Troubleshooting Single Sign-On

Security Trust Error Message

Problem When enabling the Single Sign-On feature, a 'Security trust error' message displays.

Possible Cause There may be a security certificate issue causing the IM and Presence Service node to not trust the OpenAM node.

Solution Ensure that the following certificates have been uploaded to the IM and Presence Service node and that the Tomcat service on the IM and Presence Service node has been restarted: OpenAM self-signed certificate if that was the chosen approach when Java was installed and Root certificate and any intermediate certificate that signed the OpenAM certificate if that was the chosen approach when Java was installed. You must also ensure that the correct OpenAM URL is specified on the GUI when enabling SSO. The OpenAM URL must be the Fully Qualified Domain Name with the port number. For example, `https://openam-01.corp28.com:8443/opensso`.

Related Topics

Install Java

"Invalid Profile Credentials" Message

Problem When enabling SSO, an 'Invalid Profile Credentials' message displays.

Possible Cause You may be specifying the incorrect name and password for the IM and Presence Service node J2EE Agent.

Solution Confirm the name and password values that are set for the J2EE agent profile on the OpenAM server. These are the values that you must specify when enabling SSO.

Related Topics

Set Up J2EE Agent Profile On OpenAM Server

"Module Name Is Invalid" Message

Problem When enabling Single Sign-On, a 'Module Name is Invalid' message displays.

Possible Cause You may be specifying the incorrect name for the SSO Module Instance.

Solution Review the instructions to set up the SSO module instance.

Related Topics

Set Up SSO Module Instance

"Invalid OpenAM Access Manager (Openam) Server URL" Message

Problem When enabling Single Sign-On, an 'Invalid OpenAM Access Manager (Openam) Server URL' message displays.

Possible Cause The OpenAM URL specified on the GUI or CLI when enabled SSO may not be correct.

Solution Ensure that the correct OpenAM URL is specified on the GUI when you enable SSO. The OpenAM URL must be the Fully Qualified Domain Name with the port number. For example, `https://server1.cisco.com:8443/opensso`. You must also ensure that the OpenAM server is up and running and that the OpenAM administration GUI is accessible.

Web Browser Indicates a 401 Error

Problem When accessing an SSO-enabled web application for an IM and Presence node, the web browser indicates an HTTP 401 error code.

Possible Cause There may be a problem with the user's browser settings.

Solution Review the instructions to set up the client browser for Single Sign-On.

Related Topics

Client Browser Setup for Single Sign-On

Web Browser Indicates a 403 Error or Displays a Blank Screen

Problem When accessing an SSO-enabled web application for an IM and Presence Service node, the web browser indicates an HTTP 403 error code or I get a blank screen.

Possible Cause There may be a problem with OpenAM policy configuration for this IM and Presence Service node.

Solution Ensure that you added all six policy rules for this IM and Presence Service node and that all policy rules have been enabled with GET/POST actions and are set to Allow. You must also ensure that the Subject has been added to the policy.

Related Topics

Set Up Policies On OpenAM Server

"User is not Authorized to Perform this Function" Error

Problem After accessing the web application and trying to access a page, the following message displays: "User is not authorized to perform this function".

Possible Cause There may be a problem with the user's assigned permissions for IM and Presence Service.

Solution If access to IM and Presence Service web applications is failing, ensure that the user is a member of the *Standard CCM Super Users* group or a group with the equivalent roles on this IM and Presence Service node.

Web Browser Indicates an HTTP 404 Error

Problem When accessing an SSO-enabled web application for an IM and Presence Service node, the web browser indicates an HTTP 404 error code.

Possible Cause There may be a problem with one of the following configurations for this IM and Presence Service node: OpenAM policy configuration or OpenAM J2EE Agent configuration.

Solution Ensure you are not attempting to access this IM and Presence Service node using a URL that contains the hostname only; this is not supported when SSO is enabled for a web application. Review the policy rules for this IM and Presence Service node. Also ensure that you have added the Login Processing URIs to this IM and Presence Service J2EE agent configuration on the OpenAM server.

Related Topics

Set Up Policies On OpenAM Server

Set Up J2EE Agent Profile On OpenAM Server

Web Browser Indicates an HTTP 500 Error or Displays a Blank Screen

Problem When accessing an SSO-enabled web application for an IM and Presence Service node, the web browser indicates an HTTP 500 error code or a blank screen displays.

Possible Cause There may be a problem with OpenAM J2EE Agent configuration for this IM and Presence Service node.

Solution Ensure that you have, 1) added the Login Processing URLs for the J2EE Agent for this node and, 2) that you have added the Login Processing URL on the OpenAM Services tab and removed all other Login URLs.

Related Topics

Set Up J2EE Agent Profile On OpenAM Server

"Authentication Failed" Message

Problem When accessing an SSO-enabled web application for an IM and Presence Service node, the web browser displays an OpenAM login screen with an "Authentication failed" message.

Possible Cause There may be a problem with the WindowsDesktopSSO login module.

Solution Ensure that, 1) all the SSO Module Instance settings are correct, 2) the keytab file exists at the specified directory, and 3) the clocks are synchronized for the following devices:

- **Solution** User's Windows-based computer

- **Solution** Active Directory

- **Solution** OpenAM Server

- **Solution** IM and Presence Service node

Related Topics

Set Up SSO Module Instance

Web Browser Displays OpenAM Login Screen

Problem When accessing an SSO-enabled web application for an IM and Presence Service node, the web browser displays an OpenAM login screen.

Possible Cause There may be a problem with OpenAM J2EE Agent configuration for this IM and Presence Service node.

Solution Ensure you have added the Login URL on the **OpenAM Services** tab and removed all other Login URLs.

Related Topics

Set Up J2EE Agent Profile On OpenAM Server

Web Browser Displays IM and Presence Service Login Screen

Problem When accessing an SSO-enabled web application for an IM and Presence Service node, the web browser displays the web application login screen.

Possible Cause There may be a problem with OpenAM J2EE Agent configuration for this IM and Presence Service node.

Solution Ensure you have added the Login Processing URLs for this IM and Presence Service node J2EE Agent.

Related Topics

Set Up J2EE Agent Profile On OpenAM Server

Internet Explorer Prompts for Username and Password

Problem When accessing an SSO-enabled web application for an IM and Presence Service node, the Internet Explorer web browser prompts you for a username and password.

Possible Cause There may be a problem with the user's browser settings.

Solution Review the instructions to set up the client browser for Single Sign-On.

Related Topics

Client Browser Setup for Single Sign-On

"User has no profile on this organization" Message

Problem When accessing an SSO-enabled web application for an IM and Presence Service node, the web browser displays an OpenAM screen with a "User has no profile on this organization" message.

Possible Cause The OpenAM User Profile may not be set to **ignored**.

Solution See the instructions to set up OpenAM using the GUI Configurator.

Related Topics

Set Up OpenAM Using GUI Configurator

Problems Enabling SSO

Problem You are unable to enable the SSO feature.

Possible Cause If the Tomcat instance on which the OpenAM server is deployed becomes unresponsive or shuts down unexpectedly, you may not be able to enable the SSO feature on IM and Presence Service. In order to enable SSO successfully on IM and Presence Service, OpenAM must be operational. IM and Presence does not monitor the OpenAM Tomcat instance. As a result, no IM and Presence Service alarm or notification generated for this occurrence.

Solution If you experience difficulty when enabling SSO from either the Cisco Unified IM and Presence Operating System Administration GUI, verify that Tomcat is running on the OpenAM server. If you continue to experience difficulty after verifying that Tomcat is running on the OpenAM server, restart Tomcat on the OpenAM server and try enabling SSO again.

Solution When Tomcat crashes on the OpenAM server, OpenAM becomes unresponsive; IM and Presence Service may not be notified.

Certificate Failure

Problem When using the Certificate Import Tool to validate the communication between OpenAM and IM and Presence Service, you may encounter an error with the "Verify SSL connectivity to the specified certificate server" test. This test may fail with the following error: "The Troubleshooter has encountered an internal error".

> **Possible Cause** This error may be the result of the way the OpenAM/Tomcat instance has configured its HTTP Connector.

Solution Perform the following steps to resolve the certificate failure.

1. Locate the server.xml configuration file on the OpenAM/Tomcat server. This file is typically located here:

    ```
    C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf\server.xml
    ```

2. Check the value set for the **clientAuth** attribute of the **Connector** with a port value of 8443. If this attribute is set to True, this can cause the **Certificate Import Tool** to fail.

3. Change the **clientAuth** attribute to **want** or **false**.

4. Restart the Tomcat service on the OpenAM server.

5. Re-run the **Certificate Import Tool** and import the OpenAM certificate into IM and Presence Service.

6. Change the **clientAuth** attribute back to its original value.

7. Restart the Tomcat service on the OpenAM server.

Related Topics

> Import OpenAM Certificate Into IM and Presence Service