# Providers

In order to enable ISE-PIC to provide identity information to consumers that subscribe to the service (subscribers), you must first configure an ISE-PIC probe, which connects to the identity provider.

The table below provides details about all of the provider and probe types available from ISE-PIC. For more information about Active Directory, see Active Directory as a Probe and a Provider.

You can define these provider types:

*Table 1: Provider Types*

| Provider Type (Probe) | Description | Source System (Provider) | Technology | User Identity Information Collected | Document Link |
|---|---|---|---|---|---|
| Active Directory (AD) | A highly secure and precise source, as well as the most common, from which to receive user information. As a probe, AD works with WMI technology to deliver authenticated user identities. In addition, AD itself, rather than the probe, functions as a source system (a provider) from which other probes retrieve user data as well. | Active Directory Domain Controller | WMI | • User name <br> • IP address <br> • Domain | Active Directory as a Probe and a Provider |
| Agents | A native 32-bit application installed on Active Directory domain controllers or on member servers. The Agent probe is a quick and efficient solution when using Active Directory for user identity information. | | Agents installed on the domain controller or on a member server. | • User name <br> • IP address <br> • Domain | Active Directory Agents, on page 3 |
| Endpoint | Always runs in the background in addition to other configured probes, in order to verify whether the user is still connected. | | WMI | Whether the user is still connected | Endpoint Probe, on page 35 |
| SPAN | | | SPAN, installed on the switch, and Kerberos messages | • User name <br> • IP address <br> • Domain | SPAN, on page 12 |

| Provider Type (Probe) | Description | Source System (Provider) | Technology | User Identity Information Collected | Document Link |
|---|---|---|---|---|---|
| | Sits on the network switch in order to listen to network traffic, and extract user identity information based on Active Directory data. | | | | |
| API providers | Gather user identity information from any system programmed to communicate with a RESTful API client, using the RESTful API service offered by ISE-PIC. | Any system programmed to communicate with a REST API client. | RESTful APIs. User identity sent to subscribers in JSON format. | • User name<br>• IP address<br>• Port range<br>• Domain | API Providers, on page 7 |
| Syslog | Parse syslog messages and retrieve user identities, including MAC addresses. | • Regular syslog message providers<br>• DHCP servers | Syslog messages | • User name<br>• IP address<br>• MAC address<br>• Domain | Syslog Providers, on page 14 |

**Note** pxGrid sends 200 events per second for session topics to avoid overloading the clients. If the publisher sends more than 200 events, the additional events are queued and sent in next batch.

If pxGrid consistently receives more than 200 events per second for a prolonged period of time, it might consume more memory than usual for storing the backlog events. This might affect the performance of pxGrid.

# Active Directory Agents

From ISE-PIC install the native 32-bit application, Domain Controller (DC) agents, anywhere on the Active Directory (AD) domain controller (DC) or on a member server (based on your configurations) to retrieve user

identity information from AD and then send those identities to the subscribers you have configured. The Agent probe is a quick and efficient solution when using Active Directory for user identity information. Agents can be installed on a separate domain, or on the AD domain, and once installed, they provide status updates to ISE-PIC once every minute.

The agents can be either automatically installed and configured by ISE-PIC , or you can manually install them. Upon installation, the following occurs:

- The agent and its associated files are installed at the following path: **Program Files/Cisco/Cisco ISE PassiveID Agent**

- A config file called **PICAgent.exe.config** is installed indicating the logging level for the agent. You can manually change the logging level from within the config file.

- The CiscoISEPICAgent.log file is stored with all logging messages.

- The nodes.txt file contains the list of all nodes in the deployment with which the agent can communicate. The agent contacts the first node in the list. If that node cannot be contacted, the agent continues to attempt communication according to the order of the nodes in the list. For manual installations, you must open the file and enter the node IP addresses. Once installed (manually or automatically), you can only change this file by manually updating it. Open the file and add, change or delete node IP addresses as necessary.

- The Cisco ISE PassiveID Agent service runs on the machine, which you can manage from the Windows Services dialog box.

- ISE-PIC has been validated with 74 domain controllers.

- The Active Directory agents are only supported on Windows Server 2008 and higher. If you cannot install agents, then use the Active Directory probe for passive identity services. For more information, see Active Directory as a Probe and a Provider.

> ✎
>
> **Note**  Even if you are running the AD agent on a member server, it still queries the Active Directory for the login requests.

## Automatically Install and Deploy Active Directory Agents

When configuring the Agent provider to monitor domain controllers for user identities, the agent must be installed on either a member server or on a domain controller. The agents can be either automatically installed by ISE-PIC , or you can manually install them. After installation, automatic or manual, you must then configure the installed agent to monitor specified domain controllers rather than the default WMI. This process describes how to enable automatic installation and configure the agent to monitor a domain controller.

### Before you begin

- Configure reverse lookup for the relevant DNS servers from the server side. For more information about the DNS server configuration requirements for ISE-PIC, see DNS Server

- Ensure Microsoft .NET Framework is updated for the machine designated for the agents, to a minimum of version 4.0. For more information about the .NET framework, see https://www.microsoft.com/net/framework.

- Create an AD join point and add at least one domain controller. For more information about creating join points, see Active Directory as a Probe and a Provider.

  Use AD user groups for the AD, Agents, SPAN and Syslog probes. For more information about AD groups, see Configure Active Directory User Groups.

**Step 1**    Choose **Providers** > **Agents**.

**Step 2**    To add a new agent, click **Add** from the top of the table.

**Step 3**    To create the new agent and automatically install it on the host that you indicate in this configuration, select **Deploy New Agent**.

**Step 4**    Complete all mandatory fields in order to configure the client correctly. For more information, see Active Directory Agent Settings, on page 6.

**Step 5**    Click **Deploy**.
The agent is automatically installed on the host according to the domain that you indicated in the configuration, and the settings are saved. The agent now also appears in the Agents table and can be applied to monitor specified domain controllers, as described in the following steps.

**Step 6**    Choose **Providers** > **Active Directory** to view all currently configured join points.

**Step 7**    Click the link for the join point from which you would like to enable the agent you created.

**Step 8**    Choose the **Passive ID** tab to configure the domain controllers that you added as part of the prerequisites.

**Step 9**    Select the domain controller that you would like to monitor with the agent you created and click **Edit**.

**Step 10**   From the **Protocol** drop-down list, select **Agent**

**Step 11**   Select the agent you created from the **Agent** drop-down list. Enter the user name and password credentials of the agent that you created, and click **Save**.

The user name and password credentials are used to install the agent on the domain controller. Finally, when you click on **Deploy**, the *picagent.exe* is copied from */opt/pbis/bin* to the specified Windows machine.

# Manually Install and Deploy Active Directory Agents

When configuring the Agent provider to monitor domain controllers for user identities, the agent must be installed on either a member server or on a domain controller. The agents can be either automatically installed by ISE-PIC , or you can manually install them. After installation, automatic or manual, you must then configure the installed agent to monitor specified domain controllers rather than the default WMI. This process describes how to manually install and configure the agent to monitor a domain controller.

**Before you begin**

- Configure reverse lookup for the relevant DNS servers from the server side. For more information about the DNS server configuration requirements for ISE-PIC, see DNS Server

- Ensure Microsoft .NET Framework is updated for the machine designated for the agents, to a minimum of version 4.0. For more information about the .NET framework, see https://www.microsoft.com/net/framework.

- Create an AD join point and add at least one domain controller. For more information about creating join points, see Active Directory as a Probe and a Provider.

Use AD user groups for the AD, Agents, SPAN and Syslog probes. For more information about AD groups, see Configure Active Directory User Groups.

**Step 1** Choose **Providers** > **Agents**.

**Step 2** Click **Download Agent** to download the `picagent-installer.zip` file for manual installation.
The file is downloaded to your standard Windows Download folder.

**Step 3** Place the zip file on the designated host machine and run the installation.

**Step 4** From the ISE-PIC GUI, again choose **Providers** > **Agents**.

**Step 5** To configure a new agent, click **Add** from the top of the table.

**Step 6** To configure the agent that you have already installed on the host machine, select **Register Existing Agent**.

**Step 7** Complete all mandatory fields in order to configure the client correctly. For more information, see Active Directory Agent Settings, on page 6.

**Step 8** Click **Save**.
The agent settings are saved. The agent now also appears in the Agents table and can be applied to monitor specified domain controllers, as described in the following steps.

**Step 9** Choose **Providers** > **Active Directory** to view all currently configured join points.

**Step 10** Click the link for the join point from which you would like to enable the agent you created.

**Step 11** Choose the **Passive ID** tab to configure the domain controllers that you added as part of the prerequisites.

**Step 12** Select the domain controller that you would like to monitor with the agent you created and click **Edit**.

**Step 13** From the **Protocol** drop-down list, select **Agent**.

**Step 14** Select the agent you created from the **Agent** drop-down list. Enter the user name and password to connect to the agent, and click **Save**

The user account must have the necessary permissions to read security events. A user account for a WMI-based agent must have WMI/DCOM permissions.

# Uninstall the Agent

Agents, installed automatically or manually, can be easily (manually) uninstalled directly from Windows.

**Step 1** From the Windows dialog, go to **Programs and Features**.

**Step 2** Find and select the Cisco ISE PassiveID Agent in the list of installed programs.

**Step 3** Click **Uninstall**.

# Active Directory Agent Settings

Allow ISE-PIC to automatically install agents on a specified host in the network in order to retrieve user identity information from different Domain Controllers (DC) and deliver that information to ISE-PIC subscribers.

To create and manage agents, choose **Providers** > **Agents**. See Automatically Install and Deploy Active Directory Agents, on page 4.

**Table 2: Agents Window**

| Field Name | Description |
| --- | --- |
| **Name** | The agent name as you configured it. |
| **Host** | The fully qualified domain name of the host on which the agent is installed. |
| **Monitoring** | This is a comma separated list of domain controllers that the specified agent is monitoring. |

**Table 3: Agents New**

| Field | Description |
| --- | --- |
| **Deploy New Agent or Register Existing Agent** | • Deploy New Agent: Install a new agent on the specified host.<br><br>• Register Existing Agent: Manually install the agent on the host and then configure that agent from this screen for ISE-PIC to enable the service. |
| **Name** | Enter a name by which you can easily recognize the agent. |
| **Description** | Enter a description by which you can easily recognize the agent. |
| **Host FQDN** | This is the fully qualified domain name for the host on which the agent is installed (register existing agent), or is to be installed (automatic deployment). |
| **User Name** | Enter your user name in order to access the host on which to install the agent. ISE-PIC uses these credentials in order to install the agent for you.<br><br>The user account must have permissions to connect remotely and install the PIC agent. |
| **Password** | Enter your user password in order to access the host on which to install the agent. ISE-PIC uses these credentials in order to install the agent for you. |

# API Providers

The API Providers feature in Cisco ISE-PIC enables you to push user identity information from your customized program or from the terminal server (TS)-Agent to the built-in ISE-PIC REST API service. In this way, you can customize a programmable client from your network to send user identities that were collected from any network access control (NAC) system to the service. Furthermore, the Cisco ISE-PIC API provider enables

you to interface with network applications such as the TS-Agent on a Citrix server, where all users have the same IP address but are assigned unique ports.

For example, an agent running on a Citrix server that provides identity mappings for users authenticated against an Active Directory (AD) server can send REST requests to ISE-PIC to add or delete a user session whenever a new user logs in or off. ISE-PIC then takes the user identity information, including the IP address and assigned ports, delivered from the client and sends it to pre-configured subscribers, such as the Cisco Firepower Management Center (FMC).

The ISE-PIC REST API framework implements the REST service over the HTTPS protocol (no client certificate validation necessary) and the user identity information is delivered in JSON (JavaScript Object Notation) format. For more information about JSON, see http://www.json.org/ .

The ISE-PIC REST API service parses user identities and in addition, maps that information to port ranges, in order to distinguish between the different users logged in simultaneously to one system. Everytime a port is allocated to a user, the API sends a message to ISE-PIC.

### The REST API Provider Flow

After you have configured a bridge to your customized client from ISE-PIC by declaring that client as a Provider for ISE-PIC and enabling that specific customized program (the client) to send RESTful requests, the ISE-PIC REST service works in the following way:

1. For client authentication, Cisco ISE-PIC requires an authentication token. A customized program on the client machine sends a request for an authentication token when initiating contact and then every time ISE-PIC notifies that the previous token has expired. The token is returned in response to the request, enabling ongoing communication between the client, and the ISE-PIC service.

2. After a user has logged into the network, the client retrieves user identity information and posts that information to the ISE-PIC REST service using the API Add command.

3. Cisco ISE-PIC receives and maps the user identity information.

4. Cisco ISE-PIC sends the mapped user identity information to the subscriber.

5. Whenever necessary, the customized machine can send a request to remove user information by sending a Remove API call and including the user ID received as the response when the Add call was sent.

### Work with REST API Providers in ISE-PIC

Follow these steps to activate the REST service in ISE-PIC:

1. Configure the client side. For more information, see the client user documentation.

2. Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from ISE-PIC. For more information about the DNS server configuration requirements for ISE-PIC, see DNS Server

3. See Configure a Bridge to the ISE-PIC REST Service for Passive Identity Services, on page 9.

**Note**  To configure the API Provider to work with a TS-Agent add the TS-Agent information when creating a bridge from ISE-PIC to that agent, and then consult with the TS-Agent documentation for information about sending API calls.

**4.** Generate an authentication token and send add and remove requests to the API service.

# Configure a Bridge to the ISE-PIC REST Service for Passive Identity Services

In order to enable the ISE-PIC REST API service to receive information from a specific client, you must first define the specific client from Cisco ISE-PIC. You can define multiple REST API clients with different IP addresses.

### Before you begin

- Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from Cisco ISE-PIC. For more information about the DNS server configuration requirements for Cisco ISE-PIC, see DNS Server

**Step 1** The API Providers table is displayed, including status information for each existing client.

**Step 2** To add a new client, click **Add** from the top of the table.

**Step 3** Complete all mandatory fields in order to configure the client correctly. For more information, see API Provider Settings, on page 10.

**Step 4** Click **Submit**.
The client configuration is saved and the screen displays the updated API Providers table. The client can now send posts to the ISE-PIC REST service.

### What to do next

Set up your customized client to post authentication tokens and user identities to the ISE-PIC REST service. See Send API Calls to the ISE-PIC REST Service, on page 9.

# Send API Calls to the ISE-PIC REST Service

### Before you begin

Configure a Bridge to the ISE-PIC REST Service for Passive Identity Services, on page 9

**Step 1** Enter the Cisco ISE URL in the address bar of your browser (for example, *https://<ise hostname or ip address>/admin/*)

**Step 2** Enter the username and password that you specified and configured from the **API Providers** window. For more information, see Configure a Bridge to the ISE-PIC REST Service for Passive Identity Services, on page 9.

**Step 3** Press **Enter**.

**Step 4** Enter the API call in the URL Address field of the target node.

**Step 5** Click **Send** to issue the API call.

#### What to do next

See for more information and details about the different API calls, their schemas and their results.

# API Provider Settings

✎

**Note** The full API definition and object schemas can be retrieved with a request call as follows:

- For the full API specifications (wadl)—https://YOUR_ISE:9094/application.wadl

- For the API model and object schemas—https://YOUR_ISE:9094/application.wadl/xsd0.xsd

*Table 4: API Providers Settings*

| Field | Description |
|---|---|
| Name | Enter a unique name for this client that distinguishes it quickly and easily from other clients. |
| Description | Enter a clear description of this client. |
| Status | Select **Enabled** to enable the client to interact with the REST services immediately upon completing configuration. |
| Host/ IP | Enter the IP address for the client host machine. Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from ISE-PIC. |
| User name | Create a unique user name to be used when posting to the REST service. |
| Password | Create a unique password to be used when posting to the REST service. |

# API Calls

Use these API calls to manage user identity events for Passive Identity services with Cisco ISE-PIC.

**Purpose: Generate Authentication Token**

- **Request**

  POST

  https://<PIC IP address>:9094/api/fmi_platform/v1/identityauth/generatetoken

The request should contain the BasicAuth authorization header. Provide the API provider's credentials as previously created from the ISE-PIC GUI. For more information see .

- **Response Header**

  The header includes the X-auth-access-token. This is the token to be used when posting additional REST requests.

- **Response Body**

  HTTP 204 No Content

### Purpose: Add User

- **Request**

  POST

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity

  Add X-auth-access-token in the header of the POST request, for example, Header: X-auth-access-token, Value: f3f25d81-3ac5-43ee-bbfb-20955643f6a7

- **Response Header**

  201 Created

- **Response Body**

  {

  "user": "<username>",

  "srcPatRange": {

  "userPatStart": <user PAT start value>,

  "userPatEnd": <user PAT end value>,

  "patRangeStart": <PAT range start value>

  },

  "srcIpAddress": "<src IP address>",

  "agentInfo": "<Agent name>",

  "timestamp": "<ISO_8601 format i.e. "YYYY-MM-DDTHH:MM:SSZ" >",

  "domain": "<domain>"

  }

- **Notes**

  - srcPatRange can be removed in above json to create a single IP user binding.

  - Response body contains the "ID" which is the unique identifier for the user session binding created. Use this ID when sending a DELETE request to indicate which user should be removed.

  - This reponse also contains the self link which is the URL for this newly created user session binding.

**Purpose: Remove User**

- **Request**

  DELETE

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity/<id>

  In <id> enter the ID as was received from the Add response.

  Add the X-auth-access-token in the header of the DELETE request, for example, Header: X-auth-access-token, Value: f3f25d81-3ac5-43ee-bbfb-20955643f6a7

- **Response Header**

  200 OK

- **Response Body**

  Response body contains the details about the user session binding which got deleted.

# SPAN

SPAN allows you to quickly and easily enable Cisco ISE-PIC to listen to the network and retrieve user information without having to configure Active Directory to work directly with Cisco ISE-PIC. SPAN sniffs network traffic, specifically examining Kerberos messages, extracts user identity information also stored by Active Directory and sends that information to ISE-PIC. ISE-PIC then parses the information, ultimately delivering user name, IP address and domain name to the subscribers that you have also already configured from ISE-PIC.

In order for SPAN to listen to the network and extract Active Directory user information, ISE-PIC and Active Directory must both be connected to the same switch on the network. In this way, SPAN can copy and mirror all user identity data from Active Directory.

With SPAN, user information is retrieved in the following way:

1. The user endpoint logs in to the network.

2. Log in and user data are stored in Kerberos messages.

3. When the user logs in and the user data passes through the switch, SPAN mirrors the network data.

4. Cisco ISE-PIC listens to the network for user information and retrieves the mirrored data from the switch.

5. Cisco ISE-PIC parses the user information and updates passive ID mappings.

6. Cisco ISE-PIC delivers the parsed user information to the subscribers.

# Working with SPAN

**Before you begin**

In order to enable ISE-PIC to receive SPAN traffic from a network switch, you must first define which nodes and node interfaces are to listen to the switch. You can configure SPAN in order to listen to the different installed ISE-PIC nodes. For each node, only one interface can be configured to listen to the network and the interface used to listen must be dedicated to SPAN only.

In addition, you must:

- Ensure Active Directory is configured on your network.

- Run a CLI on the switch in the network that is also connected to Active Directory in order to ensure the switch can communicate with ISE-PIC.

- Configure the switch to mirror the network from AD.

- Configure a dedicated ISE-PIC network interface card (NIC) for SPAN. This NIC is used only for SPAN traffic.

- Ensure the NIC that you have dedicated to SPAN is activated via the command line interface.

- Create a VACL that sends only Kerberos traffic into the SPAN port.

**Step 1**    Choose **Providers** > **SPAN** to configure SPAN.

**Step 2**    **Note**    We recommend that the GigabitEthernet0 network interface card (NIC) remain available and that you select any other available NIC for configuring SPAN. GigabitEthernet0 is used for system management purposes.

Enter a meaningful description (optional), select status **Enabled**, and choose the nodes and the relevant NICs that will be used to listen to the network switch. For more information, see .

**Step 3**    Click **Save**.
The SPAN configuration is saved and ISE-PIC is now actively listening to network traffic.

# SPAN Settings

From each node that you have deployed, quickly and easily configure ISE-PIC to receive user identities by installing SPAN on a client network.

*Table 5: SPAN Settings*

| Field | Description |
|---|---|
| **Description** | Enter a unique description to remind you of which nodes and interfaces are currently enabled. |
| **Status** | Select **Enabled** to enable the client immediately upon completing configuration. |
| **Interface NIC** | Select one or both of the nodes installed for ISE-PIC, and then for each selected node, choose the node interface that is to listen to the network for information. <br><br> **Note**    We recommend that the GigabitEthernet0 NIC remain available and that you select any other available NIC for configuring SPAN. GigabitEthernet0 is used for system management purposes. |

# Syslog Providers

ISE-PIC parses syslog messages from any client (identity data provider) that delivers syslog messages, including regular syslog messages (from providers such as InfoBlox, Blue Coat, BlueCat, and Lucent) as well as DHCP syslog messages, and sends back user identity information, including MAC addresses. This mapped user identity data is then delivered to subscribers.

You can specify the syslog clients from which to receive the user identity data (see Configure Syslog Clients, on page 14). While configuring the provider, you must specify the connection method (TCP or UDP) and the syslog template to be used for parsing.

**Note**  When TCP is the configured connection type, if there is a problem with the message header and the host name cannot be parsed, ISE-PIC attempts to match the IP address received in the packet to the IP address of any of the providers in the list of providers that have already been configured for Syslog messages in ISE-PIC. To view this list, choose **Providers** > **Syslog Providers**. We recommend that you check the message headers and customize if necessary to guarantee parsing succeeds. For more information about customizing headers, see Customize Syslog Headers, on page 20.

The syslog probe sends syslog messages that are received to the ISE-PIC parser, which maps the user identity information, and publishes that information to ISE-PIC. ISE-PIC then delivers the parsed and mapped user identity information to ISE-PIC subscribers.

**Note**  DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that ISE-PIC can first check users registered in the local session directory (displayed from Live Sessions) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, in order to correctly parse and deliver user identity information. If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, the message is not parsed and user identity is not delivered.

To parse syslog messages for user identity from ISE-PIC :

- Configure syslog clients from which to receive user identity data. See Configure Syslog Clients, on page 14.

- Customize a single message header. See Customize Syslog Headers, on page 20.

- Customize message bodies by creating templates. See Customize the Syslog Message Body, on page 19.

- Use the message templates pre-defined in ISE-PIC when configuring your syslog client as the message template used for parsing, or base your customized header or body templates on these pre-defined templates. See Work with Syslog Predefined Message Templates, on page 23.

# Configure Syslog Clients

In order to enable Cisco ISE-PIC to listen to syslog messages from a specific client, you must first define the specific client from Cisco ISE-PIC. You can define multiple providers with different IP addresses.

**Step 1**    The Syslog Providers table is displayed, including status information for each existing client.

**Step 2**    To configure a new syslog client, click **Add** from the top of the table.

**Step 3**    Complete all mandatory fields (see Syslog Settings, on page 15 for more details) and create a message template if necessary (see Customize the Syslog Message Body, on page 19 for more details) to configure the client correctly.

**Step 4**    Click **Submit**.

## Syslog Settings

Configure Cisco ISE-PIC to receive user identities, including MAC addresses, by way of syslog messages from a specific client. You can define multiple providers with different IP addresses.

**Table 6: Syslog Providers**

| Field Name | Description |
|---|---|
| **Name** | Enter a unique name that distinguishes this configured client quickly and easily. |
| **Description** | A meaningful description of this Syslog provider. |
| **Status** | Select **Enabled** to enable the client immediately upon completing configuration. |
| **Host** | Enter the FQDN of the host machine. |
| **Connection Type** | Enter UDP or TCP to indicate the channel by which ISE-PIC listens for syslog messages.<br><br>**Note**    When TCP is the configured connection type, if there is a problem with the message header and the host name cannot be parsed, then Cisco ISE attempts to match the IP address received in the packet to the IP address of any of the providers in the list of providers that have already been configured for Syslog messages in Cisco ISE.<br><br>To view this list, choose **Providers** > **Syslog Providers**. We recommend that you check the message headers and customize if necessary to ensure that parsing succeeds. For more information about customizing headers, see Customize Syslog Headers, on page 20. |

| Field Name | Description |
|------------|-------------|
| **Template** | |

| Field Name | Description |
|---|---|
|  | A template indicates precise body message structure so that the parser can identify the pieces of information within the syslog message that should be parsed, mapped and delivered. |
|  | For example, a template can indicate the exact position of the user name so that the parser can find the user name in every message received. |
|  | From this field, indicate the template (for the body of the syslog message) to be used in order to recognize and correctly parse the syslog message. |
|  | Choose either from the pre-defined dropdown list, or click **New** to create your own customized template. For more information about creating new templates, see Customize the Syslog Message Body, on page 19. Most of the pre-defined templates use regular expressions, and customized templates should also use regular expressions. |
|  | **Note** Only customized templates can be edited or removed, while pre-defined system templates in the dropdown cannot be altered. |
|  | ISE-PIC currently offers these pre-defined DHCP provider templates: <br>• InfoBlox <br>• BlueCat <br>• Lucent_QIP <br>• DHCPD <br>• MSAD DHCP |
|  | **Note** DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that Cisco ISE can first check users registered in the local session directory (displayed from Live Sessionss) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, in order to correctly parse and deliver user identity information. <br><br> If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, then the message |

| Field Name | Description |
|---|---|
| | is not parsed and user identity is not delivered. |
| | Cisco ISE offers these pre-defined regular syslog provider templates: |
| | • ISE |
| | • ACS |
| | • F5_VPN |
| | • ASA_VPN |
| | • Blue Coat |
| | • Aerohive |
| | • Safe connect_NAC |
| | • Nortel_VPN |
| | For information about templates, see Work with Syslog Predefined Message Templates, on page 23. |
| **Default Domain** | If the domain is not identified in the syslog message for the specific user, this default domain is automatically assigned to the user in order to ensure that all users are assigned a domain. |
| | With the default domain or with the domain that was parsed from the message, the user name is appended to username@domain, thereby including that domain, in order to get more information about the user and user groups. |

# Customize Syslog Message Structures (Templates)

A template indicates precise message structure so that the parser can identify the pieces of information within the syslog message that should be parsed, mapped and delivered. For example, a template can indicate the exact position of the user name so that the parser can find the user name in every message received. Templates determine the supported structures for both new and remove mapping messages.

Cisco ISE-PIC enables you to customize a single message header and multiple body structures, to be used by the ISE-PIC parser.

The templates should include regular expressions to define the structure for user name, IP address, MAC address and domain in order to enable the ISE-PIC parser to correctly identify whether the message is to add or remove user identity mapping and to correctly parse the user details.

When customizing your message templates, you can choose to base your customization on the message templates pre-defined in ISE-PIC by consulting with the regular expressions and message structures used within those pre-defined options. For more information about the pre-defined template regular expressions, message structures, examples and more, see Work with Syslog Predefined Message Templates, on page 23.

You can customize:

- A single message header—Customize Syslog Headers, on page 20

- Multiple message bodies—Customize the Syslog Message Body, on page 19.

**Note** DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that Cisco ISE can first check users registered in the local session directory (displayed from Live Sessionss) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, in order to correctly parse and deliver user identity information. If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, then the message is not parsed and user identity is not delivered.

The delay necessary to properly match, parse and map details from DHCP messages cannot be applied to customized templates, and therefore it is not recommended that DHCP message templates be customized. Instead, use any of the pre-defined DHCP templates.

## Customize the Syslog Message Body

Cisco ISE-PIC enables you to customize your own syslog message templates (by customizing the message body) to be parsed by the ISE-PIC parser. The templates should include regular expressions to define the structure for user name, IP address, MAC address and domain.

**Note** DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that Cisco ISE can first check users registered in the local session directory (displayed from Live Sessionss) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, to correctly parse and deliver user identity information. If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, then the message is not parsed and user identity is not delivered.

The delay necessary to properly match, parse and map details from DHCP messages cannot be applied to customized templates, and therefore it is not recommended that DHCP message templates be customized. Instead, use any of the pre-defined DHCP templates.

Create and edit syslog message body templates from within the syslog client configuration screen.

**Note** You can only edit your own customized templates. Pre-defined templates offered by the system cannot be changed.

**Step 1** The Syslog Providers table is displayed, including status information for each existing client.

**Step 2** Click **Add** to add a new syslog client or **Edit** to update an already configured client. For more information about configuring and updating syslog clients, see Configure Syslog Clients, on page 14.

**Step 3** In the **Syslog Providers** window, click **New** to create a new message template. To edit an existing template, select the template from the dropdown list and click **Edit**.

**Step 4**       Complete all mandatory fields.

For information about how to enter the values correctly, see Syslog Customized Template Settings and Examples, on page 21.

**Step 5**       Click **Test** to ensure the message is correctly parsed based on the strings you have entered.

**Step 6**       Click **Save**.

## Customize Syslog Headers

Syslog headers also contain the host name from which the message originated. If your syslog messages are not recognized by the Cisco ISE-PIC message parser, you may need to customize the message header by configuring the delimiter that proceeds the host name, thereby enabling Cisco ISE-PIC to recognize the host name and parse the message correctly. For more details about the fields in this screen, see Syslog Customized Template Settings and Examples, on page 21. The customized header configuration is saved and added to the header types that are used by the parser whenever messages are received.

**Note**       You can only customize a single header. After you customize a header, when you click **Custom Header** and create a template, only the newest configuration is saved.

**Step 1**       The Syslog Providers table is displayed, including status information for each existing client.

**Step 2**       Click **Custom Header** to open the Syslog Custom Header screen.

**Step 3**       In the **Paste sample syslog** field, enter an example of the header format in your syslog messages. For example, copy and paste this header from one of your messages: `<181>Oct 10 15:14:08 Cisco.com`.

**Step 4**       In the **Separator** field, indicate whether words are separated by spaces or tabs.

**Step 5**       In the **Position of hostname in header** field, indicate which place in the header is the host name. For example, in the header offered above, the host name is the fourth word in the header. Enter 4 to indicate this.

The **Hostname** field displays the host name based on the details indicated in the first three fields. For example, if the header example in **Paste sample syslog** is as follows:
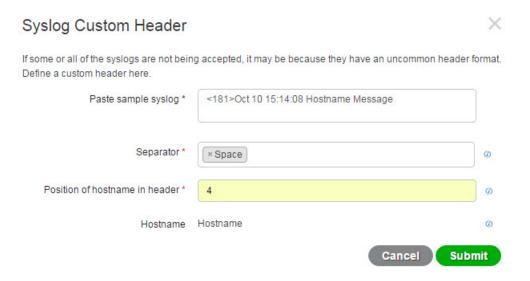
<181>Oct 10 15:14:08 Cisco.com

The separator is indicated as **Space** and the **Position of hostname in header** is entered as 4.

The **Hostname** will automatically appear as Cisco.com, which is the fourth word in the header phrase pasted in the **Paste sample syslog** field.

If the host name is incorrectly displayed, check the data you have entered in the **Separator** and **Position of hostname in header** fields.

This example is as in the following screen capture:

*Figure 1: Customize Syslog Headers*



**Step 6**    Click **Submit**.

The customized header configuration is saved and added to the header types that are used by the parser whenever messages are received.

## Syslog Customized Template Settings and Examples

Cisco ISE-PIC enables you to customize your own syslog message templates to be parsed by the ISE-PIC parser. Customized templates determine the supported structures for both new and remove mapping messages. The templates should include regular expressions to define the structure for user name, IP address, MAC address and domain in order to enable the ISE-PIC parser to correctly identify whether the message is to add or remove user identity mapping and to correctly parse the user details.

**Note**    Most of the pre-defined templates use regular expressions. Customized templates should also use regular expressions.

### Syslog Header Parts

You can customize a single header that is recognized by the Syslog probe by configuring the delimiter that proceeds the host name.

The following table describes the different parts and fields that can be included in your customized syslog header. For more information about regular expressions, see Table 9: Regular Expressions for Customized Templates, on page 23.

**Table 7: Syslog Custom Header**

| Field | Description |
|---|---|
| Paste sample syslog | Enter an example of the header format in your syslog messages. For example, copy and paste this header:<br><br>`<181>Oct 10 15:14:08 Hostname Message` |
| Separator | Indicate whether words are separated by spaces or tabs. |
| Position of hostname in header | Indicate which place in the header is the host name. For example, in the header offered above, the host name is the fourth word in the header. Enter 4 to indicate this. |
| Hostname | Displays the hostname based on the details indicated in the first three fields. For example, if the header example in **Paste sample syslog** is as follows:<br><br><181>Oct 10 15:14:08 Hostname Message<br><br>The separator is indicated as **Space** and the **Position of hostname in header** is entered as 4.<br><br>The **Hostname** will automatically appear as Hostname.<br><br>If the host name is incorrectly displayed, check the data you have entered in the **Separator** and **Position of hostname in header** fields. |

**Syslog Template Parts and Descriptions for the Message Body**

The following table describes the different parts and fields that can be included in your customized syslog message templates. For more information about regular expressions, see Table 9: Regular Expressions for Customized Templates, on page 23.

**Table 8: Syslog Template**

| Part | Field | Description |
|---|---|---|
|  | Name | A unique name by which to recognize the purpose of this template. |
| Mapping Operations | New Mapping | A regular expression that describes the kind of mapping used with this template to add a n<br>For example, enter "logged on from" in this field to indicate a new user that has logged or<br>F5 VPN. |
|  | Removed Mapping | A regular expression that describes the kind of mapping used with this template to remov<br>For example, enter "session disconnect" in this field to indicate a user that should be remc<br>ASA VPN. |

| Part | Field | Description |
|------|-------|-------------|
| User Data | IP Address | A regular expression that indicates the IP addresses to be captured. |
| | | For example, for Bluecat messages, to capture identities for users within this IP addres enter: |
| | | (on\s\|to\s)((?:(?:25[0-5]\|2[0-4][0-9]\|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]\|2[0-4][0-9]\|[01]?[ |
| | User Name | A regular expression that indicates the user name format to be captured. |
| | Domain | A regular expression that indicates the domain to be captured. |
| | Mac Address | A regular expression that indicates the MAC address format to be captured. |

### Regular Expression Examples

In order to parse messages use regular expressions. This sections offers regular expression examples in order to parse IP address, user name and add mapping messages.

For example, use regular expressions to parse the following messages:

<174>192.168.0.1 %ASA-4-722051: Group <DfltGrpPolicy> User <user1> IP <192.168.0.10> IPv4 Address <192.168.0.6> IPv6 address <::> assigned to session

<174>192.168.0.1 %ASA-6-713228: Group = xyz, Username = user1, IP = 192.168.0.12, Assigned private IP address 192.168.0.8 to remote user

The regular expressions are as defined in the following table.

*Table 9: Regular Expressions for Customized Templates*

| Part | Regular Expression |
|------|--------------------|
| IP address | Address <([^\s]+)>\|address ([^\s]+) |
| User name | User <([^\s]+)>\| Username = ([^\s]+) |
| Add mapping message | (%ASA-4-722051\|%ASA-6-713228) |

# Work with Syslog Predefined Message Templates

Syslog messages have a standard structure which include a header and the message body.

The predefined templates offered by Cisco ISE-PIC are described in this section, including content details for the headers that are supported, as well as the supported body structure, based on the origin of the messages.

In addition, you can create your own templates with customized body content for sources that are not predefined in the system. The supported structure for customized templates is also described in this section. You can configure a single customized header to be used in addition to the headers predefined in the system, when parsing messages, and you can configure multiple customized templates for the message body. For more information about customizing the header, see Customize Syslog Headers, on page 20. For more information about customizing the body, see Customize the Syslog Message Body, on page 19.

✎

| Note | Most of the predefined templates use regular expressions, and customized templates should also use regular expressions. |

**Message Headers**

There are two header types recognized by the parser, for all message types (new and remove), for all client machines. These headers are as follows:

- <171>Host message

- <171>Oct 10 15:14:08 Host message

Once received, the header is parsed for host name, which can be IP address, hostname, or full FQDN.

Headers can also be customized. To customize your headers, see Customize Syslog Headers, on page 20.

# Syslog ASA VPN Pre-Defined Template

The supported syslog message format and types for ASA VPN are as described below.

**Headers**

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 23.

**New Mapping Body Messages**

There are different ASA VPN body messages that are recognized by the parser as described in the following table.

| Body Message | Parsing Example |
|---|---|
| %ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11.11/20 on interface eth1/1 | [UserA,10.0.0.11] |
| %ASA-6-602303 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created. | |
| %ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created. | |
| %ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11,ffg123 #% UserA is UserA, MPPE_key_strength is string | |
| %ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11, UserA is user | |
| %ASA-6-113039 Group group User UserA IP 10.0.0.11 AnyConnect parent session started. | |
| %ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started. | |
| %ASA-6-713228: Group = xyz, UserA = xxxx227, IP = 192.168.0.11, Assigned private IP address 172.16.0.11 to remote user | [UserA,172.16.0.11]<br><br>**Note** The parsed IP address from this message type is the private IP address, as indicated in the message. |
| %ASA-4-722051: Group <DfltGrpPolicy> User <UserA> IP <172.16.0.12> IPv4 Address <172.16.0.21> IPv6 address <::> assigned to session | [UserA,172.16.0.12]<br><br>**Note** The parsed IP address from this message type is the IPv4 address. |

### Remove Mapping Body Messages

The Remove Mapping messages supported for ASA VPN by the parser are as described in this section.

Once received, the body is parsed for user details as follows:

**[UserA,10.1.1.1]**

| Body Message |
|---|
| %ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected. Session Type: type, Duration:\ duration, Bytes xmt: count,Bytes rcv: count, Reason: reason |

| Body Message |
| --- |
| %ASA-4-717052 Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number |
| %ASA-6-602304 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.1.1.1 (UserA) has been deleted. |
| %ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted. |
| %ASA-4-722049 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA |
| %ASA-4-722050 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user. |
| %ASA-6-802002 User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated. |
| %ASA-3-716057 Group group User UserA IP 10.1.1.1 Session terminated, no type license available. |
| %ASA-3-722046 Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel. |
| %ASA-4-113035 Group group User UserA IP 10.1.1.1 Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA. |
| %ASA-4-716052 Group group-name User UserA IP 10.1.1.1 Pending session terminated. |
| %ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted. |

## Syslog Bluecat Pre-Defined Template

The supported syslog message format and types for Bluecat are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in .

### New Mapping Body Messages

The messages supported for New Mapping for Bluecat syslog are as described in this section.

Once received, the body is parsed for user details as follows:

**[macAddress=nn:xx:nn:ca:xx:nn,ip=172.16.0.12]**

| Body |
| --- |
| Nov 7 23:37:32 xx-campus1 dhcpd: DHCPACK on 172.16.0.13 to nn:xx:nn:ca:xx:nn via 172.16.0.17 |

### Remove Mapping Messages

There are no remove mapping messages known for Bluecat.

# Syslog F5 VPN Pre-Defined Template

The supported syslog message format and types for F5 VPN are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 23.

### New Mapping Body Messages

There are different F5 VPN body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

**[user=UserA,ip=172.16.0.12]**

| Body |
| --- |
| Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security[nnnnn]: [UserA@vendor-abcr] User UserA logged on from 172.16.0.21 to \ 172.16.0.12 Sid = xyz\ |

### Remove Mapping Messages

Currently there are no remove messages for F5 VPN that are supported.

# Syslog Infoblox Pre-Defined Template

The supported syslog message format and types for Infoblox are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 23.

### New Mapping Body Messages

There are different ASA VPN body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

**[macAddress= nn:xx:xx:xx:nn:nn,ip=10.0.10.100]**

| Body Message |
| --- |
| Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:nx:nn:nn (android-df67ddcbb1271593) via eth2 relay 10.0.0.24 lease-duration 3600 |
| Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:xn:nn:nn (DESKTOP-HUDGAAQ) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW) |
| Nov 15 11:38:11 192.168.0.12 dhcpd[25595]: DHCPACK to 10.0.0.11 (nn:xx:xx:xn:nn:nx) via eth1 |

### Remove Mapping Messages

Once received, the body is parsed for user details as follows:

- If MAC address is included:

  **[00:0c:29:a2:18:34,10.0.10.100]**

- If MAC address is not included:

  **[10.0.10.100]**

| Body Message |
| --- |
| 07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPEXPIRE 10.0.10.100 has expired |
| 07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 \ (win10) via eth1 uid 01:00:0c:29:a2:18:34 |
| 07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[25595]: RELEASE on 10.20.31.172 to c0:ce:cd:44:4f:bd |

## Syslog Linux DHCPd3 Pre-Defined Template

The supported syslog message format and types for Linux DHCPd3 are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 23.

### New Mapping Messages

There are different Linux DHCPd3 body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

**[macAddress=24:ab:81:ca:f2:72,ip=172.16.0.21]**

| Body Message |
| --- |
| Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 to 00:0c:29:a2:18:34 (win10) via eth1 |
| Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 (00:0c:29:a2:18:34) via eth1 |

### Remove Mapping Body Messages

The Remove Mapping messages supported for Linux DHCPd3 by the parser are as described in this section.

Once received, the body is parsed for user details as follows:

**[00:0c:29:a2:18:34 ,10.0.10.100]**

| Body Message |
| --- |
| Nov 11 23:37:32 dhcpsrv dhcpd: DHCPEXPIRE 10.0.10.100 has expired |

| Body Message |
| --- |
| Nov 11 23:37:32 dhcpsrv dhcpd: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 (win10) via eth1 |

## Syslog MS DHCP Pre-Defined Template

The supported syslog message format and types for MS DHCP are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 23.

### New Mapping Body Messages

There are different MS DHCP body messages that are recognized by the parser as described in the following table.

Once received, the parser divides data by searching for the comma (,) and then messages of these formats are parsed as in the following example:

**[macAddress=000C29912E5D,ip=10.0.10.123]**

| Body Message |
| --- |
| Nov 11 23:37:32 10,07/21/16,16:55:22,Assign,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,724476048,0,,,,0x4D53465420352E30,MSFT,5.0 |

### Remove Mapping Body Messages

The Remove Mapping messages supported for MS DHCP by the parser are as described in this section.

Once received, the parser divides data by searching for the comma (,) and then messages of these formats are parsed as in the following example:

**[macAddress=000C29912E5D,ip=10.0.10.123]**

| Body Message |
| --- |
| Nov 11 23:37:32 12,07/21/16,16:55:18,Release,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,3128563632,\ 0,,,,,,,,,0 |

## Syslog SafeConnect NAC Pre-Defined Template

The supported syslog message format and types for SafeConnect NAC are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 23.

### New Mapping Body Messages

There are different SafeConnect NAC body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

**[user=galindk1i,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]**

| Body Message |
| --- |
| Apr 10 09:33:58 nac Safe*Connect: authenticationResult\|xxx.xx.xxx.xxx\|xxx.xx.xxx.xxx\|UserA\|true\|Resnet-Macs\|TCNJ-Chain\|001b63b79018\|MAC |

### Remove Mapping Messages

Currently there are no remove messages for Safe Connect that are supported.

## Syslog Aerohive Pre-Defined Templates

The supported syslog message format and types for Aerohive are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in .

### New Mapping Body Messages

There are different Aerohive body messages that are recognized by the parser as described in the following table.

Details parsed from the body include user name and IP address. The regular expression used for parsing is as in the following examples:

- `New mapping—auth\:`
- `IP—ip ([A-F0-9a-f:.]+)`
- `User name—UserA ([a-zA-Z0-9\_]+)`

Once received, the body is parsed for user details as follows:

**[UserA,10.5.50.52]**

| Body Message |
| --- |
| 2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA |

### Remove Mapping Messages

Currently the system does not support remove mapping messages from Aerohive.

## Syslog Blue Coat Pre-Defined Templates—Main Proxy, Proxy SG, Squid Web Proxy

The system supports the following message types for Blue Coat:

- BlueCoat Main Proxy
- BlueCoat Proxy SG
- BlueCoat Squid Web Proxy

The supported syslog message format and types for Bluecoat messages are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 23.

### New Mapping Body Messages

There are different Blue Coat body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

**[UserA,192.168.10.24]**

| Body Message (this example is taken from a BlueCoat Proxy SG message) |
| --- |
| 2016-09-21 23:05:33 58 10.0.0.1 UserA - - PROXIED "none" http://www.example.com/ 200 TCP_MISS GET application/json;charset=UTF-8 http site.api.example.com 80 /apis/v2/scoreboard/header ?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable |

The following table describes the different regular expression structures used per client for new mapping messages.

| Client | Regular expressions |
| --- | --- |
| BlueCoat Main Proxy | New mapping<br>**(TCP_HIT\|TCP_MEM){1}**<br>IP<br>\s(?:?[09]{13}\.){3}[09]{13})(?:?[azA-Z09]{14}:{12})[17]{azA-Z09]{14})\s<br>User name<br>\s\-\s([a-zA-Z0-9\_]+)\s\-\s |
| BlueCoat Proxy SG | New mapping<br>**(\-\sPROXIED){1}**<br>IP<br>\s(?:?[09]{13}\.3[09]{13}(?:?azA-Z09]{14}:{12}[17]{azA-Z09]{14})\s[azA-Z09_]+\s<br>User name<br>\s[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\s([a-zA-Z0-9\_]+)\s- |

| Client | Regular expressions |
|---|---|
| BlueCoat Squid Web Proxy | New mapping<br><br>**(TCP_HIT\|TCP_MEM){1}**<br><br>IP<br><br>**\s(?2?09]{1,3}\3[09]{1,3})(?:?:[a-zA-Z0-9]{1,4}:{1,2})[1?[a-zA-Z0-9]{1,4})sTCP**<br><br>User name<br><br>**\s([a-zA-Z0-9\._]+)\s\-\/** |

### Remove Mapping Messages

Remove mapping messages are supported for Blue Coat clients, though no examples are currently available.

The following table describes the different known regular expression structure examples used per client for remove mapping messages.

| Client | Regular expressions |
|---|---|
| BlueCoat Main Proxy | **(TCP_MISS\|TCP_NC_MISS){1}** |
| BlueCoat Proxy SG | No example currently available. |
| BlueCoat Squid Web Proxy | **(TCP_MISS\|TCP_NC_MISS){1}** |

## Syslog ISE and ACS Pre-Defined Templates

When listening to ISE or ACS clients, the parser receives the following message types:

- Pass authentication: When the user is authenticated by ISE or ACS, the pass authentication message is issued notifying that authentication succeeded, and including user details. The message is parsed and the user details and session ID are saved from this message.

- Accounting start and accounting update messages (new mapping): The accounting start or accounting update message is parsed with the user details and session ID that were saved from the Pass Authentication message and then the user is mapped.

- Accounting stop (remove mapping): The user mapping is deleted from the system.

The supported syslog message format and types for ISE and ACS are as described below.

### Pass Authentication Messages

The following messages are supported for Pass Authentication.

- **Header**

  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message

  For example: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **Body**

Passed-Authentication 000011 1 0 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12, DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius, RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5

- **Parsing Example**

  User name and session ID only are parsed.

  **[UserA,5]**

## Accounting Start/Update (New Mapping) Messages

The following messages are supported for New Mapping.

- **Header**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  For example: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **Body**

  CISE_RADIUS_Accounting 000011 1 0 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5

- **Parsing Example**

  Parsed details include user name, and framed IP address, as well as the MAC address if it is included in the message.

  [UserA,10.0.0.16]

## Remove Mapping Messages

The following messages are supported for Remove Mapping.

- **Header**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  For example: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **Body**

  2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS Accounting stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop, Acct-Session-Id=104, cisco-av-pair=audit-session-id=5

- **Parsing Example**

  Parsed details include user name, and framed IP address, as well as the MAC address if it is included in the message.

[UserA,10.0.0.16]

## Syslog Lucent QIP Pre-Defined Template

The supported syslog message format and types for Lucent QIP are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 23.

### New Mapping Body Messages

There are different Lucent QIP body messages that are recognized by the parser as described in the following table.

The regular expression structure for these messages is as follows:

**DHCP_GrantLease|:DHCP_RenewLease**

Once received, the body is parsed for user details as follows:

**[00:0C:29:91:2E:5D,10.0.0.11]**

| Body Message |
|---|
| DHCP:subtype=0:Single:$IGNORE_N$ DHCP_GrantLease: Host=$HOSTNAME$ P=10.0.0.11 MAC= 00:0C:29:91:2E:5D |
| DHCP:subtype=0:Single:$IGNORE_N$ DHCP_RenewLease: Host=$HOSTNAME$ P=10.0.0.11 MAC= 00:0C:29:91:2E:5D |

### Remove Mapping Body Messages

The regular expression structure for these messages is as follows:

**Delete Lease:|DHCP Auto Release:**

Once received, the body is parsed for user details as follows:

**[10.0.0.11]**

| Body Message |
|---|
| DHCP:subtype=0:Single:$IGNORE_N$ Delete Lease: IP=10.0.0.11 $IGNORE_N$ |
| DHCP:subtype=0:Single:$IGNORE_N$ DHCP Auto Release: IP=10.0.0.11 $IGNORE_N$ |

# Filter Passive Identity Services

You can filter certain users, based on their name or IP address. For example, if you have an administrator from IT services who logs in to an endpoint in order to assist the regular user with that endpoint, you can filter out the administrator activity so it does not appear in Live Sessions, but rather only the regular user of that endpoint will appear. The Live Session shows Passive Identity service components that are not filtered out

by the Mapping Filters. You can add as many filters as needed. The "OR" logic operator applies between filters. If both the fields are specified in a single filter, the "AND" logic operator applies between these fields.

**Step 1**     Choose **Providers** > **Mapping Filters**.

**Step 2**     Click **Add**, enter the Username and or IP address of the user you want to filter and click **Submit**.

# Endpoint Probe

In addition to the customized providers that you can configure the Endpoint probe is enabled in ISE-PIC by default upon installation and always runs in the background. The Endpoint probe periodically checks whether each specific user is still logged in to the system.
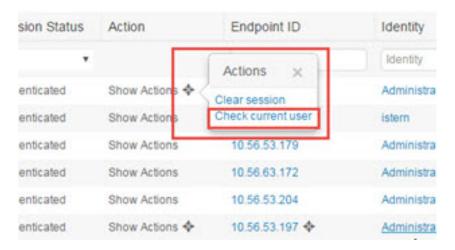
**Note**      In order to ensure Endpoint runs in the background, you must first configure an initial Active Directory join point and ensure you choose to **Store Credentials**. For more information about configuring the Endpoint probe, see Work with the Endpoint Probe, on page 36.

To manually check for endpoint status go to **Live Sessions** , from the **Actions** column, click **Show Actions** and choose **Check current user**, as in the following figure.

*Figure 2: Check Current User*



For more information about endpoint user status, and manually running the check, see Live Sessions.

When the Endpoint probe recognizes that a user has connected, if 4 hours have passed since the last time the session was updated for the specific endpoint, it checks whether that user is still logged in and collects the following data:

• MAC address

• Operating system version

Based on the this check, the probe does the following:

- When the user is still logged in, the probe updates Cisco ISE-PIC with the status Active User.

- When the user has logged out, the session state is updated as Terminated and fifteen minutes later, the user is removed from the Session Directory.

- When the user cannot be contacted, for example, when a firewall prevents contact or the endpoint has shut down, the status is updated as Unreachable and the Subscriber policy will determine how to handle the user session. The endpoint will remain in the Session Directory.

# Work with the Endpoint Probe

### Before you begin

The Endpoint Probe is enabled by default when ISE-PIC is installed. To enable and disable the probe, first ensure you have configured the following:

- Endpoints must have network connectivity to port 445.

- From ISE-PIC, configure an initial Active Directory join point. For more information about join points, see Active Directory as a Probe and a Provider.

**Note** In order to ensure Endpoint runs in the background, you must first configure an initial Active Directory join point, which enables the Endpoint probe to run even when the Active Directory probe is not fully configured.

**Step 1** Choose **Providers** > **Endpoint Probes**.

**Step 2** Choose **Enabled** or **Disabled**.
The screen does not change. However, the probe is enabled or disabled based on your selection, and if enabled, is now running in the background and collecting data.