



User Control with the Passive Identity Agent

The following topics discuss how to configure and use the passive identity agent.

- [The Passive Identity Agent Identity Source, on page 1](#)
- [Deploy the Passive Identity Agent, on page 3](#)
- [How to Create a Passive Identity Agent Identity Source, on page 8](#)
- [Configure the Passive Identity Agent , on page 10](#)
- [Monitor the Passive Identity Agent, on page 28](#)
- [Manage the Passive Identity Agent, on page 29](#)
- [Troubleshoot the Passive Identity Agent, on page 31](#)
- [Security Requirements for the Passive Identity Agent, on page 32](#)
- [Internet Access Requirements for the Passive Identity Agent, on page 33](#)
- [History for the Passive Identity Agent, on page 34](#)

The Passive Identity Agent Identity Source

The passive identity agent identity source sends session data from Microsoft Active Directory (AD) to the Secure Firewall Management Center. All you need is a supported Microsoft AD setup as discussed in [About Realms and Realm Sequences](#).

The passive identity agent version 1.0 sends IPv4 user sessions only but Version 1.1 sends IPv4 and IPv6 user sessions.



Note You do not need to configure the Cisco Identity Services Engine (ISE) to use this identity source.

Passive identity agent roles

The passive identity agent supports the following roles:

- **Standalone:** A passive identity agent that is not part of a redundant pair. A standalone agent can read users and groups from multiple Active Directory servers and domain controllers, provided the software is installed on all of them.
- **Primary:** (Primary agent in a redundant pair.) Can be installed on a Microsoft AD domain controller, directory server, or any network client.

Handles all communication with the Secure Firewall Management Center unless it stops communicating, in which case communication is handled by secondary agents.

- Secondary: (Secondary, or backup, agent in a redundant pair.) Can be installed on a Microsoft AD domain controller, directory server, or any network client.

Monitors the health of the primary agent and takes over if the primary agent stops communicating with the Secure Firewall Management Center.

Passive identity agent system requirements

The passive identity agent requires the following:

- If you install the passive identity agent on a Windows Active Directory server, the server must run Windows Server 2008 or later.
- If you install it on a Windows client attached to the domain, the client must run Windows 8 or later.
- The system clock on all systems must be synchronized. We strongly recommend using the same NTP servers on all of them. This means:
 - The Secure Firewall Management Center.
For more information, see [Time Synchronization](#).
 - All Windows Active Directory servers and domain controllers.
 - The machine on which the passive identity agent is installed.
- Secure Firewall Management Center must run 7.6 or later.
- Any Secure Firewall Threat Defense managed by the Secure Firewall Management Center must run 7.1 or later.
- You must enable Snort 3 on the Secure Firewall Threat Defense devices.

Passive identity agent limitations

The passive identity agent the following limitations:

- Up to 10 agents simultaneously
- One passive identity agent identity source can monitor up to 50 AD directories
- Up to 300,000 concurrent user sessions
- IPv6 addresses are *not* supported (passive identity agent 1.0)
- IPv6 addresses are supported (passive identity agent 1.1)

Deploy the passive identity agent

For information about deployment options, see [Deploy the Passive Identity Agent, on page 3](#).

**Note**

We recommend you use the latest version of the passive identity agent. To see the available versions, go to software.cisco.com. To upgrade the passive identity agent, see [Upgrade the Passive Identity Agent Software, on page 28](#)

Deploy the Passive Identity Agent

You can install the Passive Identity Agent software on any machine that is part of a Microsoft Active Directory (AD) domain you want to use for user awareness and control. In other words, you can install it on any of the following:

- The Microsoft Active Directory server
- A domain controller
- A client connected to the network that is neither the directory server nor a domain controller

Any particular passive identity agent can monitor one or several Active Directory domain controllers in the same domain.

The machine on which the passive identity agent must communicate with the Secure Firewall Management Center using the TLS/SSL protocol. For more information, see [Internet Access Requirements for the Passive Identity Agent, on page 33](#).

Types of agents

You can configure the following types of agents on the Microsoft AD directory server, domain controller, or on any client connected to the domain:

- Standalone agent: One agent that can monitor one or several Active Directory domain controllers in the same domain.
- Primary agent and secondary agent that can monitor one or several AD domain controllers in the same domain: To provide redundancy, you can install a primary and secondary agent on different machines. The primary is responsible for communicating with the Secure Firewall Management Center but if communication fails, the secondary agent takes over.

See one of the following topics for more information.

Related Topics

[Simple Passive Identity Agent Deployment](#), on page 3

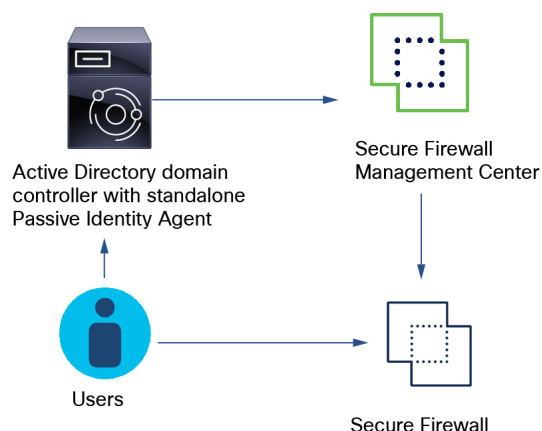
[Single Passive Identity Agent Monitoring Multiple Domain Controllers](#), on page 4

[Multiple Passive Identity Agents Monitoring Multiple Domain Controllers](#), on page 5

[Passive Identity Agent Primary/Secondary Agent Deployments](#), on page 7

Simple Passive Identity Agent Deployment

The following diagram shows the simplest passive identity agent deployment.

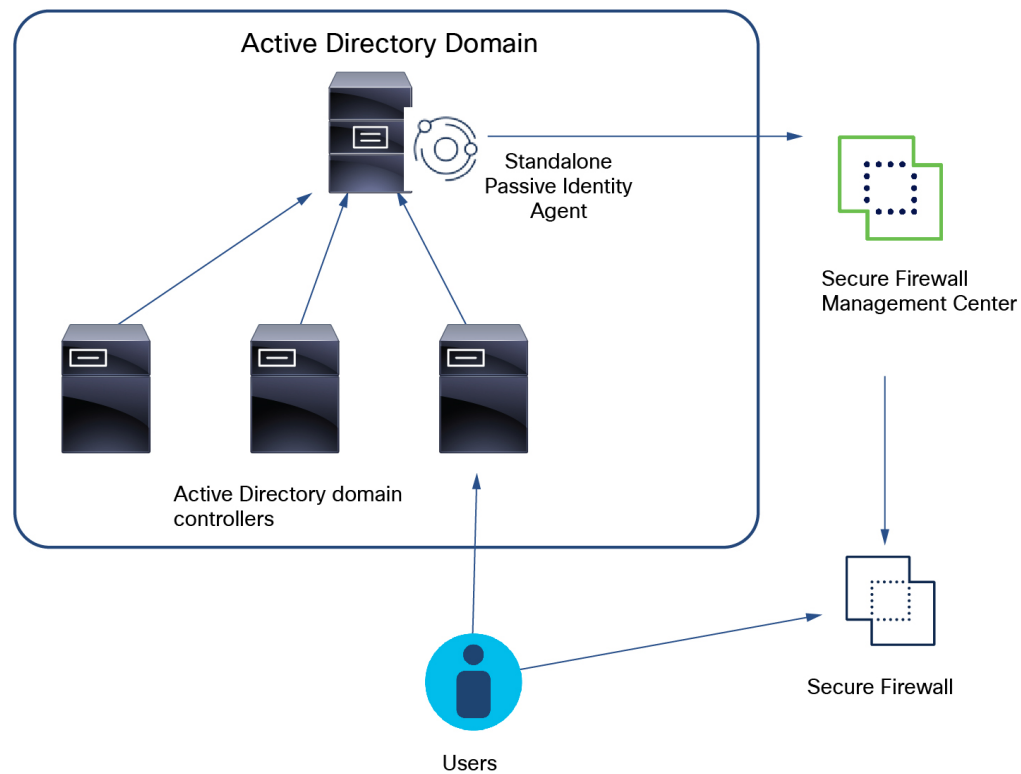


In the preceding example, a standalone passive identity agent is installed on the AD domain controller. Users log in and out of the AD domain and the agent sends user name and IP address information to the Secure Firewall Management Center. As users access the network, access control and identity policies deployed to the Secure Firewall Threat Defense determine whether or not, and how, access is allowed.

You can install a passive identity agent on the AD domain controller, directory server, or on any client connected to the domain you wish to monitor.

Single Passive Identity Agent Monitoring Multiple Domain Controllers

The following diagram shows a standalone passive identity agent that monitors several AD domain controllers.



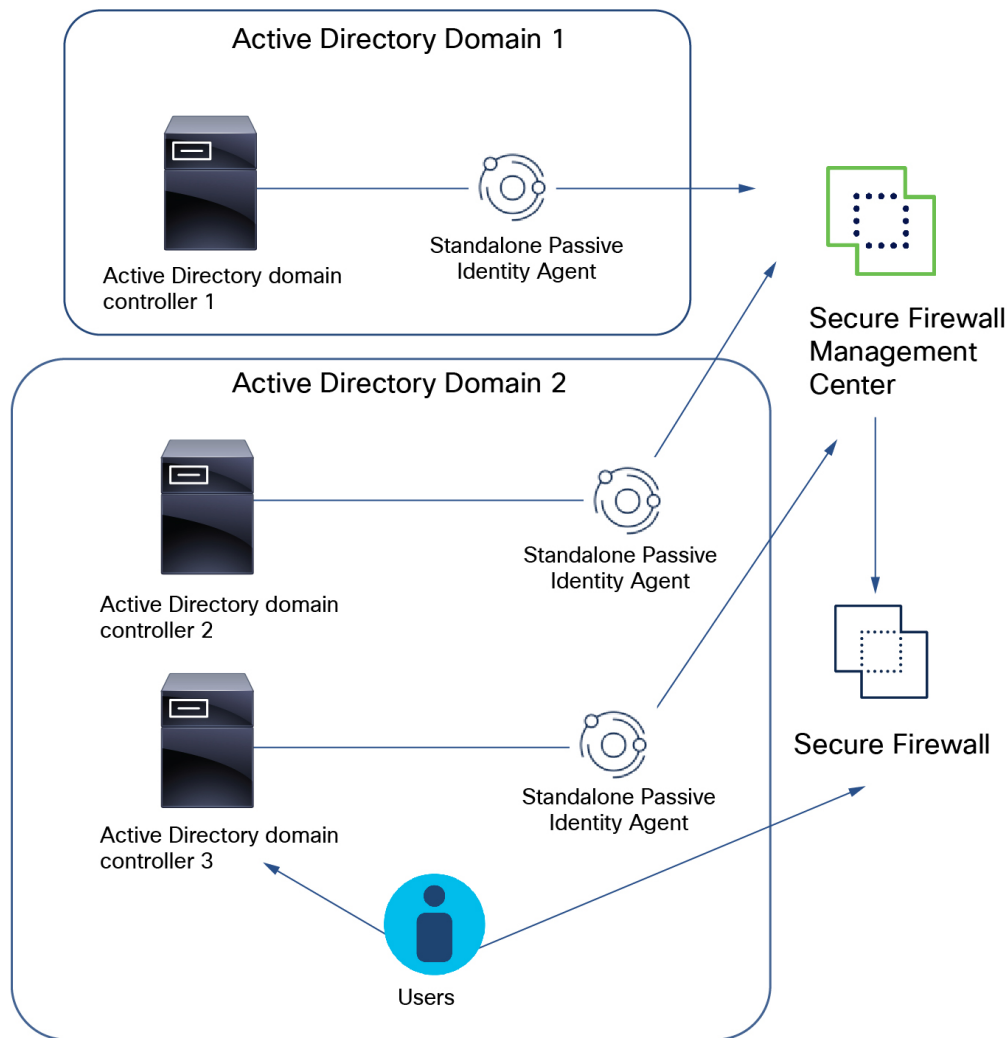
In the preceding diagram, the standalone passive identity agent is installed on a client attached to the AD domain (or on the domain controller itself). Users log in to any domain controller and the agent sends user and IP address information to the Secure Firewall Management Center. As users access the network, access control and identity policies deployed to the Secure Firewall Threat Defense determine whether or not, and how, access is allowed.

You can install a passive identity agent on the AD domain controller, directory server, or on any client connected to the domain you wish to monitor.

Multiple Passive Identity Agents Monitoring Multiple Domain Controllers

The following figure shows standalone monitoring multiple AD domain controllers:

- In AD domain 1, a standalone passive identity agent installed on a machine attached to AD domain controller 1 sends user and IP address mapping data to the Secure Firewall Management Center.
- In AD domain 2, standalone agents installed on AD domain controllers 1 and 2 send user and IP address mapping data to the Secure Firewall Management Center.



You can install a passive identity agent on the AD domain controller, directory server, or on any client connected to the domain you wish to monitor.

The preceding figure shows three passive identity agents, each configured as a standalone. To do this:

1. Create two Microsoft AD realms: one for each AD domain.
See [Create an LDAP Realm or an Active Directory Realm and Realm Directory](#).
2. For AD domain 2, create two directories, one for each domain controller.
3. Install the Passive Identity Agent software on a client that can log in to the domain.
Configure each passive identity agent individually to communicate with the Secure Firewall Management Center on which you configure the passive identity agent source.
See [Install the Passive Identity Agent Software, on page 23](#).
4. Create the passive identity agent identity source.
See [Create a Primary or Secondary Passive Identity Agent Identity Source, on page 13](#).

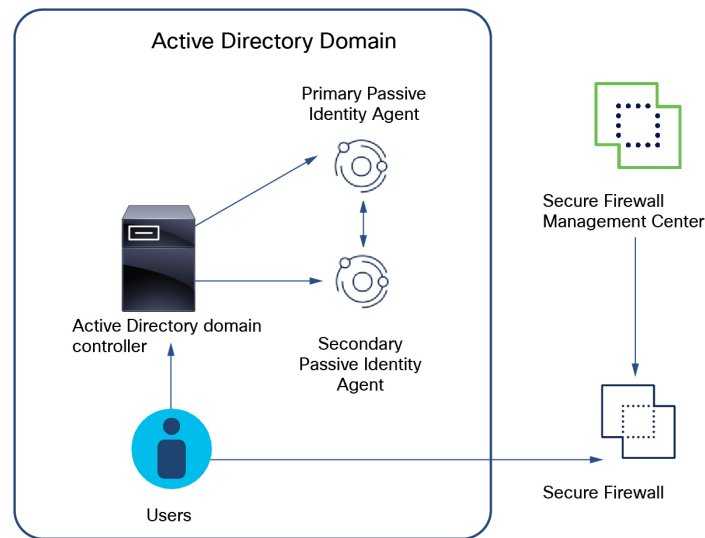
Passive Identity Agent Primary/Secondary Agent Deployments

To provide redundancy and to avoid a single point of failure, you can configure primary and secondary passive identity agents in any of the ways shown in this topic.

You can install a passive identity agent on the AD domain controller, directory server, or on any client connected to the domain you wish to monitor.

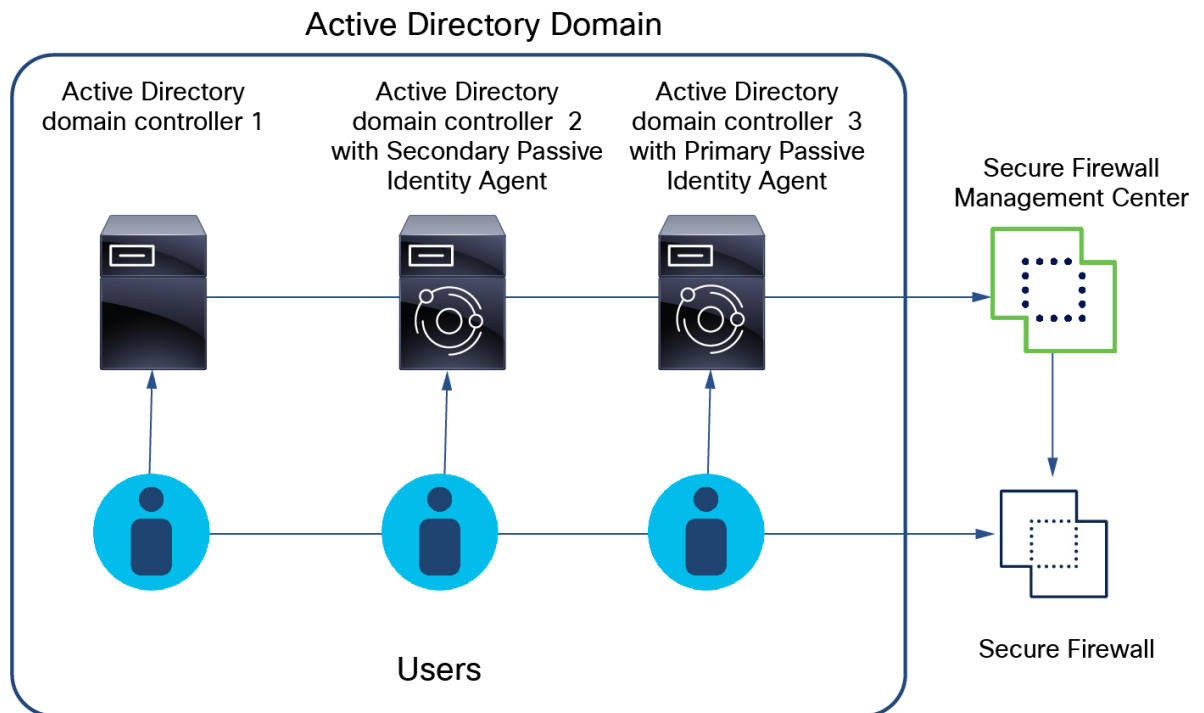
Single AD domain controller with primary and secondary agents

The following figure shows how to set up primary and secondary passive identity agents on one AD domain controller. If the primary agent fails, the secondary takes over.



To set this up:

1. Create a Microsoft AD realm that has one directory for the domain controller.
See [Create an LDAP Realm or an Active Directory Realm and Realm Directory](#).
2. Install the passive identity agent software on any two network machines connected to the domain controller.
Configure each passive identity agent individually to communicate with the Secure Firewall Management Center on which you configure the passive identity agent source.
See [Install the Passive Identity Agent Software, on page 23](#).
3. Create the identity source.
See [Create a Primary or Secondary Passive Identity Agent Identity Source, on page 13](#).

Multiple AD domain controllers, primary and secondary agents

The preceding figure shows how to configure primary and secondary agents to monitor three AD domain controllers. If the primary agent fails, the secondary agent takes over.

To set this up:

1. Create a Microsoft AD realm that has one directory for the domain controller.

See [Create an LDAP Realm or an Active Directory Realm and Realm Directory](#).

2. Install the passive identity agent software on any machine connected to the domain controller.

Configure each passive identity agent individually to communicate with the Secure Firewall Management Center on which you configure the passive identity agent source.

See [Install the Passive Identity Agent Software, on page 23](#).

3. Create the identity source.

See [Create a Primary or Secondary Passive Identity Agent Identity Source, on page 13](#).

How to Create a Passive Identity Agent Identity Source

The following provides high-level tasks required to configure the passive identity agent identity source in the Secure Firewall Management Center and to deploy agent software to your Microsoft Active Directory (AD) servers.

Procedure

	Command or Action	Purpose
Step 1	Enable the Cisco Secure Dynamic Attributes Connector.	The dynamic attributes connector is a requirement to use the passive identity agent. See Enable the Cisco Secure Dynamic Attributes Connector .
Step 2	Create a realm for your Microsoft AD domain and domain controllers.	<i>Realms</i> are connections between the Secure Firewall Management Center and the user accounts on the servers you monitor. They specify the connection settings and authentication filter settings for the server. For more information, see Create an LDAP Realm or an Active Directory Realm and Realm Directory .
Step 3	Create a passive identity agent identity source.	The identity source allows the Secure Firewall Management Center and passive identity agent to communicate with each other. Create standalone, primary, or secondary agents, depending on your needs. For more information, see: <ul style="list-style-type: none"> • About Passive Identity Agent Roles, on page 16 • Create a Passive Identity Agent Identity Source, on page 10
Step 4	Create a passive identity agent user on the Secure Firewall Management Center.	We provide a role sufficient for the agent and manager to communicate with each other. We recommend using that role and no other for the passive identity agent user.
Step 5	Install the passive identity agent software.	The way you install the agent depends on your deployment. You can install a passive identity agent on the AD domain controller, directory server, or on any client connected to the domain you wish to monitor. For more information, see: <ul style="list-style-type: none"> • Deploy the Passive Identity Agent, on page 3 • Install the Passive Identity Agent Software, on page 23

What to do next

[Create an LDAP Realm or an Active Directory Realm and Realm Directory.](#)

Configure the Passive Identity Agent

The following topics discuss how to configure the passive identity agent.

Related Topics

[Create an LDAP Realm or an Active Directory Realm and Realm Directory](#)

[Create a Passive Identity Agent Identity Source](#), on page 10

[Install the Passive Identity Agent Software](#), on page 23

[Create a Secure Firewall Management Center User for the Passive Identity Agent](#), on page 16

Enable the Cisco Secure Dynamic Attributes Connector

This task discusses how to enable the Cisco Secure Dynamic Attributes Connector in the Secure Firewall Management Center. The dynamic attributes connector is an integration that enables objects from cloud networking products to be used in Firewall Management Center access control rules.

Procedure

-
- | | |
|---------------|--|
| Step 1 | Log in to the Secure Firewall Management Center if you have not done so already. |
| Step 2 | Click Integration > Dynamic Attributes Connector . |
| Step 3 | Slide to Enabled . |
| Step 4 | Messages are displayed while the dynamic attributes connector is enabled. |
- In the event of errors, try again. If errors persist, contact Cisco TAC.
-

Create a Microsoft Active Directory Realm

The passive identity agent requires you to create a Microsoft Active Directory (AD) realm and directories in the Secure Firewall Management Center as discussed in [Create an LDAP Realm or an Active Directory Realm and Realm Directory](#).

Create a Passive Identity Agent Identity Source

This task discusses how to create a passive identity agent that sends user session activity to the Secure Firewall Management Center.

Before you begin

Complete the following:

- Review passive identity agent roles as discussed in [About Passive Identity Agent Roles](#), on page 16.

- Create a Microsoft AD realm as discussed in [Create an LDAP Realm or an Active Directory Realm and Realm Directory](#).

Procedure

- Step 1** Log in to the Secure Firewall Management Center as an administrator.
- Step 2** Click **Integration > Other Integrations > Identity Sources**.
- Step 3** **Integration > Other Integrations > Identity Sources**.
- Step 4** Click **Passive Identity Agent**.
- Step 5** If the Cisco Secure Dynamic Attributes Connector has not been enabled yet, you are prompted to do so. For more information about enabling the dynamic attributes connector, see [Enable the Cisco Secure Dynamic Attributes Connector](#).
- Step 6** Click **Create Agent**.
- Step 7** In the Configure Agent dialog box, enter the following information:

Item	Description
Name	Enter a unique name to identify this passive identity agent.
Description	Enter an optional description.
Role	<p>Click one of the following:</p> <ul style="list-style-type: none"> • Primary: The agent responsible for communicating with the Secure Firewall Management Center. Not available if you choose Standalone. • Secondary: Becomes the primary if the primary loses contact with the Secure Firewall Management Center. Not available if you choose Standalone. • Standalone: If there is only one passive identity agent. <p>For more information about roles, see About Passive Identity Agent Roles, on page 16.</p>

- Step 8** Continue with:
- [Create a Standalone Passive Identity Agent Identity Source](#), on page 11
 - [Create a Primary or Secondary Passive Identity Agent Identity Source](#), on page 13

Create a Standalone Passive Identity Agent Identity Source

This task discusses how to configure a standalone passive identity agent.

Before you begin

Complete the tasks discussed in [Create a Passive Identity Agent Identity Source](#), on page 10.

Procedure

Step 1 In the Configure Agent dialog box, enter the following information:

Item	Description
Role	Click Standalone .
Domain Controller	From the list, select the check box next to each domain controller that has a passive identity agent you wish to use for identity management and user control. (Optional.) Click Add (+) to add a new one.

The following figure shows an example of a standalone passive identity agent identity source.

Configure Agent ⓘ

Name *
Standalone

Description

Role ⓘ
☐ Primary ☐ Secondary ☒ Standalone
[Learn more about the agent role.](#)

Domain Controller *
 bogus.example.com x v +
 Agent will monitor this domain controller.

Important:
 This agent will be created and assigned to the selected domain controller. Install it on the domain controller (or on its member machine) to start the tracking.

Cancel Save

Step 2 In the Configure Agent dialog box, click **Save**.

Step 3 In the top right corner of the page, click **Save**.

The following figure shows an example.

Configure Identity Sources

Select the service type and start configuring the identity source. Deploy the changes after you're finished.

Service Type:

☐ None ☐ Identity Services Engine ☒ Passive Identity Agent

Message: Your changes will be effective after you save Passive Identity Agent as the Identity Source.

Search: Search by agent name or domain controller name Create Agent

Domain Controllers	Monitoring Agents	Hostname	Connection Status
> bogus			
> forest.example.com			

Note

The passive identity agent won't be active until you create a user and install the software.

What to do next

- See [Create a Secure Firewall Management Center User for the Passive Identity Agent](#), on page 16
- See [About Passive Identity Agent Installation](#), on page 19

Create a Primary or Secondary Passive Identity Agent Identity Source

The following task continues from [Create a Passive Identity Agent Identity Source](#), on page 10.

Before you begin

Complete the tasks discussed in [Create a Passive Identity Agent Identity Source](#), on page 10.

Procedure

Step 1 In the Configure Agent dialog box, enter the following information:

Item	Description
Role	<p>Click one of the following:</p> <ul style="list-style-type: none"> • Primary: The agent responsible for communicating with the Secure Firewall Management Center. • Secondary: Becomes the primary if the primary loses contact with the Secure Firewall Management Center. <p>For more information about roles, see About Passive Identity Agent Roles, on page 16.</p>

Item	Description
Primary Agent Hostname/IP Address	(Primary agent only.) Enter the fully qualified domain name or IP address of the server on which the primary passive identity agent is installed. The passive identity agent version 1.0 supports IPv4 addresses and fully qualified domain names only. Version 1.1 supports IPv4, IPv6, and fully qualified domain names.
Secondary Agent Hostname/IP Address	(Secondary agent only.) Enter the fully qualified host name or IP address of the server on which the secondary passive identity agent is installed. The passive identity agent version 1.0 supports IPv4 addresses and fully qualified domain names only. Version 1.1 supports IPv4, IPv6, and fully qualified domain names.
Primary Agent	(Secondary agent only.) From the list, click the name of the primary passive identity agent.
Domain Controller	(Primary agent only.) From the list, select the check box next to each domain controller that has a passive identity agent you wish to use for identity management and user control.

The following figure shows an example of a primary agent:

Configure Agent ⓘ

Name *
Primary

Description

Role ⓘ
☒ Primary
 ☐ Secondary
 ☐ Standalone
[Learn more about the agent role.](#)

Primary Agent Hostname/IP Address *
192.0.2.110
Enter an HA host name where you would want to host the agent.

Domain Controller *
 forest.example.com x v +
Agent will monitor this domain controller.

Important:
 This agent will be created and assigned to the selected domain controller. Install it on the domain controller (or on its member machine) to start the tracking.

Cancel Save

The following figure shows an example of a secondary agent:

Configure Agent ?

Name *

Description

Role ⓘ

☐ Primary
 ☒ Secondary
 ☐ Standalone

[Learn more about the agent role.](#)

Secondary Agent Hostname/IP Address *

Enter an HA host name where you would want to host the agent.

Primary Agent *

Select a primary agent for your secondary agent.

Important:
This agent will be associated with the selected primary agent. Install it on the domain controller (or to a member machine) to make it a high availability peer.

Cancel
Save

Step 2 In the Configure Agent dialog box, click **Save**.

Step 3 In the top right corner of the page, click **Save**.

The following figure shows an example.

You have unsaved changes Cancel Save

Configure Identity Sources

Select the service type and start configuring the identity source. Deploy the changes after you're finished.

Service Type:

☐ None
 ☐ Identity Services Engine
 ☒ Passive Identity Agent

! Your changes will be effective after you save Passive Identity Agent as the Identity Source.

Search by agent name or domain controller name Create Agent

Domain Controllers	Monitoring Agents	Hostname ⓘ	Connection Status ⓘ ⓘ
> bogus			
> forest.example.com			
forest.example.com	Primary (primary) Secondary (secondary)	192.0.2.110 192.0.2.111	

Note

The passive identity agent won't be active until you create a user and install the software.

What to do next

- See [Create a Secure Firewall Management Center User for the Passive Identity Agent](#), on page 16
- See [About Passive Identity Agent Installation](#), on page 19

About Passive Identity Agent Roles

The passive identity agent has the following roles:

- **Standalone:** A passive identity agent that is not part of a redundant pair. A standalone agent can read users and groups from multiple Active Directory servers and domain controllers, provided the software is installed on all of them.
- **Primary:** (Primary agent in a redundant pair.) Can be installed on a Microsoft AD domain controller, directory server, or any network client.

Handles all communication with the Secure Firewall Management Center unless it stops communicating, in which case communication is handled by secondary agents.

- **Secondary:** (Secondary, or backup, agent in a redundant pair.) Can be installed on a Microsoft AD domain controller, directory server, or any network client.

Monitors the health of the primary agent and takes over if the primary agent stops communicating with the Secure Firewall Management Center.

The can monitor several AD domain controllers that are part of the same domain.

Create a Secure Firewall Management Center User for the Passive Identity Agent

This task discusses how to create a Secure Firewall Management Center user with sufficient permissions to communicate with the passive identity agent. This user has limited privileges to perform other tasks; the user is expected only to enable communication with the passive identity agent.



Note Use *only* the **Passive Identity User** role for the passive identity agent user. In particular, *do not* use the **Administrator** role for the passive identity agent because **Administrator** will be logged off at a regular basis as the passive identity agent communicates with the Secure Firewall Management Center.

Before you begin

Complete the tasks discussed in [Create a Passive Identity Agent Identity Source](#), on page 10.



Note You *cannot* use external authentication with the Passive Identity Agent user.

Procedure

- Step 1** Log in to the Secure Firewall Management Center as an administrator.
- Step 2** Click **System** (🔑) > **Users** > **Users**.
- Step 3** Click **Create User**.
- Step 4** Create the user as discussed in [Add or Edit an Internal User](#) in the *Cisco Secure Firewall Management Center Administration Guide*.
- Step 5** Select the **Passive Identity User** role.

The following figure shows an example.

The screenshot displays the 'User Configuration' and 'User Role Configuration' sections of the Secure Firewall Management Center interface.

User Configuration

- User Name:
- Real Name:
- Email Address:
- Authentication: ☐ Use External Authentication Method
- Password:
- Confirm Password:
- Maximum Number of Failed Logins: (0 = Unlimited)
- Minimum Password Length:
- Days Until Password Expiration: (0 = Unlimited)
- Days Before Password Expiration Warning:
- Options:
 - ☐ Force Password Reset on Login
 - ☐ Check Password Strength
 - ☐ Exempt from Browser Session Timeout

User Role Configuration

Default User Roles:

- ☐ Administrator
- ☐ External Database User (Read Only)
- ☐ Security Analyst
- ☐ Security Analyst (Read Only)
- ☐ Security Approver
- ☐ Intrusion Admin
- ☐ Access Admin
- ☐ Network Admin
- ☐ Maintenance User
- ☐ Discovery Admin
- ☐ Threat Intelligence Director (TID) User
- ☒ Passive Identity User

Buttons:

Note

Do not choose a role for the passive identity agent user other than **Passive Identity User** because the agent will not function properly.

Step 6 Click **Save**.

What to do next

[About Passive Identity Agent Installation, on page 19.](#)

Troubleshoot the Passive Identity Agent

This topic discusses how you can troubleshoot the passive identity agent software on your Windows AD domain controller or directory server.

(Optional.) Set the log level

By default, the passive identity agent logs at the INFO level. To optionally change the log level, open **C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent\CiscoPassiveIdentityAgentService.exe.config** in a text editor, save the file, and restart the Cisco Passive Identity Agent service.

Do not rename the logging service

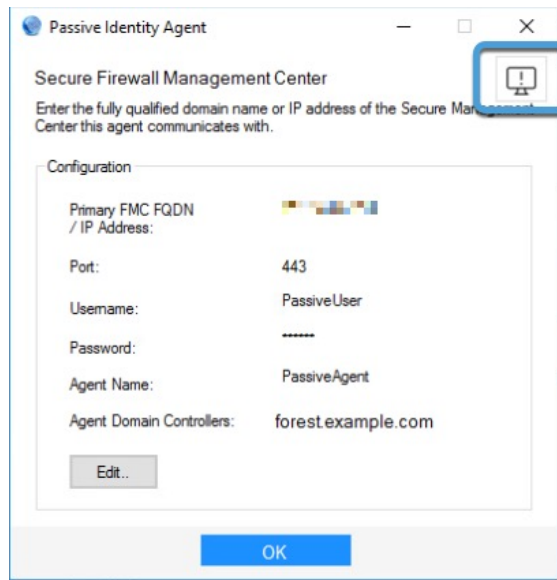
Do not rename **C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent\CiscoPassiveIdentityAgentService.exe.config**; otherwise, the passive identity agent will stop generating log files. Do not remove or change the **.exe.config** file extension.

Generate troubleshooting files

To generate a .zip containing troubleshooting files:

1. Log in to the Microsoft Active Directory domain controller.
2. Start the passive identity agent software.
3. Click the Troubleshooting button in the top right corner of the window.

The following figure shows an example.



A confirmation message is displayed.

Your troubleshoot logs are saved to your system's Downloads folder; the file name starts with **TroubleshootLogs**.

Manually view log files

Passive identity agent log files are stored in plain text format in the agent's installation directory: **C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent**.

Use Notepad or another text editor to view these files. Log files rotate after reaching 10MB in size.

Use the Microsoft Active Directory event viewer

In the event you are not seeing user sessions in the Secure Firewall Management Center, you can look on your Microsoft Active Directory server's event viewers for the following Kerberos-related events:

- 4770
- 4768

For general information about audit policy, see [Audit Policy Recommendations](#) on learn.microsoft.com.

For more information about Windows Group Policy Object settings, see [Group Policy Objects](#) on learn.microsoft.com.

About Passive Identity Agent Installation

The following topics discuss prerequisites and tasks required to install the passive identity agent.



Note We recommend you use the latest version of the passive identity agent. To see the available versions, go to software.cisco.com. To upgrade the passive identity agent, see [Upgrade the Passive Identity Agent Software](#), on page 28

Prerequisites to Installing the Passive Identity Agent

You must complete all of the following tasks before you install the passive identity agent software.

Passive Identity Agent System Requirements

Passive identity agent system requirements

The passive identity agent requires the following:

- If you install the passive identity agent on a Windows Active Directory server, the server must run Windows Server 2008 or later.
- If you install it on a Windows client attached to the domain, the client must run Windows 8 or later.
- The system clock on all systems must be synchronized. We strongly recommend using the same NTP servers on all of them. This means:
 - The Secure Firewall Management Center.
 - For more information, see [Time Synchronization](#).
 - All Windows Active Directory servers and domain controllers.
 - The machine on which the passive identity agent is installed.
- Secure Firewall Management Center must run 7.6 or later.
- Any Secure Firewall Threat Defense managed by the Secure Firewall Management Center must run 7.1 or later.
- You must enable Snort 3 on the Secure Firewall Threat Defense devices.

Enable the Windows Event Viewer to Log Kerberos Authentication Attempts

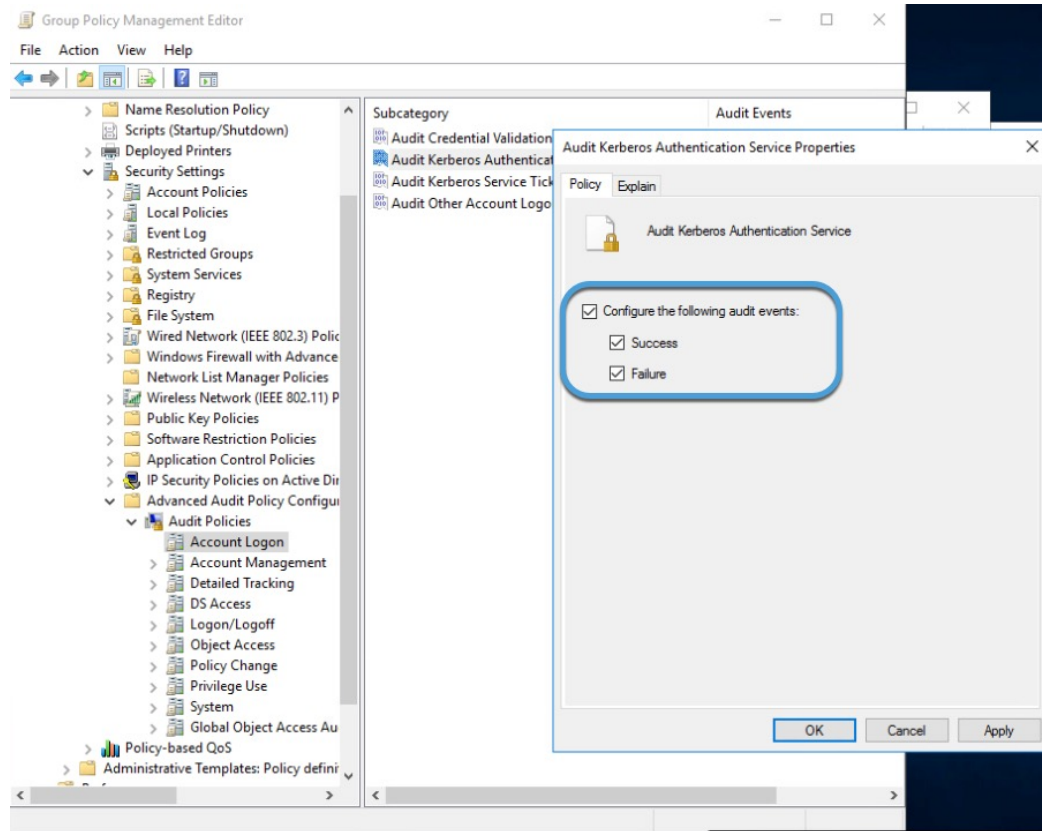
The following task shows how to configure Windows Group Policy Object (GPO) security settings to enable the Windows Event Viewer to log successful and unsuccessful Kerberos authentication attempts. The passive identity agent reads user sessions from the Event Viewer so this setting is required for the passive identity agent to function properly.

For more information, see [System audit policy recommendations](#) on learn.microsoft.com.

Procedure

-
- | | |
|---------------|---|
| Step 1 | Log in to the Active Directory Server as an administrator. |
| Step 2 | As Administrator, open a DOS command prompt. |
| Step 3 | Enter <code>gpmmc.msc</code> to start the Group Policy Management Editor. |

- Step 4** If necessary, create a new GPO; if one already exists, edit it.
- For more information about creating a GPO, see a resource like [Create a Group Policy Object](#) on [learn.microsoft.com](#).
- Step 5** In your GPO, expand **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Policy Configuration > Audit Policies**.
- Step 6** Click **Account Logon**.
- Step 7** In the right pane, double-click **Audit Kerberos Authentication Service**.
- Step 8** In the dialog box that is displayed, select all checkboxes which enables the system to log successes and failures.
- The following figure shows an example.



- Step 9** Follow the prompts on your screen to save the changes.
- Step 10** (Optional.) To update GPO immediately, enter **gpupdate /force** in your DOS command prompt window.

What to do next

See [Add the Active Directory User to Groups](#), on page 21.

Add the Active Directory User to Groups

Use this procedure to give the Active Directory and passive identity agent service user sufficient privileges to Active Directory.

To function normally, the passive identity agent must be able to connect to the domain and to read the Windows Event Log. This topic discusses how to give the proper privileges to:

- The passive identity agent service user.
- Active Directory user (namely, the **Directory Username** user in the Active Directory realm on the Secure Firewall Management Center).

Before you begin

You must be a Microsoft Server administrator familiar with how to add a user to a group and how to set a Windows service to run as a specific user.

Procedure

Step 1 Log in as an administrator to the system on which the passive identity agent is running.

You can log into any of the following:

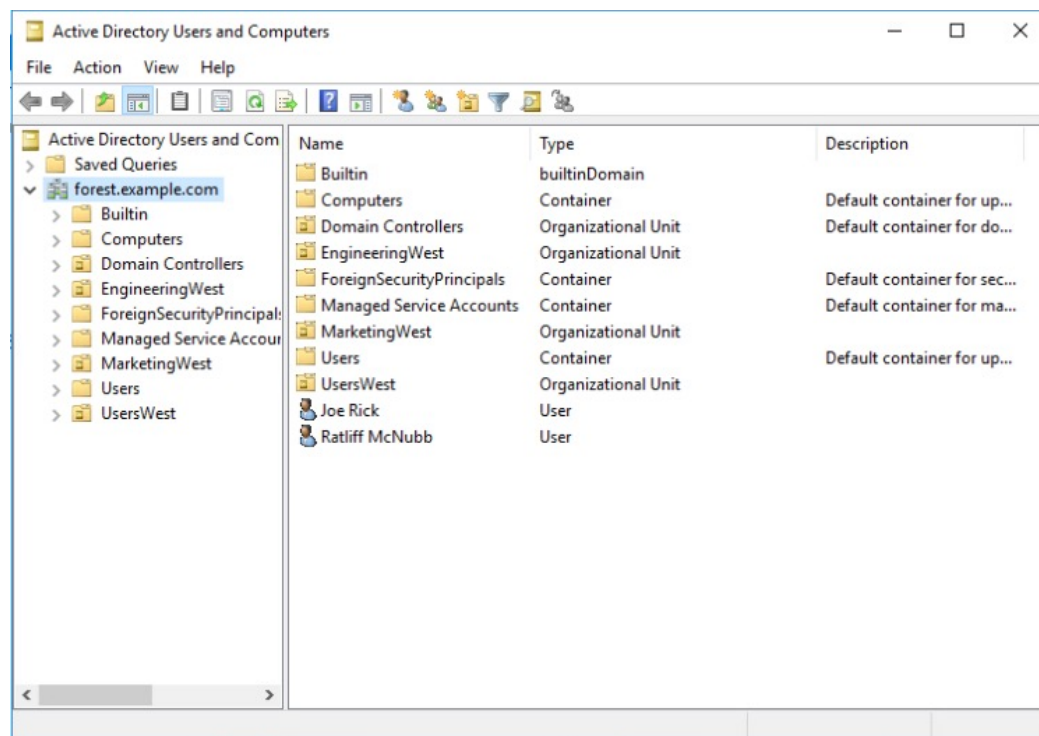
- The domain controller.
- The Active Directory server.

Step 2 Start the Server Manager.

Step 3 Click **Tools > Active Directory Users and Computers**.

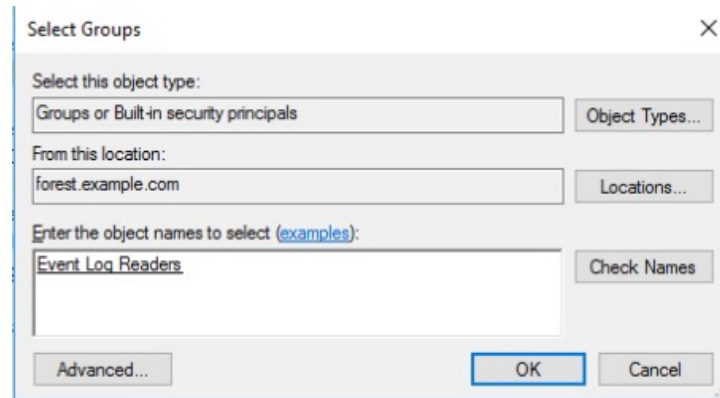
Step 4 Under Active Directory Users and Computers, expand the forest in which the directory user is defined.

The following figure shows an example.



- Step 5** Expand the organization unit or group to reveal the directory user. (You can create a new user by clicking **New > User**).
- Step 6** Right-click the directory user and click **Add to a group**.
- Step 7** In the Select Groups dialog box, enter **Event Log Readers** and click **Check Names**.

The following figure shows an example.



- Step 8** Repeat the preceding tasks to add the user to the Domain Users group.
- Step 9** In the Add Groups dialog box, click **OK**.

The directory user now has the appropriate permissions and the passive identity agent service runs as that user.

What to do next

See [Install the Passive Identity Agent Software, on page 23](#).

Install the Passive Identity Agent Software

This task discusses how to install the passive identity agent software. For a simple installation, you can install it on your Microsoft Active Directory (AD) domain controller; for other options, see [Deploy the Passive Identity Agent, on page 3](#).



Note We recommend you use the latest version of the passive identity agent. To see the available versions, go to software.cisco.com. To upgrade the passive identity agent, see [Upgrade the Passive Identity Agent Software, on page 28](#)

Before you begin

Complete all of these tasks:

- [Enable the Windows Event Viewer to Log Kerberos Authentication Attempts, on page 20](#)
- [Add the Active Directory User to Groups, on page 21](#)
- [Add Log On to the Passive Identity Agent Service, on page 26](#)

Procedure

- Step 1** Download the passive identity agent from software.cisco.com.
- Step 2** Log in as a member of the Administrators group to the machine on which to install the passive identity agent.
- Step 3** Double-click **CiscoPassiveIdentityAgentInstaller-1.1.msi**.
- Step 4** Click **Next**.
- Step 5** Choose a folder in which to install the passive identity agent and click **Next**.
The default installation folder is **Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent**.
- Step 6** Click **Next**.
- Step 7** Click **Install**.
- Step 8** When the installation is done, click **Finish** and optionally check the box to start the passive identity agent.
- Step 9** When the passive identity agent starts, click the **On-Prem** tab if you are using the agent with an on-premises Secure Firewall Management Center (physical or virtual) or click the **Cloud** tab if you are using the agent with Cloud-Delivered Firewall Management Center.
- Step 10** In the Cisco Passive Agent dialog box, enter the following information:

Item	Description
FMC FQDN / IP Address	Enter the address of the Secure Firewall Management Center on which you created the passive identity agent identity source. The passive identity agent version 1.0 supports IPv4 addresses and fully qualified domain names only. Version 1.1 supports IPv4, IPv6, and fully qualified domain names.
Port	Enter the Secure Firewall Management Center listen port (by default, 443).
Username	Enter the username of the user you created in Create a Secure Firewall Management Center User for the Passive Identity Agent , on page 16.
Password	Enter the user's password.
Agent	Click the list to locate the domain controller of the passive identity agent you created previously on the Secure Firewall Management Center.

The following figure shows an example.

The screenshot shows the 'Cisco Passive Identity Agent 1.1.0-1' configuration window. The title bar includes standard window controls. The main content area is titled 'Secure Firewall Management Center' and contains the instruction: 'Enter the fully qualified domain name or IP address of the Secure Management Center this agent communicates with.' Below this, there is an 'Integration' section with two buttons: 'On-Prem' (selected) and 'Cloud'. The 'On-Prem' section includes fields for 'Primary FMC FQDN / IP address' (containing '192.0.2.100') and 'Port' (containing '443'), with a label 'The FMC FQDN or IP address and port' below them. There are also fields for 'Username' (containing 'IdentityAgent') and 'Password' (masked with dots and an eye icon), with a label 'The credentials for the connection (Primary or Secondary)' below them. A dropdown menu is labeled 'Agent' with the text 'Select Agent to DCs pair' and a downward arrow. Below the dropdown is a 'Test' button. At the bottom, there is a link 'I have Secondary FMC' with a downward arrow, and two large buttons: 'Save' (blue) and 'Cancel' (gray).

Step 11 Click the **Agent** list.

Step 12 From the list, click the name of the domain controller to monitor.

Step 13 Click **Test**.

The following figure shows an example.

Add Log On to the Passive Identity Agent Service

Cisco Passive Identity Agent 1.1.0-1

Secure Firewall Management Center

Enter the fully qualified domain name or IP address of the Secure Management Center this agent communicates with.

Integration

On-Prem Cloud

Primary FMC FQDN / IP address : Port

192.0.2.100 : 443

FMC FQDN or IP address and Port of the FMC

Username Password

IdentityAgent

The credentials for the connection (Primary or Secondary)

Agent	DCs (Domain Controllers)
Standalone	forest.example.com

You need to select Agent-DCs pair to be able to save configuration

Tested successfully Primary FMC was tested successfully.

I have Secondary FMC

Save Cancel

- Step 14** If you have a high availability pair, click **I have Secondary FMC** and enter the secondary's IP address or fully qualified host name and its listen port.
- Step 15** Only if the test succeeds, click **Save**.

What to do next

See [Add Log On to the Passive Identity Agent Service, on page 26](#).

Add Log On to the Passive Identity Agent Service

Use this procedure to enable the passive identity agent service to run as the Active Directory user. (Namely, the **Directory Username** user in the Active Directory realm on the Secure Firewall Management Center).

This task is optional but recommended so the passive identity agent service runs with the minimal permissions required to send login information to the Secure Firewall Management Center

Before you begin

Complete the tasks discussed in [Add the Active Directory User to Groups, on page 21](#).

You must be a Microsoft Server administrator familiar with how to add a user to a group and how to set a Windows service to run as a specific user.

Procedure

- Step 1** Log in as an administrator to the system on which the passive identity agent is running.
- You can log into any of the following:
- The domain controller.
 - The Active Directory server.
- Step 2** In the Windows search bar, enter **Services**.
- Step 3** In the Services window, right-click **Cisco Passive Identity Agent**.
- Step 4** Click **Properties**.
- Step 5** In the Properties dialog box, click the **Log On** tab.
- Step 6** Click **This account**.
- Step 7** Click **Browse** and follow the prompts on your screen to select the directory user.
- Step 8** Enter the user's password in the provided fields.
- Step 9** Click **Apply**.
-

What to do next

- Specify users to control and other options using an identity policy as described in [Create an Identity Policy](#).
- Associate the identity rule with an access control policy, which filters and optionally inspects traffic, as discussed in [Associating Other Policies with Access Control](#).
- Deploy your identity and access control policies to managed devices as discussed in [Deploy Configuration Changes](#).
- Monitor user activity as discussed in *Using Workflows* in the [Cisco Secure Firewall Management Center Administration Guide](#).

Uninstall the Passive Identity Agent Software

This task discusses how to uninstall the passive identity agent software from your Microsoft AD servers.

Procedure

- Step 1** Log in as an administrator to the machine on which the passive identity agent is installed.
- Step 2** Search for Add or Remove Programs.
- Step 3** Click **Cisco Passive Identity Agent**.

Step 4 Click **Uninstall**.

Step 5 You are required to confirm the uninstallation.

Upgrade the Passive Identity Agent Software

To upgrade to a newer version of the passive identity agent, you must uninstall the earlier version then install the later version.

See the following information:

- [Uninstall the Passive Identity Agent Software, on page 27](#)
- [About Passive Identity Agent Installation, on page 19](#)

Monitor the Passive Identity Agent

The passive identity agent indicates whether or not it can communicate with the Secure Firewall Management Center and other agents if it's configured as primary-secondary. You can view the status at **Integration > Other Integrations > Identity Sources**.

Deployments






A standalone passive identity agent is represented as follows.



A primary-secondary pair is represented as follows.






The following table explains the meaning of the indicators.

Object	Meaning
	Secure Firewall Management Center
	Standalone Passive Identity Agent
	Active Directory domain controller
	Primary agent
	Secondary agent

Status indicators and colors

The passive identity agent indicates status using lines (that indicate whether communication with the Secure Firewall Management Center is active or standby) and colors (that indicate whether or not communication is successful).

The following table shows the meanings of lines and colors:

Object	Meaning
Solid line	The agent that is responsible for communicating with the Secure Firewall Management Center.
Dashed line	Primary/secondary configuration only. The agent that is acting as the backup agent. In the event of a communication failure between the active (solid line) agent, this agent communicates with the Secure Firewall Management Center.
Blue 	Agent communication is normal.
Amber 	Agent has never successfully communicated with the Secure Firewall Management Center. A newly created agent line is amber and remains so until configuration is complete.
Red 	Communication is failing. To resolve the issues: <ul style="list-style-type: none"> • Check sure the network connections between agents and the Secure Firewall Management Center. • Make sure you have completed configuring the system (Microsoft AD server, domain controllers, and the Secure Firewall Management Center). For more information, see How to Create a Passive Identity Agent Identity Source , on page 8.

Manage the Passive Identity Agent

The following topics discuss how to edit or delete passive identity agents you previously configured on the Secure Firewall Management Center.

Related Topics

[Edit Passive Identity Agents](#), on page 30

[Delete a Standalone Passive Identity Agent](#), on page 30

[Delete Primary and Secondary Passive Identity Agents](#), on page 30

[Uninstall the Passive Identity Agent Software](#), on page 27

Edit Passive Identity Agents

This task discusses how to edit passive identity agents you previously configured in the Secure Firewall Management Center.

Procedure

- Step 1** Log in to the Secure Firewall Management Center as an administrator.
 - Step 2** Click **Integration > Other Integrations > Identity Sources**.
 - Step 3** Click **Passive Identity Agent**.
 - Step 4** Click **Edit** (✎) next to the agent to edit.
 - Step 5** Make the desired changes.
 - Step 6** Click **Save**.
-

Delete a Standalone Passive Identity Agent

This task discusses how to delete a standalone passive identity agent.

Procedure

- Step 1** Log in to the Secure Firewall Management Center as an administrator.
 - Step 2** Click **Integration > Other Integrations > Identity Sources**.
 - Step 3** Click **Passive Identity Agent**.
 - Step 4** Click **Edit** (✎) next to the agent to delete.
 - Step 5** Click **Delete**.
 - Step 6** You are required to confirm the action.
-

Delete Primary and Secondary Passive Identity Agents

This task discusses how to delete primary and secondary passive identity agents. You must delete a secondary agent before you can delete a primary agent.

Procedure

- Step 1** Log in to the Secure Firewall Management Center as an administrator.
- Step 2** Click **Integration > Other Integrations > Identity Sources**.
- Step 3** Click **Passive Identity Agent**.
- Step 4** Click **Edit** (✎) next to a secondary agent to delete.

- Step 5** Click **Delete**.
- Step 6** You are required to confirm the action.
- Step 7** If you wish to delete a primary agent, first delete all secondary agents.
-

Troubleshoot the Passive Identity Agent

This topic discusses how you can troubleshoot the passive identity agent software on your Windows AD domain controller or directory server.

(Optional.) Set the log level

By default, the passive identity agent logs at the INFO level. To optionally change the log level, open **C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent\CiscoPassiveIdentityAgentService.exe.config** in a text editor, save the file, and restart the Cisco Passive Identity Agent service.

Do not rename the logging service

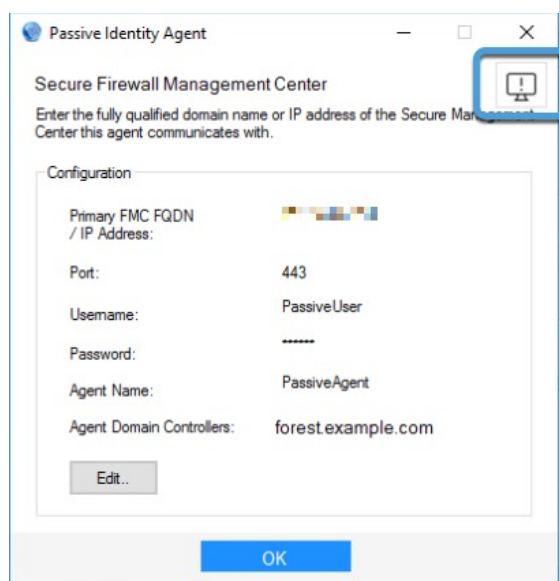
Do not rename **C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent\CiscoPassiveIdentityAgentService.exe.config**; otherwise, the passive identity agent will stop generating log files. Do not remove or change the **.exe.config** file extension.

Generate troubleshooting files

To generate a .zip containing troubleshooting files:

1. Log in to the Microsoft Active Directory domain controller.
2. Start the passive identity agent software.
3. Click the Troubleshooting button in the top right corner of the window.

The following figure shows an example.



A confirmation message is displayed.

Your troubleshoot logs are saved to your system's Downloads folder; the file name starts with **TroubleshootLogs**.

Manually view log files

Passive identity agent log files are stored in plain text format in the agent's installation directory: **C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent**.

Use Notepad or another text editor to view these files. Log files rotate after reaching 10MB in size.

Use the Microsoft Active Directory event viewer

In the event you are not seeing user sessions in the Secure Firewall Management Center, you can look on your Microsoft Active Directory server's event viewers for the following Kerberos-related events:

- [4770](#)
- [4768](#)

For general information about audit policy, see [Audit Policy Recommendations](#) on learn.microsoft.com.

For more information about Windows Group Policy Object settings, see [Group Policy Objects](#) on learn.microsoft.com.

Security Requirements for the Passive Identity Agent

To safeguard the system, you should install the passive identity agent on a protected internal network. Although the passive identity agent is configured to have only the necessary services and ports available, you must make sure that attacks cannot reach it.

If the passive identity agent and the Secure Firewall Management Center reside on the same network, you can connect the Secure Firewall Management Center to the same protected internal network as the passive identity agent.

Regardless of how you deploy your appliances, inter-system communication is encrypted. However, you must still take steps to ensure that communications between appliances cannot be interrupted, blocked, or tampered with; for example, with a distributed denial of service (DDoS) or man-in-the-middle attack.

Internet Access Requirements for the Passive Identity Agent

By default, the passive identity agent is configured to communicate with the Firepower System over the internet using HTTPS on port 443/tcp (HTTPS). If you do not want the passive identity agent to have direct access to the internet, you can configure a proxy server.

The following information informs you of the ports the passive identity agent use to communicate with each other, with the Secure Firewall Management Center, and with Microsoft Active Directory.

Table 1: Passive Identity Agent port requirements

Port	Reason
443	Communicate with the Secure Firewall Management Center.
135	Communicate with Microsoft Active Directory using the MSRPC protocol.
9095	Communicate with each other using the UDP protocol.

History for the Passive Identity Agent

Table 2: History for the Passive Identity Agent

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Passive Identity Agent	7.6	7.1	<p>This feature is introduced.</p> <p>Passive Identity Agent version 1.1 is compatible with 7.6.0 and later and adds the following:</p> <ul style="list-style-type: none"> • You can use either FQDN, IPv4, or IPv6 to connect from the Passive Identity Agent to the Secure Firewall Management Center or Cisco Security Cloud Control. • Sends both IPv4 and IPv6 user sessions from Microsoft Active Directory (AD) to the Firewall Management Center. • You can zip troubleshooting logs. • When you start the Passive Identity Agent software, a list of prerequisites is displayed. <p>The Passive Identity Agent identity source sends session data from Microsoft Active Directory (AD) to the Firewall Management Center. Passive identity agent software is supported on:</p> <ul style="list-style-type: none"> • Microsoft AD server (Windows Server 2008 or later) • Microsoft AD domain controller (Windows Server 2008 or later) • Any client connected to the domain you want to monitor (Windows 8 or later)