CHAPTER 2

Installing and Configuring Active Directory Agent

Active Directory Agent is a software application that comes packaged as a Windows installer. You must install it on a Windows machine and configure it with client devices and AD domain controllers.

This chapter contains the following topics:

- Requirements
- Installing Active Directory Agent
- Confirming Active Directory Agent Installation
- Uninstalling Active Directory Agent
- Configuring Active Directory Agent, page 2-8
  - Configuring AD Agent to Send Logs to a Syslog Server, page 2-9
  - Configuring AD Agent to Obtain Information from AD Domain Controllers, page 2-9
  - Configuring AD Agent to Allow Client Devices to Obtain Information from AD Agent, page 2-11

Note You must refer to the ASA end-user documentation for configurations related to the ASA device.

Requirements

This section contains the following topics:

- Hardware Requirements, page 2-2
- Connectivity Requirements, page 2-2
- List of Open Ports, page 2-4
- Active Directory Requirements, page 2-5

Hardware Requirements

To install the Active Directory Agent, you need any one of the following:

- A Windows 2003 machine
- A Windows 2008 machine
- A Windows 2008 R2 machine

Note Windows 2003 R2 is not supported.

Note Internationalization is not supported.

This AD Agent machine could be one of the Active Directory domain controller machines that you will be monitoring, or it can be a separate, dedicated, Windows machine.

If your solution requires multiple AD Agent machines to be installed, remember that:

- There is no limit on the number of AD Agent machines that are not domain controller machines.
- For a given AD domain, you can directly install the AD Agent on only one domain controller machine.

In all cases, an AD Agent machine must meet the minimum hardware specifications listed in Table 2-1.

Table 2-1 Minimum Required Hardware Specifications for the AD Agent Machine

Component	Specification
CPU	Intel Xeon 2.66 GHz Q9400 (Quad Core)
System memory	4 GB of SDRAM
Hard disk space	500 GB

Connectivity Requirements

For the AD Agent to function properly, it must be able to communicate freely with all the client devices, Active Directory domain controller machines, and target syslog servers that are configured with it. If Windows Firewall (or any other comparable third-party firewall software) is running on the AD Agent machine, or on any of the Active Directory domain controller machines, then the firewall software on each of these endpoints must be configured with the necessary exceptions to allow this communication to flow freely.

This section uses the Windows Firewall as an example and details the exceptions that must be defined on any of the endpoints that might be running Windows Firewall:

- Windows Firewall Exceptions to be Configured on the AD Agent Machine, page 2-3
- Windows Firewall Exceptions to be Configured on Each Separate Active Directory Domain Controller Machine, page 2-4

For any other comparable third-party firewall software, refer to that vendor's documentation on how to configure the corresponding exceptions.

Windows Firewall Exceptions to be Configured on the AD Agent Machine

If Windows Firewall is enabled on the AD Agent machine, then:

a. You must explicitly define Windows Firewall exceptions for the following programs:

- C:\IBF\adObserver\ADObserver.exe
- C:\IBF\radiusServer\runtime\win32\bin.build\rt_daemon.exe

If the AD Agent machine is running Windows Server 2008 or Windows Server 2008 R2, then you can use the following Windows command lines (each written on a single line) to define these exceptions:

- **netsh advfirewall firewall add rule name="Cisco AD Agent (AD Observer)" dir=in action=allow program="C:\IBF\adObserver\ADObserver.exe" enable=yes**
- **netsh advfirewall firewall add rule name="Cisco AD Agent (RADIUS Server)" dir=in action=allow program="C:\IBF\radiusServer\runtime\win32\bin.build\rt_daemon.exe" enable=yes**

If the AD Agent machine is running Windows Server 2003 (with SP1 or later installed), then you can use the following Windows command lines (each written on a single line) to define these exceptions:

- **netsh firewall add allowedprogram C:\IBF\adObserver\ADObserver.exe "Cisco AD Agent (AD Observer)" ENABLE**
- **netsh firewall add allowedprogram C:\IBF\radiusServer\runtime\win32\bin.build\rt_daemon.exe "Cisco AD Agent (RADIUS Server)" ENABLE**

Note The original Windows Server 2003 did not support Windows Firewall. Windows Server 2003 SP1 added support for Windows Firewall, but left it disabled by default. Windows Server 2003 SP2 enables Windows Firewall by default.

1. If you use the **adacfg dc create** command to configure any Active Directory domain controller machine that is separate from the AD Agent machine, then you must also define a Windows Firewall exception on the AD Agent machine that will allow the necessary WMI-related communication.

Note In every case where the Windows Firewall is enabled on the AD Agent machine and on another separate, domain controller machine, and the AD Agent must communicate with the AD domain controller machine, each machine must have an exception for WMI. If the Windows Firewall is not running on either one of these machines, then a WMI exception is not required on that particular machine. A WMI exception is also not required when there is one single AD domain controller and the AD Agent is running on that same machine.

If the AD Agent machine is running Windows Server 2008 or Windows Server 2008 R2, then you can use the following Windows command line (written on a single line) to configure this WMI-related exception:

```
netsh advfirewall firewall set rule group="Windows Management Instrumentation (WMI)"
new enable=yes
```

If the AD Agent machine is running Windows Server 2003 (with SP1 or later installed), then you can use the following Windows command lines (each written on a single line) to configure this WMI-related exception:

- `netsh firewall add portopening protocol=tcp port=135 name="Cisco AD Agent (WMI_DCOM_TCP135)"`
- `netsh firewall add allowedprogram program=%windir%\system32\wbem\unsecapp.exe name="Cisco AD Agent (WMI_UNSECAPP)"`

Windows Firewall Exceptions to be Configured on Each Separate Active Directory Domain Controller Machine

For each separate Active Directory domain controller machine that is configured on the AD Agent machine using the **adacfg client create** command, if Windows Firewall is enabled on that separate domain controller machine, then you must define a Windows Firewall exception on that particular domain controller machine that will allow the necessary WMI-related communication.

If that domain controller machine is running Windows Server 2008 or Windows Server 2008 R2, then you can configure this WMI-related exception using the following Windows command line (written on a single line):

```
netsh advfirewall firewall set rule group="Windows Management Instrumentation (WMI)" new enable=yes
```

If that domain controller machine is running Windows Server 2003 (with SP1 or later installed), then you can configure this WMI-related exception using the following Windows command line (written on a single line):

```
netsh firewall set service RemoteAdmin enable
```

List of Open Ports

Table 2-2 lists some of the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports that the AD Agent uses for communication with client devices and Active Directory domain controllers. These ports must be open on the AD Agent.

Note This list does not include the dynamically allocated (random) port numbers that are used by WMI.

Table 2-2 List of Open Ports on the AD Agent

Port No.	Protocol	Service
8888 (on the local host)	TCP	Configuration changes
514	UDP	Syslog
1645 (on all interfaces)	UDP	Legacy RADIUS
1646 (on all interfaces)	UDP	Legacy RADIUS accounting

Table 2-2 List of Open Ports on the AD Agent (continued)

Port No.	Protocol	Service
1812 (on all interfaces)	UDP	RADIUS
1813 (on all interfaces)	UDP	RADIUS accounting

The port numbers for configuration changes and RADIUS are hardwired and not configurable. No other software application that uses these ports should be running on the AD Agent machine. For example, the AD Agent machine must not be running another RADIUS server.

Active Directory Requirements

For the AD Agent to communicate with the domain controllers, you must ensure that the following prerequisites are met:

- Each individual AD domain controller machine through which users will be authenticating during login and whose Security Log will be monitored by the AD Agent must run one of the following supported versions of Windows Server:
  - Windows Server 2003
  - Windows Server 2008
  - Windows Server 2008 R2

Note Windows Server 2003 R2 is not supported.

Note Internationalization is not supported

- Also, each individual domain controller machine running Windows Server 2008 or Windows Server 2008 R2 must have the appropriate Microsoft hotfixes installed. You must install the hotfixes regardless of whether the AD Agent is installed directly on the domain controller machine, or is monitoring the domain controller machine remotely.

  For domain controller machines running Windows Server 2008, the following two Microsoft hotfixes must be installed:

  a. http://support.microsoft.com/kb/958124

     This patch fixes a memory leak in Microsoft's WMI, which if left unfixed can prevent the AD Agent from successfully connecting with that domain controller and achieving an "up" status.

  b. http://support.microsoft.com/kb/973995

     This patch fixes a memory leak in Microsoft's WMI, which if left unfixed can sporadically prevent Active Directory from writing the necessary authentication-related events to the Security Log for that domain controller and would prevent the AD Agent from learning about the mappings corresponding to some of the user logins that authenticate through that domain controller.

  For domain controller machines running Windows Server 2008 R2, the following Microsoft hotfix must be installed (unless SP1 is installed):

http://support.microsoft.com/kb/981314

This patch fixes a memory leak in Microsoft's WMI, which if left unfixed can sporadically prevent Active Directory from writing the necessary authentication-related events to the Security Log for that domain controller and would prevent the AD Agent from learning about the mappings corresponding to some of the user logins that authenticate through that domain controller.

- Similarly, each individual AD domain controller machine through which users will be authenticating during login and whose Security Log will be monitored by the AD Agent must have an "Audit Policy" (part of the "Group Policy Management" settings) that allows successful logons to generate the necessary events in the Windows Security Log of that domain controller machine. See "Configuring AD Agent to Obtain Information from AD Domain Controllers" section on page 2-9.
- Before you configure even a single domain controller machine using the **adacfg dc create** command, ensure that the AD Agent machine is first joined to a domain (for example, domain *J*) that has a trust relationship with each and every domain (for example, domain *D[i]*) that it will monitor for user authentications (through the domain controller machines that you will be configuring on the AD Agent machine).

  Depending on your Active Directory domain structure, the following scenarios are possible:

  1. Single Forest, Single Domain—There is only one domain, *D[i]* for all domain controller machines, which is one and the same as domain *J*. The AD Agent machine must first be joined to this single domain, and since no other domains are involved, there is no need to configure any trust relationship with any other domain.
  2. Single Forest, Multiple Domains—All the domains in a single forest already have an inherent two-way trust relationship with each other. Thus, the AD Agent must first be joined to one of the domains, *J*, in this forest, with this domain *J* not necessarily being identical to any of the domains *D[i]* corresponding to the domain controller machines. Because of the inherent trust relationship between domain *J* and each of the domains *D[i]*, there is no need to explicitly configure any trust relationships.
  3. Multiple Forests, Multiple Domains—It is possible that domain *J* might belong to a forest that is different than the forest to which one or more of the domains *D[i]* corresponding to the domain controller machines belong. In this case, you must explicitly ensure that each of the domains *D[i]* has an effective trust relationship with domain *J*, in at least one of the following two ways:

     a. A two-way external trust relationship can be established between the two domains, *D[i]* and *J*

     b. A two-way forest trust relationship can be established between the the forest corresponding to domain *D[i]* and the forest corresponding to domain *J*

  To configure trust relationships, choose **Start > All Programs > Administrative Tools > Active Directory Domains and Trusts**.

Note If you ignore this requirement, and the AD Agent machine is not joined to a domain that has the necessary trust relationship with the domain associated with a particular DC machine, then your attempts to configure that DC machine, using the **adacfg dc create** command might appear to succeed. However, that DC machine might begin to have various problems, such as an extremely high CPU loading.

Installing Active Directory Agent

To install Active Directory Agent, complete the following steps:

Step 1 Copy the Active Directory Agent installer executable file to the Windows machine where you are going to install the Active Directory Agent.

Step 2 Run the **AD_Agent-v1.0.0.32-build-539.Installer.exe** file.

The Cisco AD Agent Setup dialog box appears.

Step 3 Click **Yes** to proceed with the installation.

The installer will install the AD Agent in the C:\IBF\ directory of your Windows machine. You can view the progress of the installation procedure. If the installation was successful, you will see a Completed message.

Step 4 Click **Close** to close the installer.

Confirming Active Directory Agent Installation

To confirm if the Active Directory Agent is running after installation, complete the following steps:

Step 1 Go to the Windows Command Line Prompt (**Start > All Programs > Accessories > Command Prompt**).

Step 2 Type **cd C:\IBF\CLI**.

Step 3 Type **adactrl.exe show running**.

You will see an output similar to the following:

```
running C:\\IBF\\watchdog\\radiusServer.bat since 2010-12-27 T15:32:31
running C:\\IBF\\watchdog\\adObserver.bat since 2010-12-27 T15:32:38
```

This output provides information on the date and time from which the AD Agent internal processes are running on this machine.

Uninstalling Active Directory Agent

To uninstall the Active Directory Agent, complete the following steps:

Step 1 Go to the C:\IBF\ folder.

The Active Directory Agent is by default installed in the C:\IBF\ directory of your Windows machine.

Step 2 Run the **AD_Agent.Uninstaller.exe** file.

The AD Agent is uninstalled.

Configuring Active Directory Agent

After you install the AD Agent, you must first ensure that if any firewall such as Windows Firewall is running on the AD Agent machine, then the necessary exceptions are configured on the AD Agent machine as described in "Windows Firewall Exceptions to be Configured on the AD Agent Machine" section on page 2-3. Then, you must configure the AD Agent with:

- Each individual Active Directory domain controller machine through which users will be authenticating during their logins, and whose Security Log will be monitored by the AD Agent to learn of new mappings through that particular domain controller.

Note You must also include any backup domain controller machines that you are deploying.

- Client devices, such as ASA devices, that have been properly configured to obtain the IP-to-user-identity mappings from the AD Agent machine.

You can also configure AD Agent to send logs to a syslog server.

Note If you configure the AD Agent with a syslog server first before you configure the AD domain controllers and client devices, then troubleshooting information will also be available in the syslog server in addition to the localStore. Having this troubleshooting information in the syslog server might be helpful in case you run into any issues during the setup process.

After you install the AD Agent, wait for a short while (about 30 seconds) for the AD Agent to properly initialize before you issue any of the adacfg commands.

- If you issue any of the adacfg commands when the AD Agent is not running, you will see the following message:

```
Error: HTTP request sending failed with error "Couldn't connect to server"! For
further syntax information, use adacfg help.
```

- If you issue any of the adacfg commands before the AD Agent has fully initialized, you will see the following message:

```
Caught exception: Module PipConfigurator not initialized!
```

This section contains the following topics:

- Configuring AD Agent to Send Logs to a Syslog Server, page 2-9
- Configuring AD Agent to Obtain Information from AD Domain Controllers, page 2-9
- Configuring AD Agent to Allow Client Devices to Obtain Information from AD Agent, page 2-11

Note This section only describes the configuration that you should perform on the AD Agent. For a solution to work properly, you must configure the AD Agent and AD domain controllers in the client devices as well. Refer to the *ASA End-User Documentation* for more information.

Configuring AD Agent to Send Logs to a Syslog Server

You can configure the AD Agent to send logs to a syslog server for administrative purposes and also for obtaining troubleshooting information.

To configure AD Agent to send logs to a syslog server, complete the following steps:

Step 1 Log into your AD Agent Windows machine.

Step 2 From the command line prompt, type cd **C:\IBF\CLI**.

Step 3 Enter the following command:

adacfg syslog create -name <*syslog-target-nickname*> **-ip** <*IP-address*> [**-facility** <*syslog-facility*>]

where

- *syslog-target-nickname* is a friendly name that you assign to the syslog server.
- *IP-address* is the IP address of the syslog server.
- *syslog-facility* values range from LOCAL0 through LOCAL7. The default is LOCAL6.

You will see the following message:

```
Reply: Command completed successfully.
```

Configuring AD Agent to Obtain Information from AD Domain Controllers

Each individual Active Directory domain controller machine through which users will be authenticating during their logins must be separately configured on the AD Agent, so that the AD Agent will be able to learn new IP-to-user-identity mappings from that particular domain controller by monitoring its Security Log.

Note You must include any backup domain controller machines that you are deploying.

To configure AD Agent to obtain information from a particular AD domain controller machine, complete the following steps:

Step 1 Ensure that the AD domain controller machine is running a supported version of the Windows Server operating system, as described in "Active Directory Requirements" section on page 2-5.

Step 2 Ensure that if the AD domain controller machine is running Windows Server 2008 or Windows Server 2008 R2, then the appropriate Microsoft hotfixes are installed on that machine, as described in "Active Directory Requirements" section on page 2-5. There should be no AD domain controller machine running Windows Server 2008 or 2008 R2 without the specified hotfixes.

Step 3 Ensure that if any firewall software, such as Windows Firewall, is enabled on the AD domain controller machine, then the necessary firewall exceptions are defined on the AD domain controller machine, as described in "Windows Firewall Exceptions to be Configured on Each Separate Active Directory Domain Controller Machine" section on page 2-4.

Step 4 Ensure that the domain associated with the domain controller machine has the proper trust relationship with the domain to which the AD Agent machine is joined.

Step 5 Ensure that the “Audit Policy” (part of the "Group Policy Management" settings) allows successful logons to generate the necessary events in the Windows Security Log of that AD domain controller machine (this is normally the Windows default setting, but you must explicitly ensure that this setting is correct). To do this, choose **Start > Programs > Administrative Tools > Group Policy Management**. From the navigation pane on the left of Group Policy Management:

a. Navigate under **Domains** to the relevant domain(s).

b. Expand the navigation tree.

c. Right-click **Default Domain Policy**.

d. Choose the **Edit** menu item, which will bring up the Group Policy Management Editor.

e. From the navigation pane on the left of Group Policy Management Editor:

f. Choose **Default Domain Policy > Computer Configuration > Policies > Windows Settings > Security Settings**.

- For Windows Server 2003 or Windows Server 2008 (non-R2), choose **Local Policies > Audit Policy**. For the two Policy items, **Audit Account Logon Events** and **Audit Logon Events**, ensure that the corresponding **Policy Setting** for each of these either directly or indirectly includes the **Success** condition. To include the **Success** condition indirectly, the Policy Setting must be set to **Not Defined**, indicating that the effective value will be inherited from a higher level domain, and the Policy Setting for that higher level domain must be configured to explicitly include the **Success** condition.
- For Windows Server 2008 R2, choose **Advanced Audit Policy Configuration > Audit Policies > Account Logon**. For the two Policy items, **Audit Kerberos Authentication Service** and **Audit Kerberos Service Ticket Operations**, ensure that the corresponding **Policy Setting** for each of these either directly or indirectly includes the **Success** condition as described above.

g. If any **Audit Policy** item settings have been changed, you should then run “**gpupdate /force**” to force the new settings to take effect.

Step 6 Log into your AD Agent Windows machine.

Step 7 From the command line prompt, type cd **C:\IBF\CLI**.

Step 8 Enter the following command:

adacfg dc create -name <*DC-nickname*> **-host** <*DC-hostname-or-FQDN*> **-domain** <*full-DNS-name-of-AD-domain*> **-user** <*username-member-of-Domain-Admins-group*> **-password** <*password-of-user*>

where

- *DC-nickname* is a friendly name that you assign to the domain controller.
- *DC-hostname-or-FQDN* is the hostname or the fully qualified domain name of the AD domain controller machine to be monitored by the AD Agent.
- *full-DNS-name-of-AD-domain* is the full DNS name of the AD domain.
- *username-member-of-Domain-Admins-group* is the username of an existing account through which the security log of the domain controller machine will be monitored.

  This account must have the necessary privileges for reading the Security Log of the domain controller machine. You can easily and conveniently ensure this by specifying an account that belongs to the “Domain Admins” AD group for the domain specified with the “-domain” option.

  Alternatively, it is possible for nonmembers of the “Domain Admins” group to have the necessary privileges by satisfying all of the following requirements:

  - The account must belong to the “Distributed COM Users” AD group.

  - The account must have permission to access WMI namespaces (in particular, the "CIMV2" namespace) on the domain controller machine. You can configure this permission using the 'wmimgmt.msc' snap-in, or through Group Policy (to affect all domain controller machines). See http://blogs.msdn.com/b/spatdsg/archive/2007/11/21/set-wmi-namespace-security-via-gpo-script.aspx for more information.
  - The account must have permission to read the Security Event Log on the domain controller machine. You can configure this permission by setting the CustomSD key in the registry, or through the Group Policy (to affect all domain controller machines). See http://msdn.microsoft.com/en-us/library/aa363648%28v=vs.85%29.aspx for more information.

- *password-of-user* is the password corresponding to the username specified above.

You will see the following message:

```
Reply: Command completed successfully.
```

You can use the **adacfg dc list** command to view a list of the currently configured AD domain controller machines and their up or down status. You can periodically reenter this command to recheck the status of the AD domain controller machines.

After you run the **adacfg dc create** command for a particular AD domain controller, you must wait a short while (for about a minute or so), until the status of that AD domain controller changes from its initial "down" state to "up" or "down(no-retry)."

- The "up" state indicates that connectivity with that AD domain controller has been established. You might need to wait several more minutes (or even longer) from the time that a particular AD domain controller machine has reached the "up" state for the first time ever to the time that any historical mappings are retrieved from that machine and become visible through the **adacfg cache list** command.
- The "down(no-retry)" state indicates that connectivity could not be established (for example, due to incorrect credentials) and that the AD Agent will not re-attempt to establish connectivity.
- On the other hand, the "down" state indicates that currently the AD Agent does not have connectivity with that particular AD domain controller machine, but it will periodically re-attempt to establish connectivity.

You can also use the **adacfg dc erase** command to remove any domain controller configuration from the AD Agent.

See "adacfg dc list" section on page A-8, "adacfg cache list" section on page A-9, and "adacfg dc erase" section on page A-8 for more information on these commands.

Configuring AD Agent to Allow Client Devices to Obtain Information from AD Agent

You must configure the AD Agent with each individual client device (such as ASA) for the AD Agent to respond to requests from that particular client device to receive mapping information from this AD Agent.

Note A single AD Agent can support a maximum of 100 client devices (such as ASA devices).

To configure AD Agent to communicate with a particular client device, complete the following steps:

Step 1 Log into your AD Agent Windows machine.

Step 2 From the command line prompt, type cd **C:\IBF\CLI**.

Step 3 Enter the following command:

adacfg client create -name <*client-nickname*> **-ip** <*IP-address*>*[/*<*prefix-length-for-IP-range*>*]* **-secret** <*RADIUS-shared-secret*>

where

- *client-nickname* is a friendly name that you assign to the particular client device.
- *IP-address/*<*prefix-length-for-IP-range*> refers to the IP address of the particular client device and you can optionally define a subnet range.
- *RADIUS-shared-secret* is the shared secret that the RADIUS protocol uses for communication. This *secret* is the key that is configured on the particular client device.

Note Ensure that you enter the correct RADIUS-shared-secret. Otherwise, requests from that particular client device will be ignored.

You will see the following message:

```
Reply: Command completed successfully!
```

You can use the **adacfg client list** command to view a list of currently configured client devices and the **adacfg client erase** command to remove any client device configuration from the AD Agent. See "adacfg client list" section on page A-5 and "adacfg client erase" section on page A-5 for more information on these commands.

Step 4 Follow the instructions provided with the particular client device to configure the client device to recognize this AD Agent machine.