Active Directory as a Probe and a Provider

Active Directory (AD) is a highly secure and precise source from which to receive user identity information, including user name, IP address, and domain name.

By configuring the Active Directory probe you can also then quickly configure and enable these other probes (which also use Active Directory as their source):

- Active Directory Agents

Note The Active Directory agents are only supported on Windows Server 2008 and higher.

- SPAN
- Endpoint Probe

In addition, configure the Active Directory probe in order to use AD user groups when collecting user information. You can use AD user groups for the AD, Agents, SPAN, and Syslog probes. For more information about AD groups, see Configure Active Directory User Groups, on page 6.

- Work with Active Directory, on page 1
- Active Directory Settings, on page 10

Work with Active Directory

Before you configure the Active Directory probe for Passive Identity services, make sure that:

- The Microsoft Active Directory server does not reside behind a network address translator and does not have a Network Address Translation (NAT) address.
- The Microsoft Active Directory account intended for the join operation is valid and is not configured with the Change Password on Next Login.
- Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from ISE-PIC. For more information, see DNS Server.
- Synchronize clock settings for the NTP servers. For more information, see Specify System Time and Network Time Protocol Server Settings.

Note If you see operational issues when Cisco ISE-PIC is connected to Active Directory, see the AD Connector Operations Report under **Reports**. For more information, see Available Reports.

Getting Started with the PassiveID Setup

ISE-PIC offers a wizard from which you can easily and quickly configure Active Directory as your first user identity provider, in order to receive user identities from Active Directory. By configuring Active Directory for ISE-PIC, you also simplify the process for configuring other provider types later on. Once you have configured Active Directory, you must then configure a Subscriber (such as Cisco Firepower Management Center (FMC) or Stealthwatch), in order to define the client that is to receive the user data.

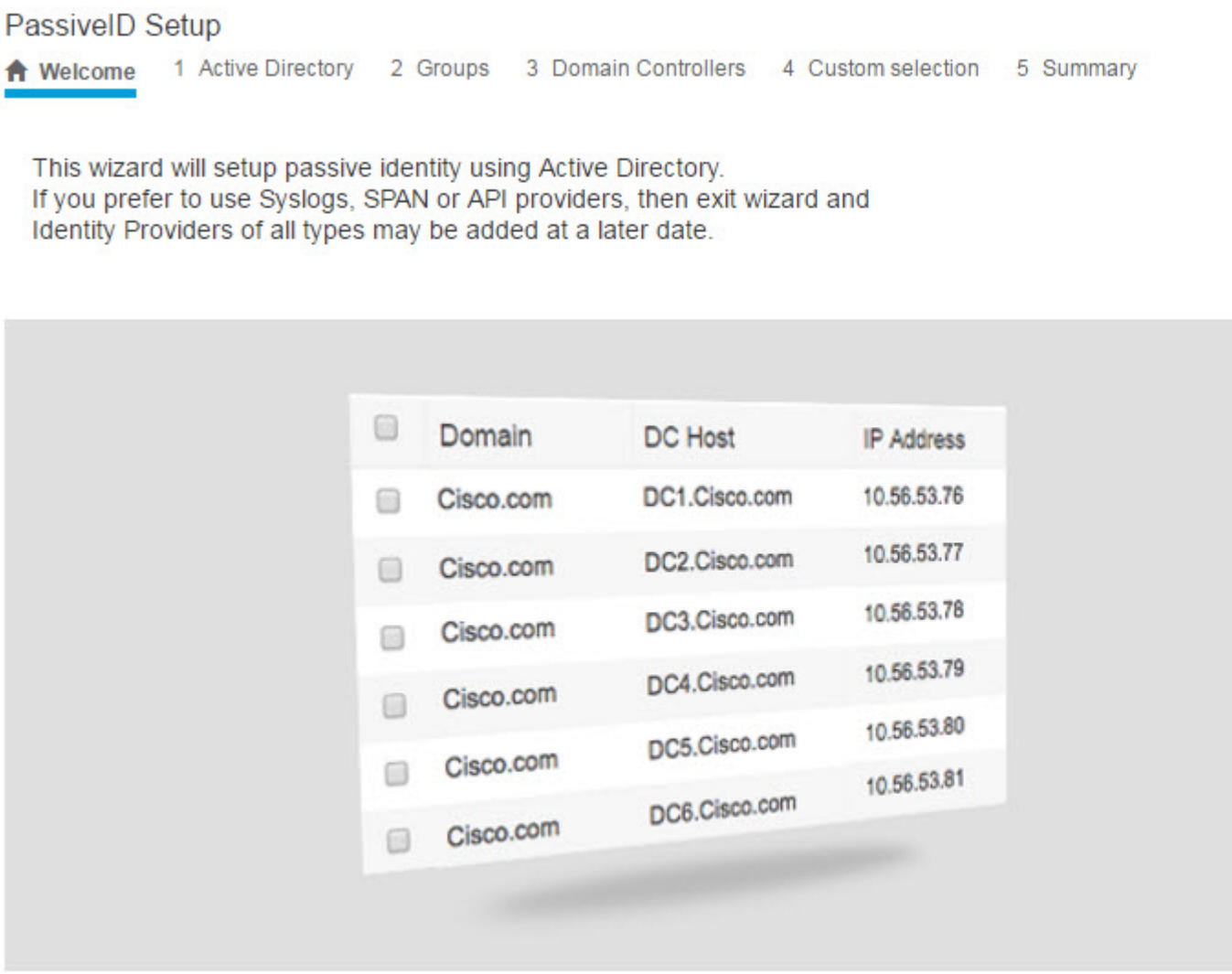
Before you begin

- Ensure the Microsoft Active Directory server does not reside behind a network address translator and does not have a Network Address Translation (NAT) address.
- Ensure the Microsoft Active Directory account intended for the join operation is valid and is not configured with the Change Password on Next Login.
- Ensure that ISE-PIC has an entry in the domain name server (DNS). Ensure you have properly configured reverse lookup for the client machine from ISE-PIC. For more information, see DNS Server

Step 1 Choose **Home** > **Introduction**. From the Passive Identity Connector Overview screen, click **Passive Identity Wizard**.

The PassiveID Setup opens:

Figure 1: The PassiveID Setup



Step 2 Click **Next** to begin the wizard.

Step 3 Enter a unique name for this Active Directory join point. Enter the domain name for the Active Directory Domain to which this node is connected, and enter your Active Directory administrator user name and password.

Your administrator's user name and password will be saved in order to be used for all Domain Controllers (DC) that are configured for monitoring.

Step 4 Click **Next** to define Active Directory groups and check any user groups to be included and monitored.
The Active Directory user groups automatically appear based on the Active Directory join point you configured in the previous step.

Step 5 Click **Next**. Select the DCs to be monitored. If you choose Custom, then from the next screen select the specific DCs for monitoring. When finished, click **Next**.

Step 6 Click **Exit** to complete the wizard.

What to do next

When you finish configuring Active Directory as your initial provider, you can easily configure additional provider types as well. For more information, see Providers. Furthermore, you can now also configure a subscriber, designated to receive the user identity information that is collected by any of the providers you have defined.

Set Up an Active Directory (WMI) Probe Step-by-Step

To configure Active Directory and WMI for Passive Identity services, use the Getting Started with the PassiveID Setup, on page 2 or follow the steps in this chapter as follows:

1. Configure the Active Directory probe. See Add an Active Directory Join Point and Join Cisco ISE-PIC Node to the Join Point, on page 4.
2. Create a list of Active Directory Domain Controllers for the WMI-configured node (or nodes) that receives AD login events.
3. Configure the Active Directory in order for it to integrate with ISE-PIC.
4. (Optional) Manage the Active Directory Provider, on page 7.

Add an Active Directory Join Point and Join Cisco ISE-PIC Node to the Join Point

Before you begin

Ensure that the Cisco ISE-PIC node can communicate with the networks where the NTP servers, DNS servers, domain controllers, and global catalog servers are located.

Join points must be created in order to work with Active Directory as well as with the Agent, Syslog, SPAN and Endpoint probes .

If you want to use IPv6 when integrating with Active Directory, then you must ensure that you have configured an IPv6 address for the relevant ISE-PIC nodes.

If you use the Google Chrome browser and have ad blocking software enabled, you must disable the ad blocker. This task contains Cisco ISE GUI elements that are affected by ad blockers. Alternatively, you can carry out this task in a Google Chrome Incognito browser.

Step 1 Choose **Providers** > **Active Directory**.

Step 2 Click **Add** and enter the domain name and identity store name from the **Active Directory Join Point Name** settings.

Step 3 Click **Submit**.

A pop-up appears asking if you want to join the newly created join point to the domain. Click **Yes** if you want to join immediately.

If you clicked **No**, then saving the configuration saves the Active Directory domain configuration globally , but none of the Cisco ISE-PIC nodes are joined to the domain yet.

Step 4 Check the check box next to the new Active Directory join point that you created and click **Edit**. The deployment join/leave table is displayed with all the Cisco ISE-PIC nodes, the node roles, and their status.

Step 5 In case the join point was not joined to the domain during Step 3, check the check box next to the relevant Cisco ISE-PIC nodes and click **Join** to join the Cisco ISE-PIC node to the Active Directory domain.

You must do this explicitly even though you saved the configuration. To join multiple Cisco ISE-PIC nodes to a domain in a single operation, the username and password of the account to be used must be the same for all join operations. If different username and passwords are required to join each Cisco ISE-PIC node, the join operation should be performed individually for each Cisco ISE-PIC node.

Step 6 Enter the Active Directory username and password in the **Join Domain** dialog box.

Your administrator's user name and password will be saved in order to be used for all Domain Controllers (DC) that are configured for monitoring.

The user used for the join operation should exist in the domain itself. If it exists in a different domain or subdomain, the username should be noted in a UPN notation, such as jdoe@acme.com.

Step 7 (Optional) Check the **Specify Organizational Unit** check box.

You should check this check box in case the Cisco ISE-PIC node machine account is to be located in a specific Organizational Unit other than CN=Computers,DC=someDomain,DC=someTLD. Cisco ISE-PIC creates the machine account under the specified organizational unit or moves it to this location if the machine account already exists. If the organizational unit is not specified, Cisco ISE-PIC uses the default location. The value should be specified in full distinguished name (DN) format. The syntax must conform to the Microsoft guidelines. Special reserved characters, such as /'+,;=<> line feed, space, and carriage return must be escaped by a backslash (\). For example, OU=Cisco ISE\,US,OU=IT Servers,OU=Servers\, and Workstations,DC=someDomain,DC=someTLD. If the machine account is already created, you need not check this check box. You can also change the location of the machine account after you join to the Active Directory domain.

Step 8 Click **OK**.

You can select more than one node to join to the Active Directory domain.

If the join operation is not successful, a failure message appears. Click the failure message for each node to view detailed logs for that node.

Note the following points while configuring the join points:

- When using multiple join points, if alternate UPN suffix is configured only for a single join point or domain, identity lookup is performed only in that join point or domain. Authentication might fail in such cases. As a workaround, you can configure the alternate UPN suffix for all the joint points or domains.
- You can only add up to 200 Domain Controllers on ISE. On exceeding the limit, you will receive the error "Error creating <*DC FQDN*> - Number of DCs Exceeds allowed maximum of 200". For more information on the tested scale limit of domain controllers for deployment, see Performance and Scalability Guide for Cisco Identity Services Engine.
- When the join is complete, Cisco ISE-PIC updates its AD groups and corresponding security identifiers (SIDs). Cisco ISE-PIC automatically starts the SID update process. You must ensure that this process is allowed to complete.

- You might not be able to join Cisco ISE-PIC with an Active Directory domain if the DNS service (SRV) records are missing (the domain controllers do not advertise their SRV records for the domain that you are trying to join to).
- We recommended that you rejoin AD after a designated maintenance window. This ensures that the AD cache is refreshed with the most recent updates.

Add Domain Controllers

Step 1 Choose **Providers** > **Active Directory**.

Step 2 Check the check box next to the Active Directory join point that you created and click **Edit**. The deployment join/leave table is displayed with all the Cisco ISE-PIC nodes, the node roles, and their statuses.

Step 3 **Note** To add a new Domain Controller (DC) for Passive Identity services, you need the login credentials of that DC.

Go to the PassiveID tab and click **Add DCs**.

Step 4 Check the check box next to the domain controllers that you would like to add to the join point for monitoring and click **OK**.
The domain controllers appear in the Domain Controllers list of the PassiveID tab.

Step 5 Configure the domain controller:

a) Checkmark the domain controller and click **Edit**. The **Edit Item** screen appears.
b) Optionally, edit the different domain controller fields.

The DC failover mechanism is managed based on the DC priority list, which determines the order in which the DCs are selected in case of failover. If a DC is offline or not reachable due to some error, its priority is decreased in the priority list. When the DC comes back online, its priority is adjusted accordingly (increased) in the priority list.

Configure Active Directory User Groups

Configure Active Directory user groups for them to be available for use when working with different probes that collect user identity information from Active Directory. Internally, Cisco ISE uses security identifiers (SIDs) to help resolve group name ambiguity issues and to enhance group mappings. SID provides accurate group assignment matching.

Step 1 Choose **Providers** > **Active Directory**. Click the join point for which you would like to add groups.

Step 2 Click the **Groups** tab.

Step 3 Do one of the following:

a) Choose **Add** > **Select Groups From Directory** to choose an existing group.
b) Choose **Add** > **Add Group** to manually add a group. You can either provide both group name and SID or provide only the group name and press **Fetch SID**.

Do not use double quotes (”) in the group name for the user interface login.

Step 4 If you are manually selecting a group, you can search for them using a filter. For example, enter **admin*** as the filter criteria and click **Retrieve Groups** to view user groups that begin with admin. You can also enter the asterisk (*) wildcard character to filter the results. You can retrieve only 500 groups at a time.

Step 5 Check the check boxes next to the groups that you want to be available for use in authorization policies and click **OK**.

Step 6 If you choose to manually add a group, enter a name and SID for the new group.

Step 7 Click **OK**.

Step 8 Click **Save**.

Note If you delete a group and create a new group with the same name as original, you must click **Update SID Values** to assign new SID to the newly created group. After an upgrade, the SIDs are automatically updated after the first join.

Manage the Active Directory Provider

Once you have created and configured your Active Directory join points, continue to manage the Active Directory probe with these tasks:

- Test Users for Active Directory Groups, on page 7
- View Active Directory Joins for a Node, on page 8
- Diagnose Active Directory Problems, on page 8
- Leave the Active Directory Domain, on page 9
- Delete Active Directory Configurations, on page 9
- Enable Active Directory Debug Logs, on page 10

Test Users for Active Directory Groups

The Test User tool can be used to verify user groups from Active Directory. You can run the test for a single join point or for scopes.

Step 1 Choose **Providers** > **Active Directory**.

Step 2 Choose one of the following options:

- To run the test on all join points, choose **Advanced Tools** > **Test User for All Join Points**.
- To run the test for a specific join point, select the joint point and click **Edit**. Select the Cisco ISE-PIC node and click **Test User**.

Step 3 Enter the username and password of the user (or host) in Active Directory.

Step 4 Choose the authentication type. Password entry in Step 3 is not required if you choose the Lookup option.

Step 5 Select the Cisco ISE-PIC node on which you want to run this test, if you are running this test for all join points.

Step 6 Check the Retrieve Groups and Attributes check boxes to retrieve the groups from Active Directory.

Step 7 Click **Test**.
The result and steps of the test operation are displayed. The steps can help to identify the failure reason and troubleshoot.

You can also view the time taken (in milliseconds) for Active Directory to perform each processing step. Cisco ISE-PIC displays a warning message if the time taken for an operation exceeds the threshold.

View Active Directory Joins for a Node

You can use the **Node View** button on the **Active Directory** page to view the status of all Active Directory join points for a given Cisco ISE-PIC node or a list of all join points on all Cisco ISE-PIC nodes.

Step 1 Choose **Providers** > **Active Directory**.

Step 2 Click **Node View**.

Step 3 Select a node from the **ISE Node** drop-down list.
The table lists the status of Active Directory by node. If there are multiple join points and multiple Cisco ISE-PIC nodes in a deployment, this table may take several minutes to update.

Step 4 Click the join point **Name** link to go to that Active Directory join point page and perform other specific actions.

Step 5 Click the link in the **Diagnostic Summary** column to go to the **Diagnostic Tools** page to troubleshoot specific issues.
The diagnostic tool displays the latest diagnostics results for each join point per node.

Diagnose Active Directory Problems

The Diagnostic Tool is a service that runs on every Cisco ISE-PIC node. It allows you to automatically test and diagnose the Active Directory deployment and execute a set of tests to detect issues that may cause functionality or performance failures when Cisco ISE-PIC uses Active Directory.

There are multiple reasons for which Cisco ISE-PIC might be unable to join or authenticate against Active Directory. This tool helps ensure that the prerequisites for connecting Cisco ISE-PIC to Active Directory are configured correctly. It helps detect problems with networking, firewall configurations, clock sync, user authentication, and so on. This tool works as a step-by-step guide and helps you fix problems with every layer in the middle, if needed .

Step 1 Choose **Providers** > **Active Directory**.

Step 2 Click the **Advanced Tools** drop-down and choose **Diagnostic Tools**.

Step 3 Select a Cisco ISE-PIC node to run the diagnosis on.

If you do not select a Cisco ISE-PIC node then the test is run on all the nodes.

Step 4 Select a specific Active Directory join point.

If you do not select an Active Directory join point then the test is run on all the join points.

Step 5 You can run the diagnostic tests either on demand or on a scheduled basis.

- To run tests immediately, choose **Run Tests Now**.
- To run the tests at an scheduled interval, check the **Run Scheduled Tests** check box and specify the start time and the interval (in hours, days, or weeks) at which the tests must be run. When this option is enabled, all the diagnostic tests are run on all the nodes and instances and the failures are reported in the **Alarms** dashlet in the **Home** dashboard.

Step 6 Click **View Test Details** to view the details for tests with Warning or Failed status.
This table allows you to rerun specific tests, stop running tests, and view a report of specific tests.

Leave the Active Directory Domain

If you no longer need to use this Active Directory domain or this join point to collect user identities, you can leave the Active Directory domain.

When you reset the Cisco ISE-PIC application configuration from the command-line interface or restore configuration after a backup or upgrade, it performs a leave operation, disconnecting the Cisco ISE-PIC node from the Active Directory domain, if it is already joined. However, the Cisco ISE-PIC node account is not removed from the Active Directory domain. We recommend that you perform a leave operation from the Admin portal with the Active Directory credentials because it also removes the node account from the Active Directory domain. This is also recommended when you change the Cisco ISE-PIC hostname.

Step 1 Choose **Providers** > **Active Directory**.

Step 2 Check the checkbox next to the Active Directory join point that you created and click **Edit**. The deployment join/leave table is displayed with all the Cisco ISE-PIC nodes, the node roles, and their statuses.

Step 3 Check the checkbox next to the Cisco ISE-PIC node and click **Leave**.

Step 4 Enter the Active Directory username and password, and click **OK** to leave the domain and remove the machine account from the Cisco ISE-PIC database.

If you enter the Active Directory credentials, the Cisco ISE-PIC node leaves the Active Directory domain and deletes the Cisco ISE-PIC machine account from the Active Directory database.

Note To delete the Cisco ISE-PIC machine account from the Active Directory database, the Active Directory credentials that you provide here must have the permission to remove machine account from domain.

Step 5 If you do not have the Active Directory credentials, check the **No Credentials Available** checkbox, and click **OK**.

If you check the **Leave domain without credentials** checkbox, the primary Cisco ISE-PIC node leaves the Active Directory domain. The Active Directory administrator must manually remove the machine account that was created in Active Directory during the time of the join.

Delete Active Directory Configurations

You should delete Active Directory configurations if you are not going to use the specific Active Directory configuration as a probe. Do not delete the configuration if you want to join another Active Directory domain. You can leave the domain to which you are currently joined and join a new domain. Do not delete the configuration if it is the only configuration in ISE-PIC

Before you begin

Ensure that you have left the Active Directory domain.

Step 1 Choose **Providers** > **Active Directory**.

Step 2 Check the checkbox next to the configured Active Directory.

Step 3 Check and ensure that the Local Node status is listed as Not Joined.

Step 4 Click **Delete**.

You have removed the configuration from the Active Directory database. If you want to use Active Directory at a later point in time, you can resubmit a valid Active Directory configuration.

Enable Active Directory Debug Logs

Active Directory debug logs are not logged by default. Enabling Active Directory debug logs may affect ISE-PIC performance.

Step 1 Choose **Administration** > **Logging** > **Debug Log Configuration**.

Step 2 Click the radio button next to the Cisco ISE-PIC node from which you want to obtain Active Directory debug information, and click **Edit**.

Step 3 Click the **Active Directory** radio button, and click **Edit**.

Step 4 Choose **DEBUG** from the drop-down list next to Active Directory. This will include errors, warnings, and verbose logs. To get full logs, choose **TRACE**.

Step 5 Click **Save**.

Active Directory Settings

Active Directory (AD) is a highly secure and precise source from which to receive user information, including user name and IP address.

To create and manage Active Directory probes by creating and editing join points, choose **Providers** > **Active Directory**.

For more information, see Add an Active Directory Join Point and Join Cisco ISE-PIC Node to the Join Point, on page 4.

Choose **Providers** > **Active Directory** and then check the join point you wish to edit and click **Edit**. For the Join Domain screen, choose **Providers** > **Active Directory**, check the join point you wish to edit and click **Join**.

Table 1: Active Directory Join Point Name Settings and Join Domain Window

Field Name	Description
Join Point Name	A unique name that distinguishes this configured join point quickly and easily.
Active Directory Domain	The domain name for the Active Directory Domain to which this node is connected.
Domain Administrator	This is the user principal name or the user account name for the Active Directory user with administrator priveleges.
Password	This is the domain administrator's password as configured in Active Directory.

Field Name	Description
Specifiy Organizational Unit	Enter the administrator's organizational unit information
Store Credentials	Your administrator's user name and password will be saved in order to be used for all Domain Controllers (DC) that are configured for monitoring. For the Endpoint probe, you must choose **Store credentials**.

Choose **Providers** > **Active Directory**.

Table 2: Active Directory Join/Leave Window

Field Name	Description
ISE Node	The URL for the specific node in the installation.
ISE Node Role	Indicates whether the node is the Primary or Secondary node in the installation.
Status	Indicates whether the node is actively joined to the Active Directory domain.
Domain Controller	For nodes that are joined to Active Directory, this column indicates the specific Domain Controller to which the node is connected in the Active Directory Domain.
Site	Only relevant for a full ISE installation. For more information, see Upgrading ISE-PIC to a Full ISE Installation.

Table 3: Passive ID Domain Controllers (DC) List

Field	Description
Domain	The fully qualified domain name of the server on which the domain controller is located.
DC Host	The host on which the domain controller is located.
Site	Only relevant for a full ISE installation. For more information, see Upgrading ISE-PIC to a Full ISE Installation.
IP Address	The IP address of the domain controller.
Monitor Using	Monitor Active Directory domain controllers for user identity information by one of these methods: • WMI: Monitor Active Directory directly with the WMI infrastructure. • Agent name: If you have defined agents to monitor Active Directory for user information, select the Agent protocol and choose the agent from the dropdown list that you would like to use. For more information about agents, see Active Directory Agents.

Table 4: Passive ID Domain Controllers (DC) Edit Window

Field Name	Description
Host FQDN	Enter the fully qualified domain name of the server on which the domain controller is located.
Description	Enter a unique description for this domain controller in order to easily identiy it.
User Name	The administrator's user name for accessing Active Directory.
Password	The administrator's password for accessing Active Directory.
Protocol	Monitor Active Directory domain controllers for user identity information by one of these methods: • WMI: Monitor Active Directory directly with the WMI infrastructure. • Agent name: If you have defined agents to monitor Active Directory for user information, select the Agent protocol and choose the agent from the dropdown list that you would like to use. For more information about agents, see Active Directory Agents.

Active Directory groups are defined and managed from Active Directory and the groups for the Active Directory that is joined to this node can be viewed from this tab. For more information about Active Directory, see https://msdn.microsoft.com/en-us/library/bb742437.aspx.

Choose **Providers** > **Active Directory** > **Advanced Settings**.

Table 5: Active Directory Advanced Settings

Field Name	Description
History interval	The time during which the Passive Identity service reads user login information that already occurred. This is required upon startup or restart of the Passive Identity service to catch up with events generated while it was unavailable. When the Endpoint probe is active, it maintains the frequency of this interval.
User session aging time	The amount of time the user can be logged in. The Passive Identity service identifies new user login events from the DC, however the DC does not report when the user logs off. The aging time enables ISE-PIC to determine the time interval for which the user is logged in.
NTLM Protocol settings	You can select either NTLMv1 or NTLMv2 as the communications protocol between ISE-PIC and the DC. NTLMv2 is the recommended default.

Field Name	Description
Authorization Flow	Check this check box to configure authorization policies for PassiveID login users. You can configure an authorization policy to assign an SGT to a user based on the Active Directory group membership. This allows you to create TrustSec policy rules even for PassiveID authorization. You can use the **PassiveID_Provider**, **PassiveID_Username**, or **PassiveID_Groups** attribute in the **PassiveID** dictionary to create the authorization rules for PassiveID login users. The following values can be set for the **PassiveID_Provider** attribute: • **API** • **Agent** • **SPAN** • **Syslog** • **WMI** • **Other** The IP-SGT mapping and Active Directory group details of PassiveID login users are included in the session topic. These details can be published through pxGrid, pxGrid Cloud, or SXP. You can view the authorization policy status and the SGT details in the **RADIUS Live Logs** window (**Operations > RADIUS > Live Logs**) and the **RADIUS Live Sessions** window (**Operations > RADIUS > Live Sessions**). **Note** • Ensure that the PassiveID, pxGrid, pxGrid Cloud, and SXP services are enabled on the node. To enable these services, choose **Administration > System > Deployment**. • You must enable the **Add RADIUS and PassiveID Mappings into SXP IP SGT Mapping Table** option in the **SXP Settings** window (**Work Centers > TrustSec > Settings > SXP Settings**) to include PassiveID mappings in the SXP mappings. • SGT details of the PassiveID login users that are authenticated using API provider cannot be published using SXP. However, the SGT details of these users can be published through pxGrid and pxGrid Cloud.