Managing Security Assertion Markup Language Single Sign-On (SAML SSO) in Cisco Unity Connection 10.x

See the following sections:

Overview of SAML SSO in Unity Connection 10.x

Cisco Unity Connection 10.0(1) and later release introduces an enhanced signed in feature using open industry standard protocol SAML (Security Assertion Markup Language) referred to as SAML SSO. SAML SSO allows a user to gain single sign-on access with Unity Connection subscriber web interfaces and across the administrative web applications on the following Unified Communication products:

- Cisco Unity Connection
- Cisco Unified Communications Manager
- Cisco Unified IM/Presence

Unity Connection supports SAML 2.0 protocol for the SAML SSO feature. SAML SSO uses Identity Provider (LDAP based) to provide single sign-on access to client applications. For more information on access to web applications on Unity Connection using SAML SSO, see Access to Unity Connection web applications using SAML SSO.

With Unity Connection 10.5 and later, VMRest APIs expand single sign-on access (SSO) support to include authentication using a SSO OAuth 2.0 token. Make sure that SAML SSO is already configured on the Unity Connection server.

Note With Cisco Unity Connection10.0(1), PAWS APIs are supported with SAML single sign-on access. Cisco Unity Connection Rest APIs are not supported using SAML SSO.

SAML SSO allows the LDAP user to login with a username and password that authenticates on Identity Provider. **Identity Provider** is an online service or website that authenticates users by means of security tokens. It authenticates the end user and returns a SAML Assertion. SAML Assertion shows either a Yes (authenticated) or No (authentication failed) response. Currently, the supported Identity Providers are:

- ADFS (Active Directory Federated Services) version 2.0
- Ping Federate version 6.10.0.4
- Oracle Identity Provider version 11.0
- OpenAM version 10.1

Note Only one Identity Provider is deployed at one time as Identity Provider cluster is not supported with SAML SSO.

The non-LDAP users with administrator rights login to Cisco Unity Connection Administration using Recovery URL. The Recovery URL option is present in Unity Connection product landing page just below the Cisco Unity Connection option. When SSO login fails(e.g. If Identity Provider or Active directory is inactive), Recovery URL provides alternate access to the administrative and serviceability web applications via username and password. A non-LDAP user can access the following web applications on Unity Connection using Recovery URL:

- Cisco Unity Connection Administration
- Cisco Unity Connection Serviceability
- Cisco Unified Serviceability

Note LDAP users are the users that are integrated to Active Directory. Non-LDAP users are the users that reside locally on Unity Connection server.

Access to Unity Connection web applications using SAML SSO

A user signed into any of the supported web applications on Unified Communication products (after enabling the SAML SSO feature) also gains access to the following web applications on Unity Connection (apart from Cisco Unified Communications Manager and Cisco Unified CM IM/Presence):

Unity Connection users	Web applications
LDAP users with administrator rights	• Unity Connection Administration • Cisco Unity Connection Serviceability • Cisco Unified Serviceability • Cisco Personal Communications Assistant • Web Inbox • Mini Web Inbox (desktop version)
LDAP users without administrator rights	• Cisco Personal Communications Assistant • Web Inbox • Mini Web Inbox (desktop version)

Note To access Web Inbox and Mini Web Inbox, you must have a user with mailbox. Also, navigate to Unity Connection Administration> Class of Service> Licensed features and make sure that the **Allow Users to Use the Web Inbox, Messaging Inbox and RSS Feeds** check box is checked.

The users (LDAP or non-LDAP) do not gain access to the following web applications using SAML SSO:

- Disaster Recovery System
- Cisco Unified Operating System Administration

System Requirements for SAML SSO in Unity Connection 10.x

The following Security Assertion Markup Language single sign-on requirements exist for Cisco Unity Connection:

- Cisco Unity Connection release 10.0(1) or later release on both the servers in case of cluster. The feature requires the following third-party applications for configuring the SAML SSO feature:
- Microsoft Windows Server 2008 R2 Server / Windows Server 2012 Installation Media.
- Microsoft Active Directory server.
- Any of the following supported Identity Provider servers:
  - Active Directory Federated Service (ADFS) 2.0 Federation Server
  - OpenAM 10.1
  - Ping Federate 6.10.0.4
  - Oracle Identity Manager Server 11.0
- Self Signed Certificate (SSL) for Internet Information Services (IIS) Manager 7.0 and later. The SAML SSO feature on Cisco Unity Connection uses Identity Provider (LDAP based) simultaneously to provide single sign-on access to many web applications on the Unity Connection server.

The third party applications required for the SAML SSO feature must meet the following configuration requirements:

- In case of Active directory, it must be deployed in a Windows domain-based network configuration, not just as an LDAP server.
- The Identity Provider must be accessible by hostname on the network to Connection server, all client systems and the Active directory server.
- The clocks of all the entities participating in SAML SSO must be synchronized.

Note SAML SSO or single sign-on feature cannot be enabled on tenant partitions.

See the third party documentation for more information about these products.

Prerequisites for SAML SSO in Unity Connection 10.x

Revised March, 2014

To use the SAML SSO feature, you must configure any of the following Identity Provider servers:

- ADFS (Active Directory Federated Services) version 2.0
- OpenAM version 10.1
- Ping Federate version 6.10.0.4
- Oracle Identity Manager version 11.0

Note Make sure that the clocks of Unity Connection and the Identity Provider (chosen for SAML SSO) are synchronized with each other.

Using Active Directory Federated Services (ADFS)

This section provides the prerequisites for configuring the SAML SSO feature using ADFS as Identity Provider in the network.

Table 14-1 *Prerequisites to Enable SAML SSO Using ADFS*

	Configuration Steps	Related Topics and Documentation
Step 1	Ensure that your environment meets the requirements described in the prerequisites.	
Step 2	Provision the ADFS (Active Directory Federated Services) 2.0 server in Active Directory and then, generate keytab files.	Microsoft Active Directory documentation
Step 3	Configure the ADFS Identity Provider server for Unity Connection.	Configuring ADFS Server, page 14-7
Step 4	Import the ADFS server certificate into the Cisco Unified Communications Manager Tomcat-trust store.	
Step 5	Configure Windows single sign-on with Active directory and ADFS.	
Step 6	Configure client browsers for single sign-on.	https://supportforums.cisco.com/docs/DOC-14462
Step 7	Enable SAML SSO on Unity Connection.	Configuring SAML SSO in Unity Connection 10.x, page 14-6

Using OpenAM

This section provides the prerequisites for configuring the SAML SSO feature using OpenAM as Identity Provider in the network.

Table 14-2 Prerequisites to Enable SAML SSO Using OpenAM

	Configuration Steps	Related Topics and Documentation
Step 1	Ensure that your environment meets the requirements described in the prerequisites.	
Step 2	Provision the OpenAM server in Active Directory and then, generate keytab files. **Note** If your Windows version does not include the ktpass tool for generating keytab files,then you must obtain it separately.	Microsoft Active Directory documentation
Step 3	Configure the OpenAM Identity Provider 10.1 server for Unity Connection.	Configuring OpenAM Server, page 14-8
Step 4	Import the OpenAM server certificate into the Cisco Unified Communications Manager Tomcat-trust store.	
Step 5	Configure Windows single sign-on with Active directory and OpenAM.	
Step 6	Configure client browsers for single sign-on	https://supportforums.cisco.com/docs/DOC-14462
Step 7	Enable SAML SSO on Unity Connection.	Configuring SAML SSO in Unity Connection 10.x, page 14-6

Using Ping Federate

This section provides the prerequisites for configuring the SAML SSO feature using Ping Federate as Identity Provider in the network.

Table 14-3 Prerequisites to Enable SAML SSO Using Ping Federate

	Configuration Steps	Related Topics and Documentation
Step 1	Ensure that your environment meets the requirements described in the prerequisites.	
Step 2	Provision the Ping Federate server in Active Directory and then, generate keytab files. **Note** If your Windows version does not include the ktpass tool for generating keytab files,then you must obtain it separately.	Microsoft Active Directory documentation
Step 3	Configure the Ping Federate Identity Provider 6.10.0.4 server for Unity Connection.	Configuring Ping Federate Server, page 14-9
Step 4	Import the Ping Federate server certificate into the Cisco Unified Communications Manager Tomcat-trust store.	
Step 5	Configure Windows single sign-on with Active directory and Ping Federate.	

Table 14-3 Prerequisites to Enable SAML SSO Using Ping Federate

	Configuration Steps	Related Topics and Documentation
Step 6	Configure client browsers for single sign-on	https://supportforums.cisco.com/docs/DOC-14462
Step 7	Enable SAML SSO on Unity Connection.	Configuring SAML SSO in Unity Connection 10.x, page 14-6

Using Oracle Identity Manager

This section provides the prerequisites for configuring the SAML SSO feature using Oracle Identity Manager as Identity Provider in the network.

Table 14-4 Prerequisites to Enable SAML SSO Using Oracle Identity Manager

	Configuration Steps	Related Topics and Documentation
Step 1	Ensure that your environment meets the requirements described in the prerequisites.	
Step 2	Provision the Oracle Identity Manager server in Active Directory and then, generate keytab files. **Note** If your Windows version does not include the ktpass tool for generating keytab files,then you must obtain it separately.	Microsoft Active Directory documentation
Step 3	Configure the Oracle Identity Manager Identity Provider 11.0 server for Unity Connection.	Configuring Oracle Identity Provider Server, page 14-11
Step 4	Import the Oracle Identity Manager server certificate into the Cisco Unified Communications Manager Tomcat-trust store.	
Step 5	Configure Windows single sign-on with Active directory and Oracle Identity Manager.	
Step 6	Configure client browsers for single sign-on	https://supportforums.cisco.com/docs/DOC-14462
Step 7	Enable SAML SSO on Unity Connection.	Configuring SAML SSO in Unity Connection 10.x, page 14-6

Configuring SAML SSO in Unity Connection 10.x

This section outlines the key steps and/or instructions that must be followed for Unity Connection specific configuration. However, if you are configuring SAML SSO feature for the first time, it is trongly recommended to follow the detailed instructions given below:

- Configuring Identity Provider
- Configuring SAML SSO in Cisco Unity Connection
- Running CLI commands for SAML SSO

Configuring Identity Provider

Added March, 2014

Configuring ADFS Server

If you choose ADFS as the Identity Provider for SAML SSO:

Step 1 Download the ADFS 2.0. Install the ADFS 2.0 server by accepting the license and select FINISH when the installation is complete.

Step 2 Launch the ADFS configuration wizard by selecting the ADFS 2.0 Management under Administrative Tools. When the AD FS Management Console opens, select the ADFS 2.0 Federation Server Configuration

Wizard Link.

Step 3 Select AD FS 2.0 Federation Server Configuration Wizard, then select Next (Create a new Federation Service should be automatically selected).

Step 4 Select Stand-alone federation server and then select **Next**. Select your SSL certificate and the default Federation Service name and select Next. Make sure that the SSL certificate is signed by a provider. E.g.-

Thawte or Verisign. Select **Next** and then select **Close**.

Step 5 Select **Required: Add a trusted relying party** and then select **Start**. If you have an URL or file containing the configuration use this option otherwise select **Enter data** about the relying party manually and then select **Next**.

Step 6 Enter a Display name and then select **Next**. Select ADFS 2.0 profile and then select **Next**. Select **Browse** and select the same certificate you used earlier and then select **Next**.

Step 7 Select **Enable support for SAML 2.0 WebSSO protocol** and then enter the URL to the service providing the integration. After this, select **Next**. Enter the Relying party trust identifier and select **Add**, then select **Next**.

Step 8 Select **Next** (Permit all users to access this relying party is automatically selected, you may want to change this later once testing is complete). Select **Next** and then select **Close** (Open the Edit Claim Rules

dialog for this relying party trust when the wizard closes should be automatically selected).

Step 9 Select **Add Rule** and then select **Next** (Send LDAP Attributes as Claims should be automatically selected).

Enter a Claim rule name and then select Active Directory under Attribute store. Select an LDAP Attribute and a corresponding Outgoing Claim Type. Then select **Finish** and select **OK.**

In addition to the above Unity Connection specific configuration, ensure the following points:

- Launch ADFS 2.0 from programs menu and then select **Add Relying Party Trust**.
- Select **Start** button and select option Import data about the relying party from a file and choose Fedlet metadata file from a desktop which you downloaded from Call Manager or using REST API. then, select **Next**.
- Enter Display name and select **Next**. Choose **Permit All Users** to access this relying party and then select **Next**.
- Review the setting and then select **Next**. Select **Close** and ensure that the check box to **Add Claim Rules** is enabled.

- Click on **Add Rule**. Enter the Claim rule name and select the **Attribute Store**.The syntax for the Name ID claim rule is:

"c:[Type=="http://schemas.microsoft.com/ws/2008/06/identity/claims/windows account name"]=> issue(Type= "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer= c.Issuer, OriginalIssuer= c.OriginalIssuer, Value= c.Value, ValueType=c.ValueType, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]="urn:oasis:names:tc:SAML:2.0:nameid-format: transient", Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]="http:// <FQDN of ADFS server>/adfs/com/adfs/service/trust", Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"]="<FQDN of Unity Connection server>");"

Note A default **Name ID** claim rule is necessary to configure ADFS to support SAML SSO.

- Select **Next** button with default claim rule template **Send LDAP Attributes as Claims In Configure Rule**, enter the Claim Rule name, select Attribute store as Active Directory and then configure LDAP Attribute and Outgoing Claim Types. Select **Finish**. Then select **Apply** followed by **OK**.

Configuring OpenAM Server

If you choose OpenAM Server as the Identity Provider for SAML SSO:

Step 1 To configure policies on OpenAM server, you must log in to OpenAM and select the Access Control tab. Click the Top Level Realm option, select the Policies tab, and then create a new policy. Follow the steps as given in the Cisco white paper, https://supportforums.cisco.com/docs/DOC-14462, for creating a new policy. While following the instructions given in the white paper, make sure to create policies with the below mentioned Unity Connection-specific information:

- Ensure the following points while adding rules to the policy:
  - Each rule should be of the URL Policy Agent service type.
  - Make sure to check the GET and POST checkbox for each rule.
  - Create a rule for each of the following resources, where 'fqdn' is the fully qualified domain name of your Unity Connection server:

https://<fqdn>:8443/*

https://<fqdn>:8443/*?*

https://<fqdn>/*

https://<fqdn>/*?*

http://<fqdn>/*

http://<fqdn>/*?*

- Ensure the following points while adding a subject to the policy:
  - Make sure that the **Subject Type** field is **Authenticated Users**.
  - Specify a subject name.
  - Do not check the **Exclusive** check box.

- Ensure the following points while adding a condition to the policy:
  - Mention the **Condition** type as **Active Session Time**.
  - Specify a condition name.
  - Configure active session timeout as 120 minutes and select **No** for the Terminate Session option.

Step 2 Configure a Windows Desktop SSO login module instance.

Follow the instructions for configuring Windows Desktop as given in the Cisco white paper,

https://supportforums.cisco.com/docs/DOC-14462.

Step 3 Configure a J2EE Agent Profile for Policy Agent 3.0.

Follow the instructions to create a new J2EE agent as given in the Cisco white paper,

Step 4 https://supportforums.cisco.com/docs/DOC-14462 with the below mentioned Unity Connection-specific settings:

- The name mentioned as agent profile name is the name that you need to enter when enabling SSO on the Unity Connection server, when it prompts as: “Enter the name of the profile configured for this policy agent.”
- The agent password entered here is the password that is entered on the Unity Connection server when it prompts as: “Enter the password of the profile name.”
- Make sure to add the following URIs to the Login Form URI section on the Application tab:

–/cuadmin/WEB-INF/pages/logon.jsp

–/cuservice/WEB-INF/pages/logon.jsp

–/ciscopca/WEB-INF/pages/logon.jsp

–/inbox/WEB-INF/pages/logon.jsp

–/ccmservice/WEB-INF/pages/logon.jsp

–/vmrest/WEB-INF/pages/logon.jsp

- Under the Application tab, add the following URI in the Not Enforced URI Processing session: **–/inbox/gadgets/msg/msg-gadget.xml**

In addition to above Unity Connection-specific configuration, ensure the following points:

- Import users from LDAP to Connection. Users must be configured with the appropriate roles to log in to Cisco Unity Connection Administration, or Cisco Unity Connection Serviceability.
- Upload the OpenAM certificate into Connection as described in the Configuring SSO onCisco Unified Communications Manager 8.6 section of the Cisco white paper,
- https://supportforums.cisco.com/docs/DOC-14462.

Configuring Ping Federate Server

If you choose Ping Federate Server as the Identity Provider for SAML SSO:

Step 1 Install JDK. Download JDK from the given location:
www.oracle.com/technetwork/java/javase/downloads

Step 2 Set the JAVA_HOME environment variable to the JDK installation directory path and add the /bin directory to the PATH variable for your platform.

MyComputer>Properties>Advanced>Envoirnment variables>Path.

C:\WINDOWS\java;C:\Program Files\Java\jdk1.7.0_21\bin

Step 3 Download Ping federate.zip file and lic file.

Step 4 Unzip the Ping Federate file.

Step 5 Save the license key file in the directory:

<pf_install>/pingfederate/server/default/conf

Step 6 Run the Ping Federate as service.

run install-service.bat from the directory:

<pf_install>\pingfederate\sbin\win-x86-32

Step 7 Access the PingFederate administrative console:

https://<IP >:9999/pingfederate/app

Step 8 Login to Ping Federate.

Username: Administrator

Password: 2Federate

Step 9 Change your password on the Change Password screen and select **Save.**

Step 10 Configure server. Browse to **Welcome** page and then select **Next.**

Step 11 Accept the lic file and select Next.

Step 12 Select **Single-user Administration** and select **Next**.

Step 13 Add System Info details as below and select **Next.**

- Select **Next** on **Runtime Notifications**.
- Select **Next** on **Runtime Reporting**.

Step 14 Enable Account Management details as below:

- Select Roles and Protocols.
- Provide the Base URL and Realm. Base URL is the IP address of Ping Federate server.
- Select **Next**. Select **Save** on Summary page.

Configuring SP Connection

Step 1 Select Create New under SP Connections. Select Next. Select the Browser SSO option and then select Next.

Step 2 Browse sp.xml file and select Next.

Note sp.xml file is donwloaded from Cisco Unified CM

Step 3 After importing the sp.xml file successfully, select **Next**.

Step 4 Configure Base URL as **https://<server name>:8443**. Select **Next**.

Step 5 Select Configure Browser SSO. Select Next.

Step 6 Select **SP-Initiated SSO**. Select **Next.**

Step 7 Specify the **Assertion Lifetime**. Select **Next**.

Step 8 Select **Assertion Creation**. Select **Transient** and make sure Include attributes in addition to the transient identifier checkbox is checked.

Step 9 Select snap shot details under Attribute Contract.

Step 10 Select **Map New Adapter Instance**. Select **Next**.

Step 11 Select LDAP under Adapter Instance. Select **Next**.

Configuring Oracle Identity Provider Server

If you choose Oracle Identity Provider Server as the Identity Provider for SAML SSO:

Step 1 Login to Oracle Enterprise Manager where Oracle Identity Federation has been installed as a component.

Step 2 Under **Identity and Access** in the drop down, select **Oracle Identity Federation**.

Step 3 Under **Oracle Identity Federation** drop down, select **Federations**.

Step 4 Select Federations. In the Federations window - > Add New Federations. In this case the Metadata file is imported from the CUCM. After the Metadata has been loaded, the CUCM hostname is displayed under Federations.

Step 5 Select the CUCM node and select edit button. Under the edit option, select Attribute Mappings and Filters. Then select the check box **Enable Attributes in Single Sign-On (SSO).**

Step 6 Check the below check boxes -

a. **Unspecified**
b. **Email Address**
c. **Persistent Identifier**
d. **Transient/One-Time Identifier**

Apply the above changes with the Apply button on the window and then select Attribute Mappings and Filters which would open up a new window.

Step 7 Under Name Mappings, select Add, a new window opens up. Add a new Attribute.
"User Attribute Name" uid.
"Assertion Attribute Name" uid.
"Send with SSO Assertion" check box should be checked.

Step 8 Another attribute to be added is Email:
"User Attribute Name" mail
"Assertion Attribute Name" email
"Send with SSO Assertion" check box should be checked.
Click on Ok and exit out after saving the configuration.
Generating and Importing Metadata into the Call Manager -

1. Navigate to Oracle Identity Federation drop down - > Administration- > Security and Trust.

2. In the Security and Trust Window - Generate Metadata xml with the option Provider Type as Identity Provider and Protocol as SAML 2.0.
3. Import the Metadata into the CUCM.

Configuring SAML SSO in Cisco Unity Connection

In Unity Connection 10.5(2) and later releases, the option **Export All Metadata** is enabled by default. This option allows you to export the metadata from Unity Connection before enabling SAML SSO. If this option is enabled, you can skip **Step 4** or choose to continue with the procedure given below:

To configure SAML SSO feature on Unity Connection server, you must perform the following steps:

Step 1 To enable SAML SSO on Unity Connection server, log on to the Unity Connection Administration.

Note The cluster status should not be affected while enabling or disabling the SAML SSO feature. SAML SSO cannot be enabled from publisher server if subscriber server is inactive or vice versa.

Navigate to **System settings> SAML Single Sign-On>** select the option **Enable SAML SSO**. When you select **SAML SSO** option, a wizard opens as **Web server connections will be restarted**, select **Continue**.

Note When enabling SAML SSO from Cisco Unity Connection, make sure you have at least one LDAP user with administrator rights in Unity Connection.

Step 2 To initiate the IdP Metadata import, navigate to Identity Provider (IdP) Metadata Trust File, select the option **Browse** to upload the IdP metadata from your system. Then select the option Import IdP Metadata. Follow the link below to download IdP metadata trust file for ADFS:

https://localhost/FederationMetadata/2007-06/FederationMetadata.xml

Step 3 If the import of metadata is successful, a success message appears Import succeeded for all servers. Then select Next to continue the wizard.

Step 4 For SAML metadata exchange, select the option **Download Trust Metadata Fileset**.

Caution If the Trust Metadata has not been imported then a warning message prompts on the screen as The server metadata file must be installed on the IdP before this test is run.

Then select **Next**. A window appears for valid administrator IDs that automatically populates the LDAP user with administrator rights into that window. If you find the LDAP user with administrator rights automatically populated in the above window, then select **Run Test** to continue.

Step 5 The wizard continues and a window appears for user login to IdP. Enter the credentials for the LDAP user with administrator role that was automatically populated in the previous window.

This enables the SAML SSO feature completely. Select **Finish** to complete the configuration wizard.

Note After enabling/disabling SAML SSO on Unity Connection, a user must wait for approximately (2-3 minutes) to get the web applications initialized properly and then the Tomcat service needs to be restarted from Cisco Unity Connection Serviceability page or using the CLI command **utils service restart Cisco Tomcat**.

Running CLI commands for SAML SSO

The following section describes the CLI commands for SAML single sign-on. All the commands are valid for cluster and stand- alone nodes as well:

- utils sso disable
- utils sso status
- utils sso enable
- utils sso recovery-url enable
- utils sso recovery-url disable
- set samltrace level <trace level>
- show samltrace level

- **utils sso disable**

This command disables both (OpenAM SSO or SAML SSO) based authentication. This command lists the web applications for which SSO is enabled. Enter Yes when prompted to disable SSO for the specified application. You must run this command on both the nodes if in a cluster. SSO can also be disabled from graphical user interfce (GUI) by selecting Disable button, under specific SSO in Cisco Unity Connection Administration.

Command Syntax

utils sso disable

- **utils sso status**

This command displays the status and configuration parameters of SAML SSO. It helps to verify the SSO status, enabled or disabled, on each node individually.

Command Syntax

utils sso status

- **utils sso enable**

This command returns an informational text message that prompts that the administrator can enable SSO feature only from graphical user interface (GUI). Both OpenAM based SSO and SAML based SSO cannot be enabled with this command.

Command Syntax

utils sso enable

- **utils sso recovery-url enable**

This command enables the Recovery URL SSO mode. It also verifies that this URL is working successfully. You must run this command on both the nodes if in a cluster.

Command Syntax

utils sso recovery-url enable

- **utils sso recovery-url disable**

This command disables the Recovery URL SSO mode on that node. You must run this command on both the nodes if in a cluster.

Command syntax

utils sso recovery-url disable

- **set samltrace level <trace-level>**

This command enables the specific traces and trace-levels that can locate any error, debug, information, warning or fatal. You must run this command on both the nodes if in a cluster.

Command syntax

set samltrace level <trace-level>

- **show samltrace level**

This command displays the log level set for SAML SSO. You must run this command on both the nodes if in a cluster.

Command syntax

show samltrace level