the Update Service. The Update Service provides an avenue to update client systems with files deployed by the MSI Packages object, Patches as well as Anti-Spyware definition updates. Configure the Update Service in Server Manager.



Action
Install
☐ Show User Messages

Scan Options
☑ Quick
☐ Full
☐ Custom
☐ Memory
☐ Registry
☐ Local Disks
☐ Removable Disks
☑ Real-time Process Monitor

Scan Action
Clean Action
Quarantine
Minimum threat to take action
None

☐ Delete items from quarantine older than ____ days.

Settings

Action

Select Install or Remove from the Action list. An Install action will update the client workstation with the Anti-spyware client component. A Remove action will uninstall all Anti-spyware client-side files.

Show User Messages

Select this box to show the user messages from the system about the installation or removal of the anti-spyware client component.

Scan Options

Quick

Select this box to perform a fast search on the system. The system is scanned for anti-spyware in locations that are most often affected by spyware.

Full

Select this box to perform a scan on custom options Memory, Registry and Local Disks.

Custom

Customize scan options to include scanning of specific hardware.

Memory

Select this box to include a search through all running processes and attached processes during logon or logoff to detect spyware. The time at which memory is scanned depends upon the selected Validation Logic Timing.

Registry

Select this box to include a search through the registry files to detect spyware.

Local Disks

Select this box to include a search through all local drives to detect spyware. All files, including cookies, will be scanned.

Removable Disks

Select this box to include a search through all removable drives to detect spyware.

Real-time Process Monitor

Select this box to monitor memory for newly started processes. When a new process is detected it is automatically scanned for spyware.

Scan Action

Clean Action

The Clean Action tells the Anti-Spyware object how to handle the results of the spyware scan.

- **Leave Alone (Log Only)** - The log only mode will scan the system for spyware and report on anything found. All spyware that is found will remain on the system. This mode is used for Evaluation versions and systems that do not have a current Anti-Spyware license.
- **Quarantine**- Quarantining spyware results in moving the found spyware programs to a folder on the client. The spyware is moved and renamed so it can not be found and detected in future scans. Spyware programs are quarantined on the client computer in the folder \Program Files\ScriptLogic\Anti-Spyware\Quarantine. If a program is mistakenly determined to be spyware it's variant name should be put in the Exclude list. The next time a scan is run on the client, the program will be automatically restored.
- **Remove**- The Remove option will perform a deletion of all detected spyware programs from the system. Once a program is removed, it cannot be restored.

Minimum threat to take action

Spyware programs are divided into several threat levels based on the degree of malicious intent. Selecting a minimum level from the list will force the scan to only look for spyware with the selected threat level and above. All spyware with a threat level lower than the selected one will be ignored.

Excluded Spyware

The Excluded Spyware list is used to tell the anti-spyware object which programs to ignore. This may include any programs that are deemed to be spyware but are not, or a program which the company determines to be safe to run on their clients.

Press **Add** to define the spyware variant name in the entry. The Variant name of a detected spyware program can be found in the SpywareItems.log file. This file is created on each client as the spyware is run. The SpywareItems.log file contains information regarding all spyware found on the client. Press Modify to edit an entry in the Permissions list. Press Delete to remove an entry from the Permissions list.

Delete items from quarantine older than xx days.

Specify a number of days in which the Quarantine folder is to be cleaned. This folder contains all quarantined programs deemed to be spyware.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

*This feature is not a standard part of Desktop Authority Express. To obtain this feature, Desktop Authority Express must be upgraded to the full version of Desktop Authority.

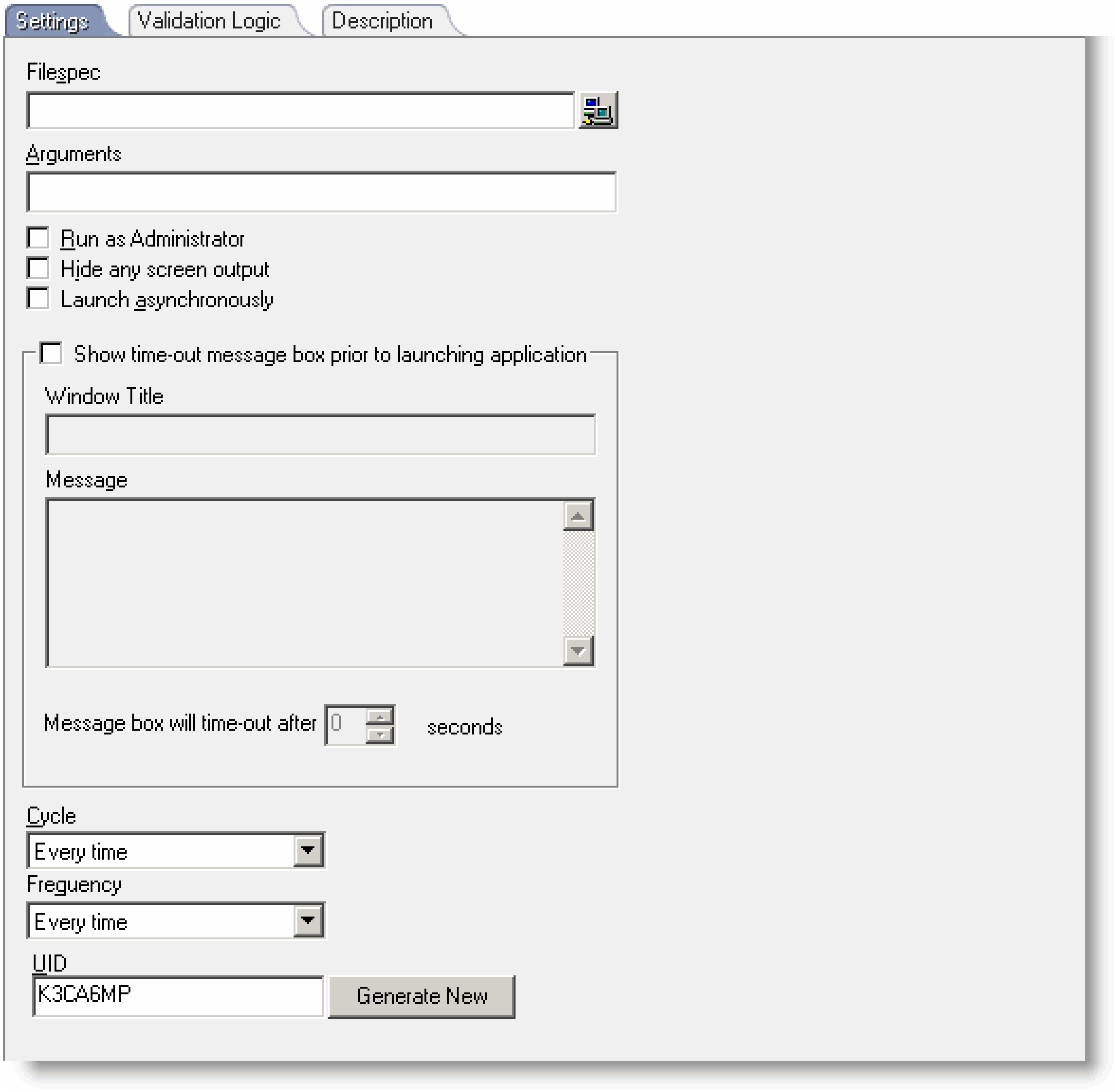
**If more than one Anti-Spyware element is validated for on a client, only the last element in the list will be applied to the client. All other elements will be ignored.

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

Filespec

Enter the complete path and filename where the application’s executable exists or click 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.

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.

Show time-out message box prior to launching application

Select this box to pop up a message box before the application is executed.

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.

Message box will time-out after 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

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 5th 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.

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.

UID

The UID 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 UID can manually be changed by clicking **Generate New**.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

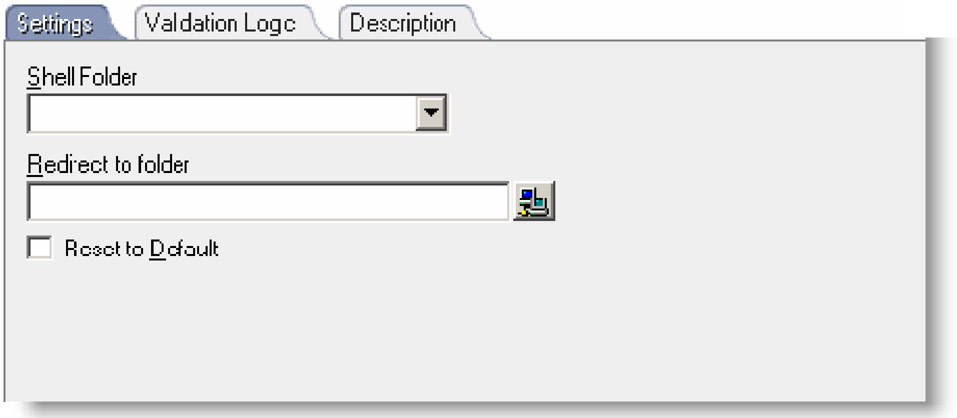
Common Folder Redirection

The **Common Folder Redirection** object allows you to change the location of where Windows 2000/XP/2003/Vista/2008 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 Application Data, 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 2000/XP/2003/Vista/2008 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

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 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.

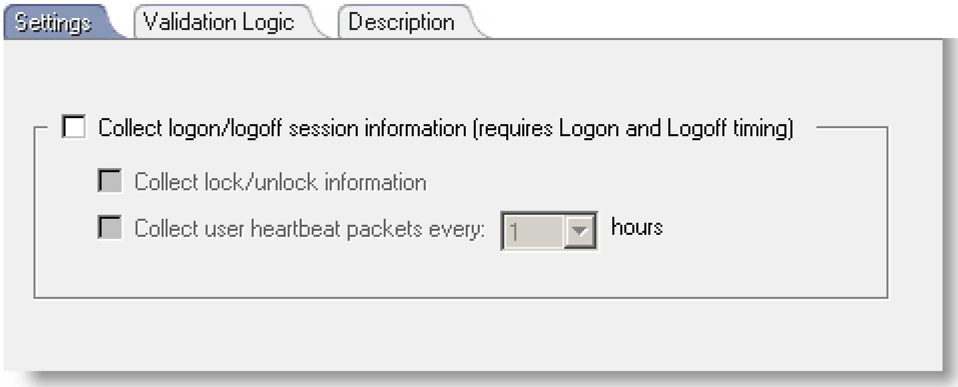
Description

Select the **Description** tab to set the description for this element.

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 OpsMaster service and the ETLProcessor plugin. These two plugins are available in the Server Manager > Ops Master Service tab for configuration.



□ Collect logon/logoff session information (requires Logon and Logoff timing)

□ Collect lock/unlock information

□ Collect user heartbeat packets every: 1 hours

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.

Collection logon/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/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 this allows for more accurate reporting.

Validation Logic

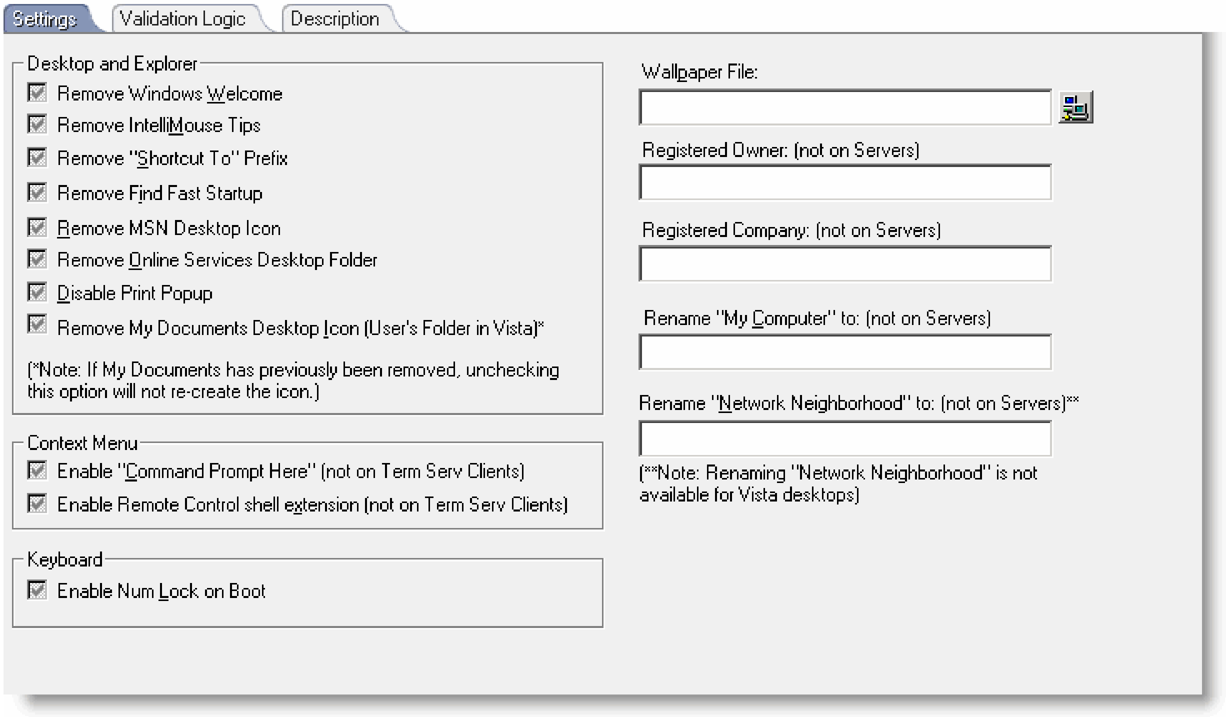
Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

DISPLAY

The **Display** object provides several options that control general operating system settings including the desktop and user interface.



Desktop and Explorer

- ☑ Remove Windows Welcome
- ☑ Remove IntelliMouse Tips
- ☑ Remove "Shortcut To" Prefix
- ☑ Remove Find Fast Startup
- ☑ Remove MSN Desktop Icon
- ☑ Remove Online Services Desktop Folder
- ☑ Disable Print Popup
- ☑ Remove My Documents Desktop Icon (User's Folder in Vista)*

(*Note: If My Documents has previously been removed, unchecking this option will not re-create the icon.)

Context Menu

- ☑ Enable "Command Prompt Here" (not on Term Serv Clients)
- ☑ Enable Remote Control shell extension (not on Term Serv Clients)

Keyboard

- ☑ Enable Num Lock on Boot

Wallpaper File:

Registered Owner: (not on Servers)

Registered Company: (not on Servers)

Rename "My Computer" to: (not on Servers)

Rename "Network Neighborhood" to: (not on Servers)**

(**Note: Renaming "Network Neighborhood" is not available for Vista desktops)

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.

Remove My Documents Desktop Icon (User's Folder in Vista)*

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 (User's Folder in Vista). Clear this check box to leave this default icon on the desktop (User's Folder in Vista). Gray the check box to leave the client’s setting untouched (User's Folder in Vista).

The default for this option is cleared.

Note: If the My Documents Desktop Icon (User's Folder in Vista) has previously been removed from the Windows desktop, unchecking this box will not re-create the icon.

Keyboard

Enable Num Lock on Boot

Select this 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.

Context Menu

Enable Command Prompt Here (not on Term Serv 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 extension (not on Term Serv Client) (not available in Desktop Authority Express)

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

Wallpaper file

Specify a bitmap file (.BMP) 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 to locate the image file. 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)

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 Vista desktops

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.

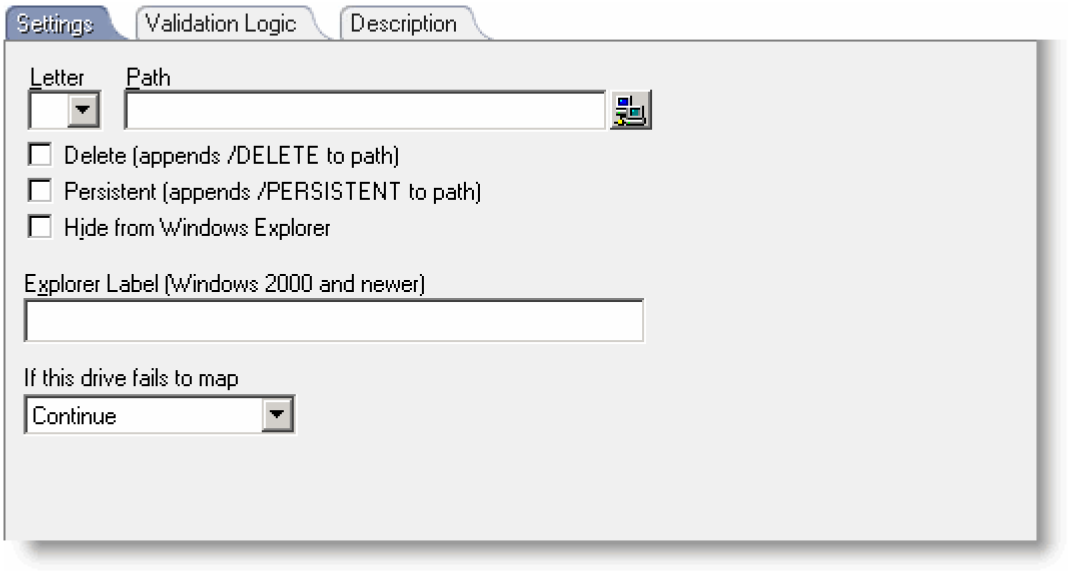
Description

Select the **Description** tab to set the description for this element.

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:.



□ Delete (appends /DELETE to path)
□ Persistent (appends /PERSISTENT to path)
□ Hide from Windows Explorer

Explorer Label (Windows 2000 and newer)

If this drive fails to map: Continue

Settings

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. All lowercase letters will be converted to uppercase when the dialog box is saved.

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 to navigate to the network share. Desktop Authority's dynamic variable selection is available for this field by pressing the **F2** key.

Mapping drive H: to all users's 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 and browsing out to select the 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 check 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 (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.

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

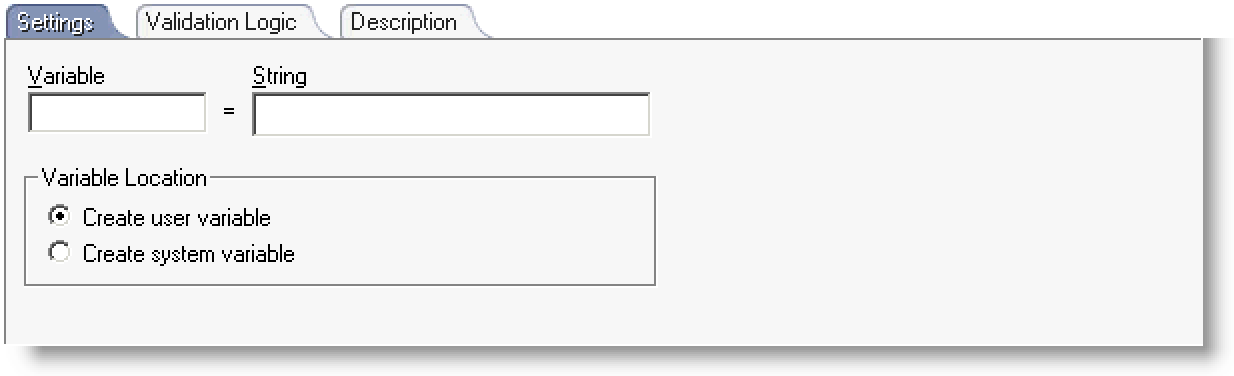
Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

ENVIRONMENT

The **Environment** object allows environment variables to be centrally configured on the client using static text, Desktop Authority dynamic variables or KiXtart macros.



Variable [ ] = String [ ]

Variable Location

● Create user variable

○ Create system variable

Settings

Variable

Enter the environment variable to be defined.

String

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.

Create user variable

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.

Create system variable

Select this option to set a system environment variable. System Environment variables are the same for all users who log on to the workstation.

Validation Logic

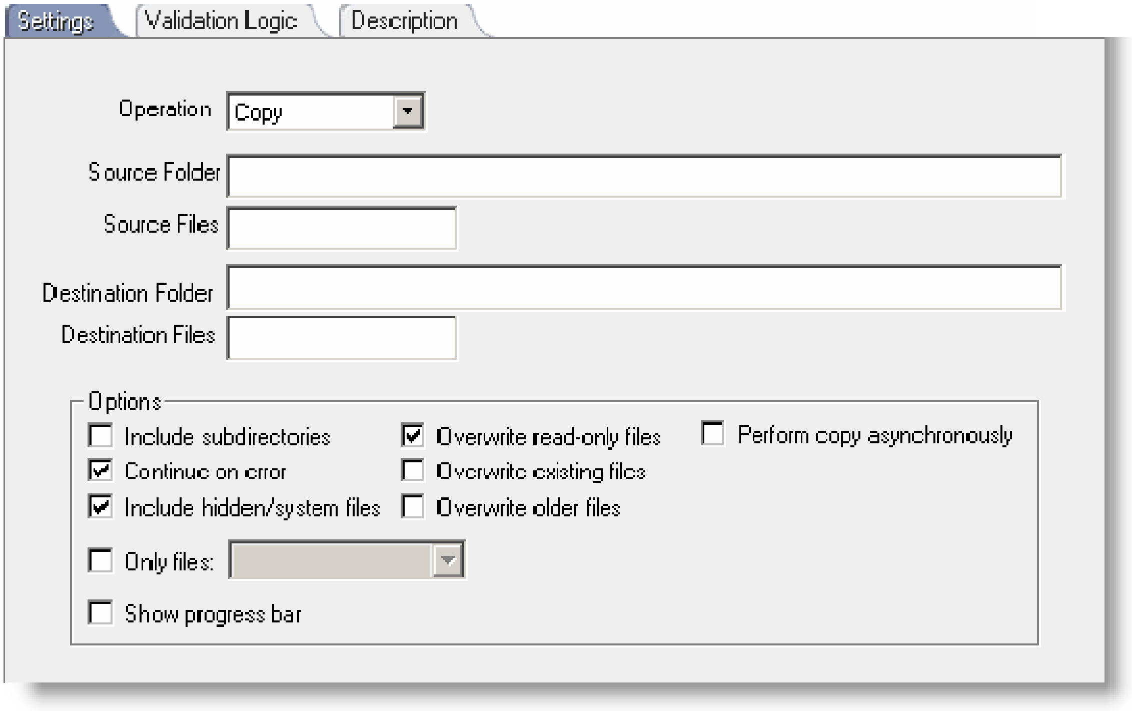
Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

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.



Operation: Copy

Source Folder

Source Files

Destination Folder

Destination Files

Options

☐ Include subdirectories
☑ Continue on error
☑ Include hidden/system files
☑ Overwrite read-only files
☐ Overwrite existing files
☐ Overwrite older files
☐ Perform copy asynchronously
☐ Only files:
☐ Show progress bar

Settings

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 Files

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 Files

For Copy or Move/Rename operations, specify the file names to be used for the destination of the selected Operation.

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.

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.

Overwrite/Delete 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/move/delete 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 OS's

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

For Move/Rename and Delete operations, select this check box to securely remove files/folders from the specified source using the DoD 3 specification.

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
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

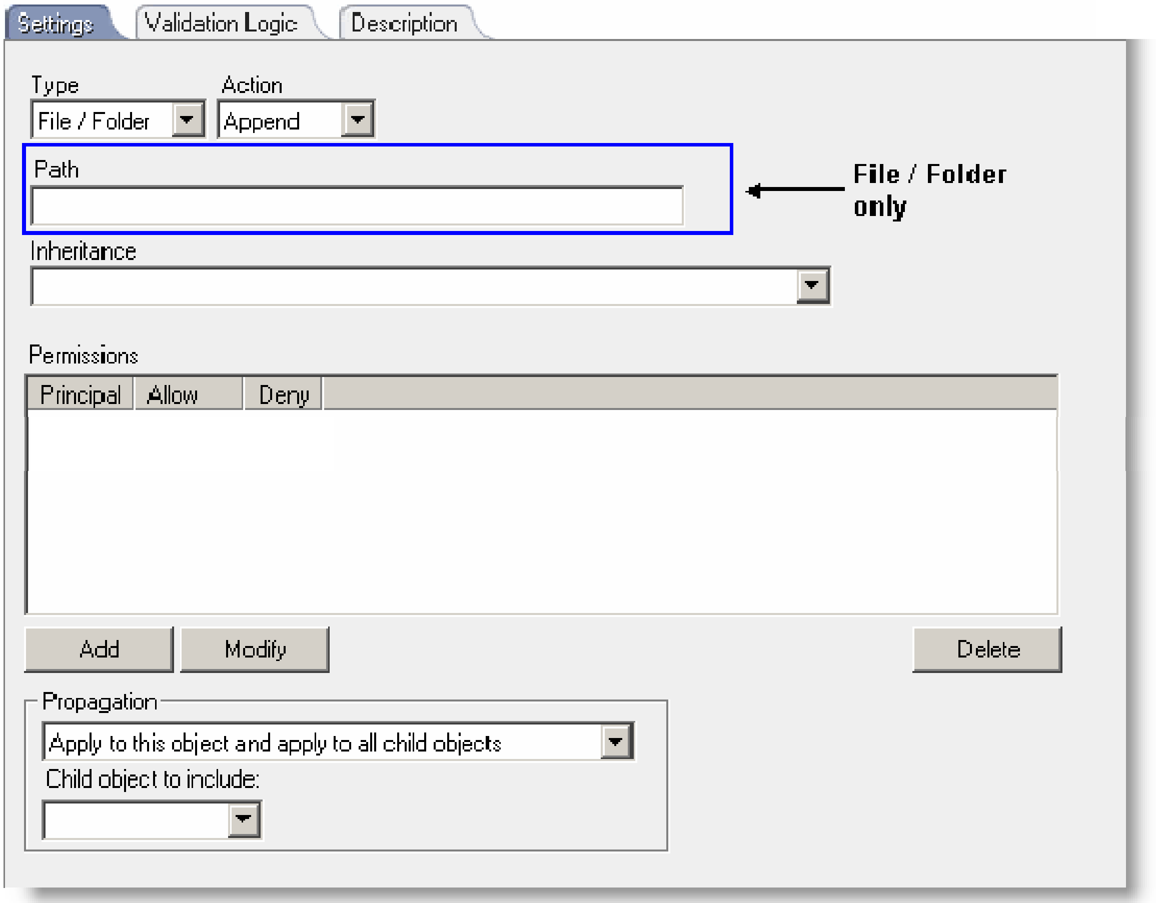
Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

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 2000, XP, 2003, 2008 and Vista systems only.

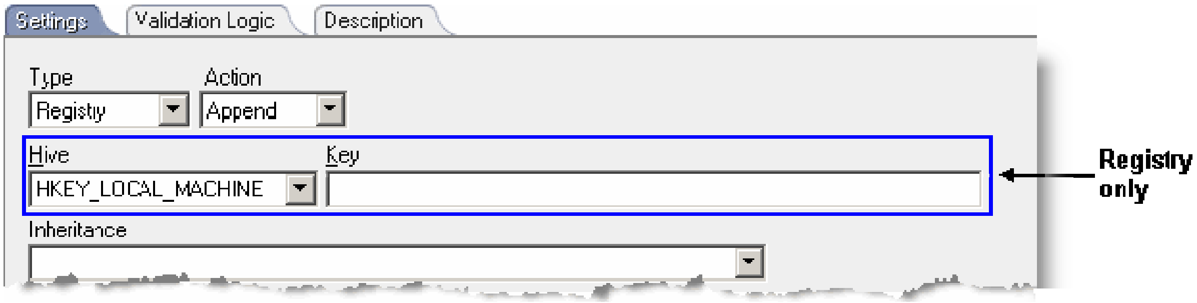


Type: File / Folder
Action: Append
Path
Inheritance

Principal	Allow	Deny

Apply to this object and apply to all child objects
Child object to include:

File / Folder only



Type: Registry
Action: Append
Hive: HKEY_LOCAL_MACHINE
Key
Inheritance

Registry only

Settings

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.

Inheritance

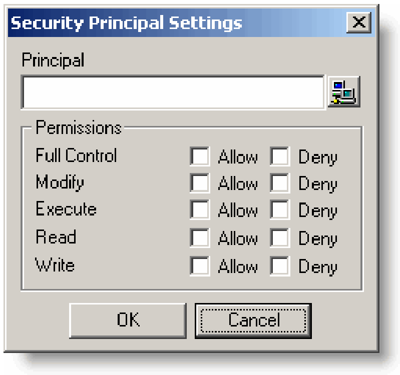
Select Do not modify this object's inheritance, Allow this object to inherit from parent, Do not allow this object to inherit from parent and discard inherited permissions, Do not allow this object to inherit from parent and copy inherited permissions from the Inheritance list. The Inheritance selection 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 Modify to edit an entry in the Permissions list. Press Delete to remove an entry from the Permissions list.



Security Principal Settings

Principal

Permissions

Full Control	□ Allow	□ Deny
Modify	□ Allow	□ Deny
Execute	□ Allow	□ Deny
Read	□ Allow	□ Deny
Write	□ Allow	□ Deny

Principal

Specify a user or group that will be assigned the designated permissions.

Permissions

The permissions 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.

Description

Select the **Description** tab to set the description for this element.

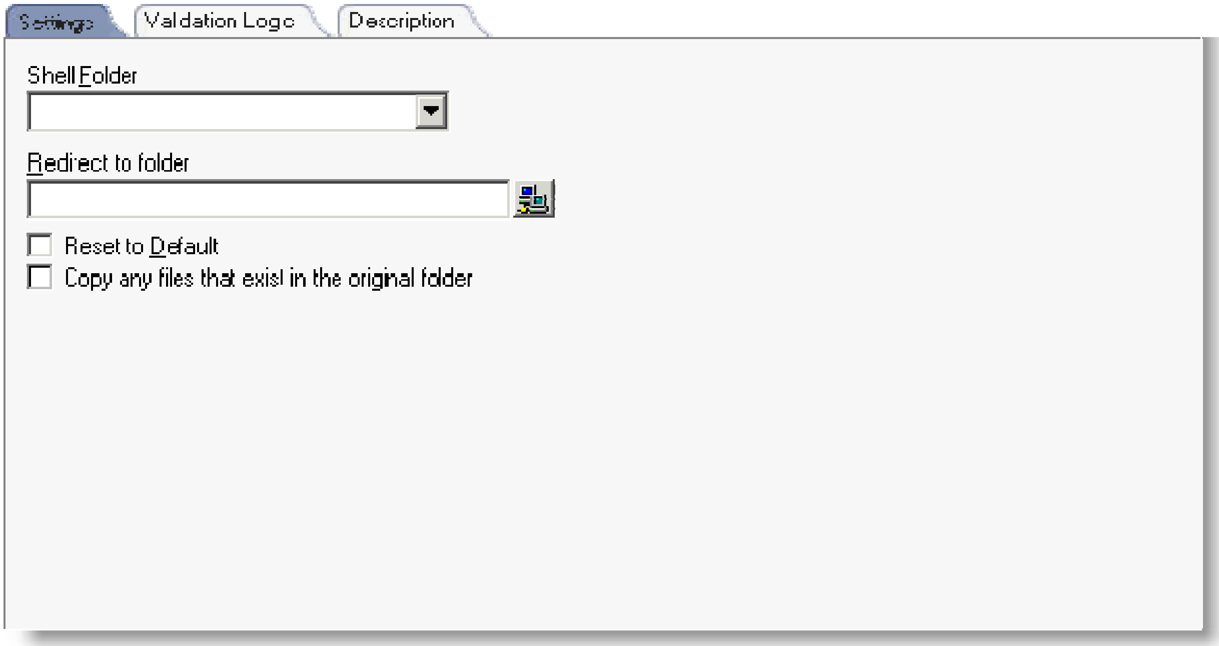
Folder Redirection

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 user. They include the Cookies, Desktop, Favorites (IE Bookmarks), History, My Pictures, Personal (My Documents), Recent, Temporary Internet Files, Send To, Start Menu, Programs Group and the Startup Group.

Windows 2000 and newer operating systems locates the shell folders under the user's profile, and the location of user profiles is C:\Documents and Settings*profilename*\.

By defaulting the location of these folders to a network share (or mapped drive), rather than the local computer's own hard drive, 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 nightly.

In addition to user-specific shell folders, Windows 2000/XP/2003/Vista/2008 also includes a common set of shell folders that is available to all users of the computer. This common set of shell folders is often referred to as the "All Users" profile.



Settings

Shell Folder

Select a shell folder from the Shell Folder list.

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 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.

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

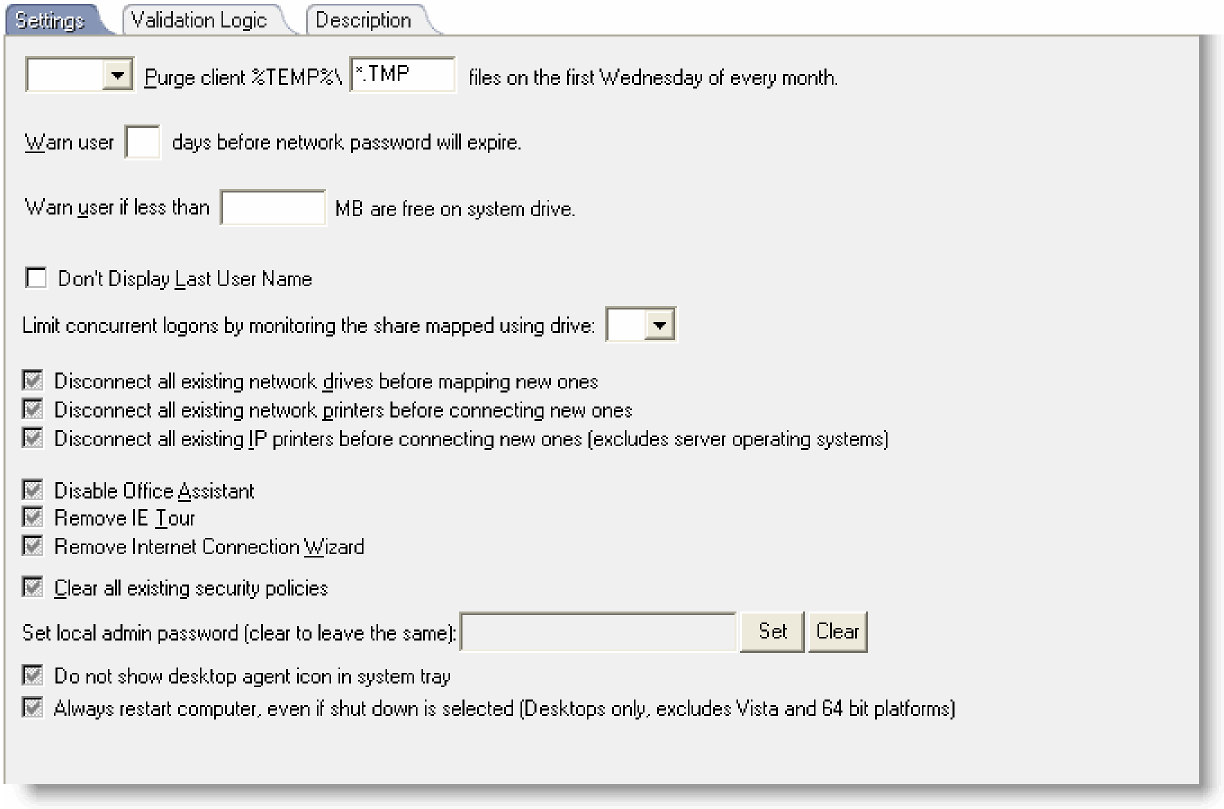
Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

GENERAL

The **General** object provides several miscellaneous settings including settings to purge the client TEMP files, password expiration warnings and others.



Purge client %TEMP%\ *.TMP files on the first Wednesday of every month.

Warn user days before network password will expire.

Warn user if less than MB are free on system drive.

□ Don't Display Last User Name

Limit concurrent logons by monitoring the share mapped using drive:

☑ Disconnect all existing network drives before mapping new ones
☑ Disconnect all existing network printers before connecting new ones
☑ Disconnect all existing IP printers before connecting new ones (excludes server operating systems)

☑ Disable Office Assistant
☑ Remove IE Tour
☑ Remove Internet Connection Wizard

☑ Clear all existing security policies

Set local admin password (clear to leave the same):

☑ Do not show desktop agent icon in system tray
☑ Always restart computer, even if shut down is selected (Desktops only, excludes Vista and 64 bit platforms)

Settings

Purge client %TEMP%\ xxxx.xxx files on the first Wednesday of every month

%TEMP% is an environment variable that defines the location of the Windows' 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 **Never** from the list to disable the automatic purging of files in the **%TEMP%** folder. 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 defaults for purging are **[Never]** purge and **[*.tmp]** files.

Warn user xx days before network password will expire

Enter a numeric value (number of days) to enable a warning to the client when 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.

Warn user if less than 999999999 MB are free on system drive

Enter a numeric value (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.

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.

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.

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.

IP printers on servers will not be disconnected by this option.

Disable Office Assistant

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 disable "Clippy", the annoying Office Assistant. Clear this check box to enable the office assistant. Gray this check box to preserve the user’s current profile setting.

Remove IE Tour

Select this check box to remove the Internet Explorer *Take a Tour* splash screen. Once removed, it can not 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 can not be reactivated (added back to the desktop) by Desktop Authority.

Clear all existing security policies first

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.

Set local admin password (clear to leave the same)

Click Set to define a local admin password for clients that this element validates for. After entering the local admin password, click OK. The password will be encrypted for display purposes in the Manager. Click Clear to remove the local admin password from the element.

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.

This check box can be set to one of three (3) different states: on (enabled), ☑, force the computer to Restart even if a Shut down was selected, off (disabled) □, allow the computer to shut down if requested, or grayed, ☑, preserve Global Desktop Agent setting. 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.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

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.

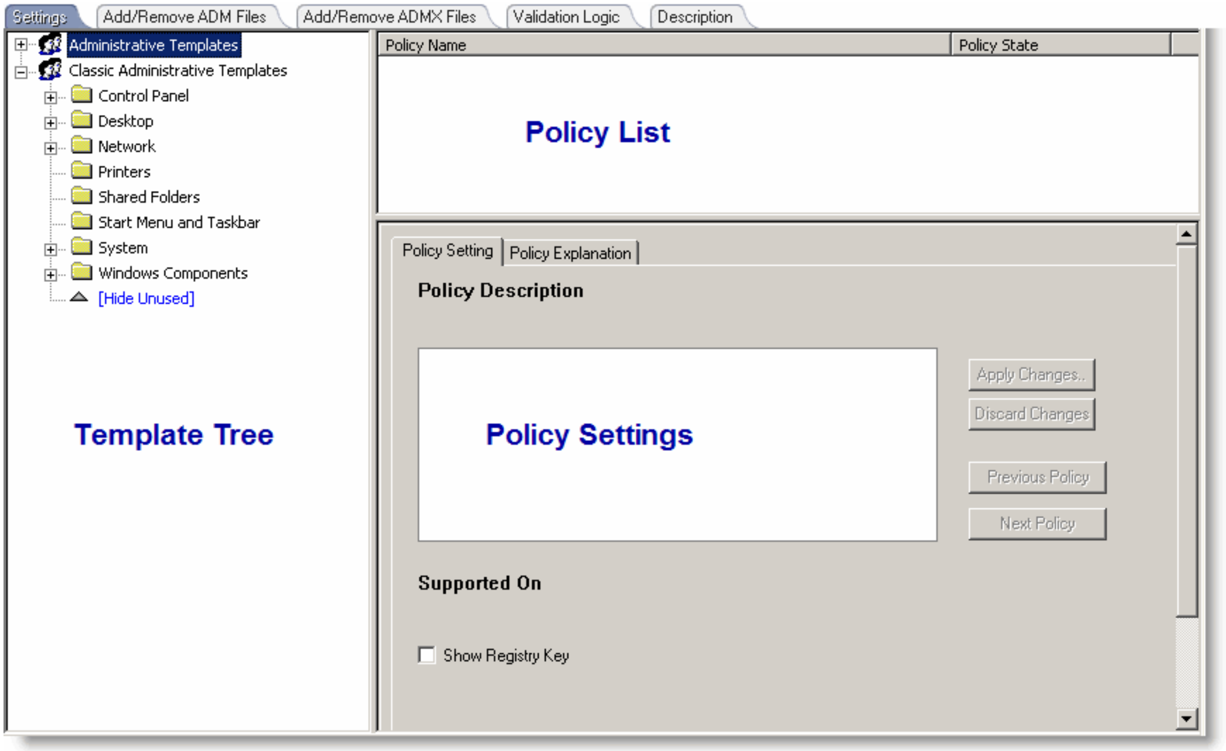
There are several standard administrative templates that are installed with Windows 2000, XP, 2003 and Vista. Additional Administrative templates are available in several of Microsoft's Resource kits, service packs and the Microsoft Download center. Templates can also be created from scratch or customized 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 Vista. ADMX Templates are used by Microsoft Windows Vista 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.

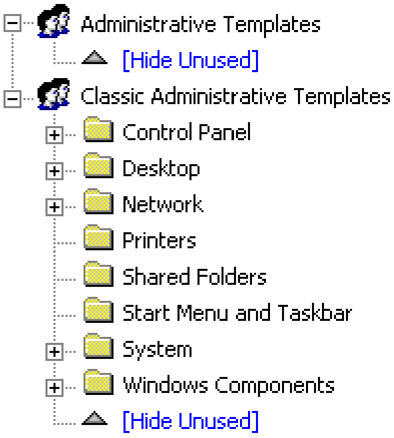
Configure the Policy on the Policy Setting tab. Once configured, click Apply Changes to accept the changes for the current Group Policy element. Click Discard changes to undo the latest changes. Review a description on the Policy Explanation tab. To save the Group Policy element, click the 💾 toolbar button.

Settings



Administrative Template Trees

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 Template tree. Each category displays the policies available for configuration in a list to the right of the category.



Click [Hide Unused] to hide policies in the list that are not yet configured. If policies are hidden, click [Show Unused] 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. The policy is configured on the Policy Setting tab.

Policy Setting

The Policy Setting 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 Apply Changes to accept the changes for the current Group Policy element. Click Discard Changes to undo the most recent changes.

Policy Explanation

The Policy Explanation tab provides a complete description of the policy and its settings.

Apply Changes

Click Apply Changes to accept the changes for the current Group Policy element.

Discard Changes

Click Discard Changes to undo the most recent changes.

Previous Policy

Click Previous Policy to load the previous policy in the list.

Next Policy

Click Next Policy to load the next policy in the list.

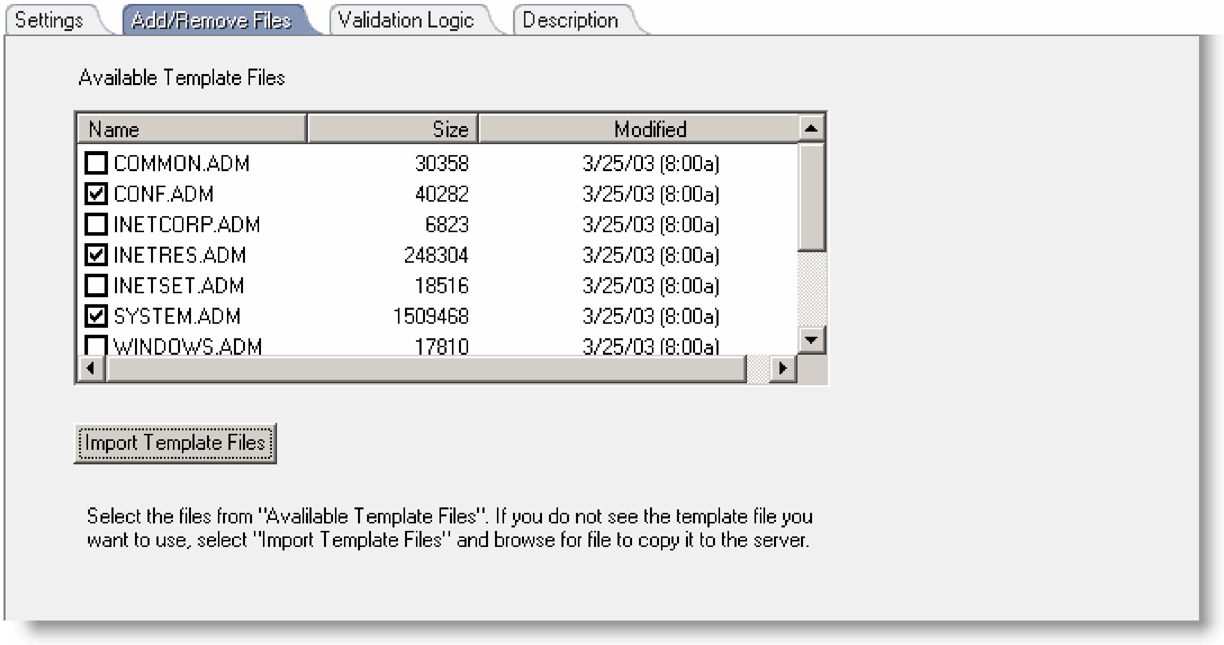
Show Registry Settings

Select Show Registry Settings to display the actual registry key and value that will be configured for the selected Policy.

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.



Available Template Files

Name	Size	Modified
□ COMMON.ADM	30358	3/25/03 (8:00a)
☑ CONF.ADM	40282	3/25/03 (8:00a)
□ INETCORP.ADM	6823	3/25/03 (8:00a)
☑ INETRES.ADM	248304	3/25/03 (8:00a)
□ INETSET.ADM	18516	3/25/03 (8:00a)
☑ SYSTEM.ADM	1509468	3/25/03 (8:00a)
□ WINDOWS.ADM	17810	3/25/03 (8:00a)

Select the files from "Avalilable Template Files". If you do not see the template file you want to use, select "Import Template Files" and browse for file to copy it to the server.

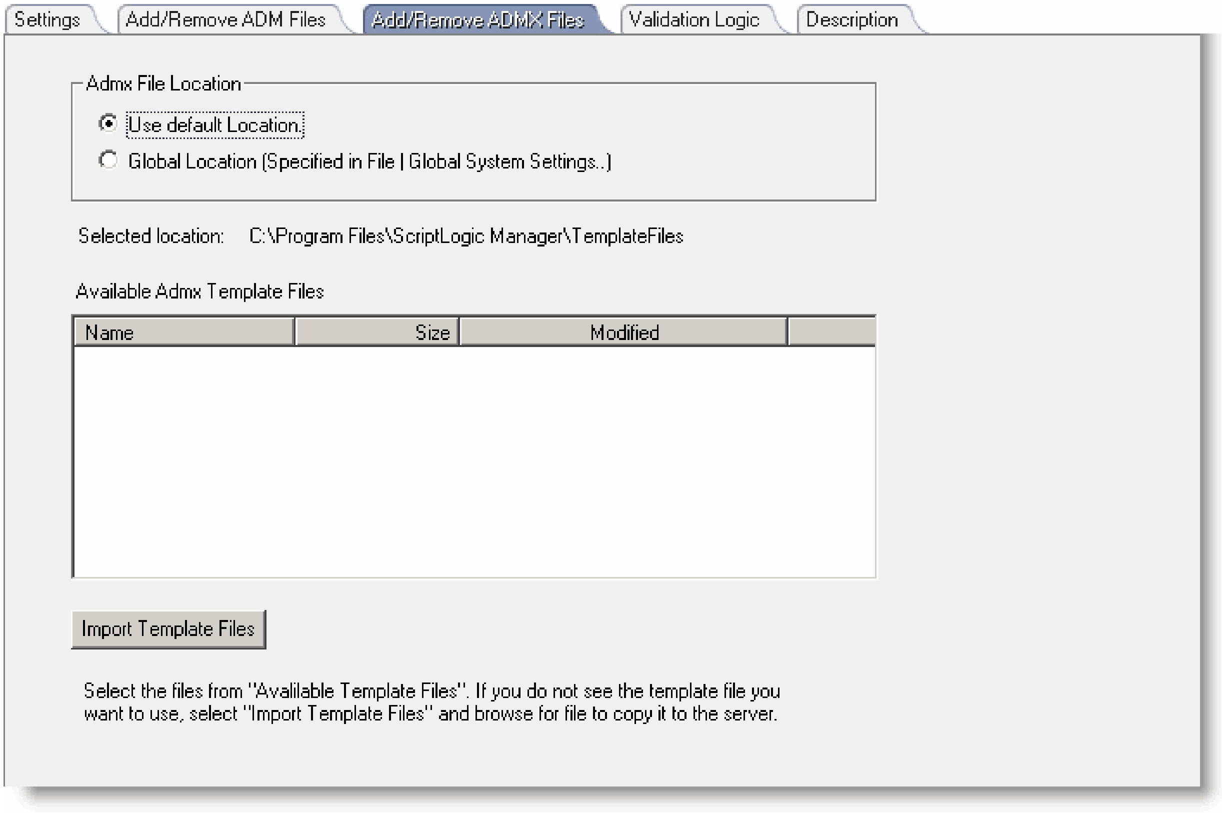
To add a new ADM template to the list, click Import Template Files. Browse to the ADM template file and select it. Click Open to confirm the selection. The template file will be automatically be imported and added to the list. All policies within the template file are immediately available for use in 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.

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 that Administrative templates be imported into the system.



Admx File Location

● Use default Location.

○ Global Location (Specified in File | Global System Settings..)

Selected location: C:\Program Files\ScriptLogic Manager\TemplateFiles

Available Admx Template Files

Select the files from "Avalilable Template Files". If you do not see the template file you want to use, select "Import Template Files" and browse for file to copy it to the server.

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 DA default path for ADMX files. This path is %program files%/ScriptLogic Manager/TeamplateFiles. To select another path, choose Global Location. The Global Location path is set on the Global Settings dialog.

To add a new ADMX template to the list, click Import Template Files. Browse to the ADMX template file and select it. Click Open 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 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

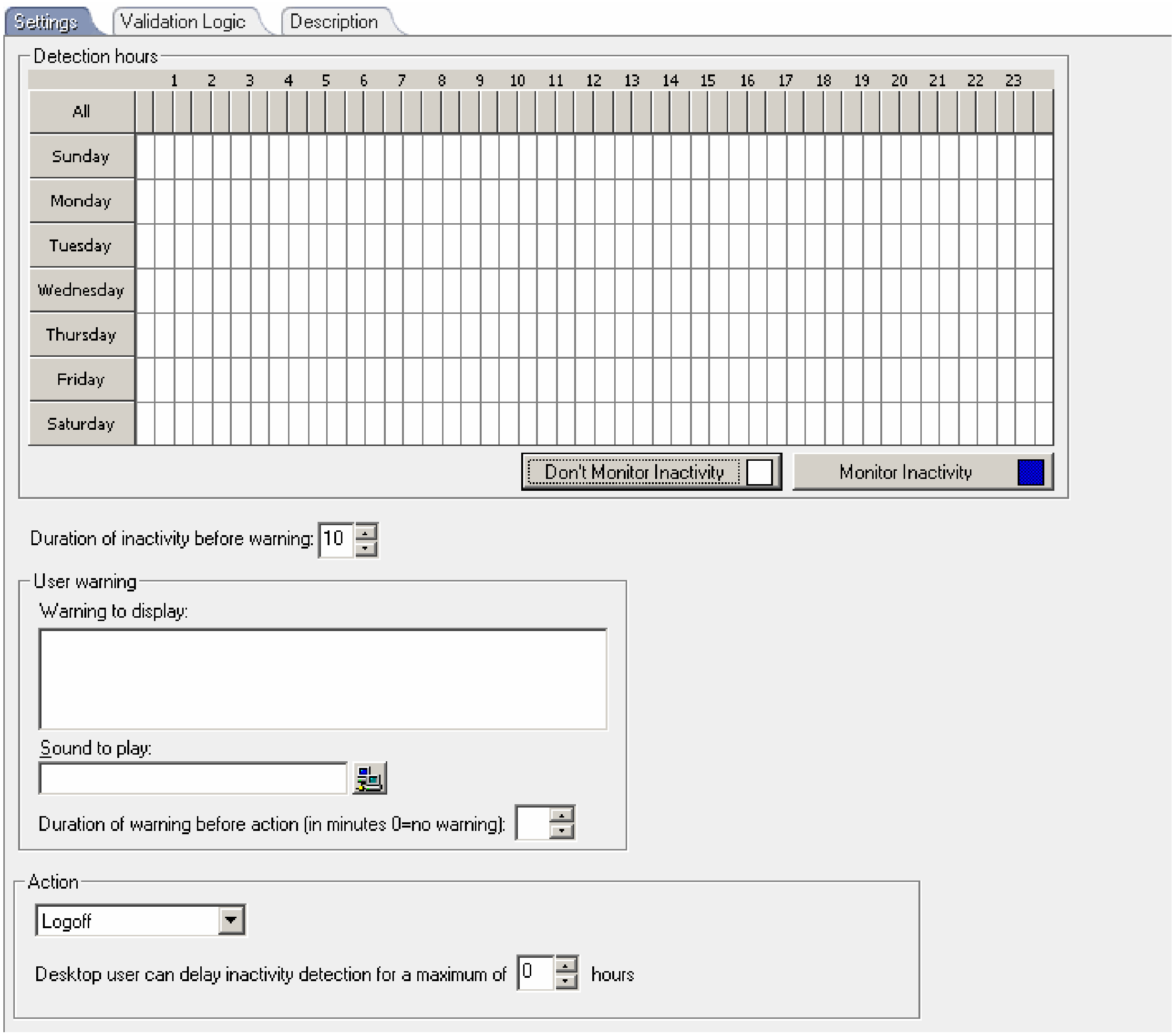
Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

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 2000, XP, 2003 and Vista operating systems only.



Duration of inactivity before warning: 10

Warning to display:

Sound to play:

Duration of warning before action (in minutes 0=no warning):

Logoff

Desktop user can delay inactivity detection for a maximum of 0 hours

To select or clear an inactivity period, highlight a range of cells in the inactivity grid. Press **Don't Monitor Inactivity** to clear the cells. Press **Monitor Inactivity** to select the cells. To select an entire day, 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, click the hour label 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

Detection hours

Don't Monitor Inactivity

Click Don't Monitor Inactivity to set the selected period of time as unmonitored time.

Monitor Inactivity

Click **Monitor Inactivity** to set the selected period of time as monitored time. Monitored time periods will display as colored blocks.

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

Warning to display

Prior to the selected Action (Logoff, Always Shutdown, Shutdown, Restart, Standby, Hibernate, Lock) occurrence, a warning dialog will 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.

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.

Action

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 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.

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.

Validation Logic

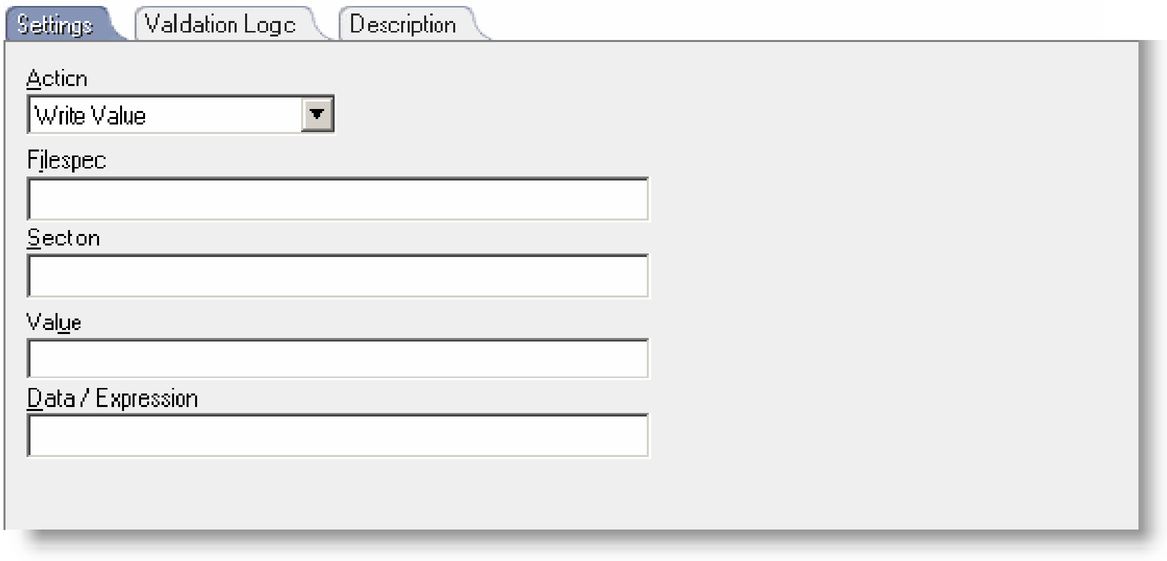
Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

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.



Action: Write Value

Filespec:

Secton:

Value:

Data / Expression:

Settings

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

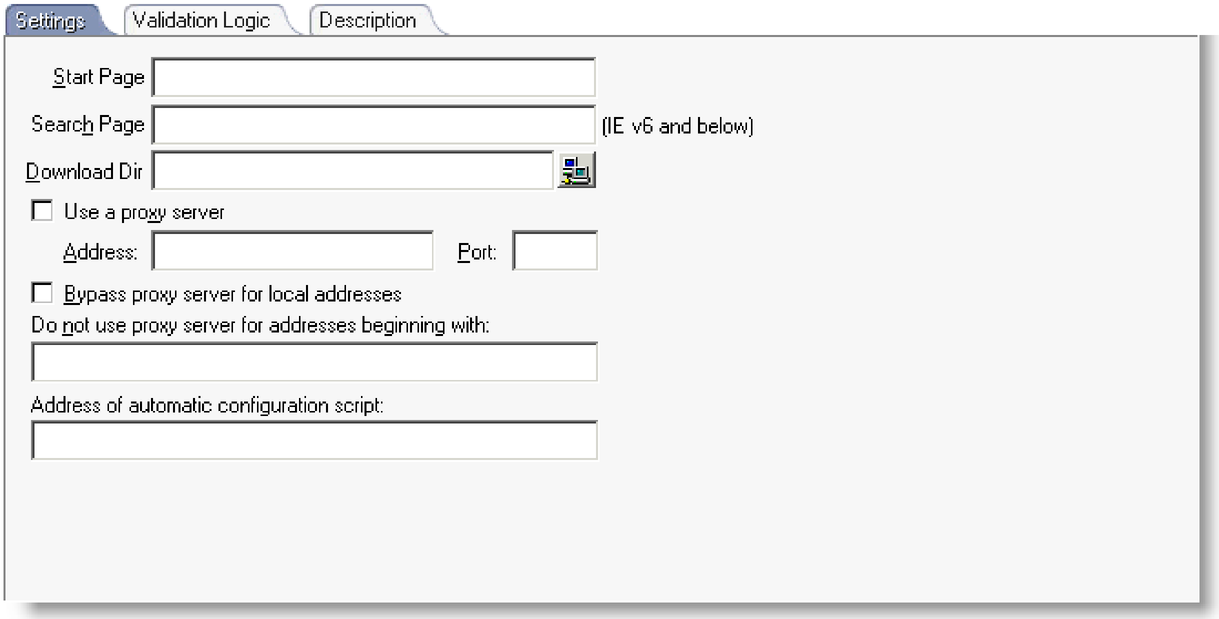
Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

INTERNET EXPLORER SETTINGS

The Internet Explorer Settings object provides the ability to configure Internet Explorer. Settings such as the Start Page, Search Page, Download Directory, and Proxy Server information.


Settings
Validation Logic
Description
Start Page
Search Page
(IE v6 and below)
Download Dir
□ Use a proxy server
Address:
Port:
□ Bypass proxy server for local addresses
Do not use proxy server for addresses beginning with:
Address of automatic configuration script:

Settings

Start Page

Enter a valid HTML start page for Internet Explorer. Specifying a start page forces all employees to view a common page each time they load Internet Explorer. A good use for the start page is the corporate web site or Intranet.

Leaving this field blank will allow your users to select and set a start page of their own choice.

Search Page (IE v6 and below)

If you have created your own search page, or would like your users to use a specific search engine, enter the URL in this field.

If this field is left blank, your users will be able to select and retain the search page of their choice.

Download Dir

Specify a default path that all file downloads should be redirected to. The path may be in the form of a physical path, mapped drive or UNC. Click ▦ to navigate to the path. Desktop Authority's dynamic variable selection is available for this field by pressing the **F2** key.

Use a proxy server

Select this check box to enable a proxy server for an Internet connection. Clear this check box if a proxy server is not used.

Address

Enter the name or TCP/IP address or host name of your network’s proxy server.

Example:

```
192.168.100.205
```

If your organization has different proxy servers for different protocols, you may use the **Address** field for all applications. Create a single string in the **Address** field and leave the **Port** field blank.

Example:

```
http=10.0.0.5:80;https=10.0.0.7:443;ftp=10.0.0.9:21
```

Port

Enter the TCP/IP port number of your network’s proxy server.

Bypass proxy server 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.

Do not use proxy server for addresses beginning with:

Specify Internet addresses that should not use a proxy server. Multiple addresses can be specified and should be separated by a semicolon (;). An asterisk (*) may be used as a wildcard.

Example:

```
www.*.com; 192.*; 192.168.*
```

Address of automatic configuration script:

Type an address (URL) or file name that will be used to configure the proxy settings for Internet Explorer. Leave this field blank if you do not use a configuration script file.

Validation Logic

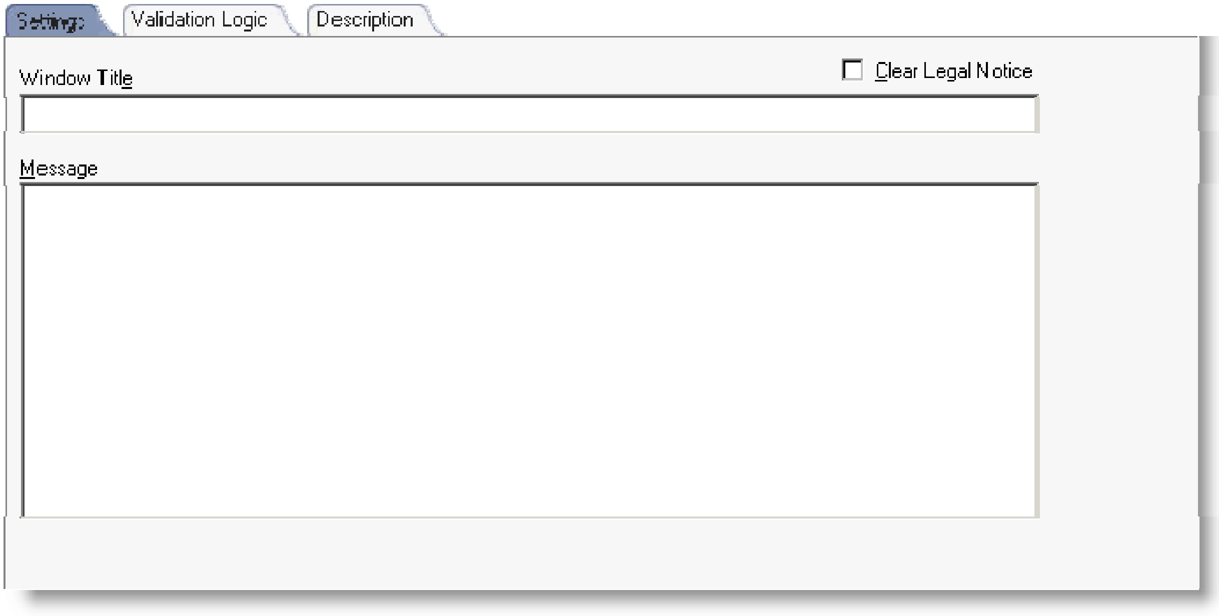
Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

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 2000XP/2003/Vista/2008 computer if the computer has AutoAdminLogon enabled.

Settings

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.

Description

Select the **Description** tab to set the description for this element.

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 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 Insert to add a new element to the current position in the list. The entry is added to the list just above the highlighted element.

Click Modify to edit the existing highlighted element in the list.

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

Log File Location

Enter the location where the log files will be created or press 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 the **F2** key 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 **Log File Location**.

View Logs...

Click View Logs... to open the Log File Viewer.

Log Entry

When modifying the log file entries, select an entry from the Log Entry list, enter static text, and/or press **F2** or the **Insert Variable** button to use insert a dynamic variable. The dynamic variable selected from the popup list is inserted into the field at the current cursor position.

LOG FILE VIEWER

The Log File Viewer is used to view available log files. These files are created and updated each time a client logs on to the network. A log file is a Comma Separated Value (comma delimited) file and can be viewed in any text editor or directly within Desktop Authority. A new log file is created each day for each profile. The log file's name is constructed using the profile name as well as the date of the file. For example, on April 10, 2001, profile SLP00001, the log file created will be SPL00001_20010410.CSV.

The Log File Viewer is accessible by clicking **View** on the Logging object.

Filter Available Logs To

Since there are most likely numerous log files located in the Log share, select a Profile, Month and Year to limit the files listed in the Available logs list.

Available Logs

This list displays all available log files from the Log share. This list is filtered based on the Month and Year specified in the **Filter Available Logs To** field. To add a log file to the Selected Logs list click **Add>>** or double click on an entry.

Selected Logs

This list displays all selected log files. The selected files will be opened in the log file viewer when View is clicked.

Add >>

Click **Add>>** to add the selected Available Logs file(s) to the *Selected Logs* **list**.

Add All

Click **Add All** to add all Available Log files to the *Selected Logs* list.

<< Remove

Click **<<Remove** to remove the selected file(s) from the *Selected Logs* list and restore them to the *Available Logs* list.

Remove All

Click **Remove All** to remove all files from the *Selected Logs* list and restore them to the *Available Logs* list.

Purge log files older than [xx] months

Desktop Authority can automatically purge log files older than xx months. Specify the number of months in this entry. To disable the automatic purge of log files, enter 0 in this field. Old log files are purged when the Log File Viewer button is pressed. Once a log file is purged, it is no longer available in the Log File Viewer list.

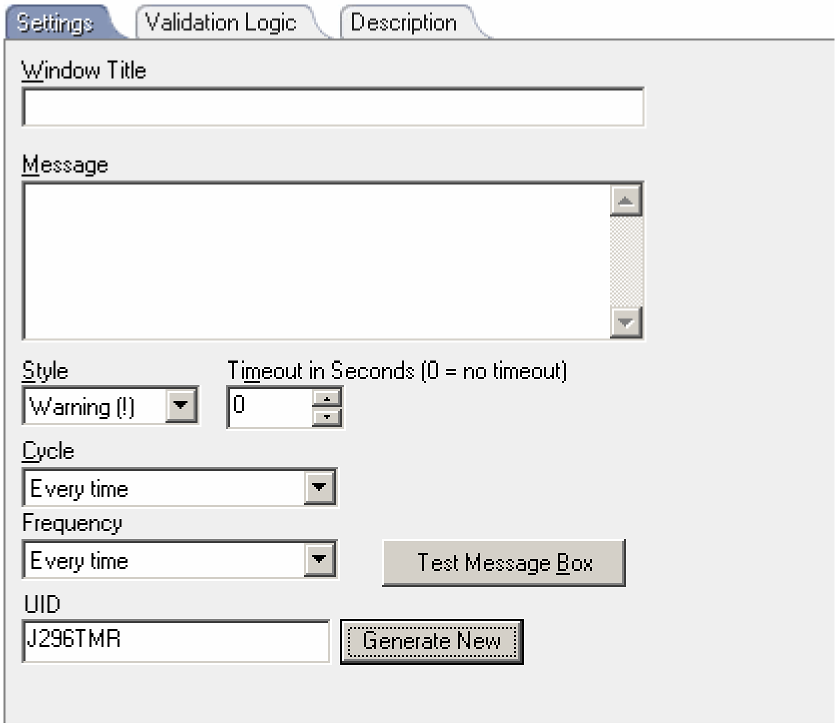
View

Click **View** to view the contents of all selected log files. The log files are combined and displayed as one contiguous list of entries in date/time default order. This list can be sorted by any column specified for the log file definition. Click on a column header to sort the entries. When viewing log files, the number of unique clients is determined and displayed on the bottom of the *View Log File* dialog.

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.



Style: Warning (!)

Timeout in Seconds (0 = no timeout): 0

Cycle: Every time

Frequency: Every time

UID: J296TMR

Settings

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 makes use of the following icons in the message box:

ℹ Information

⚠ Warning

✖ Error

Timeout in Seconds (0 = no 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.

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 5th 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.

Frequency

S.*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.

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 **Generate New**.

Test Message Box

Click the Test Message Box button to preview the popup message dialog box. The preview is shown exactly as it will appear on the client. The only exception to this is that dynamic variables used anywhere in the Window Title or Message. Since dynamic variables are evaluated at the time a user logs in, the manager is not able to resolve this variable while configuring the message box. The dynamic variable will be shown in place of the actual value of the variable.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

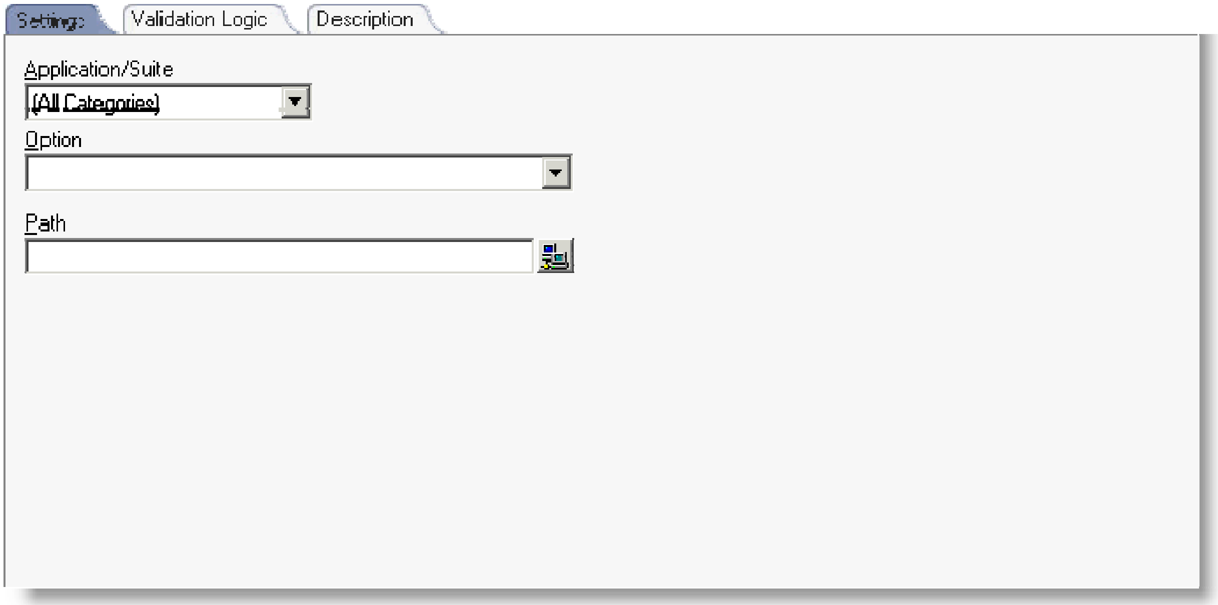
Description

Select the **Description** tab to set the description for this element.

Microsoft Office Settings

The Microsoft Office Settings 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.



Application/Suite
(All Categories)

Option

Path

Settings

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 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.

Description

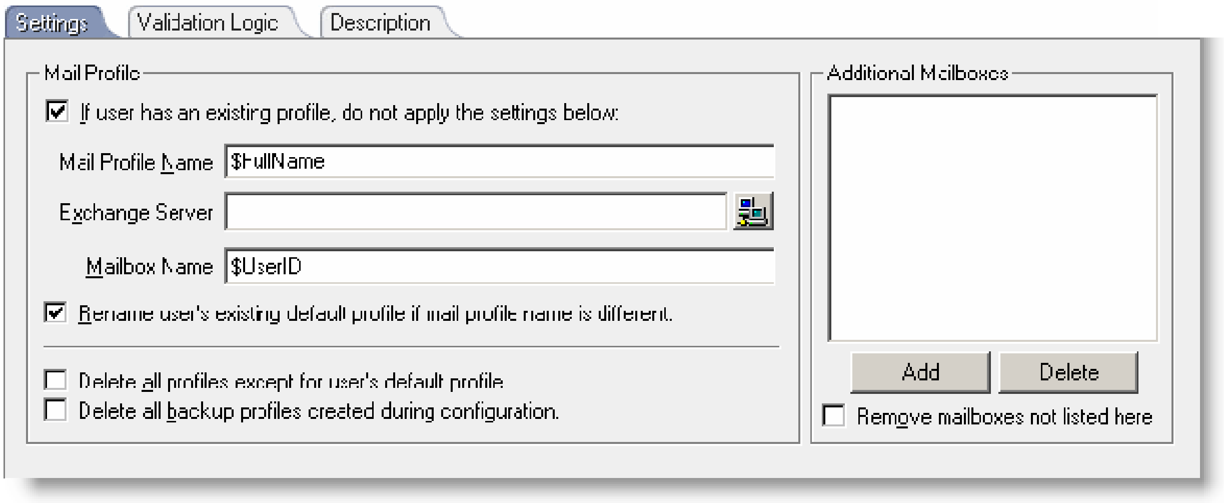
Select the **Description** tab to set the description for this element.

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.



☑ If user has an existing profile, do not apply the settings below:

Mail Profile Name: $FullName

Exchange Server:

Mailbox Name: $UserID

☑ Rename user's existing default profile if mail profile name is different.

☐ Delete all profiles except for user's default profile

☐ Delete all backup profiles created during configuration.

☐ Remove mailboxes not listed here

Settings

If user has 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 enable the creation of mail profiles regardless of whether there are existing profiles for the user.

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.

Exchange 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 to locate and select a server.

Mailbox Name

Enter the name of the mailbox the user will be connected to on the Exchange Server.

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.

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 profiles except for user's default profile

Select this check box to delete all profiles for this user except the user's default profile.

Delete all backup profiles created during configuration

Select this check box to remove all backup profiles.

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

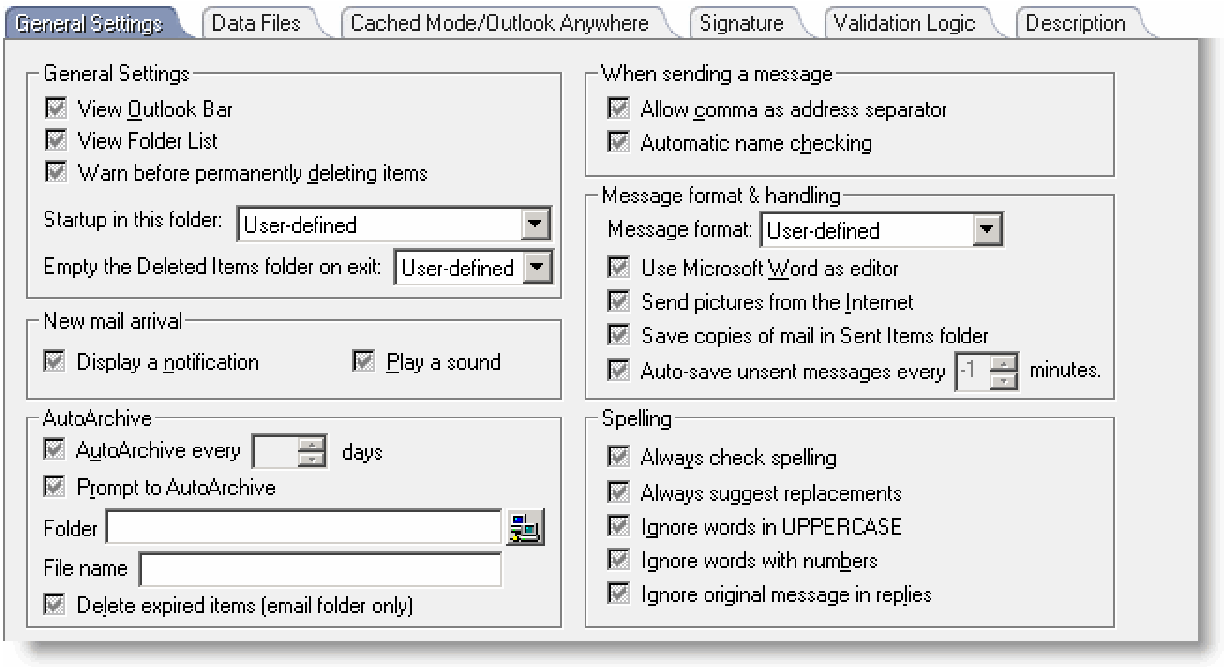
Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

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.



General Settings
▣ View Outlook Bar
▣ View Folder List
▣ Warn before permanently deleting items
Startup in this folder: User-defined
Empty the Deleted Items folder on exit: User-defined

New mail arrival
▣ Display a notification ▣ Play a sound

AutoArchive
▣ AutoArchive every days
▣ Prompt to AutoArchive
Folder
File name
▣ Delete expired items (email folder only)

When sending a message
▣ Allow comma as address separator
▣ Automatic name checking

Message format & handling
Message format: User-defined
▣ Use Microsoft Word as editor
▣ Send pictures from the Internet
▣ Save copies of mail in Sent Items folder
▣ Auto-save unsent messages every -1 minutes.

Spelling
▣ Always check spelling
▣ Always suggest replacements
▣ Ignore words in UPPERCASE
▣ Ignore words with numbers
▣ Ignore original message in replies

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 📁 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 & 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.

Data Files

Select the Data Files tab for Outlook settings pertaining to **PAB & Personal Folder Settings and Offline Access Settings.**

Cached Mode/RPC

Select the Cached Mode/RPC tab to configure Outlook's Cached Exchange Mode.

Signature

Select the Signature tab 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.

Validation Logic

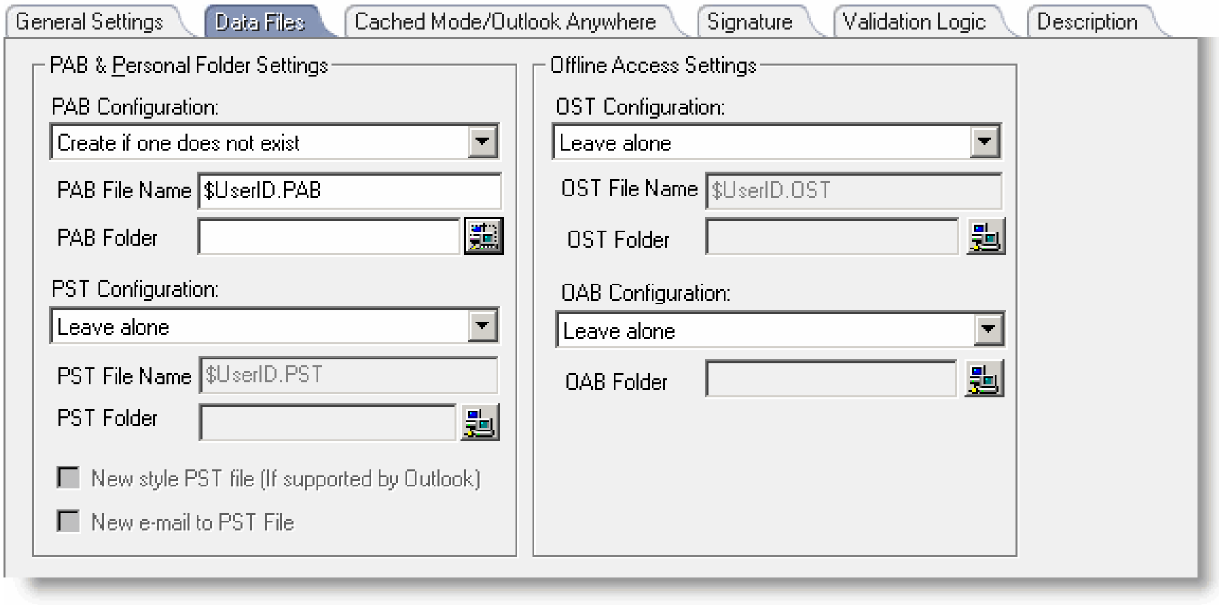
Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

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 & Personal Folder Settings

PAB Configuration: Create if one does not exist

PAB File Name: $UserID.PAB

PAB Folder:

PST Configuration: Leave alone

PST File Name: $UserID.PST

PST Folder:

□ New style PST file (If supported by Outlook)

□ New e-mail to PST File

Offline Access Settings

OST Configuration: Leave alone

OST File Name: $UserID.OST

OST Folder:

OAB Configuration: Leave alone

OAB Folder:

PAB & Personal Folder Settings

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 ▦ to navigate to the folder if it is located on a network share. 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 📁 to navigate to the folder if it is located on a network share. 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.

New e-mail to PST file

Select this check box, ☑, to send new mail to the defined PST folder/file. Clear the check box, □, to use the user's current Outlook inbox. Gray the check box, ▣, to preserve the user's current Outlook setting. 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**.

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 📁 to navigate to the folder. If the specified folder does not exist, Desktop Authority will create it.

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.

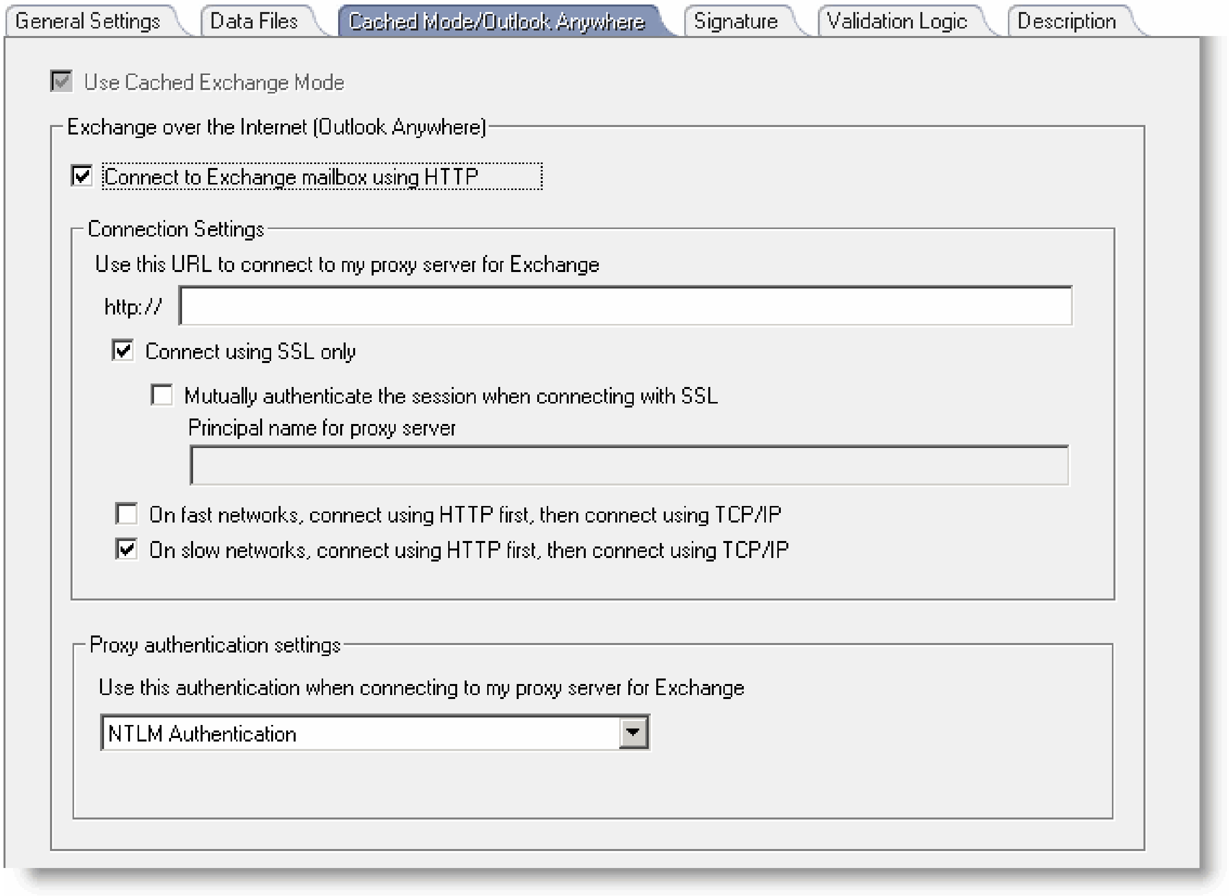
OAB Folder

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 to navigate to the folder. If the specified folder does not exist, Desktop Authority will create it.

Microsoft Outlook Cached Mode/Outlook Anywhere

The Microsoft Cached Mode/Outlook Anywhere 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.



☑ Use Cached Exchange Mode

Exchange over the Internet (Outlook Anywhere)

☑ Connect to Exchange mailbox using HTTP

Connection Settings

Use this URL to connect to my proxy server for Exchange

http://

☑ Connect using SSL only

□ Mutually authenticate the session when connecting with SSL

Principal name for proxy server

□ On fast networks, connect using HTTP first, then connect using TCP/IP

☑ On slow networks, connect using HTTP first, then connect using TCP/IP

Proxy authentication settings

Use this authentication when connecting to my proxy server for Exchange

NTLM Authentication

Use Cached Exchange Mode

Select this check box, ☑, to configure Outlook to use it's 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.

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.

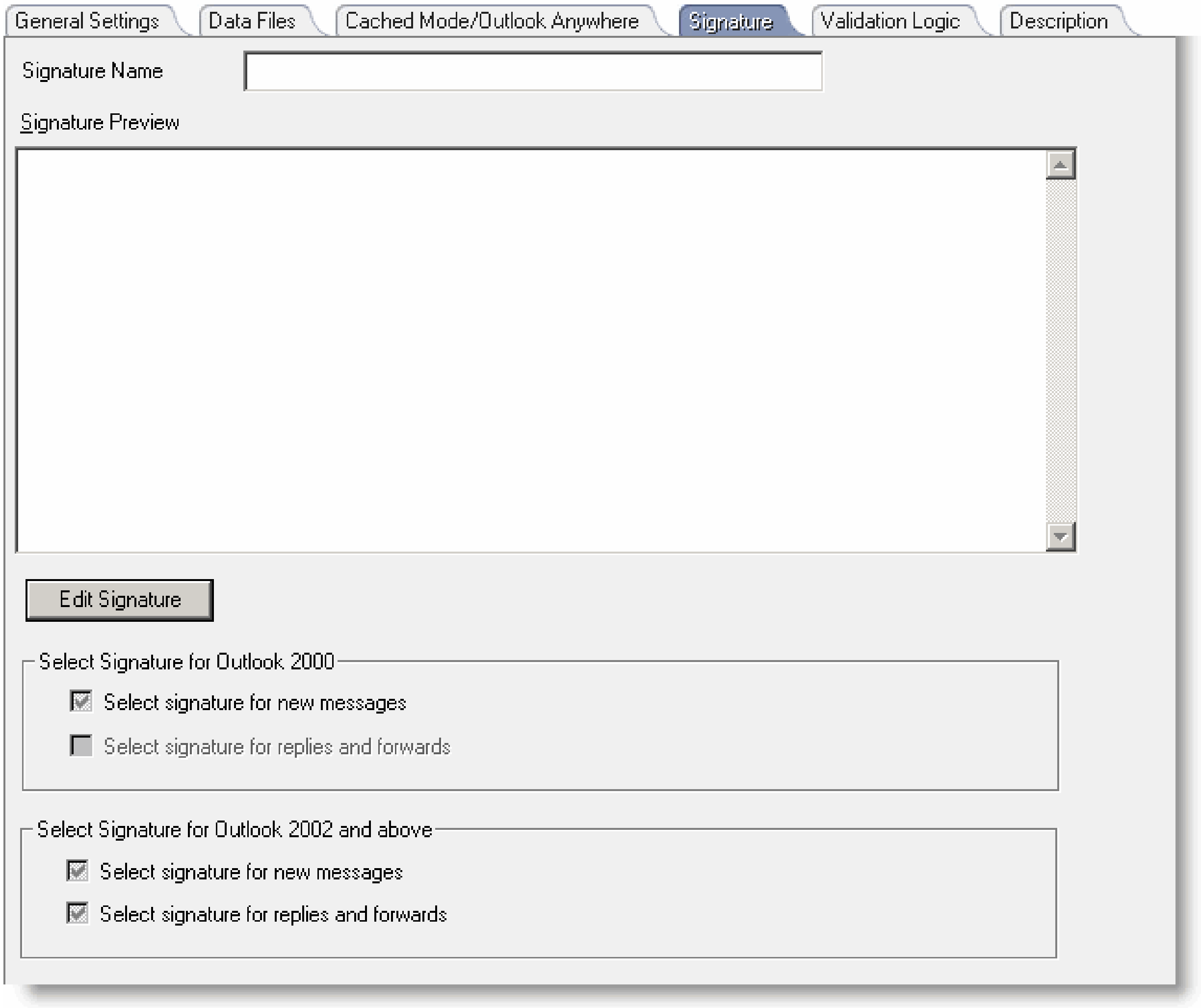
Proxy authentication settings

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.

MICROSOFT OUTLOOK 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.



Select Signature for Outlook 2000

☑ Select signature for new messages

☐ Select signature for replies and forwards

Select Signature for Outlook 2002 and above

☑ Select signature for new messages

☑ Select signature for replies and forwards

Signature Name

Enter a name for the signature. This will be the name of the signature used in Outlook.

Signature Code

Enter plain text or HTML code to be included in Outlook messages as the signature.

Preview Signature

Click the Preview Signature button to preview the Outlook signature. The preview is shown exactly as it will appear in the message.

Edit Signature

Click the Edit Signature button to open the system's default HTML editor. Once opened, create the signature code and exit the editor. The newly created signature will be displayed in the Signature Code box.

If the signature is created in another editor, it may not be able to read into the signature code box. If this is the case, a message will be posted and a manual copy and paste will be necessary.

Select Signature for Outlook 2000

Select signature for new messages

Select this check box, ☑, to configure Outlook 2000 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 2000 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 2000 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 2000 setting regarding the use of signatures at the end of every message that is a reply or forward of a previous message.

Select Signature for Outlook 2002 and above

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.

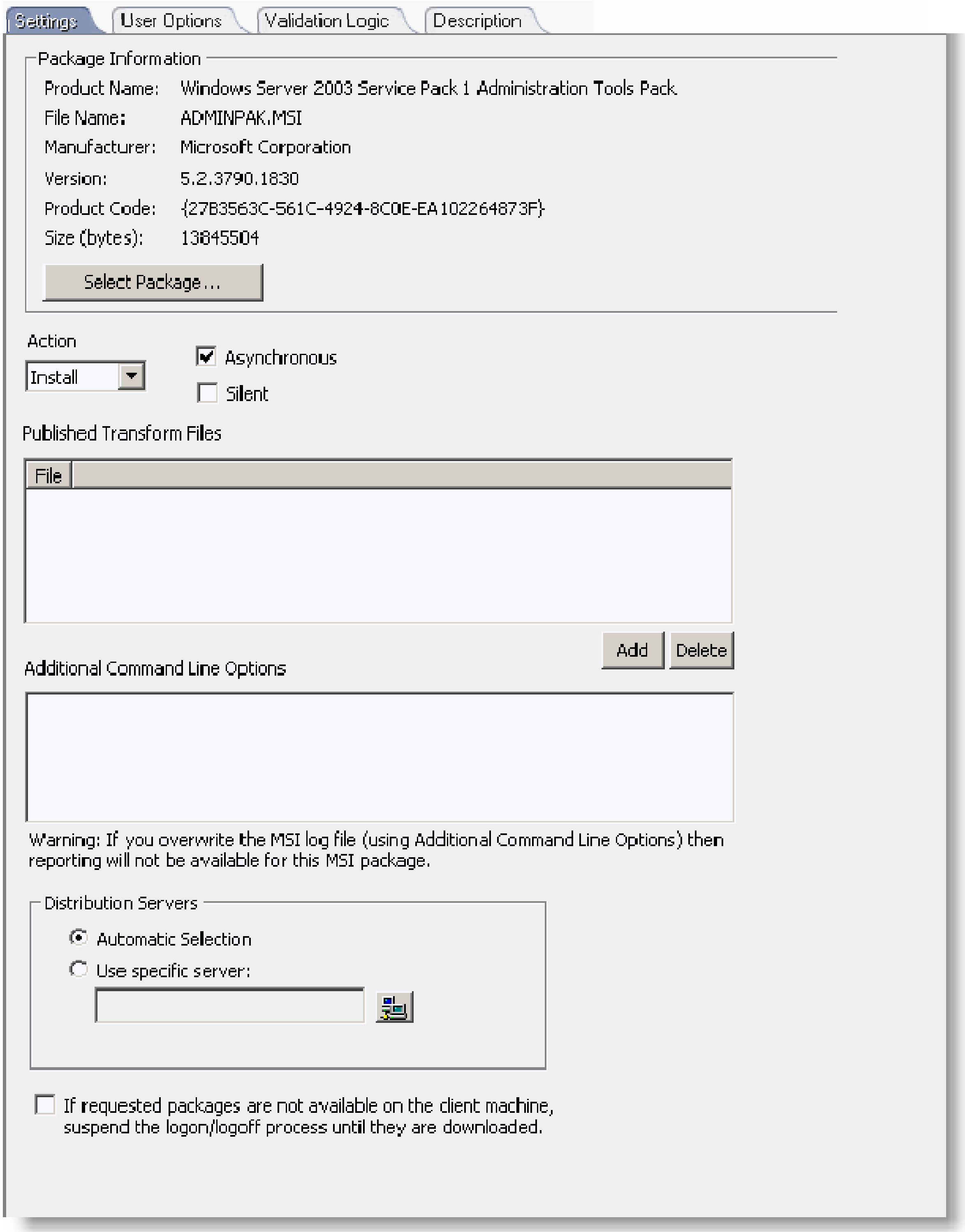
MSI PACKAGES*

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.

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.



Package Information

Product Name: Windows Server 2003 Service Pack 1 Administration Tools Pack

File Name: ADMINPAK.MSI

Manufacturer: Microsoft Corporation

Version: 5.2.3790.1830

Product Code: {27B3563C-561C-4924-8C0E-EA102264873F}

Size (bytes): 13845504

Action: Install

☑ Asynchronous

□ Silent

Published Transform Files

Additional Command Line Options

Warning: If you overwrite the MSI log file (using Additional Command Line Options) then reporting will not be available for this MSI package.

Distribution Servers

● Automatic Selection

○ Use specific server:

□ If requested packages are not available on the client machine, suspend the logon/logoff process until they are downloaded.

Settings

Package Information

The package information box displays information regarding the selected package. Product Name, File Name, Manufacturer, Version, Product Code and File Size information are displayed.

Select Package

Click Select Package to choose a package from a list of published packages. When clicked, a popup list is displayed with packages available for selection.

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.

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 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.

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 the 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?

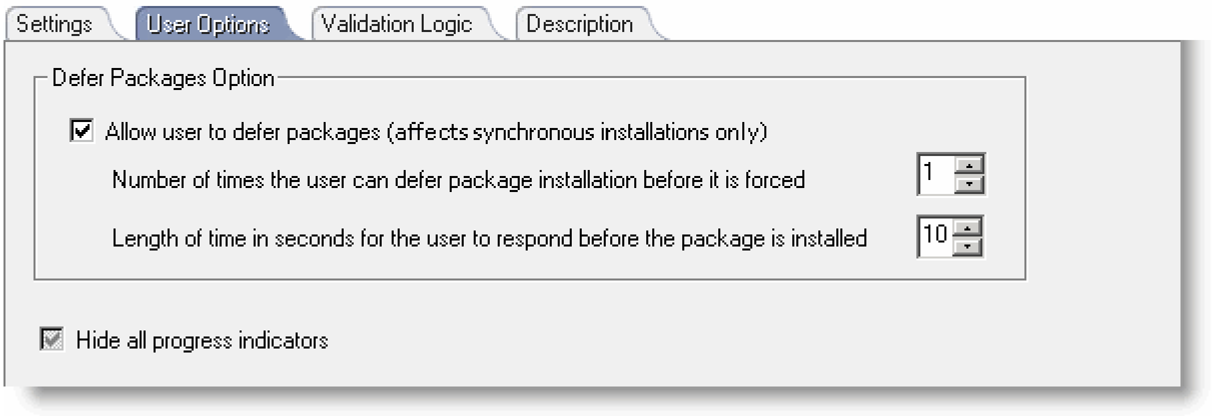
If requested packages are not available on the client machine, suspend the logon/logoff process until they are downloaded.

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



Defer Packages Option

☑ Allow user to defer packages (affects synchronous installations only)

Number of times the user can defer package installation before it is forced: 1

Length of time in seconds for the user to respond before the package is installed: 10

☑ Hide all progress indicators

Defer Packages Option

Allow user to defer packages (affects synchronous installations only)

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 it is forced

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.

Length 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 expire, the package will automatically be installed.

Hide all progress indicators

Select this box to hide the package deployment progress indicators. This includes the machine assessment dialog as well as package download and install/uninstall dialogs.

*This feature is not a standard part of Desktop Authority Express. To obtain this feature, Desktop Authority Express must be upgraded to the full version of Desktop Authority.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

*This feature is not a standard part of Desktop Authority Express. To obtain this feature, Desktop Authority Express must be upgraded to the full version of Desktop Authority.

✚ PATCH DEPLOYMENT*

Desktop Authority's Patch Distribution and Deployment feature ensures that your Microsoft desktop Operating Systems and applications are kept up-to-date with the latest patches from Microsoft. Patches may be deployed to Microsoft Windows 2000, Microsoft Windows XP and Microsoft Windows Vista workstations, both 32- and 64-bit operating systems.

The Patch Deployment object provides the ability to deploy patches on clients during the logon, logoff or shut down events, based on the specified Validation Logic. Before a patch is installed, several checks are completed to ensure that the Operating System, product, version, language, and etc. match the intended recipient's configuration. Patches may also be uninstalled from a client machine if the patch contains uninstall capabilities.

Desktop Authority will not attempt to install patches if the client does not have enough available disk space. The engine determines the amount of available disk space before the patch is installed. By default, 200 mb of disk space must be available to install any patch. This default can be overridden by defining a value in the global or profile definition file.

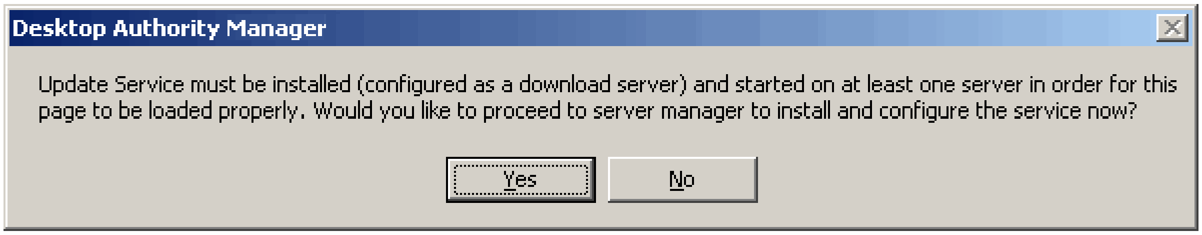
The variable #HotFixFreeSpaceNeededInMB is used to override the available disk space amount. Select Global Options > Definitions or select the Definitions tab on the profile's settings.

Example:

```
#HotFixFreeSpaceNeededInMB="100"
```

Patch Deployment, in evaluation mode, allows patches to be downloaded from Microsoft. However, only Low severity patches can be installed via desktop Authority in this evaluation mode.

Once the Patch Deployment Subscription service is purchased, all patch file(s) available from Microsoft can be downloaded and installed/uninstalled centrally with Desktop Authority. The Update Service must be installed and configured in order for Desktop Authority to retrieve the latest patch listings and files. If it is not configured at the time the Patch Deployment object is selected in the Navigation Pane, a message will be displayed with an opportunity to install and configure the service.


Desktop Authority Manager

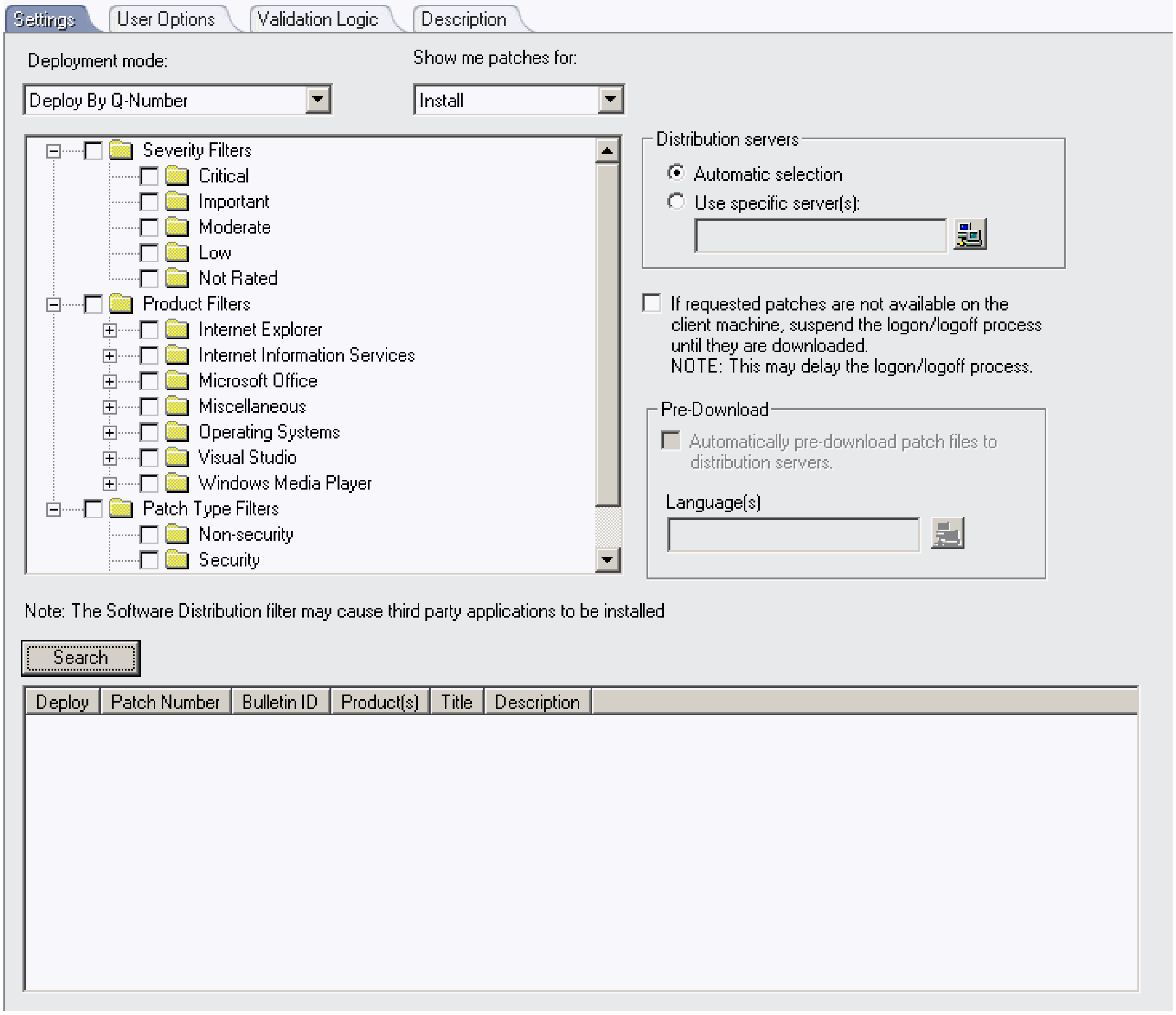
Update Service must be installed (configured as a download server) and started on at least one server in order for this page to be loaded properly. Would you like to proceed to server manager to install and configure the service now?

Once configured, the download servers will query scriptlogic.com to determine the product mode and download updated patch file listings, when available, and requested patch files. For more information on the Update Service, see What is the Update Service?

Timely installation of patches is essential to the security of the enterprise network. Following the recommended configurations will help to administer, distribute and install Microsoft operating system and product patches in a timely manner, without compromise to the security of the network.

Note: If the server does not have Internet access, the Desktop Authority Updates and Patch Download Service (DAUPDS) can be used to provide the Enterprise the ability to download patches and updates for Desktop Authority Servers that may not or can not have Internet access. This tool will download the updates and patches which can be imported into Desktop Authority for consumption by the Update Service. For more information on this tool, go to the Desktop Authority support page on the ScriptLogic website.

Settings



Deployment mode: Deploy By Q-Number

Show me patches for: Install

Distribution servers

● Automatic selection

○ Use specific server(s):

□ If requested patches are not available on the client machine, suspend the logon/logoff process until they are downloaded.
NOTE: This may delay the logon/logoff process.

Pre-Download

□ Automatically pre-download patch files to distribution servers.

Language(s)

Note: The Software Distribution filter may cause third party applications to be installed

The Software Distribution list may contain third party applications such as Firefox, Adobe Reader, etc. and may be chosen to be deployed to client machines.

Deploy by Q-Number/Deploy by Criteria/Deploy by Individual Patch

Deploy by Individual Patch allows one or more individual patches to be selected for deployment. Patches that are available for more than one installation platform are selected only once based on the actual patch number or bulletin id. The patch will be installed for all target installation platforms that the patch supports. Use the Filter criteria to locate and select the necessary patch files. When a client logs on and validates for the patch, the selected patch files will be installed.

Deploy by Criteria allows all patches with specific severities and products to be installed. Simply select the severities and products in the Filter criteria box. When a client logs on and validates for the patch deployment element, all patch files for the selected severities and products will be installed.

Deploy by Q-Number allows one or more individual patches to be selected for deployment. Patches that are available for more than one installation platform are selected based on the actual installation platform. A single patch number or bulletin id may be selected more than once in order to patch the selected target platforms. Use the Filter criteria to locate and select the necessary patch files. When a client logs on and validates for the patch, the specified patch files will be installed.

Show me patches for

Select from Install/Rollback (Uninstall) from the drop list. Selecting Install will show all patches that can be chosen for installation on target machines. Selecting Rollback will show all patches that contain an Uninstall procedure. Any patch selected with this option will be removed from target machines it if exists.

Filter

Use the Filter tool to minimize the available patch list based on severity and/or product. Select the Severity Filters box to automatically select each severity listed below it or select individual severities below the Severity Filters box. Clear the Severity Filters check box to clear all selected severities.

Select the Product Filters box to automatically select all products listed below it or select individual products below the Product Filters box. Clear the Product Filters box to clear all selected products.

Search

Click Search to filter the patch list based on the Severity and Product filters chosen in the Filter list. A count of selected patches will be displayed following the search.

Patch List

The Patch list is available when the Deploy by Individual Patch or Deploy by Q-Number option is selected. This list displays all patches matching the filter criteria. Information regarding each patch includes the Patch number and Affected Products. The patch list is sortable by any one of the columns available in the list. Sort the list by clicking on a column header.

Select a patch to deploy by selecting the Deploy box. To deploy multiple consecutive patches from the list, click on the first one. While holding down the SHIFT key, select the last consecutive patch, and then select the Deploy box. Multiple non-consecutive patches may be selected from the list by pressing the CTRL key while selecting each individual patch and then selecting the Deploy box.

Distribution servers

Select Automatic selection to copy the patch file(s) to the client from the selected server. Select Use specific servers to define a specific server(s) to copy the patch file(s) from. Separate multiple server names using a semicolon (;).

If requested patches are not available on the client machine, suspend the logon/logoff process until they are downloaded.

Select this box to download the necessary patch file if it does not exist on the client. The download request is sent to a server that is a designated download server. Once requested, the patch file will be downloaded (if necessary) and duplicated on the distribution server. Any client that requests the same patch file from the distribution server following, the duplication of the patch file, will receive the patch file for installation. Clear this box to continue processing if the patch file does not exist at the specified location. The client will check for the patch during future logons until it can be installed successfully.

Pre-Download

Automatically pre-download patch files to distribution servers. (Available for Deploy by criteria only)

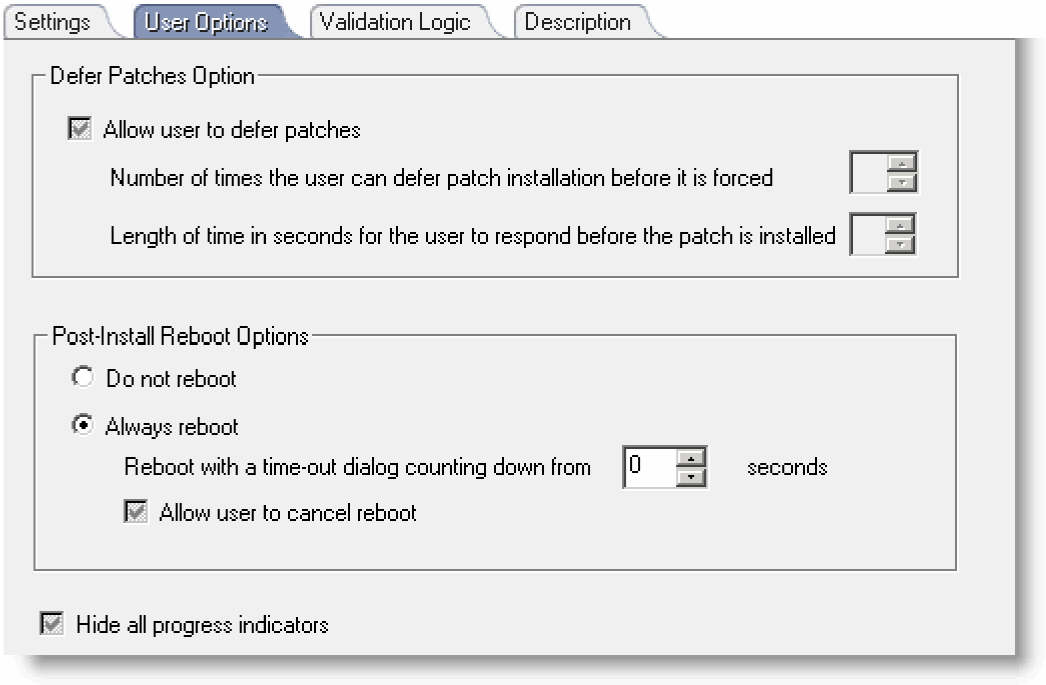
Select this box to allow the Update Service to automatically download new patches when there are any that match the specified Products and Severities.

Languages

Click to select one or more languages for the automatic pre-download patch files to download. Select from German, English, French and/or Spanish.

User Options

The Client Options allow settings to be configured to allow the end user to defer the installation of a patch. A patch can be deferred for a specified number of times.



Defer Patches Option

☑ Allow user to defer patches

Number of times the user can defer patch installation before it is forced

Length of time in seconds for the user to respond before the patch is installed

Post-Install Reboot Options

○ Do not reboot

● Always reboot

Reboot with a time-out dialog counting down from 0 seconds

☑ Allow user to cancel reboot

☑ Hide all progress indicators

Defer Patches Option

Allow user to defer patches

Select this box to allow the end user to defer the installation of a patch to another session.

Number of times the user can defer patch installation before it is forced

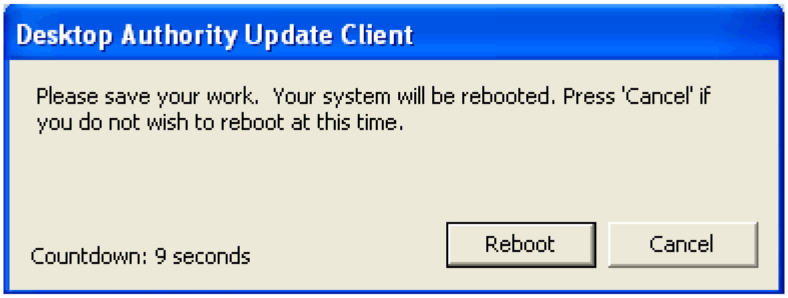
Enter the number of times a user can defer a patch. Once the patch has been deferred the selected number of times, the patch installation will no longer be allowed to be deferred and will automatically be installed.

Length of time in seconds for the user to respond before the patch is installed

Enter the number of seconds the user has to respond to the defer patch installation dialog. If there is no response to the dialog and the number of seconds expire, the patch will automatically be installed.

Post-Install Reboot Options

Some patches require the machine to be rebooted once the patch is installed. The Post-Install Reboot options provide the possibility for the end user to cancel the reboot process.



Desktop Authority Update Client

Please save your work. Your system will be rebooted. Press 'Cancel' if you do not wish to reboot at this time.

Countdown: 9 seconds

Do not reboot

Select this option to cancel the reboot of the machine following the install of a patch.

Always reboot

Select this option to always reboot of the machine following the install of a patch. This reboot operation has an optional message to the end user.

Reboot with a timeout dialog counting down from xx seconds

To warn the end user of the impending reboot operation enter the number of seconds to display the warning dialog for. Leave this setting to 0 to disable the warning dialog.

Allow user to cancel reboot

Select this box to allow the user to cancel the reboot operation when the warning dialog is displayed.

Note: Opting to delay a reboot after patches are installed is not recommended as the installation of many patches do not complete until after a reboot has occurred.

Hide all progress indicators

Select this box to hide the patch deployment progress indicators. This includes the machine assessment dialog as well as patch download and install/uninstall dialogs.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Installing patches during Refresh Validation Logic Timing is not recommended. Each time a patch installation is requested, the patch assessment process will run. Setting the installation to execute at Refresh will cause the patch assessment process to execute at this time as well (every hour) on all target machines. The patch assessment process could turn into a CPU intensive procedure.

Description

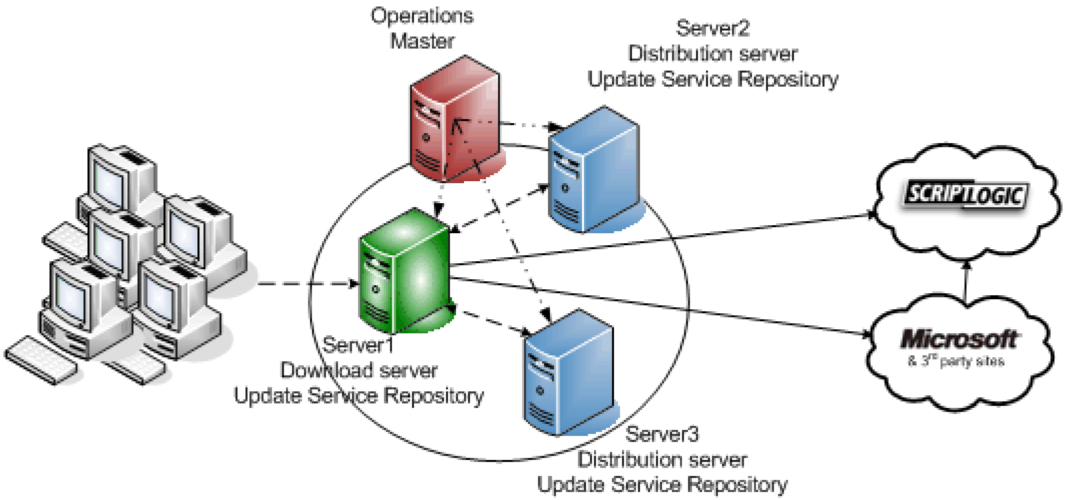
Select the **Description** tab to set the description for this element.

*This feature is not a standard part of Desktop Authority Express. To obtain this feature, Desktop Authority Express must be upgraded to the full version of Desktop Authority.

UPDATE SERVICE BEST PRACTICES

Timely installation of updates and patches are essential to the security of the enterprise network. Following the recommended configurations below will help to administer, distribute and install Microsoft operating system and product patches and updates in a timely manner, without compromise to the security of the network.

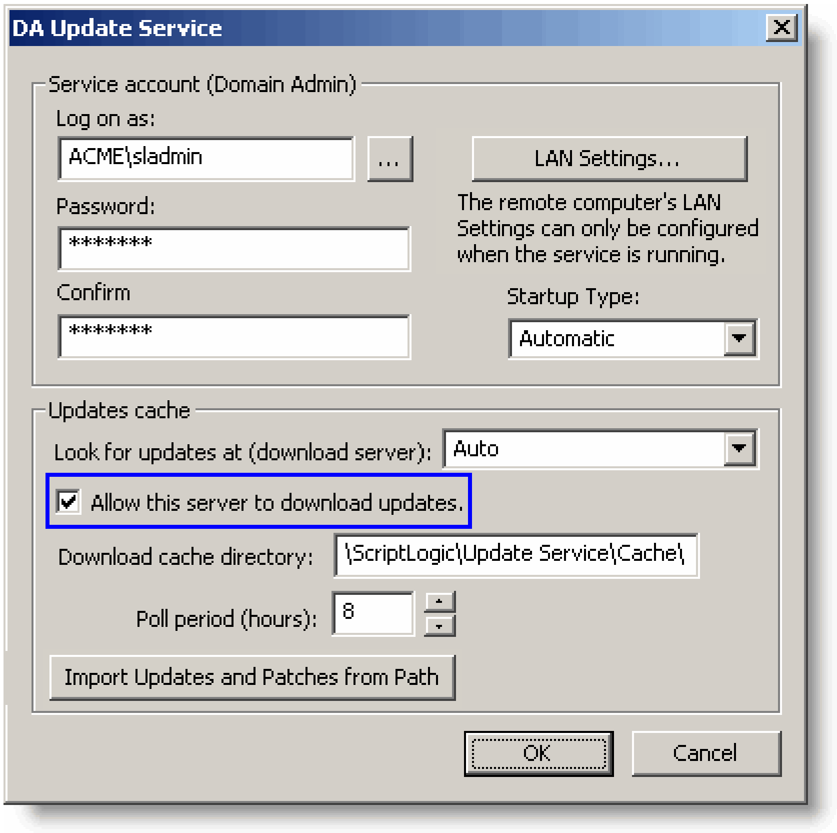
Single Site LAN



The installation of the Update Service is required in order to use Software Management, USB/Port Security, Patch Management and/or Anti-Spyware objects. The Update Service is installed within the Server Manager.

The MSI Packages object publishes packages to each server that has the Update Service installed.

To best configure the Update Service for a single site network, there should be one server that is designated as the download server. A server is configured to be a download server in the Update Service configuration dialog.



DA Update Service

Service account (Domain Admin)

Log on as: ACME\sladmin

Password: *******

Confirm: *******

The remote computer's LAN Settings can only be configured when the service is running.

Startup Type: Automatic

Updates cache

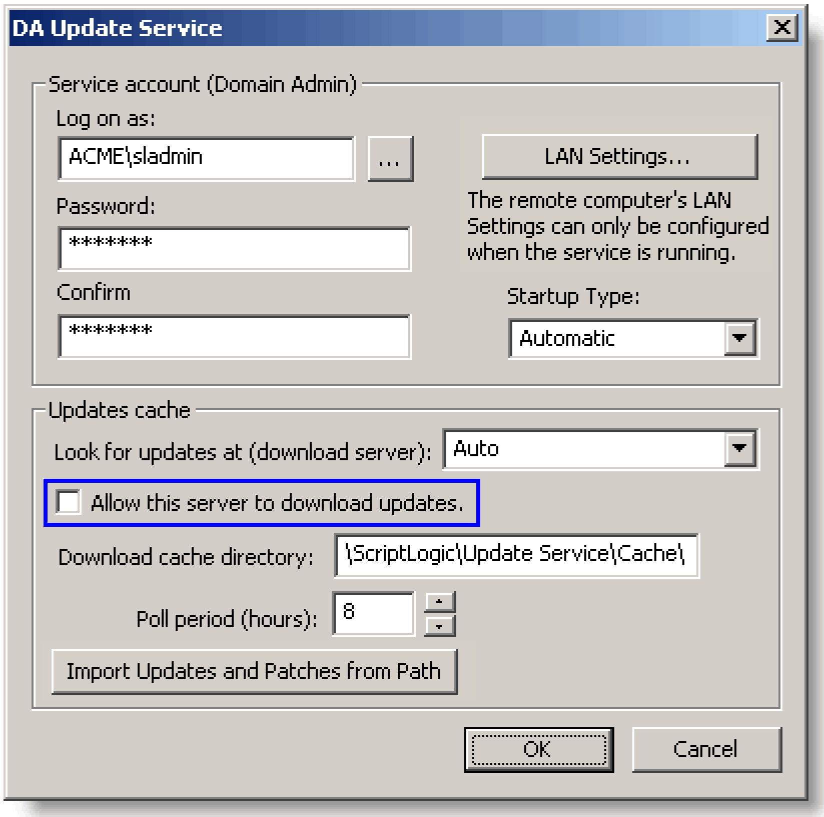
Look for updates at (download server): Auto

☑ Allow this server to download updates.

Download cache directory: \ScriptLogic\Update Service\Cache\

Poll period (hours): 8

Download Server configuration



Log on as: ACME\sladmin

Password: *******

Confirm: *******

The remote computer's LAN Settings can only be configured when the service is running.

Startup Type: Automatic

Look for updates at (download server): Auto

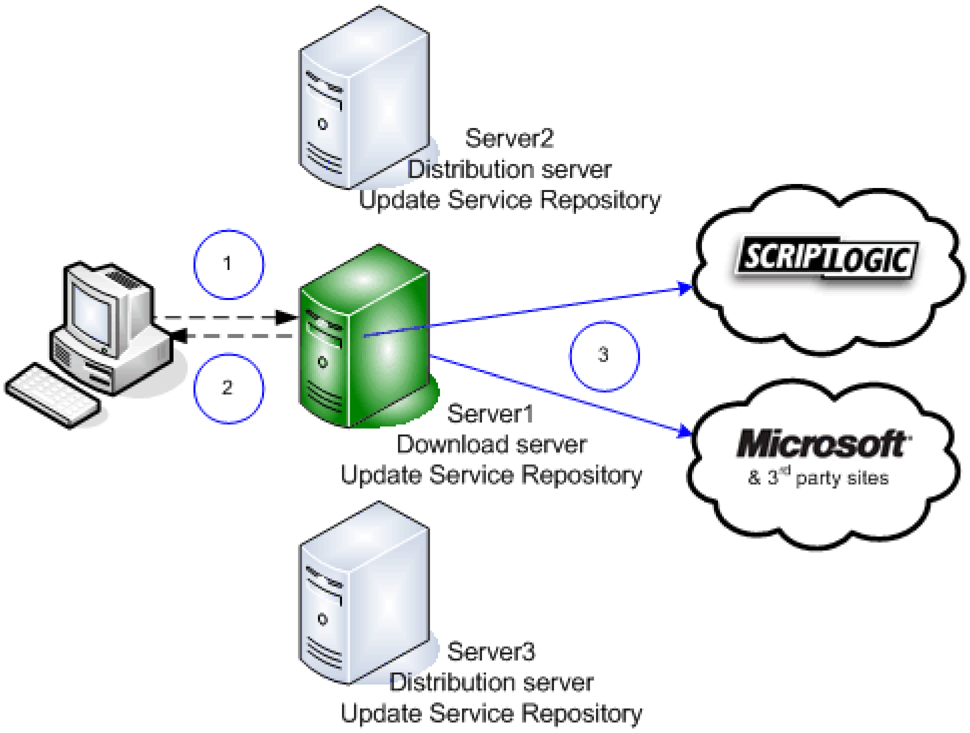
□ Allow this server to download updates.

Download cache directory: \ScriptLogic\Update Service\Cache\

Poll period (hours): 8

Distribution server configuration

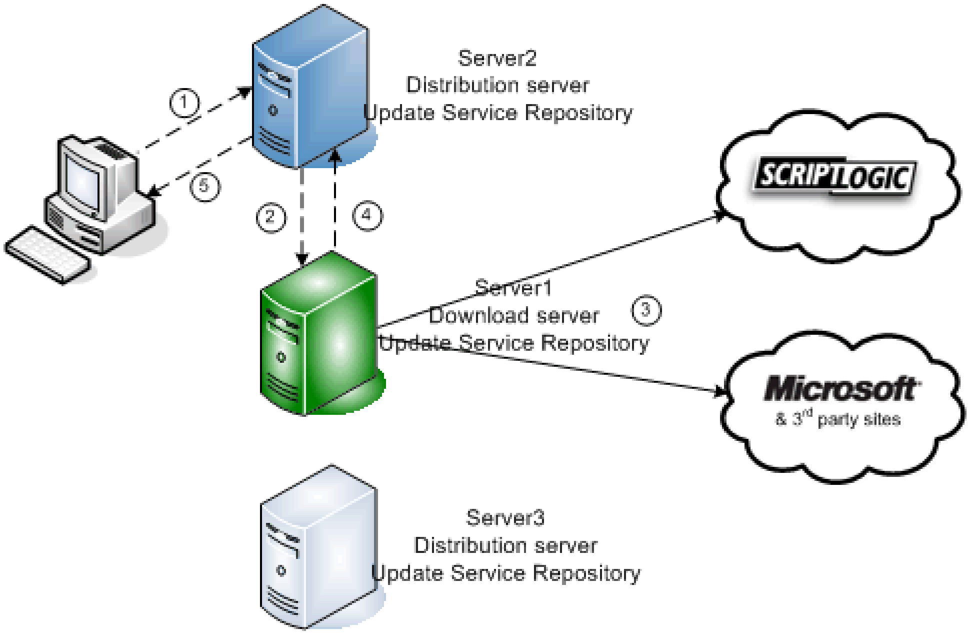
The download server pulls patch files from Microsoft. The downloaded patch files are stored in the directory specified in the Update Service configuration dialog. This directory by default is %Program Files%/ScriptLogic/Update Service/Cache. The download server also connects with ScriptLogic to pull down licenses information, anti-spyware definition updates, patch database updates and ScriptLogic Patch Management updates. The connection to the ScriptLogic web site is a secure connection.



In the illustration above, a client logs on to the network and is connected to Server11 via a random selection by the Desktop Authority engine. In this scenario, Server1 is configured as the download server. If the patch exists on the server, it is distributed to the client as requested, based on the validation logic specified for the patch file(s).

If the patch file has not yet been downloaded by the server, a request is sent via the Update Service to Microsoft and the patch file(s) is downloaded3. In this case, one of two scenarios will occur on the client. Depending on the configuration of the "If patch is not available, do not continue" prompt on the Patch Deployment element, either Desktop Authority will continue to process on the client without installing the patch, or it will pause and wait for the patch to download and install before going any further. If the prompt is selected (checked on), the client will wait for the patch to download and install. If the prompt is cleared (checked off), the client will attempt to install the patch during the next logon attempt.

In this scenario, Server2 and Server3 are designated as distribution servers. This means that these servers will never directly request a patch file from Microsoft. Instead, these servers will send a request to the networks download server for the patch file. At this time, the patch file will be delivered to the distribution server that requested it.

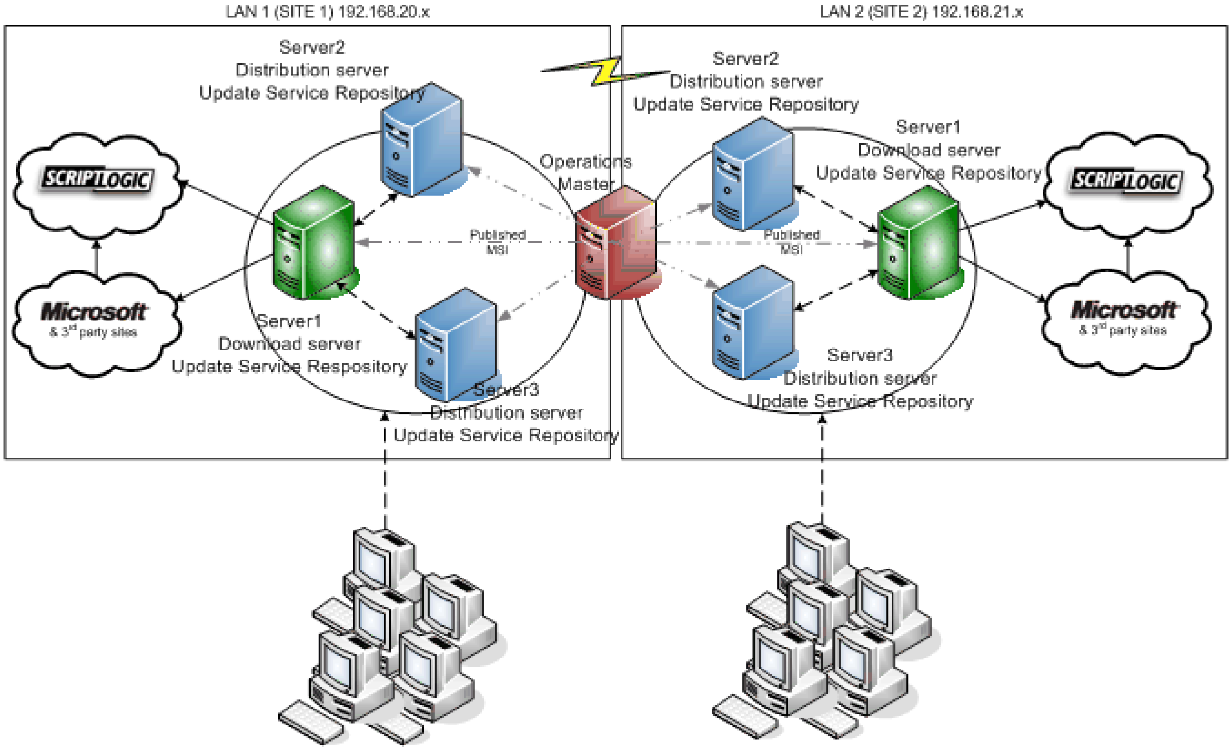


When a client logs onto the network and is connected to a distribution server1, a request is sent from the distribution server to the download server for the patch file (if it does not already exist on the distribution server)2. If the patch file does not already exist on the download server, it is downloaded by the Update Service3. The patch file is then distributed to the distribution server4 and then deployed to the client5.

Again, one of two scenarios will occur on the client when connected to a distribution server. Depending on the configuration of the "If patch is not available, do not continue" prompt on the Patch Deployment element, either Desktop Authority will continue to process on the client without installing the patch, or it will pause and wait for the patch to download and install before going any further. If the prompt is selected (checked on), the client will wait for the patch to download and install. If the prompt is cleared (checked off), the client will attempt the patch installation the on the next logon attempt.

Multiple Site LAN

On a network configured with multiple sites, the Patch Deployment process is similar as discussed above. However, there are some differences which are explained below.



In the above illustration, the network consists of two sites. Each site should have its own single download server. All other servers on the site should be set up as distribution servers. The Operations Master publishes all packages for the MSI Packages object to all servers (on all sites) that have a running Update Service.

Upon logon, a client is connected to a server within the site the client exists in. Upon a patch deployment request, a server within its own site is randomly chosen by the Desktop Authority engine. If the download server is chosen, the necessary patches are deployed to the client as requested.

If the patch file has not yet been downloaded by the server, a request is sent via the Update Service to Microsoft and the patch file(s) is downloaded. In this case, one of two scenarios will occur on the client. Depending on the configuration of the "If patch is not available, do not continue" prompt on the Patch Deployment element, either Desktop Authority will continue to process on the client without installing the patch, or it will pause and wait for the patch to download and install before going any further. If the prompt is selected (checked on), the client will wait for the patch to download and install. If the prompt is cleared (checked off), the client will attempt the patch installation the on the next logon attempt.

If a distribution server is selected via the Desktop Authority engine and the patch is available it is automatically deployed to the client.

If the patch file is not yet available on the distribution server, a request will be sent to the download server. The patch will be downloaded from Microsoft (if necessary) moved to the distribution server and then deployed to the client. Again, at this time, one of two scenarios will occur on the client when authenticated by the distribution server. Depending on the configuration of the "If patch is not available, do not continue" prompt on the Patch Deployment element, either Desktop Authority will continue to process on the client without installing the patch, or it will pause and wait for the patch to download and install before going any further. If the prompt is selected (checked on), the client will wait for the patch to download and install. If the prompt is cleared (checked off), the client will attempt the patch installation the on the next logon attempt.

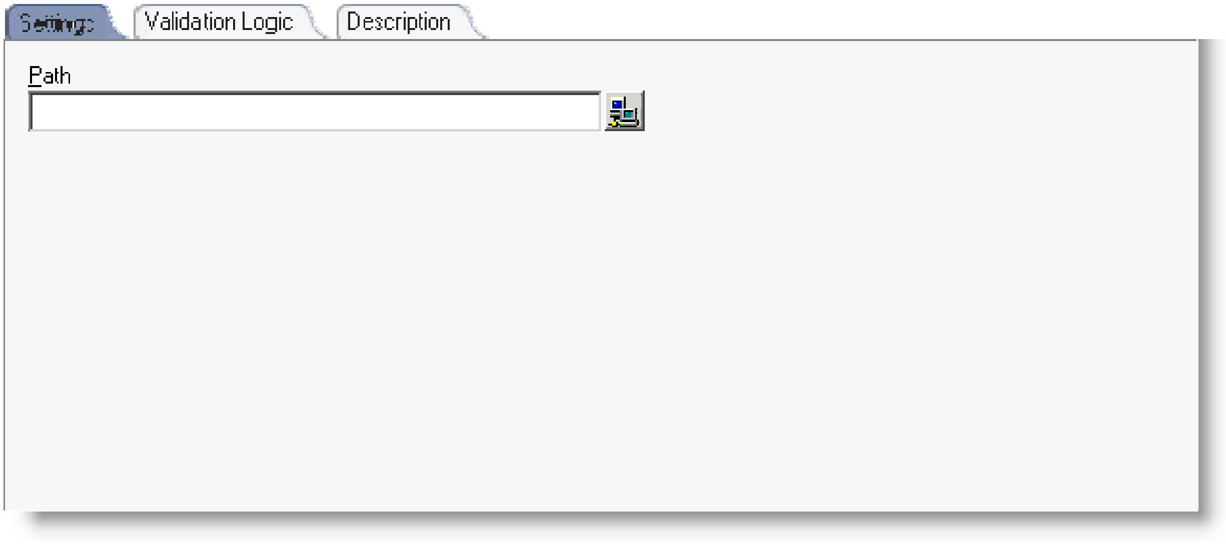
It is important to note that depending upon the speed of the link between the sites in this type of configuration versus the speed of the Internet connection, it may be faster to manually copy the download cache between sites versus allowing the patch files to propagate through the system as they are needed.

Miscellaneous Notes

- Although the Service Pack Deployment and Patch Deployment objects seem very similar, use the Service Pack Deployment object to install full service packs offered by Microsoft. A patch is an interim update which fixes one or more specific problems. A service pack is a cumulative update to fix multiple bugs and may include product enhancements. A service pack includes many patches bundled into a single service pack update.
- Prior to deploying a patch to the enterprise, use Desktop Authority's Validation Logic to target specific users or groups of users and/or specific computers or groups of computers for testing of patch installations.
- Since some patch installations may take considerable time to complete, It is recommended to target significant patches to occur at logoff time rather than logon.
- Patches for Office applications may require access to the original media (CD or DVD). To support Office patches without prompting the user to insert any form of media, the original product media should be made available on a CD/DVD drive that is accessible to all over the network.
- The Update Service requires Internet access to www.scriptlogic.com and www.microsoft.com. If a proxy is used to access the Internet, the download server must be configured to work with the proxy.

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 2000/XP/2003/Vista/2008.



Settings

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 ▦ 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.

Description

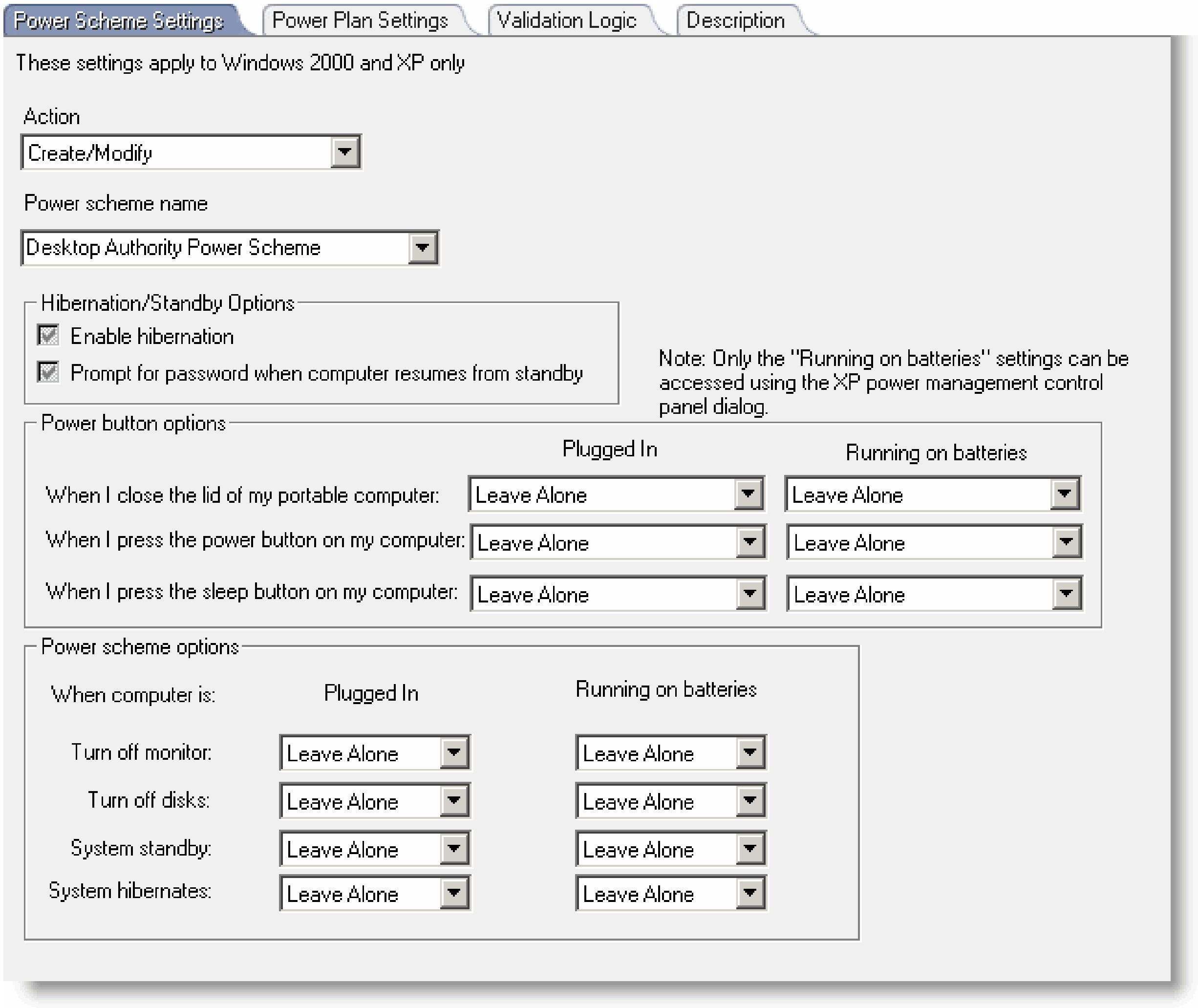
Select the **Description** tab to set the description for this element.

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 2000 and XP. Power Schemes cannot be configured to run on Terminal Servers, Member Servers or Domain Controllers and 2003 and 2008 operating systems.

To configure Power settings on Vista machines and above, select the Power Plan Settings tab.



These settings apply to Windows 2000 and XP only

Action: Create/Modify

Power scheme name: Desktop Authority Power Scheme

Hibernation/Standby Options

☑ Enable hibernation

☑ Prompt for password when computer resumes from standby

Note: Only the "Running on batteries" settings can be accessed using the XP power management control panel dialog.

Power button options

	Plugged In	Running on batteries
When I close the lid of my portable computer:	Leave Alone	Leave Alone
When I press the power button on my computer:	Leave Alone	Leave Alone
When I press the sleep button on my computer:	Leave Alone	Leave Alone

Power scheme options

When computer is:	Plugged In	Running on batteries
Turn off monitor:	Leave Alone	Leave Alone
Turn off disks:	Leave Alone	Leave Alone
System standby:	Leave Alone	Leave Alone
System hibernates:	Leave Alone	Leave Alone

Power Scheme Settings (2000 and XP operating systems only)

Action

Select *Create/Modify or Remove* from the Action list. The Create/Modify action will create a new Power scheme if one does not already exist with the specified Power Scheme name or modify the existing Power scheme if one already exists with the specified name. Remove will delete an existing Power scheme if one exists with the specified Power scheme name.

Power scheme name

Select from existing Power Schemes Always On, Home/Office Desk, Max Battery, Minimum Power Management, Portable/Laptop, or Presentation pre-defined power schemes. The pre-defined schemes exist on 2000 and XP operating systems and can be used for commonly used settings. Enter a new Power scheme name to define a new configuration set. Enter an existing power scheme name to update an existing scheme.

Hibernation/Standby Options

Enable Hibernation

This box can be set to one of three (3) different states: on (enabled) ☑, off (disabled) □, or grayed (preserve current setting) ☑.

Select the box to enable hibernation on the computer. Hibernation mode will store the contents from memory on the hard drive and then shut down. When the computer comes out of hibernation, it will return to its previous state. Clear the box to disable Hibernation mode and enable Standby mode. Standby mode will switch the computer into a low-power state. Gray the box to leave the current setting untouched.

The default for this option is grayed.

Prompt for password when computer resumes from standby

This box can be set to one of three (3) different states: on (enabled) ☑, off (disabled) □, or grayed (preserve current setting) ☑.

Select the box to prompt for a password when the system resumes. Clear the box to disable password prompting. Gray the box to leave the current setting untouched.

The default for this option is grayed.

Power button options

When I close the lid of my portable computer

Select a power option from the list. Select from Leave Alone, Do Nothing, Sleep, Hibernate, Shutdown, Shutdown and reset, Shutdown and power of or Warm eject.

When I press the power button on my computer

Select a power option from the list. Select from Leave Alone, Do Nothing, Sleep, Hibernate, Shutdown, Shutdown and reset, Shutdown and power of or Warm eject.

When I press the sleep button on my computer

Select a power option from the list. Select from Leave Alone, Do Nothing, Sleep, Hibernate, Shutdown, Shutdown and reset, Shutdown and power of or Warm eject.

Power scheme options

Turn off monitor

Specify the amount of video idle time to wait before turning off the monitor. Select Leave alone if monitor power settings are not wanted.

Turn off disks

Specify the amount of hard disk idle time to wait before spinning down the disks. Select Leave alone if power settings are not wanted with hard disk drives.

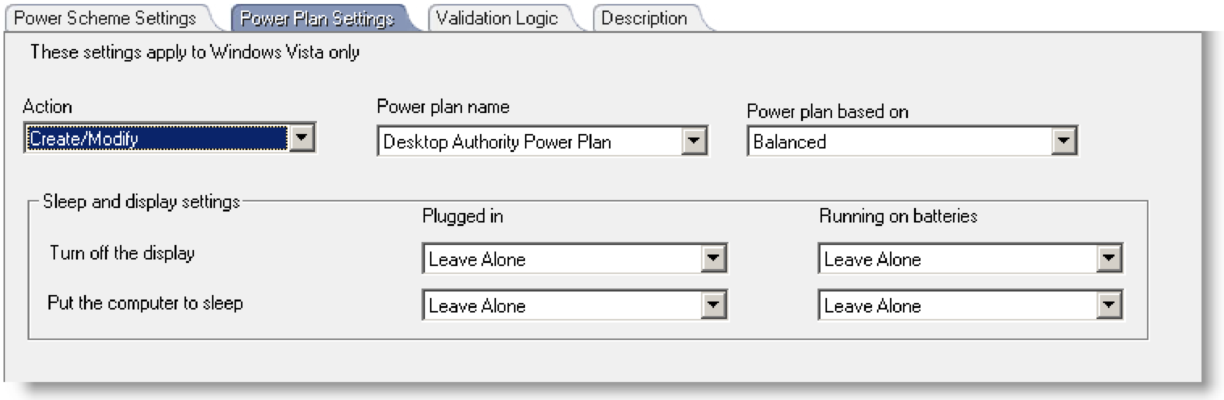
System standby

Specify the amount of idle time to wait before going into Standby mode. Select Leave alone if Standby mode is not wanted.

System hibernates

Specify the amount of idle time to wait before going into Hibernation mode. Select Leave alone if Hibernation mode is not wanted.

Power Plan Settings (Windows Vista only)



These settings apply to Windows Vista only

Action: Create/Modify

Power plan name: Desktop Authority Power Plan

Power plan based on: Balanced

Sleep and display settings

	Plugged in	Running on batteries
Turn off the display	Leave Alone	Leave Alone
Put the computer to sleep	Leave Alone	Leave Alone

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 scheme name

Select from existing Power plans Desktop Authority Power Plan, Balanced, Power Saver, and High performance pre-defined power plans. The pre-defined plans exist on Microsoft Windows Vista and can be used for common circumstances. 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

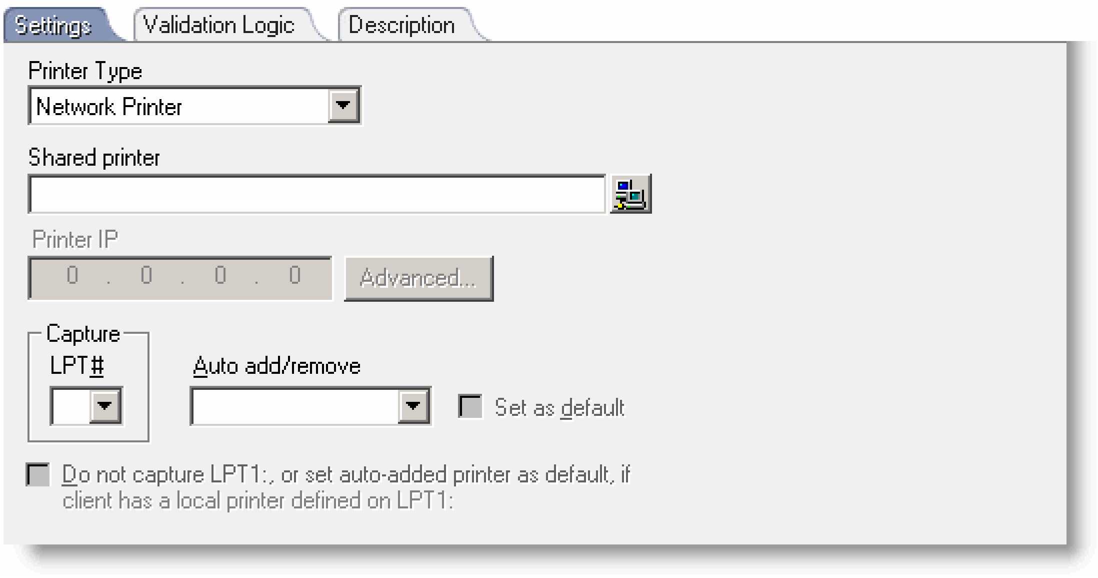
Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

PRINTERS

The **Printers** object configures printer mappings. Printer mappings redirect local printer ports (LPTx) and printer resources to a shared network printer.



Printer Type: Network Printer

Shared printer:

Printer IP: 0 . 0 . 0 . 0

Capture LPT#:

Auto add/remove:

□ Set as default

□ Do not capture LPT1:, or set auto-added printer as default, if client has a local printer defined on LPT1:

Settings

Printer Type

Select either *Network Printer* or *IP Printer* from the Printer Type list.

Shared Printer

Enter the path of the network printer. The path should be specified in the form of **\\server\share\**. Optionally, click 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.

When configuring an IP Printer, a shared printer is required in order to install the necessary drivers on the specified clients.

Printer IP

Enter the TCP/IP address defined on the printer.

Advanced

These settings will be automatically detected if an IP address was entered and the printer was detected at that address.

Protocol

Select the printer's supported printing protocol.

Port Number/Queue Name

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

Specify the printer name.

Port Name

Specify the name that will appear in Windows Printer properties port list.

SNMP Name

Specify the community name used by the printer.

LPT#

Select a port number from the list or type a new LPT port. Valid LPT port numbers are 1 - 9.

Auto add/remove

Select *Add*, *Delete*, - from the list. This allows you to choose from automatically adding or removing a printer driver on the client. This applies to clients with Microsoft Windows 2000/XP/2003/2008/Vista operating.

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".

Do not capture LPT1:, or set auto-added printer as default, if client has a local printer defined on LPT1:

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.

Description

Select the **Description** tab to set the description for this element.

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.

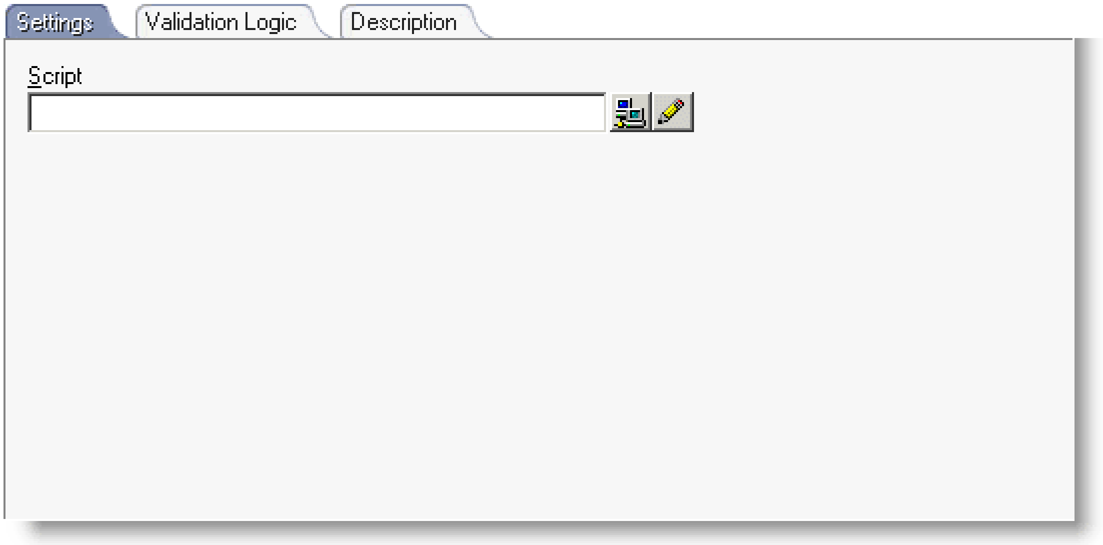
Custom scripting is relatively easy and can be as simple or complex as necessary -- though it does require programming in KiXtart and often requires a working knowledge of the Windows registry. Custom scripts contain KiXtart scripting code and may launch additional executables, batch files, or scripts of any type using the "shell" or "run" commands.

Creating a Custom Script

A custom script is an ASCII text file written using the KiXtart scripting language. 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, an element must first be created within the Pre/Post-Engine Scripts object. First, decide at which point the script should run, **Pre** or **Post Engine**. Create the element by right-clicking inside the element list on the Pre/Post-Engine Scripts object. Select New Element from the shortcut menu. Once the element is created, specify a script filename on the Settings tab. This filename should end with a .KIX extension. Once the .KIX extension is recognized by the Manager, the ✎ button will be enabled.

Documentation about the KiXtart scripting language can be found at KiXtart.org, the official home of KiXtart.

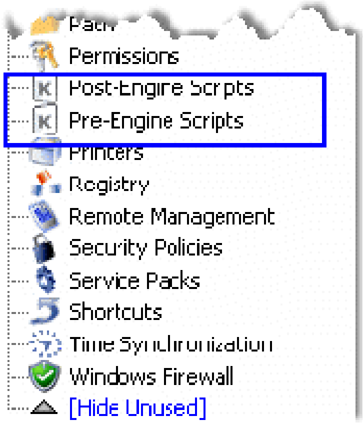


The ✎ button can be used to create or modify KiXtart scripts. When clicked, the script file will be opened within the defined Custom Script Editor. The default script editor is Microsoft's Notepad. This can be changed to load a favorite text editor by clicking File > Preferences on the Manager's File menu.

To create a script outside of the Manager, simply load your favorite text editor and start typing. Once it is complete (and tested) it may be added to the Pre and/or Post-Engine object within the Manager.

Configuring Custom Scripts within the Manger

To use a script within the Manger, first select the point at which the script should run, either **Pre** or **Post Engine**. Select the appropriate object within the profile.



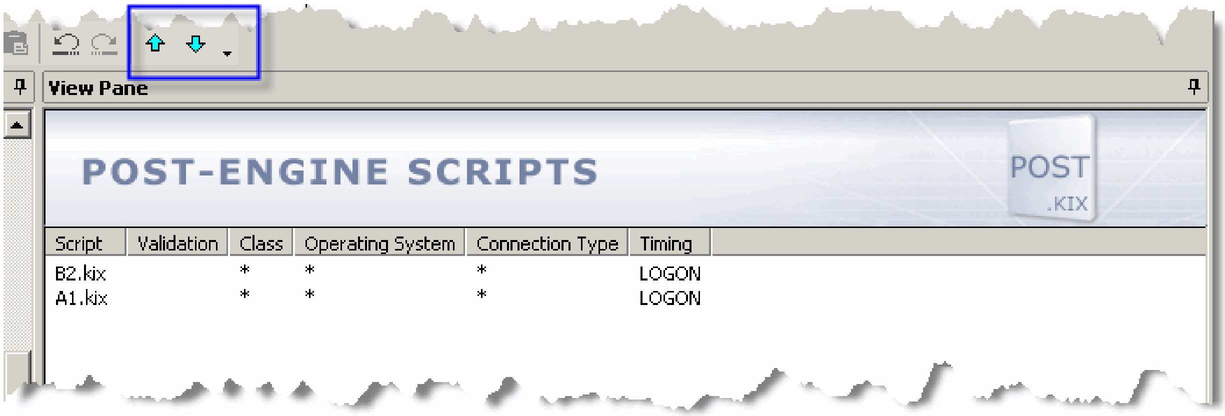
Custom scripts can be processed before and/or after the Desktop Authority object configurations are processed.

Pre-engine custom scripts are launched after the 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.

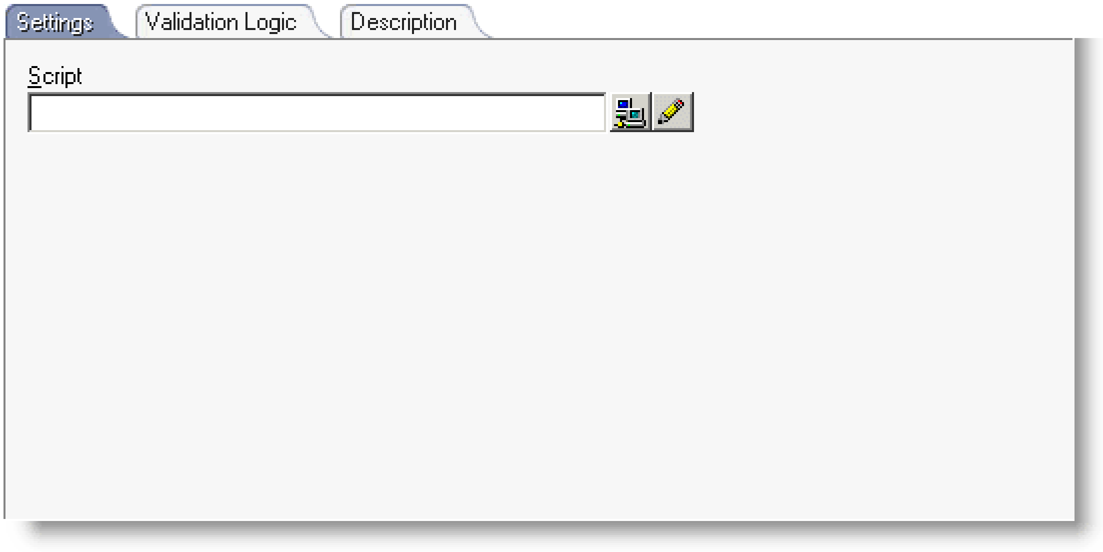
Script Execution

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 top of the list. Prioritize the list entries by clicking **Move Up (⇧)** and **Move Down (⇩)** to reorganize the list.



Script	Validation	Class	Operating System	Connection Type	Timing
B2.kix		*	*	*	LOGON
A1.kix		*	*	*	LOGON

Settings



Script

Enter the name of the custom script file. The script file name must have an extension of .KIX for the KiXtart engine to process it. Click to locate and select the script file from a network share. If the file does not already exist, Desktop Authority will let you write the script directly from this dialog box. Once a file name with a .KIX extension is entered into the script field the file may be edited. Click to edit it. Notepad is opened with the new or existing script loaded. If a new script is being created, some comments are automatically added to the file by Desktop Authority.

Dynamic variables, environment variables or macros may be used as part of the custom script filename. These variables are translated during the client logon process.

Example:

Script: $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.

There are not many rules about editing custom scripts, however, remember that each script must end with a RETURN statement so that control is returned to the Desktop Authority Engine when the script is finished processing.

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

A variety of custom scripting examples can be found on the ScriptLogic web site.

If you would rather develop custom scripts in VBscript, you can launch them using the Application Launcher tab.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

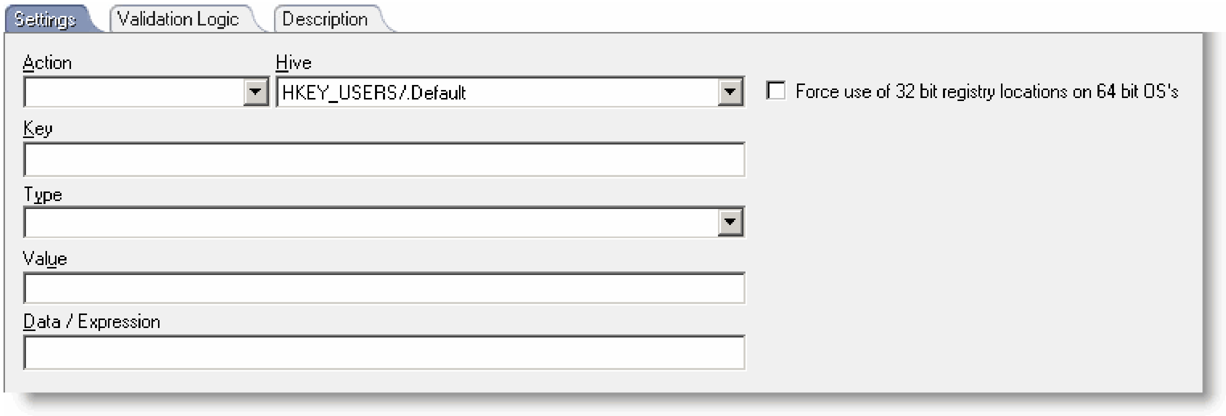
Description

Select the **Description** tab to set the description for this element.

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 ScriptLogic Service, which allows Desktop Authority to modify any Windows 2000/XP/2003/2008/Vista 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.

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.



Hive: HKEY_USERS/.Default

□ Force use of 32 bit registry locations on 64 bit OS's

Settings

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.
- Delete Key
  Remove the specified key from the hive. For safety reasons, DeleteKey will only delete a single key. DeleteKey will not delete a key if there are subkeys beneath it.
- *Add Key*
  Create a key in the specified hive.

Hive

Select the hive on which to perform the action from the list. The following hives can be selected:

- HKEY_CLASSES_ROOT
  Contains all file associations, OLE information and shortcut data.
- 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_USERS/.DEFAULT
  Contains default profile preferences.
- HKEY_CURRENT_CONFIG
  Represents the currently used computer hardware profile.

Force use of 32 bit registry locations of 64 bit OS's

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.

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
- REG_DWORD
- REG_DWORD_BIG_ENDIAN
- REG_DWORD_LITTLE_ENDIAN
- REG_EXPAND_SZ
- REG_FULL_RESOURCE_DESCRIPTOR
- REG_LINK
- REG_MULTI_SZ
- REG_NONE
- REG_QWORD
- 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*.

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, enter the word clear surrounded by parentheses.

Example:

```
(clear)
```

Validation Logic

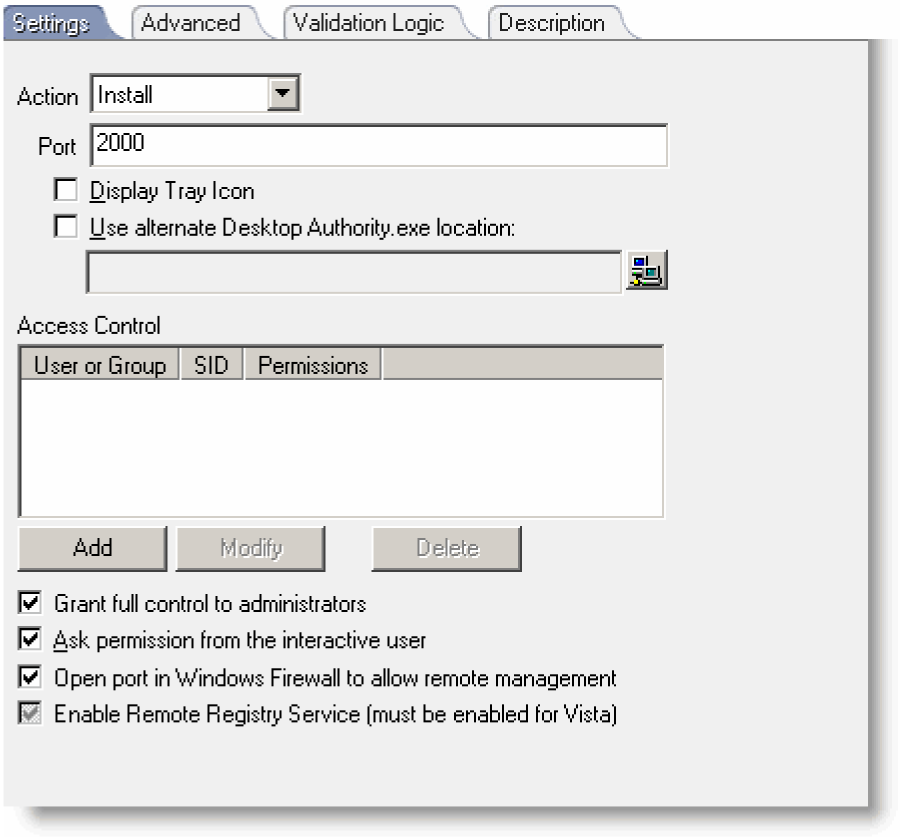
Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

REMOTE MANAGEMENT*

The **Remote Management** object provides the ability to install, configure or remove the Remote Management component to/from host computers.



Action: Install

Port: 2000

☐ Display Tray Icon

☐ Use alternate Desktop Authority.exe location:

Access Control

User or Group	SID	Permissions

☑ Grant full control to administrators

☑ Ask permission from the interactive user

☑ Open port in Windows Firewall to allow remote management

☑ Enable Remote Registry Service (must be enabled for Vista)

Settings

Action

Select an action from the list. Select *Install* to configure client workstations with the Desktop Authority host software. Select *Remove* from the list to remove the Desktop Authority host software from 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.

Use alternate DesktopAuthority.exe location

By default the Remote Management component is deployed to each validating client from the SLDACLIENT$ share. SLDACLIENT$ is a share that exists on the Operations Master (where Desktop Authority is installed to). The folder ScriptLogic Manager\DesktopAuthority is shared as SLDACLIENT. This default location can be changed to an alternate path to accommodate clients located over slow WAN links. Specify the new path and copy the contents of the Desktop Authority folder to this new path. Click to select an existing path.

Note: The specified alternate location is not updated when newer versions of Desktop Authority are installed. It must manually be updated by copying the updated files from the SLDACLIENT$ share into the alternate location upon completion of the installation.

Access Control

The Access Control List allows permissions to be controlled for Remote Management sessions.

Configure Credentials for 2000/XP machines

Specify a valid User or Group to grant Remote Management permissions to.

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.

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.

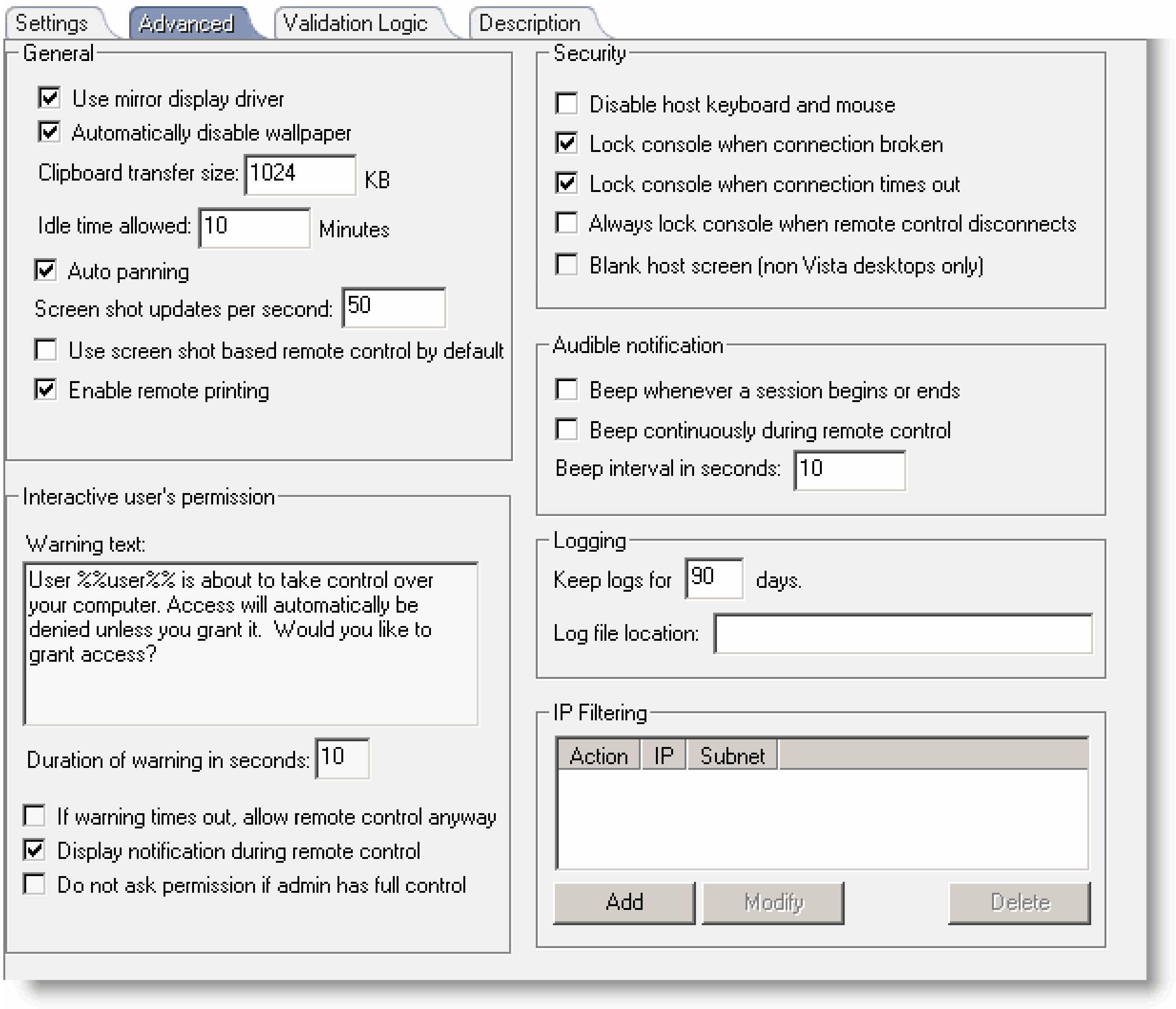
Enable Remote Registry Service (must be enabled for Vista)

Select this box, ☑, to turn on the Remote Registry service on desktops. This is required for use of Remote Management on Vista clients as the service is turned off by default. Turning on this service enables the Desktop Authority Manager to determine the status of the DA Remote Management service.

Select this box to set the Remote Registry service startup type to automatic and the service is started. Clear this box, □, to set the Remote Registry service startup type to manual and the service is stopped. Gray the check box, ☑, to leave the startup type and service status as is.

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
☑ Automatically disable wallpaper
Clipboard transfer size: 1024 KB
Idle time allowed: 10 Minutes
☑ Auto panning
Screen shot updates per second: 50
□ Use screen shot based remote control by default
☑ Enable remote printing

Interactive user's permission

Warning text:
User %%user%% is about to take control over your computer. Access will automatically be denied unless you grant it. Would you like to grant access?

Duration of warning in seconds: 10
□ If warning times out, allow remote control anyway
☑ Display notification during remote control
□ Do not ask permission if admin has full control

Security

□ Disable host keyboard and mouse
☑ Lock console when connection broken
☑ Lock console when connection times out
□ Always lock console when remote control disconnects
□ Blank host screen (non Vista desktops only)

Audible notification

□ Beep whenever a session begins or ends
□ Beep continuously during remote control
Beep interval in seconds: 10

Logging

Keep logs for 90 days.
Log file location:

IP Filtering

Action	IP	Subnet

General

Use mirror display driver

Desktop Authority provides a mirror display driver on the W2K/XP 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 (non Vista desktops only)

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.

Type

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.

Address/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.

Description

Select the **Description** tab to set the description for this element.

For details on the use of the Remote Management component, following deployment to client workstations, see the Remote Control Manager document available for download from the ScriptLogic web site.

*This feature is not a standard part of Desktop Authority Express. To obtain this feature, Desktop Authority Express must be upgraded to the full version of Desktop Authority.

SECURITY POLICIES

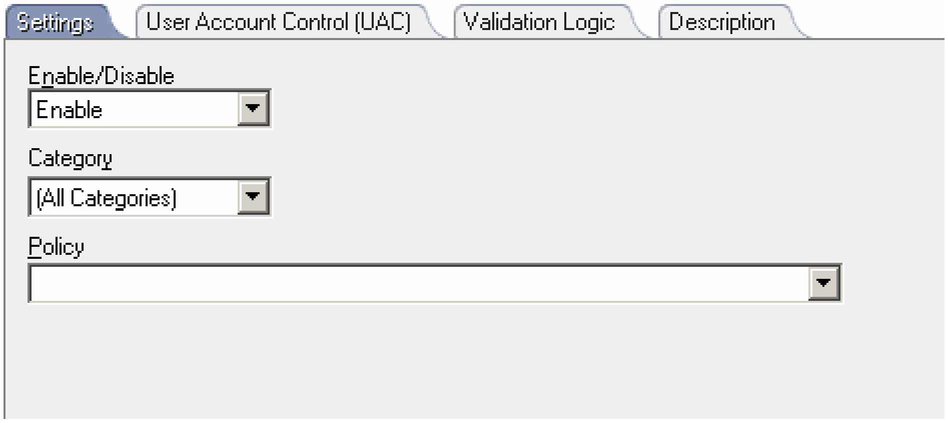
The Security **Policies** object allows user security settings to be centrally configured. Security policies can be set for individual users or computers.

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 2000/XP/2003/2008/Vista 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.



Enable/Disable: Enable

Category: (All Categories)

Policy:

Settings

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), Active Desktop, Computer, Explorer, Internet Explorer, Network, System and WinOldApp. (All Policies) will display policies for all categories. WinOldApp provides policy settings for MS-DOS apps.

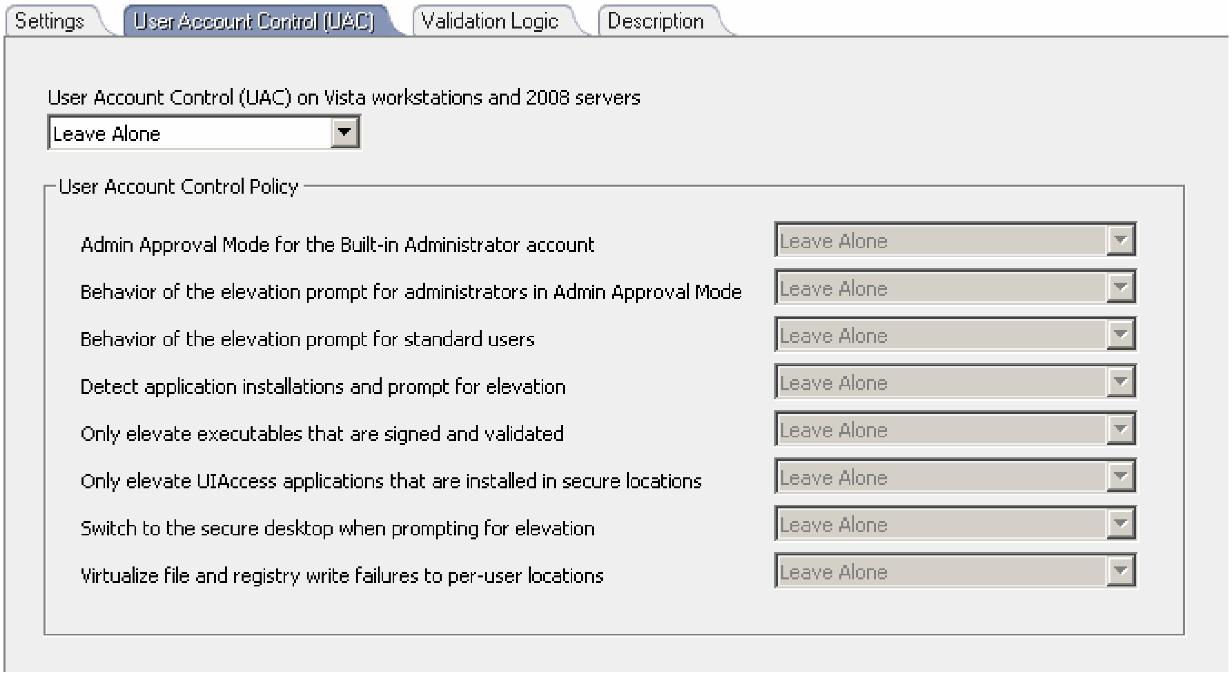
Selecting a policy category will filter the policy selection list below the category.

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 Microsoft Windows Vista and 2008**.**



User Account Control (UAC) on Vista workstations and 2008 servers: Leave Alone

User Account Control Policy

Admin Approval Mode for the Built-in Administrator account	Leave Alone
Behavior of the elevation prompt for administrators in Admin Approval Mode	Leave Alone
Behavior of the elevation prompt for standard users	Leave Alone
Detect application installations and prompt for elevation	Leave Alone
Only elevate executables that are signed and validated	Leave Alone
Only elevate UIAccess applications that are installed in secure locations	Leave Alone
Switch to the secure desktop when prompting for elevation	Leave Alone
Virtualize file and registry write failures to per-user locations	Leave Alone

User Account Control (UAC) on Vista and 2008 servers

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 Vista and Windows 2008 servers.

UAC changes on Windows Server 2008 machines requires 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 Policy

All individual UAC security policy settings are disabled for individualized configuration unless the User Account Control (UAC) on Vista and 2008 servers selection is enabled.

Admin Approval Mode for the Built-in Administrator account

By default the Built-in Administrator account will run all applications on a Windows Vista workstation 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.

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.

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

Select the Leave Alone option to preserve the system's current setting, which by default is Prompt for Consent.

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 UIAccess 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 users 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 users desktop. Select Leave Alone to preserve the system's current settings. By default, this setting is Enabled on Windows Vista workstations.

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. By default, this setting is Enabled on Windows Vista workstations.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

SERVICE PACK DEPLOYMENT

The **Service Pack Deployment** object allows you to deploy service packs for all 2000/XP/Vista clients. User Management Service Pack Deployment does not support 64-bit operating systems.

A few items to note regarding service pack deployment:

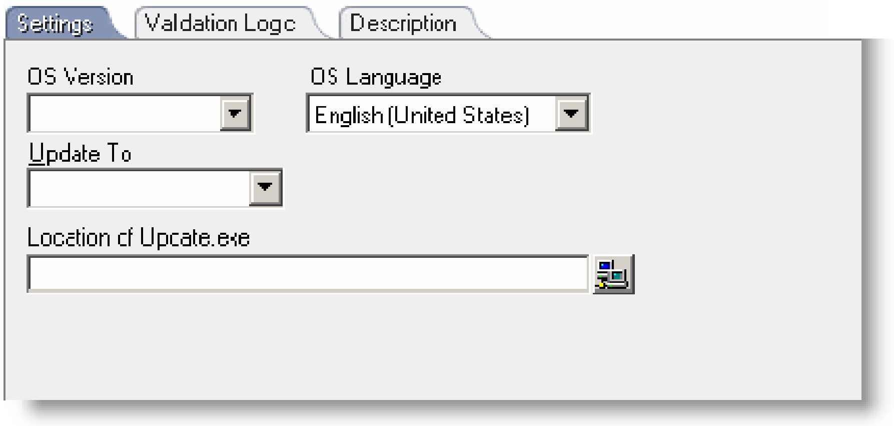
- User Management Service Pack Deployment will only install service packs to 2000/XP/Vista clients if connected over a LAN connection. The Connection validation logic is disabled.
- User Management Service Pack Deployment will never downgrade the currently installed service pack on a computer. Desktop Authority will only install the requested service pack if the client has an older or no service pack installed.
- 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, 1.5G (1500mb) 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"
  ```
- 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.
- User Management Service Pack Deployment will not install service packs on any Windows Embedded operating system.
- User Management Service Pack Deployment will not install any service packs to a server.
- 64-bit service packs are not supported in the User Management Service Pack Deployment object.

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.



OS Language: English (United States)

Settings

OS Version

Select a client Operating System version from the list. Valid selections are Windows 2000, Windows Vista and Windows XP. 64-bit service packs are not supported in User Management Service Pack Deployment object.

OS 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 Update.exe

Enter the complete path and filename where the Update.exe executable exists or click to locate the executable's path.

Windows Vista uses spinstall.exe, not update.exe for the service pack install executable.

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*.

Validation Logic

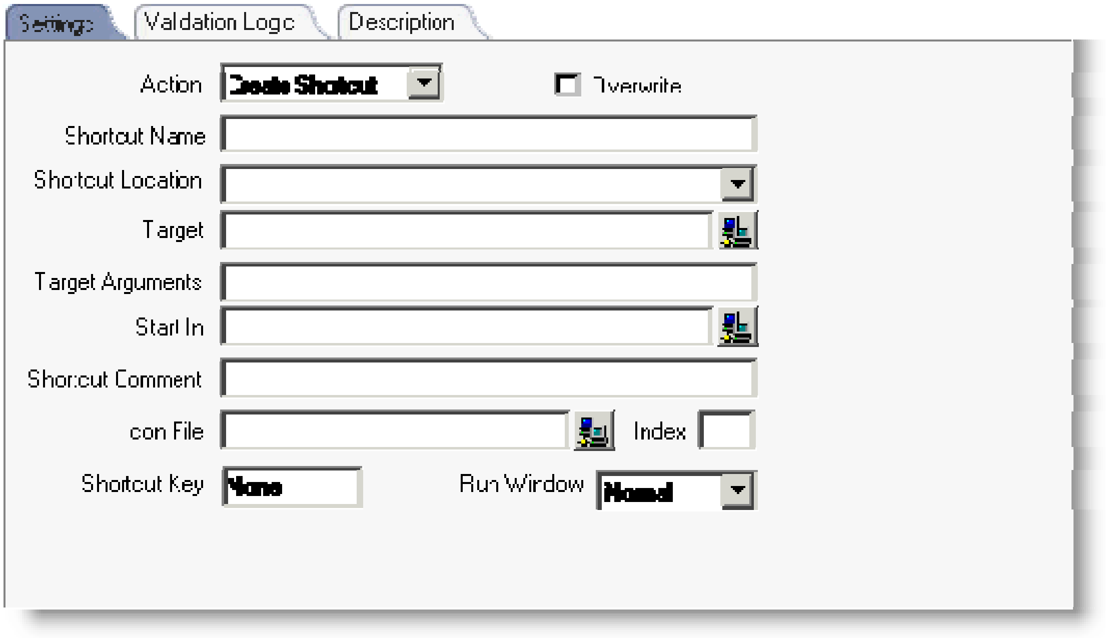
Select the **Validation Logic** tab to set the validation rules for this element. Service Packs may only be applied to computers classified as a Desktop or Portable. Operating System and Connection type are disabled.

Description

Select the **Description** tab to set the description for this element.

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.



Action: Create Shortcut

□ Overwrite

Shortcut Key: None

Run Window: Normal

Settings

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.

Shortcut Name

Enter a name for the shortcut. This name will appear below the icon for the shortcut. This field is required.

Shortcut Location

Specify the folder where the shortcut will be created or removed from. Type a location or select one from the list.

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.

Target

Sif it exists in a shared folder. This field is required. pecify the program or folder location that the shortcut will point to. The target program may be located by clicking

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 . In most cases this field will contain the path used in the Target field. This field is required.

Shortcut 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 **Index** entry. An icon file may be selected by clicking .

Shortcut 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 Window*, *Minimized Window*, *or Maximized Window*.

Validation Logic

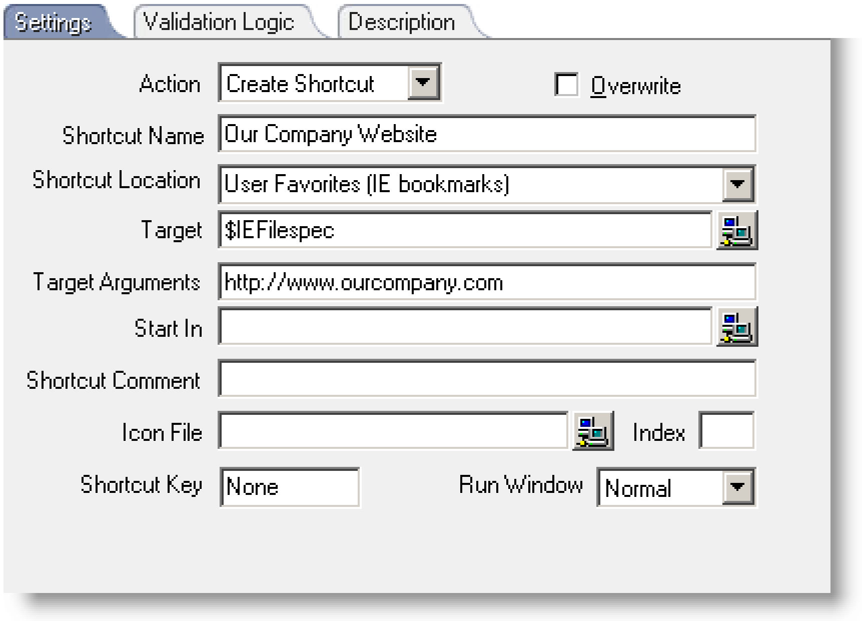
Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

Example

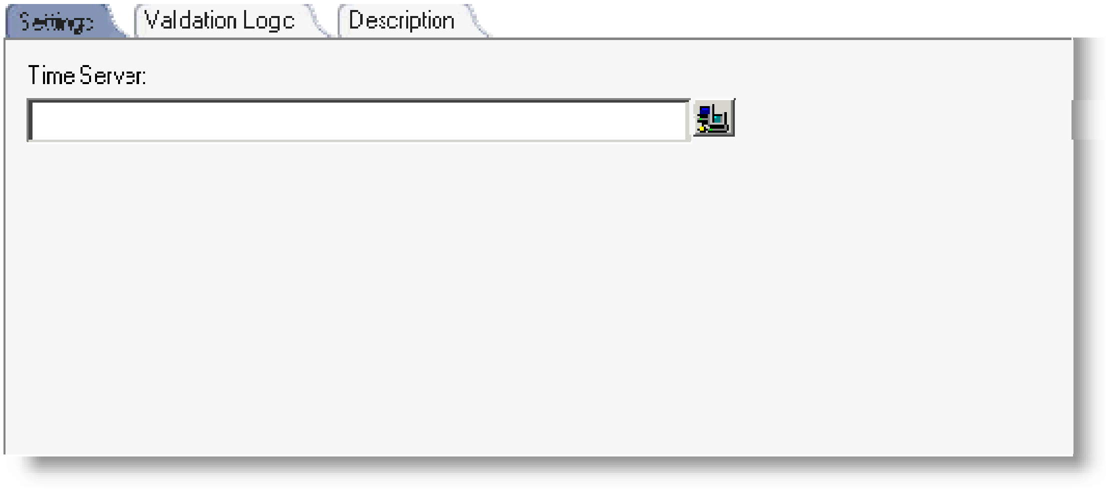
One way to make use of shortcuts is to create a shortcut in your user's Internet Explorer Favorites. This example demonstrates how to create the Favorites shortcut.



Action	Create Shortcut
☐ Overwrite	
Shortcut Name	Our Company Website
Shortcut Location	User Favorites (IE bookmarks)
Target	$IEFilespec
Target Arguments	http://www.ourcompany.com
Start In	
Shortcut Comment	
Icon File	
Index	
Shortcut Key	None
Run Window	Normal

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

Time Server

Enter the name of the Time Server which the client will by synchronized with. Type the server name or click to locate and select a server.

Validation Logic

Select the **Validation Logic** tab to set the validation rules for this element.

Description

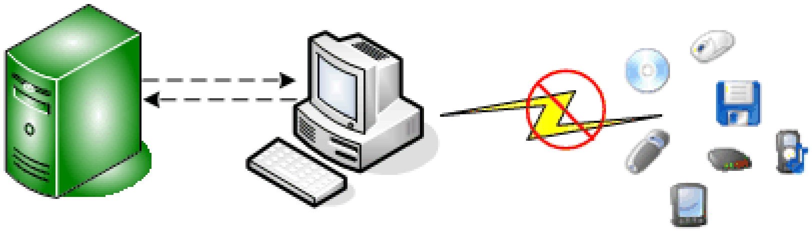
Select the **Description** tab to set the description for this element.

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.

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, WiFi, Ethernet, IDE, SCSI, PCMCIA, IoMega, Blackberry, Pocket PC devices, Pocket OS devices, Hard disk, DVD, CD ROM, Floppy Disk, Network Adapter, Modem, Plug and Play Storage, Flash Memory, PDA, USB Printers, USB Scanners and MP3 Player devices. 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\ScriptLogic\PortSecurity\EmbargoDeviceClasses.xml file on each desktop

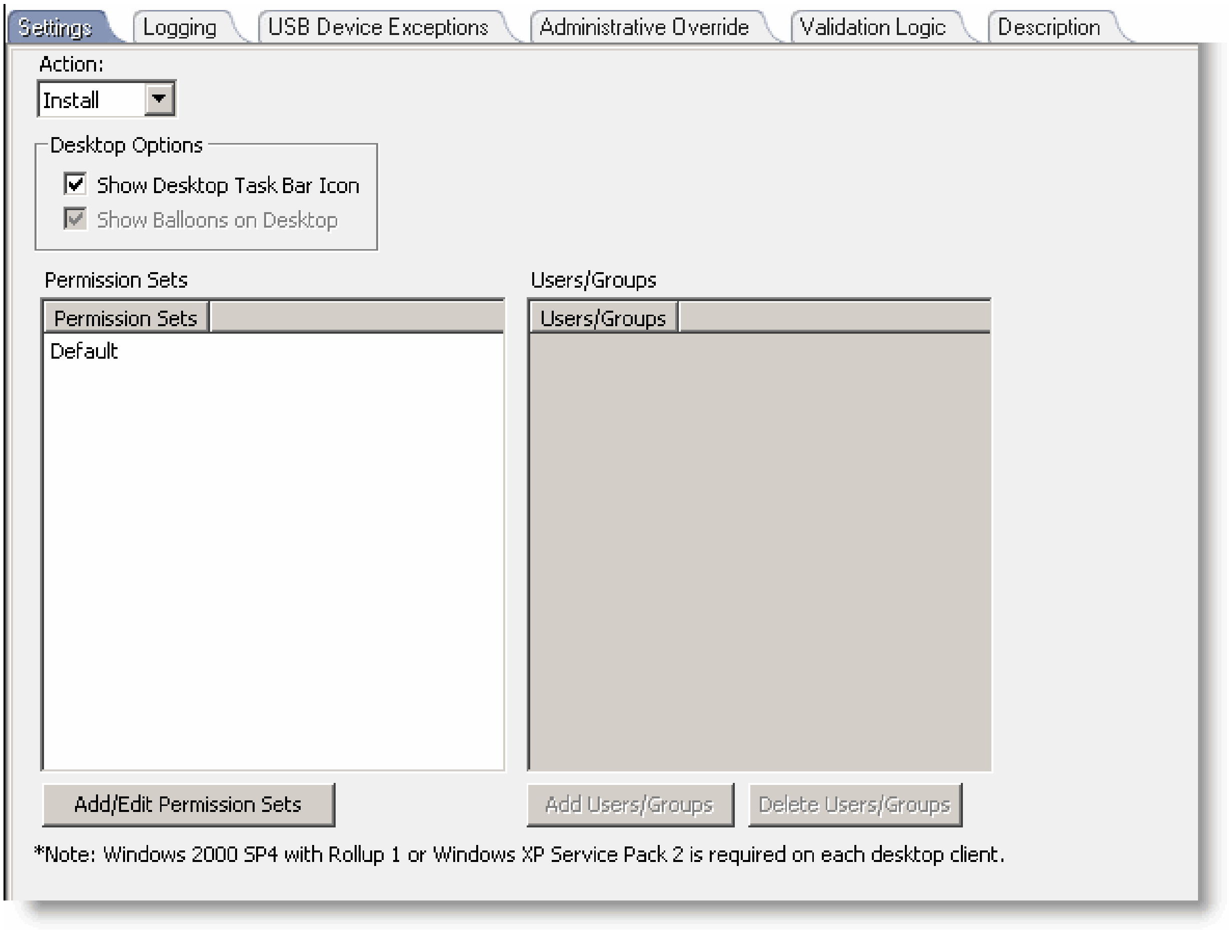
** Does not include partitions containing virtual memory, boot files or Windows system files

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.



Action: Install

Desktop Options

☑ Show Desktop Task Bar Icon

☑ Show Balloons on Desktop

Permission Sets: Default

*Note: Windows 2000 SP4 with Rollup 1 or Windows XP Service Pack 2 is required on each desktop client.

Note: USB/Port Security configurations require clients to be running Update Rollup 1 for Windows 2000 SP4 or Windows XP SP2 clients.

Settings

Action

Select Install or Remove from the Action list. 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.

Desktop Options

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.

Permission Sets

The Permission Sets list shows all of the sets of rules which have been configured for certain removable storage devices.

Add/Edit Permission Sets

Click **Edit Permission Sets** to define a rule that authorizes certain removable storage devices and allows specific type of access to them.

Users/Groups

The Users/Groups list shows the Users and/or Groups that have been authorized for the selected Permission set.

Add Users/Groups

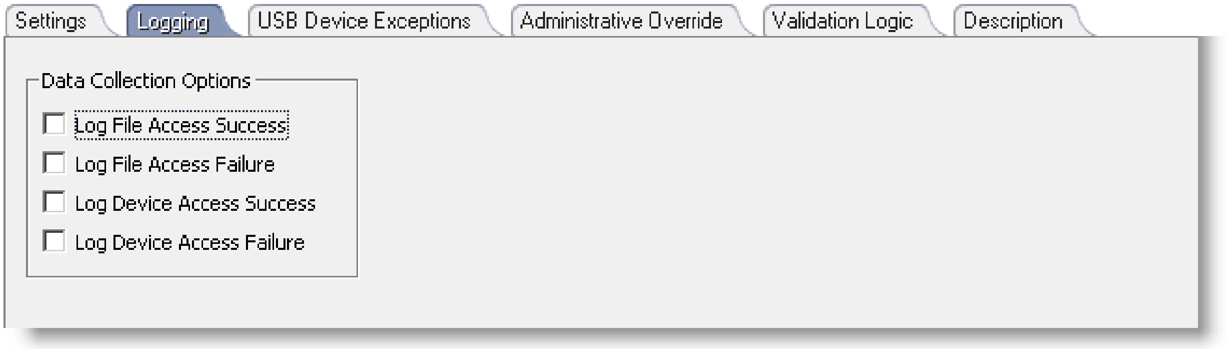
Click **Add Users/Groups** to add Users and/or Groups to the selected Permission set. A Permission set must be created before any users and/or groups can be assigned to it.

Delete Users/Groups

Click **Delete Users/Groups** to remove the set of Users and/or Groups from 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

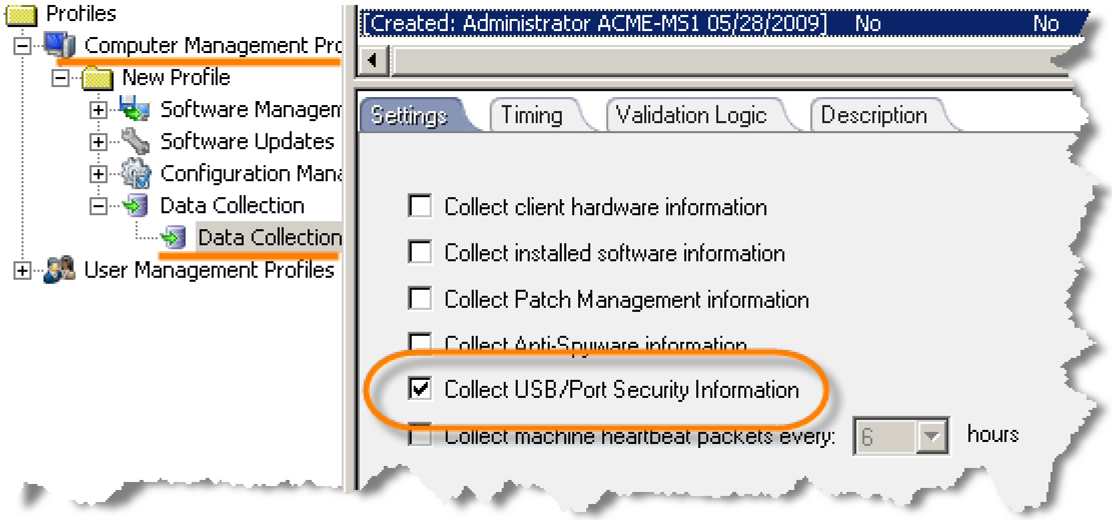
☐ Log File Access Success

☐ Log File Access Failure

☐ Log Device Access Success

☐ Log Device Access Failure

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.



☐ Collect client hardware information

☐ Collect installed software information

☐ Collect Patch Management information

☐ Collect Anti-Spyware information

☑ Collect USB/Port Security Information

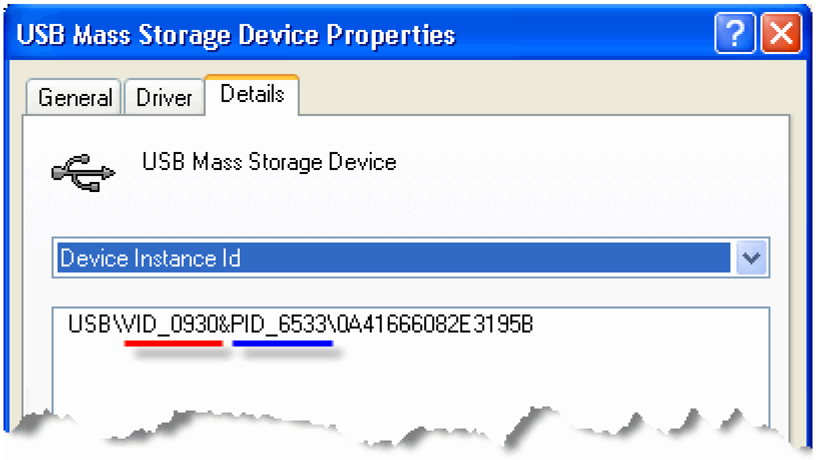
☐ Collect machine heartbeat packets every: 6 hours

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

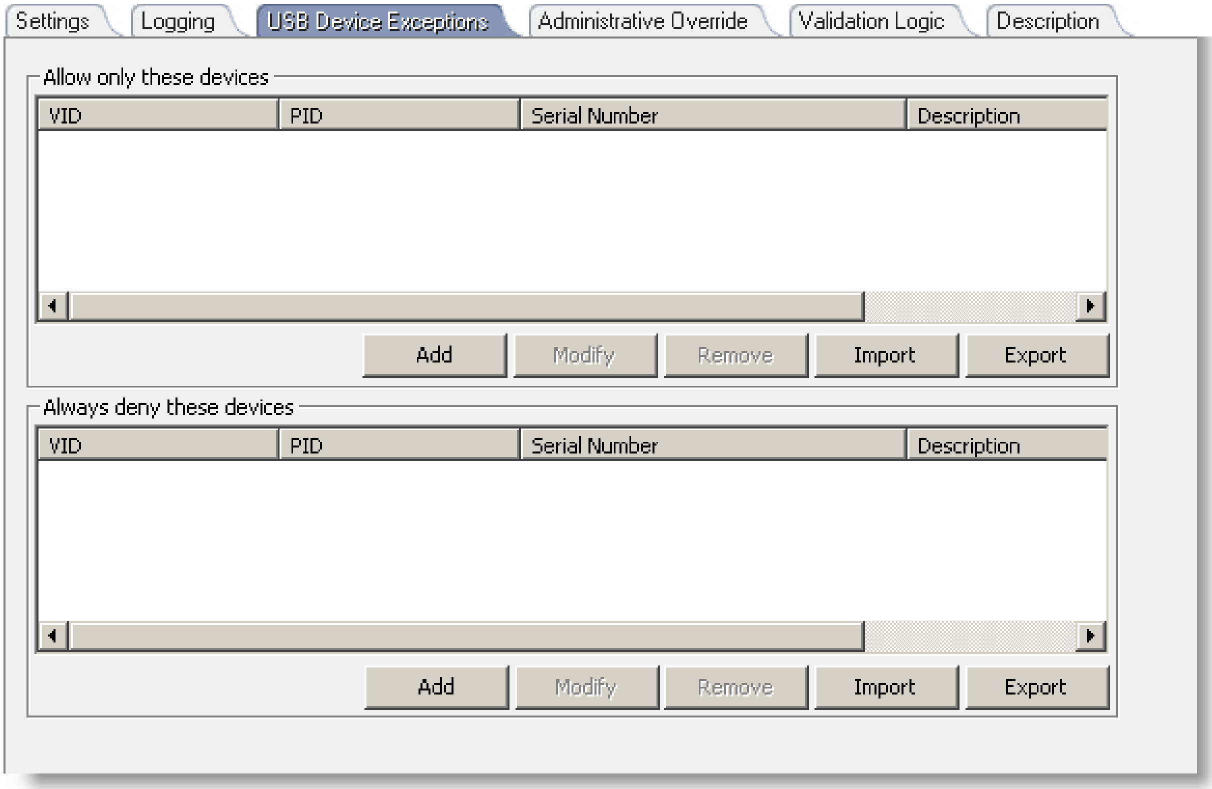
To look up the VID and PID of a device, go to the Device Manager. Locate the device in the list of components. Right-click on it and choose Properties. From the Properties dialog, select the Details tab.



Device Instance Id

USB\VID_0930&PID_6533\0A41666082E3195B

The VID and PID identifiers can be found within the Device Instance Id as shown above.



Allow only these devices

VID	PID	Serial Number	Description

Always deny these devices

VID	PID	Serial Number	Description

Allow only these devices

This list contains all devices that are allowed in the Enterprise's environment. Click **Add** to add a device to the list. When adding a device to the list the VID and PID numbers are required. The serial number of the device and description is optional. Click **Modify** to change the PID, VID, Serial number and/or description. Click **Remove** to delete the device from the list.

Devices can also be listed in a Comma-Separated file (CSV) with the VID,PID,Serial Number,Description. Click **Import** to read the file into the list.

Click **Export** to write the devices in the list to a Comma-Separated file (CSV).

Always deny these devices

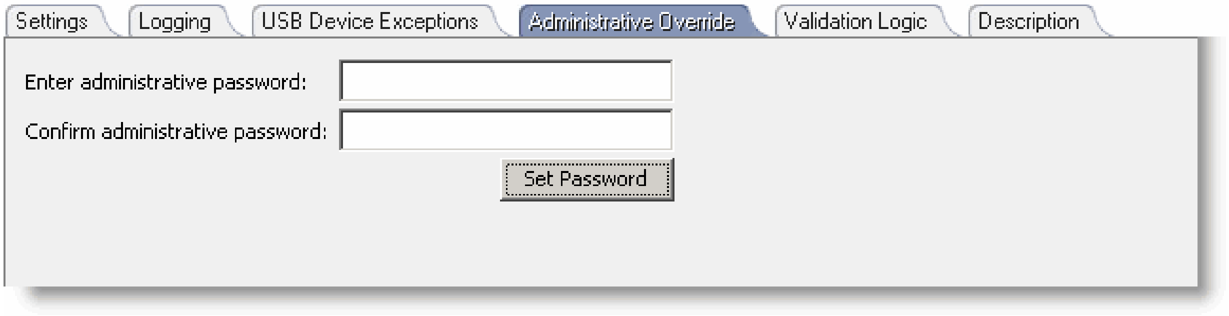
This list contains all devices that are prohibited from being used in the Enterprise's environment. Click **Add** to add a device to the list. When adding a device to the list the VID and PID numbers are required. The serial number of the device and description is optional. Click **Modify** to change the PID, VID, Serial number and/or description. Click **Remove** to delete the device from the list.

Devices can also be listed in a Comma-Separated file (CSV) with the VID,PID,Serial Number,Description. Click **Import** to read the file into the list.

Click **Export** to write the devices in the list to a Comma-Separated file (CSV).

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.



Enter an administrative password on this dialog. 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.

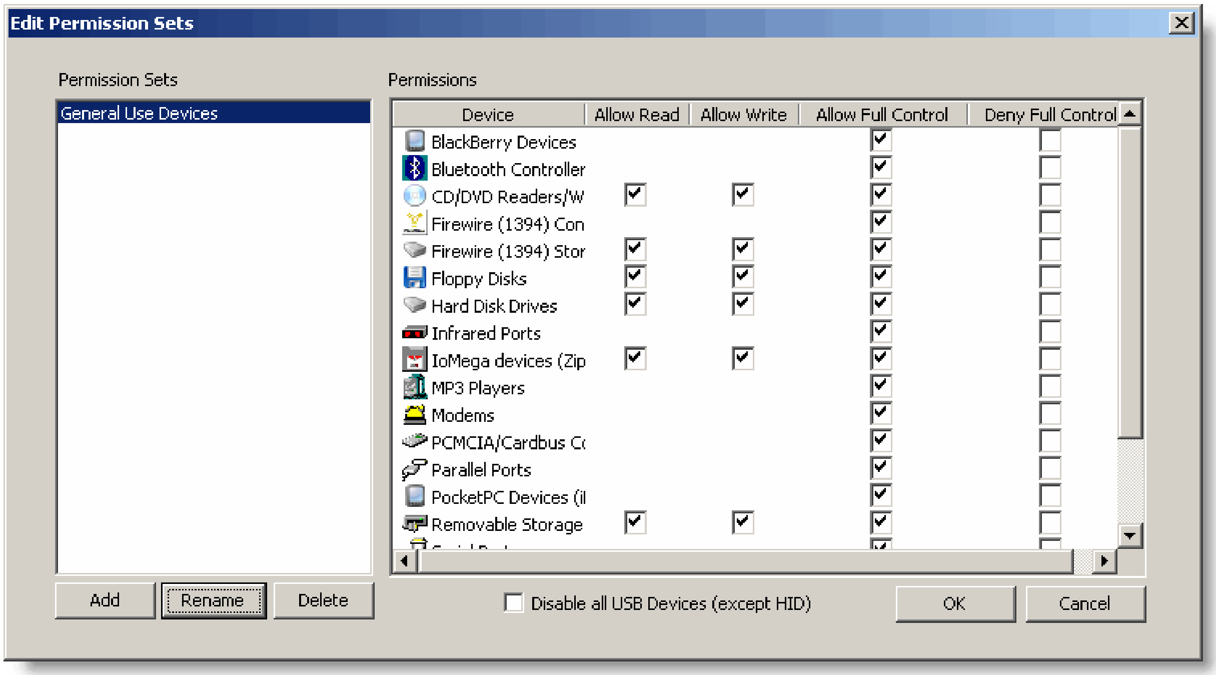
Description

Select the **Description** tab to set the description for this element.

*This feature is not a standard part of Desktop Authority Express. To obtain this feature, Desktop Authority Express must be upgraded to the full version of Desktop Authority.

USB/Port Security - Edit Permission Sets

The Edit Permission Sets dialog is where the USB/Port Security permission sets are created and maintained. 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 Allow Read, Allow Write, Allow Full Control and Deny Full Control.



Permission Sets: General Use Devices

Device	Allow Read	Allow Write	Allow Full Control	Deny Full Control
BlackBerry Devices			☑	□
Bluetooth Controller			☑	□
CD/DVD Readers/W	☑	☑	☑	□
Firewire (1394) Con			☑	□
Firewire (1394) Stor	☑	☑	☑	□
Floppy Disks	☑	☑	☑	□
Hard Disk Drives	☑	☑	☑	□
Infrared Ports			☑	□
IoMega devices (Zip	☑	☑	☑	□
MP3 Players			☑	□
Modems			☑	□
PCMCIA/Cardbus C(			☑	□
Parallel Ports			☑	□
PocketPC Devices (il			☑	□
Removable Storage	☑	☑	☑	□

□ Disable all USB Devices (except HID)

Add

Click **Add** to create a new Permission Set. By default, all devices in the permission set are given Full Control permissions.

Rename

Click **Rename** to modify the name of the selected permission set.

Delete

Click **Delete** to remove an existing permission set.

Disable all USB Devices (except HID)

Select this box to Deny access to all USB devices except HIDs (Human Interface Devices) such as keyboard and mouse devices.

OK

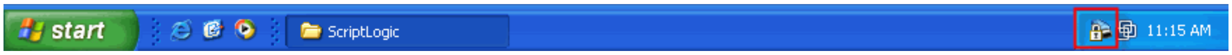
Click **OK** to save all permission set changes and return to the USB/Port Security object.

Cancel

Click **Cancel** to undo all permission changes and return to the USB/Port Security object.

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.



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.

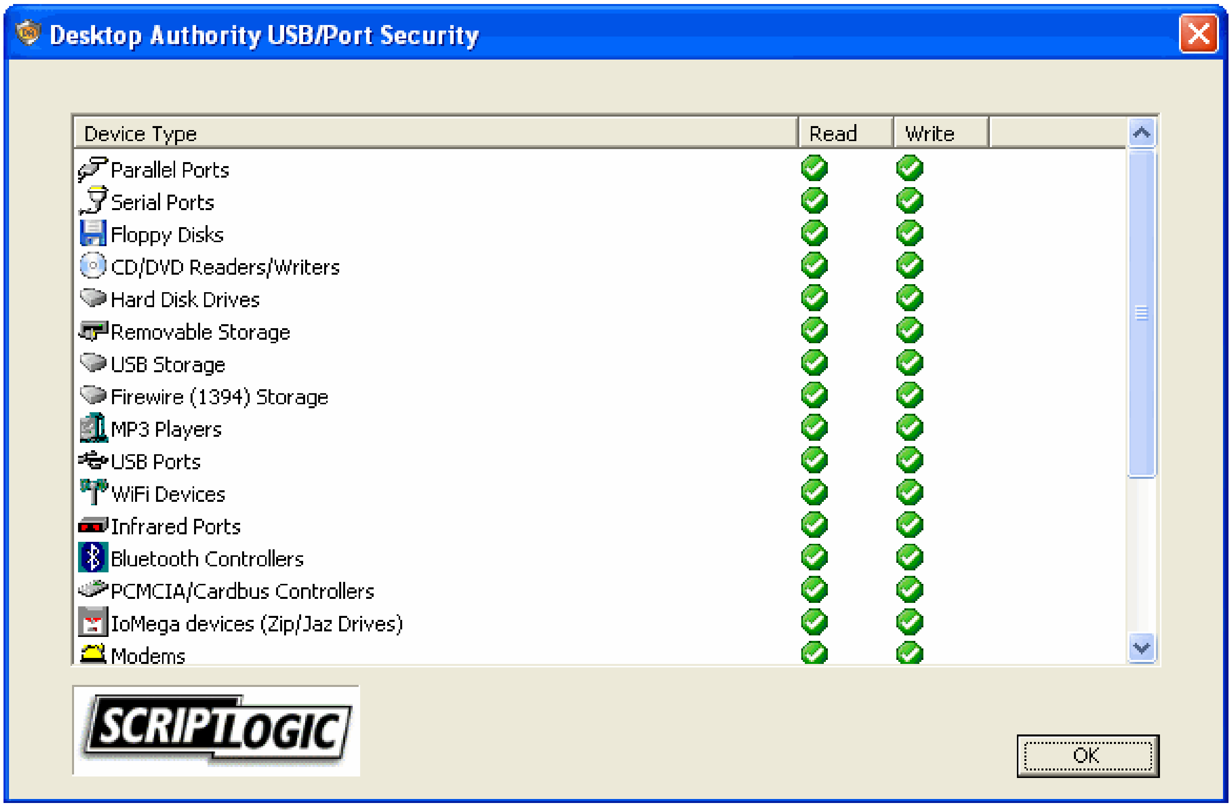
Disable Restrictions

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.

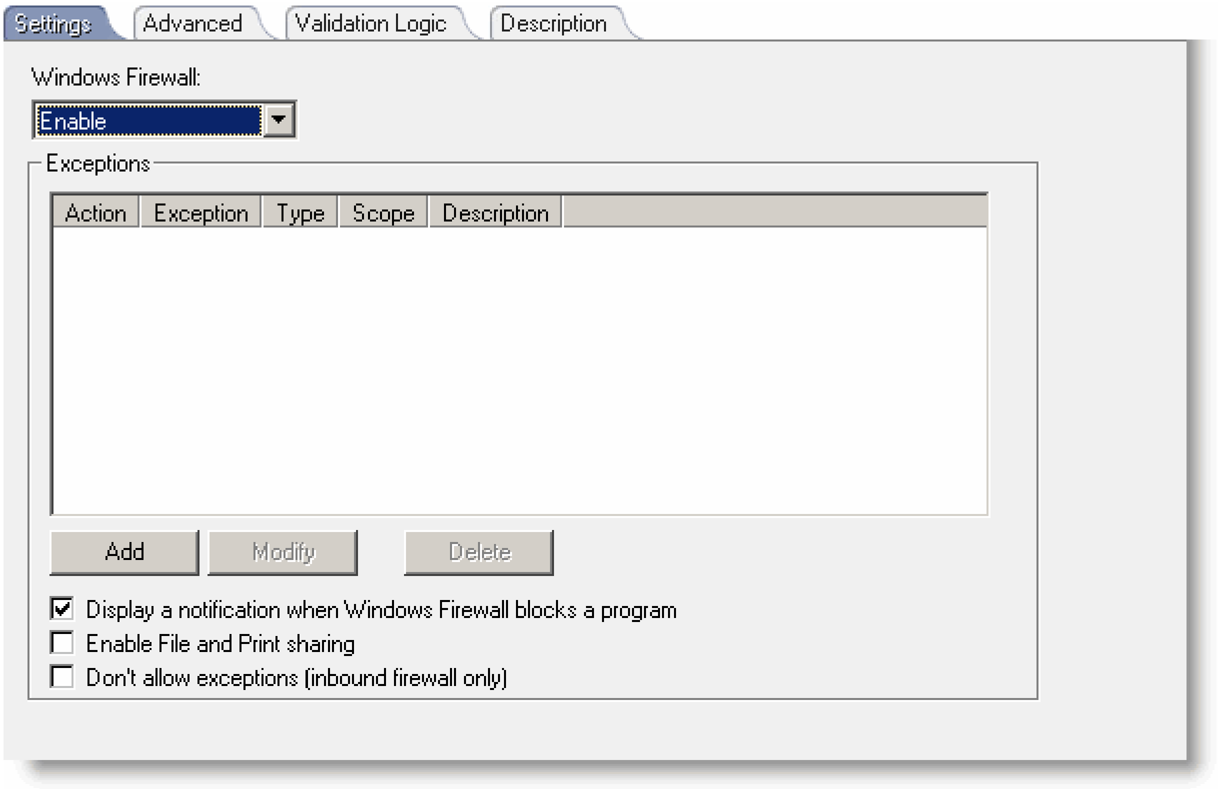


Desktop Authority USB/Port Security

Device Type	Read	Write
Parallel Ports	✓	✓
Serial Ports	✓	✓
Floppy Disks	✓	✓
CD/DVD Readers/Writers	✓	✓
Hard Disk Drives	✓	✓
Removable Storage	✓	✓
USB Storage	✓	✓
Firewire (1394) Storage	✓	✓
MP3 Players	✓	✓
USB Ports	✓	✓
WiFi Devices	✓	✓
Infrared Ports	✓	✓
Bluetooth Controllers	✓	✓
PCMCIA/Cardbus Controllers	✓	✓
IoMega devices (Zip/Jaz Drives)	✓	✓
Modems	✓	✓

WINDOWS FIREWALL

The **Windows Firewall** object allows Microsoft's Windows Firewall to be enabled or disabled on any validated computer having the Windows XP 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 SP2 or greater.



Windows Firewall: Enable

Exceptions

Action	Exception	Type	Scope	Description

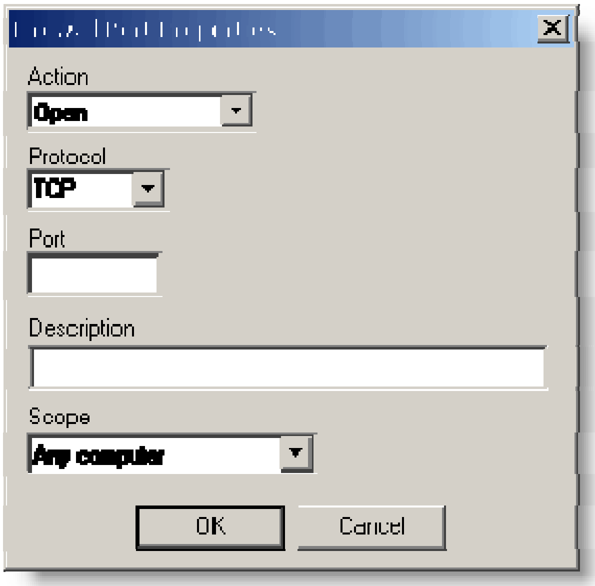
☑ Display a notification when Windows Firewall blocks a program
□ Enable File and Print sharing
□ Don't allow exceptions (inbound firewall only)

Settings

Windows Firewall

Select an action (Enable/Disable) from the Windows Firewall list to configure the Windows Firewall component.

The Exceptions list is a holding place for all Firewall port and program exceptions. Click **Add** to add a new port or program to the Exception list. Click **Modify** to edit an existing port or program on the list. Click **Delete** to remove a configured port or program from the Exception list.



Action: Open

Protocol: TCP

Port

Description

Scope: Any computer

Action

Select *Open* or *Close* from the Action list. This will configure the specified port to be opened or closed for incoming traffic.

Exception Type

Select *TCP*, *UDP* or *Program* from the Protocol list to specify the type of port or program to be configured.

Port

When the Exception Type is set to TCP or UDP, type the port number to be opened or closed.

Image Path

When the Exception Type is set to Program, specify the path to the executable program.

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.

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.

ICMP

Select the ICMP tab to configure settings for Windows Firewall ICMP (Internet Control Message Protocol). This tab allows specific types of ICMP messages to be enabled or disabled

Validation Logic

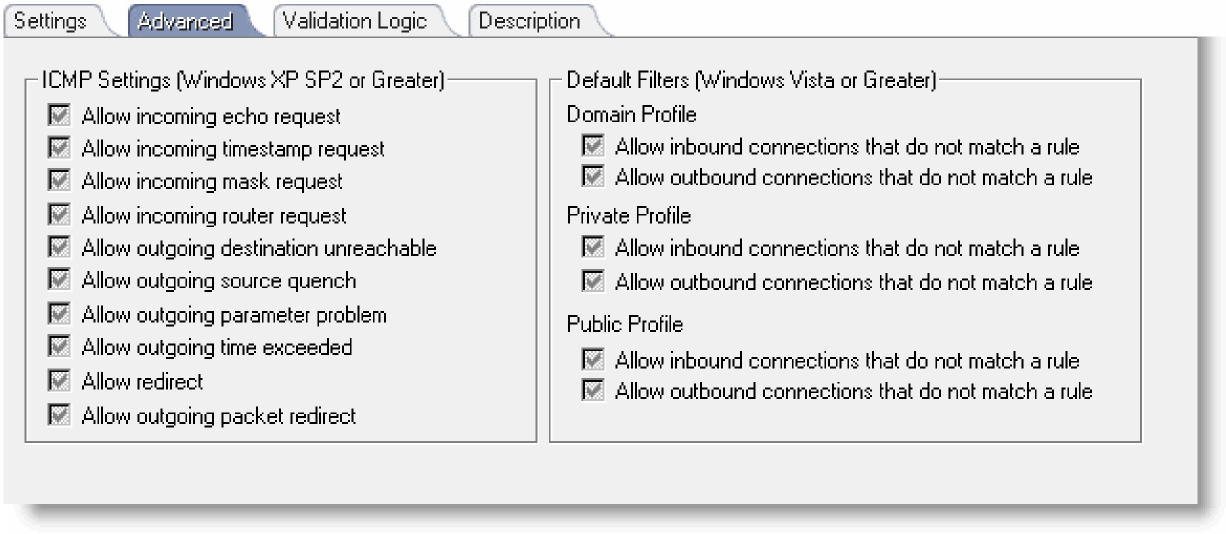
Select the **Validation Logic** tab to set the validation rules for this element.

Description

Select the **Description** tab to set the description for this element.

Windows Firewall ICMP

The Windows Firewall ICMP (Internet Control Message Protocol) 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.



ICMP Settings (Windows XP SP2 or Greater)

- ▣ Allow incoming echo request
- ▣ Allow incoming timestamp request
- ▣ Allow incoming mask request
- ▣ Allow incoming router request
- ▣ Allow outgoing destination unreachable
- ▣ Allow outgoing source quench
- ▣ Allow outgoing parameter problem
- ▣ Allow outgoing time exceeded
- ▣ Allow redirect
- ▣ Allow outgoing packet redirect

Default Filters (Windows Vista or Greater)

Domain Profile

- ▣ Allow inbound connections that do not match a rule
- ▣ Allow outbound connections that do not match a rule

Private Profile

- ▣ Allow inbound connections that do not match a rule
- ▣ Allow outbound connections that do not match a rule

Public Profile

- ▣ Allow inbound connections that do not match a rule
- ▣ Allow outbound connections that do not match a rule

ICMP Settings (Windows XP SP2 or greater)

Allow incoming echo request

This check box can be set to one of three (3) different states: on (enabled) ☑, off (disabled) □, or grayed (preserve client setting) ▣.

Select this request type to force any messages sent to this computer to be repeated back to the sender. Clear this box to not allow incoming echo requests. Gray the check box to leave the client’s setting untouched.

The default for this option is grayed.

Allow incoming timestamp request

This check box can be set to one of three (3) different states: on (enabled) ☑, off (disabled) □, or grayed (preserve client setting) ▣.

Select this request type to send an acknowledgement message (containing the time the data was received) back to the sender. Clear this box to not allow incoming timestamp requests. Gray the check box to leave the client’s setting untouched.

The default for this option is grayed.

Allow incoming mask request

This check box can be set to one of three (3) different states: on (enabled) ☑, off (disabled) □, or grayed (preserve client setting) ☑.

Select this request type to enable the computer to listen for and respond to requests for more information about the network to which it is connected to. Clear this box to not allow incoming mask requests. Gray the check box to leave the client’s setting untouched.

The default for this option is grayed.

Allow incoming router request

This check box can be set to one of three (3) different states: on (enabled) ☑, off (disabled) □, or grayed (preserve client setting) ☑.

Select this request type for the computer to respond to requests for information about the routes it recognizes. Clear this box to not allow incoming router requests. Gray the check box to leave the client’s setting untouched.

The default for this option is grayed.

Allow outgoing destination unreachable

This check box can be set to one of three (3) different states: on (enabled) ☑, off (disabled) □, or grayed (preserve client setting) ☑.

Select this request type to discard and acknowledge that sent data failed to reach the computer. Clear this box to not allow outgoing destination unreachable acknowledgements. Gray the check box to leave the client’s setting untouched.

The default for this option is grayed.

Allow outgoing source quench

This check box can be set to one of three (3) different states: on (enabled) ☑, off (disabled) □, or grayed (preserve client setting) ☑.

If the computers ability to process incoming data cannot keep up with the data coming in, excess data will be dropped and a request will be sent to the sender to transmit the data at a slower pace. Select this box to allow the computer to transmit slower. Clear this box to not allow the computer to quench outgoing data. Gray the check box to leave the client’s setting untouched.

The default for this option is grayed.

Allow outgoing parameter problem

This check box can be set to one of three (3) different states: on (enabled) ☑, off (disabled) □, or grayed (preserve client setting) ☑.

If the computer receives bad header data, a reply will be sent with a "bad header" error message. Clear the box to not allow an outgoing error replies. Gray the check box to leave the client’s setting untouched.

The default for this option is grayed.

Allow outgoing time exceeded

This check box can be set to one of three (3) different states: on (enabled) ☑, off (disabled) □, or grayed (preserve client setting) ☑.

If the computer discards data due to a timing issue, a reply will be sent with a "time expired" error message. Select this box to allow the outgoing error message. Clear this box to not allow an outgoing "time expired" error message. Gray the check box to leave the client’s setting untouched.

The default for this option is grayed.

Allow redirect

This check box can be set to one of three (3) different states: on (enabled) ☑, off (disabled) □, or grayed (preserve client setting) ☑.

Data sent from this computer will be rerouted if the default path changes. Select this box to allow the data to be rerouted. Clear the box to disallow the data route to be changed. Gray the check box to leave the client’s setting untouched.

The default for this option is grayed.

Allow outgoing packet redirect

This check box can be set to one of three (3) different states: on (enabled) ☑, off (disabled) □, or grayed (preserve client setting) ☑.

When received data blocks are too big for this computer to forward, a reply will be sent with a "packet too big" error message. Select this box to allow the error message to be sent. Clear the box to not allow the error message to be sent. Gray the check box to leave the client’s setting untouched.

The default for this option is grayed.

Default Filters (Windows Vista or greater)

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.

REFERENCE

DESKTOP AUTHORITY VERSIONS

Desktop Authority is available in three versions, Desktop Authority, Desktop Authority Express and Desktop Authority for Configuration Manager. Desktop Authority Express is a scaled down version of Desktop Authority. It does not include the following standard features included by default in the full version -- Patch Management, Software Management, Anti-Spyware, USB/Port Security, Hardware and Software Inventory and Custom Reporting and the Desktop Authority Remote Management tool.

Desktop Authority for Configuration Manager is a version of Desktop Authority that is geared towards enterprises who already use Microsoft's System Center Configuration Manager (SCCM) or other similar management tools. Since SCCM provides tools for Software Distribution and Asset Management, Desktop Authority does not include its own built-in Software Distribution or Asset Management capabilities.

Feature	DA	DA DSCCM	DA Express
Desktop Configuration	✓	✓	✓
Power Management	✓	✓	✓
Group Policy Template Import	✓	✓	✓
Wake On LAN	✓	✓	✓
Role Based Administration	✓	✓	▪
Remote Management and Control (inc RSC 2.0)	✓	✓	▪
Reporting of user logons and activity	✓	✓	▪
Reporting of administrator activity	✓	✓	▪
Software Deployment	✓	▪	▪
Hardware and software inventory	✓	▪	▪

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

A complete list of Desktop Authority's predefined variables can be found on the ScriptLogic web site.

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.

A complete list of the Desktop Authority API functions can be found on the ScriptLogic web site.

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.

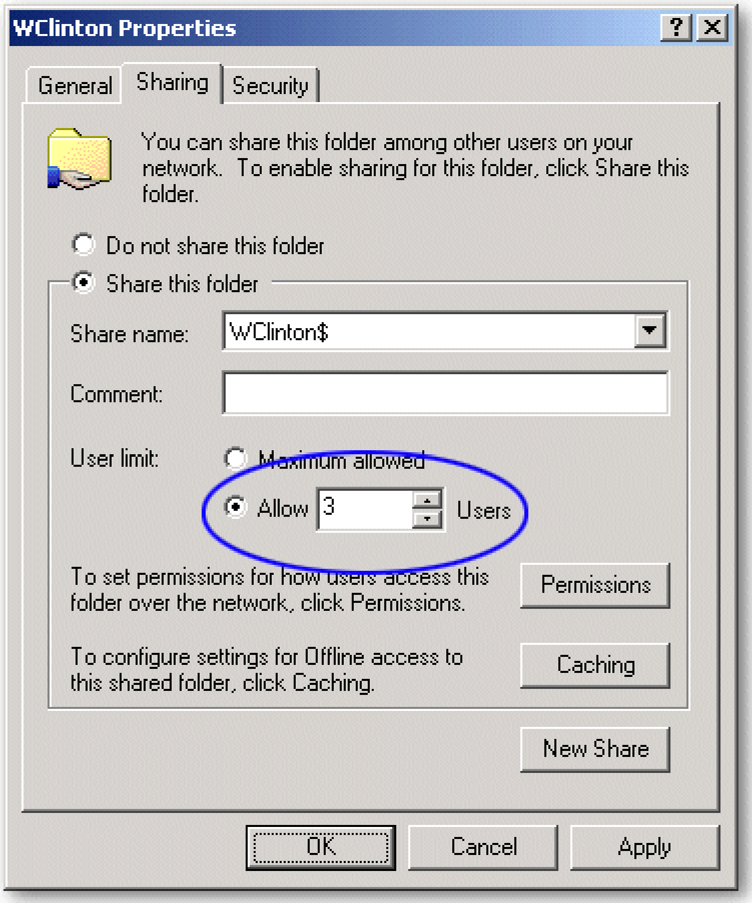
To **Limit Concurrent Logons**, you must:

Share each user's home directory.

The task of sharing each user's home directory as well as specifying the maximum number of connections can be daunting if there are a lot of users for which this must be done. ScriptLogic's AutoShare utility can help. AutoShare will simply share all users' home directories at the click of a button.

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. AutoShare can also be set to accomplish this task.



You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: WClinton$

Comment:

User limit: ○ Maximum allowed

● Allow 3 Users

To set permissions for how users access this folder over the network, click Permissions.

To configure settings for Offline access to this shared folder, click Caching.

Provide a drive mapping in Desktop Authority.

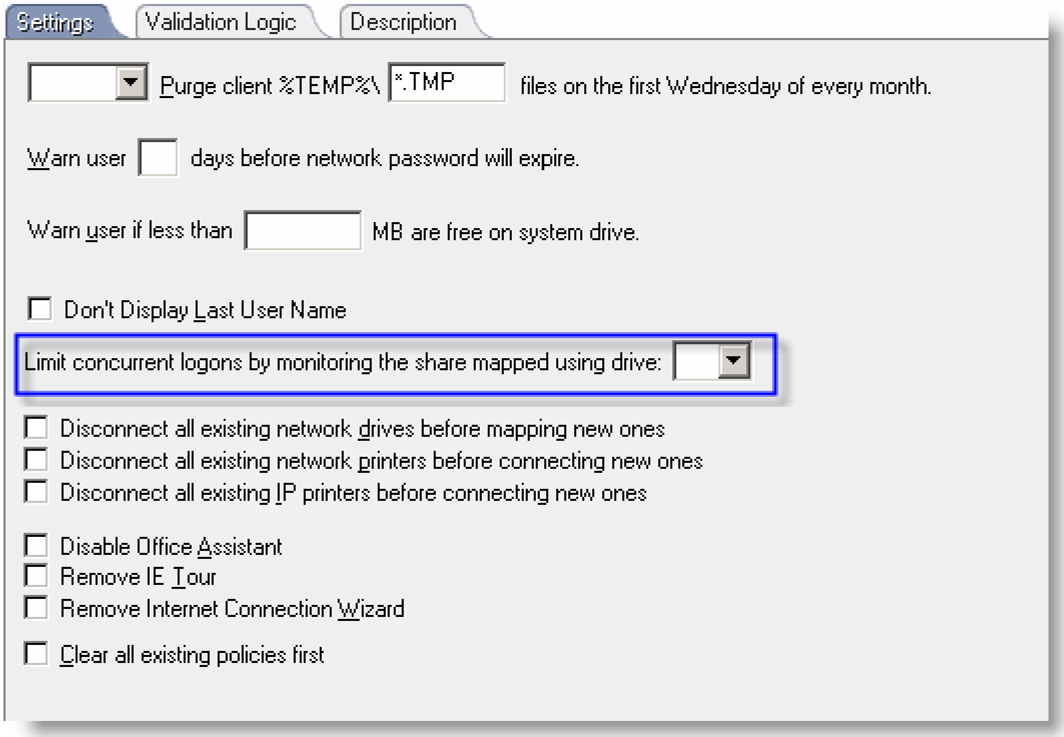
Using the Drive Mappings object within the Manager, map a drive to each user's Home Directory.

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.



[▾] Purge client %TEMP%\ [*.TMP] files on the first Wednesday of every month.

Warn user [ ] days before network password will expire.

Warn user if less than [ ] MB are free on system drive.

□ Don't Display Last User Name

Limit concurrent logons by monitoring the share mapped using drive: [▾]

□ Disconnect all existing network drives before mapping new ones
□ Disconnect all existing network printers before connecting new ones
□ Disconnect all existing IP printers before connecting new ones

□ Disable Office Assistant
□ Remove IE Tour
□ Remove Internet Connection Wizard

□ Clear all existing policies first

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.

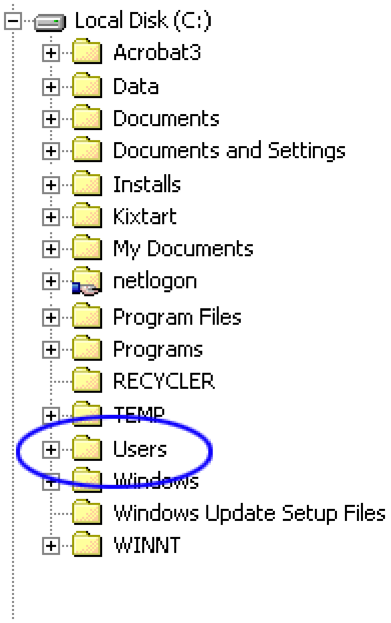
Root Mapping to the user's home directory provides a simple path to the directory. Since all other users' home directories on the drive are invisible to the user, there is no confusion as to where the directory is. The user does not have to scroll through a list of folders to search for their own folder. 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!

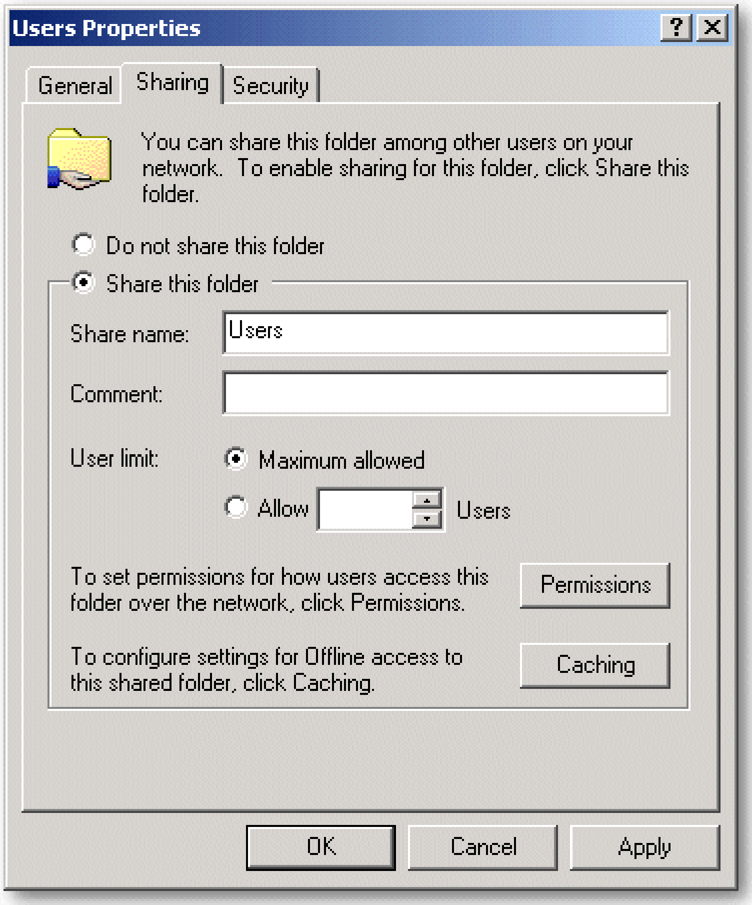
Step 1

Create a base share point for your user's home directories.

Open Window's Explorer on the server to house home directories. Create a folder called "Users".



Right click the Users folder you just created and select the Sharing tab. Share this folder as "Users".



Users Properties

General | Sharing | Security

You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Users

Comment:

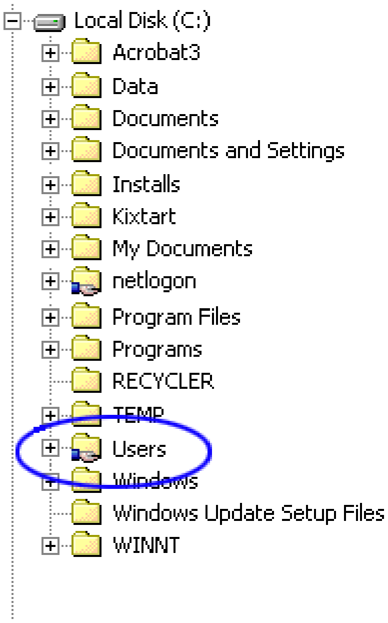
User limit: ● Maximum allowed

○ Allow [ ] Users

To set permissions for how users access this folder over the network, click Permissions.

To configure settings for Offline access to this shared folder, click Caching.

The folder should now look like the following in Windows Explorer.



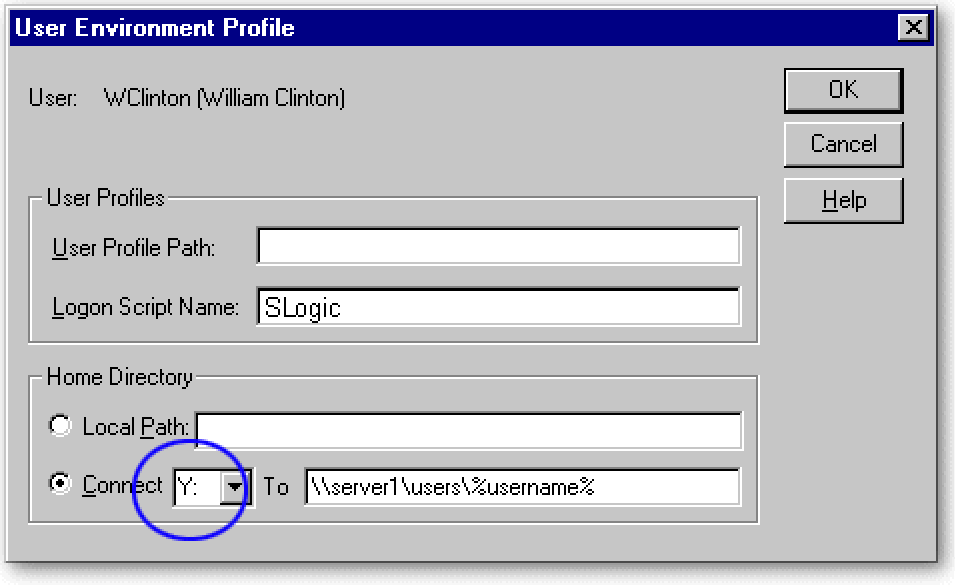
Note: You may elect to have multiple base share points spread across one or many servers. Since Desktop Authority can use dynamic variables when mapping drives, you will only need a single entry on the Drive Mappings object to accommodate any configuration you wish. If you have hundreds or thousands 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.

Step 2

Create your users with User Manager for Domains (UMD), or Active Directory - Users and Computers if you have Windows 2000/2003 Domain Controllers.

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.



User Environment Profile

User: WClinton (William Clinton)

User Profiles

User Profile Path:

Logon Script Name: SLogic

Home Directory

○ Local Path:

● Connect Y: To \\server1\users\%username%

Now specify the path to the user's home directory. Notice in the example above 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. 2000 will only grant the user Full Control NTFS permission to their home directory. While this is done for security purposes, this typically presents two problems:

1. Even as an administrator you don't have NTFS rights to this folder so you can't share it, and
2. Your third-party tape backup software may not be able to backup the documents in your user's home directory if it logs on with an Administrator account.

To overcome these two problems, 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.

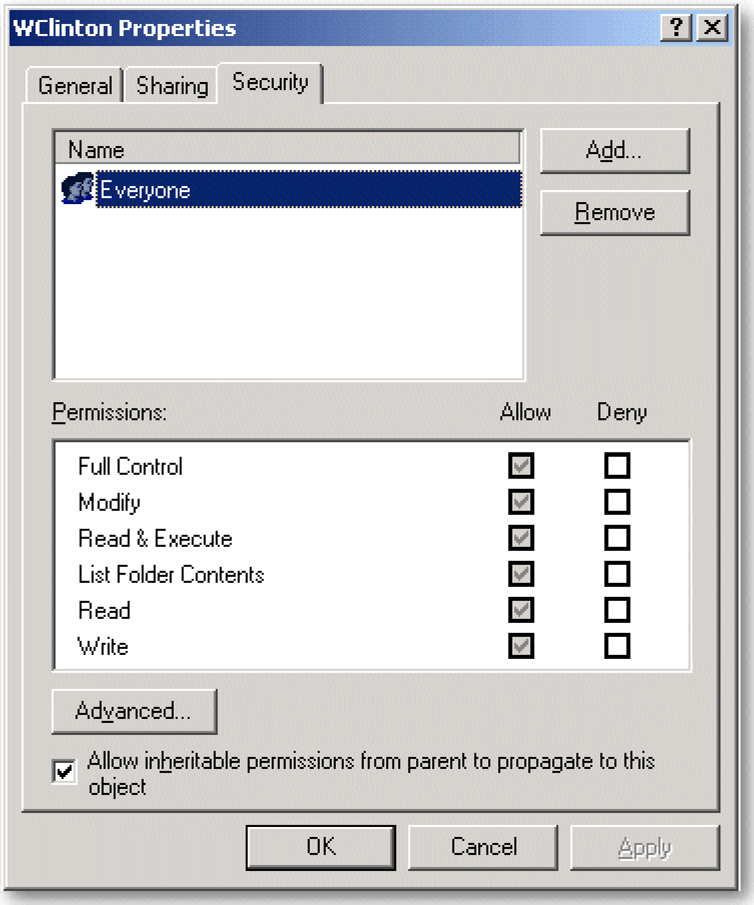
Step 3

Apply NTFS permissions and share each user's home directory.

To completely automate the application of NTFS permissions and sharing of each user's home directory, we created a utility called AutoShare. AutoShare consists of two components: The AutoShare Manager which is the intuitive GUI interface for managing your configuration and the AutoShare Service, which runs as a service on one or more NT/2000 servers.

Without AutoShare, you'll need to use Windows Explorer to manually change the NTFS permissions and share each user's home directory.

To accomplish this task using the manual method, 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.



Name

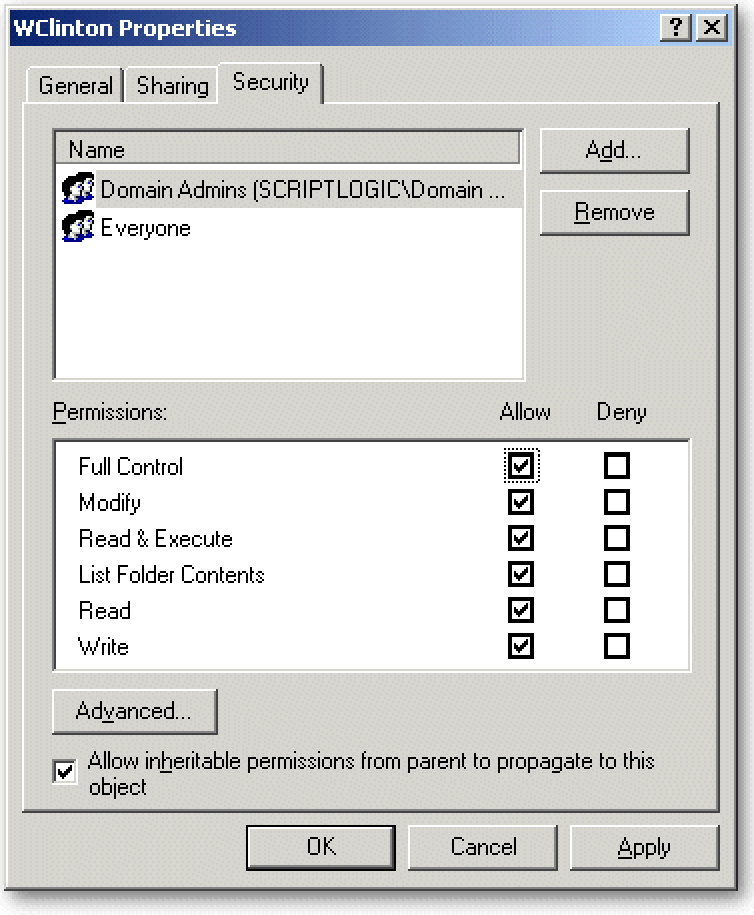
Everyone

Permissions:

	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

☑ Allow inheritable permissions from parent to propagate to this object

Add your administrative group (e.g. Domain Admins) to the list with Full Control rights.

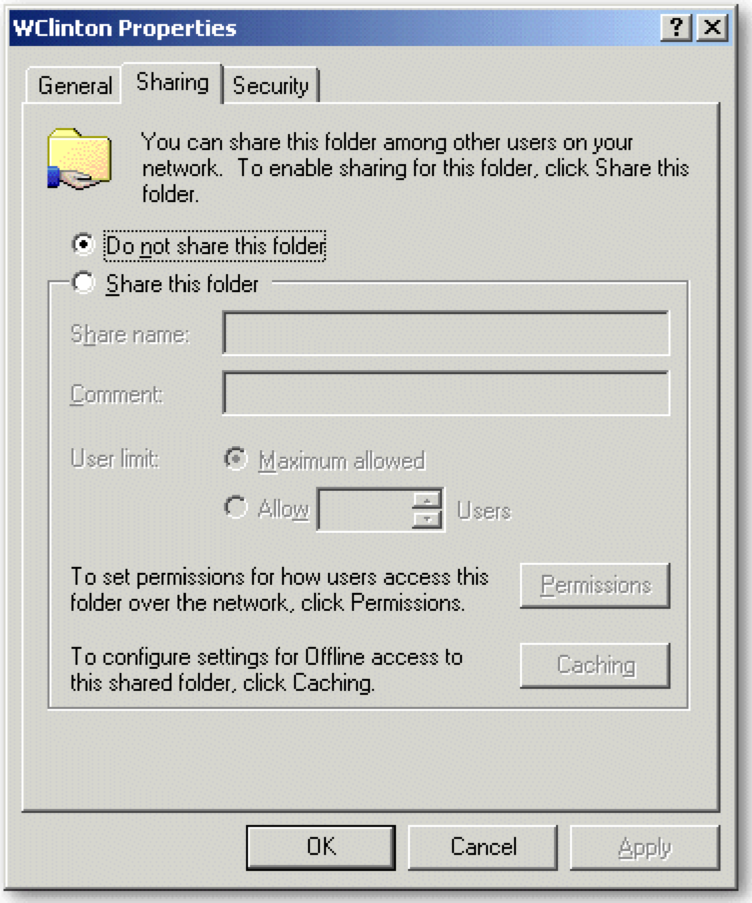


Name
Domain Admins (SCRIPTLOGIC\Domain ...
Everyone

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

☑ Allow inheritable permissions from parent to propagate to this object

Apply and then select the Sharing tab.



WClinton Properties

You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

● Do not share this folder

○ Share this folder

Share name:

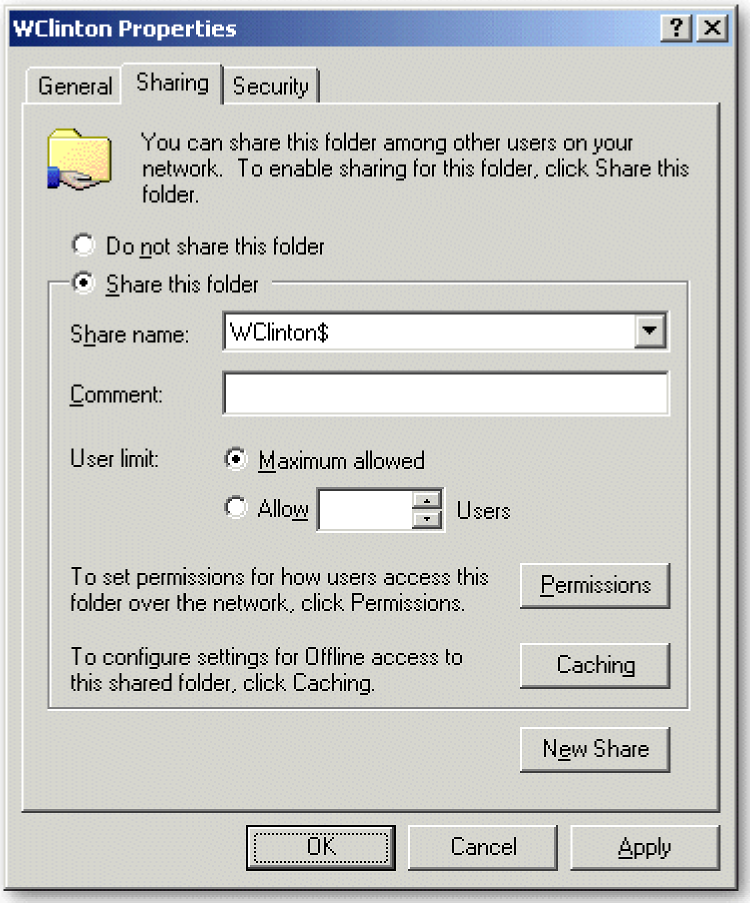
Comment:

User limit: ● Maximum allowed ○ Allow Users

To set permissions for how users access this folder over the network, click Permissions.

To configure settings for Offline access to this shared folder, click Caching.

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.



WClinton Properties

You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: WClinton$

Comment:

User limit: ● Maximum allowed

○ Allow Users

To set permissions for how users access this folder over the network, click Permissions.

To configure settings for Offline access to this shared folder, click Caching.

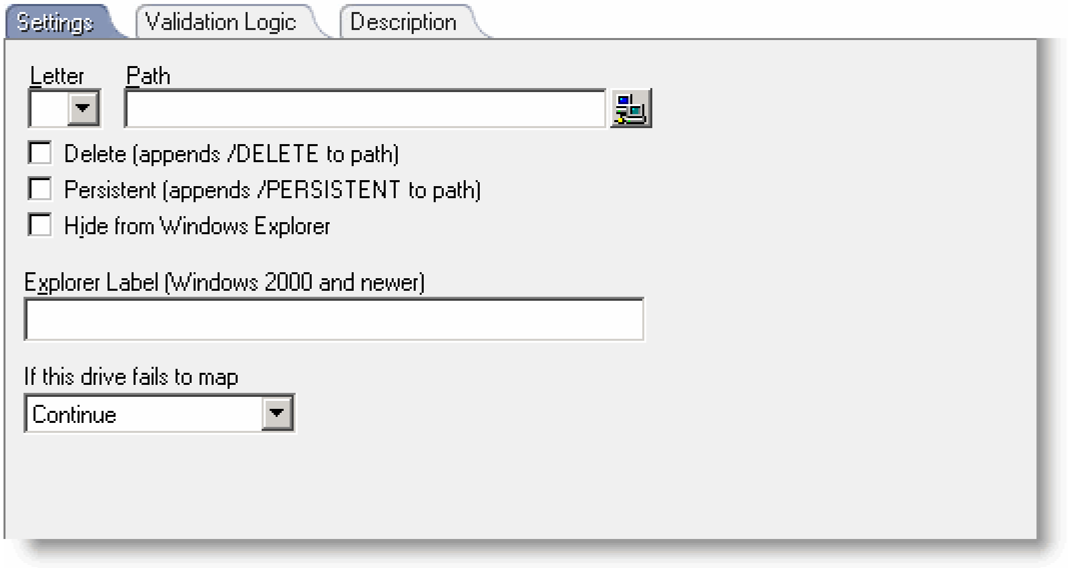
Step 4

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.

Launch the Desktop Authority Manager, from Profiles, select the profile and then the Drive Mappings object. Insert a new configuration element.

Specify drive H for the drive letter and a shared folder of \\$HomeServer\$HomeDir$$.



Letter
Path

☐ Delete (appends /DELETE to path)

☐ Persistent (appends /PERSISTENT to path)

☐ Hide from Windows Explorer

Explorer Label (Windows 2000 and newer)

If this drive fails to map: Continue

Notice how we leveraged 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).

Save the changes, replicate and exit. Logon from a client to verify your home mapping works as expected.

Implementing a Poor Man's 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.

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.

REPLICATION TO NETLOGON

Replication is the process of publishing Desktop Authority configurations from a source location to the NETLOGON share of all target domain controllers. Using a replication process allows a single "master" copy of the configurations to be maintained in a centralize location.

The following files are published during the replication process.

File	Description
*.sld	Profile Description files
*.slp	Profile configuration files
Antivirus40.kix	This ScriptLogic custom script has been designed to prevent VBscript and other scripted viruses from executing on your clients. This proactive approach is achieved by disassociating certain file type extensions from Windows Script Host.
asee.dll	ASEE Dynamic Link Library, v. 1.2.14.0
config.dat	Anti-spyware SDK (definitions) file
DAUSLoc.dll	Client-side portion of the Update service. All client-side communications go through this component.
DAUSLocCOM.dll	COM wrapper for DAUSLoc.dll.
KX16.DLL	KiXtart runtime dll's needed for communication with NETAPI.DLL.
KX32.DLL	KiXtart runtime dll's needed for communication with NETAPI.DLL.
KX95.DLL	Client side of the KIXRPC service.
msvcp71.dll	Microsoft® C Runtime Library, v. 7.50.3077.0
msvcr71.dll	Microsoft® C Runtime Library, v. 7.50.3052.4
profiles.sl	Profile listing
psapi.dll	Process Status Helper, v. 4.00
shfolder.dll	Microsoft Shell Folder Service
slAgent.dll	ScriptLogic COM object agent that runs as a local service on the client to monitory inactivity, run as admin capability among others. This is displayed as an icon in the system tray.
slAgent.exe	ScriptLogic COM object agent that runs as a local service on the client to monitory inactivity, run as admin capability among others. This is displayed as an icon in the system tray.
slAPIEng71.dll	ScriptLogic API engine used for Data Collection (Hardware/Software Collection)
slAse.exe	Anti-spyware client service
slDataCollection.dll	ScriptLogic Data Collection script
SLengine.dll	Desktop Authority engine which processes the configuration profiles.
slMapiEx.dll	Desktop Authority dll responsible for processing Outlook Mail Profiles.
SLogic.bat	Desktop Authority's logon script
SLPdefault.SL	Default ScriptLogic Profile
SLPDefault.sld	Default ScriptLogic Definitions file
daUpdateClient.exe	Update service client object
slScanEngine.exe	Patch Management Scan Engine which scans for installed and not installed patches

slSigs.ini	Desktop Authority signature file used to verify that the configuration profiles and definition files are correctly signed
slStart.exe	Runs with Desktop Authority engine to process the configuration profiles.
SLstart.ini	Client configuration file for ScriptLogic Engine and COM Object
Syg.dat	Anti-spyware SDK (definitions) file
VarDefs.sl	Global variable definitions
wKiX32.EXE	Console-less version of KiXtart program file.
xdel.exe	ScriptLogic utility to delete all files in a folder (and optionally recurse subfolders).

GLOSSARY

AD

The shortened name for Active Directory Users and Computers.

client

A computer connected to the network.

computer name (NetBios)

A unique name (up to 15 characters long) assigned to a computer for identification purposes.

custom scripts

(ScriptLogic) A KiXtart script written to provide a customized solution.

domain

A collection of resources including computers, printers, etc. grouped together to form a single networked environment.

Domain Controller

A server that authenticates and manages network logons.

drive mapping

The redirection of a network directory to a local drive letter on the client.

dynamic variables

(ScriptLogic) Variables that are used to temporarily store values that are used at a later time in a KiXtart script. The values of these variables change according to the user that is logging on to the network.

Group

A collection of users, computers, and other groups used to manage access to network resources.

hidden share

A shared folder that is hidden to the user while browsing file using Network Neighborhood and Windows Explorer.

Home Directory

A private directory located on the network that only a specific user has access to.

Host Name

The DNS Name assigned to a computer for identification purposes.

IP Address

A unique address used to identify a node on the network.

KiXtart

A logon script processor and scripting language developed by Ruud van Velsen of Microsoft Benelux

logon script

A batch (.BAT) or command (.CMD) file used to configure the users working environment when they log on to the network.

MAC Address

A hardware address that is built in to the network adapter.

Master Domain

The domain in a Single Master Domain network model that maintains the user database.

member server
A server contained on the network that is not considered a domain controller.

MSDE 2000

NETLOGON
A default shared folder, %WinDir%\System32\Repl\Import\Scripts, used to hold all logon scripts. By default, “Everyone” has read access to this folder.

Operations Master
(ScriptLogic) The Domain Controller that ScriptLogic is installed to.

OpsMaster service

Patch Management service

Post-Engine scripts
(ScriptLogic) A customized KiXtart script that is made to run following ScriptLogic’s logon script.

Pre-Engine scripts
(ScriptLogic) A customized KiXtart script that is made to run prior to ScriptLogic’s logon script.

RAS
Remote Access Service. A service that provides the ability for remote logons for the purpose of monitoring and administering networks.

RBA

replication
The process of synchronizing data from one computer to another.

Resource Domain
A separate domain to it’s Master that allocates its own network resources. Uses the Master domain to authenticate its users.

role

Role Based Administration

root mapping
Maps a network folder or drive (usually a home directory) to a drive letter on the local machine. The resource is mapped to the root of the drive letter. Any folders above the mapped resource is not seen by the user.

SAM database
The database that holds a network’s entire user account list. These user accounts are accessed by the UMD (User Manager for Domains) applet.

server
A computer designated to provide shared resources to other computers on the network.

service
An application that runs in the background and has no interaction with the desktop. The application is executed before the user logs on and runs under a system or predefined user account.

service account

An account specifically created to start and stop services. Generally this is specified as a domain account with Domain Admin privileges and the right to logon as a service.

share

A network directory that has been shared and provided permissions to authorized users.

site

A collection of network resources that physically exist in separate locations.

SQL 2000

Super User/Group

SuperBrowser

(ScriptLogic) ScriptLogic's network browser which can be found by pressing the select button to fill in an entry. It is used to locate a resource on the network.

system policies

Settings in the registry that are concerned with the current user and local computer settings. System policies are set using the Group Policy MMC snap-in (W2k) or Poledit.exe (NT).

target

UMD

The shortened name for User Manager for Domains. See Also: User Manager for Domains.

UNC

The full Windows 2000 name of a networked resource. The syntax for a UNC is \\servername\sharename.

user

The person who is using the workstation to access the network.

User Manager for Domains

An applet used to manage user accounts.

user profile

A file that holds configuration information including desktop settings, persistent network connections, and user preferences. The user profile is restored at every logon so the same working environment exists for the user.

validation logic

(ScriptLogic) The definition of rules used to determine whether a ScriptLogic setting should affect the user that is currently logging on to the network.

VPN

Virtual Private Network.

INDEX