Cisco webex

Customer Care Message

Cisco WebEx: Important Cisco WebEx Changes Impacting WebEx APIs

Versions:

- XMLAPI 8.0.0
- XMLAPI 7.3.0
- XMLAPI 6.0.0 SP5
- XMLAPI 5.9.0 SP3
- XMLAPI 5.8.0 SP3
- XMLAPI 5.6.0 SP2
- XMLAPI 5.5.0 SP2
- XMLAPI 5.4.0 SP3

Dear WebEx API Developer,

Cisco WebEx is sending this message to key business contacts. This notification applies to your integrations.

On December 5, 2014 between 7:00 p.m. and 11:59 p.m. PDT (GMT-7), Cisco will be enabling certain functionality on your WebEx service that may impact your WebEx users and have an effect on your integrated 3rd party applications.

The changes detailed below have already been introduced to your WebEx service in a previous release and available for you to use.

Upon request, Cisco can enable these changes in advance for you to test your changes. Cisco strongly recommends you enable these changes on your development site (provided through the Gold Developer Program) AND update/test your integrations several weeks in advance of December 5, 2014. If you are not part of the Gold Developer Program you should contact the third party application vendor to make sure your application is compliant with the changes below.

API CHANGES

#1 Require SSL when accessing the WebEx service using WebEx APIs

Description:

This enhancement will not allow any API calls made via an http connection; it will only allow calls made via https (SSL protocol). Please refer to Developer Guide for examples.

Affected APIs:

All URL and XML APIs

#2 SSO Sites ONLY: De-support of SAML 1.1 and SAML 2.0 Federation Update

Customer Care Message

Description:

To date, SAML 1.1 has been supported for WebEx Federated SSO Authentication Services. The WebEx Federated Authentication Service (FAS) allows employees and affiliates of a WebEx customer organization to authenticate with a WebEx site using the SAML 1.1, 2.0 or WS-Federation 1.0 protocols. Moving forward, Cisco will only support SAML 2.0 federation for SSO WebEx Authentication Services.

Key impact is that for existing SSO-enabled sites, local account passwords will be removed for all regular users, as SAML 2.0 protocol does not permit local passwords. New SSO sites that are created after this change takes effect will no longer be able to create local passwords for regular users. This change only affects regular (non-Administrator) users. Administrator users can still access WebEx services using a local password.

Thus, all sites that are SSO enabled will no longer be able to use local WebEx account passwords to access WebEx services, through WebEx APIs.

Cisco requires you to do the following:

- Configure your SSO site to use SAML 2.0, if not already configured for SAML 2.0
- Change your API based integration to assume local account passwords will not be available on WebEx servers. Modify integration implementation to use *username + session ticket*, instead of *username + password* for authentication.

Affected APIs:

CreateUser, SetUser, Login Module, URL API p.php(AT=SU,EU,LI)

#3 Non-SSO Sites ONLY: Re-authentication and Password Requirement

Description:

Users who wish to change their email address or password through the WebEx APIs will be required to provide their current password when making the API call. This is to comply with new requirement that user need to re-authenticate, if their emails or password changes. Administrators are not impacted by this change, except when changing their own password or email address. An administrator can change a user's email address or password using the WebEx APIs without the need to provide the user's password. If a Host or Attendee user tries to change a password or email address using XML API with an exception error ID = 030084 will be thrown.

Affected APIs:

SetUser, URL API p.php (AT=LI,EU)

Cisco webex

cisco

Customer Care Message

#4 POST only for APIs requiring password – WBS29/XML 8.0.0 Only

Description:

Cisco will drop support for GET calls for all XML APIs, and specific URL APIs that accept password as parameter. Cisco has provided support for POST HTTP method for many URL APIs that accept passwords as parameters. Cisco requires you to convert any GET calls to POST based calls for the affected APIs.

Affected APIs:

All URL and XML APIs that accept password as parameter.

Please refer to the Important Cisco WebEx Changes Impacting WebEx APIs (FAQs) for more details.

#5 Change in return value from GetJoinURLMeeting API – XML API 8.0.0 only

Description:

Mentioned API will start returning Join Meeting URL in a different format. The newer format is more secure but it is not possible to parse it and identify parameters anymore. Your integration can continue to add “BU” parameter to the new join URL returned. Example of new join URL: https://[site].webex.com/[site]/j.php?MTID=m6e35befcb24b5868e5298ac9800dbd69.

Affected APIs:

GetJoinURLMeeting

To Contact Support

For more information about the product enhancements to your service please reference the Important Cisco WebEx Changes Impacting WebEx APIs (FAQs).

Please contact webex-meetings-api-dev@cisco.com if you encounter any issues or have questions about the deployment.

Please contact your Customer Success Manager to get these features enabled before the December 5, 2014 deadline, or contact your third party application vendor to make sure your integration is compliant with these changes.

Failure to comply with the **December 5, 2014** deadline could result in host account that are no longer able to schedule or start WebEx meetings when using an integration or the WebEx APIs.

Customer Care Message

Regards,

Product Management

Cloud Collaborations Application Technology Group