CHAPTER 2

Installing Connector on Windows

Revised: May 8, 2012

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 fail-over 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.

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.

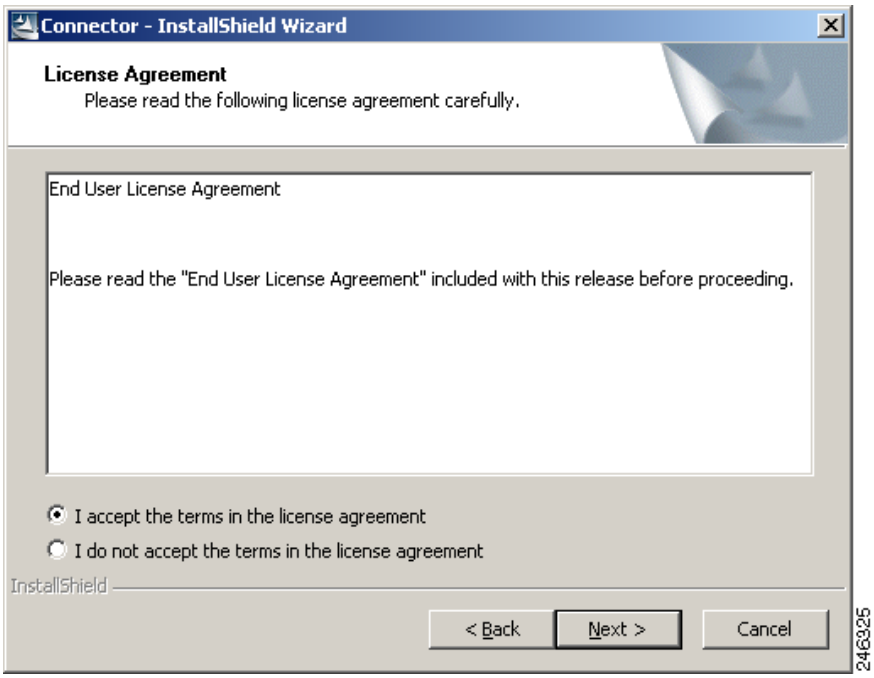
Note Following all installations you must apply the relevant Windows registry patches. See Applying the Windows Registry Patches, page 2-32.

Installing in Standalone Mode

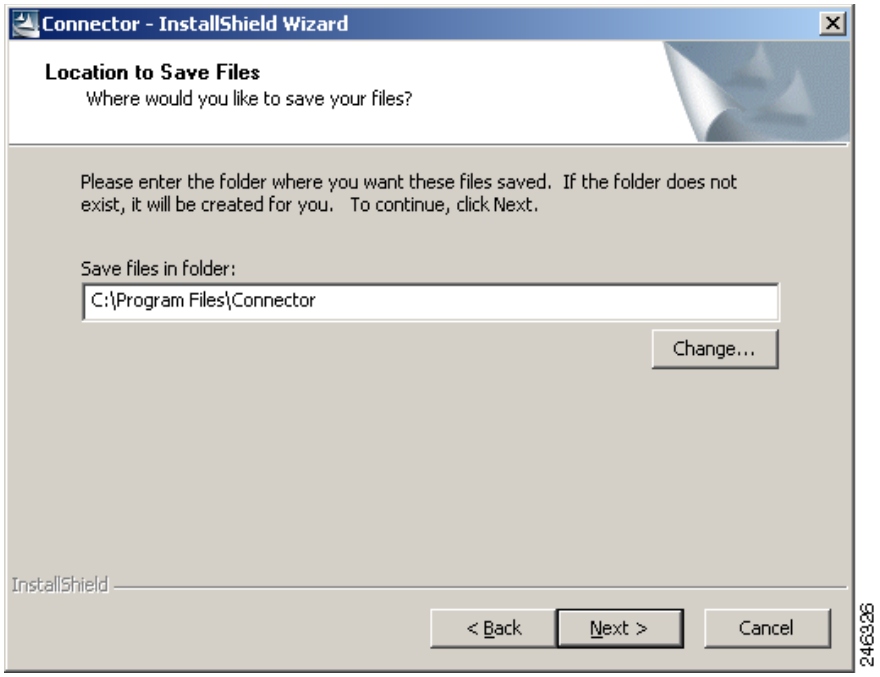
To install Connector in standalone mode:

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

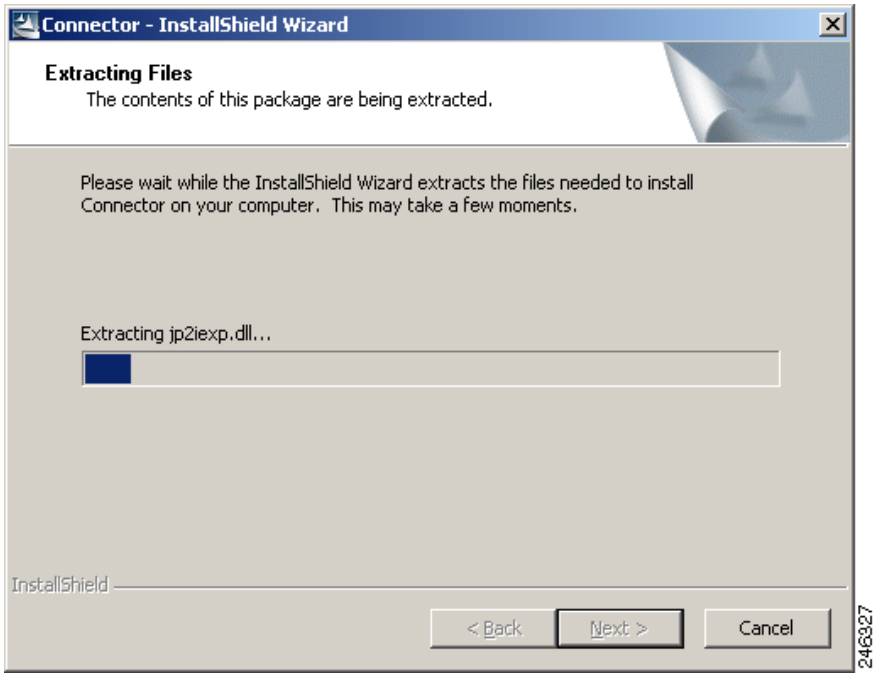
Step 2 Click **Next** to display the License Agreement dialog.



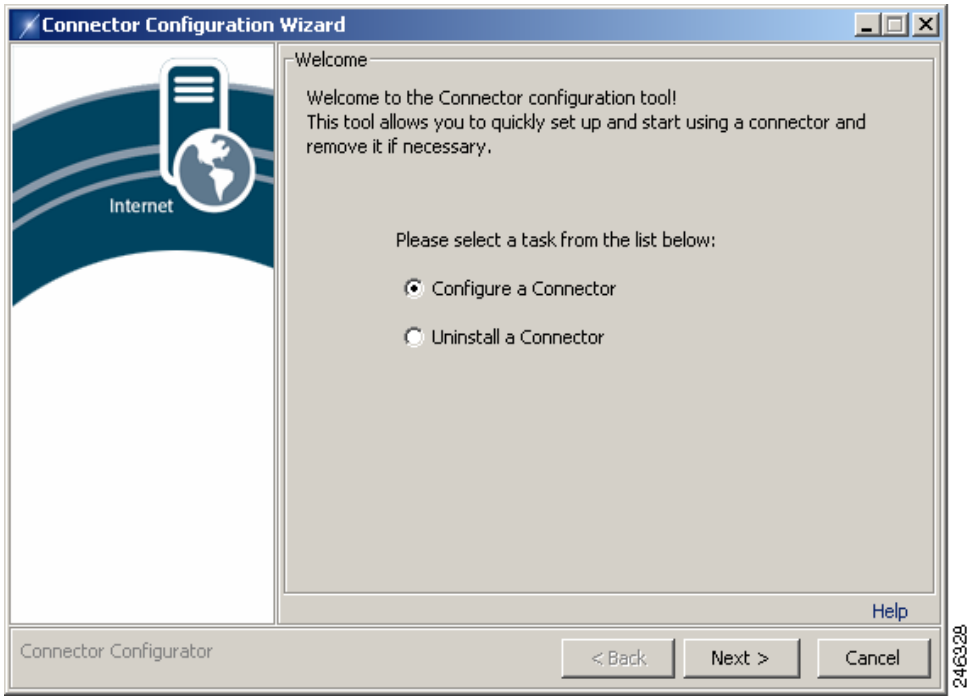
Step 3 Read the End User License Agreement. If you agree to the terms, click **I accept the terms in the license agreement** then click **Next** to display the Location to Save Files dialog. Alternatively, if you do not agree to the terms, click **Cancel** to stop the installation.



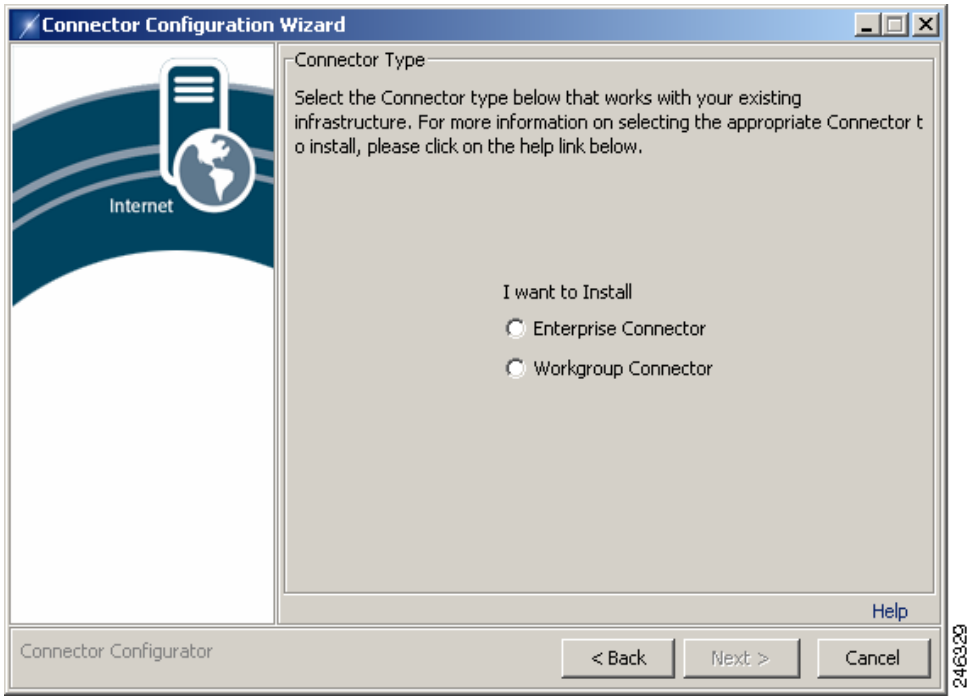
Step 4 Click **Next** to accept the default installation folder. Alternatively, enter a new path in the **Save files in folder** box, or click **Change** and navigate to the required folder, then click **Next** to display the Welcome dialog.



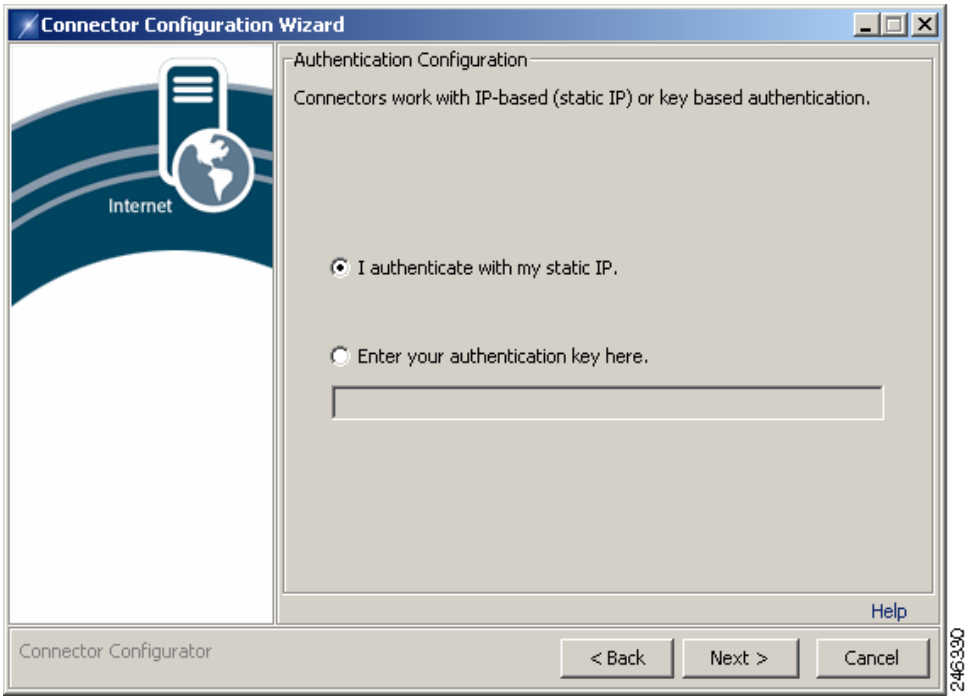
Step 5 Click **Configure a Connector** then click **Next** to display the Connector Type dialog.



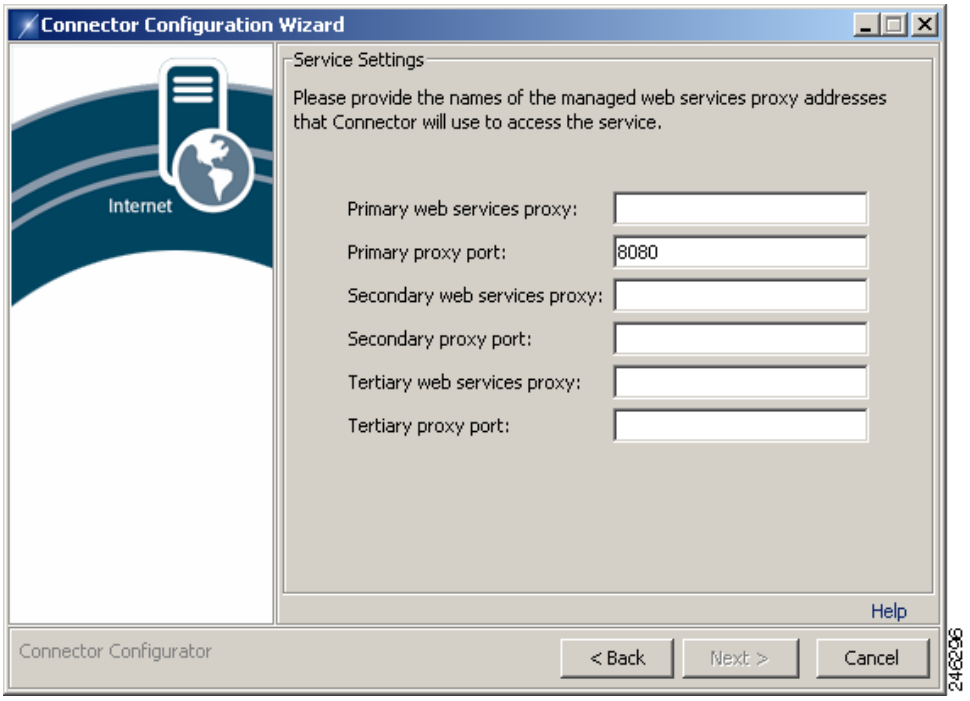
Step 6 Click **Workgroup Connector** then click **Next** to display the Authentication Configuration dialog.



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.



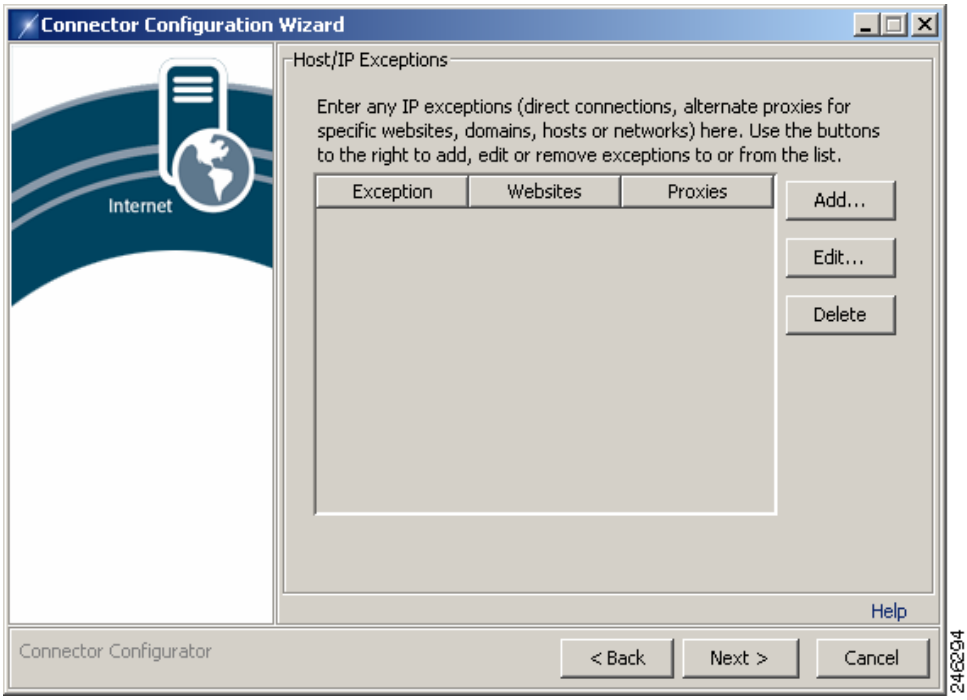
Step 8 Click **Next** to display the Service Settings dialog.



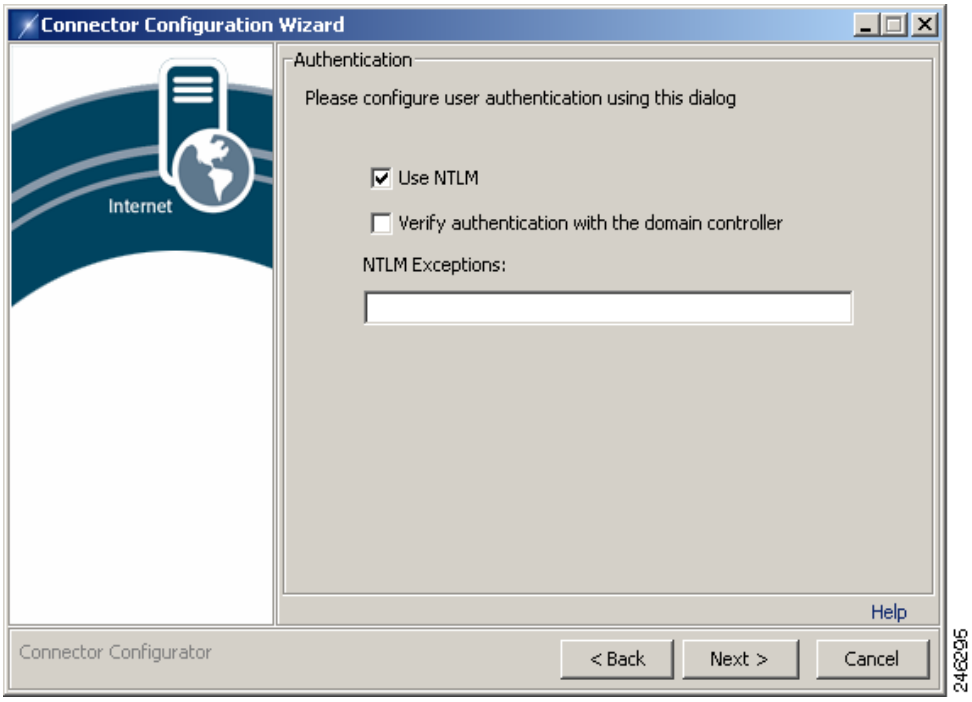
Step 9 Your proxy settings are contained in your provisioning email. If you have not received this email, contact your support representative. Normally only primary and secondary proxies are provided. You can specify up to three proxy servers:

- 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.



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.

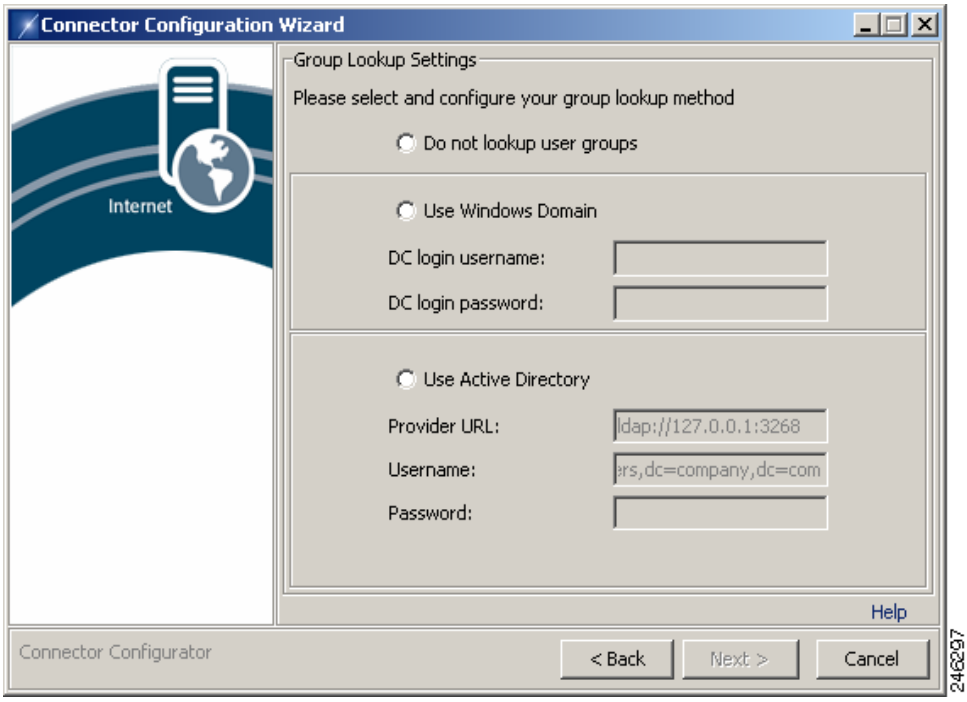


Step 12 Ensure the **Use NTLM** check box is selected. Do not clear this check box unless instructed to do so by your support representative.

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.



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.

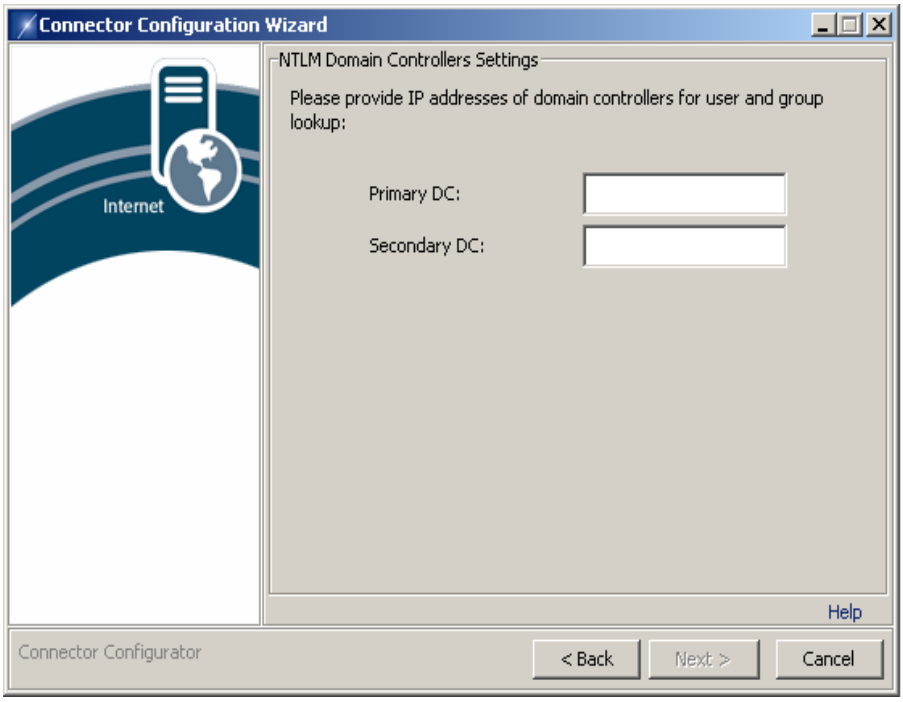
Alternatively, to use NTLM to gather group information:

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.

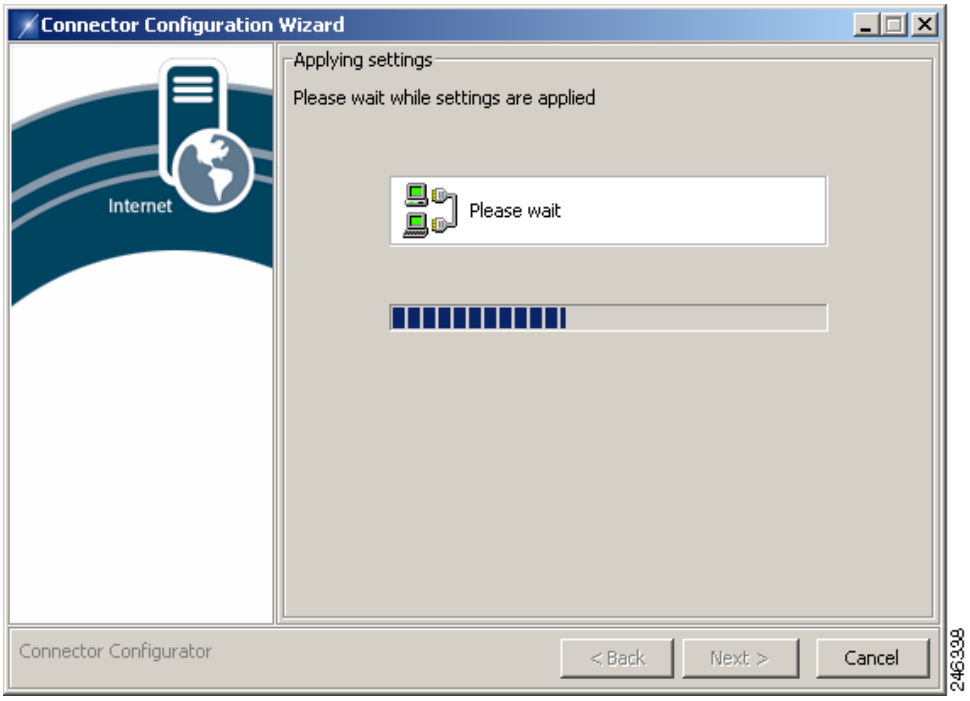


i. Enter the IP address of your primary domain controller in the Primary DC box.

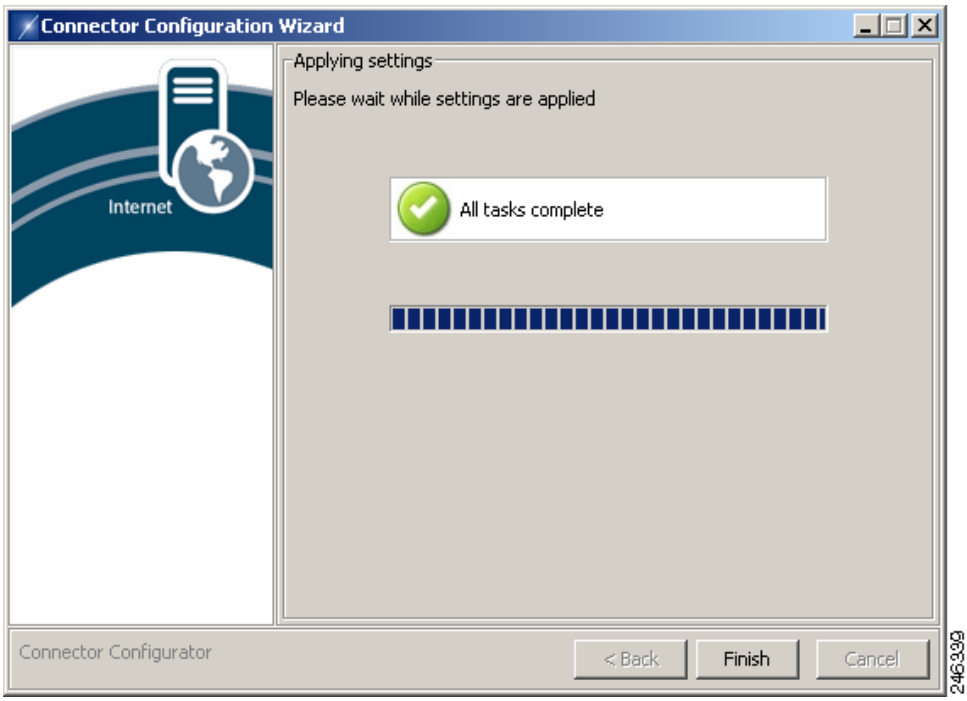
j. If you have a secondary domain controller, enter its IP address in the Secondary DC box.

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.



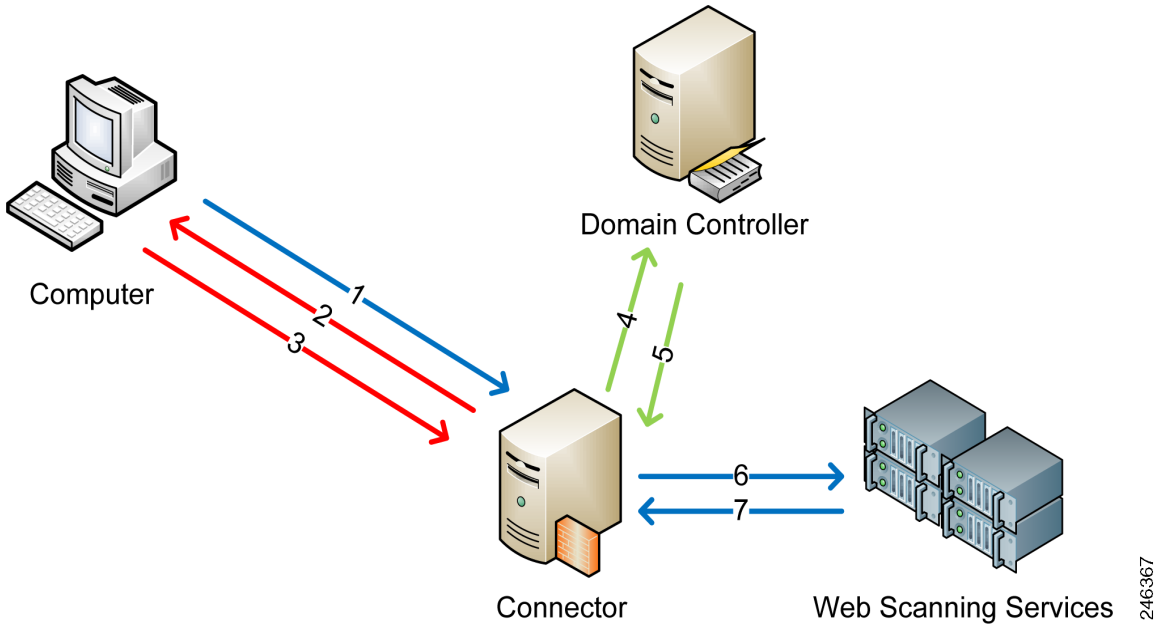
Step 19 When the installation tasks have completed successfully, the following dialog is displayed.



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 Cloud Web Security. 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 Cloud Web Security.



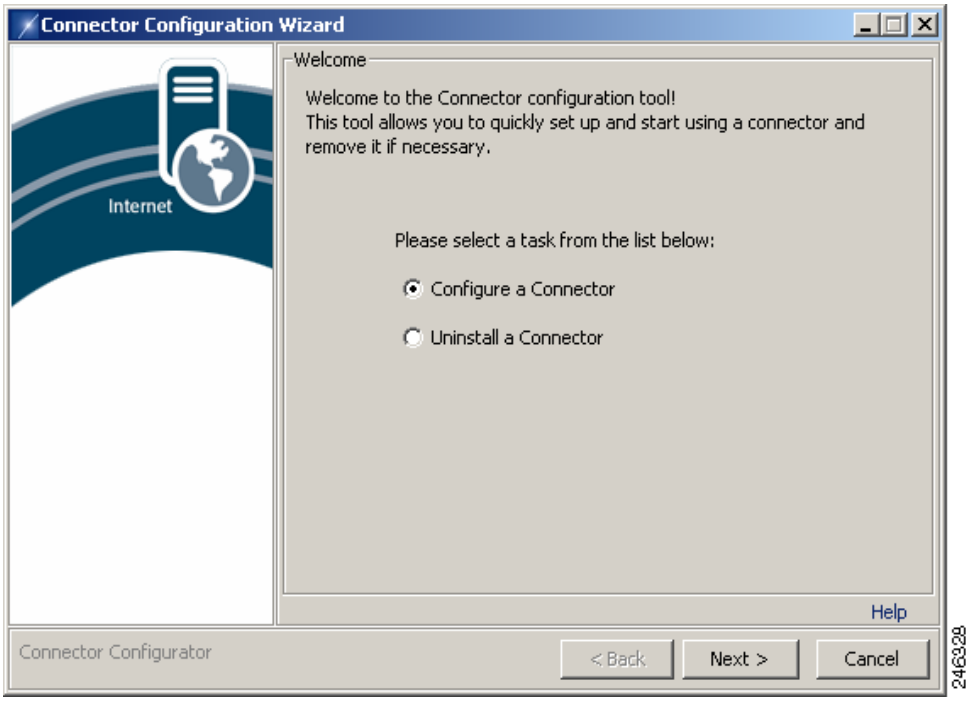
1. Web browser requests a URL.
2. Connector performs an NTLM challenge.
3. Web browser responds with NTLM user details.
4. Connector uses credentials to poll the domain controller (LDAP) for AD Groups. If the user exists, Connector performs a query based on user name to lookup groups.
5. Domain controller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

Adding Host Exceptions

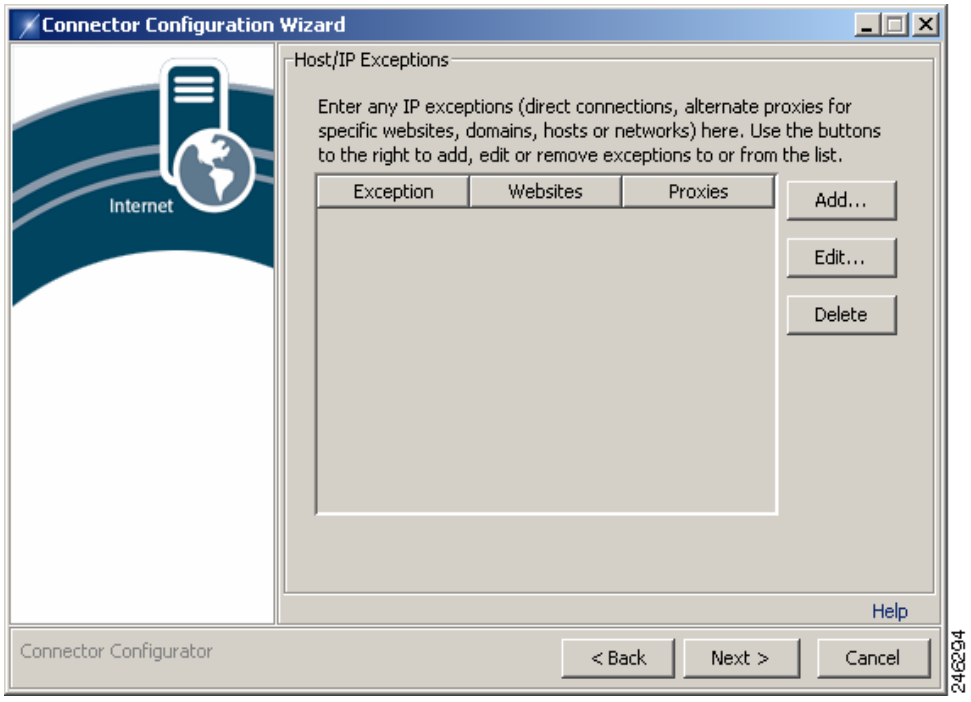
Host exceptions are used to allow users to bypass Cloud Web Security when connecting to specified websites. Exceptions can include wild cards, address ranges, and IP ports. They should not be used for connections to your own network because a proxy server (local exception) set in a user's browser is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



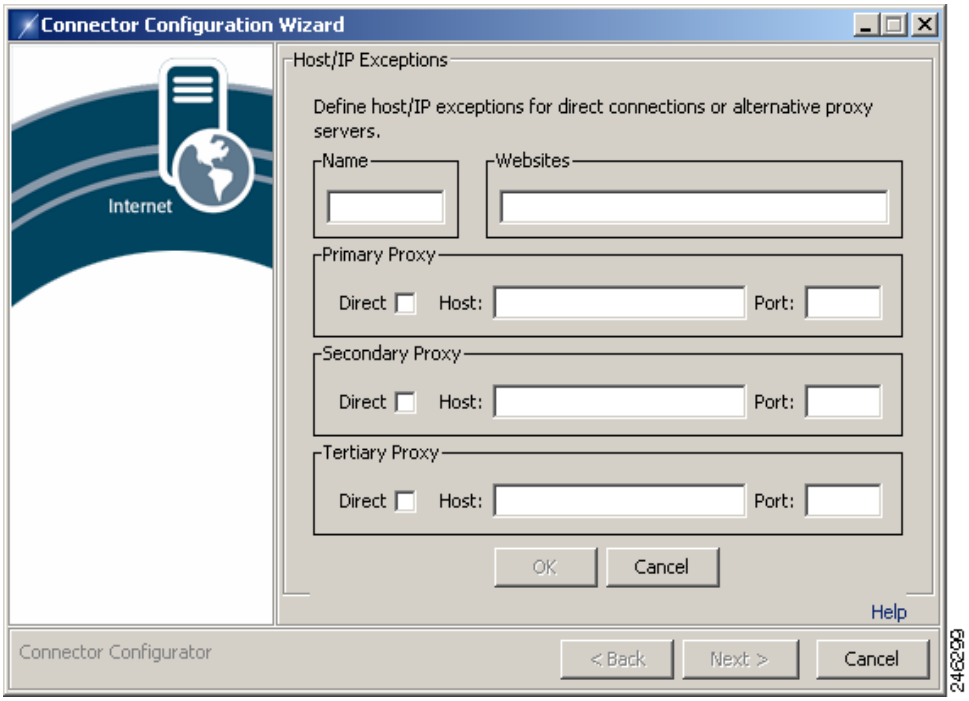
Step 2 The wizard imports the settings from your last session so it is not necessary to specify that you are using a standalone server, your method of authentication, or the service settings. At each dialog, click **Next** until the Host/IP Exceptions dialog is displayed.



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.

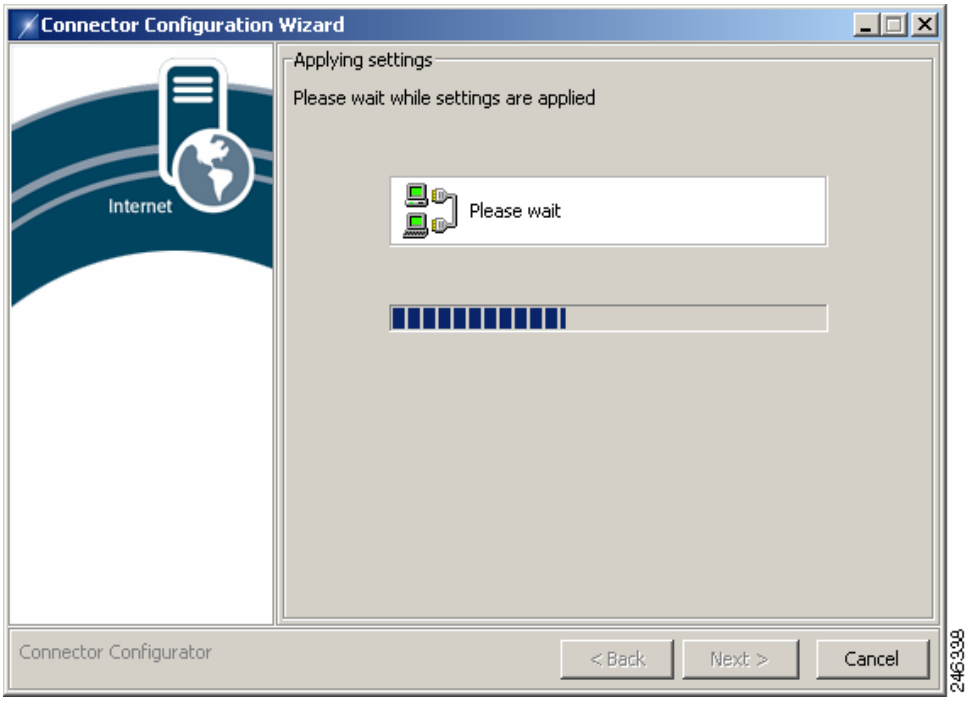
Step 4 For each exception you want to add:

1. Click **Add**.

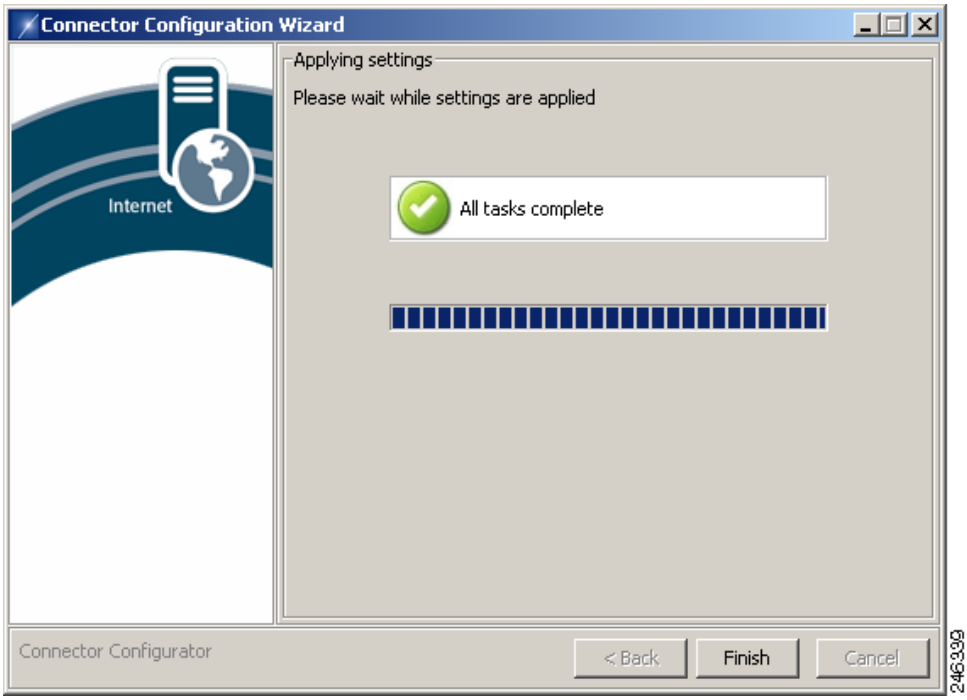


2. Enter a **Name** for the exception.
3. Enter the websites which the exception will be applied to, separated by commas. Websites can be entered:
   - in full (`www.company.com`)
   - with wildcards (`*.company.com`)
   - as an IP address (`164.35.91.46`)
   - as a range of IP addresses (`164.35.91.*`)
   - 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.



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



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

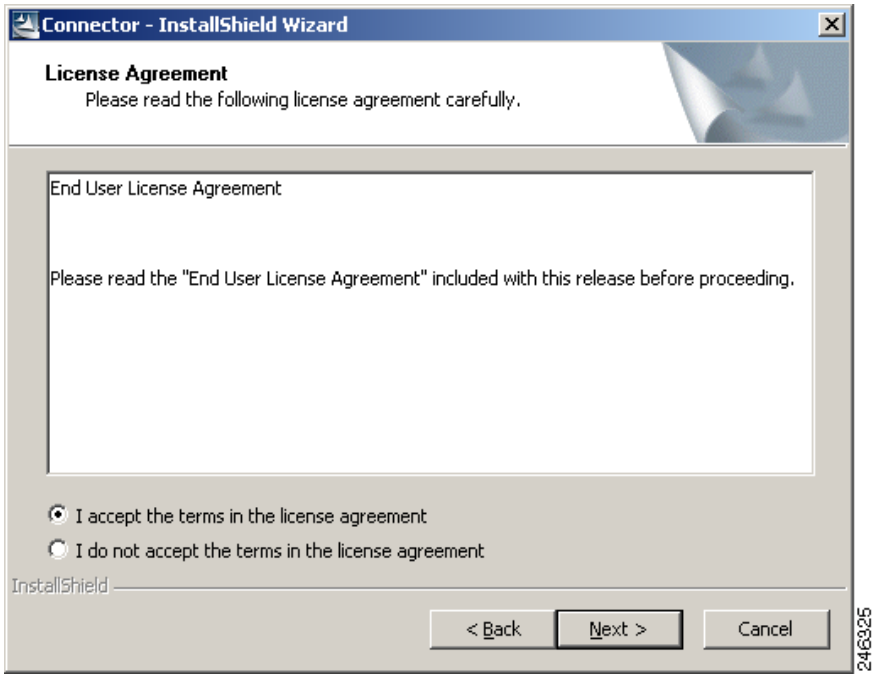
Installing in Enterprise Mode

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

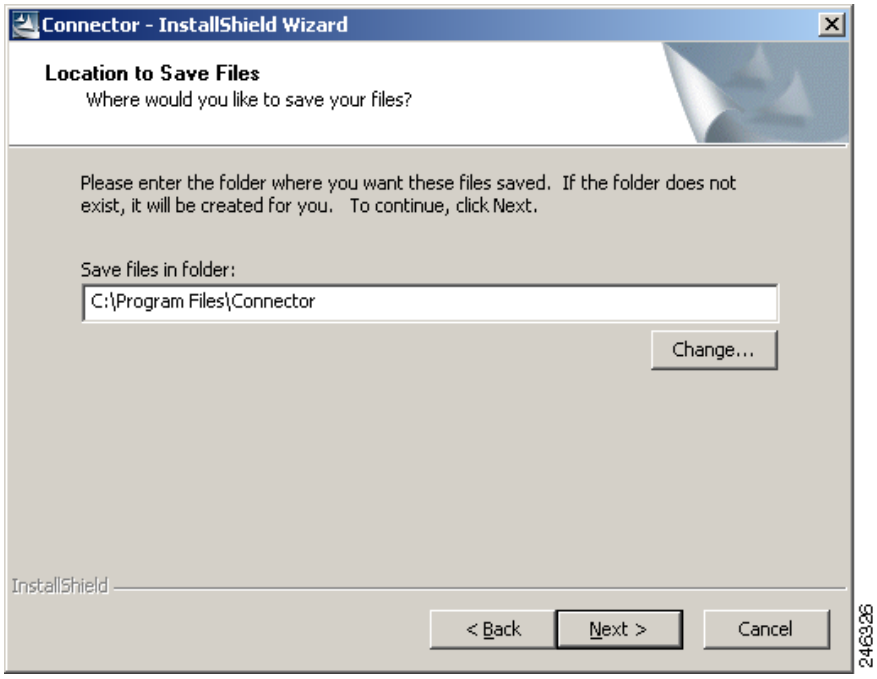
To install Connector in Enterprise mode:

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

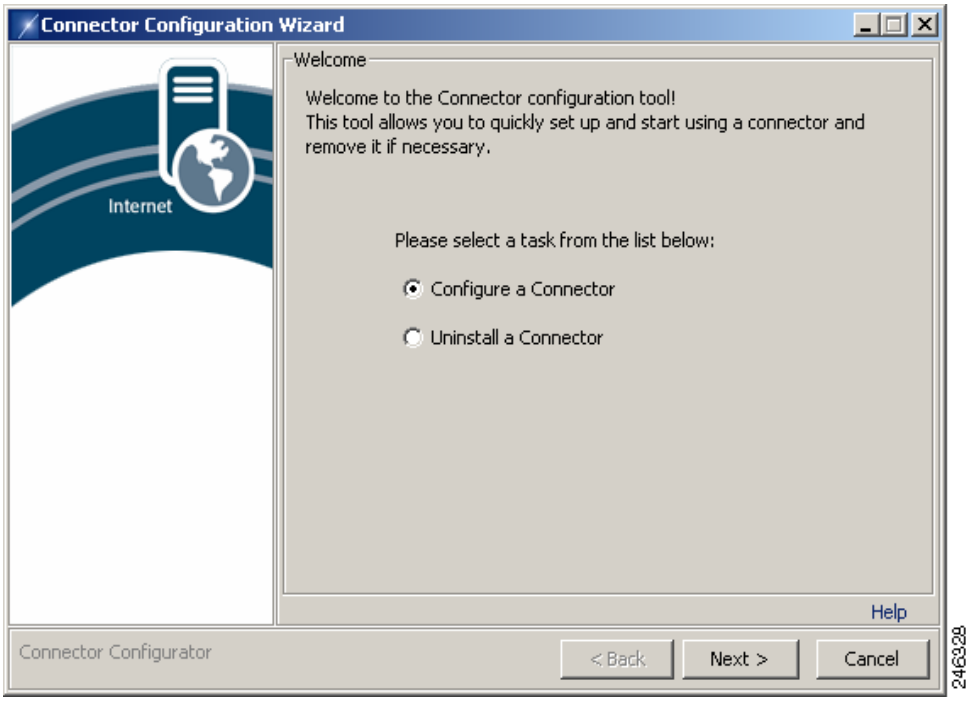
Step 2 Click **Next** to display the License Agreement dialog.



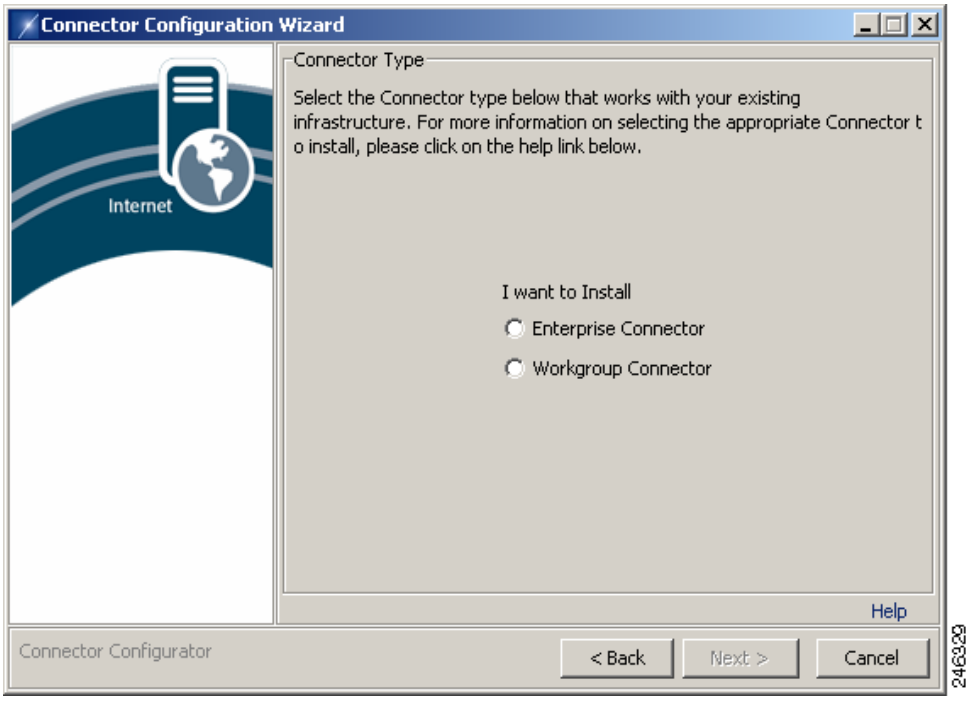
Step 3 Read the End User License Agreement. If you agree to the terms, click **I accept the terms in the license agreement** then click **Next** to display the Location to Save Files dialog. Alternatively, if you do not agree to the terms, click **Cancel** to stop the installation.



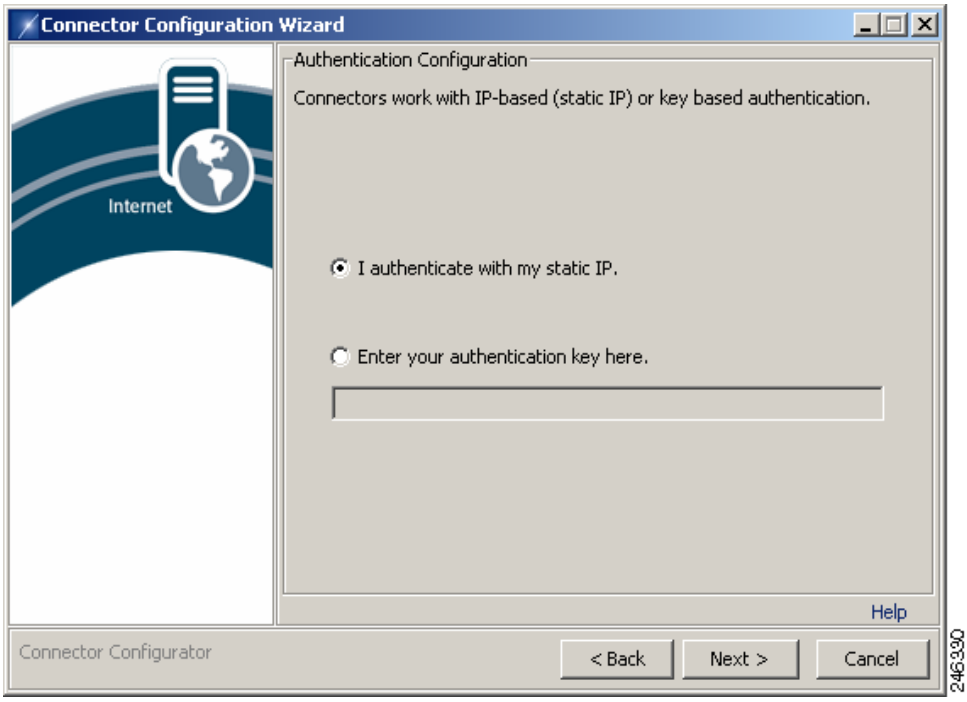
Step 4 Click **Next** to accept the default installation folder. Alternatively, enter a new path in the **Save files in folder** box, or click **Change** and navigate to the required folder, then click **Next** to display the Welcome dialog.



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

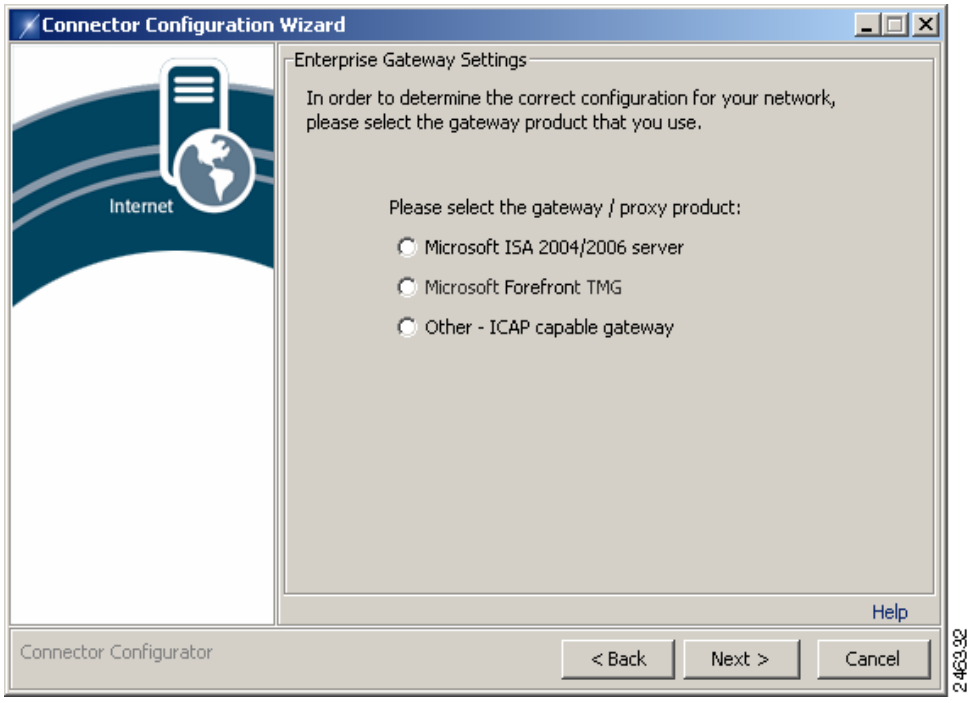


Step 6 Click **Enterprise Connector** then click **Next** to display the Authentication Configuration dialog.



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*.

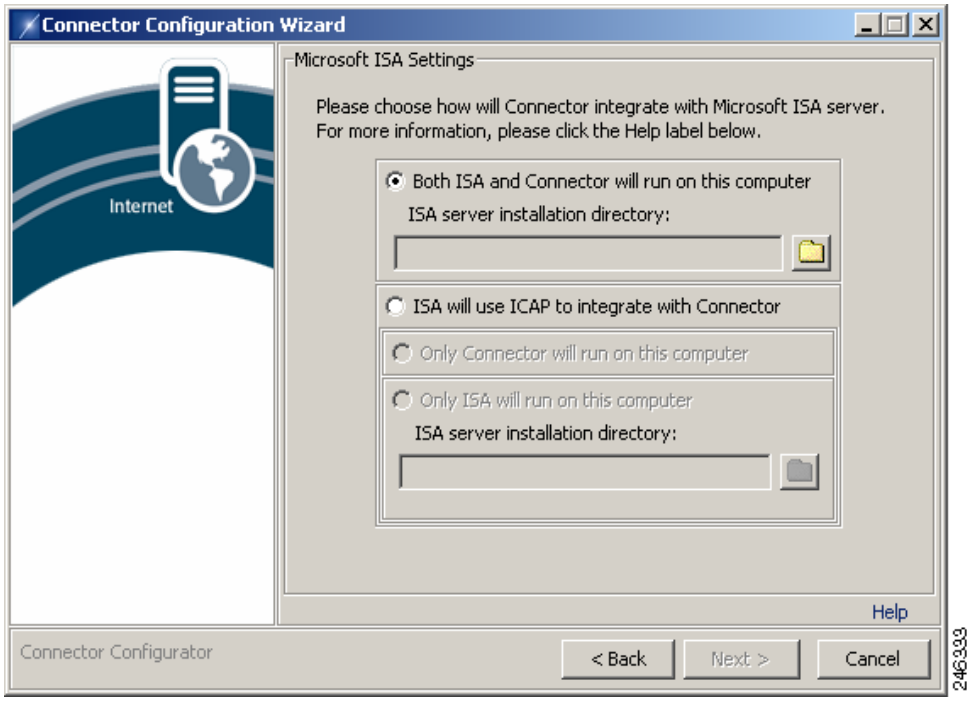
Step 8 Click **Next** to display the Enterprise Gateway Settings dialog.



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.

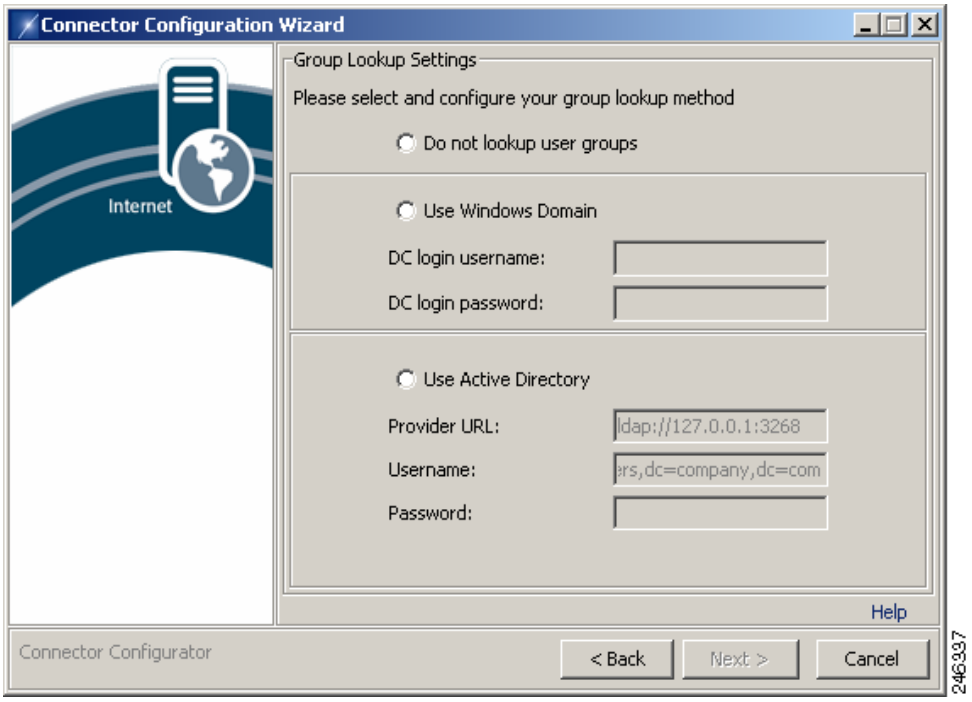


c. Click **ISA will use ICAP to integrate with Connector**.

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.



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:

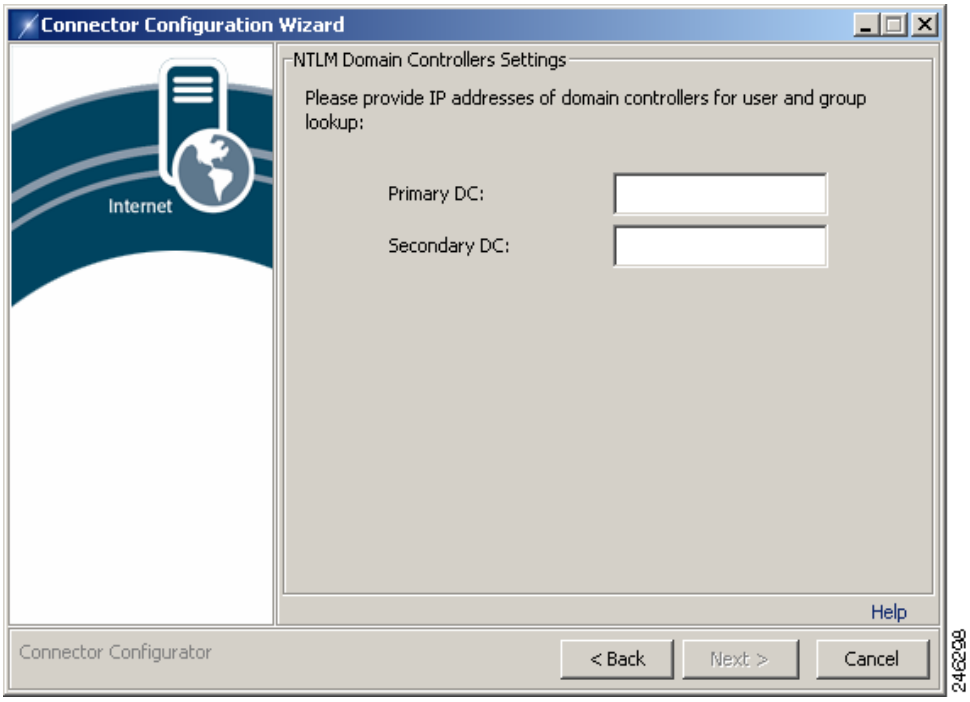
a. Click **Use Windows Domain**.

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.



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

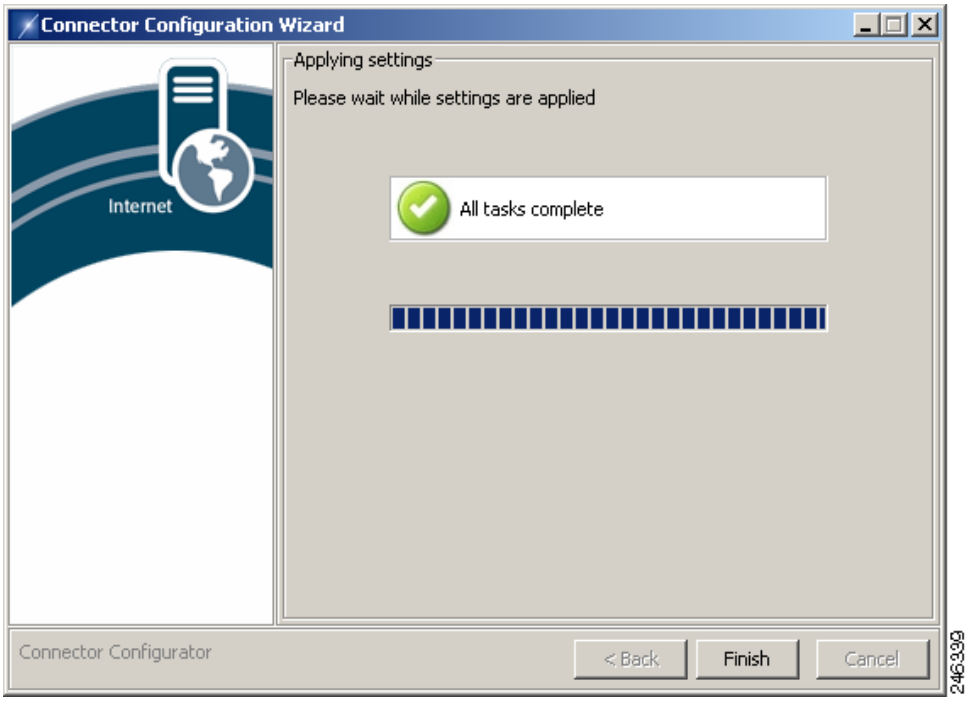
g. If you have a secondary domain controller, enter its IP address in the **Secondary DC** box.

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.

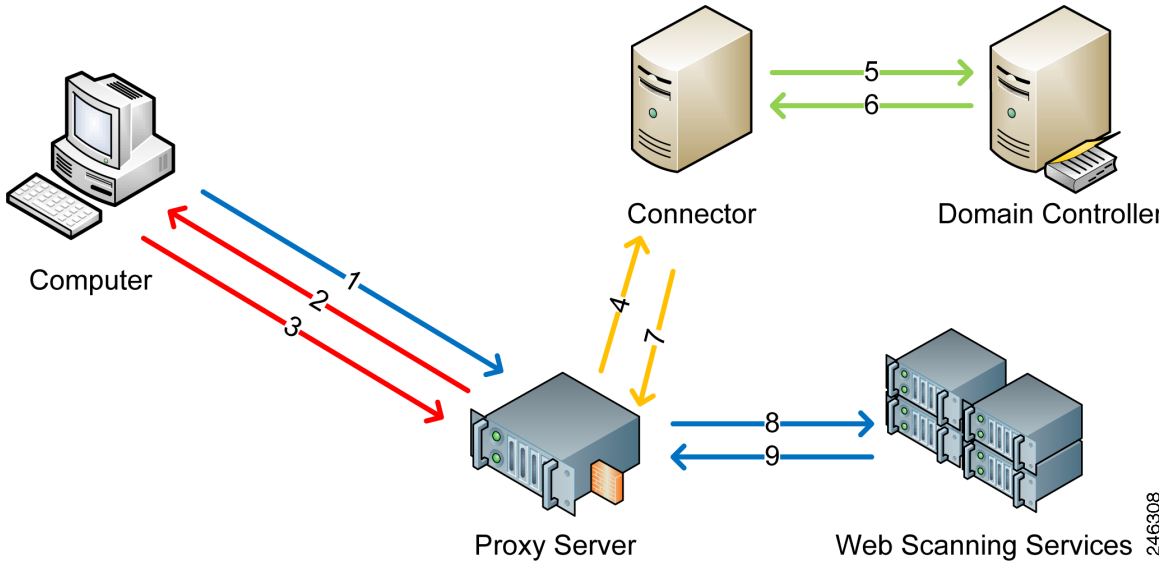
When the installation tasks have completed successfully, the following dialog is displayed:



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 Cloud Web Security. 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 Cloud Web Security.



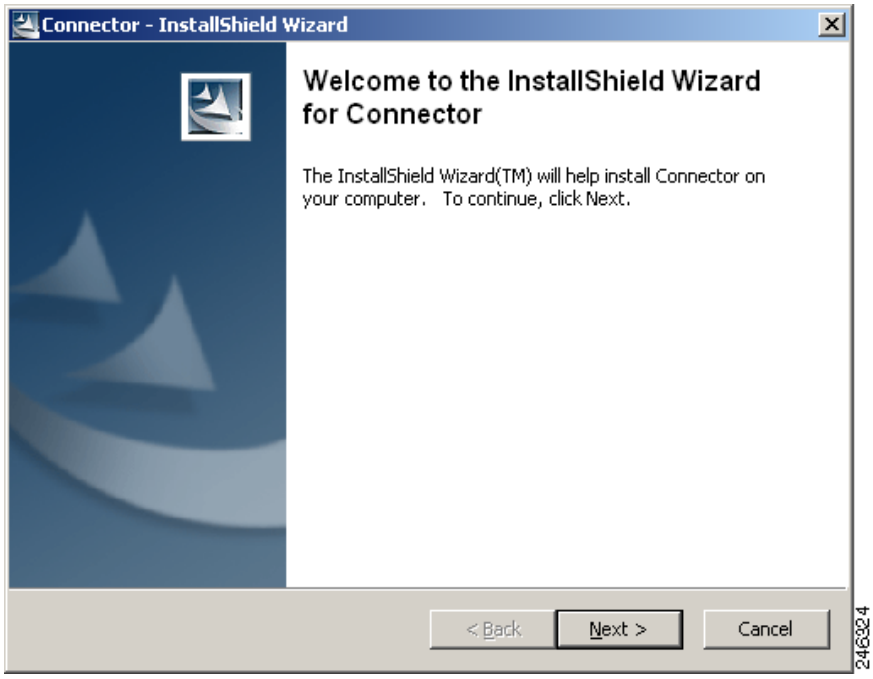
1. Web browser requests a URL.
2. Proxy server performs an NTLM challenge.
3. Web browser responds with NTLM user details.
4. URL request is forwarded with NTLM credentials to Connector.
5. Connector uses the credentials to poll the domain controller (LDAP) for AD Groups. If the user exists, Connector 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 Cloud Web Security.
9. Content sent back to the user via the proxy server.

Configuring Microsoft Forefront TMG or ISA Server

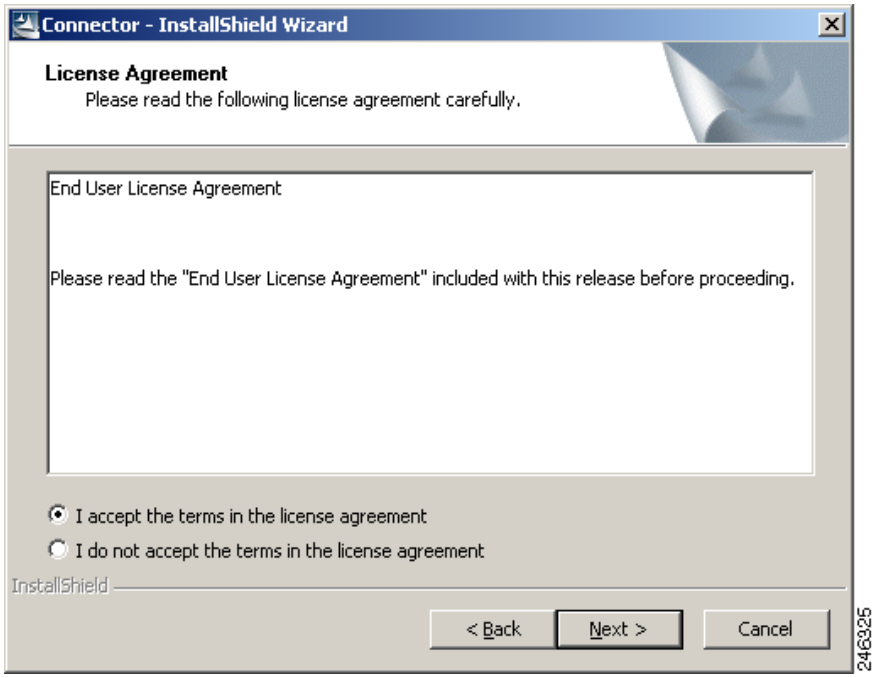
The recommended method for using Microsoft Forefront TMG or ISA Server 2004 or 2006, with Connector is to install Connector, Forefornt TMG or ISA Server, and the Forefront TMG or ISA Server plug-in on a shared server. You must use separate folders to install the ICAP sender and receiver, for example 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:

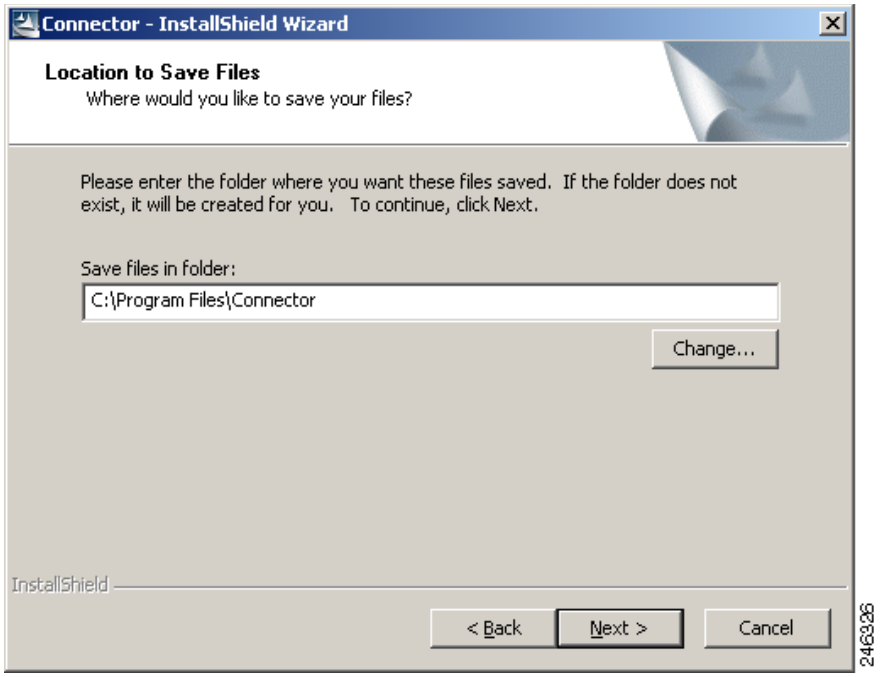
Step 1 Double-click the Connector program file to run the installation wizard.



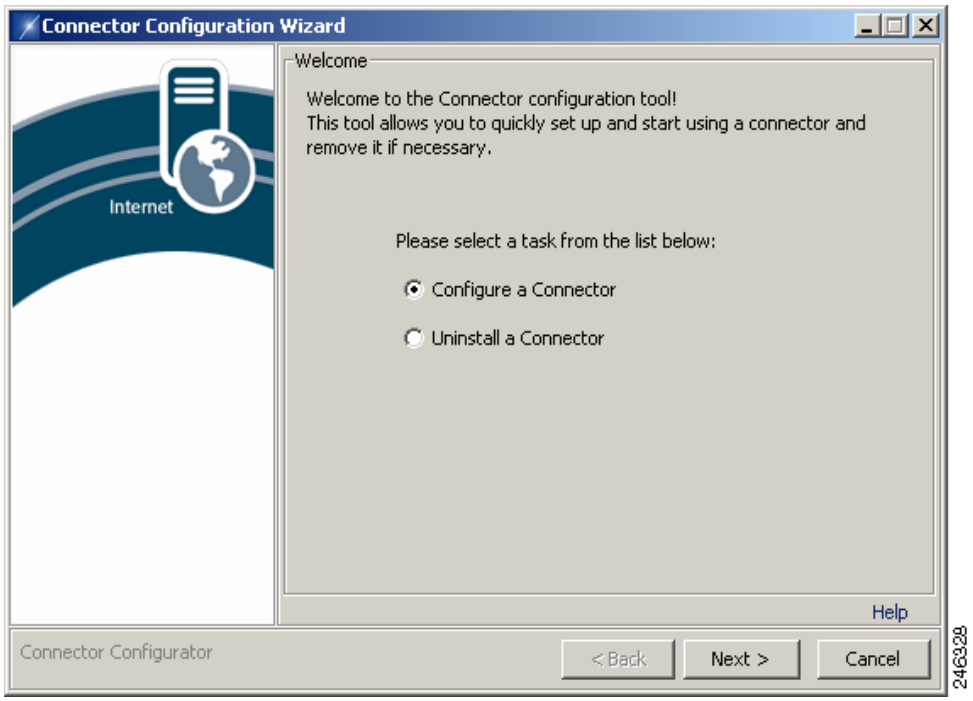
Step 2 Click **Next** to display the License Agreement dialog.



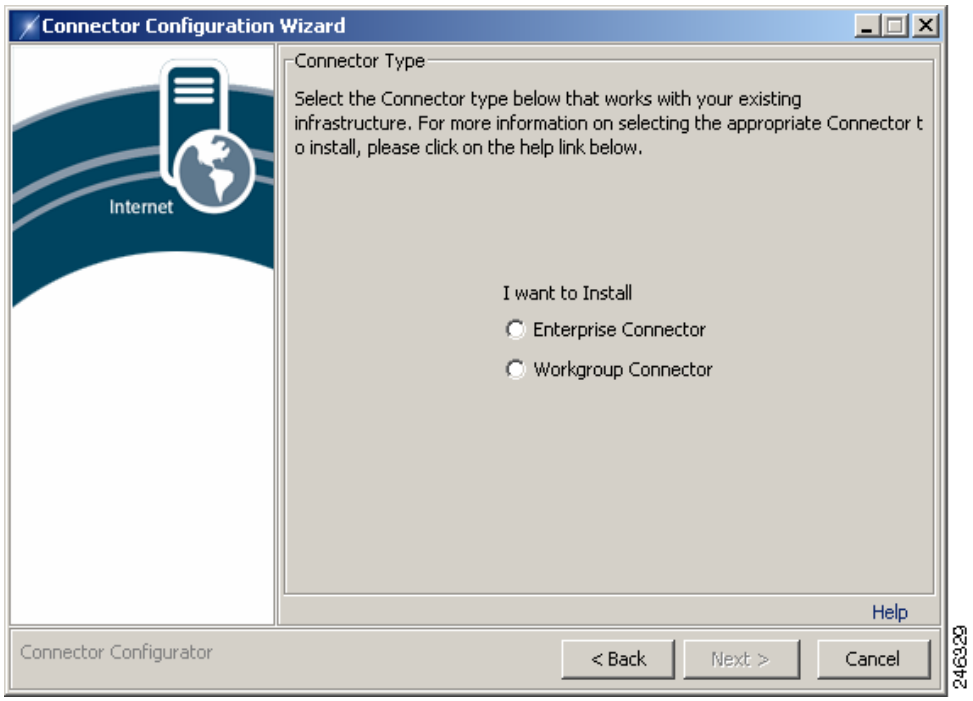
Step 3 Read the End User License Agreement. If you agree to the terms, click **I accept the terms in the license agreement** then click **Next** to display the Location to Save Files dialog. Alternatively, if you do not agree to the terms, click **Cancel** to stop the installation.



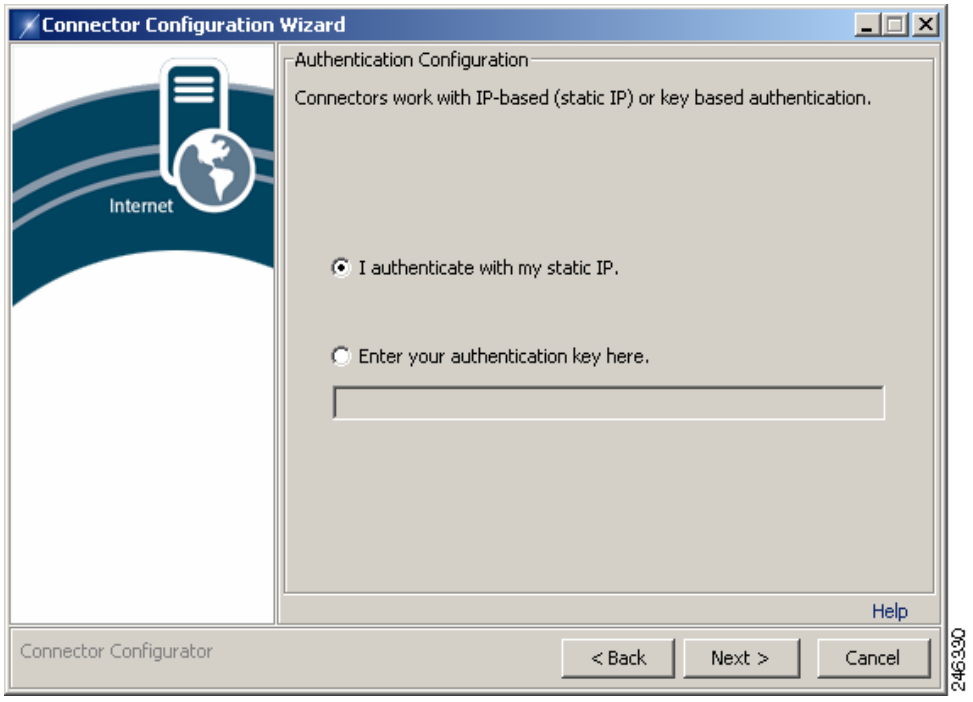
Step 4 You must choose a different folder from the one in which you installed Connector. Enter a new path in the **Save files in folder** box, or click **Change** and navigate to the required folder, then click **Next** to display the Welcome dialog.



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

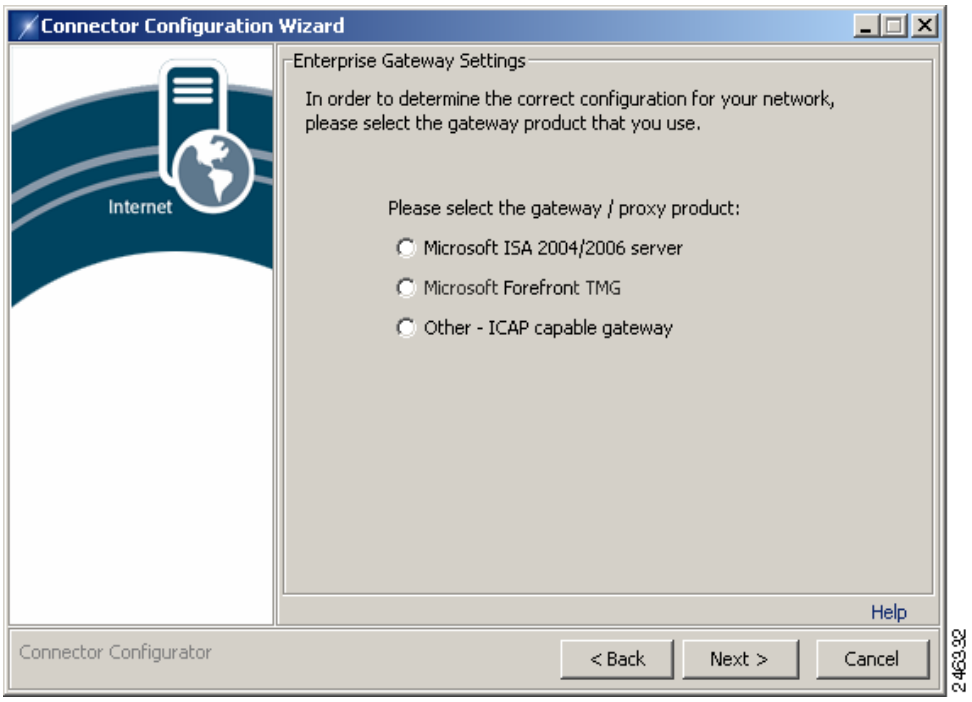


Step 6 Click **Enterprise Connector** then click **Next** to display the Authentication Configuration dialog.



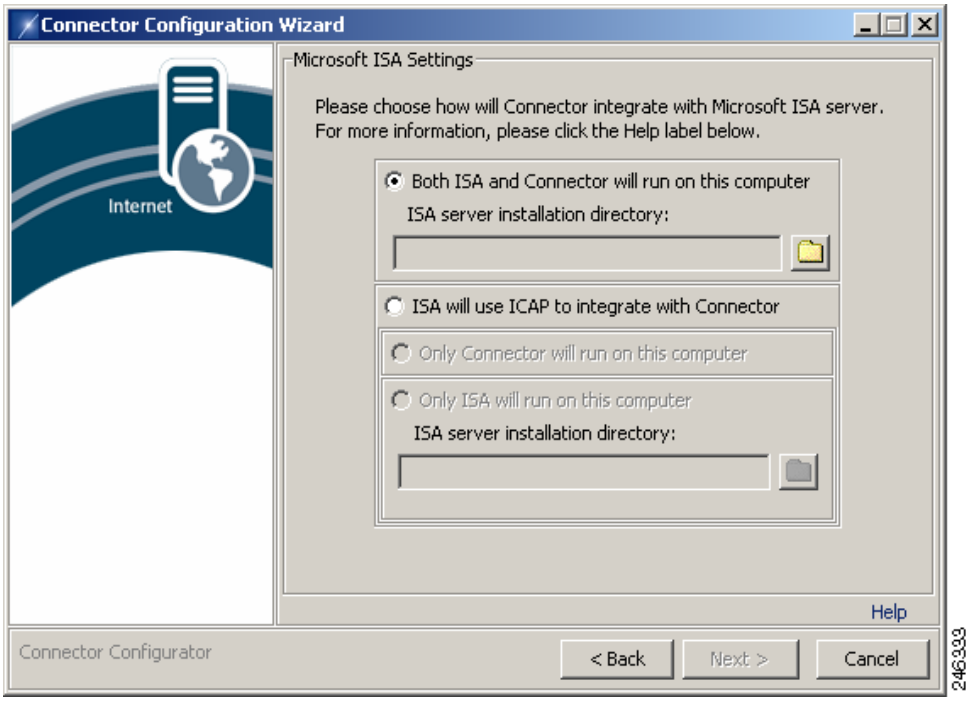
Step 7 You can use IP-based or key based authentication. IP-based authentication requires a static IP address. To use IP-based authentication, click **I authenticate with my static IP**. Alternatively, click **Enter your authentication key here** and enter a company or group authentication key. For details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

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



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

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

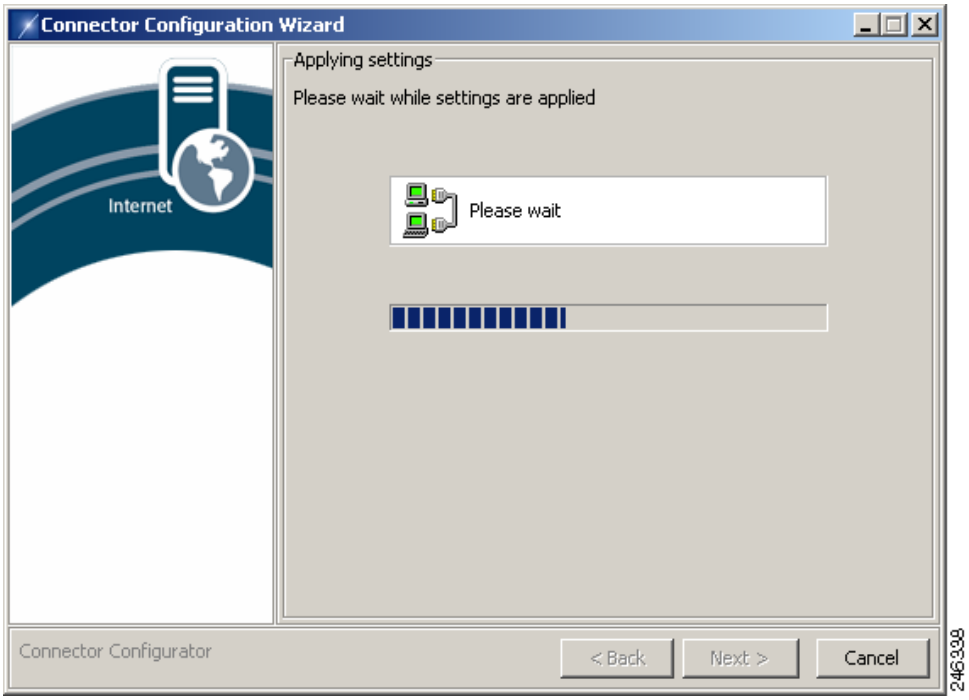


Step 11 Click **ISA will use ICAP to integrate with Connector**.

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

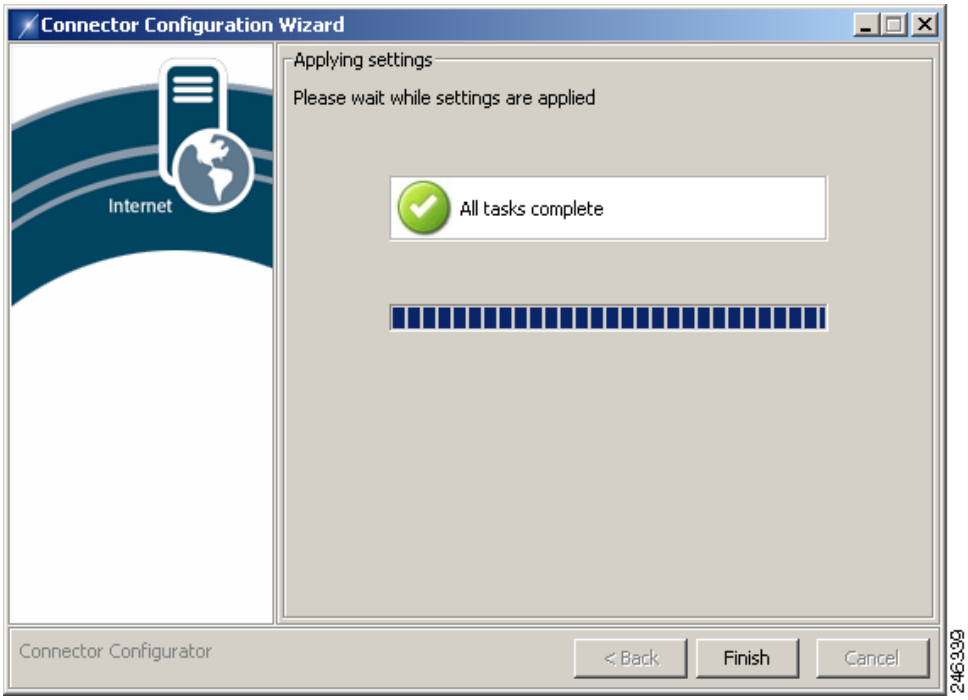
Step 13 Click the folder button and navigate to the folder where ISA is installed.

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



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.



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 Cloud Web Security 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 Cloud Web Security 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 time-out 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 Cisco Cloud Web Security

In some cases you may need to bypass Cloud Web Security 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 Cloud Web Security 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 Cloud Web Security.

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.

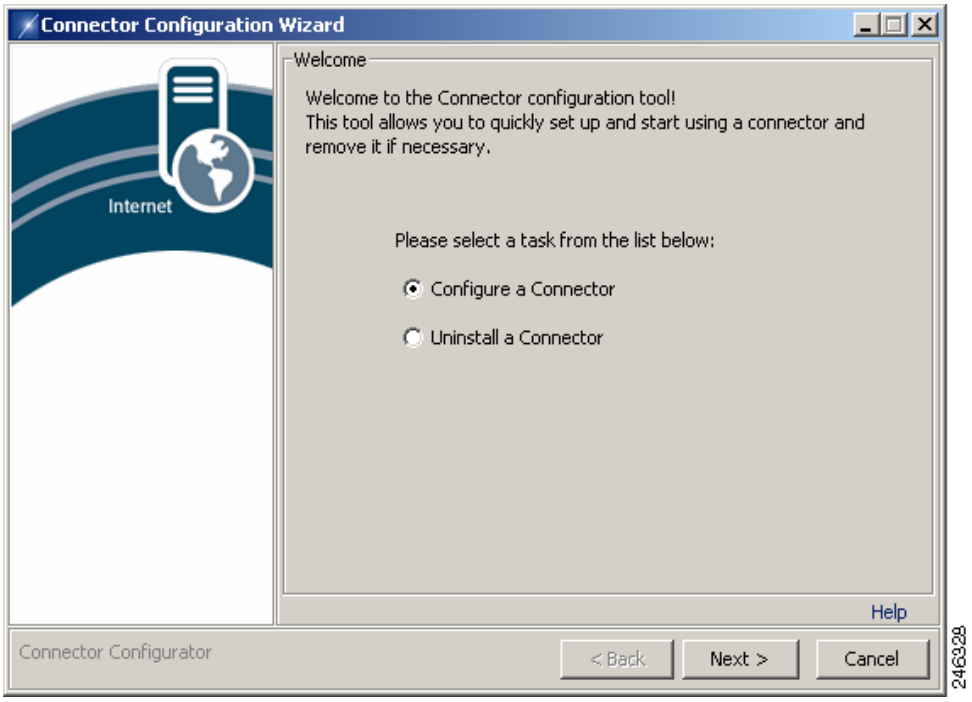
Upgrading Connector

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.

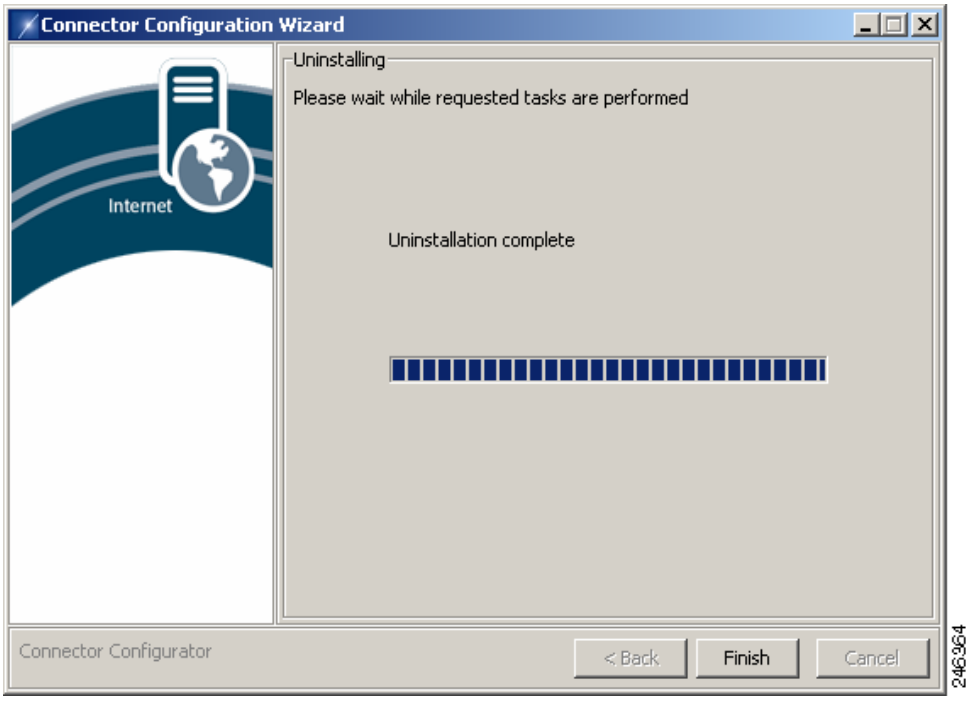
Removing Connector

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.



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



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.