



Auto Account Creation with MEETS when using SSO with WebEx

1) Auto Account Creation:

When using Single Sign-On (SSO), one can have WebEx automatically create accounts for users when they join WebEx via a SAML IdP. This allows a user who does not already have a WebEx account to create an account by merely logging into WebEx via an IdP.

The MEETS integration platform for LMSs also has the ability to auto-create WebEx accounts with or without WebEx being in SSO mode.

2) Settings in WebEx and MEETS to allow auto account creation:

In the WebEx SSO configuration, checking “Auto Account Creation” will allow the SAML IdP to automatically create WebEx accounts if it relays information about who the user logging in is.

In MEETS, turning on auto account creation is described on page 22 of the MEETS administration panel manual:

https://documentation.cirqlive.com/manuals/Admin%20Panels/Admin_Panel_for_MEETS_for_WebEx.pdf

3) SAML Assertion metadata required for auto account creation via a SAML IdP:

For a SAML IdP to create a WebEx account when this feature is enabled, assertions sent to WebEx must include the following metadata attribute fields: uid, email, firstname, and lastname.

More information about these and other attributes can be found at:

<http://kb.webex.com/WBX67566>

4) User ID defined when creating a WebEx account

When creating a WebEx account, a user ID (uid) must be sent via the SAML Assertion. WebEx user IDs are up to 64 characters in length, and can consist of letters, numbers, dashes, underscores, periods, and the @ symbol.

Often, the user name or user ID from the institution directory, when compliant, is the uid administrators will choose to send to WebEx via SAML Assertions.

When MEETS creates accounts in WebEx, since it has no access to the institution’s directory to retrieve the current user’s internal user ID or name, and as it must ensure user IDs for WebEx

are within WebEx's limitations and non-conflicting, MEETS uses the following system when assigning a user ID when creating a WebEx account:

"MEETS_AUTOGEN_" followed by a hexadecimal encoding of the user's ID number as it exists internally to MEETS. (User IDs in MEETS are simply assigned numerically ascending based on the order MEETS first encountered a user.)

5) How WebEx identifies users joining via an IdP:

As Above, a Webex account must contain a user ID, first name, last name and e-mail address.

When a user joins WebEx via an IdP, they will visit the WebEx website bearing a SAML Assertion which defines who they are. The key variable in the SAML Assertion for this is the "NameID" parameter. Contained within this parameter is the value WebEx will use to identify who a user is. How WebEx uses this information depends on the "Format" attribute of the "NameID" parameter.

If the "Format" is missing or set to some "unspecified" resource name, WebEx will "guess" which fields to look at for identifying a user. This at times can have unpredictable consequences. However, WebEx can also be told specifically which WebEx user fields to compare against when looking up an existing user.

If the "NameID" "Format" in the SAML Assertion is one of the following:

- X.509 Subject Name (urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName)
- Entity Identifier (urn:oasis:names:tc:SAML:2.0:nameid-format:entity)
- Persistent Identifier ("urn:oasis:names:tc:SAML:2.0:nameid-format:persistent")

then WebEx will compare the value contained within the "NameID" parameter against the uid field in its database.

If the "NameID" "Format" in the SAML Assertion is Email address (urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress), then WebEx will compare the value contained within the "NameID" parameter against the email field in its database.

Note: If the "NameID" "Format" specified in an assertion conflicts with the configuration option in the WebEx SSO settings, then the user bearing that assertion will be prevented from entering WebEx. If the NameID Format configuration option in WebEx is set to "Unspecified", all the aforementioned NameID Format resource names are allowed.

6) Enabling users joining WebEx via an IdP to use an account created by MEETS

1. Ensure that the e-mail addresses assigned to users in their LMS, which is relayed to MEETS, is identical to the e-mail addresses assigned to users in WebEx.
2. Set the NameID Format in SAML Assertions to Email address (urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress).

This will inform WebEx to lookup users against the email field in WebEx's database which will be identical when relayed to it via an IdP or MEETS.

Having an identical e-mail address in an LMS and WebEx will also allow MEETS to find preexisting accounts for WebEx users. However, unlike typical IdP entry, MEETS uses the WebEx APIs and can automatically adapt to finding existing WebEx users whichever NameID Format configuration option is chosen in WebEx, as long as it can find the same e-mail address for a user in the system.

Summary:

Automatic WebEx account creation when using SSO is available via the institution IdP as well as via the MEETS platform. The primary difference for WebEx accounts created by these two platforms is the value assigned in the uid field. Other important information (first name, last name, and e-mail address) is identical assuming the LMS has the same information as the IdP.

To enable WebEx to identify users joining via the institution IdP for accounts created by MEETS, the NameID Format set in SAML Assertions must be email.

Notes:

- 1) If one wishes to use a NameID Format in SAML Assertions other than email, then WebEx will not be able to identify users joining via an IdP when their account was created by MEETS. Therefore, if one wishes all users to be able to authenticate with WebEx via the institution's IdP, one must turn off auto-account creation in MEETS, and users must create their accounts by logging into WebEx via the institution IdP.
- 2) If one modifies their e-mail address, identification of users in WebEx will work fine as long as the e-mail address is updated in both the IdP's directory and WebEx simultaneously.
- 3) One should avoid altering user IDs in WebEx as that can cause issues, as WebEx-related data is normally bound against the uid field.
- 4) When using SSO with WebEx, what the uid field contains in WebEx does not need to be memorized by users, nor does it affect them, as WebEx will never prompt a user for this information.