Single Sign-On

This section includes troubleshooting topics about single sign-on (SSO) issues.

SSO Fails After Completing Disaster Recovery Operation

Problem When a user completes a disaster recovery operation, SSO fails due to expired certificates.

Possible Cause Existing SSO certificates were installed before the application was installed.

Solution Reinstall SSO certificates after completing Disaster Recovery Operation. After you perform your restoration on the disaster recovery system, sign in to the Administration site and select **Settings** > **Security** > **Certificate** > **SSL Certificate** > **Generate CSR**.Under **More Options**, select **Download CSR** to download the generated CSR. Use the CSR to obtain a new SSL Certificate. Refer to the "Generating SSL Certificates" section of the Administration Guide for more information. Import your new SSL certificate by selecting **Settings** > **Security** > **Certificate** > **More Options** (Import SSL Certificate). Import the same SSL certificate into your ADFS (Active Directory Federation Service) for the site URL's relay party.

SSO Protocol Error

Problem You receive the error message, "SSO protocol error. Contact your administrator for further support."

Possible Cause Your SSO administration site or IdP configuration contains errors.

Possible Cause SSO is not enabled.

Possible Cause Some or all of the required IdP attributes are not configured: firstname, lastname, email.

Possible Cause The NameID parameter of your SAML is not set to email.

Solution If you are unable to determine the cause of your SSO protocol error, generate a log and contact the Cisco TAC for further assistance. If you believe the cause is one of the above, make sure the required IdP

attributes are configured and make sure the following IdP attributes are set to the user's email address: uid, SAML_SUBJECT..

SSO Redirection Has Failed

Problem A user attempts to sign in and receives a "SSO Redirection Failed" message. The user is directed to an administrator for help.

Possible Cause An IdP attribute value in the user's account has violated account regulations. The following error messages can appear as a result of this problem:

- **Possible Cause** SSO protocol error. Contact your administrator for further support. See SSO Protocol Error, on page 1 for more information.
- **Possible Cause** No user account found in the system. Contact your administrator for further support.
- **Possible Cause** No X.509 certificate found in the system. Contact your administrator for further support.
- **Possible Cause** X.509 certificate has expired. Contact your administrator for further support.
- **Possible Cause** User account is locked. Contact your administrator for further support.
- **Possible Cause** User account is expired. Contact your administrator for further support.
- **Possible Cause** User account has been deactivated. Contact your administrator for further support.
- **Possible Cause** SAML assertion is expired. Contact your administrator for further support.
- **Possible Cause** Invalid Response message. Contact your administrator for further support.
- **Possible Cause** Auto Account Creation failed. Contact your administrator for further support. See Auto Account Creation or Auto Account Update Has Failed for more information.
- **Possible Cause** Auto Account Update failed. Contact your administrator for further support. See Auto Account Creation or Auto Account Update Has Failed for more information.
- **Possible Cause** SSO protocol error. Contact your administrator for further support.
- **Possible Cause** No user name found in SAML assertion. Contact your administrator for further support.
- **Possible Cause** Only POST request is supported. Contact your administrator for further support.
- **Possible Cause** Incorrect SAML SSO POST data. Contact your administrator for further support.
- **Possible Cause** A Cisco WebEx Meetings Server certificate has not been imported into the SAML IdP.
- **Possible Cause** The site is not allowed to use SSO. Contact your administrator for further support.
- **Possible Cause** Incorrect X.509 certificate to validate SAML assertion. Contact your administrator for further support. See Incorrect X.509 Certificate to Validate SAML Assertion for more information.
- **Possible Cause** Loading configuration error. Contact your administrator for further support.

- **Possible Cause** The value of NameQualifier does not match site URL. Contact your administrator for further support.
- **Possible Cause** Unable to reach Assertion Party. Contact your administrator for further support.
- **Possible Cause** Failed to resolve SAML Artifact. Contact your administrator for further support.
- **Possible Cause** Invalid SAML Assertion. Contact your administrator for further support.
- **Possible Cause** Recipient does not match webex.com. Contact your administrator for further support.
- **Possible Cause** SAML assertion is unsigned. Contact your administrator for further support.
- **Possible Cause** User role is not allowed to login. Contact your administrator for further support.
- **Possible Cause** Invalid RequestedSecurityToken. Contact your administrator for further support.
- **Possible Cause** Invalid digital signature. Contact your administrator for further support.
- **Possible Cause** Untrusted Issuer. Contact your administrator for further support.
- **Possible Cause** Name Identifier format is incorrect. Contact your administrator for further support.
- **Possible Cause** Unable to generate AuthnRequest. Contact your administrator for further support.
- **Possible Cause** Unable to generate Logout Request. Contact your administrator for further support.
- **Possible Cause** InResponseTo does not match the request ID. Contact your administrator for further support.
- **Possible Cause** Invalid Request message. Contact your administrator for further support.
- **Possible Cause** Auto Account Creation failed. Contact your administrator for further support.
- **Possible Cause** Auto Account Update failed. Contact your administrator for further support.
- **Possible Cause** Update user privilege failed or user is not allowed to update user privilege. Contact your administrator for further support.

Solution Examine your URL API to determine which account values are causing the failure. Refer to the "Setting and Changing SSO URL API Parameters" section in the Planning Guide for more information.

SSO Error Codes

The following table lists the SSO error codes.

Error Description	Error Code
SSO protocol error	1
No user name found in SAML assertion	2
No user account found in the system	3
No X.509 certificate found in the system	4
Only POST request is supported	5

Error Description	Error Code
Incorrect SAML SSO POST data	6
The site is not allowed to use SSO	7
Incorrect X.509 certificate to validate SAML assertion	8
Loading configuration error	9
The value of NameQualifier does not match site URL	10
Unable to reach Assertion Party	11
Failed to resolve SAML Artifact	12
Invalid SAML assertion	13
Recipient does not match webex.com	14
X.509 certificate has expired	15
User account is locked	16
User account is expired	17
User account has been deactivated	18
SAML assertion is expired	19
SAML assertion is unsigned	20
User role is not allowed to login	21
Invalid RequestedSecurityToken	22
Invalid digital signature	23
Untrusted Issuer	24
Name Identifier format is incorrect	25
Unable to generate AuthnRequest	26
Unable to generate Logout Request	27
InResponseTo does not match the request ID	28
Invalid Response message	29
Invalid Request message	30
Auto Account Creation failed	31
Auto Account Update failed	32