



DESKTOP AUTHORITY[®]

VERSION 8

Installation Guide

SCRIPTLOGIC

Copyright 2011 ScriptLogic Corporation and its licensors. All Rights Reserved.
Protected by U.S. Patents 6,871,221; 7,293,087; 7,353,262; 7,469,278 and 7,814,460
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 33487-2742

1.561.886.2400
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

Contacting ScriptLogic.....	4
ScriptLogic on the Web	4
System Requirements	5
Desktop Authority Versions.....	7
Desktop Authority Structure	8
Installation Backup	9
Installing Desktop Authority	10
Registration	26
Optional Components.....	28
Appendix A: Using Remote Support Center with Desktop Authority.....	29
Index	32

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.

SYSTEM REQUIREMENTS

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 or Vista 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

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^{1 4}
- Microsoft Data Access Components (MDAC) 2.8^{1 4}
- Microsoft .NET Framework version 1.1⁴
- [Microsoft .NET Framework version 2.0 \(x86\)](#)³
Place into the “%ProgramFiles%\ScriptLogic Manager\Device Policy Master” folder (to be installed Desktop Authority to client workstations, if necessary)
- [Microsoft .NET Framework version 2.0 \(x64\)](#)³
Place into the “%ProgramFiles%\ScriptLogic Manager\Device Policy Master” folder (to be installed Desktop Authority to client workstations, if necessary)
- Microsoft Visual C++ 2005 Redistributable Package^{1 4}
- Microsoft SQL Server 2005 Backward Compatibility^{1 4}
- [Microsoft SQL Server 2005 Express](#)^{2 3}
Required and installed if a SQL Server instance is not selected.
Place into:
 - x86 – “%ProgramFiles(x86)%\Common Files\SQL Server Setup\SQLExpress”
 - x64 – “%ProgramFiles%\Common Files\SQL Server Setup\SQLExpress”
- Desktop Authority will prompt to start the Computer Browser Service (if disabled)

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

² On Windows Server 2008, SQL Server Express SP2 will download and install.

³ If an internet connection is not available on the server where Desktop Authority is being installed, this file should be downloaded prior to the installation. Place the file in the folder specified above in order for Desktop Authority installer to install the application or install the application manually.

⁴ This file is packaged within the Desktop Authority installation file and does not need to be downloaded prior to installation. The installer will install the file if necessary.

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

Users of Desktop Authority Manager:

- Any user opening Desktop Authority Manager must be a member of the local Administrators group on the machine where they run the manager from (if opened on a domain controller, user must be a domain admin)

Desktop Authority supports the following localized versions of Microsoft Windows: English, Spanish, French and German. Although some parts of the product may work on non-supported languages, other parts might not. We do not provide support on non-supported language problems.

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 the [System Requirements](#) article found in ScriptLogic's Online Knowledge Base system.

DESKTOP AUTHORITY VERSIONS

Desktop Authority is available in three versions, Desktop Authority, Desktop Authority Express and Desktop Authority System Center Edition. 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 System Center Edition 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 SCE	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 is licensed based on the total number of unique seats which are managed in whole or part by Desktop Authority. A "Seat" is a desktop, laptop, or workstation computer, or thin-client session or any other user computing device.

Please refer to the [ScriptLogic website](#) for answers to any Desktop Authority Licensing questions.

DESKTOP AUTHORITY STRUCTURE

Desktop Authority Folders

The Desktop Authority installation creates the following folder structure under the Program Files folder as a default location. This default location can be changed during the installation process.

\ScriptLogic Manager

This folder consists of all necessary program files needed by the Desktop Authority application. This includes online help and default configurations. This folder is shared as **SLOGIC\$** by the default installation.

\DesktopAuthority

This shared folder contains the Desktop Authority programs to be deployed to client workstations for the Remote Management component. This folder is shared as **SLDACLient\$**.

\Device Policy Master This shared folder contains all Computer Management related files that are to be replicated throughout the system. This folder is shared as **DADevicePolicyMaster\$**.

\Logs

The *Logs* folder contains all log files created and configured as specified on the Logging object found within each profile. This folder is shared as **LOGS\$** by the default installation.

\Modules

This folder and all subfolders contain necessary program files used to run various modules of Desktop Authority.

\MS Updates

The MS updates folder contains various files that are needed for proper execution of Desktop Authority. You will be prompted if these files must be installed.

\Repositories

The Repositories folder contains all Generated Reports, Pre-Defined Reports and User-Defined Reports files.

\Scripts

The *Scripts* folder includes all necessary files to load and run KiXtart and Desktop Authority scripts. This folder includes the configurations made in the Desktop Authority Configurations dialog box. The files in the Scripts folder will be published to the domain controllers when replication is requested. This folder is shared as **SLSCRIPTS\$** by the default installation.

\Services

The *Services* folder contains the files necessary to create and configure the ScriptLogic and Update services.

\SLMSDEScripts

The SLMSDEScripts folder is used by the system. It holds database scripts that will create and update the ScriptLogic database. The contents of this folder should not be modified.

\Software Management

The Software Management folder contains necessary files for Software Management and Deployment.

\TemplateFiles

The TemplateFiles folder contains a copy of administrative templates that are imported into Desktop Authority. By default, all administrative templates found in the Windows folder are automatically imported into this folder and are automatically available for use within the Desktop Authority Manager.

INSTALLATION BACKUP



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

- To back up current configuration settings, copy \ScriptLogic Manager\ and all subfolders to a backup location.
- To back up existing Profiles, right-click on each profile name and select “Export Profile...”. Select a location to save the profile and click **OK**. Repeat for each profile.
- The installer will prompt to backup existing databases during the install process.

INSTALLING DESKTOP AUTHORITY

The following series of steps walk you through the installation of Desktop Authority. Although Desktop Authority can be installed on a Domain Controller, ScriptLogic Corporation strongly suggests installing Desktop Authority on a Member Server. Be sure to read the [System Requirements](#) to make sure your systems meet the minimum requirements.

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

Are you upgrading your current version of Desktop Authority? Desktop Authority 8.12 supports upgrades from Desktop Authority 7.8x and earlier versions of Desktop Authority 8.x.) only. If you have an earlier version of Desktop Authority, you must upgrade it to 7.81 first. The detailed installation instructions below will note where the upgrade differs from a new installation.



Special Consideration for customers upgrading from version 8.x:

Smart Client Provisioning is a new feature in Desktop Authority 8.1. Smart Client Provisioning includes both GPO-Deployment and Logon-based Deployment! Desktop Authority GPO-Deployment and Logon-based Deployment can both be used to deploy the Desktop Authority client components to workstations and servers.

When you upgrade, the new Logon-based Deployment will be automatically enabled. Therefore, the Desktop Authority client components may be installed on any workstation or server your users log on to.

If you do not wish to install the Desktop Authority client components on certain computers that your DA users may log on to, you should configure the computers in the Global Exceptions object. This will exclude them from executing Desktop Authority and disable the ability for the client components to be installed on those computers. This is the same exclusion method used by Desktop Authority prior to the introduction of GPO-Deployment.

Note: It is important to ensure that the DA GPO Deployment setting is not set to “Uninstall” as this may cause a repeated uninstall/reinstall sequence in which the DA GPO removes the client and a logon reapplies it.

The installation wizard walks through a series of dialog boxes prompting for information that is needed to copy the Desktop Authority program to your server as well as configure Desktop Authority for its initial use. Click **Next** on each dialog box to advance to the next option. Click **Back** to go to the prior dialog box. Click **Cancel** to abort the install.

1. **Welcome** is the initial dialog box. Click **Next** to continue.
2. The **License Agreement** dialog box appears. If you agree with the license agreement, select the *accept the terms of the license agreement* option. Click **Next** to continue.

- The following information dialog describes the required prerequisite components that Desktop Authority will install, if necessary. The listed components will be installed following the installation. These components include:

- Windows Installer version 3.1
- Microsoft Data Access Components (MDAC) version 2.8
- Microsoft SQL Server 2005 Backward Compatibility
- Microsoft SQL Server 2005 Express Edition (only required if this is the selected database during the install)
- Microsoft .NET Framework 1.1
- Microsoft .NET Framework 2.0
- Microsoft Visual C++ 2005 Redistributable Package (x86)

In addition, the installer will configure the following on Windows Server 2008:

- Windows Firewall Exceptions

Click **Next** to continue.

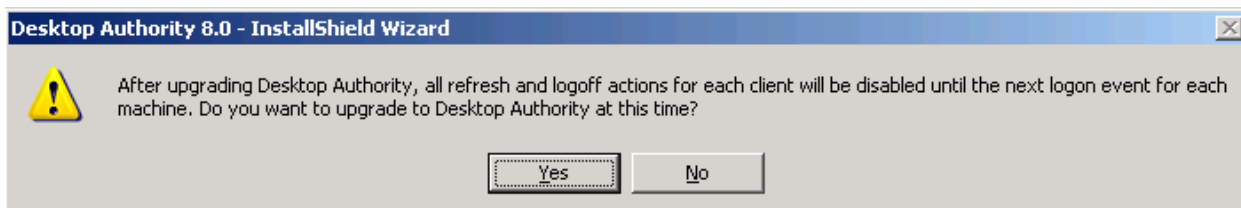
- If the install is an upgrade of Desktop Authority, select from either Typical Installation or *Express Upgrade*.

A typical installation will request Customer Information (User Name and Company Name), provide version Release Notes, destination path, Log path and Log share details. This option should be selected for first time installations of the product or to view or change any of the mentioned dialogs.

Upgrading existing 7.8 installations: Express upgrade will skip the Typical Installation dialogs and go directly to the Ready to Install the Program dialog. This option should be chosen for upgrades only.

Click **Next** to continue.

- If Express upgrade is chosen, you will be notified with the following confirmation dialog.



Skip to step 11 below.

- On the **Customer Information** dialog enter **User Name**, **Company Name** and **Serial Number** in the appropriate entries (User Name and Company Name are required). If you have purchased Desktop Authority, enter your registration code. Users evaluating Desktop Authority should leave the registration code blank.
Click **Next** to continue.
- On the **Choose Destination Location** dialog box, select a path and destination folder. The default installation path is *x:\Program Files\ScriptLogic Manager*. Press the **Change** button to select a different path. Click **Next** to continue. Select a setup destination. Select *This Computer* to install Desktop Authority to the computer which is running the installation program.
Click **Next** to continue.

8. Desktop Authority can automatically record logon information to a central location. Each day, a Comma Separated Value file will be created in the destination folder you select. The contents of the log files are customizable within each profile's logging object.

The default log path is *x:\Program Files\ScriptLogic Manager\Logs*. To select a different path, click *Browse and select a new path* and destination folder.

Choose this directory carefully. Log files grow in size as they are constantly updated every time a user logs into the network. Make sure the drive has enough available disk space to handle these logs.

Click **Next** to continue.

9. The **Select Log Share** dialog box appears. Enter the share name of the Logs folder. By default, the installation program creates this share name as *LOGS\$*. Leave this entry blank to disable logging.

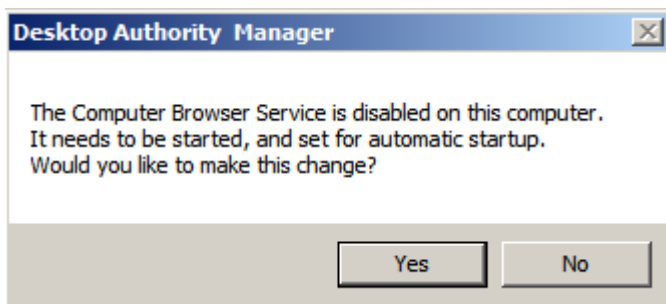
Logging may be enabled at a later time within the Desktop Authority Manager.

Click **Next** to continue.

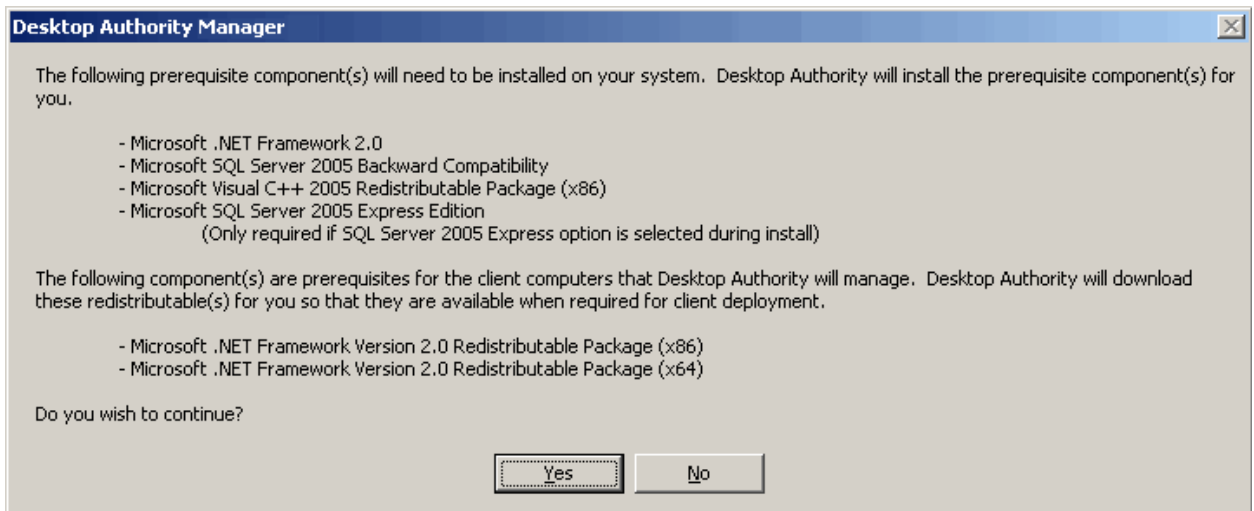
10. If you are upgrading Desktop Authority the previous version will be detected at this point. You are informed that all existing configurations will be saved. Click **OK** button to continue to accept the notification.

Before installing any product upgrade, a complete backup should be performed.

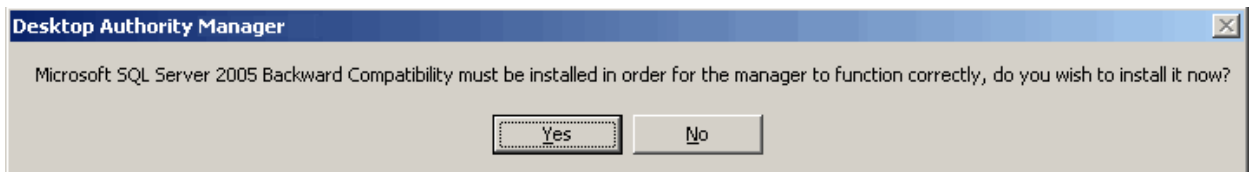
11. Click **Install** on the *Ready to Install the Program* dialog to proceed with the installation.
12. After the installation is finished, click **Finish** on the *Setup Complete* dialog to complete the installation and begin the configuration stage.
13. On Windows 2008 Servers, the Computer Browser Service is disabled by default. Desktop Authority requires this service to be started. If the service is not started, the install will prompt to set the service to Automatic Startup. Click **Yes** to start the service.



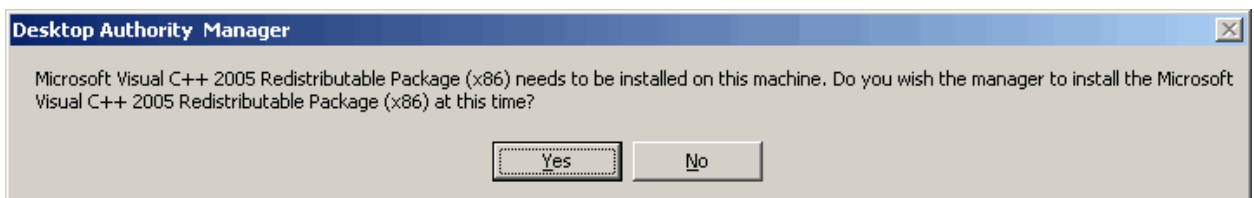
14. **New installations only:** The first time the Manager is loaded, a new installation state will be detected, prerequisites will be installed and the database configurations will be created.
Upgrades will skip this step.



Click **Yes** to allow the prerequisites to be installed. Click **No** to exit the Desktop Authority configuration phase.

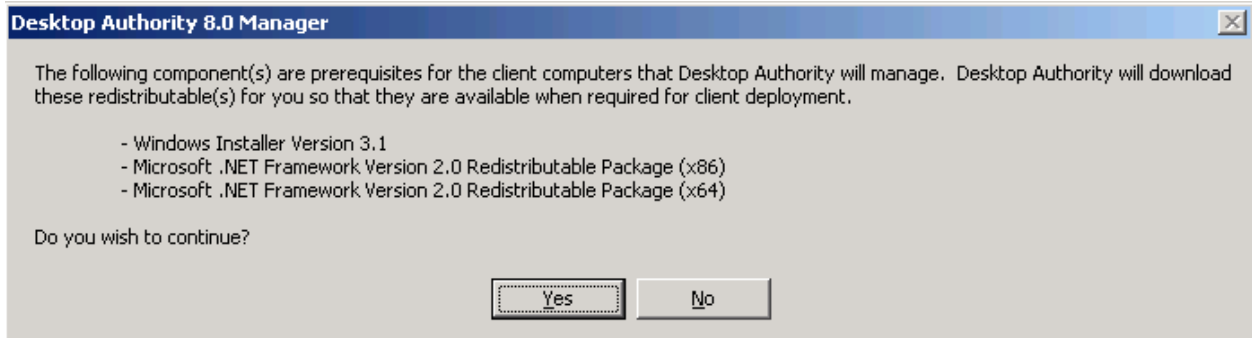


MS SQL Server 2005 Backward Compatibility provides a programmatic (COM) interface to SQL Server. Desktop Authority uses this to access SQL Server databases. Click **Yes** to install The SQL Backward Compatibility component. Click **No** to exit the Desktop Authority configuration phase.

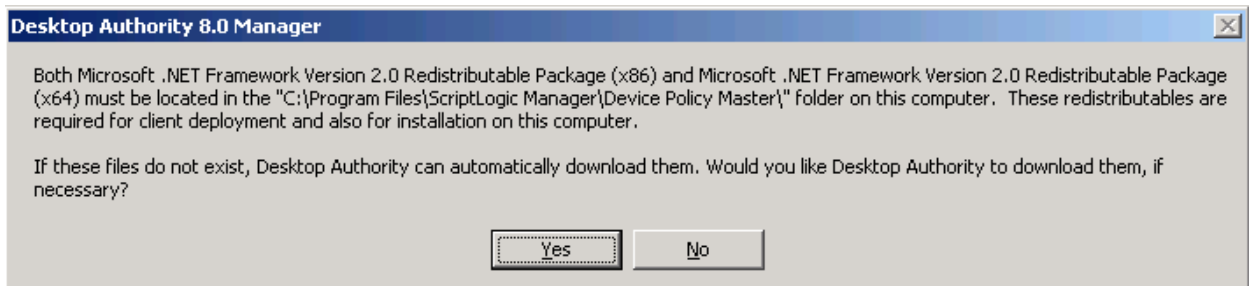


The Desktop Authority Manager requires the presence of Microsoft Visual C++ 2005 Redistributables on the machine. Click **Yes** to install this package. Click **No** to exit the Desktop Authority configuration phase.

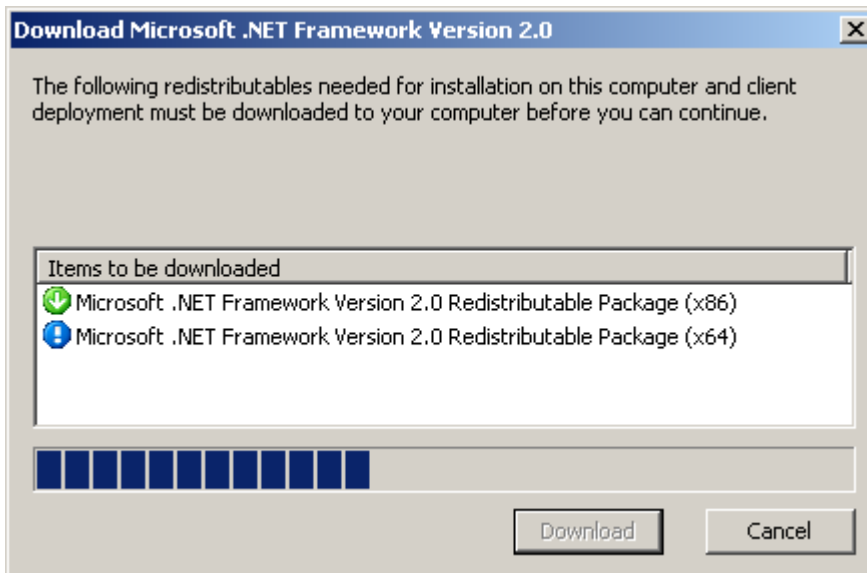
15. **Upgrade Installations Only:** The Microsoft .NET Framework 2.0 redistributable packages (both x86 and x64 versions) are required by DA to exist in the C:\Program Files\ScriptLogic Manager\Device Policy Master\ folder. These will be copied down and installed to clients during a GPO update on the client.



Clicking Yes will give you the option to download the .NET Redistributable Package automatically.

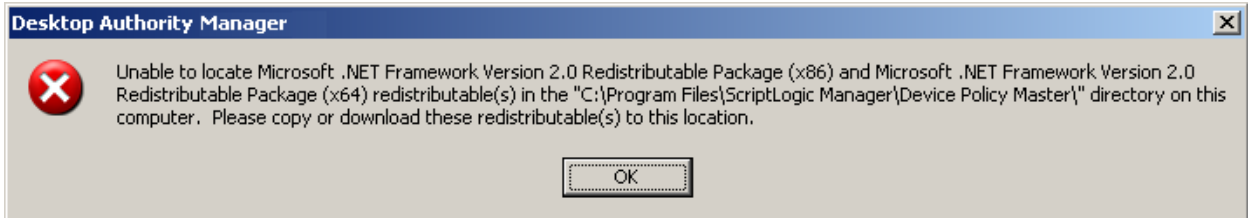


Click **Yes** to allow Desktop Authority to download the .NET Redistributable Package to the specified folder. Clicking **No** will exit the Desktop Authority configuration phase.

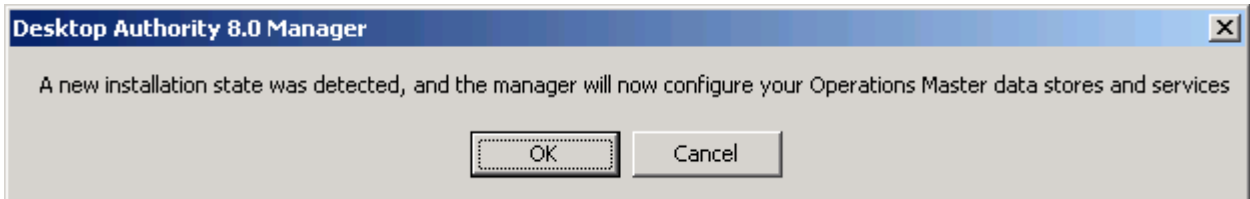


Click **Download** to begin the download process. After the download is complete, you will be prompted to install it.

If for some reason the .NET Redistributable Packages cannot be retrieved, the following dialog will be displayed. The .NET Redistributable files should be manually copied to the specified folder. The file must exist in the folder before continuing with the installation.




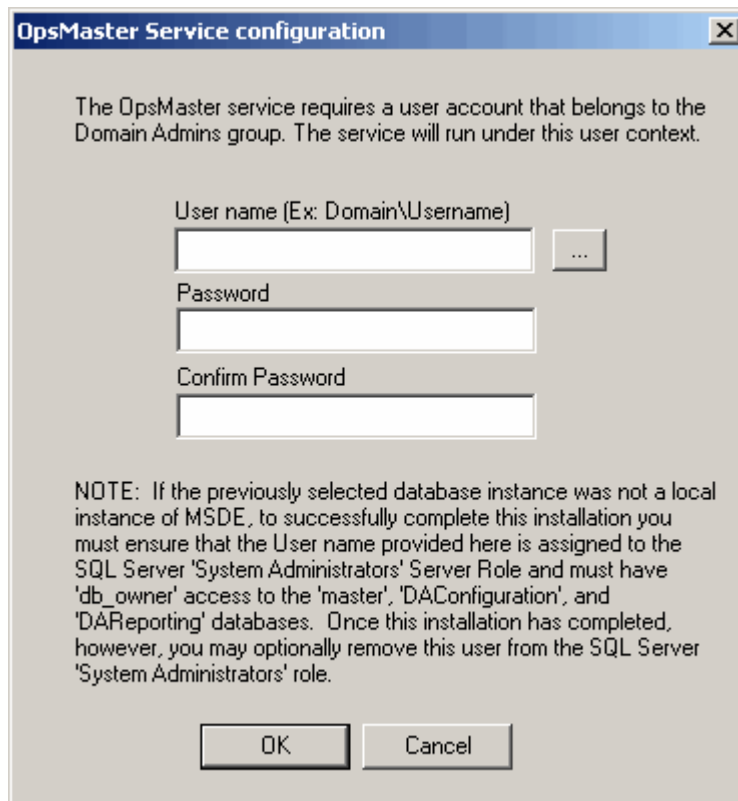
16. The database and services will now be configured.



Click OK to continue the configuration of databases and services for Desktop Authority.

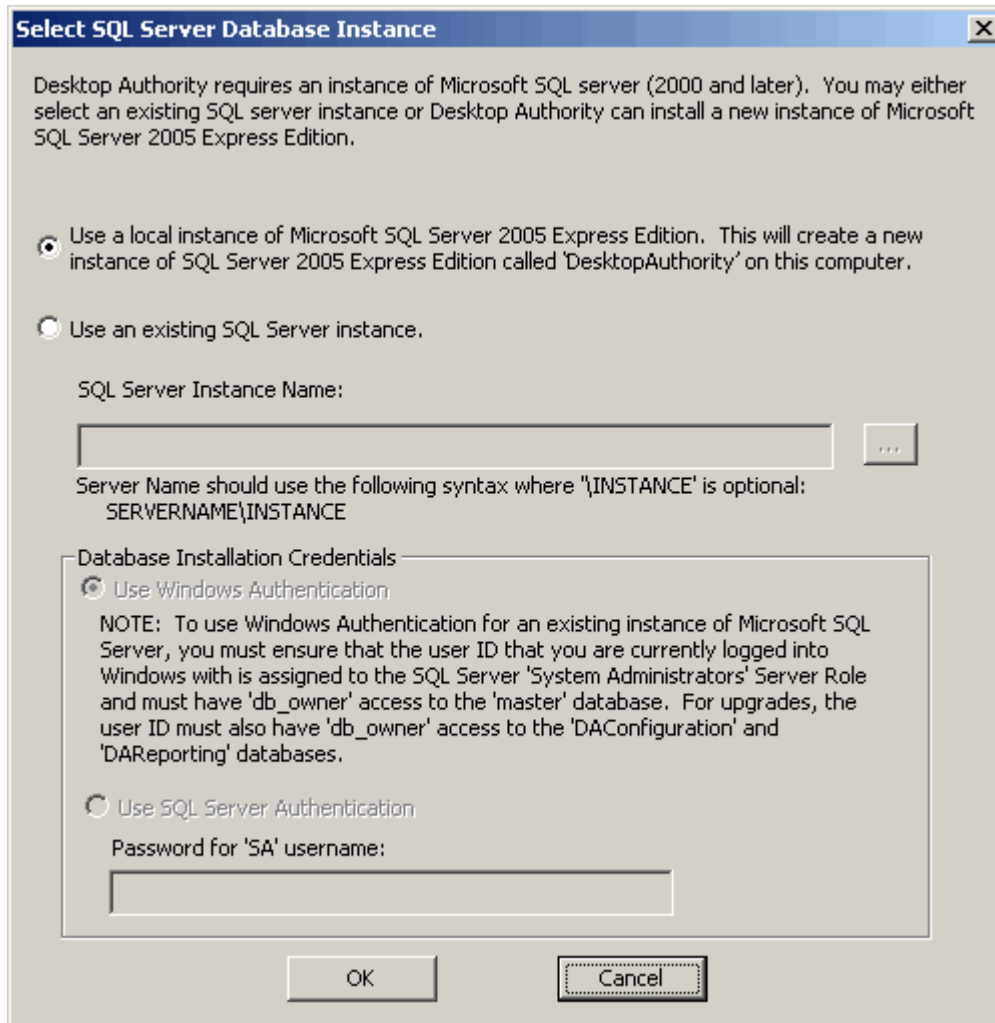
First the OpsMaster service will be configured. The older version of the service, if it exists will be stopped and removed. This service is a background service that is used to manage and configure Desktop Authority's plugins. These plugins are used to perform specific operations such as audit data collection 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. Click **OK** to continue.



17. Desktop Authority requires an instance of either Microsoft SQL or Microsoft SQL Server 2005 Express Edition. The database is used to store all configurations as well as a data collection repository for reporting. Desktop Authority can install a new instance of SQL Server 2005 Express or use an existing SQL Server instance. Select an option in the dialog.

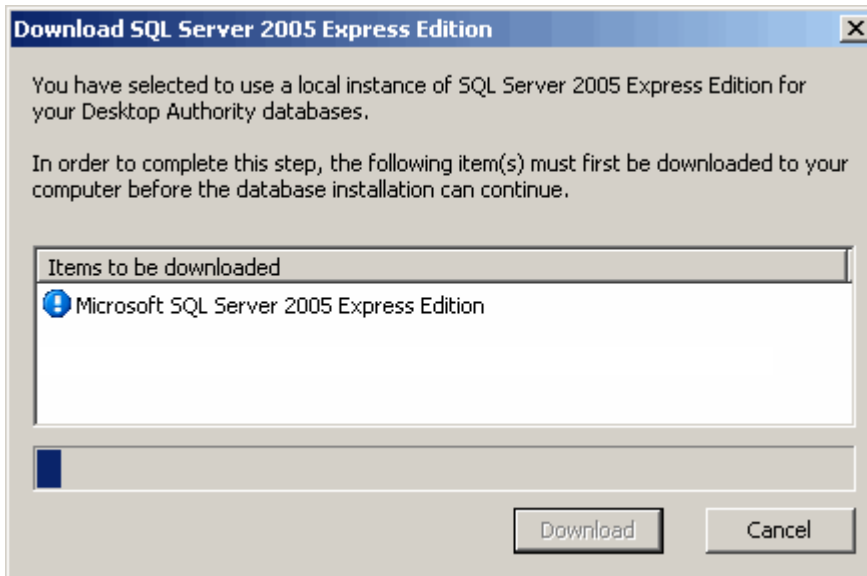
Note: Upgrade installations only require Database credentials to be entered.



When choosing to use an existing SQL Server instance, type in the SERVERNAME\INSTANCE or press the >Refresh List button to gather up existing instances for selection in the drop list. Select an authentication method for SQL Server.

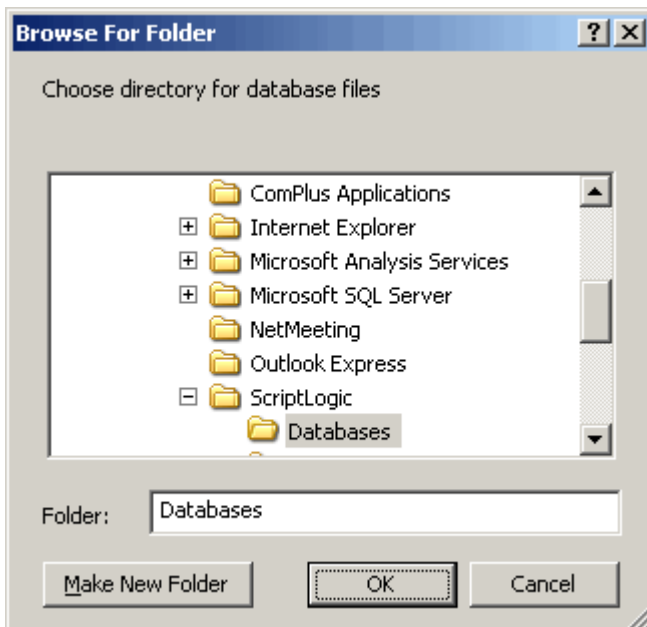
Click OK to continue. Click Cancel to exit the Desktop Authority configuration phase.

18. **New Installations Only:** If SQL Server 2005 Express Edition was selected to be used with Desktop Authority, it will now be downloaded and installed along with the Microsoft .NET Framework Version 2.0 Redistributable Package which is required by SQL Server 2005 Express.



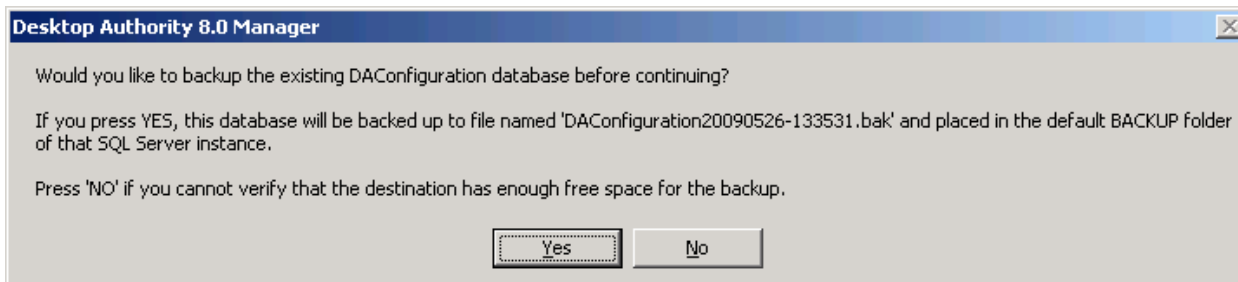
Click **Download** to start this process.

19. **New Installations Only:** Next, a folder must be selected to hold the database files. Locate and select a folder.



The default database location is *c:\Program Files\ScriptLogic\Databases*. Click **OK** to deploy and populate the database instances.

20. If an existing database is found, the installation will prompt you to back up the database before it is upgraded.



Two of these backup dialog boxes will appear. One for DAConfiguration and one for DAReporting. Click Yes to backup the existing databases. Click No to skip the backup procedure. Once this is complete, the existing databases will be upgraded.

21. Once the upgrade is complete, the Manager will start and the Desktop Authority Readiness Wizard will be opened. 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 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.

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. The option to upload a copy of the verbose trace file to a network repository may also be configured within the troubleshooting tab.

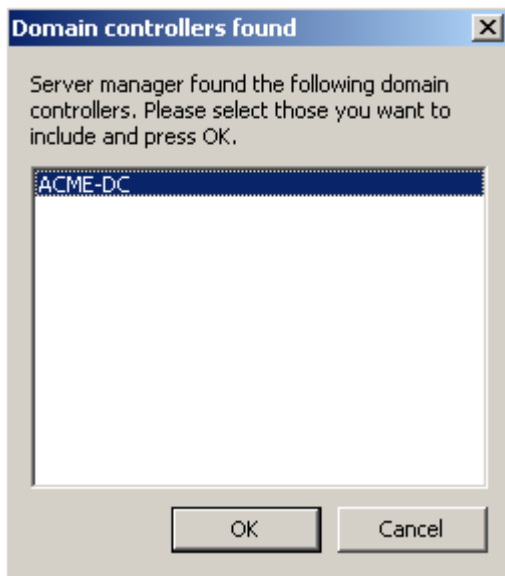
User Management Troubleshooting — User Management Troubleshooting is an optional part of the Desktop Authority deployment. It is used to troubleshoot problems arising from objects/elements that are being applied on client machines. When configured, verbose trace files will be written to each client's %temp% user temp folder. The option to upload a copy of the trace file to a network repository may also be configured 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.

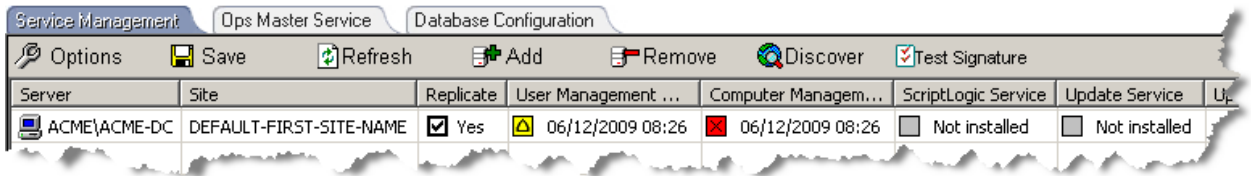
22. **Desktop Authority Readiness Wizard - Configure the Desktop Authority Services**
Configuring the ScriptLogic Service

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

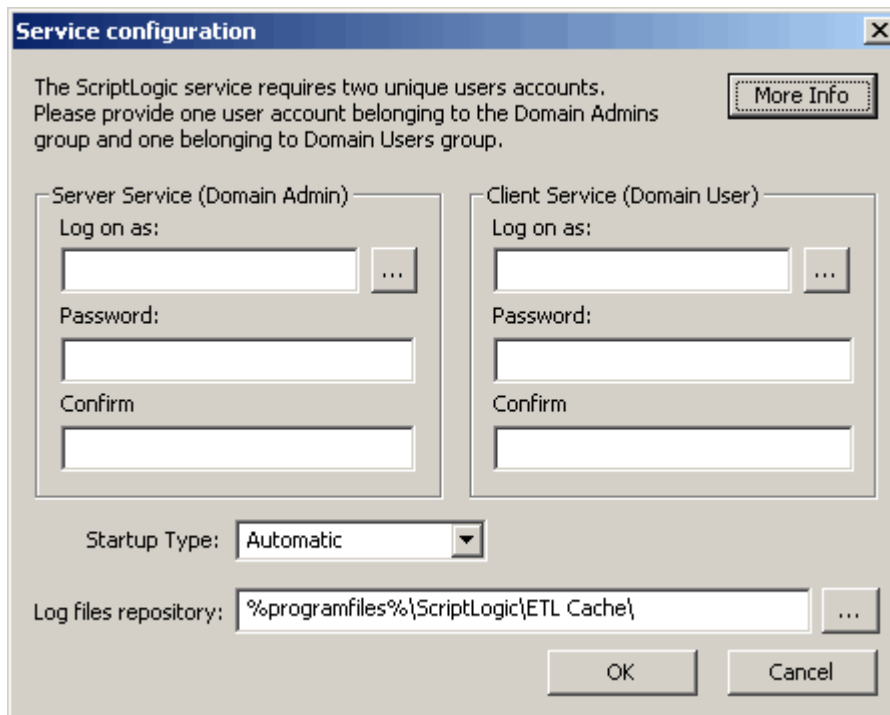
Click the Not Ready button to configure the necessary Desktop Authority services. The Server Manager dialog will be opened within the Desktop Authority Manager. The network will automatically be searched for available domain controllers. They will be presented, if found in a box similar to the one below.



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



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.



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: ...

Password:

Confirm:

Client Service (Domain User)

Log on as: ...

Password:

Confirm:

Startup Type: Automatic

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

OK Cancel

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.

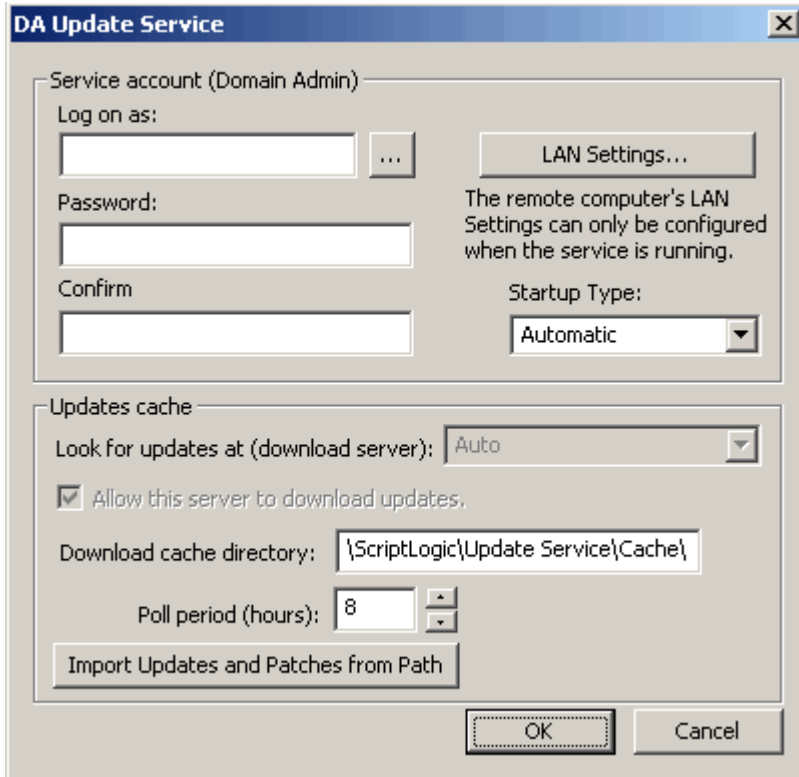
The Client Service account will be used by the ScriptLogic Client service on each workstation to perform the actual tasks that require the elevated administrative rights. This user account only needs to be a member of the Domain Users group. Installing this service to all domain controllers is the preferred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



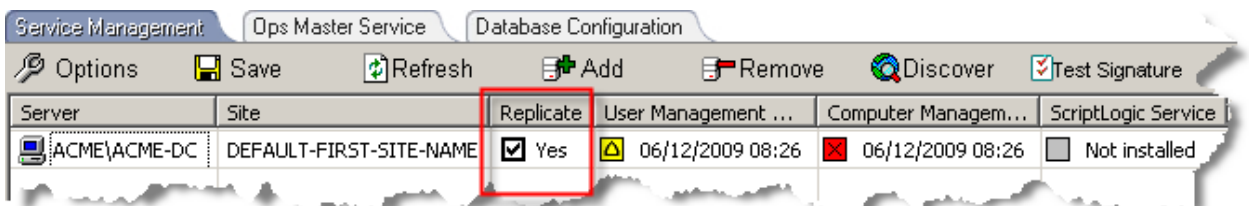
The Update service requires the use of a single user account. This user account must be a Local Administrator on the server where the Update service is being installed to.

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

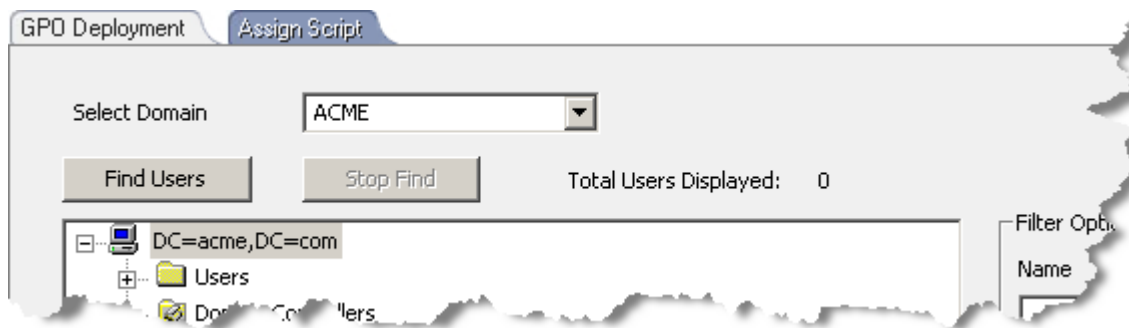
Replication is the act of publishing the configurations made in the Manager out to the network and available to the clients, users and computers, when necessary. By default, User Management configurations are pushed out to the NETLOGON share on specified domain controllers. Computer Management configurations 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.



23. **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.

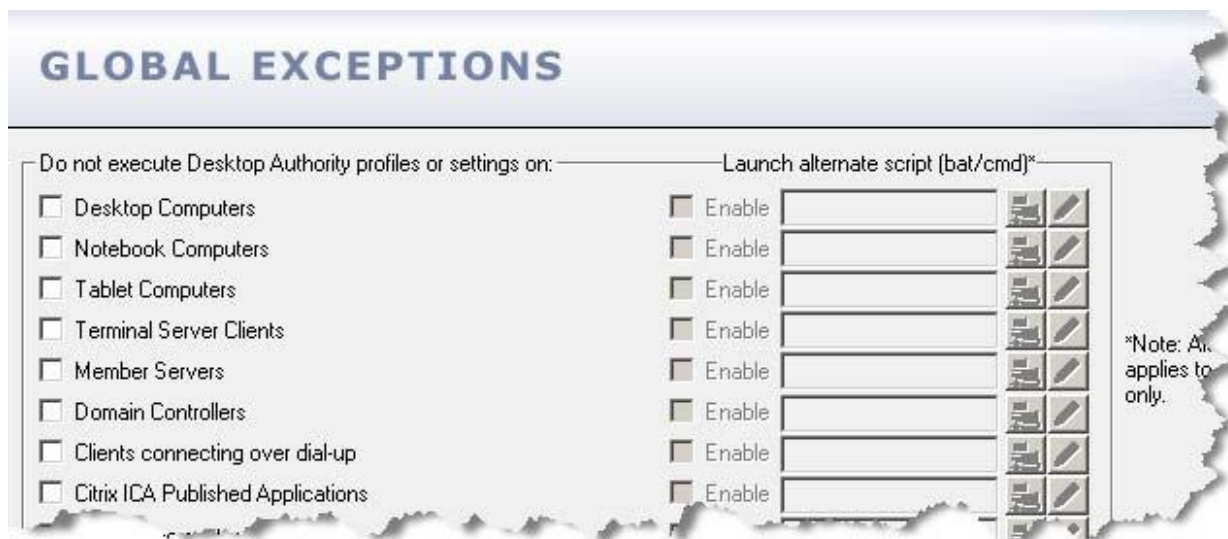
If the organization will be using User Management configurations, click on the Not Ready button to configure the Assign Script State. The Assign Script tab will be displayed in the Manager.



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.

24. **Desktop Authority Readiness Wizard - Configure Exceptions**

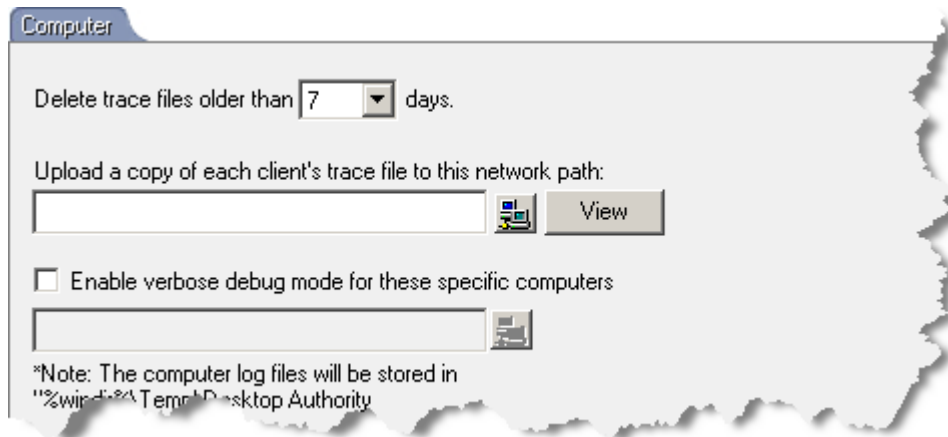
By default, Desktop Authority will be deployed to all computers in the targeted OU for GPO Deployment. Exceptions are used to exclude specific computers from being managed by Desktop Authority. This exclusion will specifically stop any Desktop Authority files from being installed to the specified computer.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



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.

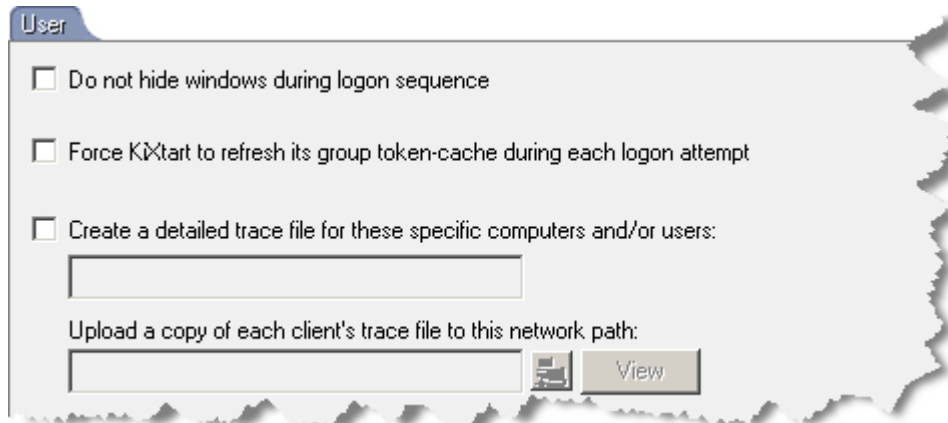
25. **Desktop Authority Readiness Wizard - Configure Computer Management Troubleshooting**

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.



26. **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.



27. 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.

28. Click **Finish** to complete the Readiness Wizard and begin exploring the Desktop Authority Manager. The Readiness Wizard can be restarted at any time by selecting it from the File menu.

Upgrade Installations

It is important to verify your Desktop Authority upgrade. Please take a few minutes to follow these verification steps:

While in Server Manager, press the **Options** button.

- Verify that the entry in Source Server matches the Computer Name of the machine Desktop Authority 8.0 is installed on. If not, update it to match the current Computer Name and press OK.

Expand the Profiles object in the Navigation pane.

- Verify that all profiles display properly and all elements are correct.
- Under each profile is a "Logging" object. Change the log file location if the path is no longer valid for each logging object under each profile. The data in this entry can be safely removed if logging is not desired.

Note: After the upgrade is verified and completed, go to the File menu and select Queue Update of Client Files. Click Yes on the message box. Now go back to the File menu and select Save Changes. Go back to the File menu once more and select Replicate All Files. The Save and Replicate process may also be accomplished by using the toolbar Save button and the Replicate button. Once the replication process is complete, go to the View menu and select Replication Log. You will see the names of the files that Desktop Authority replicated to the selected domain controller(s).

Desktop Authority requires deployment of its Group Policy Client Side Extension. This policy will deploy the necessary SL Client Service, SLAgent and Computer Management service to clients.

- Select Client Deployment from the Deployment Options on the Navigation menu. From the GPO Deployment tab, click Add to configure the deployment of Desktop Authority Client components to computers within selected Organizational Units (OUs).

Data Collection must be configured after upgrading to Desktop Authority 8.0. In prior versions the default was to automatically collect all data. This version of DA allows you to configure which data you prefer to collect.

- Data Collection is configured as an object within defined profiles. This way you can specify when the data collection should occur and what type of data should be collected.

REGISTRATION

If no registration code was entered at the time Desktop Authority was installed, you must register your product to remove the evaluation time period. A registration code is provided at the time of purchase. All configurations made during the evaluation period are immediately available after the registration key code is entered. You can continue all administrative functions immediately.

Enter the provided registration key code by selecting Product Registration from the Help menu or select the Desktop Authority Registration program in the ScriptLogic program group from your Windows Start menu. The following dialog box opens:

Desktop Authority Version 8 Registration

DESKTOP AUTHORITY
REGISTRATION

Copyright 1997 - 2009 ScriptLogic Corporation

Name

Company

Key

Register Cancel Browse...

Fill in the following entries on the registration dialog box:

Name

Enter the Name that Desktop Authority is registered with. Make sure to type this information carefully. This entry is case-sensitive and must be the same name it was purchased with.

Company

Enter the Company that Desktop Authority is registered with. Make sure to type this information carefully. This entry is case-sensitive and must be the same company name it was purchased with.

Key

Enter the registration key supplied at the time of purchase.

Click **Register** after entering the above information. If any of the above fields are incorrect, you will be prompted with an appropriate message.

If you have been supplied with a copy of a register.ini file, click Browse to locate it. If chosen, the register.ini file will automatically fill in the Name, Company and Registration Key entries.

If all registration data is entered and verified to be correct, you are prompted to replicate the change to the domain controllers. Click **Yes** to replicate the registration data or No to replicate the data at a later time. The registration process does not become effective until the data is replicated.

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

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

OPTIONAL COMPONENTS**Spyware Detection and Removal option (not available in Desktop Authority Express and Desktop Authority System Center Edition)**

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.

**Patch Deployment for Desktops option (not available in Desktop Authority Express and Desktop Authority System Center Edition)**

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.

**USB/Port Security option (not available in Desktop Authority Express and Desktop Authority System Center Edition)**

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.

Desktop Authority helps the enterprise control this problem by introducing USB/Port Security. USB/Port Security is an optional add-on that enables the enterprise to restrict users and/or groups from using specified types of removable storage devices by restricting access to them. By creating rules within Desktop Authority, a permanent access control list is made available for all portable devices and is configured on each computer that matches the defined Validation Logic.

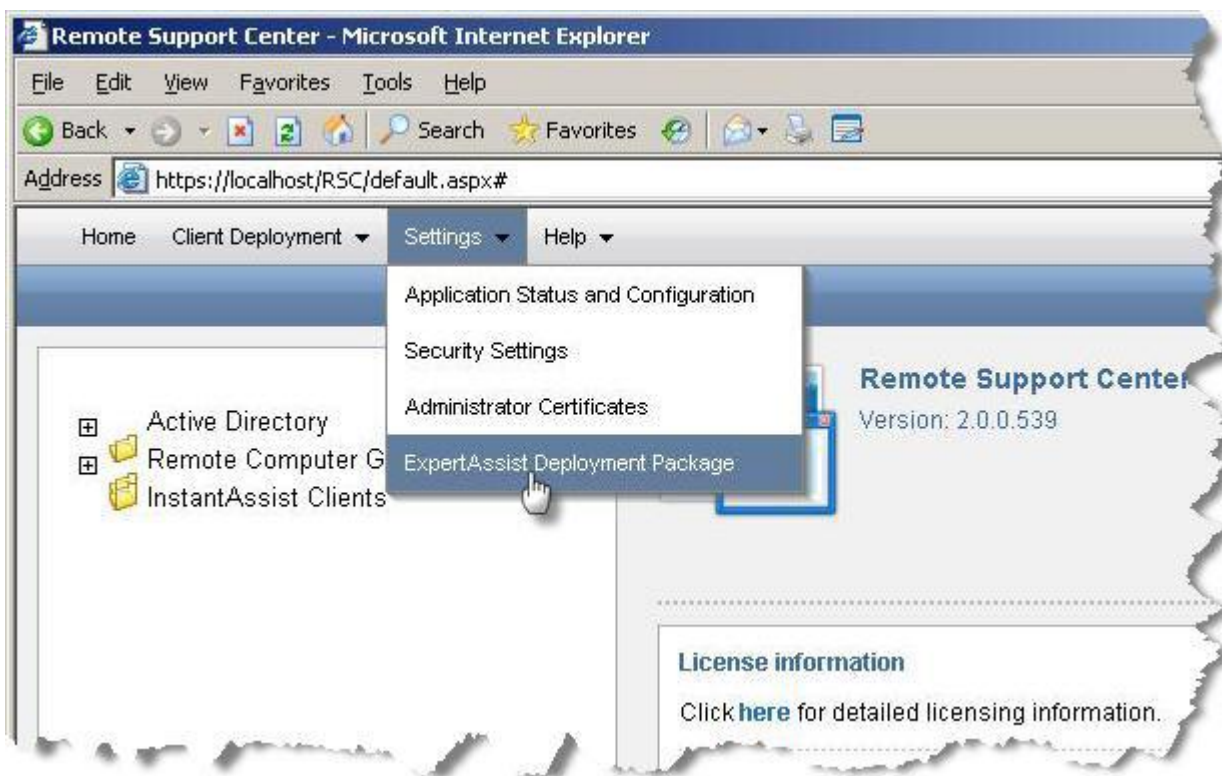
APPENDIX A: USING REMOTE SUPPORT CENTER WITH DESKTOP AUTHORITY

Beginning with Desktop Authority 8.0, Administrators will be able to download our exclusive Remote Support Center console. Remote Support Center (RSC) is a comprehensive console designed as an alternative to the remote management console in Desktop Authority. It was designed to enable designated network administrators and helpdesk specialists manage and remote control computers regardless of location.

Remote Support Center is available for download from the ScriptLogic Download Center to enterprises that have a current maintenance plan. RSC will be licensed for the same number of seats as is owned for Desktop Authority. RSC Internet Gateway and InstantAssist Technician licenses may be purchased separately.

After downloading and installing RSC, Desktop Authority can be configured to work directly with RSC. By doing this, RSC will replace the default Desktop Authority Remote Management console.

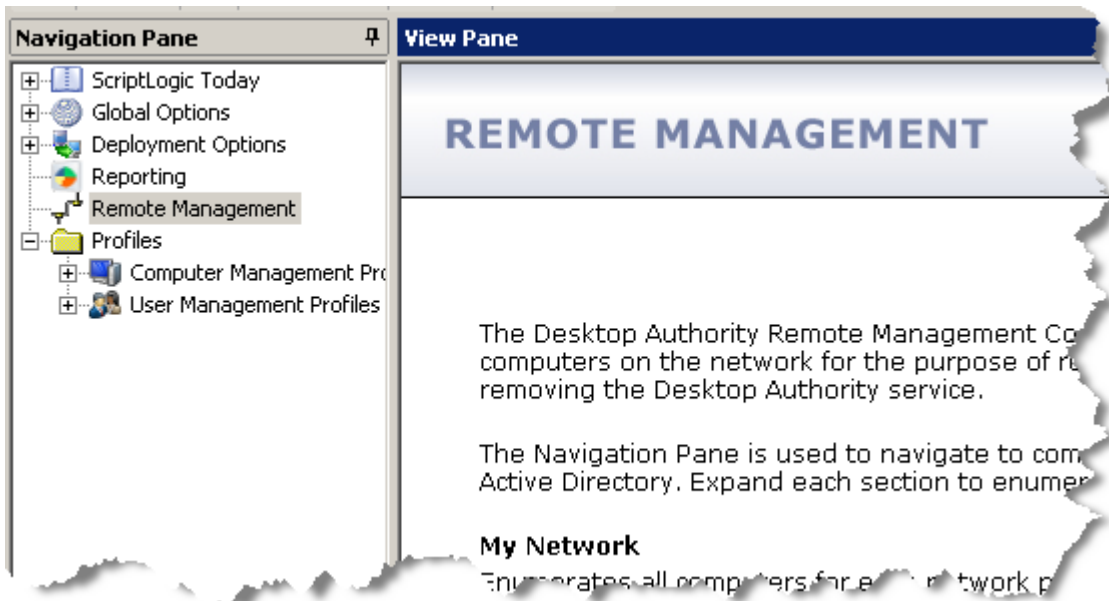
1. Within RSC, select the *Settings > ExpertAssist Deployment Package* menu item. Click on the Download button from the pop up dialog.



2. Copy the saved ExpertAssist Download Package (RSCClient.exe) to the %ProgramFiles%\ScriptLogic Manager\DesktopAuthority folder on the computer where Desktop Authority is installed to.

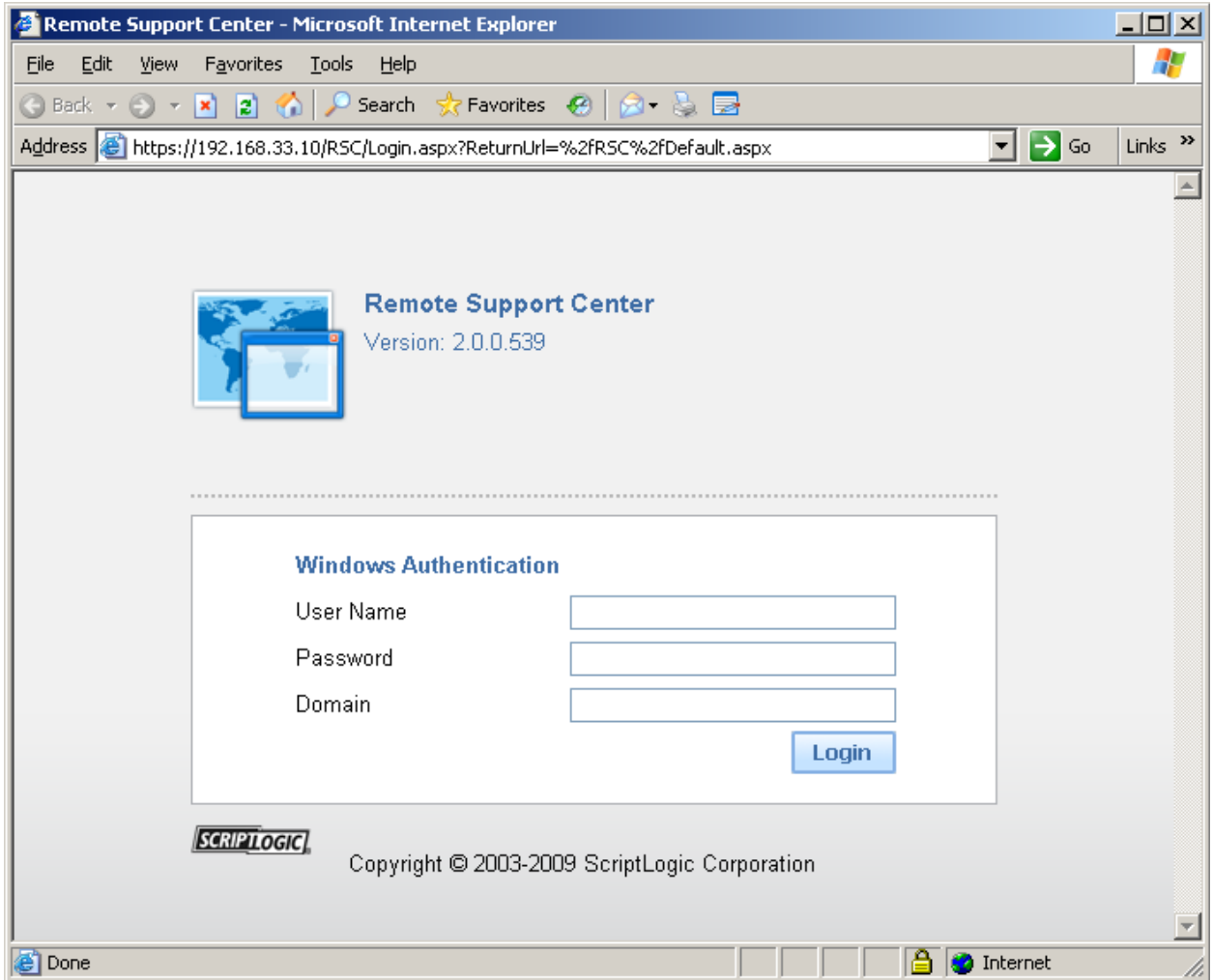
3. Start the Desktop Authority Manager. If the Manager was already running prior to copying this package, restart the Manager.

The Navigation Pane will look similar to the following screen. The Remote Management tree node will have no + icon to the left as it did prior to the placement of the new RSCClient.exe file.



4. Clicking on Remote Management will now automatically load the Remote Support Center console into a new browser window.

If DA and RSC are installed on the same server, the IP address of the server will have to be added as an IP Filter in Remote Support Center, otherwise RSC will reject the computer.



INDEX

	B		O
Backup, 9		Optional Components, 28	
	D		R
Desktop Authority Folders, 8		Register Desktop Authority, 26	
Desktop Authority Version Comparison, 7		Registration, 26	
	F		S
Folder Structure, 8		System Requirements, 5	
	I		T
Installation, 10		Technical Support, 4	
	M		V
Making a backup, 9		Version Comparison, 7	