Connector Administrator Guide

Version 2.9
June 17, 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-22628-03

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Connector Administrator Guide

CONTENTS

Preface v

Audience v

Conventions v

Obtaining Documentation and Submitting a Service Request vi

Getting Started with Connector 1-1

Overview 1-1

Basic Operations 1-1

Choosing a Connector Mode and Authentication Key Type 1-2

Deployment Scenarios 1-3

Company Authentication Key and Active Directory 1-3

Group Authentication Key 1-3

User Authentication Key 1-4

Summary 1-5

Authentication Process 1-5

Groups and Policy Application 1-6

Deriving User Data 1-6

Applying Policy to Groups 1-6

Installing Connector on Windows 2-1

Overview 2-1

Windows System Requirements 2-1

Pre-Installation Requirements 2-2

Installing in Standalone Mode 2-3

Post-Installation Firewall Configuration 2-12

Adding Host Exceptions 2-12

Installing in Enterprise Mode 2-16

Post-Installation Proxy Server Configuration 2-24

Configuring Microsoft Forefront TMG or ISA Server 2-24

Post-Installation Forefront TMG or ISA Server Configuration 2-31

Enabling Persistent ICAP Mode 2-32

Applying the Windows Registry Patches 2-32

Bypassing the Web Scanning Services 2-32

Upgrading Connector 2-33

Removing Connector 2-33

Installing Connector on Linux 3-1

Overview 3-1

Linux System Requirements 3-1

Pre-Installation Requirements 3-2

Accessing Your Server 3-3

Installing the Runtime Environment 3-4

Installing Connector 3-5

Increasing the Open Files Limit 3-5

Running the Installer 3-6

Basic Connector Operations 3-6

Configuring Connector 3-6

Applying an Exception 3-7

Upgrading Connector 3-8

Configuring Connector 4-1

Overview 4-1

Web Browser Configuration 4-1

Manual Configuration 4-2

Proxy Auto-Config File 4-2

Web Proxy Auto-Discovery Protocol 4-2

Connector Host and Client on the Same Computer 4-3

Host Exceptions 4-3

Example Host Exceptions 4-3

Acceptable Usage Policy 4-4

SSL Tunneling 4-6

LDAP Servers 4-6

Generic LDAP 4-6

Novell 4-7

Lotus Domino 4-7

Secondary LDAP Server 4-7

Multiple LDAP Servers and Domains 4-8

Groups 4-9

Multiple Authentication Keys 4-9

Excluding Groups 4-9

Global Group Exclusions 4-9
LDAP Group Exclusions 4-10
Nested Groups 4-10

Agent Properties A-1

Proxy Auto-Config Files B-1
Overview B-1
How PAC Files Work B-1
PAC File Deployment B-2
Basic PAC File Examples B-2
Example PAC File B-3
Manually Configure a Browser to Use a PAC File B-3
Windows Network Share Hosted PAC Files B-3

Web Proxy Auto Discovery Protocol C-1
Overview C-1
How WPAD Works C-1
WPAD using DHCP C-1
WPAD using DNS C-2
Manual Browser Configuration for Windows Clients C-2
Deploying WPAD with Windows Server C-2
Configure Internet Information Services C-3
Create an Option 252 Entry in DHCP C-3
Enable Option 252 for a DHCP Scope C-3
Active Directory and Group Policy Objects C-4

Installing Linux D-1
Overview D-1
Obtaining Linux Installation Media D-1
Red Hat Enterprise Linux 5 D-1
CentOS Linux 5 D-1
Installing Linux D-2
Post-Installation Configuration D-12
Troubleshooting D-16

GLOSSARY

INDEX

Preface

Revised: July 15, 2010

This preface describes the audience and conventions of the *Connector Administrator Guide*. It also described the available product documentation and provides information on how to obtain documentation and technical assistance.

- Audience
- Conventions
- Obtaining Documentation and Submitting a Service Request

Audience

This guide is intended for primarily for network administrators and channel partners.

Conventions

This guide uses the following conventions:

Item	Convention
Commands and keywords.	**boldface** font.
Variables for which you supply values.	*italic* font.
Optional command keywords. You do not have to select any options.	[enclosed in brackets]
Required command keyword to be selected from a set of options. You must choose one option.	{options enclosed in braces | separated by a vertical bar}
Displayed session and system information.	`screen` font.
Information you enter.	**`boldface screen`** font.
Variables you enter.	*`italic screen`* font.
Menu items and button names.	**boldface** font.
Choosing a menu item.	**Options > Network Preferences**

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means the described action saves time. You can save time by performing the action described in the paragraph.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

CHAPTER 1

Getting Started with Connector

Revised: July 15, 2010

Overview

This chapter will help you decided when to deploy Connector and the most appropriate deployment method for your network infrastructure. Connector is used to deliver web traffic from a client computer to Cisco's Web Scanning Services. You may not need to use Connector. It is required in the following configurations only:

- When user-level granularity is required for policy and reporting.
- When accessing the Web Scanning Services from a device with a dynamic IP address.
- When accessing the Web Scanning Services off-site or with a roaming device without Anywhere Plus installed.

Basic Operations

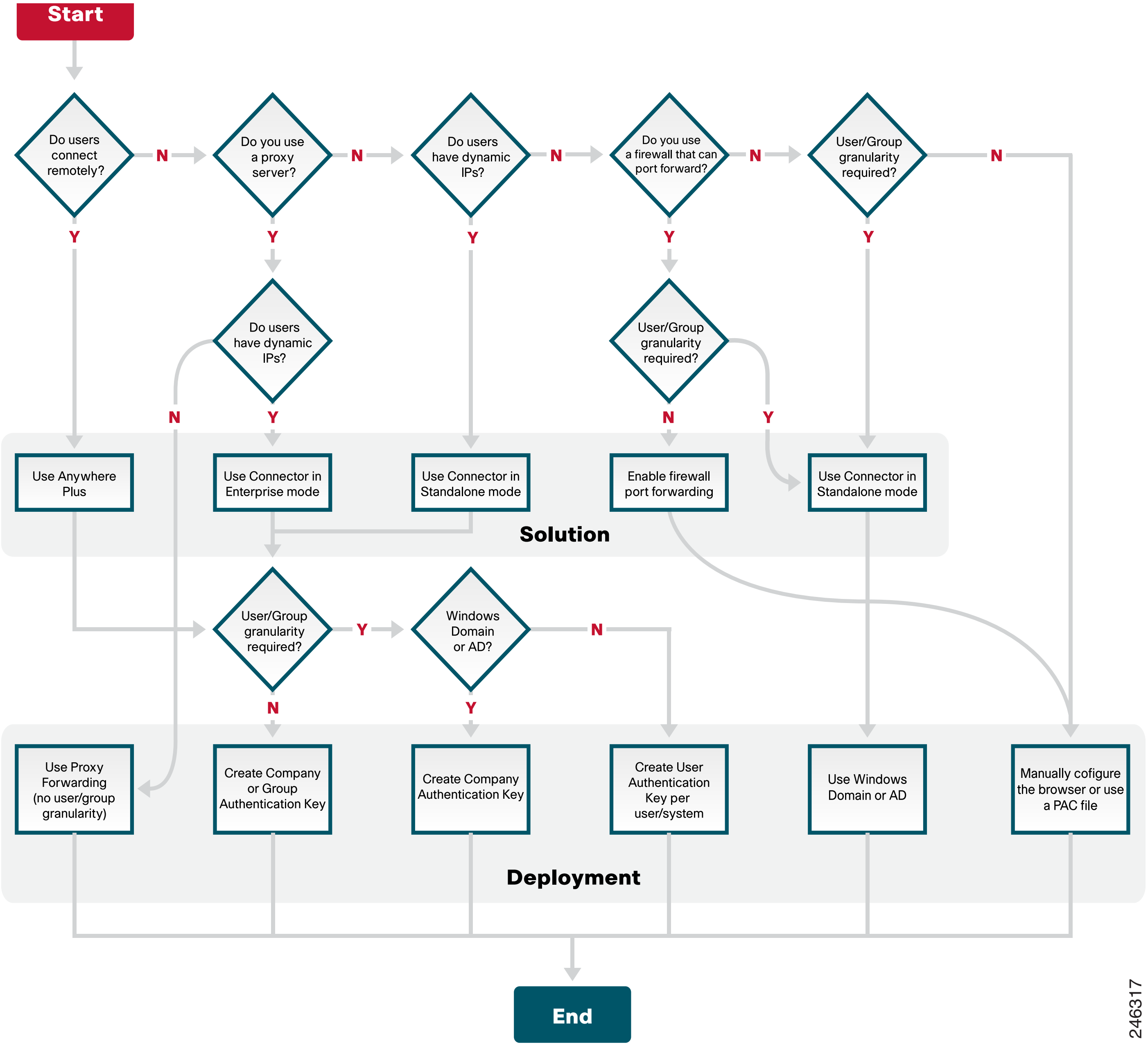
Connector identifies users by merging their details from Active Directory using LDAP, or Windows Domain integration and an authentication key. With Connector, users with a dynamic IP address can connect to the Web Scanning Services with a company, group, or user authentication key. Users with a static IP address do not require a key.

Connector encrypts user information which the Web Scanning Services uses to apply specific user or group policy information. Connector passes user web traffic requests through the Web Scanning Services for filtering, scanning, and policy enforcement, before providing the cleansed web content to the user.

Company, Group, and User authentication keys are created in ScanCenter. These enable the Web Scanning Services to identify and authenticate a user. Group authentication keys provide more detailed user behavior reporting and policy management, but may require additional key management by the administrator.

Choosing a Connector Mode and Authentication Key Type

Before installing Connector, use the following flow chart to decide the Connector mode (standalone or enterprise) and Authentication Key (Company, Group, or User) are most appropriate for your organization.


Start
Do users connect remotely?
N
Do you use a proxy server?
N
Do users have dynamic IPs?
N
Do you use a firewall that can port forward?
N
User/Group granularity required?
N
Y
Y
Y
Y
Y
Do users have dynamic IPs?
User/Group granularity required?
N
Y
N
Y
Use Anywhere Plus
Use Connector in Enterprise mode
Use Connector in Standalone mode
Enable firewall port forwarding
Use Connector in Standalone mode
Solution
User/Group granularity required?
Y
Windows Domain or AD?
N
N
Y
Use Proxy Forwarding (no user/group granularity)
Create Company or Group Authentication Key
Create Company Authentication Key
Create User Authentication Key per user/system
Use Windows Domain or AD
Manually cofigure the browser or use a PAC file
Deployment
End
246317

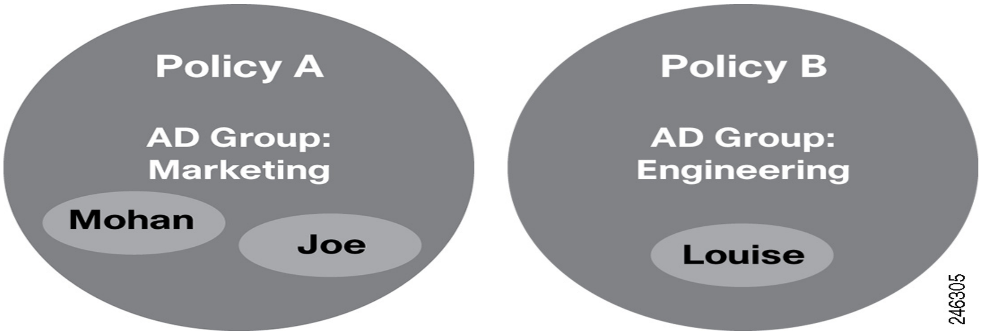
Deployment Scenarios

When you have chosen your appropriate solution and deployment method, based on your network infrastructure, you are ready to proceed. The flow chart provides for a variety of deployment scenarios, but in practise the three most common are:

- Company authentication key and Active Directory
- Group authentication key
- User authentication Key

Company Authentication Key and Active Directory

The most common scenario uses a single company authentication key for all users in the organization and Active Directory to provide User and Group granularity for policy and reporting. An example is shown below.



To create this configuration:

Step 1 Create two Active Directory groups in ScanCenter:

- WinNT://…/Marketing
- WinNT://…/Engineering

Step 2 Install Connector and the company authentication key on the Domain Controller.

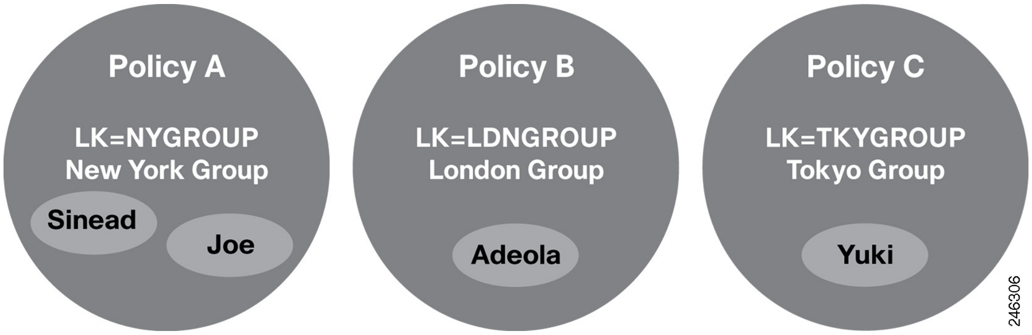
Step 3 Apply Policy A to the Marketing group and Policy B to the Engineering group.

In this scenario, Policy A is applied to Mohan and Joe, while Policy B is applied to Louise.

If a policy causes a block event for Mohan or Joe, it will be registered against WinNT://.../Marketing with User information for Mohan or Joe. Block events for Louise, it will be registered against WinNT://.../Engineering with her user information.

Group Authentication Key

The next most common scenario uses a group authentication key without Active Directory. In the following example, Connector is installed in standalone mode with a location-based key (LK), a unique group authentication key, in each of three branch offices.



To create this configuration:

Step 1 Create a group authentication key for each location group (NYGROUP, LDNGROUP, TKYGROUP).

Step 2 Install Connector in standalone mode and the relevant group authentication key at each location.

Step 3 Apply Policy A to group NYGROUP, Policy B to LDNGROUP, and Policy C to TKYGROUP.

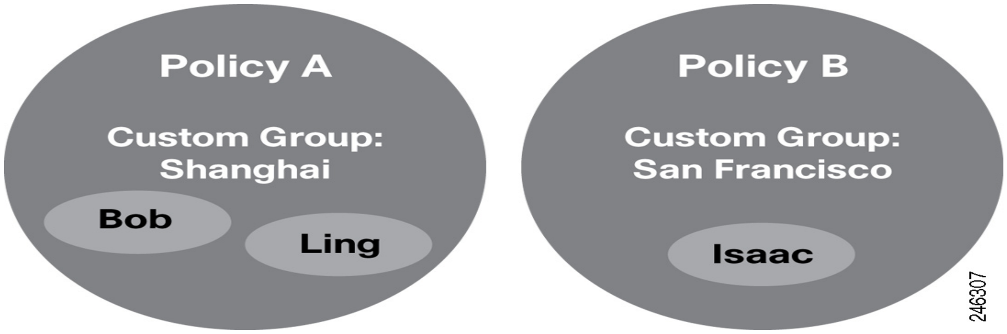
In this scenario, Policy A is applied to Sinead and Joe, Policy B is applied to Adeola, and Policy C is applied to Yuki.

If a policy causes a block event for Sinead or Joe, it will be registered against NYGROUP group. Block events for Adeola, it will be registered against the LDNGROUP group. Block events for Yuki will be registered against TKYGROUP.

Note This deployment method is suitable only when Active Directory is not used.

User Authentication Key

This scenario provides an alternative off-site solution when it is not possible to deploy Anywhere Plus or Passive Identity Management. For example, it could be used for non-Windows users. In the following example, Connector and a user authentication key are installed on each user's computer.



To create this configuration:

Step 1 Create a custom groups and assign users to those groups in ScanCenter.

Step 2 Create a user authentication key for each user in ScanCenter.

Step 3 Install Connector in standalone mode and a unique user authentication key on each computer.

In this scenario, Policy A is applied to Bob and Ling and Policy B is applied to Isaac. If a policy causes a block event for Bob, Ling, or Isaac it will be registered against their User and Custom Group.

⚠ **Caution** The user authentication key overrides all reported user information. Therefore you must deploy the key only once with a separate Connector installation for each computer.

Summary

When Active Directory is in use, a company key installed with Connector in standalone or enterprise mode on the Domain Controller will provide user and group granularity for policy and reporting.

If you have satellite offices where you want to apply group policy you should use a group authentication key.

For portable computers or remote connections where Anywhere Plus or Passive Identity Management are not viable, a user authentication key and a local installation of Connector in standalone mode should be used.

Authentication Process

Connector uses one of several possible authentication resources to annotate web requests with end-user data. The supported data sources are:

- Active Directory (using the LDAP protocol)
- Windows Domain (for example via CIFS / SMB protocols)
- Authentication Key

When a Company Authentication Key is used in conjunction with either Active Directory or Windows Domain lookup, data needs to be 'merged.' See Company Authentication Key and Active Directory, page 1-3.

There are several ways to use the authentication key:

- As end-user identification (with Anywhere Plus where appropriate)
  - To control access to the Web Scanning Services
  - To identify an organization
  - To identify groups (within an organization)
  - To identify users (within groups)
- As group identification (with Anywhere Plus where appropriate)
  - To control access to the Web Scanning Services
  - To identify an organization
  - To identify groups
- As organization identification (in enterprise mode for dynamic IP access)

  - To control access to the Web Scanning Services
  - To identify an organization

As you can see, the authentication key has a dual purpose:

- To control access to the Web Scanning Services (as opposed to using static IP lockdown)
- To provide some identification data

Data embedded in requests can be classified as follows:

- Service authentication data (optional if you use static IP addresses)
  - Authentication key
- User identification data
  - Internal IP address
  - User name
  - Groups (for example from AD or Windows Domain)
- Session data
  - Local time
  - Tallies

Note Data is combined and transmitted securely with every web request via data headers.

Groups and Policy Application

The following sections describe how user data is derived, how groups work, and how policies are applied in ScanCenter.

Deriving User Data

ScanCenter derives user data from the maximum granularity available for a given request; the user name will be chosen from the first available data item:

- Connector-supplied user name (either from Active Directory or from user Authentication Key. If both, Connector uses User Authentication Key user name)
- Basic digest auth user name (for customers who have Squid)
- Connector-supplied internal IP
- Squid internal IP (for customers who have Squid)
- External IP

Applying Policy to Groups

Within ScanCenter there are two basic group types:

- Active Directory groups: must be created to match those returned by the Connector (from a customer's Active Directory server).

- Custom groups: collections of other identification (for example usernames, internal IPs, external IPs)

A group authentication key can be assigned to either an Active Directory group or to a Custom Group.

CHAPTER 2

Installing Connector on Windows

Revised: June 17, 2011

Overview

This chapter provides a step-by-step guide to installing the Windows Connector on servers running the Microsoft Windows Server operating system. It will help you to select the appropriate Connector mode, apply the right authentication key if necessary, and install, configure, and operate Connector.

To enable Connector to integrate with the widest possible variety of software and devices it has two modes of operation, determined during installation.

- Standalone mode should be used when there are no edge devices on the corporate network. See Installing in Standalone Mode, page 2-3.
- Enterprise mode should be used when an edge device, for example Microsoft ISA, is already present in the corporate network. See Installing in Enterprise Mode, page 2-16.

Windows System Requirements

Connector is supported on the following Microsoft operating systems:

- Windows Server 2003 (32-bit)
- Windows Server 2003 R2 (32-bit)
- Windows Server 2008 (32-bit)
- Windows Server 2008 (64-bit)
- Windows Server 2008 R2 (64-bit)

For deployments of 500 or more users, Cisco strongly recommends multiple servers are deployed behind a hardware load balancer to ensure there is no interruption of service in the event of a server failure. DNS load balancing (also known as round-robin) is not recommended due to the failover delay caused by caching of DNS responses by local computers.

Your technical account manager or a member of Cisco’s customer support team will be happy to discuss deployment options with you.

Note Windows Firewall must be enabled on the server where Connector is installed.

At least one GB of available disk space and a TCP/IP network connection and outbound Internet access on TCP ports 80 and 8080 are required for all installations. Other requirements vary depending on the number of intended users.

Table 2-1 Connector Windows Processor Requirements

Users	CPU	RAM
200	1.0Ghz Intel Pentium	1GB
2,000	2.0 GHz quad-core Intel Pentium	2GB
5,000	3.2GHz quad-core Intel Pentium	2GB
10,000	2x 2.0GHz quad-core processors	2GB

Pre-Installation Requirements

Before installing Connector you must determine where it will be installed. Connector is very lightweight and does not require its own dedicated server. For standalone servers, Cisco recommends installing Connector on either a Primary Domain Controller (PDC) or Backup Domain Controller (BDC) within your network. If you are using Microsoft Forefront TMG or ISA Server, Cisco recommends installing Connector on the same server.

To prepare to install Connector:

Step 1 Determine which mode Connector will use. See Overview, page 2-1.

Step 2 In ScanCenter, generate the authentication keys, as necessary. Keys are required for users with dynamic IP addresses only. Keys can also be used with static IP addresses.

Step 3 If you require Connector to perform group lookup with Active Directory or a Windows domain, create a dedicated user within the 'Domain Users' group of the primary domain controller.

Step 4 If you are using Windows Server 2003 or later with SMB signing enabled (this is the default setting), create a dedicated user on the primary domain controller. If you have already created a user on the domain controller to enable group lookups you do not need to create a new user. When configuring Connector you will need to include the details of this user in the config file with the following arguments:

- `ntlm.preauth.domain=`
- `ntlm.preauth.username=`
- `ntlm.preauth.password=`

Step 5 Download the Connector installation program from ScanCenter.

Step 6 Remove any previously installed versions of the connector (including Proxy Agent). See Removing Connector, page 2-33.

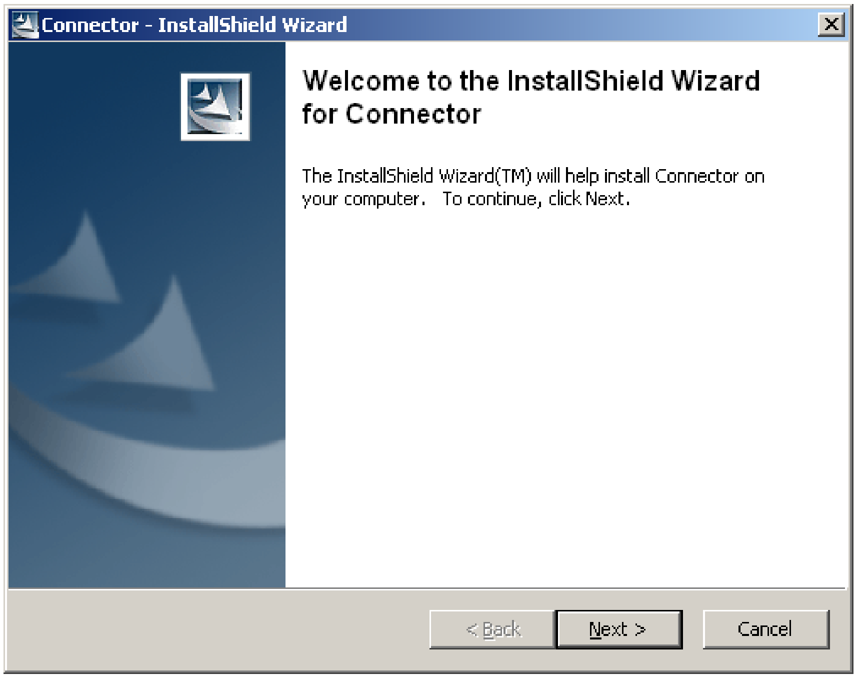
Step 7 If you will use Microsoft Forefront TMG or ISA Server 2004 or 2006, make sure it is installed and running. The server where Microsoft TMG or ISA and Connector will be installed must meet the minimum requirements for the version of Microsoft TMG or ISA you are using.

Note Following all installations you must apply the relevant Windows registry patches. See Applying the Windows Registry Patches, page 2-32.

Installing in Standalone Mode

To install Connector in standalone mode:

Step 1 Double-click the Connector program file to run the installation wizard.

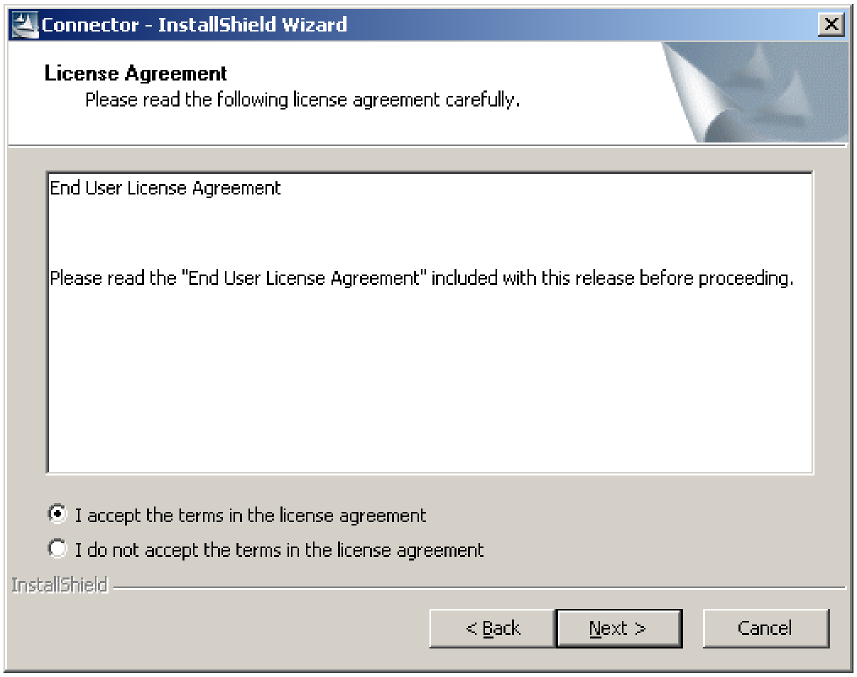


Connector - InstallShield Wizard

Welcome to the InstallShield Wizard for Connector

The InstallShield Wizard(TM) will help install Connector on your computer. To continue, click Next.

Step 2 Click **Next** to display the License Agreement dialog.



Connector - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

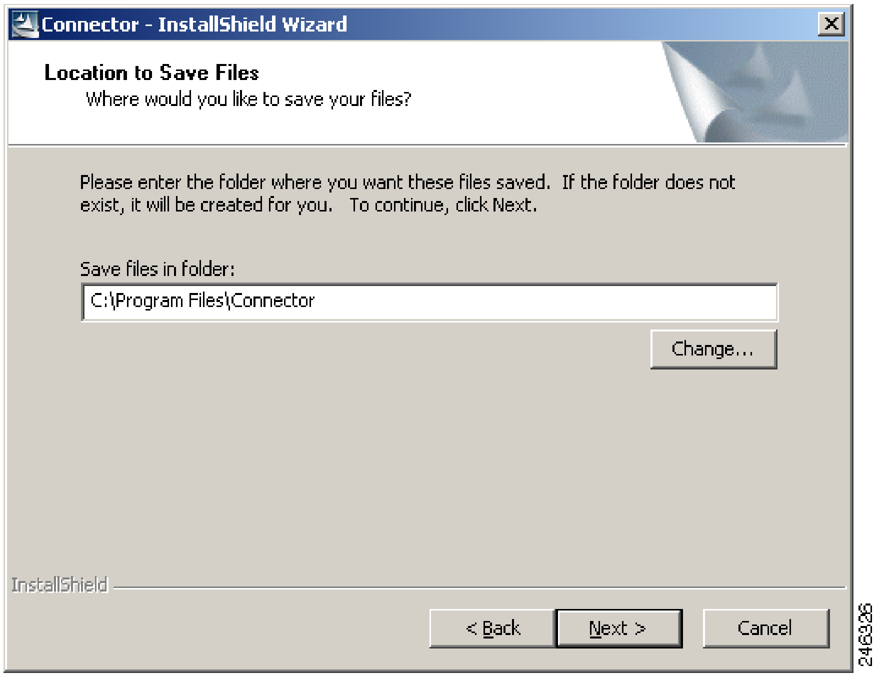
End User License Agreement

Please read the "End User License Agreement" included with this release before proceeding.

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Step 3 Read the End User License Agreement. If you agree to the terms, click **I accept the terms in the license agreement** then click **Next** to display the Location to Save Files dialog. Alternatively, if you do not agree to the terms, click **Cancel** to stop the installation.



Connector - InstallShield Wizard

Location to Save Files

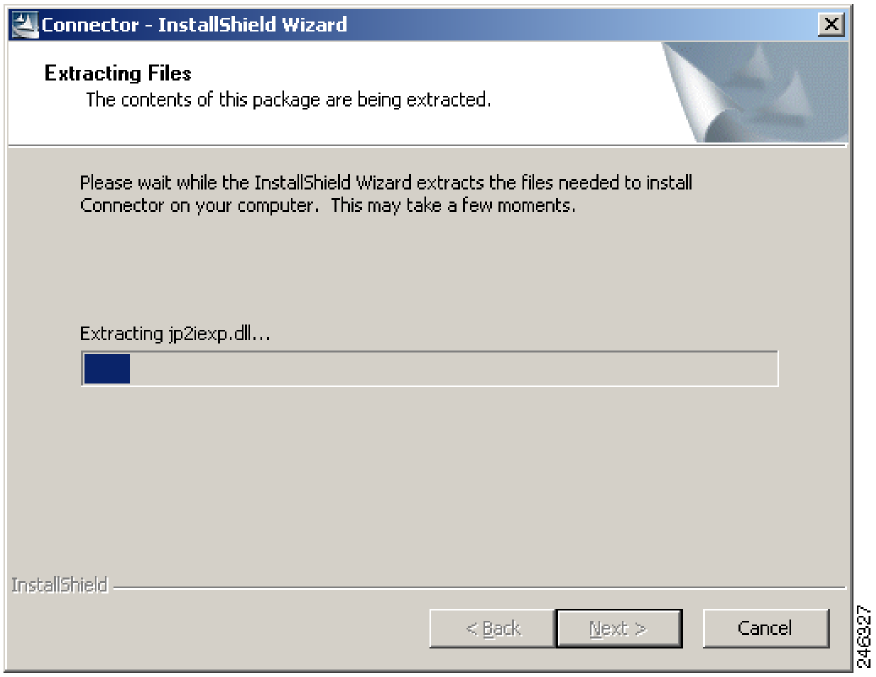
Where would you like to save your files?

Please enter the folder where you want these files saved. If the folder does not exist, it will be created for you. To continue, click Next.

Save files in folder:

C:\Program Files\Connector

Step 4 Click **Next** to accept the default installation folder. Alternatively, enter a new path in the **Save files in folder** box, or click **Change** and navigate to the required folder, then click **Next** to display the Welcome dialog.



Connector - InstallShield Wizard

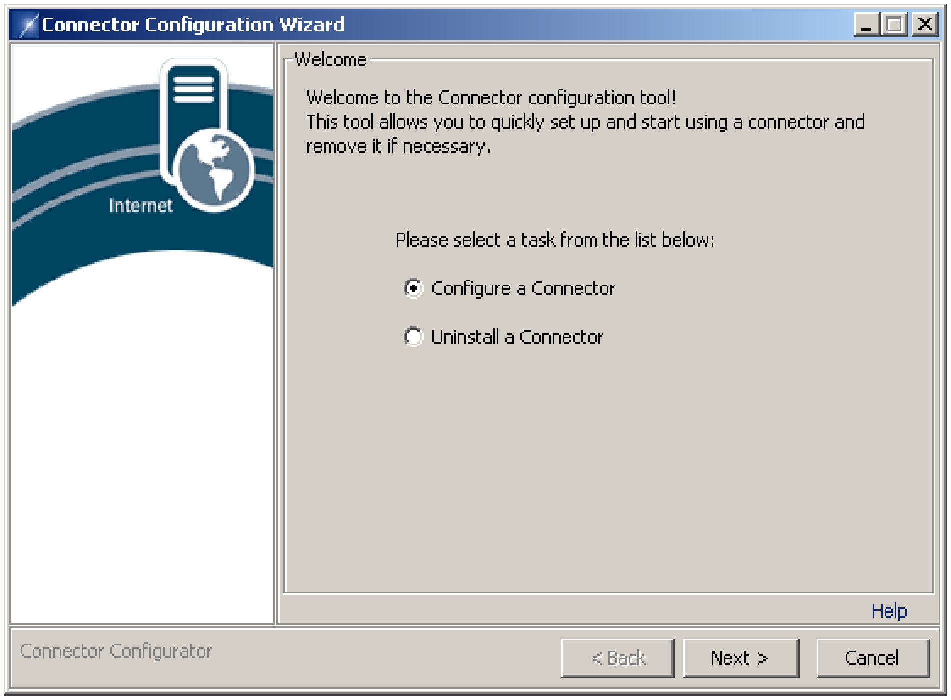
Extracting Files

The contents of this package are being extracted.

Please wait while the InstallShield Wizard extracts the files needed to install Connector on your computer. This may take a few moments.

Extracting jp2iexp.dll...

Step 5 Click **Configure a Connector** then click **Next** to display the Connector Type dialog.



Welcome to the Connector configuration tool!
This tool allows you to quickly set up and start using a connector and remove it if necessary.

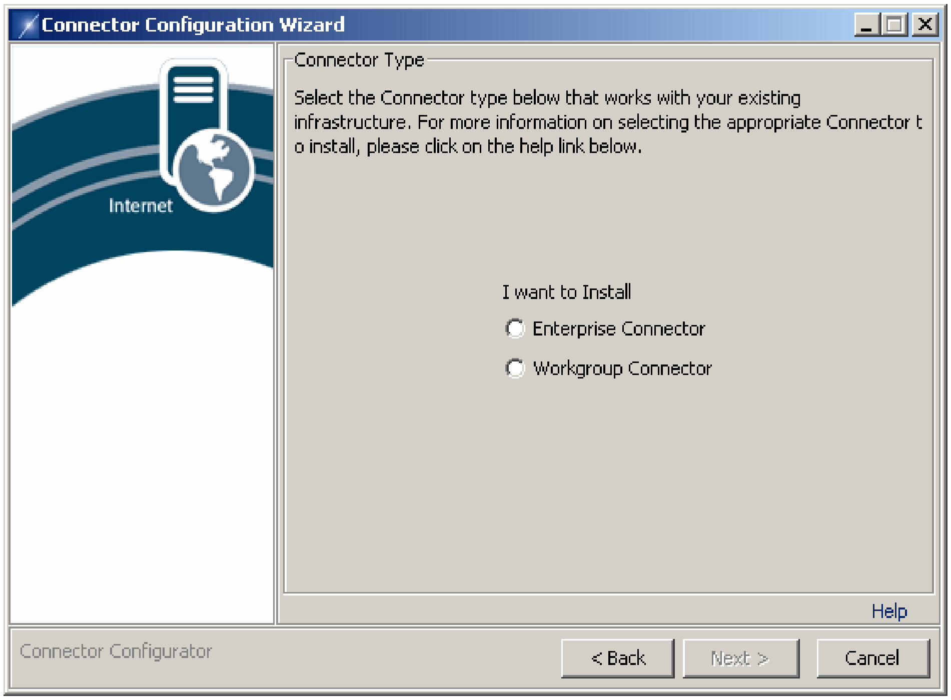
Please select a task from the list below:

● Configure a Connector

○ Uninstall a Connector

246328

Step 6 Click **Workgroup Connector** then click **Next** to display the Authentication Configuration dialog.



Select the Connector type below that works with your existing infrastructure. For more information on selecting the appropriate Connector t o install, please click on the help link below.

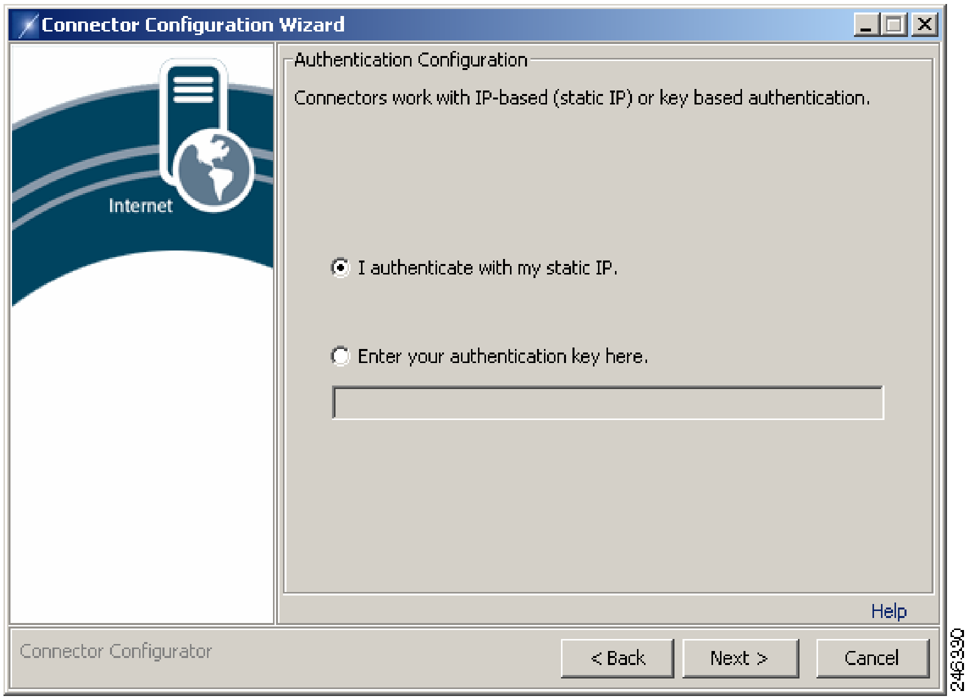
I want to Install

○ Enterprise Connector

○ Workgroup Connector

246329

Step 7 You can use IP-based or key based authentication. IP-based authentication requires a static IP address. To use IP-based authentication, click **I authenticate with my static IP**. Alternatively, click **Enter your authentication key here** and enter a company or group authentication key For details of how to generate a key, refer to the *ScanCenter Administrator Guide*.



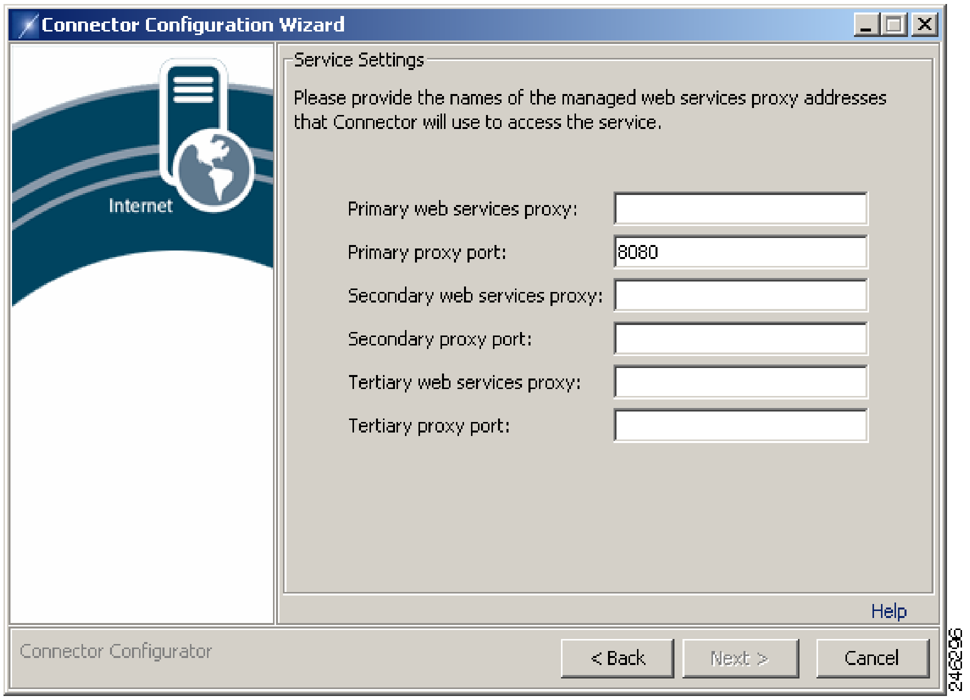
Authentication Configuration

Connectors work with IP-based (static IP) or key based authentication.

● I authenticate with my static IP.

○ Enter your authentication key here.

Step 8 Click **Next** to display the Service Settings dialog.



Service Settings

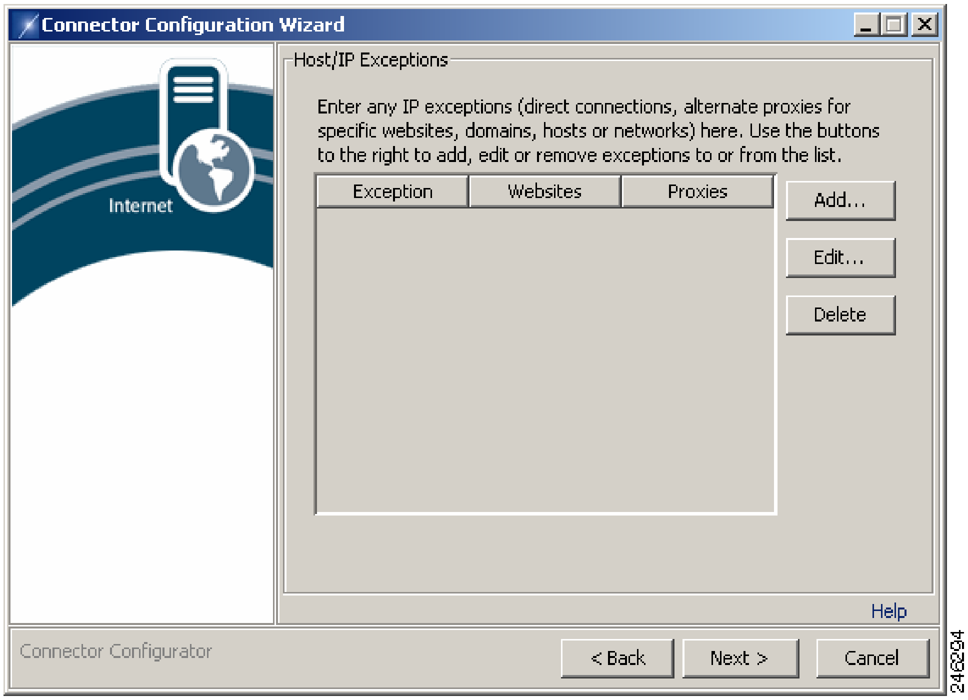
Please provide the names of the managed web services proxy addresses that Connector will use to access the service.

Primary web services proxy:	
Primary proxy port:	8080
Secondary web services proxy:	
Secondary proxy port:	
Tertiary web services proxy:	
Tertiary proxy port:	

Step 9 Your proxy settings are contained in your provisioning email. If you have not received this email, contact your support representative. Normally only primary and secondary proxies are provided. You can specify up to three proxy servers:

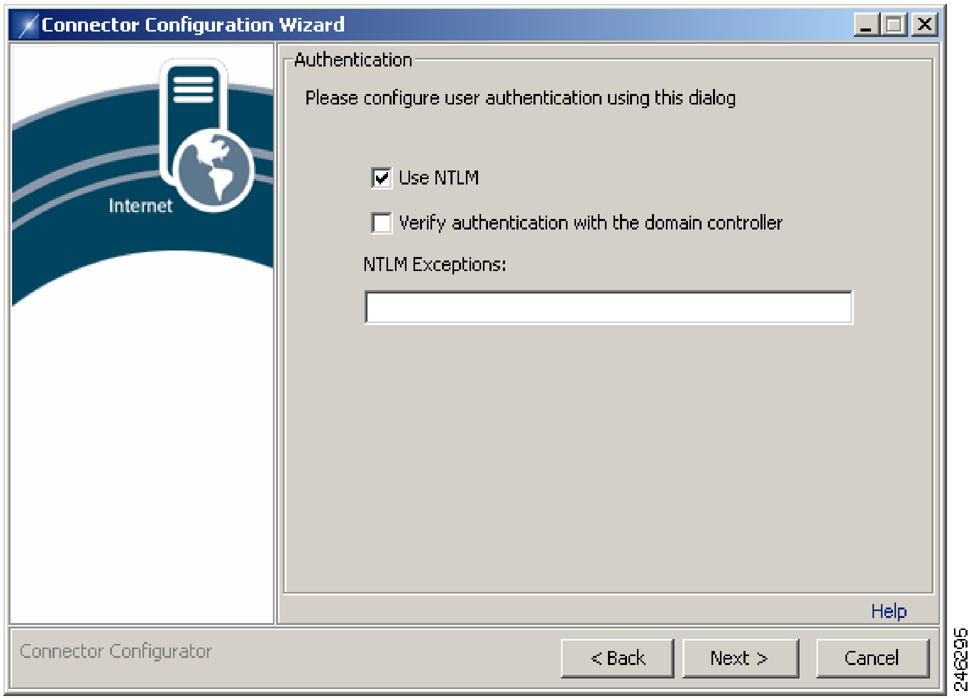
- The primary proxy is used in preference to the other proxies.
- The secondary proxy is used as a fallback in cases where the primary proxy is unreachable.
- The tertiary proxy is used as a fallback in cases where both the primary and secondary proxies are unreachable.

Step 10 Enter your proxy settings, then click **Next** to display the Host/IP exceptions dialog.



Enter any IP exceptions (direct connections, alternate proxies for specific websites, domains, hosts or networks) here. Use the buttons to the right to add, edit or remove exceptions to or from the list.

Step 11 The Host/IP Exceptions dialog enables you to create exceptions that specify direct connections or alternate proxies for specific Web sites, domains, hosts or networks. The exceptions are shown in a list. It is not necessary to configure the exceptions during the installation. See Adding Host Exceptions, page 2-12. Click **Next** to display the Authentication dialog.



Connector Configuration Wizard

Authentication

Please configure user authentication using this dialog

☑ Use NTLM

☐ Verify authentication with the domain controller

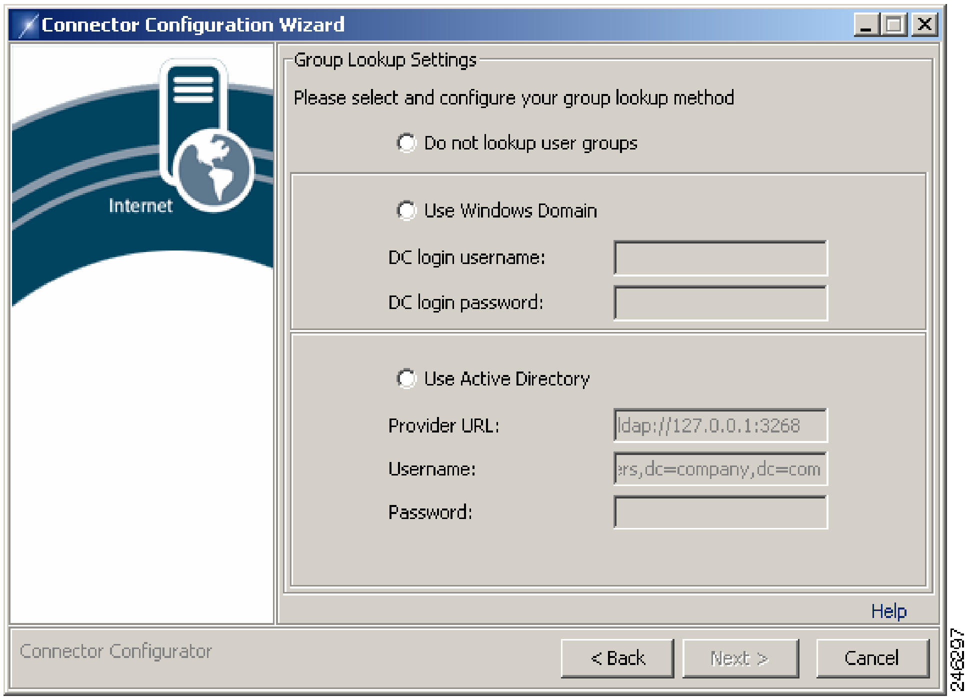
NTLM Exceptions:

Step 12 Ensure the **Use NTLM** check box is selected. Do not clear this check box unless instructed to do so by your support representative.

Step 13 Clear the **Verify authentication with the domain controller** check box. Alternatively, select the check box to verify credentials provided by clients with the domain controller.

Step 14 Enter any client IP addresses to be excluded from authentication in a comma separated list in the **NTLM Exceptions** box. This box should normally be left blank unless you have been otherwise instructed by your support representative.

Step 15 Click **Next** to display the Group Lookup Settings dialog.



Connector Configuration Wizard

Group Lookup Settings

Please select and configure your group lookup method

○ Do not lookup user groups

○ Use Windows Domain

DC login username:

DC login password:

○ Use Active Directory

Provider URL: ldap://127.0.0.1:3268

Username: ers,dc=company,dc=com

Password:

Help

Connector Configurator

< Back | Next > | Cancel

Step 16 To use LDAP to gather group information:

a. Click **Use Active Directory**.

b. Enter an LDAP URL in the Provider URL box. Alternatively, if you are installing Connector on the domain controller, accept the default LDAP URL (`ldap://127.0.0.1:3268`).

c. To enable the connector to perform LDAP group lookups, an active directory user must be created. Enter the user name of the active directory account you created for the connector in the **Username** box, for example `cn=proxyagent,cn=users,dc=company,dc=com`. See Pre-Installation Requirements, page 2-2.

d. Enter the Password for the active directory account.

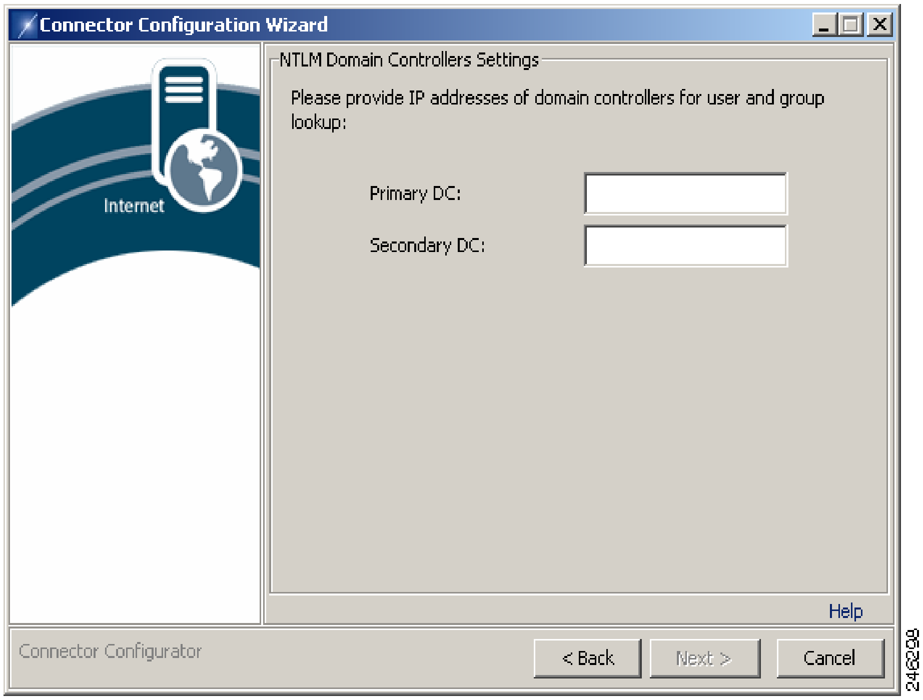
Alternatively, to use NTLM to gather group information:

e. Click **Use Windows Domain**.

f. Enter the user name of the domain controller account you created for the connector in the **DC login username** box. See Pre-Installation Requirements, page 2-2.

g. Enter the password of the domain controller account in the **DC login password** box.

h. Click **Next** to display the NTLM Domain Controllers Settings dialog.



NTLM Domain Controllers Settings

Please provide IP addresses of domain controllers for user and group lookup:

Primary DC:

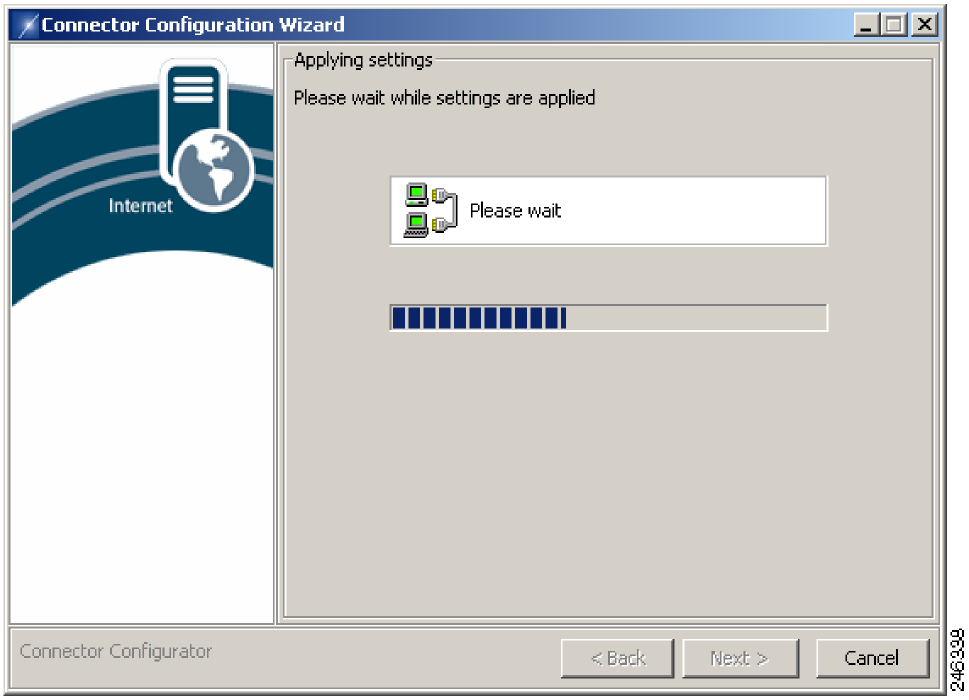
Secondary DC:

i. Enter the IP address of your primary domain controller in the Primary DC box.

j. If you have a secondary domain controller, enter its IP address in the Secondary DC box.

Step 17 Cisco recommends using LDAP to gather group information. Do not click **Do not lookup user groups** unless instructed to do so by your support representative.

Step 18 Click **Next** to begin the installation.

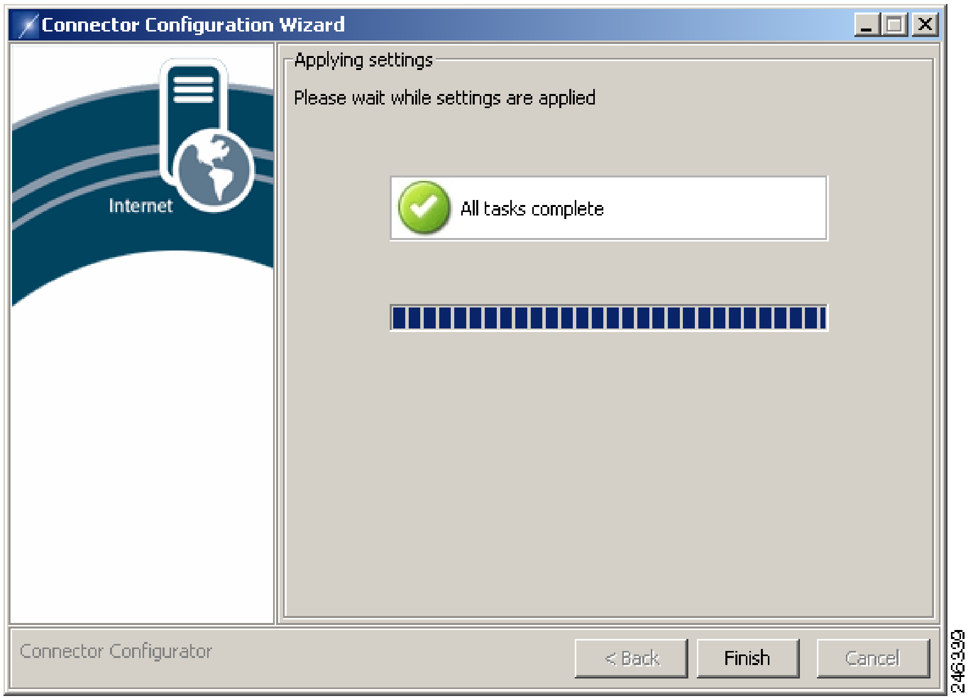


Applying settings

Please wait while settings are applied

Please wait

Step 19 When the installation tasks have completed successfully, the following dialog is displayed.



Applying settings

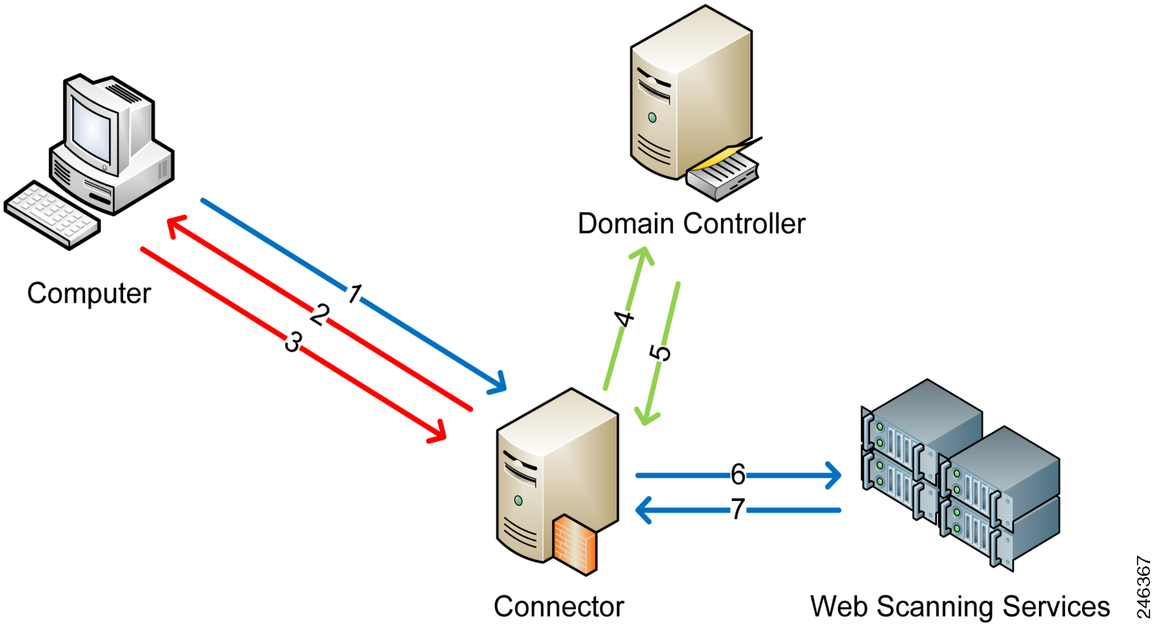
Please wait while settings are applied

All tasks complete

Step 20 Click **Finish** to close the wizard.

Post-Installation Firewall Configuration

You need to ensure the connector can forward all web traffic out of your network to the Web Scanning Services. In most cases this requires a simple change to your firewall settings to allow all TCP traffic on port 8080 originating from the IP address where the connector is running to go out to the Internet. The following diagram shows the path a user's web request must take to get to the Web Scanning Services.



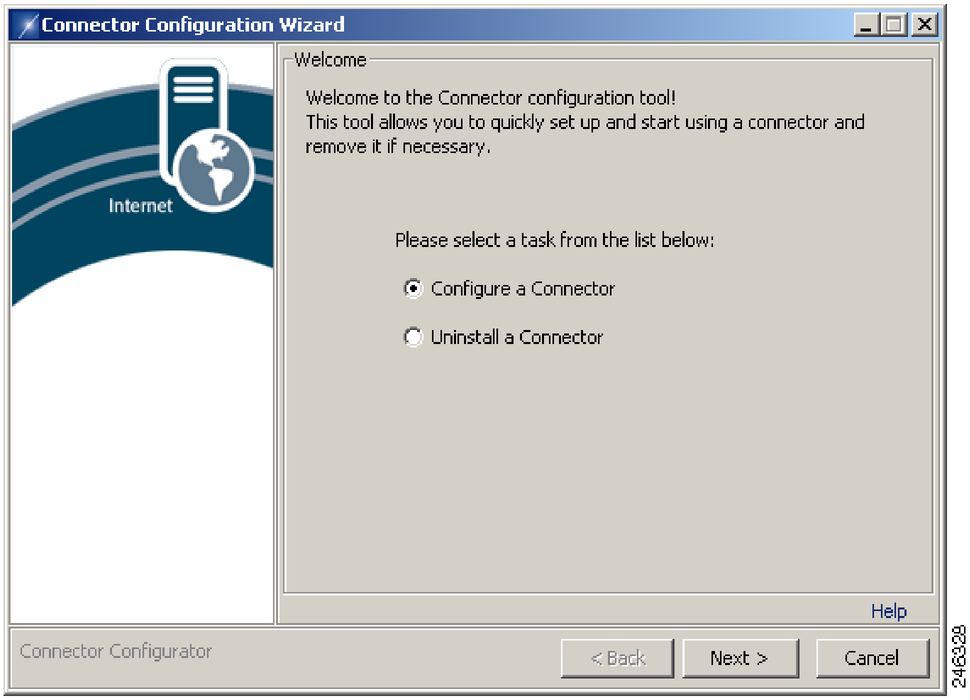
1. Web browser requests a URL.
2. Connector performs an NTLM challenge.
3. Web browser responds with NTLM user details.
4. Connector uses credentials to poll the domain controller (LDAP) for AD Groups. If the user exists, Connector performs a query based on user name to lookup groups.
5. Domain controller sends group information to Connector.
6. URL request and encrypted, user and group information forwarded from Connector to Web Scanning Services.
7. Content sent back to the user via Connector.

Adding Host Exceptions

Host exceptions are used to allow users to bypass the Web Scanning Services when connecting to specified websites. Exceptions can include wild cards, address ranges, and IP ports. They should not be used for connections to your own network because a proxy server (local exception) set in a user's browser is more efficient for this task.

To add host exceptions to Connector:

Step 1 In the folder where you installed Connector, double-click the Wizard batch file to run the configuration wizard.



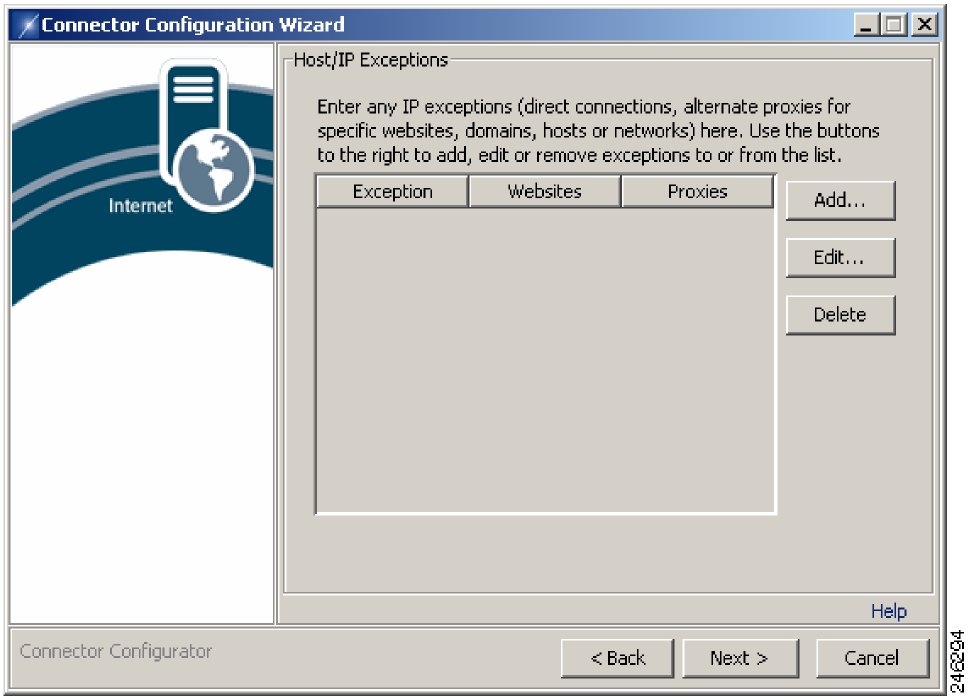
Welcome to the Connector configuration tool!
This tool allows you to quickly set up and start using a connector and remove it if necessary.

Please select a task from the list below:

● Configure a Connector

○ Uninstall a Connector

Step 2 The wizard imports the settings from your last session so it is not necessary to specify that you are using a standalone server, your method of authentication, or the service settings. At each dialog, click **Next** until the Host/IP Exceptions dialog is displayed.



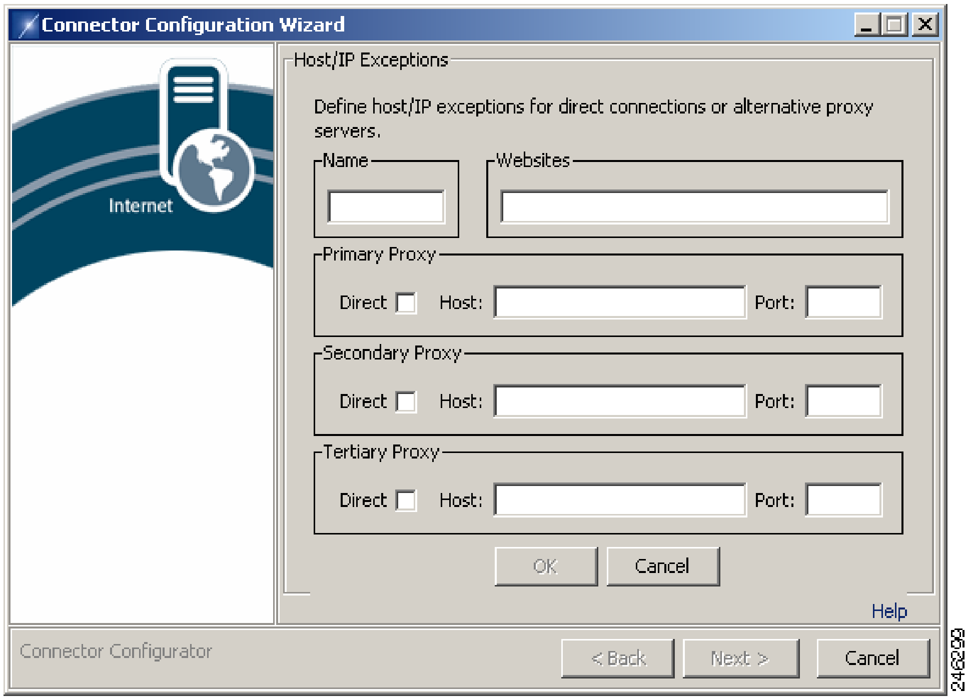
Enter any IP exceptions (direct connections, alternate proxies for specific websites, domains, hosts or networks) here. Use the buttons to the right to add, edit or remove exceptions to or from the list.

Exception	Websites	Proxies

Step 3 The Host/IP Exceptions dialog enables you to create exceptions that specify direct connections or alternate proxies for specific websites, domains, hosts or networks. The exceptions are shown in a list. You can click **Edit** to edit an existing exception or **Delete** to remove an exception.

Step 4 For each exception you want to add:

1. Click **Add**.



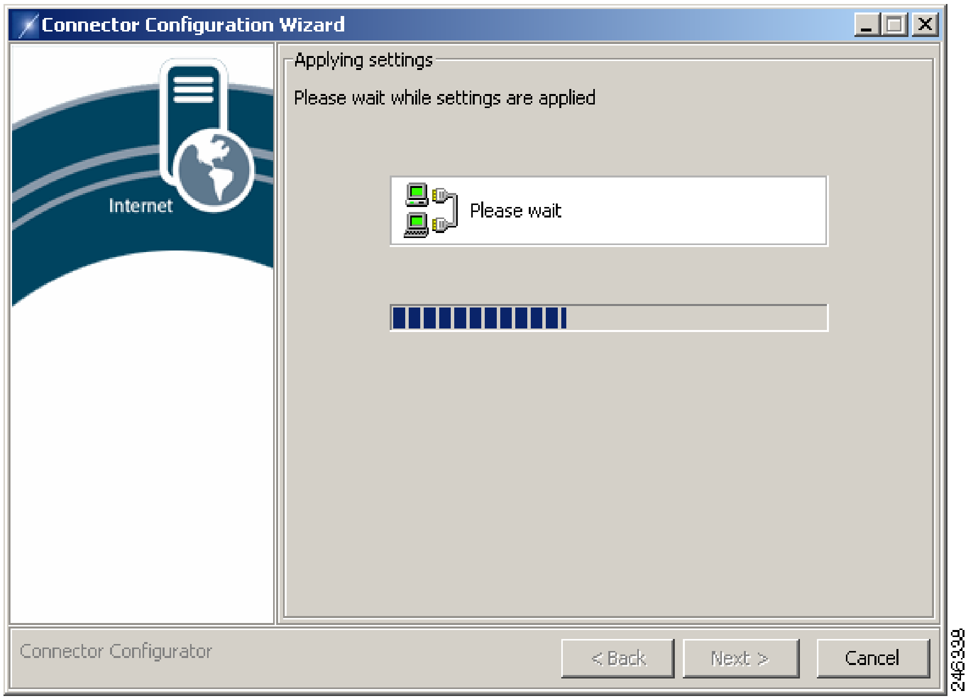
Connector Configuration Wizard

Host/IP Exceptions

Define host/IP exceptions for direct connections or alternative proxy servers.

2. Enter a **Name** for the exception.
3. Enter the websites which the exception will be applied to, separated by commas. Websites can be entered:
   - in full (`www.company.com`)
   - with wildcards (`*.company.com`)
   - as an IP address (`164.35.91.46`)
   - as a range of IP addresses (`164.35.91.*`)
   - with a port (`*.company.com/80, 164.35.91.*/8080`)
4. You can provide up to three proxies. The secondary and tertiary proxies act as fallbacks in the event that the primary proxy is unavailable. Only the primary proxy is required. If no proxy is available it will not be possible to connect to the service. For each proxy, select the Direct check box to enable users to connect directly to the specified Web sites. Alternatively, enter a Host (normally an internal proxy) and, optionally, an IP Port.
5. When you have entered the proxy details, click **OK**. Alternatively, click **Cancel** to abandon your changes.

Step 5 The wizard imports the settings from your last session so it is not necessary to specify authentication, NTLM, or Group Lookup settings. At each dialog, click **Next** until the Applying settings dialog is displayed.

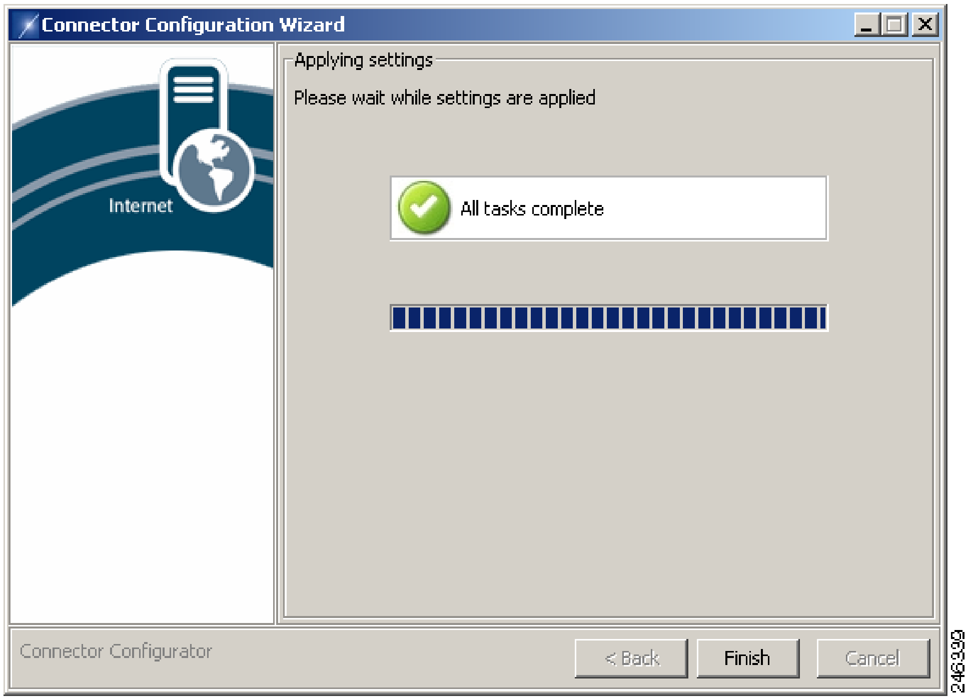

Connector Configuration Wizard

Applying settings

Please wait while settings are applied

Please wait

When the configuration tasks have completed successfully, the following dialog is displayed.


Connector Configuration Wizard

Applying settings

Please wait while settings are applied

All tasks complete

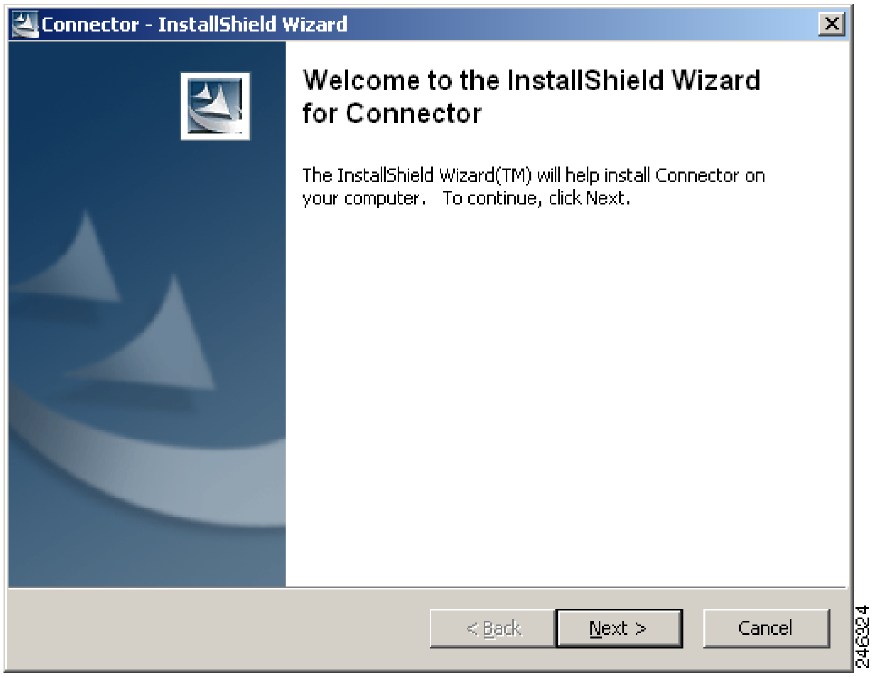
Step 6 Click **Finish** to close the wizard.

Installing in Enterprise Mode

In Enterprise mode, Connector works with a device that uses the Internet Content Application Protocol (ICAP), such as Microsoft ISA or Blue Coat.

To install Connector in Enterprise mode:

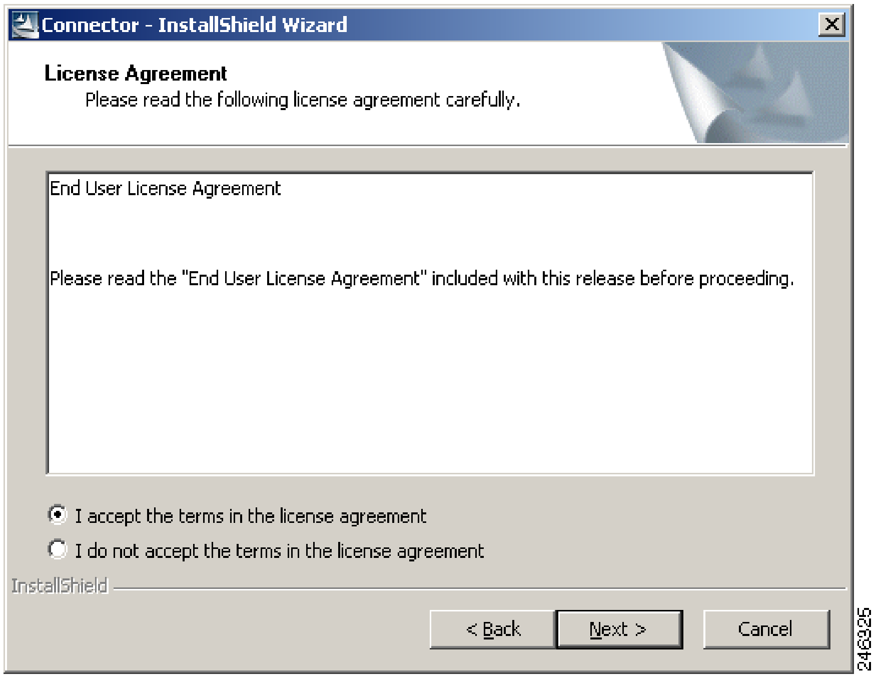
Step 1 Double-click the Connector program file to run the installation wizard.



Welcome to the InstallShield Wizard for Connector

The InstallShield Wizard(TM) will help install Connector on your computer. To continue, click Next.

Step 2 Click **Next** to display the License Agreement dialog.



Connector - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

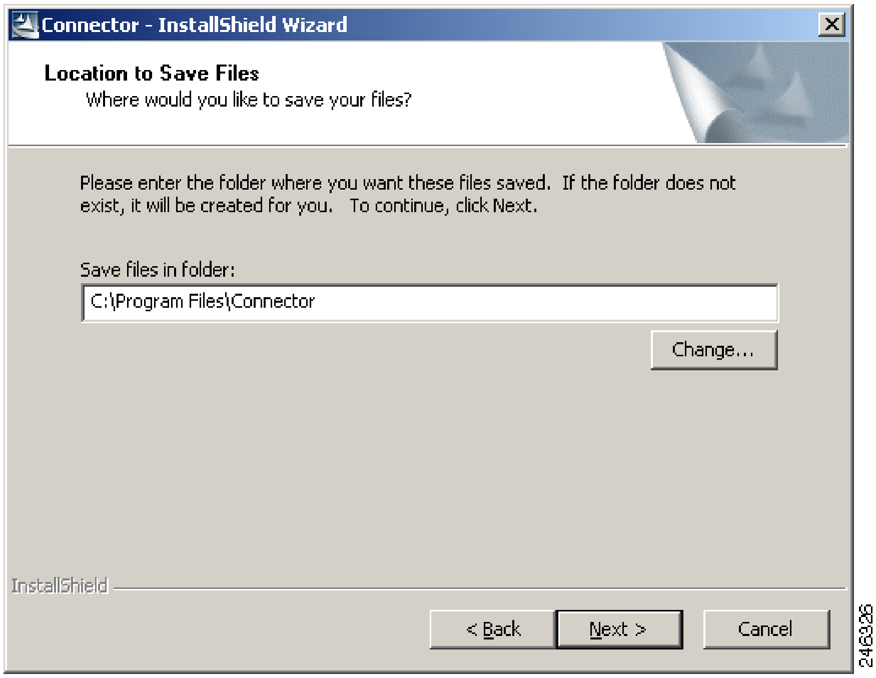
End User License Agreement

Please read the "End User License Agreement" included with this release before proceeding.

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Step 3 Read the End User License Agreement. If you agree to the terms, click **I accept the terms in the license agreement** then click **Next** to display the Location to Save Files dialog. Alternatively, if you do not agree to the terms, click **Cancel** to stop the installation.



Connector - InstallShield Wizard

Location to Save Files

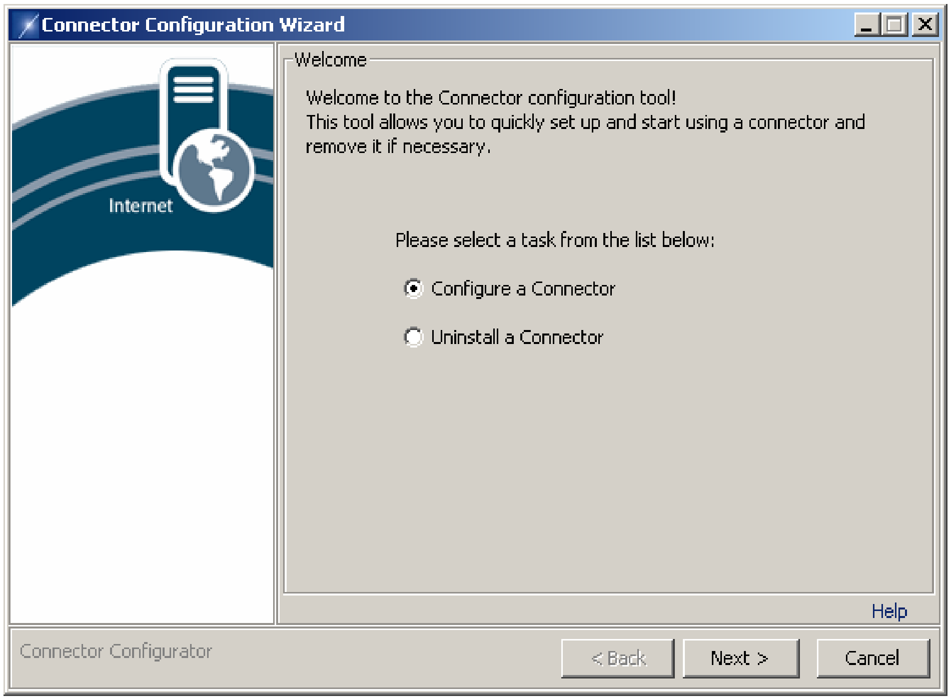
Where would you like to save your files?

Please enter the folder where you want these files saved. If the folder does not exist, it will be created for you. To continue, click Next.

Save files in folder:

C:\Program Files\Connector

Step 4 Click **Next** to accept the default installation folder. Alternatively, enter a new path in the **Save files in folder** box, or click **Change** and navigate to the required folder, then click **Next** to display the Welcome dialog.



Connector Configuration Wizard

Welcome

Welcome to the Connector configuration tool!
This tool allows you to quickly set up and start using a connector and remove it if necessary.

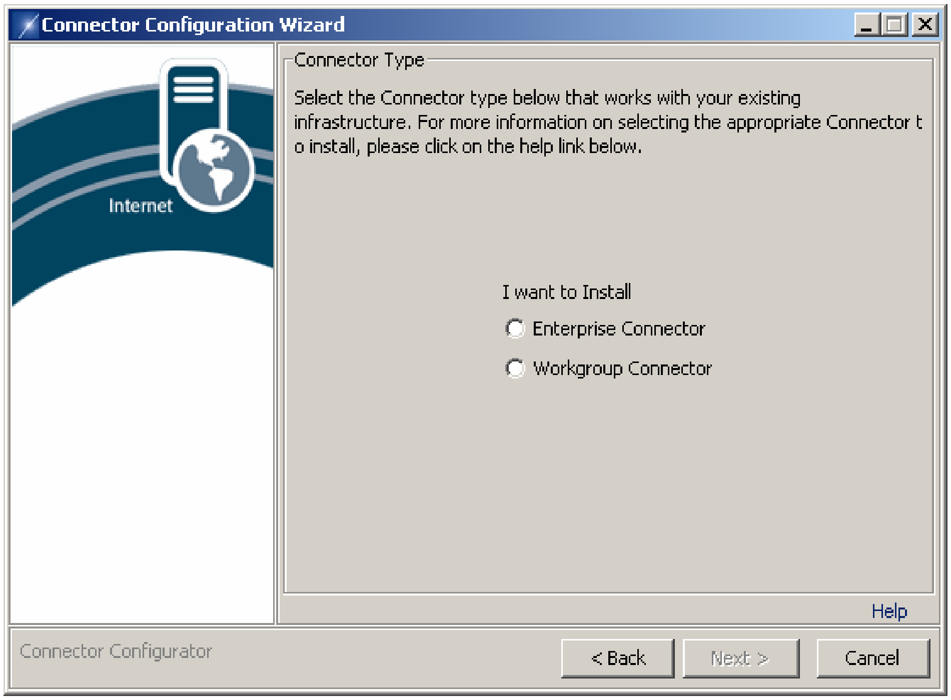
Please select a task from the list below:

● Configure a Connector

○ Uninstall a Connector

246328

Step 5 Click **Configure a Connector** then click **Next** to display the Connector Type dialog.



Connector Configuration Wizard

Connector Type

Select the Connector type below that works with your existing infrastructure. For more information on selecting the appropriate Connector t o install, please click on the help link below.

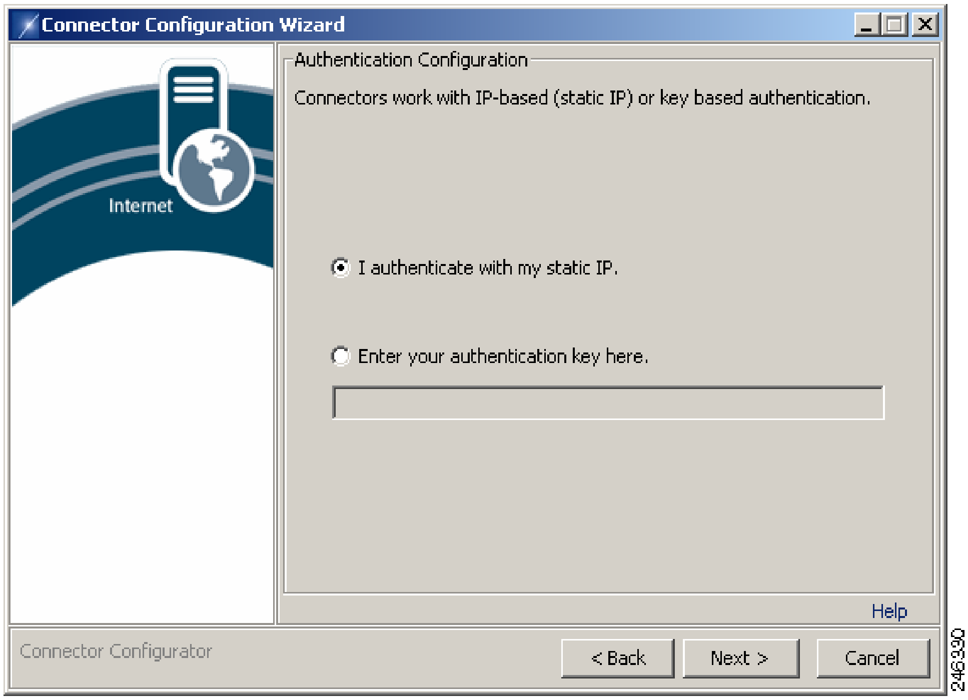
I want to Install

○ Enterprise Connector

○ Workgroup Connector

246329

Step 6 Click **Enterprise Connector** then click **Next** to display the Authentication Configuration dialog.



Authentication Configuration

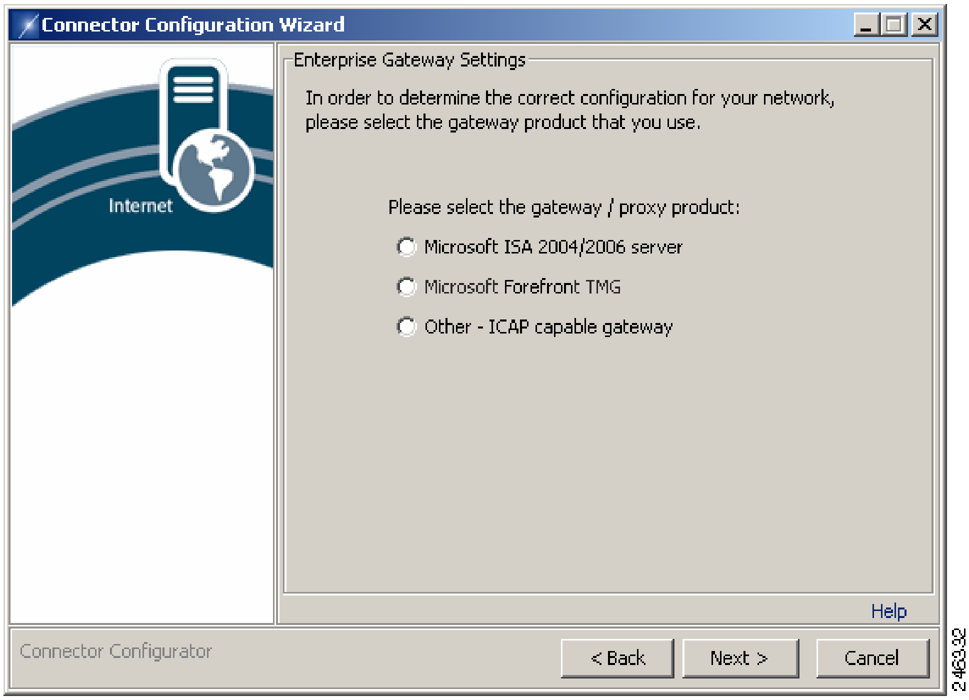
Connectors work with IP-based (static IP) or key based authentication.

● I authenticate with my static IP.

○ Enter your authentication key here.

Step 7 You can use IP-based or key based authentication. IP-based authentication requires a static IP address. To use IP-based authentication, click **I authenticate with my static IP**. Alternatively, click **Enter your authentication key here** and enter a company or group authentication key. For details of how to generate a key, refer to the Web Scanning Services documentation.

Step 8 Click **Next** to display the Enterprise Gateway Settings dialog.



Enterprise Gateway Settings

In order to determine the correct configuration for your network, please select the gateway product that you use.

Please select the gateway / proxy product:

○ Microsoft ISA 2004/2006 server

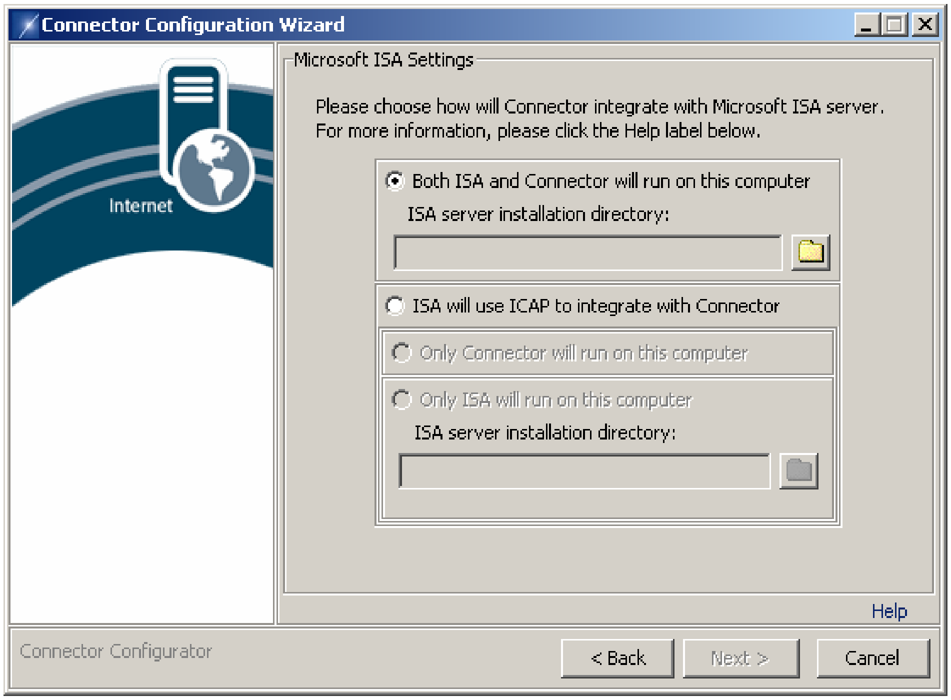
○ Microsoft Forefront TMG

○ Other - ICAP capable gateway

Step 9 If you are using Microsoft Forefront TMG the steps are the same as if you are using ISA Server, except that instead of selecting the ISA 2004/2006 Server option, you should select the Forefront TMG equivalent. To use ISA Server:

a. Click **Microsoft ISA 2004/2006 server**.

b. Click **Next** to display the Microsoft ISA Settings dialog.



Microsoft ISA Settings

Please choose how will Connector integrate with Microsoft ISA server.
For more information, please click the Help label below.

● Both ISA and Connector will run on this computer

ISA server installation directory:

○ ISA will use ICAP to integrate with Connector

○ Only Connector will run on this computer

○ Only ISA will run on this computer

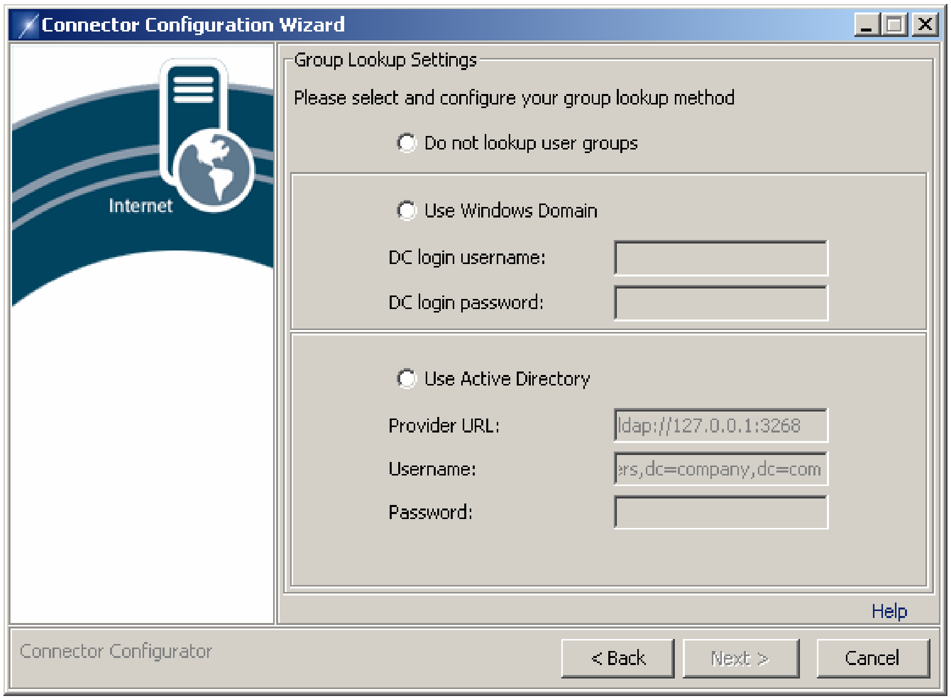
ISA server installation directory:

c. Click **ISA will use ICAP to integrate with Connector**.

d. Click **Only Connector will run on this computer**.

Alternatively, if you are not using ISA Server click **Other - ICAP capable gateway**.

Step 10 Click **Next** to display the Group Lookup Settings dialog.



Connector Configuration Wizard

Group Lookup Settings

Please select and configure your group lookup method

○ Do not lookup user groups

○ Use Windows Domain

DC login username:

DC login password:

○ Use Active Directory

Provider URL: ldap://127.0.0.1:3268

Username: ers,dc=company,dc=com

Password:

Step 11 To use LDAP to gather group information:

a. Click **Use Active Directory**.

b. Enter an LDAP URL in the **Provider URL** box.Alternatively, if you are installing the connector on the domain controller, accept the default LDAP URL (`ldap://127.0.0.1:3268`).

c. To enable the connector to perform LDAP group lookups, an active directory user must be created. Enter the user name of the active directory account you created for the connector in the **Username** box, for example `cn=proxyagent,cn=users,dc=company,dc=com`. See Pre-Installation Requirements, page 2-2.

d. Enter the **Password** for the active directory account.

Alternatively, to use NTLM to gather group information:

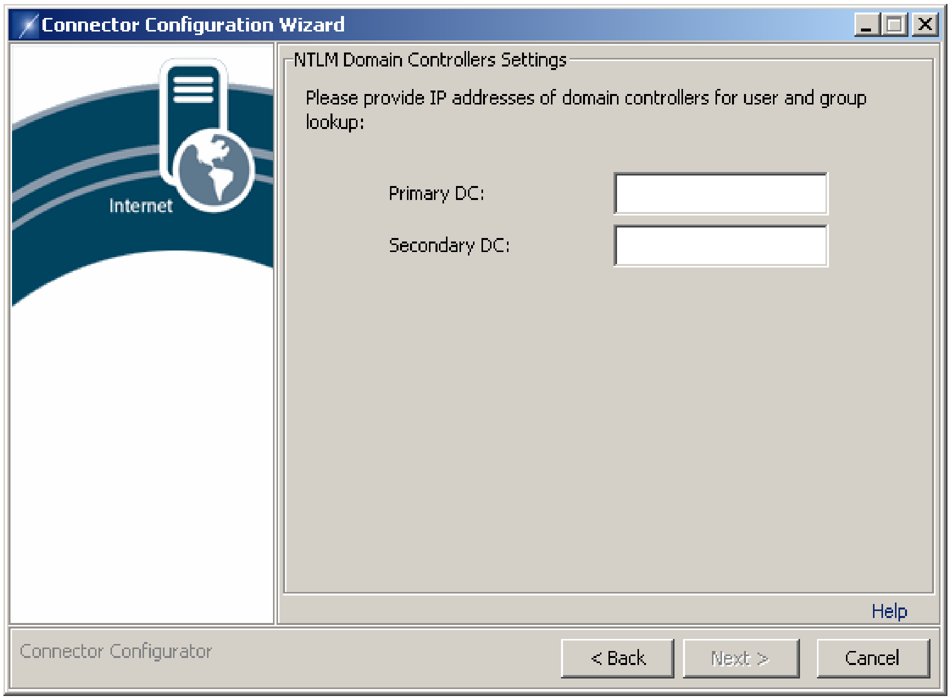
a. Click **Use Windows Domain**.

b. Enter the user name of the domain controller account you created for the connector in the **DC login username** box.

c. To enable the connector to perform LDAP group lookups, an active directory user must be created. Enter the user name of the active directory account you created for Connector in the **Username** box, for example `cn=proxyagent,cn=users,dc=company,dc=com.` See Pre-Installation Requirements, page 2-2.

d. Enter the password of the domain controller account in the **DC login password** box.

e. Click **Next** to display the NTLM Domain Controllers Settings dialog.



NTLM Domain Controllers Settings

Please provide IP addresses of domain controllers for user and group lookup:

Primary DC:

Secondary DC:

246298

f. Enter the IP address of your primary domain controller in the **Primary DC** box.

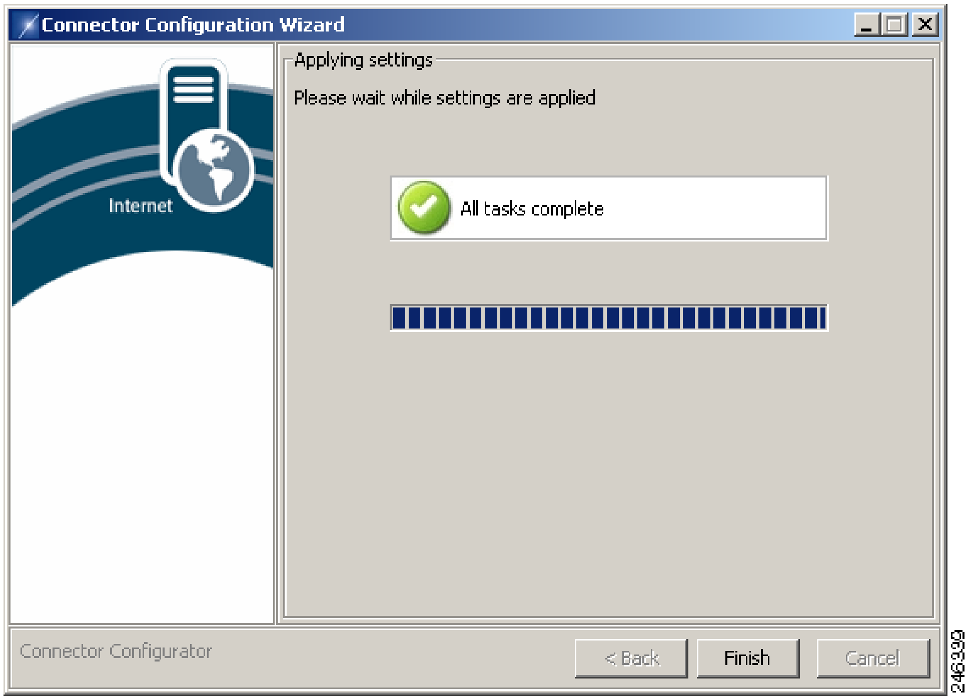
g. If you have a secondary domain controller, enter its IP address in the **Secondary DC** box.

Cisco recommends using LDAP to gather group information. Do not click **Do not lookup user groups** unless instructed to do so by your support representative.

Step 12 Click **Next** to begin the installation.

If the Microsoft Firewall service is running, you will be prompted to stop the service. The service will be restarted when the installation is complete.

When the installation tasks have completed successfully, the following dialog is displayed:



Applying settings

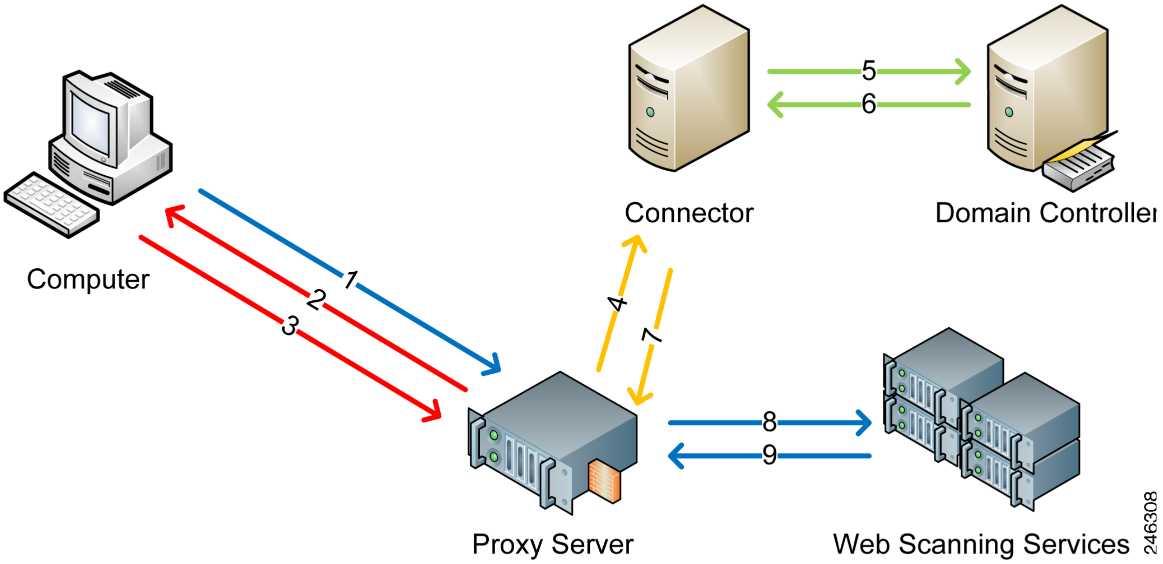
Please wait while settings are applied

All tasks complete

Step 13 Click **Finish** to close the wizard. If you installed Connector on a different computer than Forefront TMG or ISA Server you must now configure TMG or ISA. See Configuring Microsoft Forefront TMG or ISA Server, page 2-24.

Post-Installation Proxy Server Configuration

You need to ensure the connector can forward all Web traffic out of your network to the Web Scanning Services. The changes you need to make are dependent on the proxy server, or firewall appliance, you are using. For more information, refer to the quick reference for your proxy server. The following diagram shows the path a user's Web request must take to get to the Web Scanning Services.



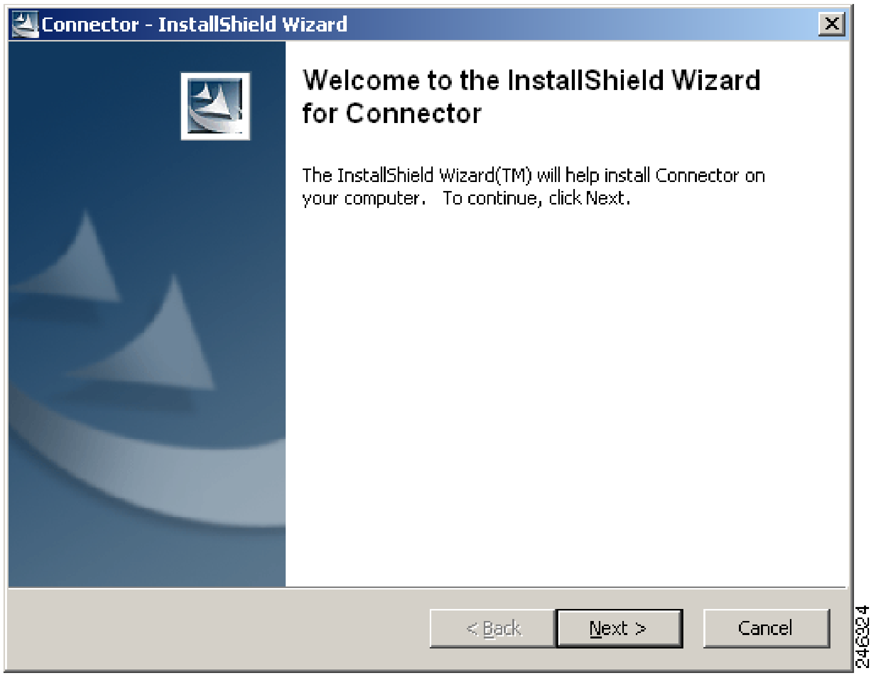
1. Web browser requests a URL.
2. Proxy server performs an NTLM challenge.
3. Web browser responds with NTLM user details.
4. URL request is forwarded with NTLM credentials to Connector.
5. Connector uses the credentials to poll the domain controller (LDAP) for AD Groups. If the user exists, Connector performs a query based on user name to lookup groups.
6. Domain controller sends group information to Connector.
7. URL request forwarded from Connector to proxy server with encrypted headers
8. URL request with encrypted group information forwarded from proxy server to Web Scanning Services.
9. Content sent back to the user via the proxy server.

Configuring Microsoft Forefront TMG or ISA Server

The recommended method for using Microsoft Forefront TMG or ISA Server 2004 or 2006, with Connector is to install Connector, Forefornt TMG or ISA Server, and the Forefront TMG or ISA Server plug-in on a shared server. You must use separate folders to install the ICAP sender and receiver, for example C:\Program Files\ConnectorICAP and C:\Program Files\ConnectorLDAP. You should not use other configurations unless instructed to do so by customer support.

If you are using Microsoft Forefront TMG the steps are the same as if you are using ISA Server, except that instead of selecting the ISA 2004/2006 Server option, you should select the Forefront TMG equivalent. To configure ISA Server:

Step 1 Double-click the Connector program file to run the installation wizard.

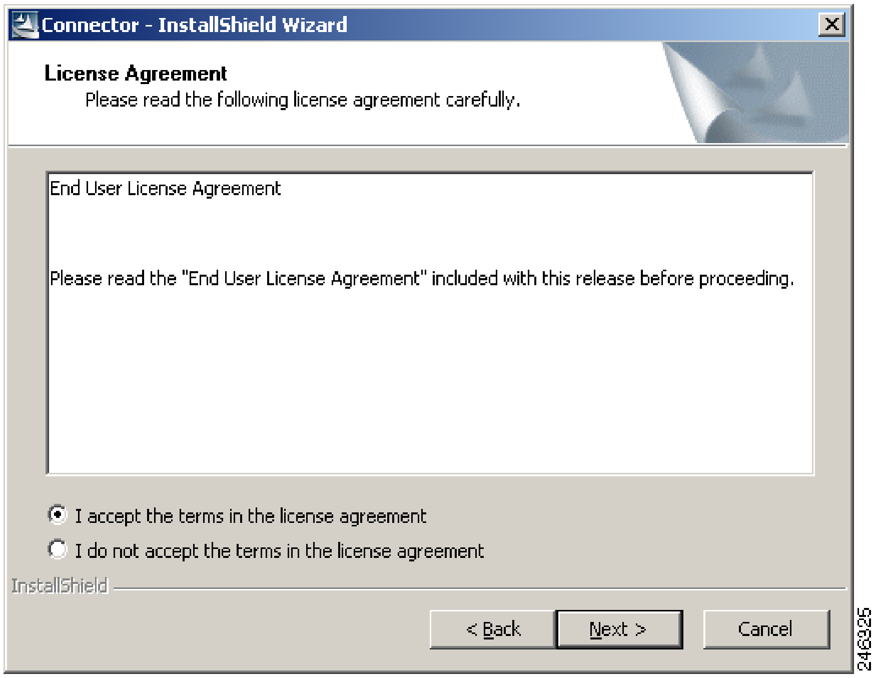


Connector - InstallShield Wizard

Welcome to the InstallShield Wizard for Connector

The InstallShield Wizard(TM) will help install Connector on your computer. To continue, click Next.

Step 2 Click **Next** to display the License Agreement dialog.



Connector - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

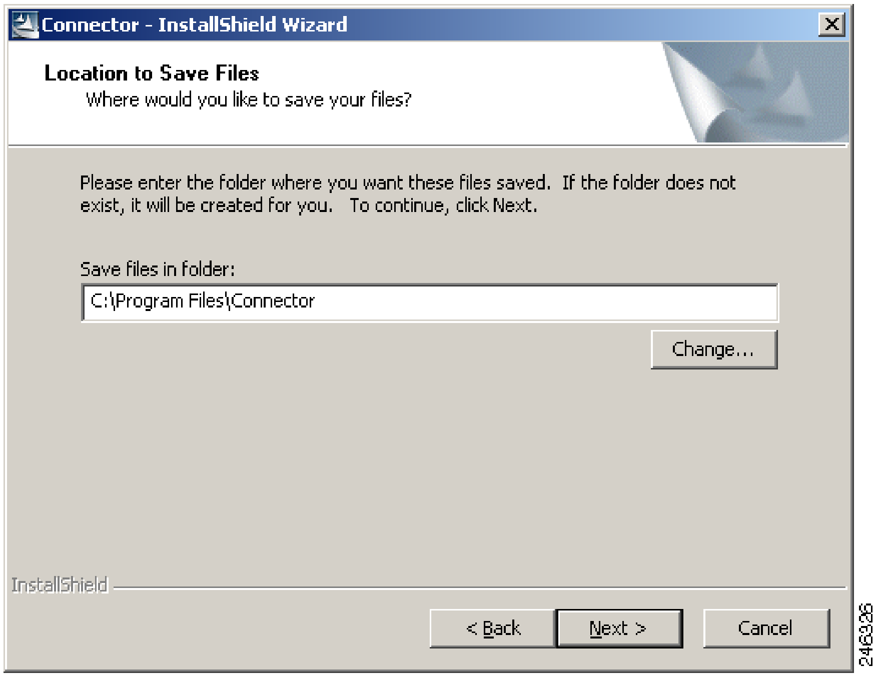
End User License Agreement

Please read the "End User License Agreement" included with this release before proceeding.

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Step 3 Read the End User License Agreement. If you agree to the terms, click **I accept the terms in the license agreement** then click **Next** to display the Location to Save Files dialog. Alternatively, if you do not agree to the terms, click **Cancel** to stop the installation.



Connector - InstallShield Wizard

Location to Save Files

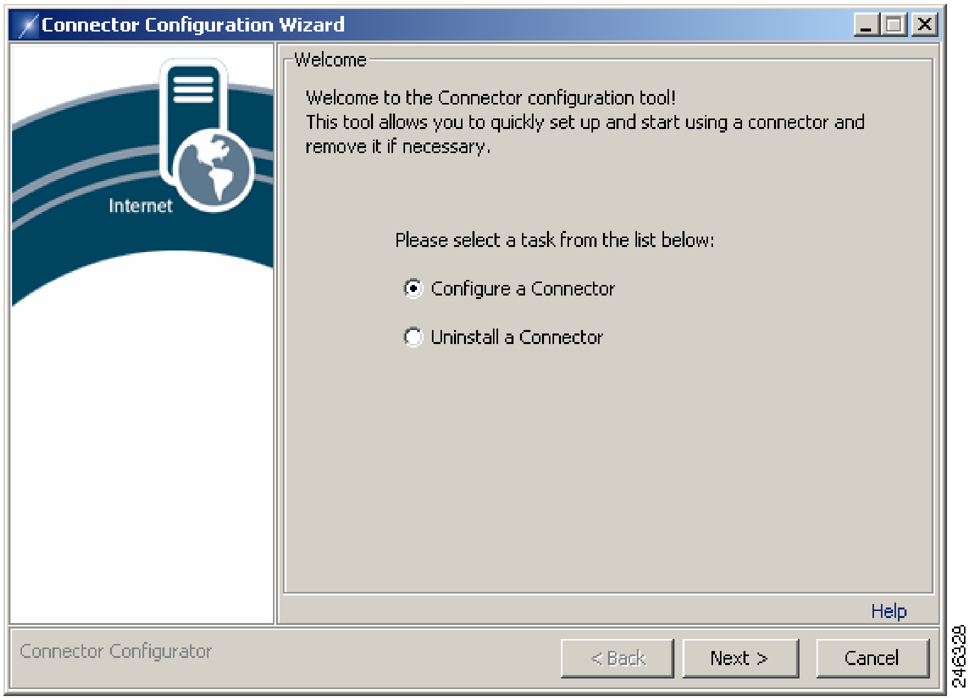
Where would you like to save your files?

Please enter the folder where you want these files saved. If the folder does not exist, it will be created for you. To continue, click Next.

Save files in folder:

C:\Program Files\Connector

Step 4 You must choose a different folder from the one in which you installed Connector. Enter a new path in the **Save files in folder** box, or click **Change** and navigate to the required folder, then click **Next** to display the Welcome dialog.



Welcome

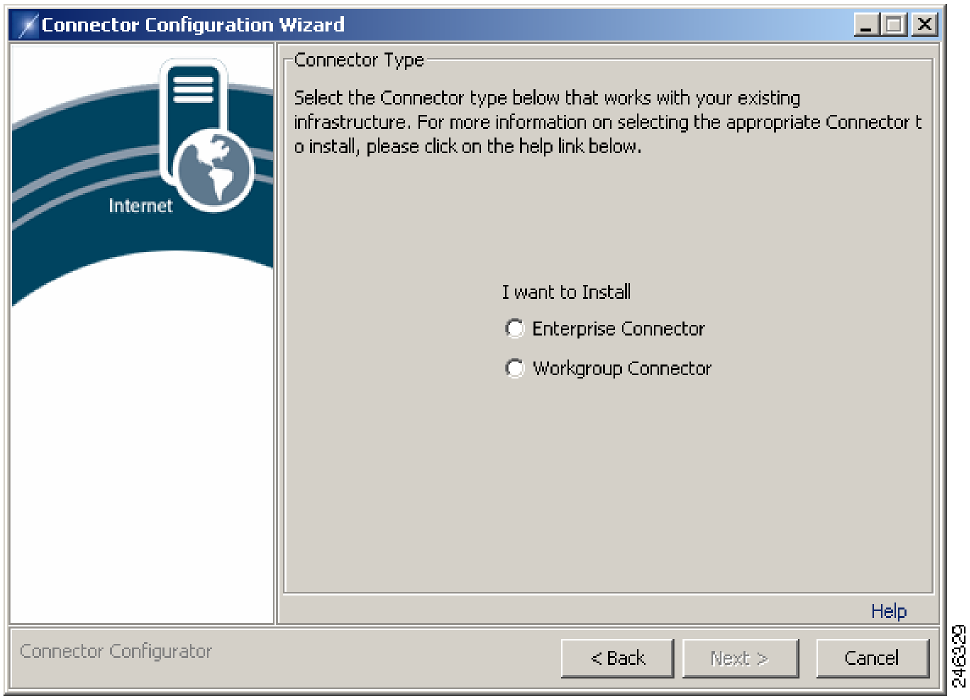
Welcome to the Connector configuration tool!
This tool allows you to quickly set up and start using a connector and remove it if necessary.

Please select a task from the list below:

● Configure a Connector

○ Uninstall a Connector

Step 5 Click **Configure a Connector** then click **Next** to display the Connector Type dialog.



Connector Type

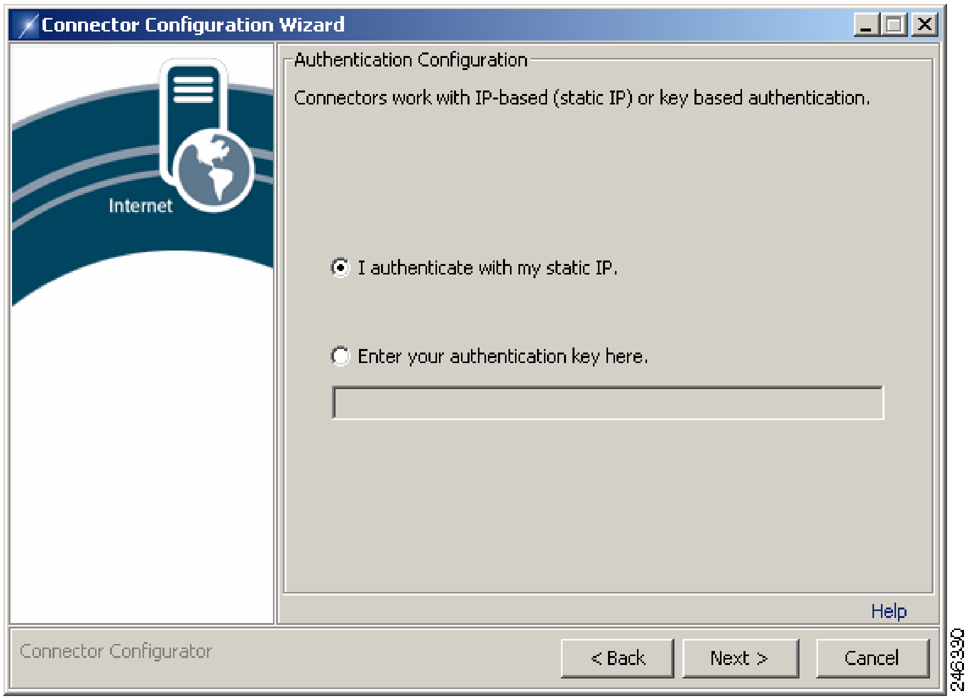
Select the Connector type below that works with your existing infrastructure. For more information on selecting the appropriate Connector t o install, please click on the help link below.

I want to Install

○ Enterprise Connector

○ Workgroup Connector

Step 6 Click **Enterprise Connector** then click **Next** to display the Authentication Configuration dialog.



Authentication Configuration

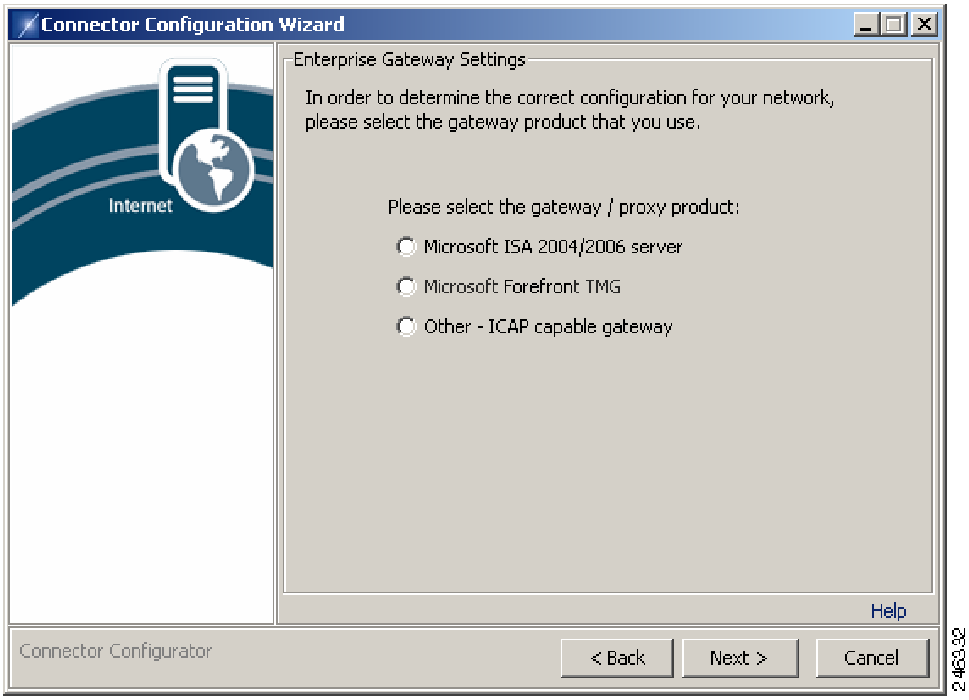
Connectors work with IP-based (static IP) or key based authentication.

● I authenticate with my static IP.

○ Enter your authentication key here.

Step 7 You can use IP-based or key based authentication. IP-based authentication requires a static IP address. To use IP-based authentication, click **I authenticate with my static IP**. Alternatively, click **Enter your authentication key here** and enter a company or group authentication key. For details of how to generate a key, refer to the *ScanCenter User Guide*.

Step 8 Click **Next** to display the Enterprise Gateway Settings dialog.



Enterprise Gateway Settings

In order to determine the correct configuration for your network, please select the gateway product that you use.

Please select the gateway / proxy product:

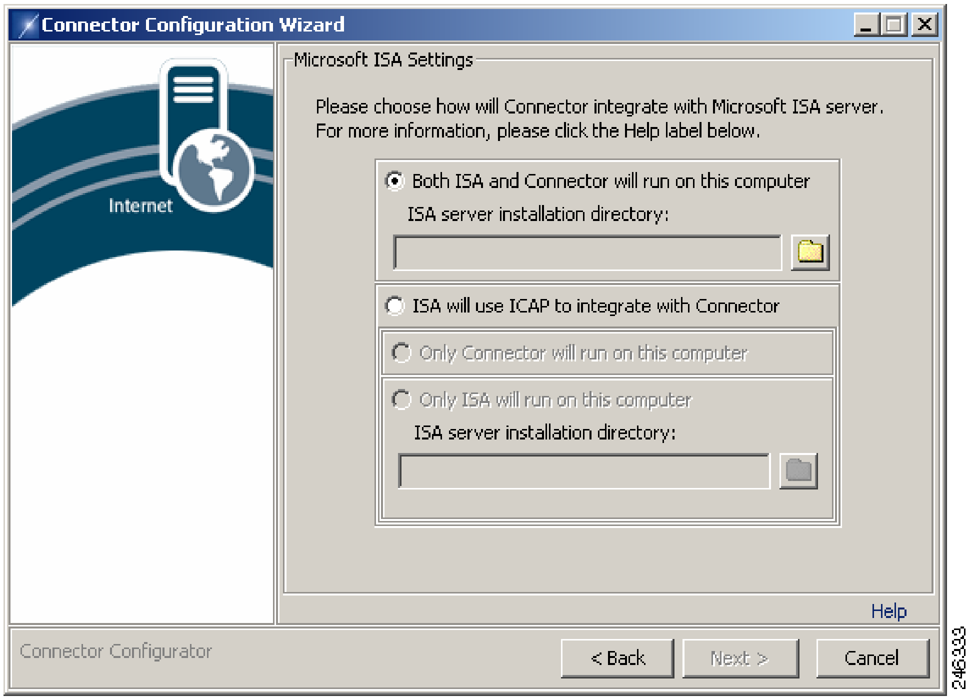
○ Microsoft ISA 2004/2006 server

○ Microsoft Forefront TMG

○ Other - ICAP capable gateway

Step 9 Click **Microsoft ISA 2004/2006 server**.

Step 10 Click **Next** to display the Microsoft ISA Settings dialog.



Microsoft ISA Settings

Please choose how will Connector integrate with Microsoft ISA server. For more information, please click the Help label below.

● Both ISA and Connector will run on this computer

ISA server installation directory:

○ ISA will use ICAP to integrate with Connector

○ Only Connector will run on this computer

○ Only ISA will run on this computer

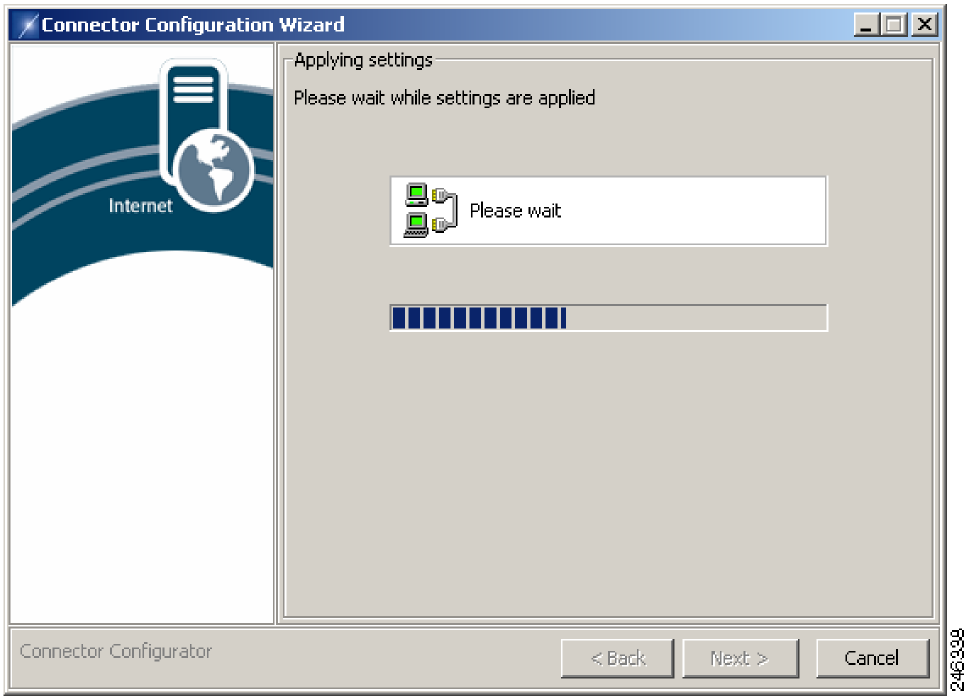
ISA server installation directory:

Step 11 Click **ISA will use ICAP to integrate with Connector**.

Step 12 Click **Only ISA will run on this computer**.

Step 13 Click the folder button and navigate to the folder where ISA is installed.

Step 14 Click **Next** to begin the configuration.



Connector Configuration Wizard

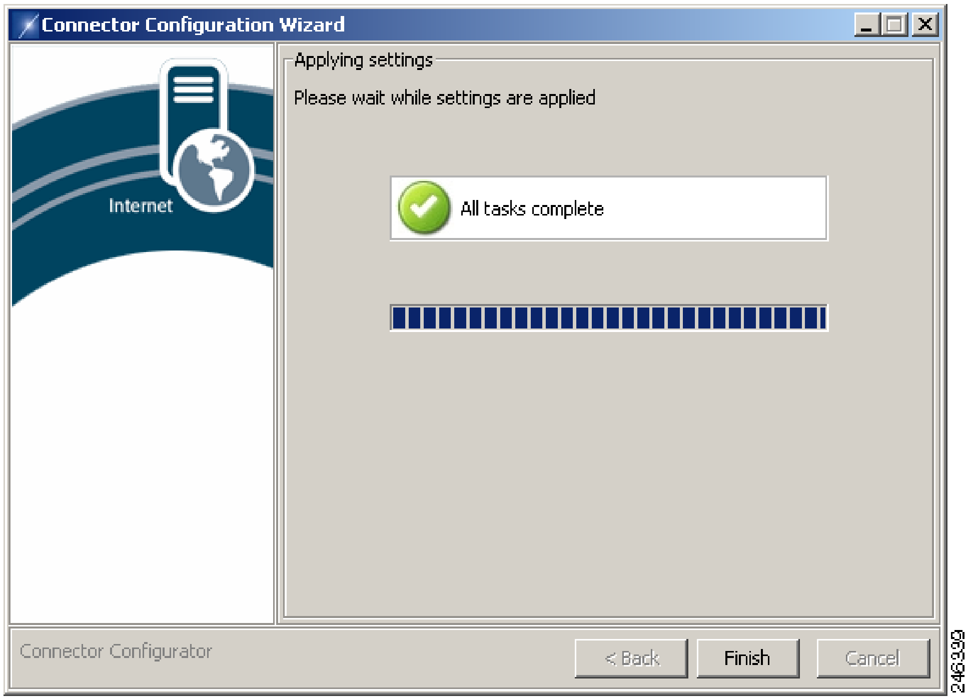
Applying settings

Please wait while settings are applied

Please wait

If the Microsoft Firewall service is running, you will be prompted to stop the service. The service will be restarted when the configuration is complete.

When the configuration tasks have completed successfully, the following dialog is displayed.



Applying settings

Please wait while settings are applied

All tasks complete

Connector Configurator

Step 15 Click **Finish** to close the wizard.

Post-Installation Forefront TMG or ISA Server Configuration

You can verify that the Connector plug-in has been installed in Forefront TMG or ISA Server by making sure you can see a Connector Plugin entry under the Web Filters tab.

To enable the plug-in you must edit the hosts file (typically C:\WINDOWS\system32\drivers\etc\hosts) and add the following entry:

```
127.0.0.1     connector
```

After Connector is installed you must configure Forefront TMG or ISA as follows:

Step 1 Ensure you have assigned your organization's Domain Name to the ISA Server's internal network object.

Step 2 Create an Access rule to allow the All Authenticated Users user set access to the Internet via FTP, HTTP and HTTPS. Ensure no other user sets are selected.

Step 3 Create a Web Chaining rule with the **Redirect them to a specified upstream server** action.

Step 4 Click Settings. In the Upstream Server Setting dialog, enter the Web Scanning Services primary proxy IP Address from your provisioning email in the **Server** box.

Step 5 Enter 8080 in the Port and SSL Port boxes.

Step 6 Ensure the **Automatically poll upstream server for the configuration** and **Use this account** check boxes are cleared.

Step 7 In the **Backup route** menu, click **Upstream proxy server**.

Step 8 Click **Settings**. In the Upstream Server Setting dialog, enter the Web Scanning Services secondary proxy IP Address from your provisioning email in the Server box.

Step 9 Ensure the **Automatically poll upstream server for the configuration** and **Use this account** check boxes are cleared.

Step 10 Apply your changes to Forefront TMG or ISA Server.

Enabling Persistent ICAP Mode

Creating a persistent connection to the ICAP server can improve performance in some circumstances. Customer support can help you to decide if you will benefit from enabling persistent ICAP mode.

Persistence ICAP mode is switched off by default. It can be enabled by adding the appropriate arguments to the connector agent.properties file and the TMG/ISA plug-in agent.properties file.

In the connector file add:

```
icap.connection.pool=true
```

In the ISA plug-in add:

```
persistentIcap=true
```

The ICAP persistence for the plug-in requires further parameters to control its operation:

```
minThreads=50
maxThreads=100
maxIdleTime=320
minIdleConnections=10
readTimeout=10
```

Note The above values are for a generic system and you may need to use different values. Contact customer support for further information on choosing appropriate values.

Applying the Windows Registry Patches

You will find two registry patch files in the folder where Connector was installed:

- `TCP-IP-BackLog.reg`
- `PortRangeAndSocketShutdownPatch.reg`

For versions of Windows prior to Windows Server 2008 R2 only, the `TCP-IP-BackLog.reg` patch should be applied. This increases the maximum number of connections in the backlog queue from 250 to 1000 and prevents Connector rejecting connections if there are already 250 ‘half open’ connections.

For all versions of Windows, the`PortRangeAndSocketShutdownPatch.reg` patch should be applied. This increases the short-lived (ephemeral) port range from 1024-5000 to 1024-65535 and changes the default timeout for these ports from four minutes to 30 seconds. This prevents the number of available ports being exhausted when a very large number of users are connecting to the service.

When you have applied the registry patches you must restart the server.

Bypassing the Web Scanning Services

In some cases you may need to bypass Web Scanning Services for particular Web sites or IP addresses, for example a Web site or Web application located on your intranet. In this case your users need to connect directly because the Web Scanning Services cannot access anything within your intranet.

To add an exception:

Step 1 Create a Web Chaining rule for System Policy Allowed Sites.

Step 2 Edit the System Policy Allowed Sites properties to include the Web sites for which you want to bypass the Web Scanning Services.

Step 3 Set the Request Action to ‘Retrieve requests directly from the specified destination.’

Step 4 Ensure the rule is applied before the Last Default rule.

Step 5 Apply your changes to ISA Server. You can add additional websites by editing the rule.

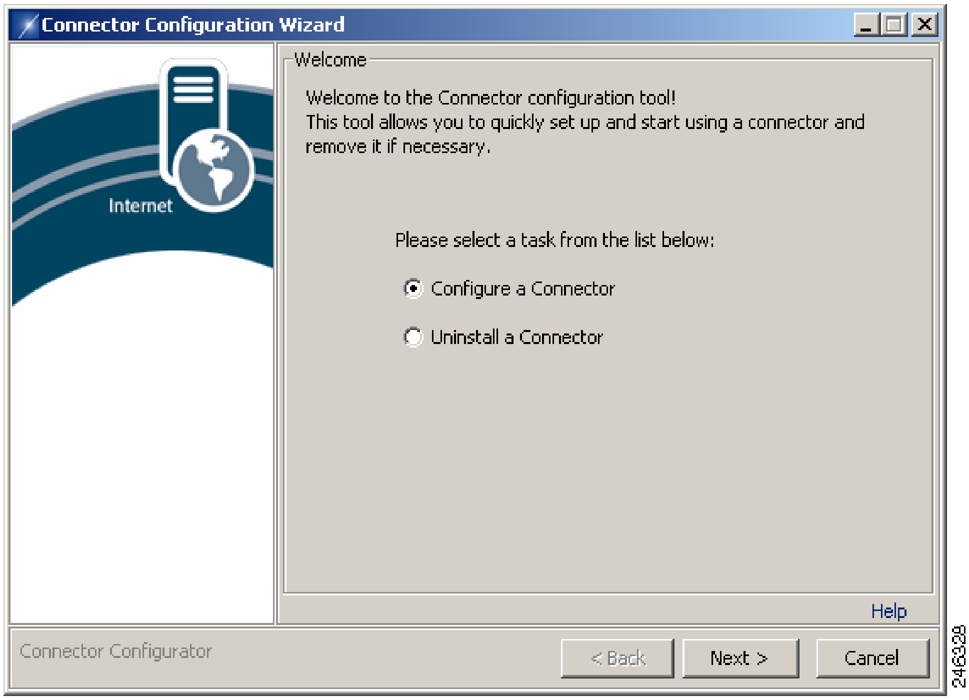
Upgrading Connector

To upgrade connector you must remove the currently installed version and then install the new version. Before removing the existing version you should make a backup of the `agent.properties` file as this contains your settings. When you have installed the new version of Connector you should replace the new version of the file with your backup.

Removing Connector

To remove Connector from a server:

Step 1 In the folder where you installed Connector, double-click the batch file to run the configuration wizard.



Connector Configuration Wizard

Welcome

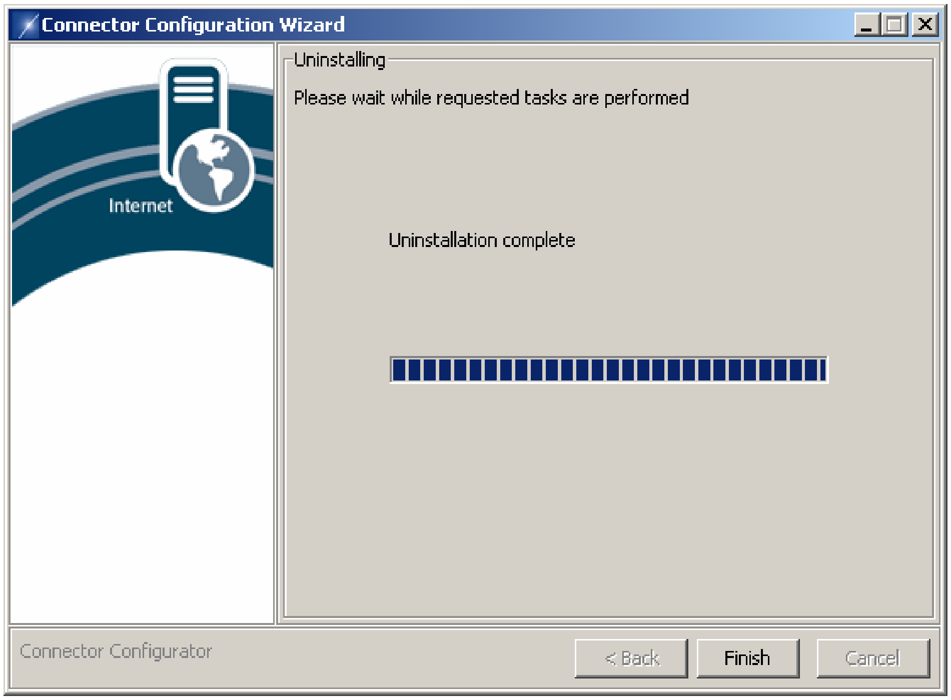
Welcome to the Connector configuration tool!
This tool allows you to quickly set up and start using a connector and remove it if necessary.

Please select a task from the list below:

● Configure a Connector

○ Uninstall a Connector

Step 2 Click **Uninstall a Connector** then click **Next** to remove Connector. When Connector has been removed successfully the following dialog is displayed:



Connector Configuration Wizard

Uninstalling

Please wait while requested tasks are performed

Uninstallation complete

Step 3 Click **Finish** to close the wizard. You will need to manually delete the folder where Connector was installed. It may be necessary to stop Forefront TMG or ISA Server to do this.

CHAPTER 3

Installing Connector on Linux

Revised: July 15, 2010

Overview

This chapter provides a step-by-step guide to installing the Linux Connector on x86 and x86-64 servers running either Red Hat Enterprise Linux version 5 or Cent OS Linux version 5. Connector is used to deliver web traffic from a client to the Web Scanning Services.

To enable Connector to integrate with the widest possible variety of software and devices it has two modes of operation, determined during installation.

- Standalone mode should be used when there are no edge devices on the corporate network.
- Enterprise mode should be used when an edge device, for example Microsoft ISA, is already present in the corporate network.

Cisco does not support the installation of the Linux Connector onto any other distributions of Linux or UNIX operating system, or any custom configuration beyond the instructions in this guide.

The chapter assumes you have followed the procedure detailed in this guide when installing either Red Hat or Cent OS Linux. Cisco strongly recommends that you follow every installation step as outlined rather than using your own Linux installation processes.

Before beginning installation, ensure that your server is suitably sized and capable of running the Linux operating system and Connector with the expected number of users. See Linux System Requirements, page 3-1.

Linux System Requirements

The Linux operating system has very basic hardware requirements. The following requirements are based the number of users expected to send their web traffic through Connector.

For deployments of 500 or more users, Cisco strongly recommends multiple servers are deployed behind a hardware load balancer to ensure there is no interruption of service in the event of a server failure. DNS load balancing (also known as round-robin) is not recommended due to the failover delay caused by caching of DNS responses by local computers.

Your technical account manager or a member of Cisco’s customer support team will be happy to discuss deployment options with you.

A TCP/IP network connection and outbound Internet access on TCP ports 80 and 8080 are required for all installations

.

Table 3-1 Test Environment (up to a maximum of 1,000 users)

Component	Requirements
CPU	Intel Xeon 2.5Ghz or higher
RAM	1GB minimum, 2GB or more recommended
Storage	1GB minimum, 4GB or more recommended

Table 3-2 SME (recommended for up to 3,500 users, theoretical maximum of 5,000 users)

Component	Requirements
CPU	Quad-core Intel Xeon 2.5Ghz or higher
RAM	2GB minimum, 3GB or more recommended
Storage	4GB minimum, 16GB or more recommended

Table 3-3 Enterprise (recommended for up to 7,500 users, theoretical maximum of 10,000 users)

Component	Requirements
CPU	Two Quad-core Intel Xeon 2.5Ghz or higher
RAM	4GB minimum
Storage	20GB minimum, 70GB or more recommended

Pre-Installation Requirements

Before installing Connector you must determine where it will be installed. Connector is very lightweight and does not require its own dedicated server. You must also ensure your firewall is configured correctly and SELinux is switched off. See Post-Installation Configuration, page D-12.

To prepare to install Connector:

Step 1 Determine which mode the connector will use See Overview, page 3-1.

Step 2 In ScanCenter, generate the authentication keys, as necessary. Keys are required for users with dynamic IP addresses only. Keys can also be used with static IP addresses.

Step 3 If you require the connector to perform group lookup with Active Directory or a Windows domain, create a dedicated user within the 'Domain Users' group of the primary domain controller.

Step 4 If you have stopped ISA Server to remove a previously installed version of the connector, restart it.

Accessing Your Server

To access your Linux server from a client computer you will need a secure shell (SSH) client.

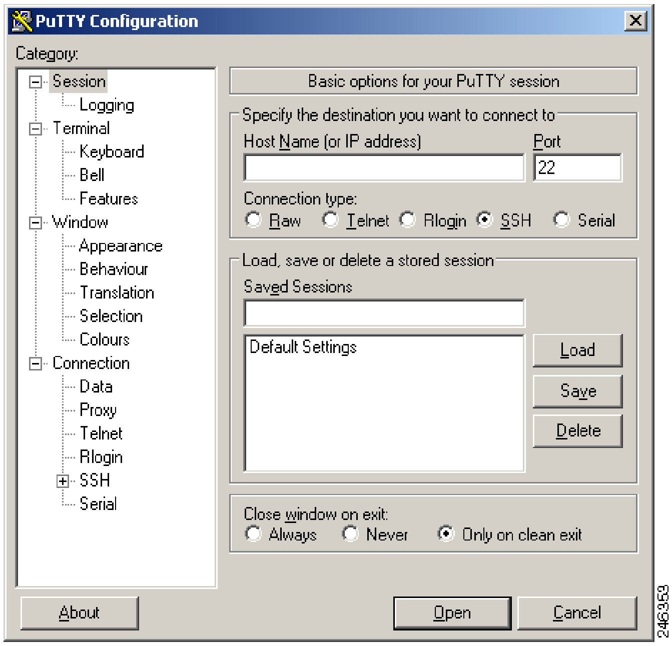
To download the free PuTTY SSH client for Microsoft Windows:

Step 1 Go to *http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html*.

Step 2 In the Binaries section, right-click the putty.exe hyperlink and then click Save Link As.

Step 3 Save the putty.exe file to your desktop.

Step 4 Double-click the putty.exe program file to run the SSH client.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions:

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

To connect to the Linux server:

Step 1 Enter the IP address of the Linux server in the Host Name box.

Step 2 Ensure the Connection type is SSH.

Step 3 Ensure the Port is 22.

Step 4 Click Open to connect to the server. The first time you connect to the server via SSH you may see a warning message about a trusted cache. This is normal, and you should accept the notification. Once a connection is established, the login screen is displayed.

Step 5 At the login prompt, type `root` and press Enter.

Step 6 At the password prompt, enter the root password you created during the Linux installation and press Enter. See Installing Linux, page D-1.

Note If you are unable to connect, confirm with your network administrator that your network firewall allows connections from your desktop computer to the Linux server on TCP port 22.

Installing the Runtime Environment

Connector is written in the Java language, which enables it to run on multiple platforms. However, like any Java application, it requires a Java runtime environment (JRE) to be installed on the host server.

Caution You must install the official Sun JRE. Alternatives such as JRockit and IcedTea are not supported and may prevent the Connector from running.

When you have logged in to your Linux server, the command prompt is displayed, for example

```
[root@localhost ~]#
```

Note The default server name is localhost. You may see a different hostname in your command prompt depending on the settings you entered during installation.

To install the Sun JRE:

Step 1 Change to the root directory to begin installation.

```
cd /root/
```

Step 2 If you have a 32-bit server, download the 32-bit Java installer.

```
wget http://80.254.145.118/linux/jre-6u13-linux-i586-rpm.bin
```

Alternatively, if you have a 64-bit server, download the 64-bit Java installer.

```
wget http://80.254.145.118/linux/jre-6u13-linux-x64-rpm.bin
```

If you are unsure if your server is 32-bit or 64-bit, download the 32-bit installer.

Step 3 Once the download has completed, make the program file executable.

```
chmod a+x ./jre-*.bin
```

Step 4 Run the program file to start the installation process.

```
./jre-*.bin
```

The Sun JRE license agreement is displayed.

Step 5 Read through the agreement. You can press Space to display the next page.

Step 6 Once you have read through the agreement, accept the terms.

```
yes
```

Step 7 Add the JAVA_HOME environment variable to the global server settings so it knows where to find the Java runtime environment:

```
echo export JAVA_HOME=/usr/java/latest >> /etc/profile
```

Step 8 Reload the profile:

```
source /etc/profile
```

Step 9 Test that Java has been installed correctly.

```
java –version
```

This command should display the Java runtime environment version. If you see any other output, please review the steps above before calling support.

Note In some instances it may be necessary to manually create a symbolic link with `ln -s /usr/java/latest/bin/java /usr/bin/java`.

Installing Connector

Before installing the Connector you must ensure the Sun JRE is installed. See Installing the Runtime Environment, page 3-4. The Linux default open file limit is too low and must be increased to support high traffic levels before installation.

Increasing the Open Files Limit

To increase the open files limit:

Step 1 At the command prompt, open the limits.conf file for editing.

```
vi /etc/security/limits.conf
```

The limits.conf file is displayed.

Step 2 Use the Down Arrow key to move the cursor to the end of the file.

Step 3 Press the A key to enter insert (or edit) mode.

Step 4 Type `conn` and press the Tab key.

Step 5 Type `hard` and press the Tab key.

Step 6 Type `nofile` and press the Tab key.

Step 7 Type `32768` and press the Tab key.

Step 8 Confirm that the text you have entered appears as follows:

```
conn hard nofile 32768
```

Step 9 Press the Esc key to exit editing mode.

Step 10 Type `:wq` to save your changes and exit the limits.conf file.

Running the Installer

When you have increased the open files limit, you can install Connector.

Step 1 At the command prompt, change to the root directory to begin installation.

```
cd /root/
```

Step 2 Download and execute the Connector installer (approximately 700 kb):

```
rpm -ivh http://80.254.145.118/linux/connector.noarch.rpm
```

Step 3 Confirm that installation was successful by typing:

```
ls /opt/connector/
```

Note You should see a listing of files including agent.properties. If you do not see a listing of files or see an error, check you have Internet connectivity and try the steps above again before contacting support.

Basic Connector Operations

To stop the Connector, at the command prompt type:

```
/etc/init.d/connector stop
```

To start the Connector, at the command prompt type:

```
/etc/init.d/connector start
```

To restart the Connector, at the command prompt type:

```
/etc/init.d/connector restart
```

For configuration instructions, see Configuring Connector, page 3-6.

Configuring Connector

Configuring the Connector is achieved by editing the main configuration file called agent.properties and restarting the Connector. There is no graphical interface for configuring the Linux Connector.

Contact your technical account manager or a member of the customer support team for assistance with configuring the Connector to your specific requirements and testing its functionality. This section is intended as a very basic overview to show you how to open the file for editing and how to apply your changes.

Note Your technical account manager or a member of the customer support team can provide a pre-configured agent.properties file which you can simply upload to the server. This is the easiest approach for new installations.

Before you can configure the Connector, you need to connect to your server either from the console or via an SSH connection. See Accessing Your Server, page 3-3. You should now be logged in to your Linux server, and see a prompt similar to:

```
[root@localhost ~]#
```

To configure the Connector:

Step 1 Open the agent.properties file for editing.

```
vi /opt/connector/agent.properties
```

Step 2 The agent.properties file will be displayed. Use the arrow keys to locate the configuration option you wish to edit, as directed by the customer support engineer.

Step 3 Press a to enter insert (or edit) mode.

Step 4 Use the Delete key to remove the existing configuration option, and type in your required modification.

Step 5 Press the Esc key (escape) to exit editing mode.

Step 6 Type `:wq` to save your changes and exit the agent.properties file.

Step 7 You must restart the Connector to apply your changes. This can take up to 60 seconds, and should be done at a quiet time.

```
/etc/init.d/connector restart
```

Step 8 When complete, type exit to close your SSH session.

Applying an Exception

An exception (or bypass) is used when you do not wish a particular website to be filtered by the Web Scanning Services. For example, you may use a secure site that restricts access to your offices egress IP address therefore in which case you would not want the web request to be routed through the shared filtering tower.

Note Your technical account manager or a member of the customer support team can provide assistance with configuring and applying exceptions. This is intended as a very basic reference.

Before you can add an exception, you need to connect to your server either from the console or via an SSH connection. See Accessing Your Server, page 3-3. You should now be logged in to your Linux server, and see a prompt similar to:

```
[root@localhost ~]#
```

To apply an exception:

Step 1 Open the agent.properties file for editing:

```
vi /opt/connector/agent.properties
```

Step 2 The agent.properties file will be displayed. Press the Page Down key to scroll to the bottom of the file.

Step 3 Press A to enter insert (or edit) mode

Step 4 Type in the exception, for example:

```
hotmail.com-exception_pattern=*hotmail.com
hotmail.com-primary_allowed=80,443
hotmail.com-primaryProxy=DIRECT
```

Step 5 Press the Esc key (escape) to exit editing mode

Step 6 Type `:wq` to save your changes and exit the agent.properties file

Step 7 You must restart the Connector to apply your changes. This can take up to 60 seconds, and should be done at a quiet time:

```
/etc/init.d/connector restart
```

Step 8 When complete, type exit to close your SSH session.

Upgrading Connector

Upgrading Connector to the latest General Availability (GA) version is straightforward.

To upgrade Connector:

Step 1 Change to the root directory to begin installation

```
cd /root/
```

Step 2 Backup the Connector configuration to the root directory

```
cp /opt/connector/agent.properties agent.properties-`date –I`
```

Step 3 Download and execute the Connector upgrade (approximately 700 kb):

```
rpm –Uvh http://80.254.145.118/linux/connector.noarch.rpm
```

Step 4 Restart the Connector to ensure the upgrade completes:

```
/etc/init.d/connector restart
```

You should now be able to browse the Internet through Connector. If you are unable to do so, you should contact support for assistance. You must provide a copy of the log files in /opt/connector/logs/.

CHAPTER 4

Configuring Connector

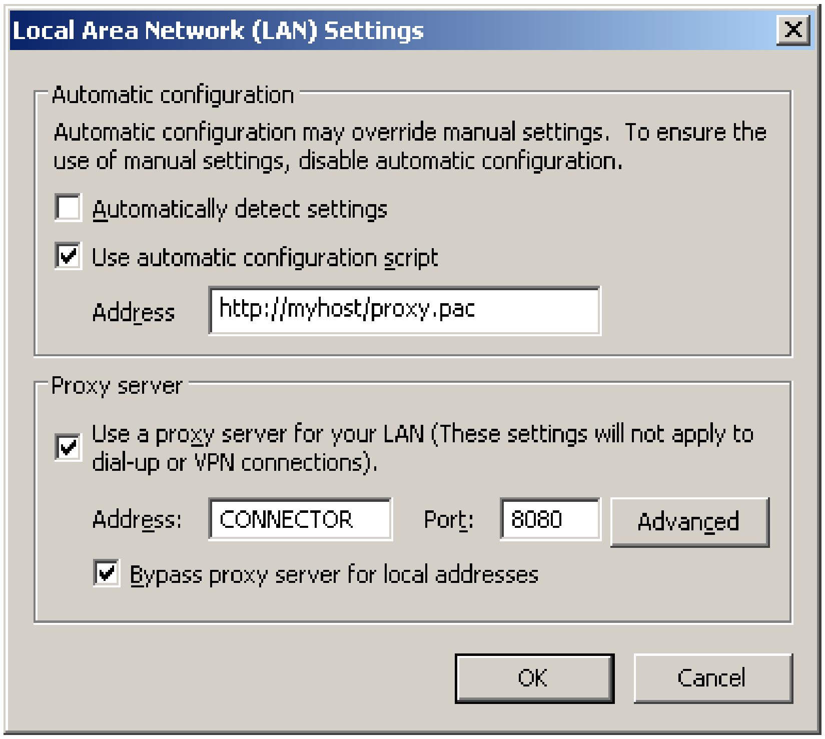
Revised: October 7, 2010

Overview

This chapter describes how to configure Connector, how to enable Acceptable Usage Policy (AUP) support, and how to configure your users' Web browser to use Connector.

Web Browser Configuration

When Connector is installed and running, you will need to configure your users' Web browser proxy settings to point to the Connector. For example, in Microsoft Internet Explorer this is configured in the Local Area Network (LAN) Settings dialog.



Local Area Network (LAN) Settings

Automatic configuration

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

□ Automatically detect settings

☑ Use automatic configuration script

Address: http://myhost/proxy.pac

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: CONNECTOR Port: 8080

☑ Bypass proxy server for local addresses

In this example the browser is configured to look for a Proxy Auto-Config (PAC) file on a local Web server and use that to configure the proxy settings automatically. In the event that the PAC file cannot be found, the browser will fall back to the local settings. The **Address** box must contain the IP address or DNS name of the server where Connector is installed. The **Port** box must contain 8080 (the default port that Connector listens to HTTP requests on).

In larger organizations, the most effective way to implement this change is either via a network Logon Script or through Group Policy Objects (GPO) in Active Directory.

The following sections are intended to help you choose the method that best suits your requirements.

Manual Configuration

This method allows the use of a single proxy defined in the browser connection settings. It is the simplest method and thus usually the more reliable choice.

The advantages are:

- It is simple to configure. All that is required is the location of the proxy and the relevant port.
- It is easy to enable the user to go direct to specified sites instead of using the proxy.
- In most situations, it is the more secure method.

The disadvantages are:

- It lacks flexibility. Only one proxy can be specified, so it is not possible to specify a failover proxy.
- The proxy setting must be applied to each machine. With Internet Explorer this can be pushed out via Group Policies, however with browsers such as Opera and Firefox the setting would have to be amended manually for each browser.

Proxy Auto-Config File

This is likely to be the preferred method in most cases. The location of the Proxy Auto-Config PAC file must still be set in each browser, either manually or by group policy. However, the PAC file allows greater control and flexibility limited only by the author’s ability to code the file in JavaScript and the infrastructure available.

The advantages are:

- The potential to implement failover proxies, load balancing, fault tolerance and so on.
- Scalability. The PAC file can be as complex as the requirements that need to be met.

The disadvantage is:

- Potentially a basic understanding of JavaScript programming may be necessary to create or amend PAC file scripts to meet requirements.

See Proxy Auto-Config Files, page B-1.

Web Proxy Auto-Discovery Protocol

The Web Proxy Auto-Discovery Protocol (WPAD) is a method used by Web browsers to locate a PAC file.

The advantages are:

- WPAD has all the advantages of using a PAC file.
- It requires the least amount of user and administrator intervention to set up each user.

The disadvantages are:

- It requires that explicit requirements are met before it can function correctly.
- The system serving the PAC file must have a high uptime level.
- There are inherent security issues.

See Web Proxy Auto Discovery Protocol, page C-1.

Connector Host and Client on the Same Computer

This method is used when Connector is installed on a portable computer for individual system use. The normal system requirements do not apply in this instance because Connector will only be processing the requests of a single user. You can use the client version of any of the supported server operating system. If you wish to use a different client opertaing system you should contact Support.

Note You must use the name localhost and port 8080 for the proxy server settings.

Host Exceptions

With Windows, host exceptions can be configured using the configuration wizard. See Adding Host Exceptions, page 2-12. It is also possible to edit or add exceptions by editing the agent.properties file in a text editor. With Linux this is the only method. See Configuring Connector, page 3-6.

Host exceptions are added using the following properties:

```
<exception name>-exception_pattern=<host patterns> (mandatory)
<exception name>-primaryProxy =<primary proxy> (mandatory)
<exception name>-primaryProxyPort=<primary proxy port> (only applicable if
primaryProxy is not DIRECT)
<exception name>-primary_allowed=<allowed port list for primary> (only applicable if
primaryProxy is DIRECT)
<exception name>-secondaryProxy=<secondary proxy>
<exception name>-secondaryProxyPort=<secondary proxy port> (only applicable if
secondaryProxy is not DIRECT)
<exception name>-secondary_allowed=<allowed port list for secondary> (only applicable
if secondaryProxy is DIRECT)
<exception name>-tertiaryProxy=<tertiary proxy>
<exception name>-tertiaryProxyPort=<tertiary proxy port> (only applicable if
tertiaryProxy is not DIRECT)
<exception name>-tertiary_allowed=<allowed port list for tertiary> (only applicable if
tertiaryProxy is DIRECT)
```

Example Host Exceptions

To configure an exception with a single proxy on a specific IP address and port for a range of domains use the following:

```
<exception name>-exception_pattern=*.<domain1>, *.<domain2>
```

```
<exception name>-primaryPorxy=<IP>
<exception name>-priumaryProxyPort=<port>
```

For example:

```
SPS-exception_pattern=*.amazon.co.uk, *.amazon.com
SPS-primaryProxy=192.168.32.122
SPS-primaryProxyPort=8081
```

To configure an exception with a direct connection for a range of domains on port 8080 (the default) use the following:

```
direct-exception_pattern=*.<domain1>, *.<domain2>
direct-primaryProxy=DIRECT
```

For example:

```
direct-exception_pattern=*.verisign.com, *.nwolb.com
direct-primaryProxy=DIRECT
```

To configure an exception with a direct connection for all hosts on a given domain using the default port use the following:

```
<exception name>-exception_pattern=*.<domain>
<exception name>-primaryProxy=DIRECT
```

For example:

```
microsoft-exception_pattern=*.microsoft.com
microsoft-primaryProxy=DIRECT
```

To enable additional ports use the following:

```
<exception name>-exception_pattern=*.<domain>
<exception name>-primaryProxy=DIRECT
<exception name>-primary_allowed=<port1>, <port2>
```

For example:

```
microsoft-exception_pattern=*.microsoft.com
microsoft-primaryProxy=DIRECT
micorsoft-primary_allowed=443, 8443, 1245
```

Note When specifying custom ports, you must explicitly specify the default ports. Ports 443 and 8443 are commonly used for HTTPS traffic. These common ports are allowed by default if no custom allowed ports are specified.

Acceptable Usage Policy

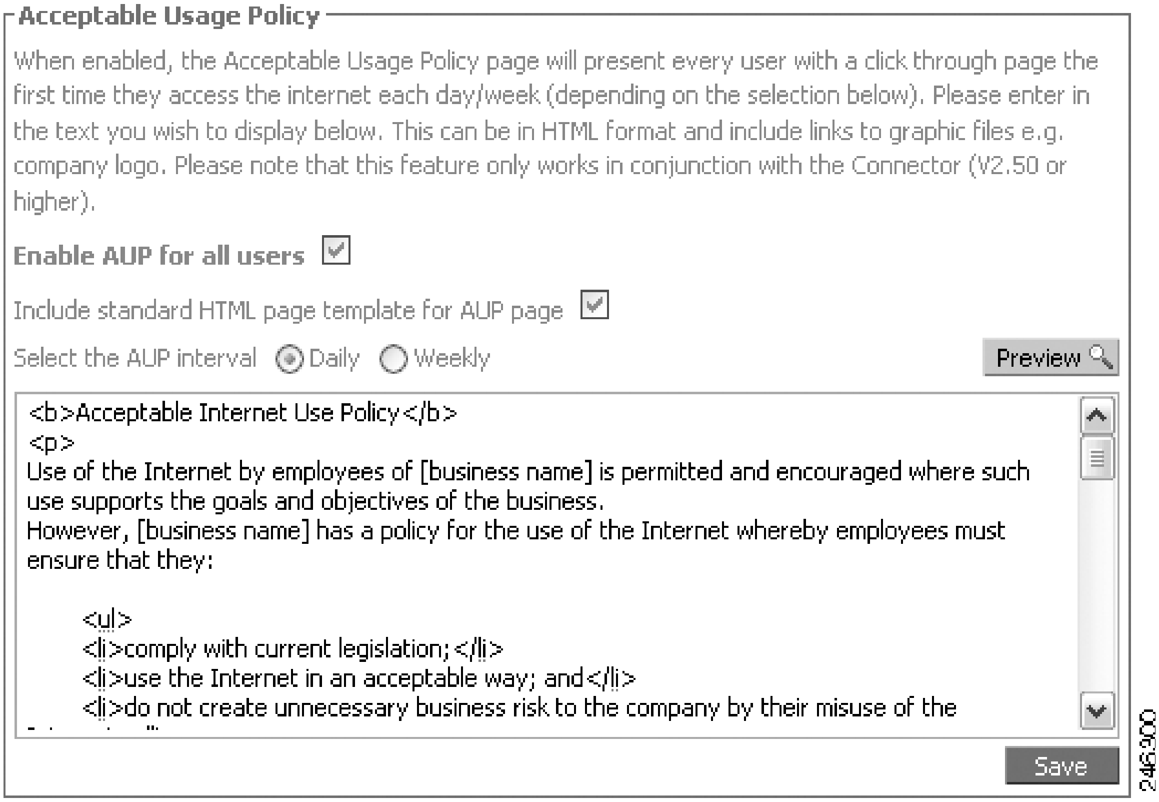
To show an Acceptable Usage Policy (AUP) page to your users on a daily or weekly basis with Connector in workgroup mode:

Step 1 Edit the agent.properties file and add the line

```
aup.enable=true
```

Step 2 Restart Connector.

Step 3 In ScanCenter, navigate to the **Global Settings** page and ensure the Acceptable Usage Policy pane is shown. If it is not shown, contact support to have this enabled for your account.



Acceptable Usage Policy

When enabled, the Acceptable Usage Policy page will present every user with a click through page the first time they access the internet each day/week (depending on the selection below). Please enter in the text you wish to display below. This can be in HTML format and include links to graphic files e.g. company logo. Please note that this feature only works in conjunction with the Connector (V2.50 or higher).

Enable AUP for all users ☑

Include standard HTML page template for AUP page ☑

Select the AUP interval ● Daily ○ Weekly

```
<b>Acceptable Internet Use Policy</b>
<p>
Use of the Internet by employees of [business name] is permitted and encouraged where such
use supports the goals and objectives of the business.
However, [business name] has a policy for the use of the Internet whereby employees must
ensure that they:

      <ul>
      <li>comply with current legislation;</li>
      <li>use the Internet in an acceptable way; and</li>
      <li>do not create unnecessary business risk to the company by their misuse of the
```

Step 4 Select the **Enable AUP for all users** check box.

Step 5 Select the **Include standard HTML page templates for AUP page** if you want to include the default image and text on the AUP page.

Step 6 Click **Daily** or **Weekly** to set how often the page is displayed.

Step 7 Edit the HTML in the box.

Step 8 Click **Save** to save your changes.

A sample page is provided as a template to use if your organization does not currently have an AUP. However, recommends you seek professional advice in creating your own AUP. Care should be taken to include references to the latest Web 2.0 technologies and you should lock down your users' portable computers so that they can only use the Internet through the Web Scanning Services (both internally and externally). Any attempt to circumvent this should be strictly prohibited in the AUP. All AUP pages will have an I Agree button at the bottom of the page for users to click. You should include this in your AUP, stating that by clicking I Agree the user agrees to abide by your organization's AUP.

When the **Include standard HTML page templates for AUP page** check box is cleared you can specify the full content of the page, from the opening `<html>` tag to the closing `/html>` tag. Any images or CSS (cascading style sheets) must be stored at a resolvable location. Normally you must host your own images and CSS. When you have saved your changes you can view the AUP page by clicking the Preview button.

Note The AUP page relies on the quota functionality of Connector. If Connector is reset, the count will also reset to zero and the AUP page will be displayed again to users.

SSL Tunneling

You can send all Web traffic to the Web Scanning Services using an SSL-based tunnel. Note that not all Web Scanning Service proxies support this functionality and you should work with the support team to make sure you are provisioned on a proxy that supports this functionality.

Note Enabling the SSL Tunneling feature will put additional load on the server running Connector. It will also add a small amount of extra latency into the link. Your organization is responsible for the use of this feature. Cisco does not condone its use to bypass country based firewall blocking.

LDAP Servers

Connector supports the use of multiple LDAP servers, including generic LDAP servers such as Lotus Domino. By default, Connector uses Active Directory LDAP.

Generic LDAP

Connector supports basic authentication lookups against generic LDAP servers. You may have to change the default settings in your LDAP server to allow this.

In order to perform generic LDAP lookups you need to enable basic authentication rather than NTLM authentication in the agent.properties file:

```
useNtlm=false
useBasic=true
auth.realm=MyRealm
passwordRequired=true
```

You can also change the name of the realm that appears in the basic authentication dialog by changing the auth.realm value.

After selecting basic authentication, the LDAP server must be configured. By default the LDAP type is Active Directory. To use generic LDAP use the following:

```
ldap.type=generic
useLdap=true
useNtlm=false
useBasic=true
providerUrl=ldap://127.0.0.1:3268
securityPrincipal=cn=proxyagent,cn=users,dc=company,dc=com
ldap.base.dn=ou=People,dc=example,dc=com
ldap.user.attr=uid
ldap.group.attr=ou
ldap.accountdisabled.attribute=
ldap.group.attr.string.parse=
```

The `ldap.base.dn` property specifies the base DN in the LDAP tree where the query starts.

The `ldap.user.attr` is the name of the user attribute in the LDAP server configuration.

The `ldap.group.attr` is the name of the group attribute in the LDAP server configuration.

The `ldap.accountdisabled`.attribute, if it has a non-empty value, represents the name of the attribute that flags if the user is allowed to browse. If a user is marked as 'disabled' in the LDAP server, then that user is not allowed to browse, even if they provide the correct password and user account when prompted with the basic authentication dialog.

The `ldap.group.attr.string.parse` property is the name of the attribute for parsing out the group name from a LDAP query response. For example, if the response to the group LDAP query is `ou=mygroup, o=mycompany, l=mylocation`, then by specifying ldap.group.attr.string.parse=ou the group name is parsed out from the LDAP response string, which in this case is mygroup.

Novell

The Connector LDAP settings for Novell LDAP are:

```
useNtlm=false
useBasic=true
auth.realm=<realm>
ldap.type=generic
useLdap=true
providerUrl=ldap://<IP address>:389
securityPrincipal=cn=<admin user name>,o=<context path>
securityCredentials=<admin password>
ldap.base.dn=o=<context path>
ldap.user.attr=cn
ldap.group.attr=groupMembership
ldap.group.attr.string.parse=cn
```

Lotus Domino

The Connector LDAP settings for Lotus Domino are:

```
useNtlm=false
useBasic=true
auth.realm=<realm>
ldap.type=generic
useLdap=true
providerUrl=ldap://<IP address>:389
securityPrincipal=cn=<admin user name>,o=<organization>
securityCredentials=<admin password>
ldap.base.dn=o=<organization>
ldap.user.attr=cn
ldap.group.attr=dominoaccessgroups
ldap.group.attr.string.parse=cn
```

Secondary LDAP Server

Connector supports secondary LDAP servers in case of primary failure. For backward compatibility, primary settings can also be specified without '.primary' suffix. For example:

```
providerUrl.primary=ldap://192.168.10.251:3268
securityPrincipal.primary=cn=proxyagent,cn=users,dc=UK,dc=mycompany,
dc=com
securityCredentials.primary=abc
providerUrl.secondary=ldap://192.168.0.251:3268
securityPrincipal.secondary=cn=proxyagent,cn=users,dc=UK,
dc=mycompany0,dc=com
securityCredentials.secondary=abc
Secondary settings can also be specified for a particular domain:
```

```
providerUrl.primary.uk=ldap://192.168.10.251:3268
securityPrincipal.primary.uk=cn=proxyagent,cn=users,dc=UK,
dc=mycompany,dc=com
securityCredentials.primary.uk=abc
providerUrl.secondary.uk=ldap://192.168.0.251:3268
securityPrincipal.secondary.uk=cn=proxyagent,cn=users,dc=UK,
dc=mycompany,dc=com
securityCredentials.secondary.uk=abc
```

Multiple LDAP Servers and Domains

Connector can support multiple LDAP Servers and domains. Default LDAP must be switched off, but otherwise the initial configuration is similar to that for a single LDAP server.

```
useLdap=false
providerUrl=ldap://192.168.0.251:3268
securityPrincipal=cn=proxyagent,cn=users,dc=UK,dc=company,dc=com
securityCredentials=mBxm8shsZArd1ds3dbw_-DsSBrGK5x
ldapRefreshTimeout=3600000
```

Connector has the ability to specify a separate LDAP server for specific domains. For example, given this authorization user name obtained from the NTLM challenge: UK\somebody, you can set up a specific LDAP server that will be queried to get the group details for this user. For example:

```
useLdap.UK=true
providerUrl.UK=ldap://127.0.0.1:3268
securityPrincipal.UK=cn=proxyagent,cn=users,dc=company,dc=com
securityCredentials.UK="?H&*FH
```

Note The `ldapRefreshTimeout` property is global. It is configured for all the configured LDAP servers.

To configure specific LDAP servers for querying groups for certain domains you will need to use the domain name as a suffix for the LDAP properties as in the previous example.

The `useLdap.`*`<domain>`* properties are always mandatory for all defined LDAP servers. The name of the domain is case sensitive.

If any of the other properties for the extending LDAP servers is missing, then the property will be inherited from the default LDAP setting.

Caution Unless a default LDAP server configuration is defined, Connector will use default values. The default configuration acts as fallback for domains for which there is no explicit configuration. For example, to find the domains for the user WinNT://SOMEDOMAIN\someuser and where there is no configuration for SOMEDOMAINdomain, the default configuration will be used.

It is also possible to assign multiple domain names to a domain configuration. You can do this with the domains property, for example:

```
useLdap.UK=true
providerUrl.UK=ldap://127.0.0.1:3268
securityPrincipal.UK=cn=proxyagent,cn=users,dc=company,dc=com
domains.UK=DOMA,DOMB,DOMC
securityCredentials.UK="?Y*FH
```

In this example the UK domain configuration will be assigned to the domains DOMA, DOMB and DOMC, but not UK. To include the UK domain name for this configuration you would need to define it in the list of the acceptable domains:

```
domains.UK=DOMA,DOMB,DOMC,UK
```

Groups

Connector enables you to manage connections based on group membership. You can enable multiple authentication keys by group, exclude groups from Web filtering, and set the depth of nested groups.

Note Group names such as WinNT://UK\dev must have the backslash escaped in the agent.properties configuration file, that is WinNT://UK\\dev.

Multiple Authentication Keys

Multiple authentication keys can be specified in the agent.properties file. Authentication keys will be mapped to the groups user belong to, for example:

```
licence.1=authkey1
licence.1.groups=a,b,c
licence.2=authkey2
licence.2.groups=d,e
licence=defaultauthkey
```

In the example, if a user belongs to group a, b, or c then the licence.1 authentication key is used. If the user belongs to group d or e then the licence.2 authentication key is used. If the user does not belong to any of these groups then the default authentication key is used.

The groups can also contain trailing wildcards, for example:

```
licence.1.groups=WinNT://UK*
```

This would match all the groups that start with WinNT://UK.

Excluding Groups

Many organizations use a large number of directory groups for different internal functionality. Adding all these groups into the headers would create a large overhead on each request. To avoid this, Connector can exclude any groups that are not relevant to Web filtering.

Groups to be excluded are specified in the agent.properties file. You can either have global group exclusions which apply across all directories or specific exclusions on a directory basis.

Any combination of filters is permitted. If no filters are defined or if both are empty, there will be no group filtering at all.

Global Group Exclusions

This exclusion applies to all groups determined by both LDAP and Domain Controller querying. The property for this filter is called groupInclude. If it is absent, or empty, there will be no global group filtering at this level. Group names are case insensitive and they must be comma separated, for example:

```
groupInclude=Winnt://UK\\Dev, Winnt://UK\\others
```

LDAP Group Exclusions

These exclusions apply per LDAP setting only. The default LDAP configuration cannot have group filters (use the global group filters in this case). If it is absent, or empty, there will be no global group filtering at this level, for example:

```
useLdap.UK=true
providerUrl.UK=ldap://127.0.0.1:3268
securityPrincipal.UK=cn=proxyagent,cn=users,dc=UK,dc=domain, dc=com
securityCredentials.UK=mBxm8Ard1dwIdTs3dbw_-DsSBrGK5x
groupInclude.UK=WinNT://UK\\dev,WinnT://UK\\test
```

Nested Groups

Connector supports nested groups. By default the depth for the nested group hierarchy is five. Nested groups can be configured by adding the following properties to the agent.properties file.

groupslookup.recursive.depth	The depth for the nested groups, the default value is 1. Nesting can be switched on by setting the value to 2 or higher.
groupslookup.recursive.exclude	A comma separated list of groups which should be excluded from nesting.

This groupslookup.recursive.exclude property can also be set for the domain, for example:

```
groupslookup.recursive.exclude.UK
```

This will contain the exception groups for UK domain.

APPENDIX A

Agent Properties

Revised: February 11, 2011

The agent.properties file contains the configuration settings for Connector. Typically, properties containing lists do not support the uses of spaces between separators.

Caution Before changing the settings of the agent.properties file you should discuss your requirements with customer support. In the worst case, certain settings could lead to Connector effectively blocking all traffic.

Setting	Description	Default	Alternate
`<exception name>-exception_pattern`	See Host Exceptions, page 4-3.		`<pattern1> [,<pattern2>...]`
`<exception name>-primaryProxy`	See Host Exceptions, page 4-3.		`<IP address or host name>`
`<exception name>-primaryProxyPort`	See Host Exceptions, page 4-3.		`<port>`
`<exception name>-secondaryProxy`	See Host Exceptions, page 4-3.		`<IP address or host name>`
`<exception name>-secondaryProxyPort`	See Host Exceptions, page 4-3.		`<port>`
`<exception name>-tertiaryProxy`	See Host Exceptions, page 4-3.		`<IP address or host name>`
`<exception name>-tertiaryProxyPort`	See Host Exceptions, page 4-3.		`<port>`
`aup.enable`	Enable Acceptable Usage Policy support for Connector in standalone mode. This is not supported in enterprise mode.	`FALSE`	`TRUE`
`auth.realm`	The name of the realm that appears in the basic authentication dialog.		`<realm>`

`backlog.size`	Maximum number of connections to queue.	`100 (Windows)`
		`900 (Linux)`
			`<number>`

`brand.file`	File that applies any branding text.	`branding.properties`	`<filename>`

Setting	Description	Default	Alternate
defaultUpstreamPort	The value used when upstream ports for primary, secondary, or tertiary upstream proxies are not specified. For example, if secondaryProxy is specified and secondaryProxyPort is not, the defaultUpstreamPort value will be used.	8080	<port>
domains.<domain>	Comma separated list of domains to be grouped under a single domain for LDAP queries. This will override individual domain settings.		<domain>
elb.buckets	Specifies how many upstream servers Connector should do load balancing to.	1	<number>
elb.enable	Used to enable enterprise load balancing.	FALSE	TRUE
elb.mode	Sets the load balancing policy.	client-ip	host
encryptHeaders	Sets whether or not Connector encrypts headers added to a request. Do not change this setting unless explicitly instructed to do so by a support engineer.	TRUE	FALSE
encryptionVersion	Sets the headed encoding: 0 - hex, 1 - base-64 encoded and gzipped (smallest but increases CPU load), or 2 - base-64 (larger than 1 but faster)	2	0
groupInclude	Comma separated list of groups to be sent to the Web Scanning Services. All other groups (which are not relevant to Web filtering) are excluded. Note the double \ and /. The domain and group only are case insensitive.	all groups	WinNT://<domain>\\<group>
groupslookup.recursive.depth	The depth for nested groups. A setting of 1 switches off support for nested groups.	1	<number>
groupslookup.recursive.exclude	A comma separated list of exception groups which should not be included in nesting.	no groups	WinNT://<domain>\\<group>
http.failover.alivePoll	Whether to check if the upstream Web Scanning Services proxy server is available.	FALSE	TRUE
http.failover.alivePollDelaySec	Delay in seconds between checks.	30	<number>
http.failover.aliveRepeatsToWhiteList	Number of successful requests before removal from the blacklist.	1	<number>

Setting	Description	Default	Alternate
http.failover.failPollDelaySec	How often in seconds to poll blacklisted proxy servers.	3	<number>
http.failover.failRepeatsToBlacklist	Number of failures before adding to blacklist.	5	<number>
http.failover.numberOfRetriesForResource	Number of retries to count as failure.	2	<number>
httpAddress	Interface to bind to for HTTP.		<IP address>
httpPort	The port which Connector listens to for HTTP traffic.	8080	<port>
icap.generate.random.istag	Enables Connector to respond with random ISTags required by some gateways.	FALSE	TRUE
icapAddress	Interface to bind to for ICAP.		<IP address>
icapPort	The port on which Connector should listen for ICAP traffic.	1344	<port>
install.mode	Sets workgroup or enterprise mode.		enterprise.install workgroup.install
keepalive.enable	Keep-Alive enabled.	FALSE	TRUE
ldap.accountdisabled.attribute	Where a value is specified, the name of the attribute that flags if the user is allowed to browse. A user with a 'disabled' account in the LDAP server is not allowed to browse, even if the correct user name and password are provided at the basic authentication dialog.		
ldap.base.dn	The base DN in the LDAP tree where the query starts.		ou=People,dc=<company>,dc=com
ldap.failover.alivePoll	When set to TRUE, the LDAP Resource Manager polls resources to determine if they are available.	FALSE	TRUE
ldap.failover.alivePollDelay	The delay in seconds between polling available LDAP resources.	30	number
ldap.failover.aliveRepeatsToWhitelist	The number of successful repeat attempts to connect to an LDAP server with its status set to unavailable before its status is changed to available.	1	<number>
ldap.failover.failPollDelay	The delay between attempts to connect to LDAP servers that have had their status changed to unavailable.	3	<number>
ldap.failover.failRepeatsToBlacklist	Number of failures before the primary LDAP server's status is changed to unavailable.	5	<number>

Setting	Description	Default	Alternate
ldap.failover.numberOfRetriesForResource	Number of retries to count as failure. Applied to both the primary and secondary LDAP server.	2	<number>
ldap.connect.timeout	Number of milliseconds before connection time-out.	0	<number>
ldap.group.attr	The name of the group attribute in the LDAP server configuration.	ou	
ldap.group.attr.string.parse	The name of the attribute for parsing out the group name from an LDAP query response. For example, if the response to the group query is ou=mygroup, o=mycompany, l=location then by setting the ldap.group.attr.string.parse to ou you would derive the group name mygroup.		
ldap.read.timeout	Number of milliseconds before read time-out.	0	<number>
ldap.type	Type of LDAP in use, either Active Directory or generic.	ad	generic
ldap.user.attr	The name of the user attribute in the LDAP server configuration.	uid	
ldapRefreshTimeout	The amount of time in milliseconds that Connector should remember a user's group details before querying the LDAP/Active Directory server again. This can greatly reduce the number of requests made via LDAP and increase the speed at which Connector services requests.	0	<number>
licence	Company, Group or User authentication key generated in the portal and used to identify computers where the egress IP has a dynamically assigned IP address.		<authentication key>
local.response.html.file	HTTP error 503 page.	etc/localresponse.html	<relative path from location of agent.properties file>
logLocation	The location of the log files. Do not change this setting unless explicitly instructed to do so by a support engineer.		<relative path from location of agent.properties file>
lowercase.user	Make user names lowercase.	FALSE	TRUE
ntlm.authenticate	Enables validation of credentials provided by the user's Web browser.	FALSE	TRUE

Setting	Description	Default	Alternate
ntlm.dc.primary	Address of the primary Windows Domain Controller. This must be specified if ntlm.authenticate or ntlm.lookup.groups are set to true.		<IP address or host name>
ntlm.dc.secondary	Address of the secondary Windows Domain Controller.		<IP address or host name>
ntlm.dc.tertiary	Address of the tertiary Windows Domain Controller.		<IP address or host name>
ntlm.icap.auth.password	The password that Connector uses when authenticating with an Active Directory/NT4 domain. Used only in ICAP mode.		<password>
ntlm.icap.auth.user	The user name Connector uses to identify itself to an Active Directory/NT4 domain. Used only in ICAP mode. Note the double \ and /. The domain and group only are case insensitive.		WinNT://<domain>\\ <user name>
ntlm.lookup.groups	Enables group lookups via NTLM using the Domain Controller. Overrides the LDAP.lookup.groups setting when TRUE.	FALSE	TRUE
ntlm.preauth.domain	The domain controller used for SMB signing. The ntlm.preauth settings are required when using Windows Server 2003 or later.		
ntlm.preauth.username	The user name of a normal user of the domain controller.		
ntlm.preauth.password	The password of the user of the domain controller.		
ntlm.timeout	Number of milliseconds before time-out.	0	<number>
ntlmIpExceptions	Comma separated list of IP addresses (not hostnames) of computers you wish to exclude from NTLM authentication requests.		<IP address>
pool.max.size	Maximum number of threads.	1500 (on Linux you should change this value to 3000)	<number>
pool.prestart.corethreads	Create threads on startup.	TRUE	FALSE
pool.queue.size	Number of threads to queue.	50	<number>
pool.start.size	Minimum number of threads created on startup.	250	<number>

Setting	Description	Default	Alternate
primaryProxy	The primary Web Scanning Services proxy included in your provisioning email.		<IP address or host name>
primaryProxyPort	The primary Web Scanning Services proxy port included in your provisioning email.		<port>
primaryProxyType	Sets whether SSL tunneling is enabled for the primary proxy.	PLAIN	SSL
providerUrl[.primary]	The primary LDAP/Active Directory server queried by Connector. The .primary part of the property is optional.		ldap://<IPaddress or host name>:3268
providerUrl.secondary	The secondary LDAP/Active Directory server queried by Connector.		ldap://<IP address or host name>:3268
publicKeyFile	The location of the public key used to encrypt headers. Do not change this setting unless explicitlyinstructed to do so by a support engineer.		<relative path from location of agent.properties file>
read.timeout.downstream	Number of milliseconds before downstream read time-out.	0	<number>
read.timeout.upstream	Number of milliseconds before upstream read time-out.	0	<number>
secondaryProxy	The secondary Web Scanning Services proxy included in your provisioning email.		<IP address or host name>
secondaryProxyPort	The secondary Web Scanning Services proxy port included in your provisioning email.		<port>
secondaryProxyType	Sets whether SSL tunneling is enabled for the secondary proxy.	PLAIN	SSL
securityAuthentication[.primary]	LDAP security strength. The .primary part of the property is optional.	none	simplestrong
securityAuthentication.secondary	LDAP security strength.	none	simplestrong
securityCredentials[.primary]	The password for the primary account Connector uses when authenticating with an LDAP/Active Directory server. The .primary part of the property is optional.		<password>
securityCredentials.secondary	The password for the secondary account Connector uses when authenticating with an LDAP/Active Directory server.		<password>

Setting	Description	Default	Alternate
securityPrincipal[.primary]	The primary user name Connector uses to identify itself to an LDAP/Active Directory server. The .primary part of the property is optional.		cc=<user name>, cn=users, dc=<company>,dc=com
securityPrincipal.secondary	The secondary user name Connector uses to identify itself to an LDAP/Active Directory server.		cc=<user name>, cn=users, dc=<company>,dc=com
server.name	Plugable Authentication Module (PAM) server		
skip.wmp.authentication	Skip NTLM authentication for Windows Media Player.	FALSE	TRUE
sslTunnelTimeout	The number of milliseconds for which Connector should keep SSL tunnel requests open.		<number>
system.telemetry	Include the OS name and version headers in the XSD when upload.stas is TRUE.		os.name, os.version
tertiaryProxy	The tertiary Web Scanning Services proxy included in your provisioning email.		<IP address or host name>
tertiaryProxyPort	The tertiary Web Scanning Services proxy port included in your provisioning email.		<port>
tertiaryProxyType	Sets whether SSL tunneling is enabled for the tertiary proxy.	PLAIN	SSL
upload.stats	Whether to send statistics to the Web Scanning Services.	TRUE	FALSE
upstream.connect.timeout	Number of milliseconds before upstream connection time-out.	0	<number>
useBasic	Whether or not to use basic authentication.	FALSE	TRUE
useHttp	Tells Connector whether or not to run in workgroup mode. It enables Connector to act as a simple Web proxy server, listening to all user web requests. If set to true, useIcap must be set to false.	FALSE	TRUE
useIcap	Whether or not to listen for Web requests using ICAP. Used with ISA Server and ICAP compatible gateways. If set to true, useHttp must be set to false.	FALSE	TRUE
useISA2000	Specifies if ISA 2000 Server is in use.	FALSE	TRUE

Setting	Description	Default	Alternate
useISA2004	Specifies if ISA Server 2004/2006 is in use.	FALSE	TRUE
useLdap	Whether or not Connector should use LDAP to query Active Directory for the groups of which the user is a member.	FALSE	TRUE
UseLdapResourceManager	The LDAP Resource Manager, handles failovers from the primary LDAP server to the secondary LDAP server. You must not modify this value unless instructed to do so by customer support.	TRUE	FALSE
useNtlm	Enables Connector to collect users' internal IP addresses and user names using the NTLM authentication protocol. In most cases this authentication is transparent to the user.	FALSE	TRUE
user.agent.skip.authentication	Enable user agent string matching.	FALSE	TRUE
user.agent.skip.authentication.regexp	When user.agent.skip.authentication is TRUE, skip authentication for user agent strings matching a regular expression, for example (Chrome | Safari 1\\.\\d). Note, if this is left blank when user.agent.skip.authentication is TRUE authentication will be effectively switched off for all sites.		<regular expression>

APPENDIX B

Proxy Auto-Config Files

Revised: July 15, 2010

Overview

Proxy Auto-Configuration (PAC) is a method used by Web browsers to select a proxy for a given URL. The method for choosing a proxy is written as a JavaScript function contained in a PAC file. This file can be hosted locally or on a network. Browsers can be configured to use the file either manually or, in Microsoft Windows environments, automatically using Group Policy Objects. This appendix explains the basics of using PAC files.

How PAC Files Work

A PAC file is referenced each time a new URL is loaded. The host, for example cnn.com, the URL, for example cnn.com/images/logo.jpg, and other information such as the local machine IP address can be evaluated and rules based on this information used to determine whether to send the traffic via a proxy or direct to the Internet.

The following example compares the URL requested by the user, with the URL ipcheckit.com/data/. If the URLs match, the PAC file will instruct the browser to send the request direct to the Internet. This can be used if you need to exception a section of a Web site from going via the Web Scanning Services; if the user had requested only ipcheckit.com, this rule would not apply:

```
if (shExpMatch(url,"ipcheckit.com/data/*"))
return "DIRECT";
```

In the next example the local IP address of the machine making a Web request is evaluated. If the IP address falls within the IP address range 10.10.1.* then the PAC file will send the request to proxy182.scansafe.net. If this proxy is unavailable it will then failover to proxy137.scansafe.net. This can be used if you have different office locations using different IP address ranges with a Web Scanning Services proxy or Connector specific to each location:

```
if (isInNet(myIpAddress(), “10.10.1.0”, “255.255.255.0”))
return “PROXY proxy182.scansafe.net:8080; PROXY proxy137.scansafe.net:8080”;
```

Although a PAC file can have any name, normally it should be called proxy.pac.

PAC File Deployment

There are three ways to deploy a PAC file:

- Local PAC: in some cases it may be appropriate to host the file on the local machine, this can be useful if the machine is likely to leave the network and doesn't have Anywhere+ installed. Rules can be specified in the PAC file to allow direct Internet access when off-network.
- Share PAC: the file can be hosted on a Windows share, assuming that the share is accessible to the machine and that the correct permissions have been applied. If the location of the PAC file is password protected then this is likely to prevent the browser from downloading the file.
- Hosted PAC: hosting the file on a Web server is the most popular and widely supported method. The only requirement is that the file be served by the Web server with a specific MIME type (application/x-ns-proxy-autoconfig).

Basic PAC File Examples

Direct all traffic through the first proxy. If it is unreachable, use the second proxy. If both are unavailable go direct:

```
function FindProxyForURL(url, host) {
   return "PROXY proxy1.my.com:8080; PROXY
   proxy2.my.com:8080; DIRECT"; }
```

Direct HTTP traffic as in the first example, but send all HTTPS traffic direct:

```
function FindProxyForURL(url, host) {
   if (url.substring(0,6)=="https:") return
   "DIRECT"; else return "PROXY
   proxy1.my.com:8080; PROXY
   proxy2.my.com:8080; DIRECT"; }
```

Direct all traffic as in the first example, but send traffic for a given domain direct:

```
function FindProxyForURL(url, host) {
   if (host=="my.com") return “DIRECT”; else
   return “PROXY proxy1.my.com:8080; PROXY
   proxy2.my.com:8080; DIRECT”; }
```

If the client computer is on the specified internal network, go through the proxy. Otherwise go direct:

```
function FindProxyForURL(url, host) {
   if (isInNet(myIPaddress(), "192.168.1.0",
   "255.255.255.0")) return “PROXY
   proxy1.my.com:8080; PROXY
   proxy2.my.com:8080; DIRECT”; else return
   "DIRECT"; }
```

Example PAC File

```
function FindProxyForURL(url, host) {

// Web sites you wish to go to direct and not through the Web Scanning Services. This
list would include internally hosted Web sites, intranets, and so on

if (shExpMatch(url,"*.somecompany.co.uk*”) ||
   shExpMatch(url,"*.example.com*") ||
   shExpMatch(url,"*.anotherexample.com*"))
{ return “DIRECT”; }

// Internal IP address ranges that you need to be able to go to directly

else if(isInNet(host, "xxx.xxx.xxx.xxx",
   "255.255.0.0") ||
isInNet(host, "xxx.xxx.xxx.xxx",
   "255.255.0.0") ||
isInNet (host, "xxx.xxx.xxx.xxx",
   "255.255.0.0"))
{ return “DIRECT”; }

// Send all other HTTP HTTPS and FTP traffic to Web Services

else { return
“PROXY proxy.example1.com:8080”; } }
```

Manually Configure a Browser to Use a PAC File

With Firefox, in the Tools menu click Options. Click the Network tab then click Settings. Click Automatic Proxy Configuration URL. Enter the URL of the PAC file in the box then click OK to save the settings.

With Internet Explorer, in the Tools menu click Internet Options. Click the Connections tab then click LAN settings. Select “Use automatic configuration script”. Enter the URL of the PAC file in the box then click OK to save the settings.

With Opera, in the Tools menu click Preferences. Click the Advanced tab then, in the left panel, click Network. Click Proxy Servers and select “use automatic proxy configuration”. Enter the URL of the PAC file in the box then click OK to save the settings.

With Safari for Windows, in the Edit menu click Preferences. Click the Advanced tab then click Change settings. Click LAN settings. Select “Use automatic configuration script”. Enter the URL of the PAC file in the box then click OK to save the settings.

Windows Network Share Hosted PAC Files

It is possible to host a PAC file on a Windows network share by using a VBScript to copy it to the local machine. This can be integrated with Windows logon scripting.

Step 1 Set a share directory on a file server that everyone has access to.

Step 2 Create the proxy.pac file in the shared directory.

Step 3 Create a script.vbs file to copy the proxy.pac file from the network share to the local machine, for example:

```
Const OverwriteExisting = True
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objName= CreateObject("wscript.network") objFSO.CopyFile
"\\server_name\share_name\proxy.pac", "C:\proxy.pac",
OverwriteExisting
```

Note Logon scripts run with the same permissions as the logged-on user, and may not have write permission for the root of C:\. Ensure the VBScript copies the PAC file to a location where the user has write permission. However, the PAC file should be write-protected to prevent users changing it.

Step 4 Open the **Active Directory Users and Computers** control panel.

Step 5 View the properties of the OU or Domain for which you want to apply the Group Policy.

Step 6 Edit the **Group Policy**.

Step 7 In the User Configuration area, expand Windows Settings and click **Scripts (Logon/Logoff)**.

Step 8 Add a **Logon Script**.

Step 9 Browse to find the script.vbs file you created earlier, then click **OK**.

Table B-1 Local PAC URL Syntax

Browser	Windows XP	Windows 7 / Vista	MacOS X	GNU/Linux
Internet Explorer	file://c:\data\proxy.pac	file://c:\data\proxy.pac		
Firefox	file:///c:/data/proxy.pac	file:///c:/data/proxy.pac	file://localhost/data/proxy.pac	file:////data/proxy.pac
Safari	Uses Internet Explorer settings	Uses Internet Explorer settings	file://localhost/data/proxy.pac	
Opera	c:\data\proxy.pac	c:\data\proxy.pac	file://localhost/data/proxy.pac	file:////data/proxy.pac

Table B-2 Share PAC URL Syntax

Browser	Windows XP	Windows 7 / Vista	MacOS X	GNU/Linux
Internet Explorer	file://\\10.10.1.2\data\proxy.pac	file://\\10.10.1.2\data\proxy.pac		
Firefox	file:///\\10.10.1.2\data\proxy.pac	file://///10.10.1.2/data/proxy.pac	file://localhost/Volumes/data/proxy.pac	file:///mnt/server/data/proxy.pac
Safari	Uses Internet Explorer settings	Uses Internet Explorer settings	file://localhost/Volumes/data/proxy.pac	
Opera	\\10.10.1.2\data\proxy.pac	\\10.10.1.2\data\proxy.pac	file://localhost/Volumes/data/proxy.pac	file:///mnt/server/data/proxy.pac

APPENDIX C

Web Proxy Auto Discovery Protocol

Revised: July 15, 2010

Overview

The Web Proxy Auto-Discovery (WPAD) protocol is a method used by Web browsers to locate a Proxy Auto-Config (PAC) file automatically. The protocol uses DHCP and DNS systems and requires minimal configuration of a user's browser; in most cases all that is required is to select a check box. WPAD is not an official Internet standard, but it is widely supported by modern Web browsers. See How PAC Files Work, page B-1.

How WPAD Works

WPAD can use DNS or DHCP to locate a PAC file. DHCP detection involves the URL being pushed to the end-user in the DHCP assignment, while DNS detection is based on an educated guess using known information about the DNS system.

A browser must be instructed to use WPAD, in most browsers this is as achieved by selecting a check box or button. The feature is most commonly known as 'Auto-Detect' and is usually labeled as such. A browser that supports both methods will check the DHCP assignment first, before attempting the DNS method.

The PAC file must have the file name wpad.dat for the DNS method to function.

When using both WPAD methods the file must be served by the web server with the MIME type 'application/x-ns-proxy-autoconfig'.

If the browser is unable to load a PAC file via the DHCP or DNS methods, it will allow direct Internet access.

WPAD using DHCP

A DHCP server must be configured to serve an additional setting in an IP address assignment; option 252. This option specifies the exact location of the PAC file. The file name does not need to follow any specific naming convention, however if WPAD DNS is to be used also, the file must have the file name wpad.dat.

A Web browser implementing this method sends the DHCP server a DHCPINFORM query, the DHCP server will return the expected IP settings along with the 252 option which defines the location of the PAC file. The browser will then download this PAC file from the URL provided.

WPAD using DNS

The DNS method differs in that it guesses the location of a PAC file. On Windows, this is based on the domain the machine is joined to, while on Linux and Mac OS X this is based on the Search Domain(s) configured in the network settings.

When attempting the WPAD DNS method, the browser will prefix the domain with wpad and attempt to download the file wpad.dat, for example wpad.domain.com/wpad.dat.

In the following example, a Windows machine is joined to the domain uk.scansafe.com, and a PAC file with the file name wpad.dat is hosted on wpad.scansafe.com:

1. After checking the network settings, the browser identifies the host machine as being part of the domain uk.scansafe.com.
2. The browser attempts to resolve wpad.scansafe.com and fails.
3. The browser attempts and succeeds in resolving wpad.scansafe.com.
4. The browser attempts to download the PAC file wpad.scansafe.com/wpad.dat.

Manual Browser Configuration for Windows Clients

You may need to restart your browser for changes to take effect.

- In Internet Explorer, select the Automatically detect settings check box in the Local Area Network (LAN) Settings dialog.
- In Firefox, click **Auto-detect proxy settings for this network** in the Connection Settings dialog.
- In Opera, open the Preferences dialog then click the Advanced tab. In the left menu click Network then click Proxy Servers. Select the **Use automatic proxy configuration** check box and enter the WPAD URL in the box. Ensure the other check boxes are cleared then click **OK**.
- Safari for Windows uses the Internet Explorer settings.

Deploying WPAD with Windows Server

Deploying WPAD on a Windows server enables you to centrally configure Internet Explorer users who are joined to a domain. It also makes it easy to configuring the browsers of users who are not members of a domain.

Before beginning the following should be installed and configured on Windows Server:

- Internet Information Services (IIS)
- DHCP Server
- DNS Server
- Active Directory

Active Directory is not a functional requirement of WPAD, but is recommended in order to simplify deployment.

Currently only Internet Explorer offers complete support for the DHCP method, therefore the DNS method is essential for support with alternate browsers.

You should test your PAC file before renaming it wpad.dat and uploading it to the Web site that will serve the file.

Configure Internet Information Services

Some browsers cannot read a PAC file served with an incorrect MIME type so you should configure IIS to use 'application/x-ns-proxy-autoconfig' for the '.dat' extension. When you have made the change, restart IIS .

When the entry for WPAD is created and activated, all users of the relevant DHCP scope will receive the wpad.dat location, ready to be used by a user's browser.

Create an Option 252 Entry in DHCP

To automatically configure proxy settings:

Step 1 Open the DHCP control panel.

Step 2 In the console tree, right-click **DHCP server**, click **Set Predefined Options**, then click **Add**.

Step 3 In the **Name** box enter WPAD.

Step 4 In the **Data type** box enter `String`.

Step 5 Clear the **Array** check box.

Step 6 In the **Code** box enter `252`.

Step 7 In the **Description box** enter http://<url>:<port>/wpad.dat, then click **OK**.

To confirm Option 252 is selected, right-click **Server Options** then click **Configure Options**.

Enable Option 252 for a DHCP Scope

To configure Option 252 for a DCHP scope:

Step 1 Open the DHCP control panel.

Step 2 Right-click **Scope Options**, click **Configure Options**, then click **Advanced**.

Step 3 In Vendor Class, click **Standard Options**.

Step 4 In **Available Options**, click **252 Proxy Autodiscovery**, then click **OK**.

Active Directory and Group Policy Objects

One of the benefits of WPAD is that it greatly reduces the amount of work it takes to configure a browser for use with a PAC file/proxy.

Using Active Directory and Group Policy Objects (GPO) you can configure Internet Explorer settings automatically. A third-party tool called FirefoxADM is available for Firefox which allows configuration via GPO.

APPENDIX D

Installing Linux

Revised: July 15, 2010

Overview

This appendix provides a step-by-step guide to performing a graphical installation of either Red Hat Enterprise or CentOS Linux version 5 on an x86 or x86-64 server in a suitable configuration for running Connector.

This appendix assumes you have no previous Linux experience, but are familiar with basic computing terminology and systems administration.

Before beginning installation, please ensure your server is capable of running the Linux operating system. See Linux System Requirements, page 3-1.

The screen shots in this appendix have Red Hat Enterprise Linux branding, but the installation steps are identical for CentOS Linux unless specifically stated otherwise.

Obtaining Linux Installation Media

Connector is not supported on any other distributions of Linux or Unix, or any custom configuration beyond the instructions in this appendix.

Red Hat Enterprise Linux 5

Red Hat Enterprise Linux 5 is a commercial distribution which can be purchased and downloaded from the Red Hat website. The advantage of using Red Hat Enterprise Linux is that vendor support is available to assist with installation and configuration issues. It is also certified for use on certain vendors' hardware.

For further information on Red Hat Enterprise Linux 5, go to http://www.redhat.com/.

CentOS Linux 5

CentOS Linux 5 is a freely-available operating system which aims to be 100 percent binary compatible with Red Hat Enterprise Linux. Within the scope of this appendix, Red Hat Enterprise Linux and Cent OS Linux are functionally identical.

To create CentOS Linux installation CD media, download the appropriate ISO image for your type of server and write it to CD.

- For x86 servers, download from http://mirror.centos.org/centos/5/isos/i386/.
- For x86-64 servers, download from http://mirror.centos.org/centos/5/isos/x86_64/.

Select the geographically closest mirror server to ensure a fast download. Cisco recommends that you download outside business hours.

When you have chosen a mirror server, download the appropriate ISO image and save it to your computer.

- For x86 servers, download CentOS-5.2-i386-bin-1of6.iso (624 MB).
- For x86-64 servers, download CentOS-5.2-x86_64-bin-1of6.iso (622 MB)

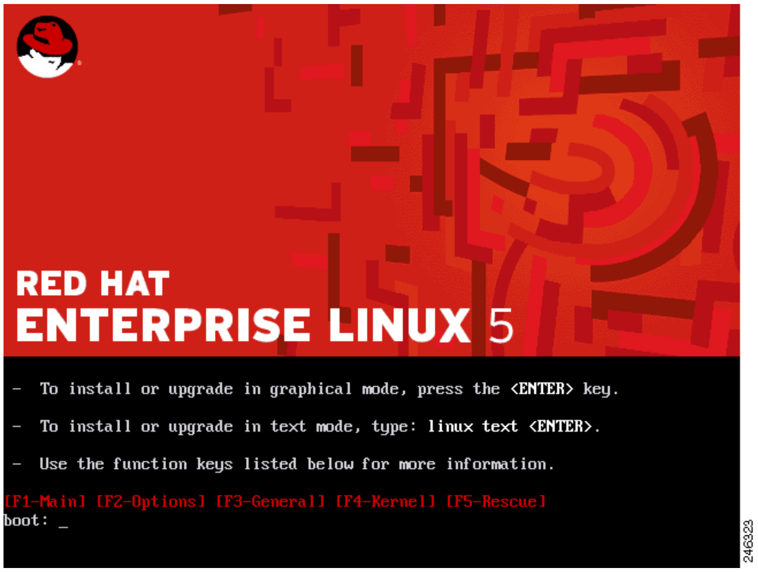
Note There are seven installation ISO images available for download, but you require installation ISO 1 only as you will perform a secure minimal installation of Linux.

When you have downloaded the ISO files, use CD-writing software to convert the ISO image into a physical CD. Please refer to you CD-writing software vendor documentation for specific instructions.

Installing Linux

To install Linux:

Step 1 Insert the first installation CD and reboot the system. After a short delay, a screen containing the boot: prompt should appear.

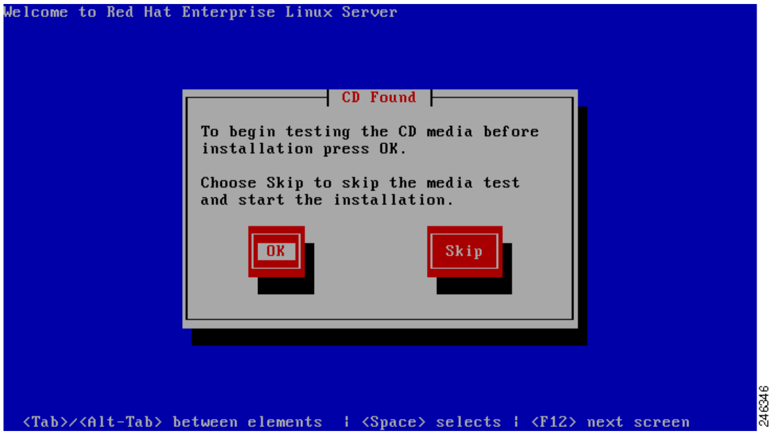


```
- To install or upgrade in graphical mode, press the <ENTER> key.

- To install or upgrade in text mode, type: linux text <ENTER>.

- Use the function keys listed below for more information.

[F1-Main] [F2-Options] [F3-General] [F4-Kernel] [F5-Rescue]
boot: _
```

Step 2 Press Enter to begin the graphical installation. Alternatively, wait 60 seconds for installation to begin automatically.

> **Note** You may need to change the system's BIOS settings to enable booting from the DVD/CD-ROM drive.

Step 3 When the DVD/CD-ROM drive is found and the driver loaded, you have the option to perform a media check on the DVD/CD.



```
Welcome to Red Hat Enterprise Linux Server

CD Found

To begin testing the CD media before
installation press OK.

Choose Skip to skip the media test
and start the installation.

OK        Skip

<Tab>/<Alt-Tab> between elements  | <Space> selects | <F12> next screen
```

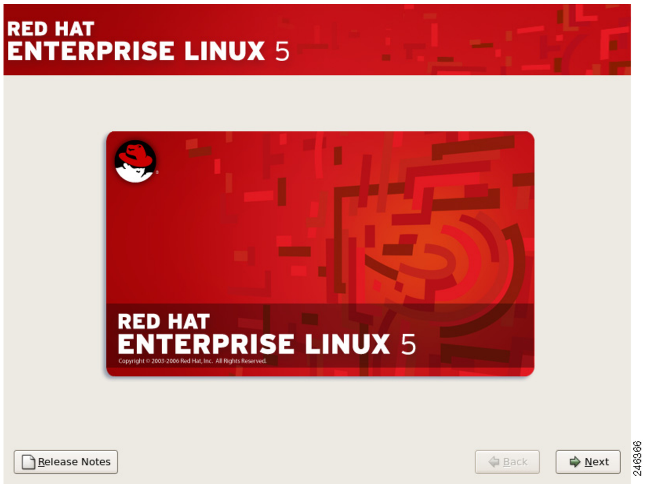
These checks ensure the server can read the installation packages from the CD media.

Press Tab to highlight **OK** and then press Enter to perform the test. When the check is completed, press Tab to highlight **Continue** and press Enter to continue.

Alternatively, press Tab to highlight **Skip** and press Enter to skip the check.

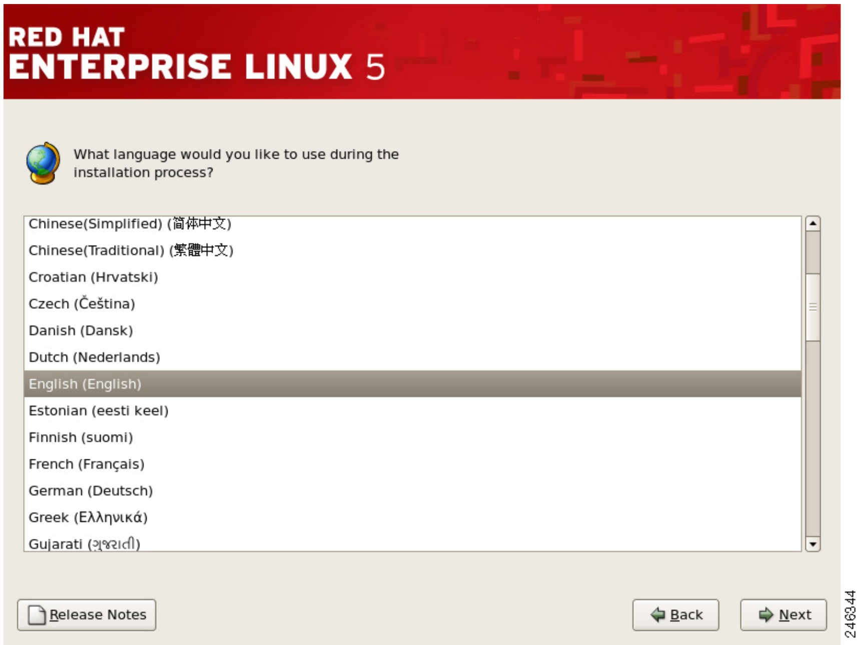
> **Note** This will take some time, and you may opt to skip over this step. However, if you later encounter problems with the installation program, you should reboot and perform the media check before calling for support.

Step 4 The welcome screen does not prompt you for any input.



Click **Next** to continue.

Step 5 The language you choose here will become the default language for the operating system once it is installed. Later on the installation program will try to guess the appropriate time zone based on your choice.



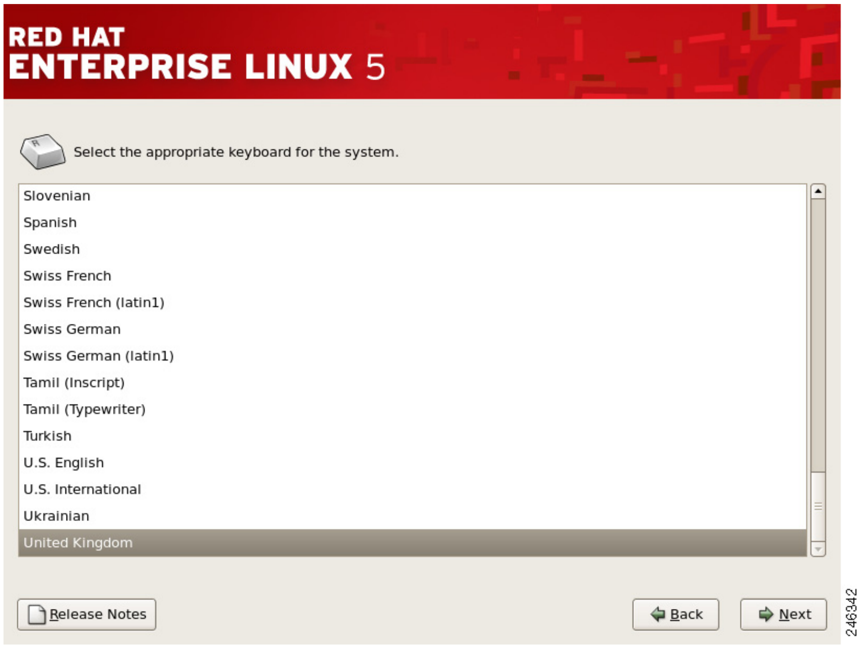
What language would you like to use during the installation process?

Chinese(Simplified) (简体中文)
Chinese(Traditional) (繁體中文)
Croatian (Hrvatski)
Czech (Čeština)
Danish (Dansk)
Dutch (Nederlands)
English (English)
Estonian (eesti keel)
Finnish (suomi)
French (Français)
German (Deutsch)
Greek (Ελληνικά)
Gujarati (ગુજરાતી)

Choose a language to use for the installation.

When you have chosen the appropriate language, click **Next** to continue.

Step 6 Choose the correct keyboard layout to be used for the installation and as the system default, for example United Kingdom.



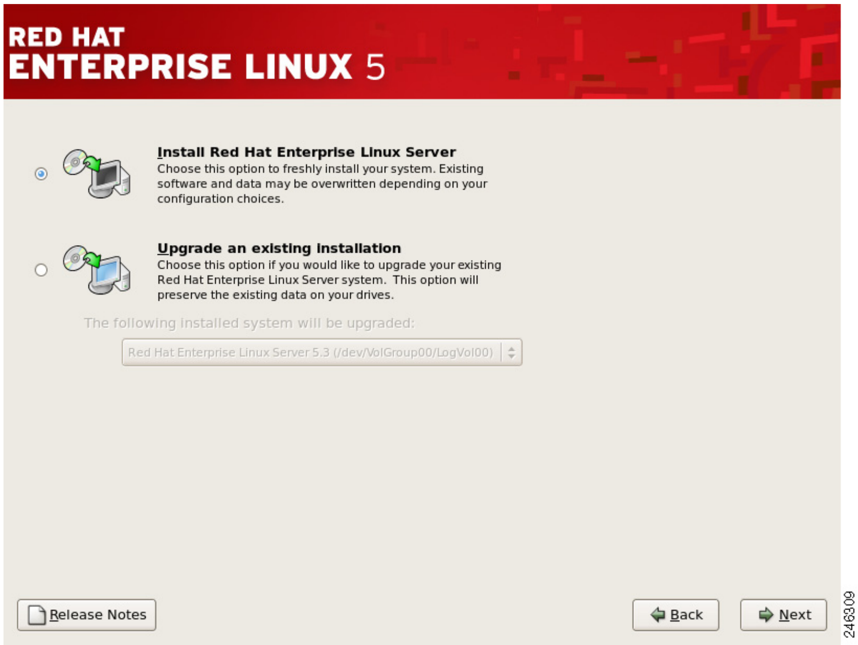
Select the appropriate keyboard for the system.

Slovenian
Spanish
Swedish
Swiss French
Swiss French (latin1)
Swiss German
Swiss German (latin1)
Tamil (Inscript)
Tamil (Typewriter)
Turkish
U.S. English
U.S. International
Ukrainian
United Kingdom

When you have made your choice, click **Next**.

If you are installing Red Hat Enterprise Linux you will be prompted to enter an Installation Number. Enter your 16 digit number in the **Installation Number** box then click **OK**.

Step 7 If there is an existing installation on the system you will be prompted to choose between a fresh install or upgrading the existing installation.



RED HAT ENTERPRISE LINUX 5

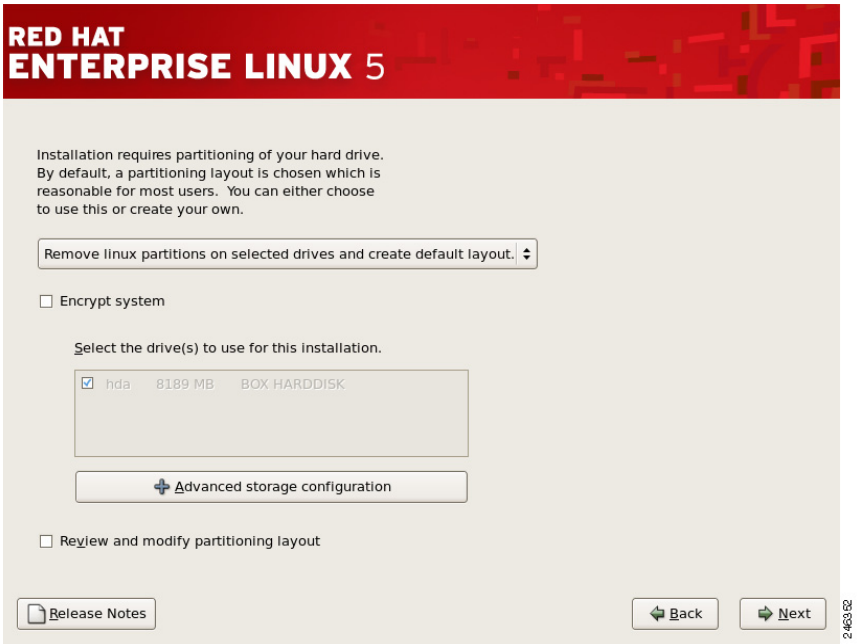
● **Install Red Hat Enterprise Linux Server**
Choose this option to freshly install your system. Existing software and data may be overwritten depending on your configuration choices.

○ **Upgrade an existing installation**
Choose this option if you would like to upgrade your existing Red Hat Enterprise Linux Server system. This option will preserve the existing data on your drives.

The following installed system will be upgraded:
Red Hat Enterprise Linux Server 5.3 (/dev/VolGroup00/LogVol00)

Click **Install** (RedHat or CentOS) then click **Next** to overwrite the previous installation.

Step 8 Partitioning enables you to divide your hard disk into isolated sections, where each section behaves as if it were a separate hard disk.



RED HAT ENTERPRISE LINUX 5

Installation requires partitioning of your hard drive. By default, a partitioning layout is chosen which is reasonable for most users. You can either choose to use this or create your own.

Remove linux partitions on selected drives and create default layout.

□ Encrypt system

Select the drive(s) to use for this installation.

☑ hda 8189 MB BOX HARDDISK

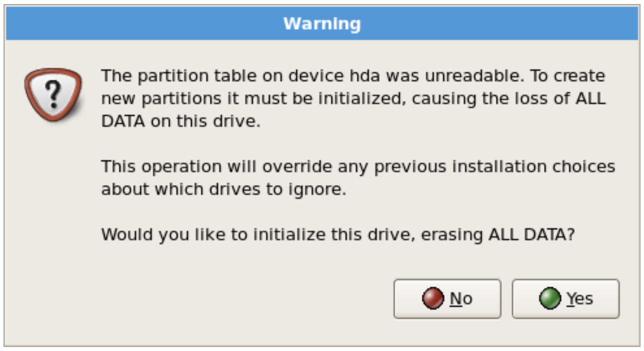
□ Review and modify partitioning layout

In the list, click **Remove all partitions on selected drives and create default layout**.

Step 9 Clear the **Review and modify partitioning layout** check box and then click **Next**.

> **Note** If you are familiar with Linux, you may wish to create a custom disk partitioning layout. However, this is outside the scope of this document and recommends you use the default layout. The Connector software will be installed into the/opt partition.

If there is no data on the hard disk, or the installation program cannot read the existing data, you will see the following warning:



Warning

The partition table on device hda was unreadable. To create new partitions it must be initialized, causing the loss of ALL DATA on this drive.

This operation will override any previous installation choices about which drives to ignore.

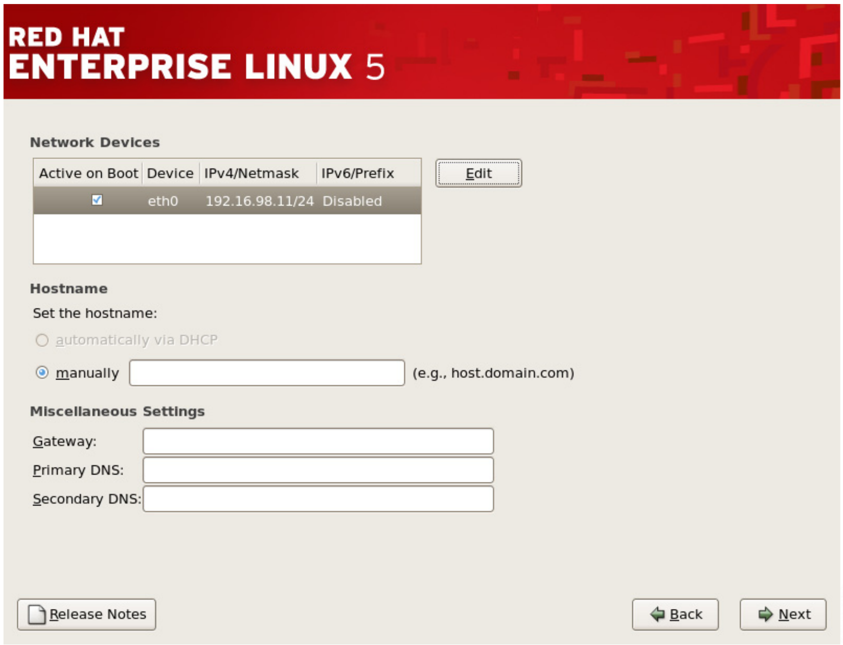
Would you like to initialize this drive, erasing ALL DATA?

246365

Click **Yes** to continue.

> **Caution** All data on the chosen hard disk(s) will be removed by the installation program. You must backup any data that you have on your systems before proceeding with the installation.

Step 10 The installation program automatically detects any network devices you have and displays them in the Network Devices list.



Network Devices

Active on Boot	Device	IPv4/Netmask	IPv6/Prefix
☑	eth0	192.16.98.11/24	Disabled

Hostname

Set the hostname:

○ automatically via DHCP

● manually (e.g., host.domain.com)

Miscellaneous Settings

Gateway:

Primary DNS:

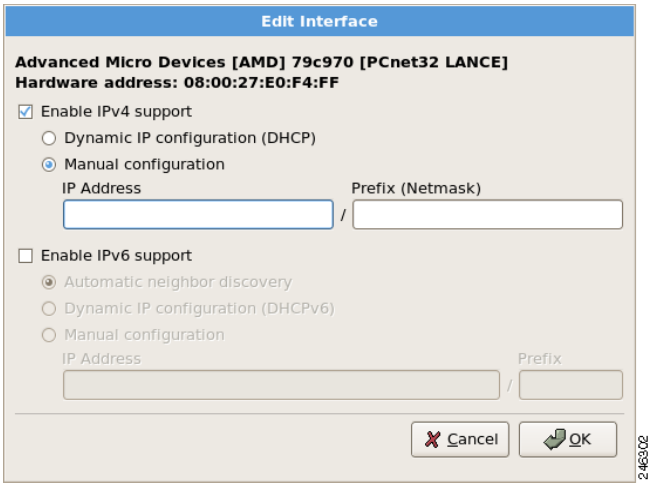
Secondary DNS:

246347

Select your primary network device, and click **Edit**.

To configure the network:

a. Ensure the **Enable IPv4 support** check box is selected.



Edit Interface

Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
Hardware address: 08:00:27:E0:F4:FF

☑ Enable IPv4 support
○ Dynamic IP configuration (DHCP)
● Manual configuration
IP Address / Prefix (Netmask)

☐ Enable IPv6 support
● Automatic neighbor discovery
○ Dynamic IP configuration (DHCPv6)
○ Manual configuration
IP Address / Prefix

b. Click **Manual Configuration**.

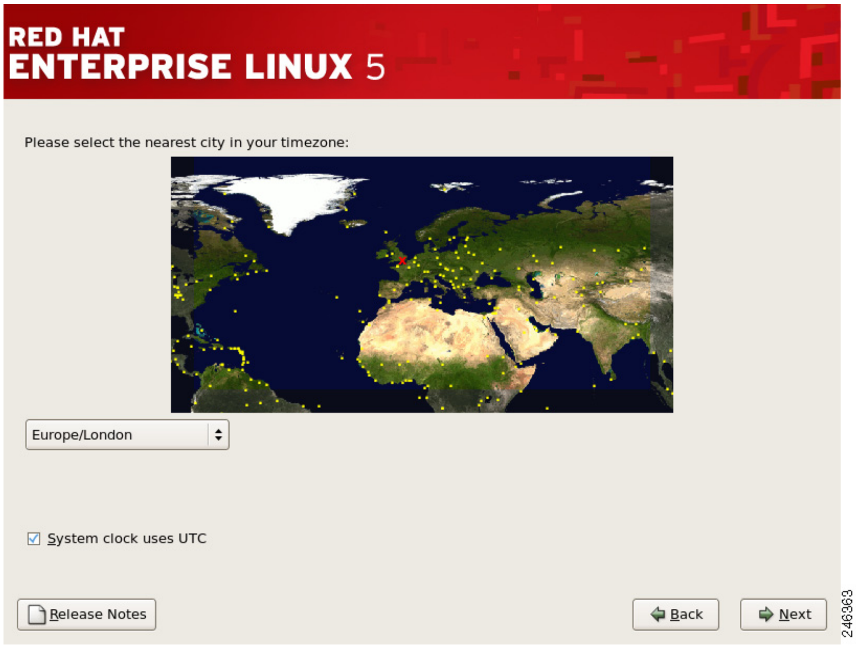
c. Enter the IP Address and Prefix (Netmask) provided by your network administrator.

d. Clear the **Enable IPv6 support** check box.

e. Click **OK** to return to the previous dialog.

In the Miscellaneous Settings section, enter your system's Gateway, Primary DNS and Secondary DNS then click **Next** to continue.

Step 11 Set your time zone by choosing the city closest to your system's physical location. The installation program will try and guess the correct location for you based on your earlier choice of language.



Please select the nearest city in your timezone:

Europe/London

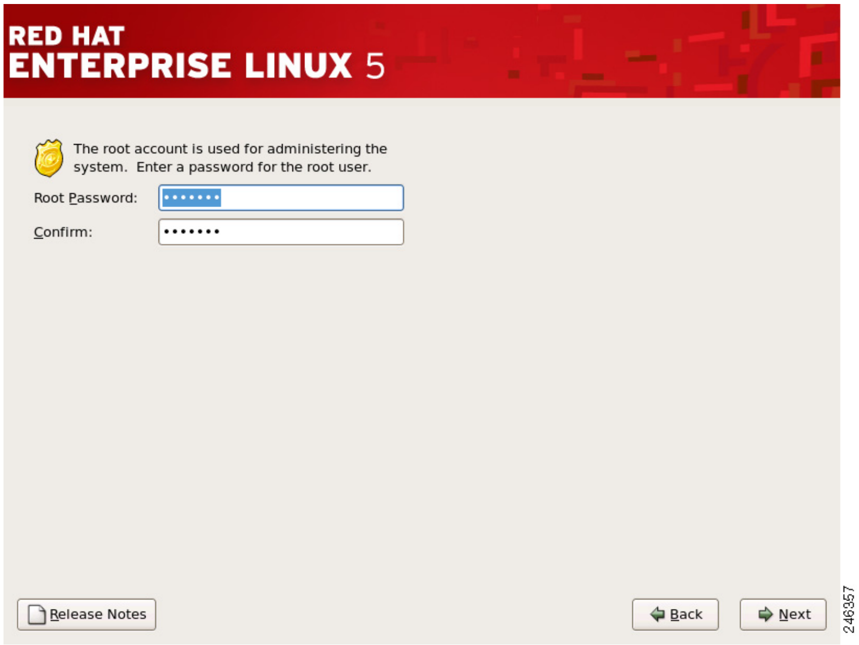
☑ System clock uses UTC

Click the interactive map to zoom in to a particular geographical region of the world.

Click a specific city (represented by a yellow dot). A red **X** indicates your choice. Alternatively, in the country list click a city.

When you have chosen your time zone, click **Next** to continue.

Step 12 Setting up a root account and password is one of the most important steps during your installation. Your root account is similar to the administrator account used on computers running Microsoft Windows operating systems. The root account is used to install packages, upgrade packages, and perform most system maintenance. Logging in as root gives you complete control over the system.



The root account is used for administering the system. Enter a password for the root user.

Root Password: •••••••

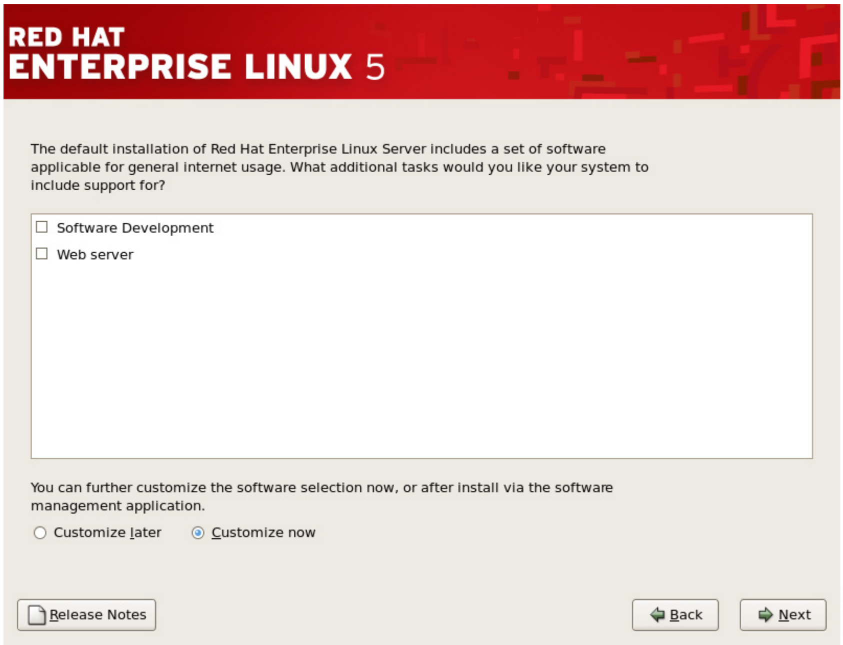
Confirm: •••••••

The root password must be at least six characters long. The password is not displayed so you must enter it twice to ensure you have entered it correctly. You cannot proceed unless the **Root Password** and **Confirm** fields match.

Caution The root user (also known as the superuser) has complete access to the entire system; for this reason it is essential that you keep the password secret.

When you have entered a suitable password, click **Next** to continue.

Step 13 You are prompted to choose the tasks you would like the system to include support for. This dialog varies slightly depending on the version of Red Hat Enterprise or CentOS Linux you are installing.



The default installation of Red Hat Enterprise Linux Server includes a set of software applicable for general internet usage. What additional tasks would you like your system to include support for?

□ Software Development
□ Web server

You can further customize the software selection now, or after install via the software management application.

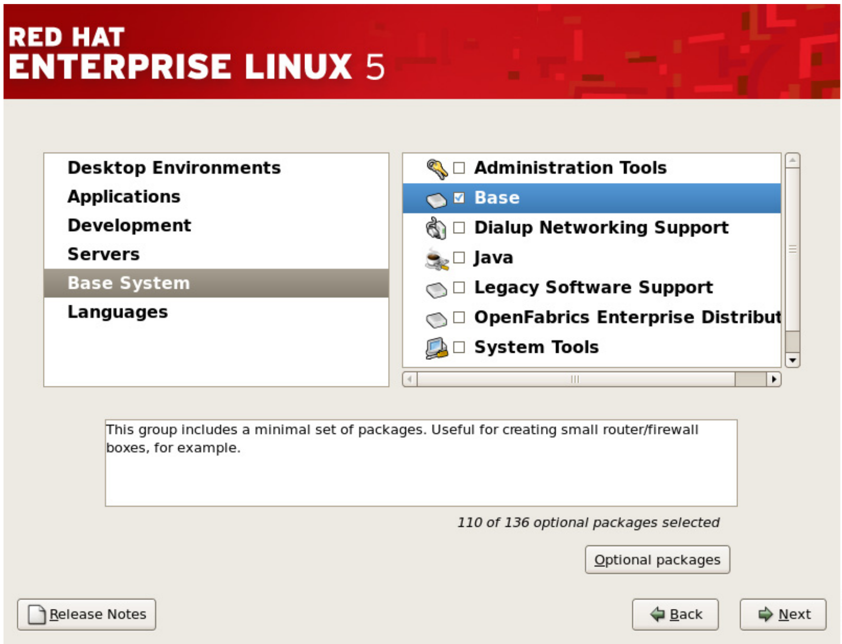
○ Customize later ● Customize now

246362

Because Connector requires a minimal installation of Linux, clear all the check boxes.

Click **Customize now**, then click **Next** to continue.

Step 14 Because Connector requires a minimal installation of Linux, clear every installation option except the **Base System:Base** package.



□ Administration Tools
☑ Base
□ Dialup Networking Support
□ Java
□ Legacy Software Support
□ OpenFabrics Enterprise Distribut
□ System Tools

This group includes a minimal set of packages. Useful for creating small router/firewall boxes, for example.

110 of 136 optional packages selected

246351

For each package group in the left column:

a. Click the package group.

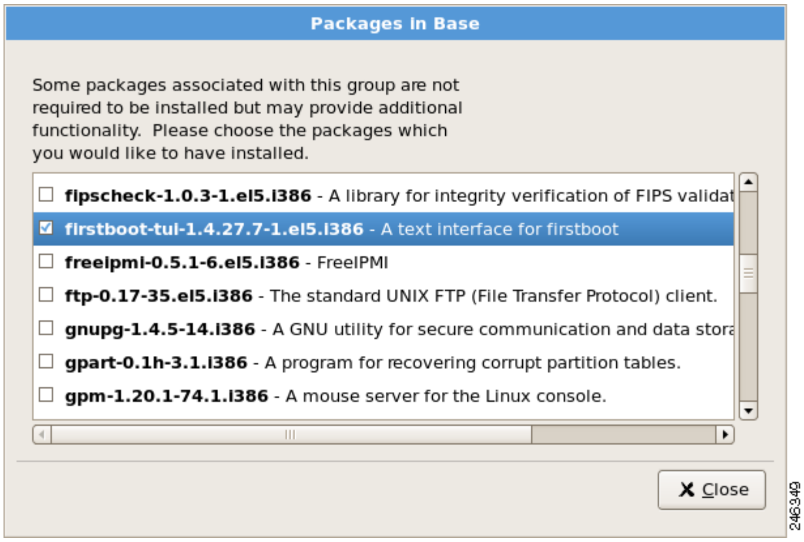
b. Clear every package in the right column.

When this is done, click the **Base System package** group in the left column. Click the **Base** package in the right column.

⚠
Caution Take care not to clear the **Base System:Base** package, or your Linux installation will be missing essential system administration commands and you will not be able to install Connector.

Only one of the optional base packages is required. To remove the others:

a. Click **Optional packages**.



Packages in Base

Some packages associated with this group are not required to be installed but may provide additional functionality. Please choose the packages which you would like to have installed.

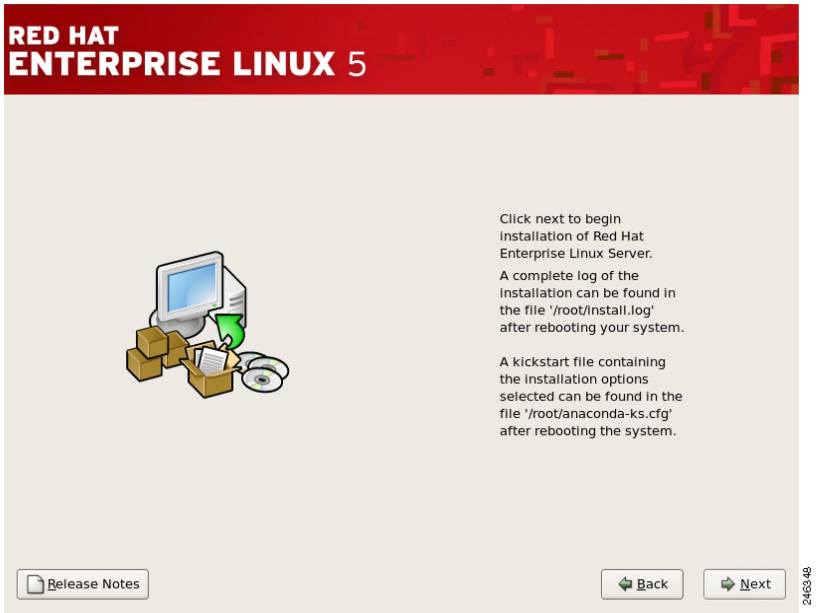
- □ **fipscheck-1.0.3-1.el5.i386** - A library for integrity verification of FIPS validat
- ☑ **firstboot-tui-1.4.27.7-1.el5.i386** - A text interface for firstboot
- □ **freeipmi-0.5.1-6.el5.i386** - FreeIPMI
- □ **ftp-0.17-35.el5.i386** - The standard UNIX FTP (File Transfer Protocol) client.
- □ **gnupg-1.4.5-14.i386** - A GNU utility for secure communication and data stora
- □ **gpart-0.1h-3.1.i386** - A program for recovering corrupt partition tables.
- □ **gpm-1.20.1-74.1.i386** - A mouse server for the Linux console.

b. Clear every check box except **firstboot**. This is required for post-installation configuration.

c. Click **Close**.

d. Click **Next** to continue.

Step 15 At the summary dialog, click **Next**.



Click next to begin installation of Red Hat Enterprise Linux Server.

A complete log of the installation can be found in the file '/root/install.log' after rebooting your system.

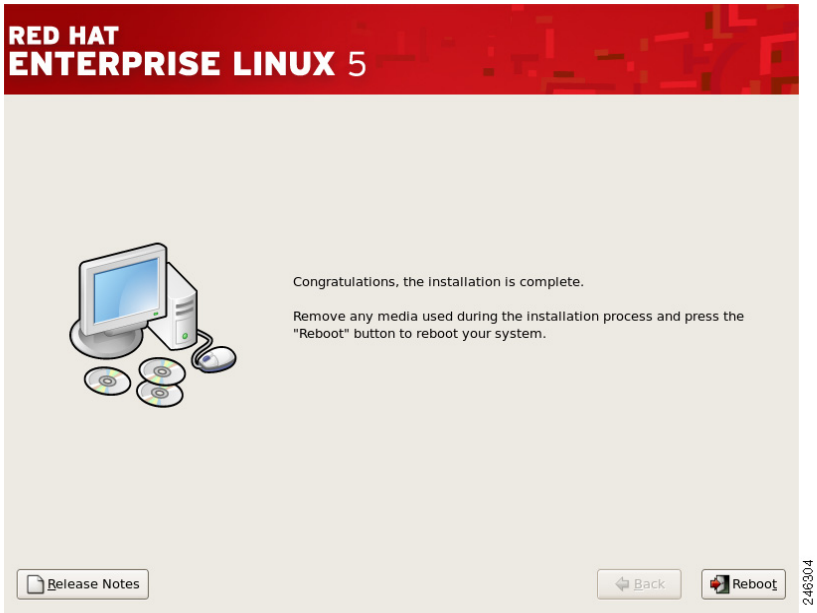
A kickstart file containing the installation options selected can be found in the file '/root/anaconda-ks.cfg' after rebooting the system.

Click **Next** to begin the installation.

Caution If, for some reason, you would rather not continue with the installation process, this is your last opportunity to safely cancel the process and reboot your machine. When you click **Next**, disk partitions are written and packages are installed. If you wish to abort the installation, you should reboot now before any existing information on any hard disk is overwritten.

At this point there is nothing left for you to do until all the packages have been installed. How quickly this happens depends on the number of packages you have selected and your computer's speed.

Step 16 When it has finished, the installation program prompts you to prepare your computer to reboot.

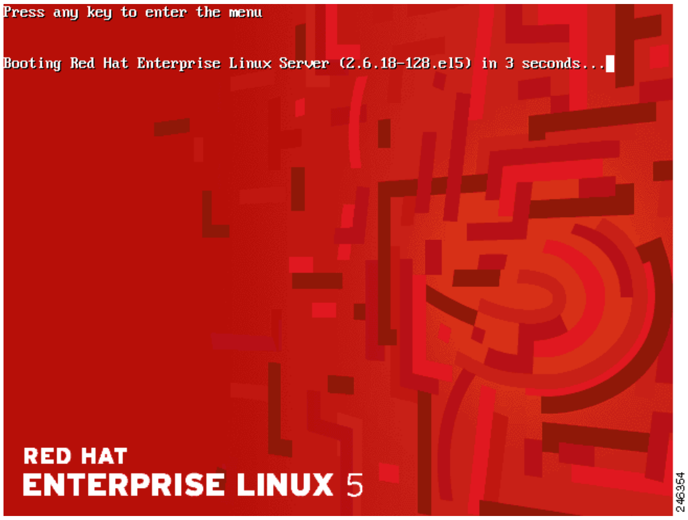


Congratulations, the installation is complete.

Remove any media used during the installation process and press the "Reboot" button to reboot your system.

Remove the CD if it is not ejected automatically, then click **Reboot** to continue.

After your system's normal power-up sequence has completed, the graphical boot loader prompt is displayed.



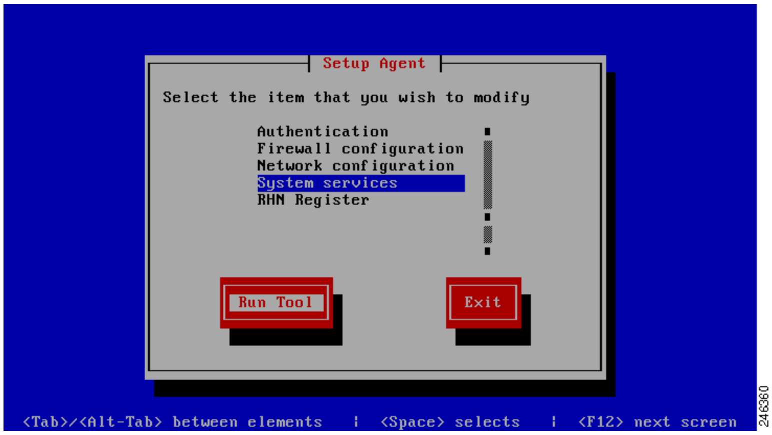
```
Press any key to enter the menu

Booting Red Hat Enterprise Linux Server (2.6.18-128.el5) in 3 seconds...
```

Press Enter to select the default boot entry. Alternatively, wait for the time-out period (normally five seconds), after which the default boot entry is loaded.

Post-Installation Configuration

The first time you boot after installing the operating system, the text mode Setup Agent is displayed. To configure your Linux installation:

Step 1 Use the arrow keys to highlight **System services**.

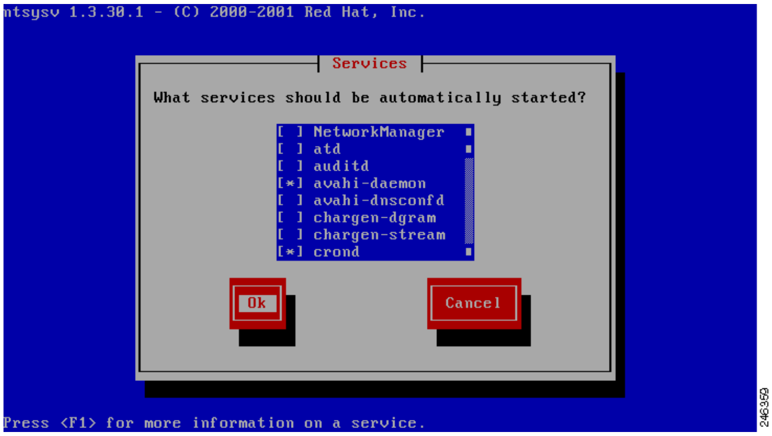


```
Setup Agent

Select the item that you wish to modify

          Authentication
          Firewall configuration
          Network configuration
          System services
          RHN Register

        Run Tool              Exit

<Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

Step 2 Press Tab to highlight **Run Tool** and then press Enter.

Note For security reasons, the Setup Agent will close after 30 seconds of inactivity and you will see the login prompt. To return to the Setup Agent, enter the root username and password you created earlier., then at the command prompt type `setup` and press Enter.

Step 3 Connector requires a minimal, secure installation of Linux therefore it is necessary to turn off all unnecessary system services.



```
ntsysv 1.3.30.1 - (C) 2000-2001 Red Hat, Inc.

                       Services

     What services should be automatically started?

                 [ ] NetworkManager
                 [ ] atd
                 [ ] auditd
                 [*] avahi-daemon
                 [ ] avahi-dnsconfd
                 [ ] chargen-dgram
                 [ ] chargen-stream
                 [*] crond

Press <F1> for more information on a service.
```

Linux automatically selects a default profile of system services, with some switched on and some switched off. Some of these enabled services (indicated with a * in the box) need to be switched off by removing the star.

Caution Do not modify the status of any service except for those listed below otherwise your system may not work correctly or may be secure.

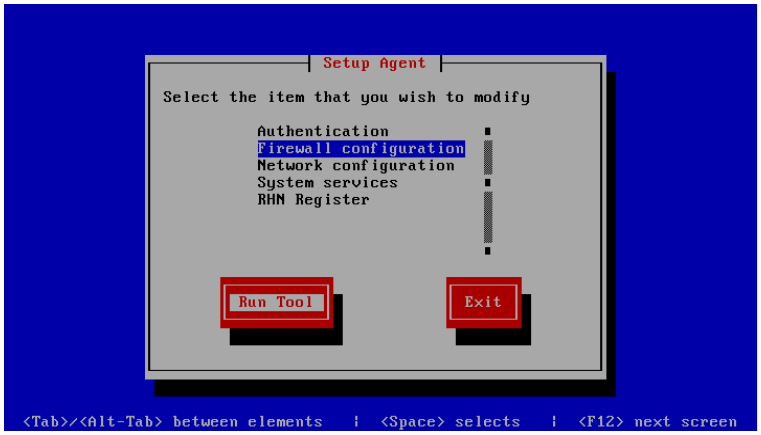
For each of the following services, use the arrow keys to highlight the service and press the space bar to switch it off:

- atd
- auditd
- cups
- firstboot
- haldaemon
- netfs
- pcscd
- portmap

When you are finished, press Tab to highlight **Ok**, then press Enter to return to the Setup Agent.

Step 4 By default the server firewall is enabled, but it is necessary to switch off a security feature called 'SELinux' before installing Connector. This will not reduce the security of the server or switch off the firewall.

Note Security-Enhanced Linux (SELinux) is a Linux feature that provides a variety of security policies, including U.S. Department of Defense style mandatory access controls, through the use of Linux Security Modules (LSM) in the Linux kernel.

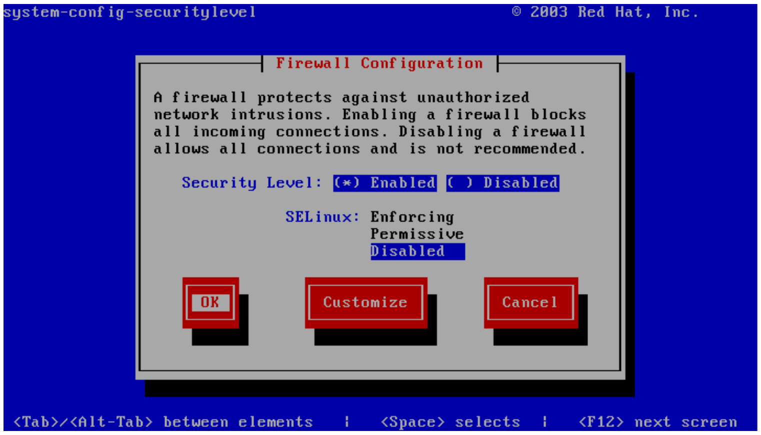


```
Setup Agent

Select the item that you wish to modify

Authentication
Firewall configuration
Network configuration
System services
RHN Register

Run Tool          Exit

<Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

246316

Use the arrow keys to highlight **Firewall configuration**.

Step 5 Use the Tab key to highlight **Run Tool** and press Enter.

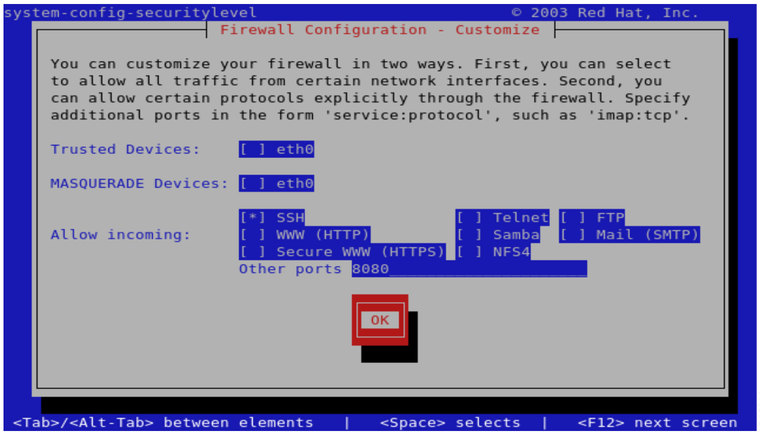


```
system-config-securitylevel                          © 2003 Red Hat, Inc.

Firewall Configuration

A firewall protects against unauthorized
network intrusions. Enabling a firewall blocks
all incoming connections. Disabling a firewall
allows all connections and is not recommended.

Security Level: (*) Enabled ( ) Disabled

SELinux: Enforcing
         Permissive
         Disabled

OK      Customize      Cancel

<Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

246358

Step 6 Ensure that Security Level has an asterisk (*) next to Enabled.

Step 7 Use the Tab key to move to highlight **Customize** and press Enter.



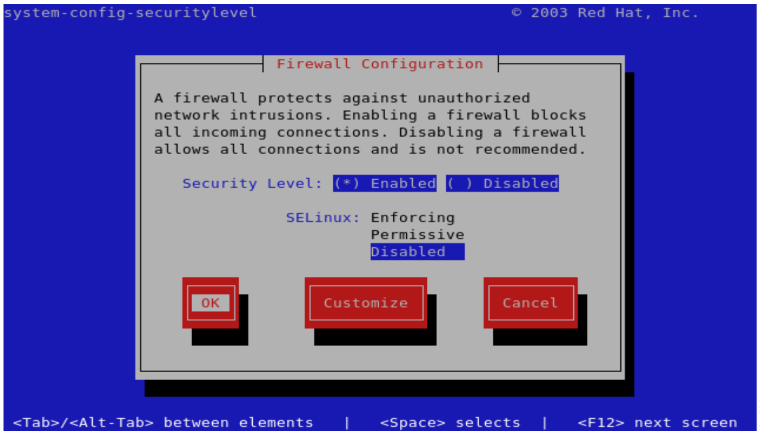
```
system-config-securitylevel                          © 2003 Red Hat, Inc.
                  ┤ Firewall Configuration - Customize ├

    You can customize your firewall in two ways. First, you can select
    to allow all traffic from certain network interfaces. Second, you
    can allow certain protocols explicitly through the firewall. Specify
    additional ports in the form 'service:protocol', such as 'imap:tcp'.

    Trusted Devices:      [ ] eth0

    MASQUERADE Devices:   [ ] eth0

                          [*] SSH                [ ] Telnet [ ] FTP
    Allow incoming:       [ ] WWW (HTTP)         [ ] Samba  [ ] Mail (SMTP)
                          [ ] Secure WWW (HTTPS) [ ] NFS4
                          Other ports 8080

                                      OK

 <Tab>/<Alt-Tab> between elements   |   <Space> selects   |   <F12> next screen
```

246313

Step 8 Use the Tab key to place the cursor in the Other Ports section. Type `8080` into the **Other ports** box.

Note If you are have modified the Connector configuration to listen on an alternative port, replace 8080 with the listening port you have chosen.

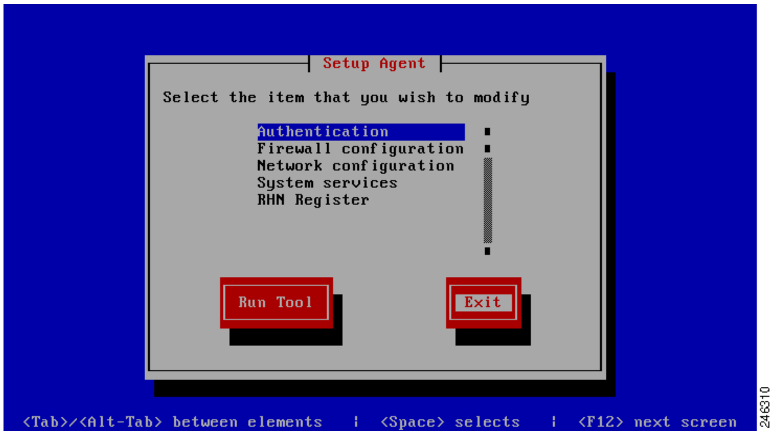
Step 9 Use the Tab key to move to highlight **OK** and press Enter.



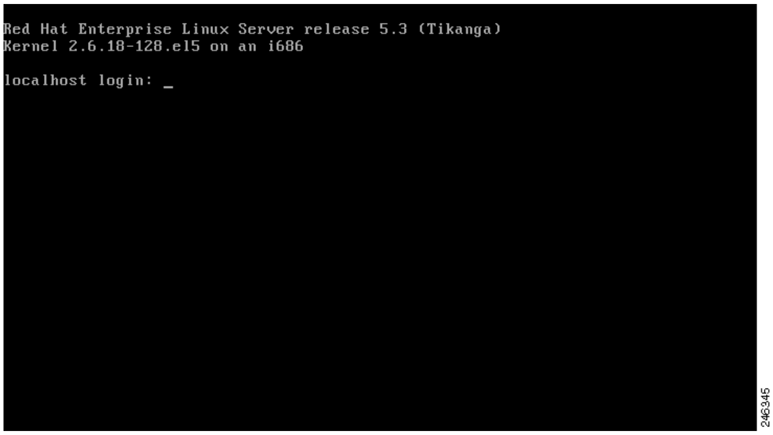
```
system-config-securitylevel                          © 2003 Red Hat, Inc.

                      ┤ Firewall Configuration ├

               A firewall protects against unauthorized
               network intrusions. Enabling a firewall blocks
               all incoming connections. Disabling a firewall
               allows all connections and is not recommended.

                  Security Level: (*) Enabled ( ) Disabled

                             SELinux: Enforcing
                                      Permissive
                                      Disabled

                    OK          Customize          Cancel

 <Tab>/<Alt-Tab> between elements   |   <Space> selects   |   <F12> next screen
```

246314

Step 10 Use the Tab key to move to highlight **OK** and press Enter.



Step 11 Use the Tab key to highlight **Exit** and then press Enter to leave the Setup Agent. You should now be presented with the server login screen:



```
Red Hat Enterprise Linux Server release 5.3 (Tikanga)
Kernel 2.6.18-128.el5 on an i686

localhost login: _
```

Step 12 Enter the username `root` and the password you chose earlier in the installation process to log in. At the command prompt type `reboot` and press Enter to perform a system restart. This will apply your configuration changes made in the setup agent and complete your post-install configuration.

Installation of Linux is now complete. Your system is now running a minimal installation of Linux, with the only externally accessible network port being SSH on TCP port 22 for remote administration.

Troubleshooting

You can ping the system's IP address from another computer on the same network to ensure that it has network connectivity.

If the system does not respond:

- Check your network settings.
- Check that the system's network card has a link light displayed.
- Ensure your firewalls are configured correctly.

GLOSSARY

Revised: July 15, 2010

A

Active Directory The directory service for Microsoft Windows network operating systems.

authentication key A key used to authenticate a computer, typically deployed group or company wide.

D

DHCP Abbreviation for *Dynamic Host Configuration Protocol*. A solution for dynamically assigning IP addresses.

DNS Abbreviation for *Domain Name System*.

domain name A human-readable name that is mapped to an IP address.

E

exception A site that is excluded from a policy.

F

firewall Personal firewalls limit the ports on which Internet traffic can travel.

G

GPO Abbreviation for *Group Policy Objects*. GPO enables Windows system administrators to push policy to users' computers.

I

ISA Server Generic name for products in the Microsoft *Internet Security and Acceleration Server* family.

J

JavaScript An implementation of the ECMAScript scripting language, common in Web browsers.

L

LDAP Acronym for *Lightweight Directory Access Protocol*. A standard for accessing information in a directory.

P

PAC file Acronym for *Proxy Auto-Config file*. A *JavaScript* file used by a browser to determine its proxy settings. Can be stored locally or remotely.

proxy A server that redirects network traffic.

S

Squid An open source proxy server and web cache daemon.

W

web scanning services Cisco's in-the-cloud security solution.

Windows service Software that runs as a background service with Microsoft Windows.

WPAD Acronym for *Web Proxy Auto-Discovery*.

INDEX

A

acceptable usage policy 4-4
Active Directory C-4
active directory 1-3
agent properties A-1
authentication key 4-9
- company 1-3
- group 1-3
- user 1-3, 1-4

authentication process 1-5

B

basic operations 1-1
browser configuration C-2
- PAC files B-3

C

CentOS D-1

D

deployment scenarios 1-3
DHCP C-1, C-3
DNS C-2
document conventions 1-v

E

enterprise mode 1-2
exceptions 4-3
- examples 4-3

F

firewall D-14

G

getting started 1-1
GPO C-4
groups 1-6, 4-9
- excluding 4-9
- nested 4-10

I

IIS C-3
installing
- on windows 2-1
- windows
  - enterprise mode 2-16

L

LDAP 4-6
- Lotus Domino 4-7
- multiple servers 4-8
- Novell 4-7
- secondary server 4-7

Linux
- configuration D-12
- installing D-1

P

PAC files B-1
- browser syntax B-4
- deployment B-2
- examples B-2
- hosted B-3

policy 1-6

R

RHEL D-1

S

SSL 4-6

standalone mode 1-2

W

WPAD C-1