



PATCH AUTHORITY ULTIMATE™

ScriptLogic®
Patch Authority Ultimate™ 5.9
Agent Quick Start Guide

© 2007 by ScriptLogic Corporation

All rights reserved.

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 Patch Authority Ultimate 5.x. 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

Patch Authority and the ScriptLogic logo are trademarks of ScriptLogic Corporation.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

All other trademarks, tradenames, or images mentioned herein belong to their respective owners.

Printed in the United States of America (7/2007)

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.

Contents

PREPARING TO USE PATCH AUTHORITY ULTIMATE AGENT	1
WELCOME	1
SET UP A DISTRIBUTION SERVER.....	1
CONFIGURE PATCH AUTHORITY ULTIMATE AGENT OPTIONS	2
<i>On the General tab</i>	2
<i>On the Patch tab</i>	2
<i>On the Installation tab</i>	3
PUSH THE AGENT CONFIGURATION TO THE DISTRIBUTION SERVER.....	3
DOWNLOAD THE PATCH FILES (OPTIONAL)	3
INSTALLING AGENTS	4
HOW TO INSTALL PATCH AUTHORITY ULTIMATE AGENT FROM THE CONSOLE	4
MANUALLY INSTALLING AGENTS	5
<i>Create the installation media</i>	5
<i>Manually install the agent service on a target machine</i>	6
MONITORING AGENTS.....	7

Preparing To Use Patch Authority Ultimate Agent

WELCOME

This document provides a roadmap of tasks you must perform when preparing to use Patch Authority Ultimate Agent. For more detailed information see the online Help system or the *Patch Authority Ultimate Administration Guide*.

All agents are configured on the console and then either “push installed” to the desired target machines or manually installed via CD or flash memory. All agents deployed by a console contain the exact same set of configuration options.

Note: ScriptLogic Corporation recommends using SQL Server with Patch Authority Ultimate Agent. You can use the default JET database for very small installations and when first getting started with Patch Authority Ultimate Agent, but SQL Server is recommended for long term use.

SET UP A DISTRIBUTION SERVER

You must set up a distribution server that the patch agents can periodically access to download various files. What you store on the distribution server is dependent on what type of network access the agents have. If the agents have Internet access then you simply need to configure it so that the agents periodically download the agent configuration from the distribution server. If the agents do not have Internet access they won't be able to download the latest scan engines, XML data files, and patch files from the default Web sites. In this case you will also need to store these additional files on the distribution server for the agents to access.

1. Select **Tools > Distribution Server**.
2. Click **New** and configure the distribution server.

In the top half of the **Configure Distribution Server** dialog box be sure to specify a location and authentication method that all the agents can use when accessing the server. The lower half of the dialog is used to specify how the console will connect to this same location on the distribution server. Although the physical location you specify must be the same in both halves of the dialog, in the top half you can specify the method used by the agents when accessing the data (**UNC** vs. **Anonymous HTTP** vs. **Authenticated HTTP**).

3. Define which target machines will use the distribution server by assigning the IP addresses of the target machines to the distribution server.

To do this, select the **IP Ranges** tab, click **New** and define a distribution server group. For additional information, press **F1** to access the associated Help topic.

4. If the agent machines do not have Internet access, select the **Synchronize** tab, select the desired distribution server and click **Synchronize Engines and XML**.

This will copy the latest scan engines and XML data files from the Patch Authority Ultimate console to the distribution server. The agents will download these files from the distribution server rather than from the Web.

See *Configuring Distribution Servers* in the online Help for more detailed information on configuring a distribution server.

CONFIGURE PATCH AUTHORITY ULTIMATE AGENT OPTIONS

Select **Agents > Patch Authority Ultimate Agent Settings** and then doing the following:

On the General tab

- In the **Engine and catalog XML download locations** section, if the agent machines do not have Internet access, specify the distribution server they will use to download the latest scan engines and XML data files.
- In the **Download location for settings** section, specify the distribution server the agents will look to for updated agent configurations.

See *Configuring General Options for Agents* in the online Help for more detailed information about the options on this tab.

On the Patch tab

- Enable the **Enable Patch Scanning** check box.

Note: If this check box is cleared each agent will not be able to scan its machine for missing patches; if this is your intent you can skip this tab.

- If you want to automatically deploy patches that are missing, enable the **Deploy Approved Patches using this deployment template** check box. On the patch deployment template you specify, if the agent machines will download missing patches from a distribution server rather than from the vendors, make sure the **Deploy patches via Distribution Servers** check box is enabled. See *Deployment Template: Distribution Servers tab* in the online Help for more information.

- Click **Select Approved Patches** and select the patches you want in the list.

Note: If the **Select Patches** dialog is empty, cancel out of this step, select **Tools > Refresh Files** and then try again.

- Specify the distribution server you want to copy the Approved Patches list to, and then click **Update Distribution Server(s)** to copy the list to the server.

See *Configuring Patch Agents* in the online Help for more detailed information.

On the Installation tab

Click **Set Installation Password** and specify the password that will be used when authenticating the installation of the agent on each machine.

PUSH THE AGENT CONFIGURATION TO THE DISTRIBUTION SERVER

On the **Agent Settings** dialog, click **Update Agent Settings**. This will:

- Generate the agent configuration file
- Copy the configuration file to the distribution server(s)

DOWNLOAD THE PATCH FILES (OPTIONAL)

If the deployment template you choose specifies the use of distribution servers for downloading patches, then you should download the patch files for the approved patches. You can download patches and service packs and push them to the distribution servers using the **Synchronize Download Center** button (see *Synchronizing Servers* in the online Help). If your deployment template does not specify the use of distribution servers, then the agents will download the patches directly from the vendor Web sites.

Installing Agents

HOW TO INSTALL PATCH AUTHORITY ULTIMATE AGENT FROM THE CONSOLE

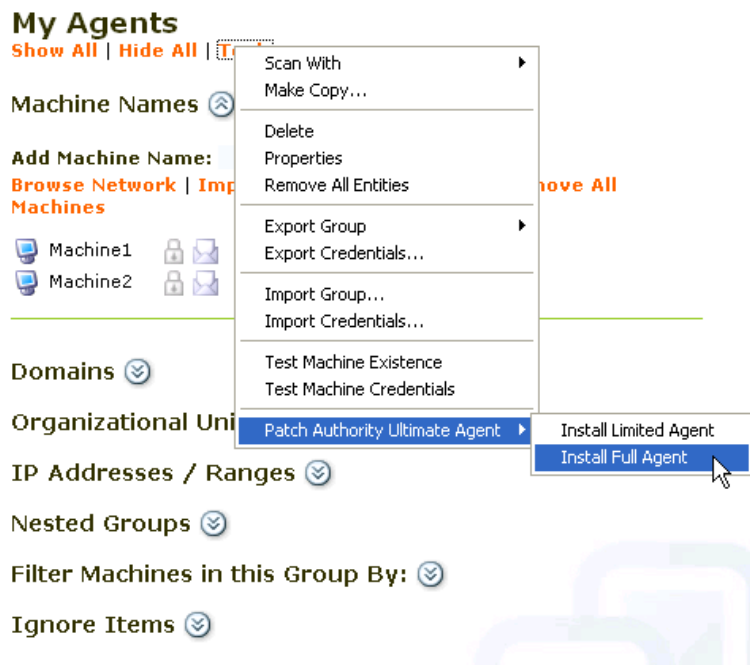
You can use the console to "push install" the Patch Authority Ultimate Agent service to connected target machines. Some target machines may have a firewall enabled that blocks the incoming ports required to install Patch Authority Ultimate Agent. On these machines you must manually install Patch Authority Ultimate Agent. See *Manually Installing Agents* for details.

Note: Each target machine must have a network connection to the console during the Patch Authority Ultimate Agent installation. This connection is required in order to exchange security information that will be used to establish an encrypted link for all future communication between the console and its agents.

The most straightforward way to install the Patch Authority Ultimate Agent service on all the desired connected machines is to:

1. Create a machine group that contains all the machines that will run agents.
2. While viewing the machine group, select **Tools > Patch Authority Ultimate Agent > Install**.

For example:



You can also install the Patch Authority Ultimate Agent service a number of other ways from the console.

- By using the **Machines > Patch Authority Ultimate Agent** menu.
- While viewing the list of managed machines (accessed via the **Tools > Manage Machines** menu) by right-clicking the selected machines and selecting **Patch Authority Ultimate Agent > Install**.
- From the **Patch Authority Ultimate Agent** tab of the **Edit Machine Properties** dialog.
- By right-clicking a machine group within the **Scan What** list and selecting **Patch Authority Ultimate Agent > Install**.
- By right-clicking a scan within the **Today's Items**, **Recent Items**, or **Archive Items** list and then selecting **Patch Authority Ultimate Agent > Install**. This will install the Patch Authority Ultimate Agent service on all of the machines that were successfully scanned in that scan.

The following occurs when you push install the Patch Authority Ultimate Agent service on a machine:

- The **Patch Authority Ultimate Agent Status** dialog is displayed and shows the status of the installation request.
- Once the Patch Authority Ultimate Agent configuration is successfully installed on a target machine, the agent is automatically started on the machine.
- You can verify the installation was successful by accessing the **Edit Machine Properties** dialog and selecting the **Patch Authority Ultimate Agent** tab.
- After an agent is installed on a machine, that machine becomes a managed machine.

MANUALLY INSTALLING AGENTS

You must manually install Patch Authority Ultimate Agent on machines that are guarded by a firewall.

Note: You must configure Patch Authority Ultimate Agent before it is installed.

Create the installation media

On the Patch Authority Ultimate console select **Agents > Patch Authority Ultimate Agent Settings**.

1. Select the **Installation** tab.
2. Specify the location of the output directory (the directory that will be used to store the installation files).

3. Verify the port number.
4. Click **Set Installation Password** and specify a password.
5. Click Generate Agent Installation Files.

There will be a pause while the files are generated and copied to the output directory. After the files are generated they can optionally be copied to a CD or to a flash drive.

Manually install the agent service on a target machine

1. Log on using an administrator account.
2. If necessary, insert the CD or flash drive containing the agent installation files and copy the installation files to the target machine.
3. Double-click the file named **AgtInstallerX.exe**.
4. When prompted, type the installation password.

The agent installation routine will connect to the console to:

- Establish a security association for encrypting communications
- Acquire an agent license
- Retrieve the latest agent configuration parameters

The agent installation routine will then download the latest scan engines and XML data files from the assigned distribution server or from the Web (as defined by the agent configuration parameters). When the download is complete the agent will be started automatically.

You can check the status of the agent using the Patch Authority Ultimate Agent client program, available by selecting **Start > All Programs > ScriptLogic Corporation > Patch Authority Ultimate Agent**. You can use this program to configure any settings that were marked as user-configurable.

Monitoring Agents

While you cannot watch the actual scans and deployments as they are performed by agents on each target machine, you can monitor what is happening on each machine by using the following tools:

- Machines that have successfully installed Patch Authority Ultimate Agent will display the *Agents Installed* icon in the Managed Machines table. This table also displays the time of the last agent check-in and the time of the last patch scans. See *Determining Which Machines Have Agents* in the online Help for more information.
- Use the **Patch Authority Ultimate Agent** tab on the **Edit Machine Properties** dialog to see how Patch Authority Ultimate Agent is currently configured on a machine.

See *Accessing Machine Properties* in the online Help for information on accessing the **Edit Machine Properties** dialog.

- Use the **Show Agent Log** button on the **Patch Authority Ultimate Agent** tab of the **Edit Machine Properties** dialog to view the Patch Authority Ultimate Agent history log on the machine. The history log will show information about the scans that were performed.

Note: The log file will not be available if the machine is not currently connected to the network or is blocked by a firewall.

- Scans and patch deployments performed by an agent will be reported to the console and will appear in the **Today's Items** list. For example:

