



The User Agent Configuration Process

To use Version 2.3 of the user agent to collect user login data from up to five Microsoft Active Directory servers and send it to Management Centers, you must install it, connect it to each Management Center and Microsoft Active Directory server, and configure general settings. For more information, see the following sections:

- [Set Up a User Agent, page 2-1](#)
- [Management Center Configurations, page 2-3](#)
- [Configure the Active Directory Server, page 2-4](#)
- [Configure the User Agent Computer, page 2-6](#)
- [Install the User Agent, page 2-18](#)
- [Configure the User Agent, page 2-20](#)
- [Troubleshoot the User Agent, page 2-31](#)

Set Up a User Agent

Setting up a user agent is a multi-step configuration.

To set up a user agent:

Access: Admin

-
- Step 1** Configure each Management Center to do the following:
- Allow agent connections from the IP address of the server where you plan to install the agent.
 - Configure and enable the Active Directory object or realm. The terminology used to describe the object depends on your Management Center version; for more information, see one of the following sections:
 - [Configure a Version 5.x Defense Center to Connect to User Agents, page 2-3](#)
 - [Configure a Version 6.x Management Center to Connect to User Agents, page 2-3](#)
- Step 2** Configure the Active Directory server to log events for the user agent to communicate to the Management Center. For more information, see [Configure the Active Directory Server, page 2-4](#).
- Step 3** Configure each computer on the domain to allow Windows Management Instrumentation (WMI) through the firewall for the domain. For more information, see [Configure Domain Computers, page 2-6](#).

- Step 4** Install the prerequisite programs on the computer where you will install the agent. Set up the computer's TCP/IP access to the Active Directory server. For more information, see [Prepare the Computer for User Agent Installation, page 2-6](#).
- Step 5** If you have a previous user agent installation, optionally back up the agent database to retain configuration settings. For more information, see [Back Up User Agent Configurations, page 2-17](#).
- Step 6** Configure permissions necessary to allow the agent to connect to an Active Directory server. For more information, see:
- [Give Limited Privileges to a Domain User \(Summary\), page 2-8](#)
 - [Give Privileges to a Local User, page 2-8](#)
- Step 7** Install the agent on the computer.
- For more information, see [Install the User Agent, page 2-18](#).
 - To optionally install more than one user agent, see [Deploy Multiple User Agents, page 1-6](#).
- Step 8** Configure connections to one or more Microsoft Active Directory servers.
- Step 9** (Optional.) Configure a polling interval and maximum poll length for the agent. For more information, see [Configure User Agent Active Directory Server Connections, page 2-21](#).
- Step 10** Configure connections to up to five Management Centers. For more information, see [Configure User Agent Management Center Connections, page 2-24](#).
- Step 11** (Optional.) Configure a list of user names and IP addresses to exclude from polling for login and logoff data. For more information, see:
- [Configure User Agent Excluded Username Settings, page 2-25](#)
 - [Configure User Agent Excluded Addresses Settings, page 2-26](#)
- Step 12** (Optional.) Configure the agent logging settings. For more information, see [Configure User Agent Logging Settings, page 2-27](#).
- Step 13** (Optional.) Configure the agent name, start and stop the service, and view the service's current status. For more information, see [Configure General User Agent Settings, page 2-29](#).
- Step 14** Click **Save** to save the user agent configuration.

**Caution**

Do *not* modify the user agent maintenance settings unless Cisco TAC directs you to do so.

Management Center Configurations

This section discusses how to prepare the Management Center to receive user data from the user agent.

Configure a Version 5.x Defense Center to Connect to User Agents

If you plan to use Version 2.3 of the user agent to send LDAP login data to your Version 5.x Defense Centers, you must configure all of the following:

- Configure each Defense Center to allow connections from the agents you plan to connect to your Active Directory servers. That connection allows the agent to establish a secure connection with the Defense Center, over which it can send data.

For more information about establishing this connection, see *Using User Agents to Report Active Directory Logins* in the Version 5.x *FireSIGHT System User Guide*.

- To implement user access control, you must configure and enable a connection between the Defense Center and at least one of your organization's Microsoft Active Directory servers. In Version 5.x, this is called an *LDAP connection* or a *user awareness object*.

This configuration contains connection settings and authentication filter settings for the server. The connection's user and group access control parameters specify the users and groups you can use in access control rules. For more information about this configuration, see *Connecting to an LDAP Server for User Awareness and Control* in the Version 5.x *FireSIGHT System User Guide*.

Configure a Version 6.x Management Center to Connect to User Agents

To use Version 2.3 of the user agent to send login data to your Version 6.x Management Centers, you must configure all of the following:

- Configure each Management Center to allow connections from the agents you plan to connect to your servers. That connection allows the agent to establish a secure connection with the Management Center, over which it can send data.

For more information about establishing this connection, see *Configuring a User Agent Connection* in the Version 6.x *Firepower Management Center Configuration Guide*.

- To implement user access control, you must configure and enable a connection between the Management Center and at least one of your organization's Microsoft Active Directory servers. In Version 6.x, this is called a *realm*.

Realms contain connection settings and authentication filter settings for servers. The connection's user download settings specify the users and groups you can use in access control rules. For more information about this configuration, see *Creating a Realm* in the Version 6.x *Firepower Management Center Configuration Guide*.

Configure the Active Directory Server

This section discusses how to verify that the Active Directory security logs are enabled so the Active Directory server can record login data to these logs.

Configure the Active Directory Server for Logging

To verify the Active Directory server is logging login data:

-
- Step 1** On the Active Directory server, click **Start > [All Programs] > Administrative Tools > Event Viewer**.
 - Step 2** Click **Windows Logs > Security**.
If logging is enabled, the Security log is displayed. If logging is disabled, see [How to configure Active Directory and LDS diagnostic event logging](#) on MSDN for information on enabling security logging.
 - Step 3** Allow WMI through the firewall on the Active Directory server. If the Active Directory server is running Windows Server 2008 or Windows Server 2012, see [Setting up a Remote WMI Connection](#) on MSDN or more information.
-

To enable auditing of logon/logoff events on Windows 2012 Server:

-
- Step 1** Click **Start > Administrative Tools > Group Policy Management**.
 - Step 2** In the navigation pane, expand **Forest: *YourForestName***, expand **Domains > *YourDomainName* > Group Policy Objects**.
 - Step 3** Right-click **Default Domain Policy** and click **Edit**.
 - Step 4** Browse to **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Logon/Logoff**.
 - Step 5** In the right pane, double-click **Audit Logoff**.
 - Step 6** In the Edit Logoff Properties dialog box, check **Configure the following audit events** and **Success**.
 - Step 7** Click **OK**.
 - Step 8** Repeat the same task for **Audit Logon**.
-



Note The user agent does not report logoff events identified by Windows Security Log event 4634. The user agent uses a remote Windows Management Instrumentation (WMI) call to query domain computers for logoffs.

Enable Idle Session Timeouts

This section discusses how to optionally enable idle session timeouts in group policy. This helps prevent the agent from detecting and reporting extraneous logins due to multiple sessions on a host.

Terminal Services (Windows Server versions up to 2008) allows multiple users to log into a server at the same time. Enabling idle session timeouts helps reduce the instances of multiple sessions logged into a server.

Remote Desktop Services (Windows Server versions 2012 and later) allows one user at a time to remotely log into a workstation. However, if the user disconnects from the Remote Desktop session instead of logging out, the session remains active. Without user input, the active session eventually idles.

If another user logs into the workstation using Remote Desktop Services while one session is idle, it's possible that two logins are reported to the Management Center. Enabling idle session timeouts causes those sessions to terminate after the defined idle timeout period, which helps prevent multiple remote sessions on a host.

Citrix sessions function similarly to Remote Desktop Services sessions. Multiple Citrix user sessions can be running on a computer at once. Enabling idle session timeouts helps prevent multiple Citrix sessions on a host, reducing extraneous login reporting.

Note that depending on the configured session timeout, there might still be situations where multiple sessions are logged into a computer.

Enable Terminal Services Session Timeout

This section applies to Windows Server versions up to 2008.

To enable Terminal Services session timeout, update the group policy settings for idle Terminal Services session timeout and disconnected Terminal Services session timeout for Windows Server 2008 or Windows Server 2012, as discussed in [Configure Timeout and Reconnection Settings for Terminal Services Sessions](#) on Microsoft TechNet.

The paths in the Group Policy Object manager are:

```
Computer Configuration\Administrative Templates\Windows Components\Terminal  
Services\Terminal Server\Session Time Limits  
User Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal  
Server\Session Time Limits
```

Set session timeouts shorter than the user agent's logoff check frequency so idle and disconnected sessions have a chance to time out before the next logoff check. If you have a mandatory idle session or disconnected session timeout, set the user agent's logoff check frequency *longer than* the session timeout. For more information on configuring the logoff check frequency, see [Configure General User Agent Settings, page 2-29](#).

When you're done, continue with [Configure the User Agent Computer, page 2-6](#).

Enable Remote Desktop Session Timeout

This section applies to Windows Server versions 2012 and later.

To enable Remote Desktop session timeout, update the group policy settings for idle remote session timeout and disconnected session timeout. See [Session Time Limits](#) on Microsoft TechNet for more information on enabling the session timeouts.

Set Remote Desktop timeouts *shorter than* the user agent's logoff check frequency so idle and disconnected sessions have a chance to time out before the next logoff check. If you have a mandatory idle session or disconnected session timeout, set the user agent's logoff check frequency *longer than* the Remote Desktop timeout. For more information on configuring the logoff check frequency, see [Configure General User Agent Settings, page 2-29](#).

The path in the Group Policy Object editor is:

User Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits

When you're done, continue with [Configure the User Agent Computer, page 2-6](#).

Enable Citrix Session Timeout

To enable Citrix session timeout, consult Citrix's documentation at <http://support.citrix.com/>

Configure Domain Computers

To enable the user agent to send logoff events to the Management Center, you must allow WMI traffic through the firewall on every computer that connects to the domain.

You have the following options:

- Use the Windows firewall to [allow WMI](#) for the domain.
- Configure firewall policies using Group Policy Object (GPO) as discussed in a resource such as [Windows Firewall with Advanced Security Deployment Guide](#) on Microsoft TechNet.

Configure the User Agent Computer

After you have prepared the Management Center and the Active Directory server, prepare the computer on which you will install and configure the agent.

Prepare the Computer for User Agent Installation

You can install the user agent on a Windows computer that meets the requirements discussed in this section.

Computer Configurations

The computer can be any of the following:

- (Recommended.) A computer on a trusted network that can access the Active Directory server. This computer should be available only to network administrators.
We recommend this installation method because it's the most secure.
- The Active Directory server.

Prerequisites for Installing the User Agent

The Windows computer must meet the following prerequisites:

- The computer is running Windows Vista, Windows 7, Windows 8, Windows Server 2008, or Windows Server 2012. For security reasons, we recommend you install the user agent on a domain computer and *not* on the Active Directory server computer.
- The computer has Microsoft .NET Framework Version 4.0 Client Profile and Microsoft SQL Server Compact (SQL CE) Version 3.5 installed.
 - The [Microsoft .NET Framework Version 4.0 Client Profile redistributable package](#) is available from the Microsoft download site (`dotNetFx40_Client_x86_x64.exe`).
 - [SQL Server Compact 3.5](#) is available from the Microsoft download site (`SSCERuntime-ENU.exe`).

**Note**

If you do not have the .NET Framework, when you start the agent executable file (`setup.exe`), it prompts you to download it. See [Install the User Agent, page 2-18](#) for more information.

- Create a user to run the user agent as discussed in [Create a User for the User Agent, page 2-7](#).
- The computer has TCP/IP access to the Active Directory servers you want to monitor, and uses the same version of the Internet Protocol as the Active Directory servers. If the agent is monitoring the Active Directory servers real time, the computer's TCP/IP access must be on at all times to retrieve login data.

**Note**

If you install the user agent on Windows Server 2003 or an older operating system, the user agent cannot collect real time statistics from an Active Directory computer.

- The computer has TCP/IP access to the Management Centers where you want to report data and an IPv4 address.
- The computer has an IPv6 address, to detect logoffs from hosts with IPv6 addresses, or an IPv4 address, to detect logoffs from hosts with IPv4 addresses.
- The computer does not have a legacy agent or Version 2.x agent already installed. Because these agents do not automatically uninstall, to uninstall an existing agent, use **Add/Remove Programs** in the Windows Control Panel.

**Caution**

If you have a previous version of the user agent installed, you must back up the database to retain configuration settings.

Continue with [Create a User for the User Agent, page 2-7](#).

Create a User for the User Agent

To be able to run the user agent with the minimum necessary permissions, you must create a user account for the user agent:

- If you're upgrading an older version of the user agent, this step isn't necessary.
In that case, see [Back Up User Agent Configurations, page 2-17](#).
- To run the user agent on a computer separate from the Active Directory server, the user must be a domain user.
- To run the user agent on the Active Directory server, the user should be a local account.

To create a user:

-
- Step 1** Log in to the Active Directory server as a member of the Domain Admins group.
- Step 2** To run the user agent on the Active Directory server, create a local user account. (This account must be in the Domain Admins group but the user does not need to be in the Administrators group.)
Skip the remaining steps in this section and continue with [Give the User Privileges, page 2-8](#).
- Step 3** To create a domain user so you can run the user agent on a separate computer, click **Start > Active Directory Users and Computers**.
- Step 4** In the left pane, expand the domain and folder in which to add the user.
- Step 5** Right-click the folder in which to add the user.
- Step 6** From the pop-up menu, click **New > User**.
- Step 7** Follow the prompts on your screen to create the domain user and to give the user a strong password.

**Caution**

For security reasons, make sure this user account is known only to network administrators.

Give the User Privileges

This section discusses the following possibilities:

- Adding a local user to the Domain Admins group on the Active Directory server.
This method is easy but it's not recommended because it's less secure. See [Give Privileges to a Local User, page 2-8](#).
- Giving a domain user minimal privileges to run the user agent. See [Give Limited Privileges to a Domain User \(Summary\), page 2-8](#).

Give Privileges to a Local User

To run the user agent on the Active Directory server, you must add the user to the Domain Admins group. To make the user agent easier to install, you can optionally add it to the Administrators group as well.

Give Limited Privileges to a Domain User (Summary)

This section provides a summary of the tasks required to give a domain user minimal privileges to run the user agent. For an example, see [Give Limited Privileges to a Domain User \(Step-by-Step Example\), page 2-9](#).

To give a domain user limited privileges:

-
- Step 1** Log in to the Active Directory server as a member of the Domain Admins group.
- Step 2** Add the user agent user to the following groups:
- **Distributed COM Users**
 - **Event Log Readers**

- Step 3** Use the Windows Management Instrumentation (WMI) Control console to give the user the following permissions to the `Root\CIMV2` node as discussed on [Microsoft TechNet](#):
- **Execute Methods**
 - **Enable Account**
 - **Remote Enable**
 - **Read Security**
- Step 4** Enable the user agent to use real time processing of the Active Directory server.
- Create a Group Policy Object (GPO) security policy for the Windows firewall rule to allow inbound network traffic to Remote Procedure Call (RPC) Endpoint Mapper service as discussed on [Microsoft TechNet](#).
 - Create a GPO security policy for the Windows firewall rule to allow inbound traffic on random RPC ports as discussed on [Microsoft TechNet](#).
- For more information about real time processing, see [Configure User Agent Active Directory Server Connections, page 2-21](#).
- Step 5** Update your Group Policy Object (GPO) policies using the `gupdate /force` command or an equivalent method.
-

Give Limited Privileges to a Domain User (Step-by-Step Example)

This section provides a step-by-step example of giving a domain user minimal privileges to run the user agent.

To follow the procedure in this section, we assume your system uses:

- Windows Server 2012
- User agent user name is `limited.ua`
- Domain name is `sesame.example.com`
- User agent connects to one Active Directory server and one Firepower Management Center
- User agent processes events from the Active Directory server in real time

Give the User Windows Management Instrumentation (WMI) Permissions

This section discusses how to give the domain user WMI privileges to the `Root > CIMV2` node on the Active Directory server so the user can retrieve logoff events from domain computers.

To give a domain user WMI permissions:

-
- Step 1** Log in to the Active Directory server as a member of the Domain Admins group.
- Step 2** Add the user agent user to the following groups:
- **Distributed COM Users**
 - **Event Log Readers**
- Step 3** Click **Start** and enter `wmicmgmt.msc`.
- Step 4** Right-click **Console Root > WMI Control (Local)** and click **Properties**.
- Step 5** In the WMI Control (Local) Properties dialog box, click the **Security** tab.

- Step 6** Click **Root > CIMV2**.
- Step 7** Click **Security**.
- Step 8** In the Security for ROOT\CIMV2 dialog box, click **Add**.
- Step 9** In the **Enter object names to select** field, enter `limited.ua` and click **Check Names**.
Windows locates the user name and displays it in the field.
- Step 10** Click **OK**.
- Step 11** Give the user the following permissions:
- **Execute Methods**
 - **Enable Account**
 - **Remote Enable**
 - **Read Security**
- Step 12** In the Security for Root\CIMV2 dialog box, click **OK**.
- Step 13** In the WMI Control Properties dialog box, click **OK**.
-

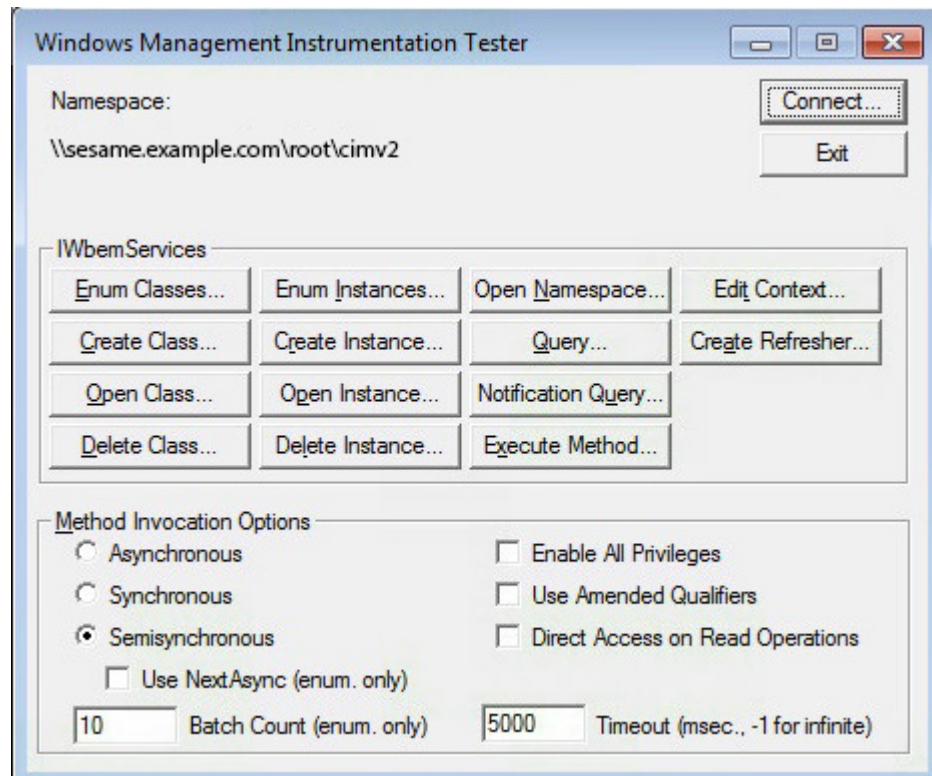
Test WMI Permissions

After giving the user agent user WMI permissions on the Active Directory server, you should test the permissions from the computer on which you will install the user agent.

To test WMI permissions:

-
- Step 1** Log in to the domain computer on which you'll install the user agent.
- Step 2** In the search field, enter `wbemtest`. (In some versions of Windows, you must click **Start** first.)
- Step 3** In the Windows Management Instrumentation Tester dialog box, click **Connect**.
- Step 4** In the Connect dialog box, enter the following information:
- **Namespace** field: Enter the name of the Active Directory server and path using the format: `\\namespace\root\cimv2`. In this example, enter `\\sesame.example.com\root\cimv2`
 - **Credentials** field: Enter the user name in the format `domain\username` in the **User** field and the user's password in the **Password** field. In this example, the user name is `sesame\limited.ua`
 - There is typically no need to change the other options in this dialog box.
- Step 5** Click **Connect**.

If the connection is successful, the Windows Management Instrumentation Tester dialog box is displayed as follows.



If errors are displayed, try the following:

- The RPC server is unavailable indicates either a bad namespace or the Active Directory server is inaccessible (network problems, server is down, and so on).
- Access is denied indicates a bad user name or password.

Step 6 If the test is successful, click **Query**.

Step 7 In the Query dialog box, enter the following:

```
select * from Win32_NTLogEvent where Logfile = 'Security' and (EventCode=672 or
EventCode=4768 or EventCode=538 or EventCode=4364 or EventCode=528 or EventCode=4624 or
EventCode=4634) and TimeGenerated > "date-code"
date-code is a Microsoft time and date code in the format
YYYYMMDDHHMMSS.fractionalSecond-utc_timezone_offset
```

For example, to query from May 1, 2017 at midnight in the US Central time zone (UTC - 6 hours), enter the following:

```
select * from Win32_NTLogEvent where Logfile = 'Security' and (EventCode=672 or
EventCode=4768 or EventCode=538 or EventCode=4364 or EventCode=528 or EventCode=4624 or
EventCode=4634) and TimeGenerated > "20170501000000.000000-600"
```

Step 8 From the **Query Type** list, click **WQL**.

Step 9 Click **Apply**.

The query is displayed in a new dialog box.

If the errors `Invalid class` or `Invalid query` are displayed, check the command syntax and try again. If no results are displayed, check your date code.

Step 10 When you're finished viewing the logs, click **Close**.

Step 11 In the Windows Management Instrumentation Tester dialog box, click **Exit**.

Allow the User Agent to Access Distributed Component Object Management (DCOM)

This section discusses how to allow DCOM access so the user agent can remotely access objects on the Active Directory server.

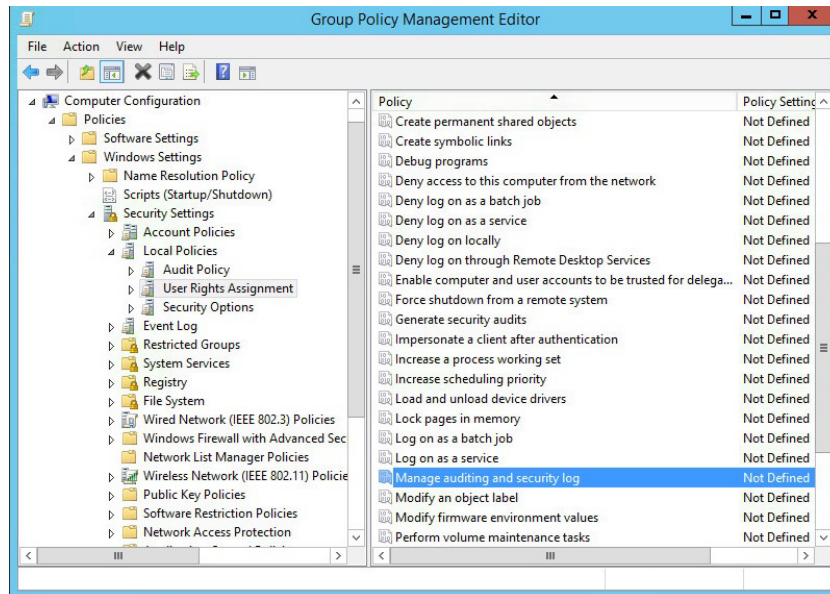
To give the user DCOM access:

- Step 1** Log in to the Active Directory server as member of the Domain Admins group.
 - Step 2** Click **Start** > **[Run]**, and enter `dcomcnfg`, then press Enter.
 - Step 3** In the Component Services window, click **Component Services** > **Computers**.
 - Step 4** Right-click **My Computer** and click **Properties**.
 - Step 5** In the My Computer Properties dialog box, click the **COM Security** tab.
 - Step 6** Under Launch and Activation Permissions, click **Edit Limits**.
 - Step 7** In the Launch and Activation Permissions dialog box, click **Add**.
 - Step 8** In the **Enter the object names to select** field, enter `limited.ua` and click **Check Names**.
 - Step 9** If the name matches, click **OK**.
 - Step 10** Grant the user the **Remote Launch** and **Remote Activation** permissions.
 - Step 11** In the Launch and Activation Permissions dialog box, click **OK**.
 - Step 12** In the My Computer Properties dialog box, click **OK**.
-

To update Group Object Policy to allow access to the Active Directory security log:

- Step 1** Click **Start** > **[All Programs]** > **Administrative Tools** > **Group Policy Management**.
- Step 2** In the navigation pane, expand **Forest: *YourForestName***, expand **Domains** > ***YourDomainName*** > **Group Policy Objects**.
- Step 3** Right-click **Default Domain Policy** and click **Edit**.
- Step 4** Browse to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**.
- Step 5** In the right pane, double-click **Manage auditing and security log**.

The following figure shows an example.



- Step 6** Check **Define these policy settings**.
- Step 7** Click **Add User or Group**.
- Step 8** In the User and group names field, either enter the user agent user name or click **Browse** to locate it.
- Step 9** In the Manage auditing and security log Properties dialog box, click **OK**.

Create Group Policy Object Rules for the Windows Firewall

This section is required for the user agent to use real time event processing for the Active Directory server. For more information about real time event processing, see [Configure User Agent Active Directory Server Connections](#), page 2-21.

To allow inbound remote procedure call (RPC) network traffic, use the Windows Firewall with Advanced Security node in Group Policy Management to create two firewall rules:

- The first rule allows incoming traffic to the RPC Endpoint Mapper service, which responds with a dynamically assigned port number that the client must use to communicate with the service.
- The second rule allows network traffic that is sent to the dynamically assigned port number.

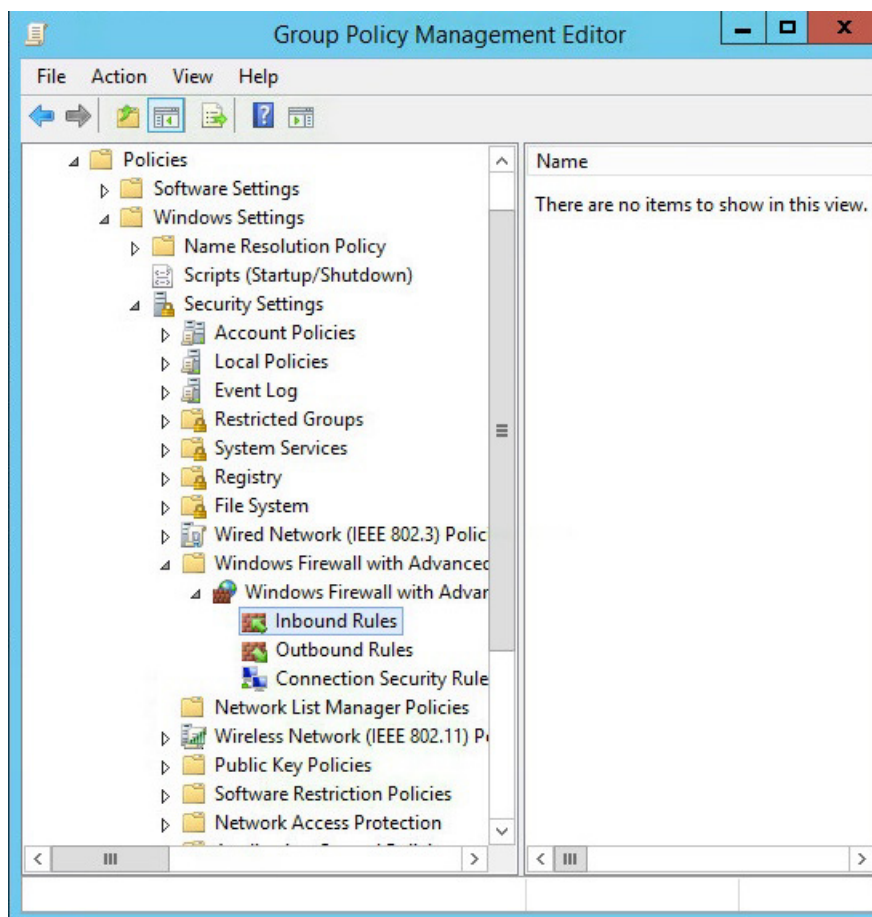
Using the two rules helps to protect your computer by allowing network traffic only from computers that have received RPC dynamic port redirection and to only those port numbers assigned by the RPC Endpoint Mapper.

Perform the tasks discussed in the following procedures on every Active Directory server to which the user agent requires access.

To create a GPO firewall rule to allow RPC traffic:

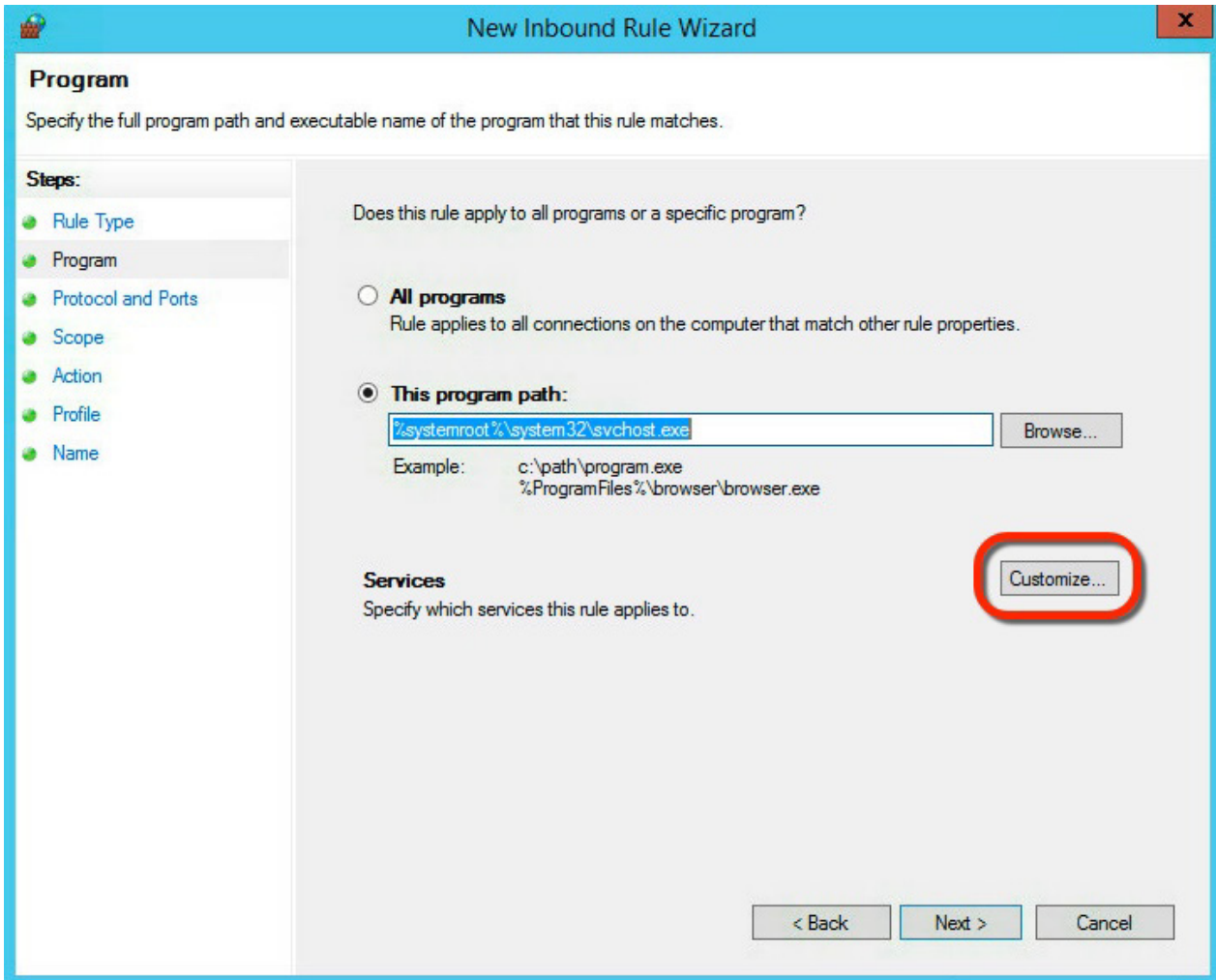
- Step 1** If you haven't done so already, log in to your Active Directory server as a member of the Domain Admins group.
- Step 2** Choose **Start > Administrative Tools**.
- Step 3** In the Administrative Tools window, double-click **Group Policy Management**.
- Step 4** In the navigation pane, expand **Forest: YourForestName**, expand **Domains, > YourDomainName > Group Policy Objects**, right-click the GPO you want to modify, and then click **Edit**.
Typically, you should edit the **Default Domain Policy**.
- Step 5** In the left pane, expand **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security**.

The following figure shows an example.



- Step 6** Right-click **Inbound Rules** and click **New Rule**.
- Step 7** In the New Inbound Rule Wizard dialog box, click **Custom** and click **Next**.
- Step 8** Click **This program path**, and then enter `%systemroot%\system32\svchost.exe`
- Step 9** Next to Services, click **Customize**.

The following figure shows an example.



- Step 10** In the Customize Service Settings dialog box, click **Apply to this service**, select **Remote Procedure Call (RPC)** with a short name of **RpcSs**, and click **OK**.
- Step 11** Click **Next**. You are required to confirm the action.
- Step 12** On the Protocol and Ports dialog box, for **Protocol type**, click **TCP**.
- Step 13** For **Local port**, choose **RPC Endpoint Mapper**, and then click **Next**.
- Step 14** On the Scope page, in the **Which remote IP addresses does this rule apply to?** section, choose **These IP addresses**, click **Add**, and enter the user agent computer's IP address.
- Step 15** Click **Next**.
- Step 16** On the Action page, select **Allow the connection**, and then click **Next**.
- Step 17** On the Profiles page, check only **Domain** and click **Next**.
- Step 18** On the Name page, enter a name to identify this rule and click **Finish**.

To create a GPO rule to allow dynamically-mapped ports:

-
- Step 1** Complete steps 1 through 4 in [Create Group Policy Object Rules for the Windows Firewall](#), page 2-13.
- Step 2** In the New Inbound Rule Wizard dialog box, click **Custom** and click **Next**.
- Step 3** Click **This program path**, and then enter `%systemroot%\system32\svchost.exe`
- Step 4** Next to Services, click **Customize**.
- Step 5** In the Customize Service Settings dialog box, click **Apply to this service**, select **Windows Event Log** with a short name of **EventLog**, and click **OK**.
- Step 6** Click **Next**. You are required to confirm the action.
- Step 7** On the Protocol and Ports dialog box, for **Protocol type**, click **TCP**.
- Step 8** For Local port, click **RPC Dynamic Ports**, and then click **Next**.
- Step 9** On the Scope page, click **These IP addresses**, click **Add**, and enter the user agent computer's IP address.
- Step 10** Click **Next**.
- Step 11** On the Action page, click **Allow the connection** and click **Next**.
- Step 12** On the Profiles page, check only **Domain** and click **Next**.
- Step 13** On the Name page, enter a name to identify this rule and click **Finish**.
-

To apply the GPO policies:

-
- Step 1** Apply the new GPO policies using the command `gpupdate /force` or an equivalent method. For more information about applying GPO policies, see the following references:
- [GPO Policy for Beginners on Microsoft TechNet](#)
 - [Policy Processing on Microsoft TechNet](#)


Note

You must run the `gpupdate /force` command using elevated permissions. Either log in to the Active Directory server as Administrator or run the command prompt as administrator. (Right-click the command prompt shortcut and click **Run as Administrator**.)





Back Up User Agent Configurations

If you have an earlier version of the user agent installed, installing a newer version of the user agent removes your existing configuration. To preserve these configuration settings, back up the database before installing the newer version of the user agent.

**Note**

If you have Version 2.2 or later of the user agent installed, you do not need to back up the database. Configuration settings are automatically imported when you install a newer version of the user agent. Continue with [Install the User Agent, page 2-18](#).

To retain your configuration settings:

-
- Step 1** On the computer where you installed the agent, click **Start > Programs > Cisco > Configure Cisco Firepower User Agent for Active Directory**.
- Step 2** Click the stop button () to stop the agent service.
- Step 3** Locate `CiscoUserAgent.sdf` on the computer where the agent is installed, and copy the file locally.
- 
- Note** If you are updating from Version 2.2 or before, locate and copy `SourcefireUserAgent.sdf`. Make copy of the file and rename the copy to `CiscoUserAgent.sdf`.
-
- Step 4** Uninstall the Cisco User Agent using the Control Panel's **Add/Remove Programs** option. Remove the agent.
- Step 5** Install the latest version of the user agent. See [Install the User Agent, page 2-18](#) for more information.
- Step 6** On the computer where the agent is installed, select **Start > Programs > Cisco > Configure Cisco Firepower User Agent for Active Directory**.
- Step 7** Click the stop button () to stop the agent service.
- Step 8** Locate `CiscoUserAgent.sdf` on the computer where the latest version of the agent is installed. Replace the current file with the local backup made from the previous version of the agent.
- Step 9** On the computer where the latest version of the agent is installed, select **Start > Programs > Cisco > Configure Cisco Firepower User Agent for Active Directory**.
- Step 10** Click  to start the service.
- Continue with [Install the User Agent, page 2-18](#).
-

Install the User Agent

License: FireSIGHT or N/A

After you configure permissions to connect to the Active Directory server, and after you configure idle remote session timeouts, install the agent.



Caution

If you have a previous version of the user agent installed, to retain configuration settings, you must complete a backup of the database before installation. For more information, see [Back Up User Agent Configurations](#), page 2-17.

By default, the agent runs as a service using the **Local System** account. If the Windows computer where the agent is running is connected to the network, the service continues to poll and send user data even if a user is not actively logged in to the computer.

For each agent, you can configure connections to one or more Active Directory servers and up to five Management Centers. Before you add a Management Center connection, make sure you add the agent to the Management Center configuration. For more information, see:

- [Configure a Version 5.x Defense Center to Connect to User Agents](#), page 2-3
- [Configure a Version 6.x Management Center to Connect to User Agents](#), page 2-3

For more information about deploying more than one user agent, see [Deploy Multiple User Agents](#), page 1-6.

In a high availability configuration, add both Management Centers to the agent to enable update of user login data to both the primary and the secondary so the data remains current on both.

To install the user agent:

Access: Any

- Step 1** Log in as the user you created in [Create a User for the User Agent](#), page 2-7 to the Windows computer on which to install the user agent:
- If you are upgrading an older version of the user agent, log in to the same computer.
 - (Recommended.) To install the user agent on a computer separate from the Active Directory server, log in to that computer.
 - To install the user agent on the Active Directory server, log in to the Active directory server as a member of the Domain Admins group, and, optionally the Administrators group.

- Step 2** Download the [User Agent setup file](#) (Cisco_Firepower_User_Agent_for_Active_Directory_2.3-10.zip) from the Support Site.



Note

Download the compressed archive containing the user agent setup files directly from the Support Site. Do not transfer the file over email because it might become corrupted.

- Step 3** Right-click the .zip file and choose **Extract All**.

- Step 4** Choose a folder in which to extract the files.

The agent requires 3 MB free on the hard drive for installation. We recommend you allocate 4 GB on the hard drive for the agent local database.

- Step 5** In the folder to which you extracted the files, double-click `setup.exe`.

**Note**

Double-click `setup.exe` and *not* `setup.msi`. `setup.msi` does not check for prerequisite software before installing the user agent, which could result in errors installing or running the agent.

**Tip**

If you are using an account that is not a member of the Administrators group and do not have permissions to install new applications on the Windows computer, you must elevate to a user that does belong to the Administrators group to have the appropriate permissions to start the installation. To access the escalation option, right click the `setup.exe` file and click **Run As**. Select an appropriate user and supply the password for that user.

- Step 6** You must accept the license agreements to continue the installation.
- Step 7** If you do not have the Microsoft .NET Framework Version 4.0 Client Profile and SQL Server Compact 3.5 on the Windows computer where you install the agent, you are prompted to download the appropriate files. Download and install the files.
- Step 8** Follow the prompts in the wizard to install the agent.
- If User Account Control is enabled on the computer, you must answer **Yes** to every prompt requesting permission to make changes.
- Step 9** To begin configuring the agent, see [Configure the User Agent, page 2-20](#).

Configure the User Agent

License: FireSIGHT or N/A

After the agent is installed, you can configure it to receive data from Active Directory servers, report the information to Management Centers, exclude specific user names and IP addresses from the reporting, and log status messages to a local event log or the Windows application log.

To configure the agent:

Access: Any

Step 1 On the computer where you installed the agent, select **Start > All Programs > Cisco > Configure Cisco Firepower User Agent for Active Directory**.

The following table describes the actions you can take when configuring the agent and where to configure them.

Table 2-1 *User Agent Configuration Actions*

To...	You can...
Change the agent name, change the logoff check frequency, start and stop the service, and set a scheduling priority	Click the General tab. See Configure General User Agent Settings, page 2-29 for more information.
Add, modify, or remove Active Directory servers, enable real time Active Directory server data retrieval, and modify the Active Directory server polling interval and maximum poll length	Click the Active Directory Servers tab. See Configure User Agent Active Directory Server Connections, page 2-21 for more information.
Add or remove Management Centers	Click the Firepower Management Centers tab. See Configure User Agent Management Center Connections, page 2-24 for more information.
Add, modify, or remove user names excluded from reporting	Click the Excluded Usernames tab. See Configure User Agent Excluded Username Settings, page 2-25 for more information.
Add, modify, or remove IP addresses excluded from reporting	Click the Excluded Addresses tab. See Configure User Agent Excluded Addresses Settings, page 2-26 for more information.
View, export, and clear the event log, log to Windows application logs, and modify how long messages should be kept	Click the Logs tab. See Configure User Agent Logging Settings, page 2-27 for more information.
Perform troubleshooting and maintenance tasks, as directed by Cisco TAC	Click the Logs tab, enable Show Debug Messages in Log , then select the Maintenance tab. See Configure User Agent Maintenance Settings, page 2-30 for more information.
Save changes to the agent settings	Click Save . A message is displayed informing you when you have unsaved changes.
Close the agent without saving changes to the agent settings	Click Cancel .

Configure User Agent Active Directory Server Connections

License: FireSIGHT or N/A

You can add connections to one or more Active Directory servers from a user agent, and configure the following:

- Whether the agent retrieves login and logoff data real time or polls the Active Directory servers at regular intervals for data.
- How often the agent polls for user activity data, or attempts to establish or re-establish a real time connection with an Active Directory server if the connection is lost.
- What IP address the agent reports for logins to the Active Directory server itself.
- How much login and logoff data the agent retrieves when it establishes or re-establishes a connection with an Active Directory server.

When a user agent is configured to retrieve data real time and real time monitoring is unavailable, the agent instead attempts to poll the Active Directory servers for data until real time monitoring is again available.



Tip

If your user agent retrieves significant amounts of user activity, We recommend configuring polling instead of real time data retrieval. In a high-activity environment, configure a 1 minute polling interval and no more than a 10 minute maximum polling length.

Note that real time monitoring requires an Active Directory server running Windows Server 2008 or later.



Note

If you install the user agent on Windows Server 2003 or an older operating system, the user agent cannot collect real time statistics from an Active Directory computer.

From the user agent, you can view the current Active Directory server polling status at the time the tab is selected, the last login reported to the agent, and the last time the agent polled an Active Directory server.

You can also view whether the agent is polling an Active Directory server in real time, and the real time data retrieval status at the time the tab is selected. See the following table for more information on server statuses.

Table 2-2 Active Directory Server Statuses

Active Directory Server Status	Polling Availability	Real Time Availability
available	The server is available for polling.	The server is available for real time data retrieval.
unavailable	The server is not available for polling.	The server is not available for real time data retrieval, or the server is configured for polling.

Table 2-2 Active Directory Server Statuses (continued)

Active Directory Server Status	Polling Availability	Real Time Availability
pending	The server configuration is added, but communication hasn't started yet.	It takes some time after you add and save a server configuration for it to start communicating with the user agent. If the <code>pending</code> status persists, check communication between the user agent and the server.
unknown	The agent has started and a status is not yet available, or the agent has not yet checked the Active Directory server.	The agent has started and a status is not yet available, or the agent has not yet checked the Active Directory server.

**Note**

You should not connect more than one user agent to the same Active Directory domain controller because the user agent reports extraneous logins as each detects the other's connections. If you do, configure each user agent to exclude the IP address of every other host running an agent that is polling the same Active Directory server and the user name the agent uses to log in. For more information, see [Configure User Agent Excluded Addresses Settings, page 2-26](#).

To configure Active Directory server connections:

Access: Any

-
- Step 1** If necessary, log in to the computer on which the user agent is installed.
- Step 2** Click **Start > [All] Programs > Cisco > Configure Cisco Firepower Agent for Active Directory**.
- Step 3** Click the **Active Directory Servers** tab.
- Step 4** You have the following options:
- To add a new connection to a server, click **Add**.
 - To modify an existing connection, double-click the server name.
 - To remove an existing connection, click the server name and click **Remove**.
- Step 5** In the **Server Name/IP Address** field, enter the Active Directory server or domain controller's fully qualified server name or IP address. To detect logins to the Active Directory server, enter the IP address.
- If the agent is installed on an Active Directory server, to add the server where you installed the agent, enter `localhost` as the server name. You have the option to add a user name and password. If you omit that information, you cannot detect logoffs for users authenticating to the Active Directory server. You can poll the server regardless of whether you enter a user name and password.

**Note**

If your Active Directory system has multiple domain controllers, enter the hostname or IP address of the domain controller with which you want the user agent to communicate. (Active Directory domain controllers don't share their security logs so you must have a separate user agent connection to each controller.) In a distributed or heavily trafficked system, you can optionally install more than one user agent as discussed in [Deploy Multiple User Agents, page 1-6](#).

Step 6 In the **Authorized User** and **Password** fields, enter a user name and password with rights to query for user login and logoff data on the Active Directory server.

To authenticate using a proxy, enter a fully qualified user name.

By default, the domain for the account you used to log into the computer where you installed the agent auto populates the **Domain** field.



Note If your user password contains 65 or more characters, you cannot configure new server connections. To regain this functionality, shorten your password.

Step 7 In the **Domain** field, enter the name of the Active Directory domain.

Step 8 To detect logins to the Active Directory server, select an IP address from the **Local Login IP Address** field. The agent automatically populates this field with all IP addresses associated with the server specified in the **Server Name/IP Address** field.

If the **Server Name/IP Address** field is blank or contains `localhost`, this field is populated with all IP addresses associated with the local host.

Step 9 Check **Process real time events** to enable the user agent to retrieve login events from this Active Directory server real time.

Step 10 Click **Add** to add a new server or click **Save** to save changes to an existing server.

The server connection definition is displayed in the list of Active Directory servers. If you have more than one server connection configured, you can sort on **Host**, **Last Reported**, **Polling Status**, **Last Polled**, **Real Time Status**, or **Real Time** by clicking the respective column headers.



Note If the user agent cannot connect to the Active Directory server at configuration time, you cannot add the server. Check that the agent has TCP/IP access to the server, that the credentials you used can connect, and that you correctly configured the connection to the Active Directory server. See [Configure the Active Directory Server, page 2-4](#) for more information.

Step 11 (Optional.) Change the interval at which the agent automatically polls the Active Directory server for user login data, select a time from the **Active Directory Server Polling Interval** list.

After you save the settings, the next poll occurs after the selected number of minutes elapse, and recurs at that interval. If a poll takes longer than the selected interval, the next poll starts in the next interval after the poll ends.

If real time event processing is enabled for an Active Directory server, and the user agent loses connectivity with the server, the agent keeps attempting polls until it receives a response and real time data retrieval is available. After the connection is established, real time data retrieval resumes.

Step 12 (Optional.) Change the maximum time span polled when the agent first establishes or reestablishes a connection to poll an Active Directory server for user login data, select a time from the **Active Directory Server Max Poll Length** list.



Note The user agent does not allow saving a configuration that would skip user activity data in each poll. Therefore, you cannot save a value in the **Active Directory Server Max Poll Length** list less than the value selected from the **Active Directory Server Polling Interval** list.

Step 13 To save and apply configuration changes to the agent, click **Save**.

Step 14 You have the following options:

- To add or remove Management Center connections, select the **Firepower Management Centers** tab. For more information, see [Configure User Agent Management Center Connections, page 2-24](#).
You must add at least one Management Center to the agent to report user login and logoff data.
- To configure the agent, you can take any of the actions described in [Table 2-1 on page 2-20](#).

Configure User Agent Management Center Connections

License: FireSIGHT or N/A

You can send Active Directory user data to up to five Management Centers from a user agent. From the agent, you can also view the Management Center status at the time the tab is selected (*available*, *unavailable*, or *unknown* when the agent first starts) and the last login reported by the agent.

Before you add a connection, make sure you add the user agent to the Management Center configuration. For more information, see [Configure a Version 5.x Defense Center to Connect to User Agents, page 2-3](#), [Configure a Version 5.x Defense Center to Connect to User Agents, page 2-3](#), or [Configure a Version 6.x Management Center to Connect to User Agents, page 2-3](#).



Note

In Version 5.x, the Management Center is referred to as a Defense Center.

In a high availability configuration, add both Management Centers to the agent to enable update of user login and logoff data to both the primary and the secondary so the data remains current on both.

To configure Management Center connections:

Access: Any

- Step 1** If necessary, log in to the computer on which the user agent is installed.
- Step 2** Click **Start > [All] Programs > Cisco > Configure Cisco Firepower Agent for Active Directory**.
- Step 3** Click the **Firepower Management Centers** tab.
- Step 4** Click **Add**.
- Step 5** Enter the hostname or IP address of the Management Center you want to add.
- Step 6** Click **Add**.

The Management Center connection configuration is added. You cannot add a hostname or IP address more than once. You should not add a Management Center by both hostname and IP address. If the Management Center has more than one network adapter, you should not add it multiple times using different IP addresses.

If you have more than one Management Center connection configured, you can sort on **Host**, **Status**, or **Last Reported** by clicking the respective column headers.



Note

If the user agent cannot connect to a Management Center at configuration time, it cannot add that Management Center. Check that the agent has TCP/IP access to the Management Center.

- Step 7** To save and apply configuration changes to the agent, click **Save**. The updated settings are applied to the agent.

Step 8 You have the following options:

- (Optional.) Add or remove user names to or from the excluded user name list, select the **Excluded Usernames** tab. For more information, see [Configure User Agent Excluded Username Settings, page 2-25](#).
- (Optional.) Add or remove IP addresses to the excluded IP address list, select the **Excluded Addresses** tab. For more information, see [Configure User Agent Excluded Addresses Settings, page 2-26](#).
- (Optional.) View the log message and configure logging, choose the **Logs** tab. For more information, see [Configure User Agent Logging Settings, page 2-27](#).
- (Optional.) Configure general agent settings, click the **General** tab. For more information, see [Configure General User Agent Settings, page 2-29](#).
- To configure the agent, you can take any of the actions described in [Table 2-1 on page 2-20](#).

Configure User Agent Excluded Username Settings

License: FireSIGHT or N/A

You can define up to 500 user names to be excluded when polling for login or logoff events. If the agent retrieves a login or logoff event by an excluded user name, the agent does not report the event to the Management Center.

Login and logoff events for a user name that are reported before the exclusion are not affected. If you remove a user name from the excluded user name list, future login and logoff events for that user name are reported to the Management Center.

You can choose whether to exclude all logins and logoffs by a user from all domains, or from specific domains. You can also export and import lists of user names and domains, stored in comma-separated value files. Note that if you exclude a user already reported to the Management Center, the user is never unmapped from the host unless the host is purged from the database.

For example, if you installed the user agent on a computer separate from the Active Directory server, you can use this option to exclude the user agent user from logging to the Management Center.

To configure excluded user names:

Access: Any

-
- Step 1** If necessary, log in to the computer on which the user agent is installed.
- Step 2** Click **Start > [All] Programs > Cisco > Configure Cisco Firepower Agent for Active Directory**. Select the **Excluded Usernames** tab.
- Step 3** In the next available row, enter a user name you want to exclude in the **Username** column.
Excluded user names cannot include the dollar sign character (\$) or the quotation mark character (").
- Step 4** Enter the domain associated with the user name in the **Domain** column.
You can define only one domain per row. If you do not specify a domain, the user name in every domain is excluded.
- Step 5** Repeat steps 3 and 4 to add additional user names. If you have more than one excluded user name configured, you can sort on **Username** or **Domain** by clicking the respective column headers.

- Step 6** To remove a row, you have the following options:
- Highlight the row and press the Delete key.
 - Place your pointer at the end of the user name and press the Backspace key until it is deleted.
- The row is removed.
- To remove multiple rows, press Control+click to select multiple rows and press Delete.
- Step 7** To export the list of user names and domains to a comma-separated value file, click **Export List**. Select a file path to save the file.
- The file is saved. By default, the file is named `Cisco_user_agent_excluded_users.csv`.
- Step 8** To import a list of user names and domains from a comma-separated value file, click **Import List**. Select a file to upload.
- The existing user names are cleared, and the user names in the file are loaded. You cannot upload a file that contains duplicate user names. If there are any syntax errors in the file, you cannot upload the file.
- Entries in the comma-separated value file must be in the following format:
- ```
"username", "domain"
```
- A domain value is optional, but quotes are required as a placeholder.
- Step 9** Click **Save** to save and apply configuration changes to the agent.
- Step 10** You have the following options:
- To add or remove IP addresses to the excluded IP address list, select the **Excluded Addresses** tab. For more information, see [Configure User Agent Excluded Addresses Settings, page 2-26](#).
  - To configure the agent, you can take any of the actions described in [Table 2-1 on page 2-20](#).

## Configure User Agent Excluded Addresses Settings

**License:** FireSIGHT or N/A

You can configure up to 100 IPv4 and IPv6 addresses to be excluded when polling for login events. If the user agent retrieves a login or logoff event that contains an excluded IP address, the agent does not report the event to the Management Center.

Login and logoff events from an IP address that are reported before the exclusion are not affected. If you remove an IP address from the excluded address list, future login and logoff events for that address are reported to the Management Center.

For example, if you installed the user agent on a computer separate from the Active Directory server, you can use this option to exclude the user agent user from logging to the Management Center.



### Note

If you use both the user agent and TS Agent in the same network, you should exclude the TS Agent's IP address to prevent non-critical errors from being logged to the Firepower Management Center. When both the TS Agent and user agent detect the same user logging in, non-critical errors are written to the logs.

### To configure excluded IP addresses:

**Access:** Any

- Step 1** If necessary, log in to the computer on which the user agent is installed.

- Step 2** Click **Start > [All] Programs > Cisco > Configure Cisco Firepower Agent for Active Directory**. Select the **Excluded Addresses** tab.
- Step 3** In the next available row, enter an IP address you want to exclude in the **Address** column. Repeat this to add additional IP addresses.
- If you have more than one excluded IP address configured, you can sort on **Address** by clicking the respective column headers.
- If you enter an invalid IP address, an exclamation mark icon (❗) is displayed in the row header. You cannot enter another address without fixing the invalid address.
- Step 4** To remove an IP address, highlight the row and press the Delete key.
- The IP address is removed. To remove multiple rows, Control+click to select multiple rows and press the Delete key.
- Step 5** To export the list of IP addresses to a comma-separated value file, click **Export List**. Select a file path to save the file.
- The file is saved. By default, the file is named `Cisco_user_agent_excluded_addresses.csv`.
- Step 6** To import a list of IP addresses from a comma-separated value file, click **Import List**. Select a file to upload.
- The existing IP addresses are cleared, and the IP addresses in the file are loaded. You cannot upload a file that contains duplicate IP addresses. If there are any syntax errors in the file, you cannot upload the file.
- Step 7** Click **Save** to save and apply configuration changes to the agent.
- Step 8** You have the following options:
- To view the log message and configure logging, select the **Logs** tab. For more information, see [Configure User Agent Logging Settings, page 2-27](#).
  - To configure the agent, you can take any of the actions described in [Table 2-1 on page 2-20](#).

## Configure User Agent Logging Settings

**License:** FireSIGHT or N/A

You can view up to 250 status messages logged by the agent in the **Logs** tab. The agent logs status messages to the local event log for the following events when they occur:

- The agent successfully polls data from an Active Directory server
- The agent fails to connect to an Active Directory server
- The agent fails to retrieve data from the Active Directory server
- The agent successfully connects to a Management Center
- The agent fails to connect to a Management Center

The agent logs each status message with a timestamp and the severity level. The following table describes the possible severity levels by increasing severity.

**Table 2-3 User Agent Logging Severity Levels**

| Level       | Color  | Description                                                                                 |
|-------------|--------|---------------------------------------------------------------------------------------------|
| Debug       | gray   | The event is logged for debugging purposes.<br>These messages are not displayed by default. |
| Information | green  | The event is consistent with normal agent operation.                                        |
| Warning     | yellow | The event is unexpected, but does not necessarily disrupt normal agent operation.           |
| Error       | red    | The event is unexpected, and normal agent operation is disrupted.                           |

The agent can log status messages to Windows application logs in addition to the local event log. The agent can also export the local event log contents to a comma-separated value file.

You can configure whether status messages are stored, how long they are stored, and you can clear the event log of all status messages. You can also configure maintenance options, such as viewing debug status messages and accessing the **Maintenance** tab.



**Note**

Debug status messages are stored for seven days before being removed from the event log. Configuring how long status messages are stored and clearing the event log does not affect debug status message storage.

**To configure user agent logging settings:**

**Access:** Any

- 
- Step 1** If necessary, log in to the computer on which the user agent is installed.
  - Step 2** Click **Start > [All] Programs > Cisco > Configure Cisco Firepower Agent for Active Directory**.
  - Step 3** Click the **Logs** tab.
  - Step 4** If directed to do so by Cisco TAC, select **Show Debug Messages in Log** to view debug status messages in the event log and enable the **Maintenance** tab page.



**Note**

Select this option only if Cisco TAC directs you to do so.

- 
- Step 5** Select **Log Messages to Windows Application Log** to log non debug status messages to both the Windows application logs and to the local event logs.  
To view the Windows application logs, open the Windows Event Viewer.
  - Step 6** Select a time period from the **Message Cache Size** drop-down list to configure how long status messages are saved before they are automatically deleted from the local event log.  
Status messages, once logged to the local event log, are saved for the time period selected in the **Message Cache Size** drop-down list, then deleted.



**Note**

The **Message Cache Size** setting affects only the local event log, not the Windows application logs, even if you select **Log Messages to Windows Application Log**.

- Step 7** Click **Refresh** to view new status messages logged since the last refresh.
- If new status messages have been logged since the last refresh, a message is displayed stating there are new status messages available. If the refresh results in more than 250 messages, the oldest status messages are removed from the **Logs** tab page. To view more than 250 messages, export the logs. See step 8 for more information.
- Step 8** Click **Export Logs** to export the local event log contents to a comma-separated value file.
- The comma-separated value file contains all event log status messages and debug messages.
- Step 9** Click **Clear Event Log** to remove all non-debug status messages from the local event log.
- The local event is cleared, except for a status message stating the agent removed the messages.
- Step 10** To save and apply configuration changes to the agent, click **Save**.
- Step 11** You have the following options:
- To configure general agent settings, select the **General** tab. For more information, see [Configure General User Agent Settings, page 2-29](#).
  - To configure the agent, you can take any of the actions described in [Table 2-1 on page 2-20](#).



## Configure General User Agent Settings

**License:** FireSIGHT or N/A

The General tab contains basic user agent configuration. You can change the agent name reported to the Management Center when the agent reports login data. You can also start and stop the agent service, change the logoff check frequency, and view the current service status.

**To configure general User Agent settings:**

**Access:** Any

- Step 1** On the computer where you installed the agent, select **Start > Programs > Cisco > Configure Cisco Firepower User Agent for Active Directory**.
- Step 2** Click start (  ) to start the agent service.
- Step 3** Click stop (  ) to stop the agent service.
- Step 4** (Optional.) Modify the **Agent Name** for the agent, which defaults to `Cisco_FUAFAD`. You can enter letters, numbers, underscores (\_), and dashes (-).
- Step 5** (Optional.) Change the frequency the agent checks for logoff data, select a time period from the **Logoff Check Frequency** list. Select **0** to disable checking for logoff data.
- Step 6** (Optional.) Change the agent scheduling priority, choose a level from the **Priority** list. Choose **High** only if your agent monitors and retrieves significant amounts of user activity and it is affecting performance.
- Step 7** To save settings, click **Save**.
- Step 8** To configure the agent, you can take any of the actions described in [Table 2-1 on page 2-20](#).

## Configure User Agent Maintenance Settings

**License:** FireSIGHT or N/A

In addition to configuration settings, the agent stores user-to-IP-address mapping information, the local event log, and reporting state information in the SQL CE database. The agent Maintenance tab allows you to clear portions of the database for maintenance purposes. You can clear cached user-to-IP-address mapping information and local event log information. You can also clear the reporting state cache, which forces a manual polling of the configured Active Directory servers.



### Caution

Do *not* change any settings on the Maintenance tab page unless Support directs you to do so.

### To configure user agent maintenance settings:

**Access:** Any

- 
- Step 1** On the computer where you installed the agent, select **Start > Programs > Cisco > Configure Cisco Firepower User Agent for Active Directory**.
  - Step 2** Click the **Logs** tab.
  - Step 3** Click **Show Debug Messages in Log** to enable the **Maintenance** tab.
  - Step 4** Click the **Maintenance** tab.
  - Step 5** Click **Clear user mapping data cache** to clear all stored user-to-IP-address mapping data.  
The agent deletes all stored user-to-IP-address mapping data from the local agent database. Stored user-to-IP-address mapping data in the Management Center database is not affected by clearing the local agent database.
  - Step 6** Click **Clear logon event log cache** to clear all stored login event data.
  - Step 7** Click **Clear reporting state cache** to clear data related to the last time the agent reported login and logoff information to the configured Management Centers.  
The agent deletes all information related to the last time it reported login and logoff information to the configured Management Centers. At the start of the next polling interval, the agent manually polls all configured Active Directory Servers, retrieving information within the time span defined in the **Active Directory Server Max Poll Length** field. See [Configure User Agent Active Directory Server Connections, page 2-21](#) for more information.
  - Step 8** Select a level of logging granularity from the **Debug Log Level** drop-down list to configure how detailed the logged debug messages are.
  - Step 9** To configure the agent, you can take any of the actions described in [Table 2-1 on page 2-20](#).
-

# Troubleshoot the User Agent

The following sections discuss solutions to issues you might encounter using the user agent:

- [Can't Connect to a Management Center, page 2-31](#)
- [User Agent Unresponsive, page 2-33](#)
- [User Agent Doesn't Show Every Login, page 2-34](#)
- [User Agent Isn't Processing Real Time Events, page 2-34](#)
- [User Agent Doesn't Show User Logoff Events, page 2-35](#)
- [User Agent and TS Agent in Same Network, page 2-35](#)

## Can't Connect to a Management Center

This section discusses the following issues that might prevent the user agent from connecting to the Firepower Management Center:

- [User Agent not an Identity Source, page 2-31](#)
- [Incorrect Windows Ciphers, page 2-32](#)

### User Agent not an Identity Source

In the user agent's **Firepower Management Centers** tab page, if the status of a Management Center is *unavailable*, make sure you added the user agent as an identity source in the Management Center. For more information about user agent configuration, see the *Configuration Guide*.

**To verify the user agent identity source in a version 6.X Management Center:**

- 
- |               |                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Log in to the Management Center as an administrator.                                                              |
| <b>Step 2</b> | Click <b>System &gt; Integration</b> .                                                                            |
| <b>Step 3</b> | Click the <b>Identity Sources</b> tab.                                                                            |
| <b>Step 4</b> | Click <b>User Agent</b> .                                                                                         |
| <b>Step 5</b> | Verify a user agent is defined and verify its IP address. If you make any changes, click <b>Save</b> .            |
| <b>Step 6</b> | Check the status of the Management Center again in the user agent's <b>Firepower Management Centers</b> tab page. |
- 

If the Management Center is configured properly and you still can't connect, try the following:

- Double-check the Management Center's hostname or IP address you've configured in the user agent.
- If you're accessing the Management Center by hostname, use the `nslookup hostname` command to verify the hostname resolves to an IP address.
- If you're accessing the Management Center by IP address, use the `ping ip-address` command to verify it is reachable by the user agent computer.

## Incorrect Windows Ciphers

If the Windows machine on which the user agent is installed does not have the appropriate ciphers installed, you observe the following symptoms:

- The user agent shows the Firepower Management Center as `unavailable` in the user agent's **Firepower Management Centers** tab page.
- The Firepower Management Center can download users and groups from the Active Directory domain controller.

This situation applies to you *only* if you restricted the ciphers on the Windows machine, which is relatively uncommon.

**To view the list of available ciphers:**

- 
- Step 1** Log in to the user agent machine.
- Step 2** At a command prompt, enter `gpedit.msc`, and then press Enter.
- Step 3** Click **Computer Configuration > Administrative Templates > Network > SSL Configuration Settings**.
- Step 4** Under SSL Configuration Settings, select **SSL Cipher Suite Order**.
- Step 5** Set the cipher list to include one or more of the ciphers shown in the following section.
- 

## Ciphers Supported by the Firepower Management Center

The Firepower Management Center supports the following ciphers for connecting with the user agent. The ciphers are shown in OpenSSL format. Windows ciphers are usually listed in RFC format. To translate the cipher names, see the [RFC mapping list](https://testssl.sh) on the <https://testssl.sh> site.



### Caution

Use caution when deciding which ciphers to select because not all ciphers are secure. For information about secure ciphers, consult a resource such as the Open Web Application Security Project (OWASP). For example, you can refer to their [TLS Cipher String Cheat Sheet](#).

Supported ciphers:

```
AES256-GCM-SHA384
AES256-SHA
AES256-SHA256
CAMELLIA256-SHA
DES-CBC3-SHA
ECDH-ECDSA-AES256-GCM-SHA384
ECDH-ECDSA-AES256-SHA
ECDH-ECDSA-AES256-SHA384
ECDH-ECDSA-DES-CBC3-SHA
ECDH-RSA-AES256-GCM-SHA384
ECDH-RSA-AES256-SHA
ECDH-RSA-AES256-SHA384
ECDH-RSA-DES-CBC3-SHA
ECDHE-ECDSA-AES128-GCM-SHA256
```



```

ECDHE-ECDSA-AES128-SHA
ECDHE-ECDSA-AES128-SHA256
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA
ECDHE-ECDSA-AES256-SHA384
ECDHE-ECDSA-DES-CBC3-SHA
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA
ECDHE-RSA-AES128-SHA256
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA
ECDHE-RSA-AES256-SHA384
ECDHE-RSA-DES-CBC3-SHA
EDH-DSS-DES-CBC3-SHA
EDH-RSA-DES-CBC3-SHA
PSK-3DES-EDE-CBC-SHA
PSK-AES256-CBC-SHA
SRP-DSS-3DES-EDE-CBC-SHA
SRP-DSS-AES-128-CBC-SHA
SRP-DSS-AES-256-CBC-SHA
SRP-RSA-3DES-EDE-CBC-SHA
SRP-RSA-AES-128-CBC-SHA
SRP-RSA-AES-256-CBC-SHA

```

## User Agent Unresponsive

If you suspect you aren't getting data from the user agent, you can do any of the following:




- Log in to the user agent computer and check its status; for more information, see [Configure General User Agent Settings, page 2-29](#).
- Set up a user agent health policy to monitor its status on the Management Center as discussed in the procedure that follows.

A user agent health policy informs you when the Management Center doesn't receive a heartbeat from the user agent. For more information, see the configuration guide.

### To set up a user agent health policy in a 6.X Management Center:

- 
- Step 1** Log in to the Management Center as a user with Administrator or Maintenance User privileges.
- Step 2** Click **System > Health > Policy**.
- Step 3** Click **Create Policy**.
- Step 4** On the Create Policy page, enter the following information:
- **Copy Policy** list: Choose any policy, such as **Default Health Policy**.
  - **New Policy Name** field: Enter a name to identify this policy.
  - **New Policy Description** field: Enter an optional policy description.

The new policy is displayed.

- Step 5** Click  (edit).
- Step 6** In the left column, click **User Agent Status Monitor**.
- Step 7** In the right column, click **On**.
- Step 8** At the bottom of the page, click **Save Policy and Exit**.
- Step 9** Click  (apply) next to the name of the policy.
- Step 10** Follow the prompts on your screen to apply the policy to managed devices.
- Step 11** To monitor user agents at any time, click **Health > Monitor** or watch the Management Center's  (monitor) icon for messages.

A message similar to the following is displayed if the user agent heartbeat isn't detected by a managed device:

---

Some user agents are not up-to-date

---

## User Agent Doesn't Show Every Login

The user agent tracks user names per IP address. If the same user logs in to the same IP address multiple times, you'll see only one User Login event in the Management Center for that user.

In the following scenario, you'll see multiple User Login events for a user:

- The user logs in from different IP addresses (for example, desktop and phone).
- User `patricia.nolan` logs in from the following IP addresses in this sequence:
  - 192.0.2.102
  - 192.0.2.210
  - 192.0.2.102

It doesn't matter if `patricia.nolan` logs out from any of the IP addresses; the Management Center reports at least two User Login events, one for each unique IP address. (In other words, the Management Center doesn't report the last login because it's from the same IP address as the first.)

## User Agent Isn't Processing Real Time Events

To be able to process real time events from the Active Directory server, the user agent requires Remote Procedure Call (RPC) access to the Active Directory server. If the status of real time processing is displayed as `unknown` or `unavailable` in the user agent's **Active Directory Servers** tab page for an extended period of time, look for errors in the user agent log and try the other suggestions discussed in this section.

**To troubleshoot real time processing issues:**

- 
- Step 1** If necessary, log in to the computer where the user agent is installed.
  - Step 2** Click **Start > Programs > Cisco > Configure Cisco Firepower User Agent for Active Directory**
  - Step 3** Click the **Logs** tab.
  - Step 4** Check **Show debug messages in log**.

**Step 5** Observe the log messages or click **Export logs** to export log messages to a file.

**Step 6** Look for messages like the following:

"error", "[2317] - Unable to attach event listener to *host or IP address*. Check firewall settings on AD server. RPC server is unavailable

The preceding message indicates a configuration issue with the Active Directory Server's firewall. Review the instructions in [Allow the User Agent to Access Distributed Component Object Management \(DCOM\)](#), page 2-12 and try again.

To isolate the firewall as the issue, optionally disable the Active Directory Server's firewall for a few minutes and see if the user agent can process real time events.

**Step 7** Try deleting the Active Directory Server configuration in the user agent and adding it back.

---

## User Agent Doesn't Show User Logoff Events

If you don't see any User Logoff events in the Management Center, make sure you allowed WMI through the firewall on all domain computers. For more information, see [Configure Domain Computers](#), page 2-6.

## User Agent and TS Agent in Same Network

If you use both the Terminal Services (TS) Agent and the user agent, you can avoid non-critical errors in the logs by excluding the TS Agent IP address from the user agent. If the same user is detected by both the TS Agent and the user agent, non-critical errors are written to logs.

For more information, see [Configure User Agent Excluded Addresses Settings](#), page 2-26.

