



# ***DESKTOP AUTHORITY***® ***VERSION 8***

## **Desktop Authority 8 Getting Started**

**SCRIPTLOGIC**

# Copyright

Copyright 1997-2009 ScriptLogic Corporation and its licensors. All Rights Reserved.  
Protected by U.S. Patents 6,871,221; 7,293,087; 7,353,262 and 7,469,278 with other patents pending.

Portions include technology used under license from Shavlik Technologies and are copyrighted. Certain portions used under license and Copyright 2004-2009 Sunbelt Software, Inc., all rights reserved. This software is based in part on the work of the Independent JPEG Group.

This publication is protected by copyright and all rights are reserved by ScriptLogic Corporation. It may not, in whole or part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent, in writing, from ScriptLogic Corporation. 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 33487-27421  
561.886.2400  
[www.scriptlogic.com](http://www.scriptlogic.com)

## Trademark Acknowledgements:

Desktop Authority, ScriptLogic and the ScriptLogic logo are either registered trademarks or trademarks of ScriptLogic Corporation in the United States and/or other countries. The names of other companies and products mentioned herein may be the trademarks of their respective owners.

## Table Of Contents

About this Guide .....	4
Introducing Desktop Authority .....	5
Installation and Upgrade Considerations .....	6
System Requirements .....	6
Installation .....	9
Evaluation .....	9
Registration .....	9
Deployment Overview .....	10
Desktop Authority Manager .....	10
Configuration and Reporting Databases .....	11
ScriptLogic Service .....	11
Update Service .....	11
OpsMaster Service .....	11
Computer Management Agent .....	11
Logon Script (User Management) .....	11
User Management Agent .....	11
Desktop Engine (User Management) .....	12
Computer Management vs. User Management .....	13
Computer Management .....	13
User Management .....	13
Deploying Client Software .....	14
GPO Deployment .....	14
Configuring GPO Deployment .....	14
Logon scripts .....	16
Deploying Network Services .....	17
Configuring the ScriptLogic Service .....	18
Configuring the Update Service .....	19
Managing Desktops and Servers .....	20
Using Validation Logic .....	20
<i>Configuring Validation Logic</i> .....	20
Configuring User and Computer Management Elements .....	21
Role Based Administration .....	25
Configuring Data Collection .....	26
Replication .....	26
Reporting .....	27
Remote Management .....	28
Troubleshooting .....	29
Trace files .....	29

## **About this Guide**

The aim of this Getting Started Guide is to familiarize Windows network administrators with the installation, deployment and configuration of Desktop Authority. It will discuss important terms to know and help in planning for installation and deployment. This guide will also review critical steps to take when deploying and configuring Desktop Authority.

This guide is not a complete detailed guide to the inner workings and configurations of Desktop Authority. For further details not discussed in this guide, the Desktop Authority Installation Guide, Administrator's Guide, Reporting Guide, Database Schema, Database Dictionary, and online help should be reviewed. Online help is installed with Desktop Authority and can be accessed by pressing F1 on any Desktop Authority Manager dialog. All other guides may be downloaded from the ScriptLogic Desktop Authority Product Downloads section on the ScriptLogic website.

## **Introducing Desktop Authority**

So you have just downloaded Desktop Authority...lets examine what is contained in this powerful desktop management product and how it will help you to reduce the cost of managing the Windows desktops in your enterprise, ease the administrative burden to support these desktops and help to support the desktop lifecycle of all machines in the enterprise.

Desktop Authority enables enterprise administrators to proactively control, inventory, secure and support all desktops from a central location. This solution provides enterprises the granular control they need over Windows desktops and applications to increase IT efficiency, meet compliance requirements, and enhance security. It helps to reduce the total cost of ownership for desktops by reducing help desk calls, managing power more efficiently, restricting the use of removable storage, and keeping your desktops patched and secured.

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, 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 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.

ScriptLogic's patented Validation Logic technology is used to proactively target specific configurations to desktops and servers based on a highly granular set of environmental criteria.

Desktop Authority also contains other features including Software Management, USB/Port Security, Patch Management, Anti-spyware, Hardware and Software Inventory, Custom Reporting and Role Based Administration features.

## Installation and Upgrade Considerations

Are you upgrading your current version of Desktop Authority? Desktop Authority 8.0 supports upgrades from Desktop Authority 7.8 (including 7.81) only. If you have an earlier version of Desktop Authority, you must upgrade it to 7.81 first.

### **System Requirements**

#### **Supported Operating Systems**

Desktop Authority can be installed on the following servers:

- Microsoft Windows 2000 Server/Advanced Server with SP4
- Microsoft Windows Server 2003 Standard/Enterprise Edition with SP2 (including 64-bit)
- Microsoft Windows Server 2008 Standard/Enterprise (including 64-bit)

The Desktop Authority Manager can be run from a shortcut on a Windows XP/Vista/2008 client with Service Pack 2 (SP2) or greater installed.

Although Desktop Authority can still be installed on a domain controller, ScriptLogic Corporation strongly suggests installing Desktop Authority on a member server.

Additionally, Windows 2008 Server has Windows Firewall enabled by default. When installing on Windows 2008 Server, the Desktop Authority installation will prompt to create firewall exceptions. If these exceptions are not set, a limited set of functionality will be lost. This includes (but is not limited to) running Desktop Authority Manager from a shortcut, installing Remote Management and running ScriptLogic Service from a member server.

#### **Supported Domains**

- Microsoft Windows 2000 domain
- Microsoft Windows 2003 domain
- Microsoft Windows 2008 domain



Desktop Authority 8.0 uses Active Directory and Group Policy for secure, consistent deployment of its management agent to all versions of Windows. In version 7.8, GPO Deployment was only required for Microsoft Vista and Windows Server 2008 clients that have User Account Control (UAC) enabled. However, in this version of Desktop Authority 8.0, GPO Deployment is required for all clients that will be managed by Desktop Authority.

**Additional Server Software Requirements**

These additional applications are required and will be installed as part of the Desktop Authority installation. Installation of these additional applications may require a system reboot.

- Microsoft Windows Installer 3.1<sup>1</sup>
- Microsoft Data Access Components (MDAC) 2.8<sup>1</sup>
- Microsoft .NET Framework version 1.1
- Microsoft .NET Framework version 2.0
- Microsoft Visual C++ 2005 Redistributable Package<sup>1</sup>
- Microsoft SQL Server 2005 Backward Compatibility<sup>1</sup>
- Microsoft SQL Server 2005 Express – Installed if a SQL Server instance is not selected.<sup>2</sup>
- Desktop Authority will prompt to start the Computer Browser Service (if disabled)

<sup>1</sup> If not already present, these applications will install on the workstation where Desktop Authority Manager runs from a shortcut.

<sup>2</sup>On Windows Server 2008, SQL Server Express SP2 will download and install.

**User Account Permission Requirements**

For use with Desktop Authority services:

- One admin level account with read/write access to all NETLOGON share(s) and a member of the local Administrators group on all applicable workstations (if installed on a domain controller, user account must be a domain admin)
- One domain user level account

Carefully consider all requirements, specifically the additional server software prerequisites, when deciding where to install Desktop Authority. If you choose to install on a domain controller, make sure these prerequisites are acceptable before starting the installation.



For detailed Operating System, Disk Space and RAM requirements, refer to [Article T1515](#), found in ScriptLogic's Online Knowledge Base system.

***Installation***

Refer to the Desktop Authority Installation and Upgrade Guide for complete details on the installation process. This guide can be downloaded from the ScriptLogic website.

***Evaluation***

Following the installation of Desktop Authority, there will be a 30-day evaluation period when installed and used for the first time. If a full registration key is supplied, no evaluation period will be exercised.

Evaluation licenses for Desktop Authority Express are available upon request.

The evaluation of Desktop Authority is fully functional with the following exceptions:

- Patch Deployment (PDD) option will only deploy patches which have been rated as "Low" or "Not Rated" severity.
- The Spyware Detection and Removal (SPY) option will only remove or quarantine spyware which has been classified as "Benign" or "Low" severity.
- Patch deployment and spyware removal for all severity levels will only be applied on computers named DATEST1, DATEST2, DATEST3, DATEST4 and DATEST5

***Registration***

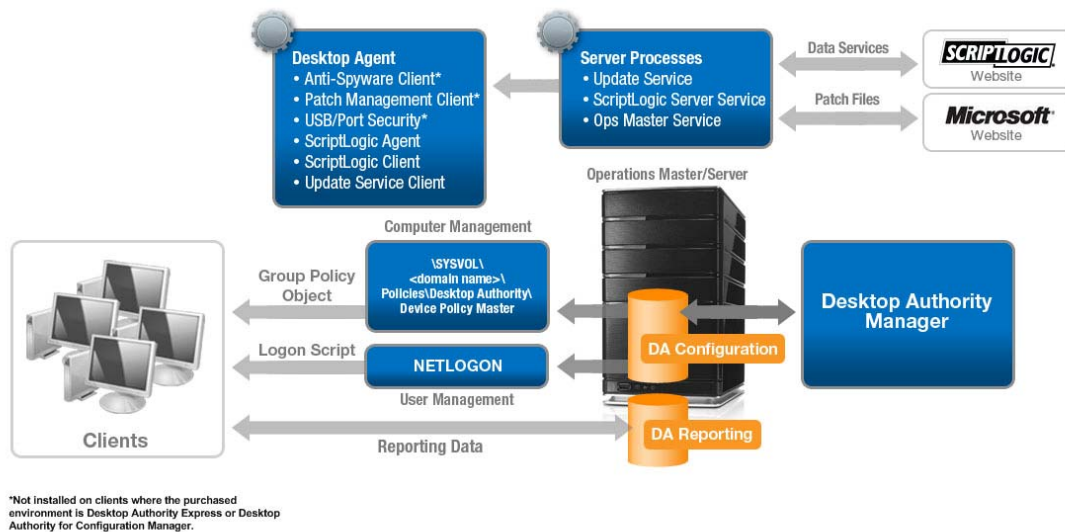
When you purchase Desktop Authority, you will be provided with a registration key and/or a license file. The product can be registered by running the Desktop Authority Registration application by selecting *Start > All Programs > Desktop Authority > Desktop Authority Registration*.

The Registration application can also be run from within the Desktop Authority Manager by selecting *Help > Product Registration*.

## Deployment Overview

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

An overview the Desktop Authority system is shown below.



### 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 setup using the manager 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.

### ***Configuration and Reporting Databases***

Desktop Authority can use an existing instance of Microsoft SQL Server (2000, 2005, 2008) or install Microsoft SQL Server 2005 Express Edition on the Operations Master Server 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 computer 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 is installed to one or more servers within the domain. When installed on a domain controller or member server, this service manages the shares used to cache information collected from the managed desktops. The OpsMaster service pulls collected files from these shares for storage into the DAREPORTING database.

### ***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](http://www.scriptlogic.com) in order to obtain option licensing information as well as download anti-spyware definition updates and Patch Management updates. This service also interfaces with [www.microsoft.com](http://www.microsoft.com) to download Microsoft patches. 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.

### ***Computer Management Agent***

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. The Desktop Authority User Management agent is launched via a logon script named SLOGIC. This script must be defined as the user's logon script in order for the agent to be invoked. The logon script performs initializations and launches the Desktop Authority User Management Agent.

### ***User Management Agent***

User Management objects are executed on each client by the User Management Agent. This agent includes the ScriptLogic Service and the Desktop Engine. This agent is invoked when the user logs on, at configured refresh intervals, and when the user logs off.

***Desktop Engine (User Management)***

The Desktop Engine initiates the configuration of objects and elements specific to the user's environment. 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 User Management settings defined in the Manager. Once these settings are complete the engine will execute post-engine custom scripts.

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

## Computer Management vs. User Management

### ***Computer Management***

Desktop Authority's Computer Management agent operates at the Computer level. Computer Management provides the ability to install software, patch computers, install service packs, collect inventory, launch programs, edit the registry and wake computers without any user logged on to the client computer.

For example, you can install software for all users, patch a machine outside business hours, collect inventory information from servers, or run maintenance tasks without interrupting users.

Computer Management uses specific system and scheduled events to perform the requested actions. These events include Startup, Shutdown, Refresh and Scheduled times.

Computer Management runs from a deployed service on the client computer. The service, ScriptLogic CBM Service, is deployed via a group policy object to every computer that exists in the OU(s) selected for deployment. This service runs using the LocalSystem account.

### ***User Management***

Desktop Authority's User Management configurations apply to the user environment. The User Management settings are configured as the user logs on or off the network and at the configured refresh interval. When a user logs on or off of a computer or during a specified refresh period, the computer is updated with the specified configurations based on the user who is logged on.

User Management configurations allow for software installations, anti-spyware scans, service pack deployment, drive mappings, printer configurations, file operations, remote management, Microsoft Outlook and Office settings, and much more to be configured.

User Management configurations are processed with the help of the ScriptLogic service. See [Configuring the ScriptLogic Service](#) for further details.

## Deploying Client Software

### ***GPO Deployment***

One of the first must-do configurations after installing Desktop Authority is to configure GPO Deployment. GPO Deployment is used to deploy the necessary client files to the computers that will be managed by Desktop Authority.



GPO Deployment is easily configured using the Desktop Authority Readiness Wizard following the installation of Desktop Authority. The Readiness Wizard can also be loaded by selecting it from the File menu.

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.

The GPO is configured by selectively targeting OUs within the enterprise. 32-bit and 64-bit systems can also be selectively targeted. This is done by filtering with a WMI filter that is automatically deployed with the GPO. 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 Desktop Authority client files that are necessary for the computer to be managed by Desktop Authority. If the client files have previously been deployed and installed to a machine that is now being excluded, the computer will still be excluded if they are specified in the exclusion list.

### ***Configuring GPO Deployment***

To configure OUs for GPO Deployment expand Deployment Options in the Navigation Pane and select Client Deployment.



Desktop Authority 8.0 uses Active Directory and Group Policy for secure, consistent deployment of its management agent to all versions of Windows. In version 7.8, GPO Deployment was only required for Microsoft Vista and Windows Server 2008 clients that have User Account Control (UAC) enabled. However, in this version of Desktop Authority 8.0, GPO Deployment is required for all clients that will be managed by Desktop Authority.



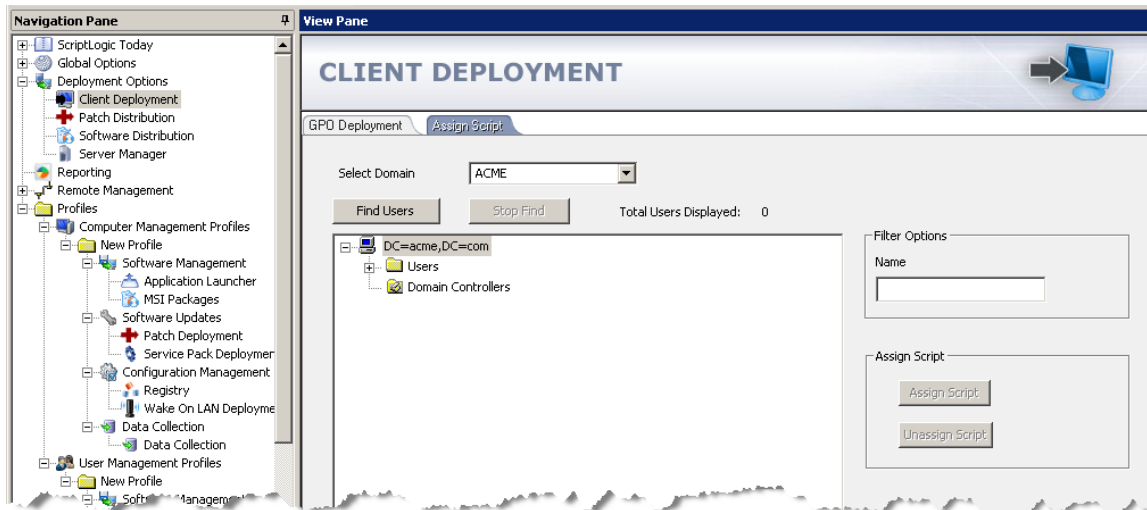
**Logon scripts**

Desktop Authority User Management settings are applied to all users who log in to the network and have the SLOGIC logon script assigned to their user account. This logon script assignment is required for each user to obtain User Management settings. The logon script performs some pre-flight checks and then launches the Desktop Authority engine.



The assignment of logon scripts can be configured using the Desktop Authority Readiness Wizard following the installation of Desktop Authority. The Readiness Wizard can also be loaded by selecting it from the File menu.

To assign logon scripts for users, expand Deployment Options in the Navigation Pane, select Client Deployment and then the Assign Script tab.



First, find the users 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.

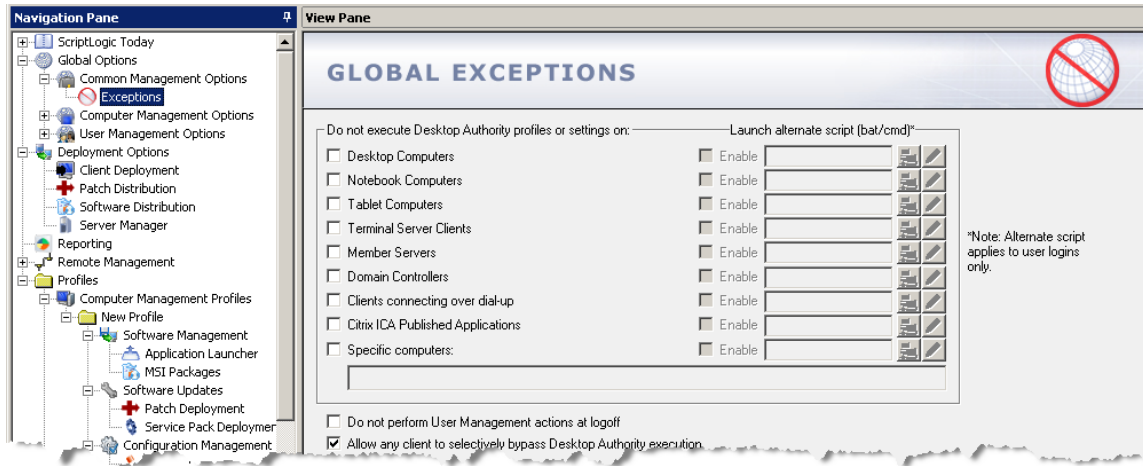
**Computer Exceptions**

By default, Desktop Authority will be deployed to all computers in the OUs targeted for GPO Deployment. There is a way, however, 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.



Computer Exceptions are easily configured using the Desktop Authority Readiness Wizard following the installation of Desktop Authority. The Readiness Wizard can also be loaded by selecting it from the File menu.

To exclude a computer, select Global Options, Common Management Options, and then Exceptions.



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.

**Deploying Network Services**



Desktop Authority services can easily be configured using the Desktop Authority Readiness Wizard following the installation of Desktop Authority. The Readiness Wizard can also be loaded by selecting it from the File menu.

Server Manager is where Desktop Authority’s network services are managed. It is used to select the servers that Desktop Authority will replicate to and also host the necessary services. These services include the ScriptLogic service and the Update service.

The ScriptLogic Service, when deployed to a network server, creates and manages the shares that are used to cache data files created by the agents on managed desktops. These data caches store log files, trace files and data collection files, which includes reporting data such as hardware and software inventory, user activity, patch results, Anti-spyware results and USB/Port Security results.

### Configuring the ScriptLogic Service

The ScriptLogic Service software component is used on network servers to manage the shares for collection of data from desktops. It is also used on managed clients (desktops) to perform configuration of User Management settings.

The ScriptLogic Service requires two Windows accounts, a server service account and a client service account. The server service account is used by the service to create and manage shares on network servers. The client service account is used by the service on managed clients (desktops) to perform User Management. Note that User Management operations are tried first, using the account of the logged in user. If the user account does not have sufficient privileges, then the client service account is used.

To configure the ScriptLogic service, navigate to Deployment Options > Server Manager object. Within the Server Manager grid, there will be a column entitled ScriptLogic service. If the service is not already started, right click on the column and choose Configure from the pop up menu.

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.

More Info

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\

OK Cancel

The Server Service user account must have local administrative rights on each computer. By default, the Domain Admins group is a member of the local Administrators group on each 2000/XP/2003/Vista/2008 computer, so selecting a user account that belongs to the Domain Admins group would satisfy this requirement.

The Client Service account is used to perform User Management tasks that require access to network resources. This user account only needs to be a member of the Domain Users group.

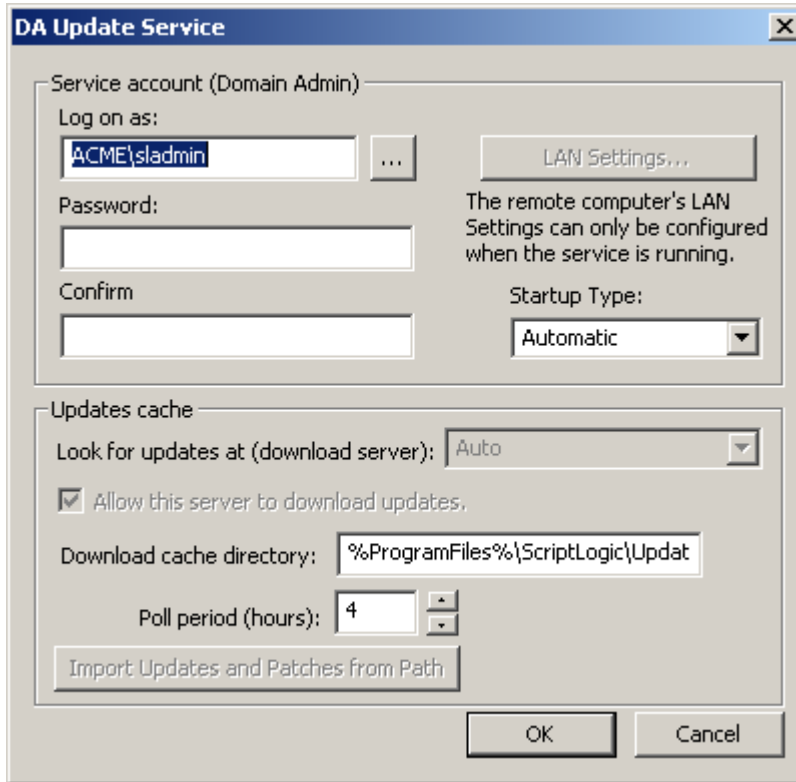
Installing this service to member servers at each of your sites is the preferred requirement for this service and provides the best configuration for load balancing the caching of data collected from desktops. When saved, the user accounts will be authorized and the Server Service will be started on each server. A successful start of the service will be denoted in the cell with a green check icon.

The Group Policy base deployment takes care of installing the Server Service to managed clients.

### **Configuring the Update Service**

The Update Service is used by the USB/Port Security, Software Management, Patch Management and Anti-Spyware objects.

To configure the Update service, navigate to Deployment Options > Server Manager object. Within the Server Manager grid, there will be a column entitled Update service. If the service is not already started, right click on the column and choose Configure from the pop up menu.



The screenshot shows the 'DA Update Service' configuration dialog box. It is divided into two main sections. The top section, titled 'Service account (Domain Admin)', contains a 'Log on as:' field with the text 'ACME\sladmin' and a browse button (...). To the right is a 'LAN Settings...' button. Below the 'Log on as:' field are 'Password:' and 'Confirm' fields. To the right of these fields is a text box stating: 'The remote computer's LAN Settings can only be configured when the service is running.' Below the 'Confirm' field is a 'Startup Type:' dropdown menu set to 'Automatic'. The bottom section, titled 'Updates cache', contains a 'Look for updates at (download server):' dropdown menu set to 'Auto'. Below this is a checked checkbox labeled 'Allow this server to download updates.'. Underneath is a 'Download cache directory:' field containing the path '%ProgramFiles%\ScriptLogic\Updat'. Below that is a 'Poll period (hours):' field with the value '4' and up/down arrow buttons. At the bottom of this section is an 'Import Updates and Patches from Path' button. At the very bottom of the dialog are 'OK' and 'Cancel' buttons.

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.

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 may reside on some other server (for storage considerations), 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.

## Managing Desktops and Servers

### *Using 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 or not. 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, computer class, operating system and many other selections, 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 at the timing specified.

User Management Validation Logic includes settings for different Validation types, classes, operating systems, connection types, and timing options for Logon, Logoff, Refresh, Shutdown 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. Computer Management Validation Logic rules relate to things that are specific to the computer environment, therefore, these Validation Logic types are a subset of the User Management Validation Logic types.

### *Configuring Validation Logic*

After creating your profile, for Computer Management or User Management, Validation Logic should be configured. To do this click on the new profile name and select the Validation Logic tab in the View Pane. You will notice however, there are two Validation Logic tabs, Validation Logic and Default Validation Logic.

The Default Validation Logic tab defines the defaults that will be used for Validation Logic on any new element added to the profile. For example, when a new Drive Mapping element is added to the profile, the Drive Mapping Validation Logic will automatically default to the Default Validation Logic settings. It is recommended to configure the Default Validation Logic to make configuring elements easier. Each element's Validation Logic can be changed, if needed, from the Default Validation Logic. Default Validation Logic applies to both Computer Management and User Management profiles.

The settings configured in the Validation Logic tab will be the rules that will be followed for a user or computer to validate for the profile.

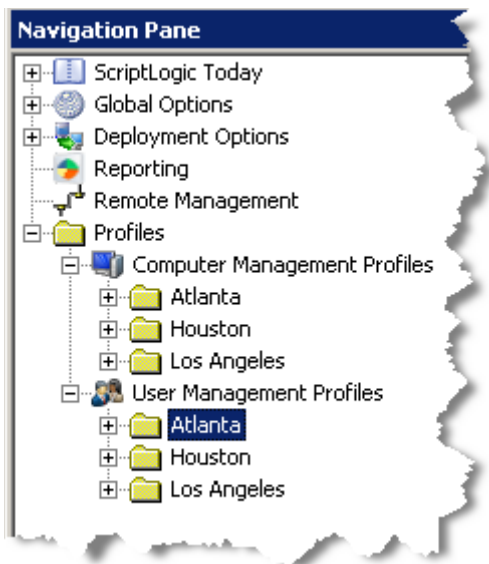
User Management Validation Logic can be set at the Profile level and at the element level. Likewise, Computer Management Validation Logic can be set at the Profile level and the element level. Computer Management also has Timing settings. Computer Management Validation Logic Timing settings can be set at both the Profile level and the element level.

### ***Configuring User and Computer Management Elements***

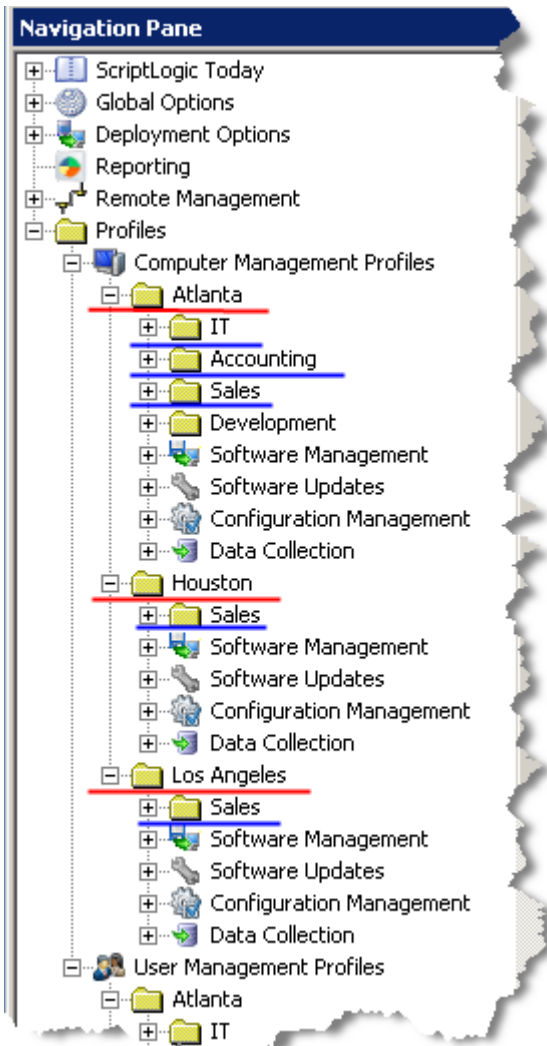
Once the Group Policy is configured and the necessary services are started it is time to start creating profiles and defining the User and Computer configurations. The first step here is to decide how the domain will be managed. How exactly will the profiles look? Will they be created based on site, location, or department? Maybe even by building or floor?

One of the most common ways administrators lay out the profiles is by location. For instance, let's say the ACME Company has locations in Atlanta, Houston, and Los Angeles.

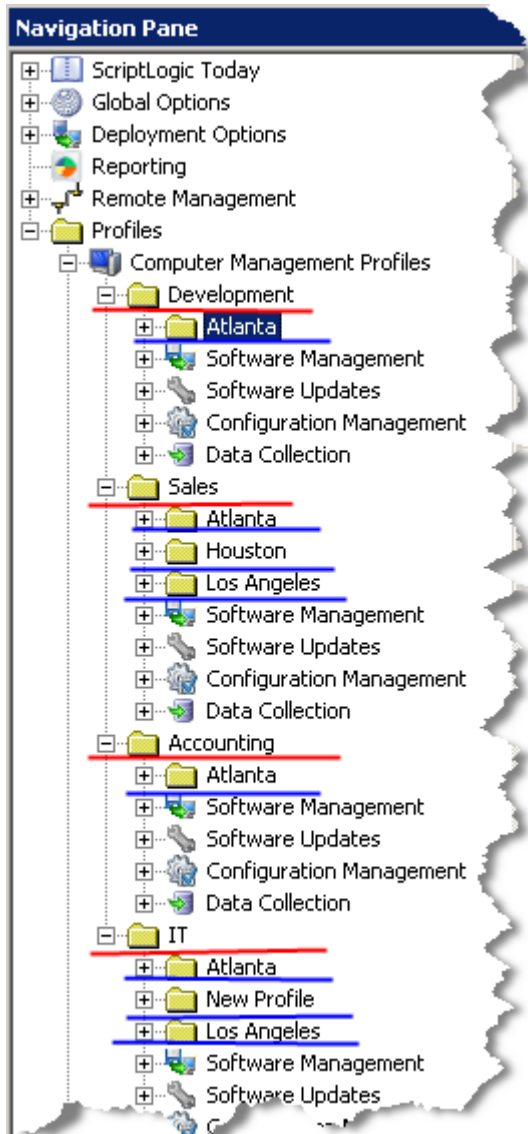
Designing profiles by location would yield the following:



For larger organizations, it is helpful to organize subprofiles by department. For example:



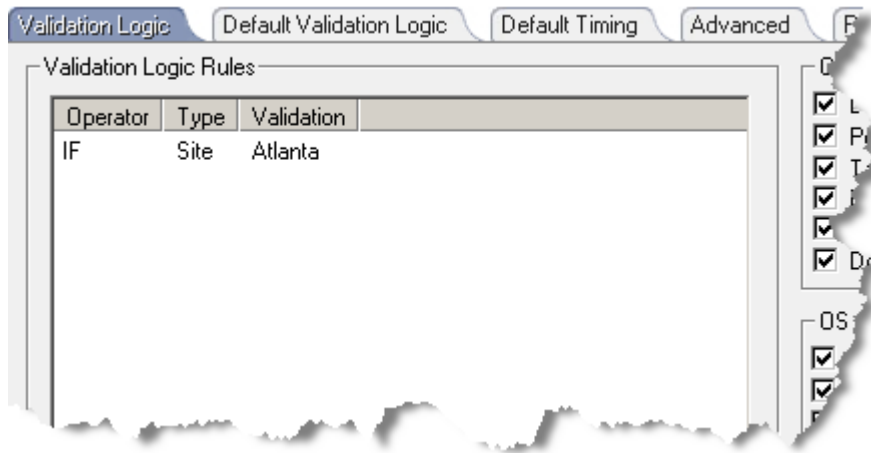
On the other hand, one could first layout the profiles departmentally, following it up by location.



Keep in mind there are many different ways to set this up and it is up to each enterprise to determine the most effective layout based on how Desktop Authority will be used to manage the computers and users in the enterprise.

Once the profiles are created, Profile Validation Logic and Role Based Permissions should be configured on each profile.

Validation Logic on the profile, Computer Management or User Management, is used to determine whether the profile should be processed for the computer or user. So if a profile is only to hold settings for the Atlanta location. The Validation Logic for the Atlanta profile might use the Site or IP validation types to determine the location, assuming Sites are configured in the domain.



This is just an example of how profile Validation Logic could be used to limit the profile to a specific location. There are many different variations that could be used depending upon the configuration of the enterprise.



All profiles should have specific Validation Logic configured for it. Profiles that do not have any Validation Logic defined will be validated on all computers or users.

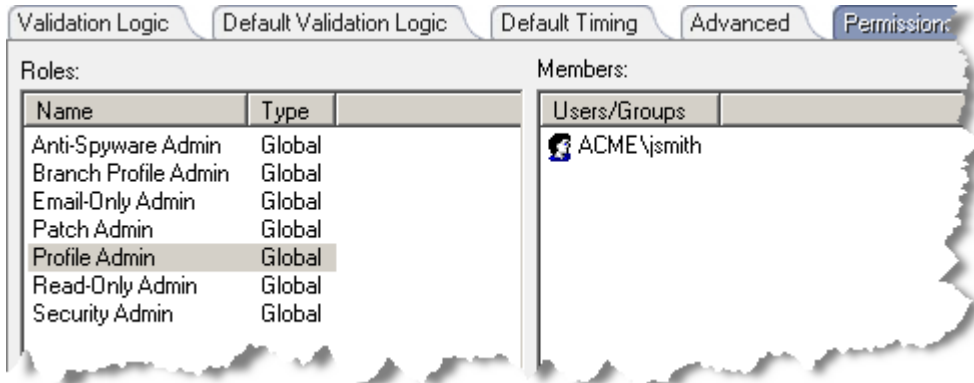
Validation Logic also includes settings for the types of computers and operating systems you need to manage. There are also timing settings that will determine when the profile will execute, i.e. Startup, Shutdown, Logon, etc.

Once a profile passes the Validation Logic test, elements within the profile are processed. Each element within a profile also contains its own Validation Logic.

**Role Based Administration**

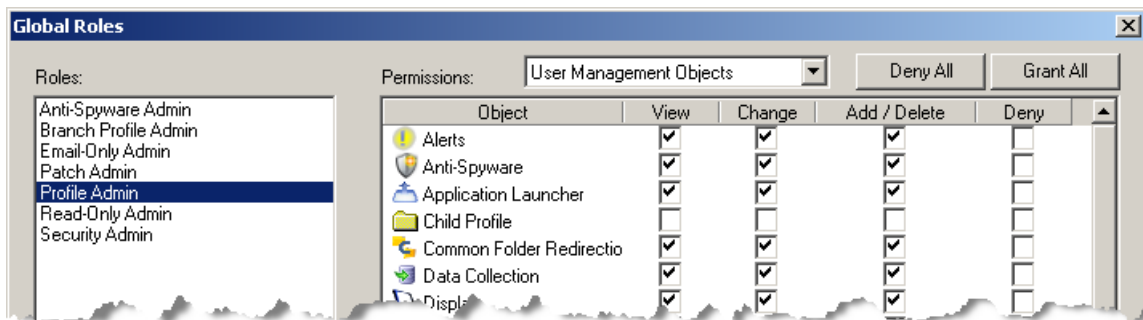
Role Based Administration (RBA) restricts Administrator access to profiles and the configuration elements contained within them. Profile access within the Desktop Authority Manager is limited to users and groups that have been granted specific permissions to them. Configuration of RBA is not required, but in larger enterprises with multiple locations, it is commonly used to delegate access to Profiles to the administrator(s) in each location.

In the case illustrated below, user jsmith, an Admin in the Atlanta office, is being defined as the Profile Admin.



The Profile Admin role is a default role that is automatically configured with Desktop Authority. The role name and also the permissions defined for it are completely editable for the enterprises needs.

The default Profile Admin role is defined with the permissions to View, Change, Add and Delete all profile objects. A partial view of this can be seen below.



The above mentioned configurations are the main settings that should be determined when getting started with Desktop Authority. There are other more advanced profile settings. Further details about them can be found in the Administrators Guide.

***Configuring Data Collection***

Desktop Authority can be configured to collect computer specific data including hardware and software inventory, 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 in the Desktop Authority Manager 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.

***Replication***

Once all of the configurations are complete, Desktop Authority must publish the configurations. This makes the configuration data available for all computers and users that are being managed by Desktop Authority.

The act of publishing is called Replication. By default User Management configurations are published to the NETLOGON share and the Computer Management configurations to the \\SYSVOL\\Policies\Desktop Authority\Device Policy Master folder.

## Reporting

Desktop Authority's Reporting center consists includes many pre-defined reports. These reports can be run as-is or they can be modified to suit the specific Enterprise needs. Once a report is modified, it will be saved as a User-Defined Report, and can be generated from the User-Defined Reports section of the reporting tree.

The Pre-defined Report categories include:

- Administrator Audit
- Anti-spyware Activity
- Hardware Activity
- Miscellaneous
- Patch Management Status
- Profile Reports
- Software Inventory
- Software Management
- USB-Port Security
- User Activity

To run an existing report, simply select the report category, select the report and either double-click on it or click the Generate button. Fill in the required report parameters and let it run.

Please note that Data Collection must be configured for the necessary User Management and Computer Management profiles. Data will be collected for each user and/or computer as the Data Collection settings denote. All reports will report from the data collected based on the Data Collection settings.

Reports can also be scheduled to run at specific days/times. To schedule a report, select Scheduled Reports in the reporting tree. Click New to create a schedule. On the Scheduled Report Settings dialog, select the report and fill in the settings. Some reports may take a long time to generate. Set up a report schedule to have it generated in the background and emailed to you.

Learn more about creating, modifying and managing reports in the Desktop Authority Reporting Guide. This guide can be downloaded from the ScriptLogic website.

## Remote Management

Desktop Authority's Remote Management module offers the ability to remotely access computers around the network for the purposes of Remote Control, File Transfer, Help Desk Chat, Computer Management, Computer Settings, Performance Monitoring and more.

To manage a remote computer, the Desktop Authority service must be deployed to the computer in question. This service can be deployed throughout the enterprise by configuring a Remote Management profile element. However, it can also be deployed to a single computer from the Remote Management tree. Right-click on the specific computer in the Remote Management tree and select Deploy Service from the pop up menu. Once the service is deployed, select Remote Control from the pop-up menu.

Learn more about Remote Management in the Desktop Authority Remote Management Guide. This guide can be downloaded from the [ScriptLogic website](#).

## Troubleshooting

Once in a while, things don't work the way you expect them to. When this happens, some troubleshooting steps are necessary. Computer Management and User Management both have their own troubleshooting steps. With each you can configure Desktop Authority to create a trace file for the User logging on and/or the Computer.

### ***Trace files***

Trace files help you to determine why a profile and/or element did not execute on a specific machine or for a specific user. User Management trace and log files are stored in the users temp directory, *%windir%\Temp\Desktop Authority* folder on each computer. Computer Management trace and log files are located in the Windows temp directory under a Desktop Authority folder.

Trace files are only created if the Global Option is turned on for the Computer and/or User.

To do this, go to either (or both) Troubleshooting dialogs by selecting

- Global Options > Computer Management Options > Troubleshooting
- Global Options > User Management Options > Troubleshooting

and select the checkbox, *Enable verbose debug mode for these specific computers (users)*. Be sure to specify the computers (users) in the space provided. Wildcards (? and \*) can be used. Separate each entry by using a semicolon (;). To specify all computers (users) enter a single asterisk (\*).