

# GoToMeeting (IdP-initiated) Integration Guide

## Introduction

Use this guide to enable Multi-Factor Authentication and Single Sign-on (SSO) access via SAML to Citrix GoToMeeting.

## Prerequisites

### 1. Have a GoToMeeting account

The primary administrator account is required for the configuration

### 2. Create a **New Realm** for the GoToMeeting integration

### 3. Configure the following tabs in the Web Admin before configuring the **Post Authentication** tab:

- **Overview** – the description of the realm and SMTP connections must be defined
- **Data** – an enterprise directory must be integrated with SecureAuth IdP
- **Workflow** – the way in which users will access this application must be defined
- **Multi-Factor Methods** – the Multi-Factor Authentication methods that will be used to access this page (if any) must be defined

## SecureAuth IdP Configuration Steps

## ▼ Profile Fields

Property	Source	Field	Data Format	Writable
Groups	<a href="#">Default Provider</a>	memberOf		<input type="checkbox"/>
First Name	<a href="#">Default Provider</a>	givenName		<input type="checkbox"/>
Last Name	<a href="#">Default Provider</a>	sn		<input type="checkbox"/>
Phone 1	<a href="#">Default Provider</a>	telephoneNumber		<input checked="" type="checkbox"/>
Phone 2	<a href="#">Default Provider</a>	mobile		<input checked="" type="checkbox"/>
Phone 3	<a href="#">Default Provider</a>	homePhone		<input checked="" type="checkbox"/>
Phone 4	<a href="#">Default Provider</a>	Pager		<input checked="" type="checkbox"/>
Email 1	<a href="#">Default Provider</a>	mail		<input checked="" type="checkbox"/>
Email 2	<a href="#">Default Provider</a>	GoToMeeting ID		<input type="checkbox"/>

1. In the **Profile Fields** section, map the directory field that contains the user's GoToMeeting ID to the SecureAuth IdP **Property**

For example, add the GoToMeeting ID **Field** to the **Email 2 Property** if it is not already contained somewhere else



Click **Save** once the configurations have been completed and before leaving the **Data** page to avoid losing changes

## Post Authentication

## ▼ Post Authentication

Authenticated User Redirect:

Redirect To:

Upload a Page:  No file chosen

[Download Customized Pages](#)

2. Select **SAML 2.0 (IdP Initiated) Assertion Page** from the **Authenticated User Redirect** dropdown in the **Post Authentication** tab in the Web Admin
3. An unalterable URL will be auto-populated in the **Redirect To** field, which will append to the domain name and realm number in the address bar (Authorized/SAML20IdPInit.aspx)
4. A customized post authentication page can be uploaded, but it is not required

## User ID Mapping

### ▼ User ID Mapping

User ID Mapping:  Transformation Engine

Name ID Format:

Encode to Base64:

5. Select the SecureAuth IdP **Property** that corresponds to the directory field that contains the GoToMeeting ID (**Email 2**)
6. Select **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress** from the **Name ID Format** dropdown
7. Select **False** from the **Encode to Base64** dropdown

## SAML Assertion / WS Federation

## ▼ SAML Assertion / WS Federation

WSFed Reply To/SAML Target URL:

SAML Consumer URL:

WSFed/SAML Issuer:

SAML Recipient:

SAML Audience:

SP Start URL:

WS-Fed Version:

WS-Fed Signing Algorithm:

SAML Signing Algorithm:

SAML Offset Minutes:

SAML Valid Hours:

8. Set the **SAML Consumer URL** to **https://login.citrixonline.com/saml/global.gotomeeting.com/acs**

9. Set the **WSFed/SAML Issuer** to a Unique Name that is shared with GoToMeeting

The **WSFed/SAML Issuer** value must match exactly on the SecureAuth IdP side and on the GoToMeeting side

10. Set the **SAML Offset Minutes** to make up for time differences between devices

11. Set the **SAML Valid Hours** to limit for how long the SAML assertion is valid



No configuration is required for the **WSFed Reply To/SAML Target URL**, **SAML Recipient**, **SAML Audience**, or **SP Start URL** fields

Signing Cert Serial Number:  [Select Certificate](#)

Assertion Signing Certificate: [certificate.wse3.cer](#)

Domain:

Metadata File: [Download](#)

12. Leave the **Signing Cert Serial Number** as the default value, unless there is a third-party certificate being used for the SAML assertion

If using a third-party certificate, click **Select Certificate** and choose the appropriate certificate

GoToMeeting requires the certificate to be in *PEM* format

13. Download the **Assertion Signing Certificate**, which is used in the GoToMeeting Configuration Steps

 Click **Save** once the configurations have been completed and before leaving the **Post Authentication** page to avoid losing changes

#### Forms Auth / SSO Token

##### ▼ Forms Auth/SSO Token

Key Generation: [View and Configure FormsAuth keys/SSO token](#)

14. Click **View and Configure FormsAuth keys / SSO token** to configure the token/cookie settings and to configure this realm for SSO

 These are *optional* configurations

## ▼ Forms Authentication

Name:	<input type="text" value=".ASPXFORMSAUTH"/>
Login Uri:	<input type="text" value="SecureAuth.aspx"/>
Domain:	<input type="text"/>
Require SSL:	<input type="text" value="True"/>
Cookieless:	<input type="text" value="UseDeviceProfile"/>
Sliding Expiration:	<input type="text" value="False"/>
Timeout:	<input type="text" value="10"/> Minute(s)

1. If SSL is required to view the token, select **True** from the **Require SSL** dropdown
2. Choose whether SecureAuth IdP will deliver the token in a cookie to the user's browser or device:
  - **UseCookies** enables SecureAuth IdP to always deliver a cookie
  - **UseUri** disables SecureAuth IdP to deliver a cookie, and instead deliver the token in a query string
  - **AutoDetect** enables SecureAuth IdP to deliver a cookie if the user's settings allow it
  - **UseDeviceProfile** enables SecureAuth IdP to deliver a cookie if the browser's settings allow it, no matter the user's settings
3. Set the **Sliding Expiration** to **True** if the cookie remains valid as long as the user is interacting with the page
4. Set the **Timeout** length to determine for how many minutes a cookie is valid

 No configuration is required for the **Name**, **Login URL**, or **Domain** fields

## Machine Key

### Machine Key

Validation:

Decryption:

Validation Key:

Decryption Key:

5. No changes are required in the **Validation** field, unless the default value does not match the company's requirement

If a different value is required, select it from the dropdown

6. No changes are required in the **Decryption** field, unless the default value does not match the company's requirement

If a different value is required, select it from the dropdown



No configuration is required for the **Validation Key** or **Decryption Key** fields

## Authentication Cookies

### Authentication Cookies

Pre-Auth Cookie:

Post-Auth Cookie:

Persistent:

Clean Up Pre-Auth Cookie:

7. Enable the cookie to be **Persistent** by selecting **True - Expires after Timeout** from the dropdown

Selecting **False - Session Cookie** enables the cookie to be valid as long as the session is open, and will expire once the browser is closed or the session expires

 No configuration is required for the **Pre-Auth Cookie**, **Post-Auth Cookie**, or the **Clean Up Pre-Auth Cookie** fields

Click **Save** once the configurations have been completed and before leaving the **Forms Auth / SSO Token** page to avoid losing changes

 To configure this realm for SSO, refer to [SecureAuth IdP Single Sign-on Configuration](#)

 To configure this realm for *Windows Desktop SSO*, refer to [Windows desktop SSO configuration](#)

The screenshot shows the 'Identity provider' configuration page in the Citrix Organization Center. The page has three tabs: 'Email domains', 'Identity provider', and 'Users'. The 'Identity provider' tab is active. Below the tabs, there is a text block explaining that users can log into Citrix products using credentials managed by the user, and that the Identity Provider can be configured to allow users to log in from either the identity provider's website or from the Citrix product's website using the 'Use my company ID' link.

Below the text, there is a dropdown menu set to 'Manual'. The 'Sign-in page url' field contains 'https://secureauth.company.com/SecureAuth2'. The 'Sign-out page url (optional)' field contains 'https://secureauth.company.com/secureauth2/restart.aspx'. The 'Identity Provider Entity ID' field contains 'UniqueName'. The 'Verification certificate' field has a text input area with the placeholder 'Paste or upload certificate' and a blue 'Upload certificate' button. At the bottom right, there are 'Delete' and 'Save' buttons.

© 2015 Citrix Systems, Inc. All rights reserved. Support | About Us | Terms of Service | Privacy Policy

1. Log into the **Citrix Organization Center** (<https://account.citrixonline.com/organization/administration/>)
2. Select **Identity provider** from the top menu
3. Select **Manual** from the dropdown
4. Set the **Sign-in page url** to the Fully Qualified Domain Name (FQDN) of the SecureAuth IdP appliance, followed by the GoToMeeting-integrated realm, e.g. **https://secureauth.company.com/SecureAuth2**
5. Set the **Sign-out page url** to the FQDN of the SecureAuth IdP appliance, followed by the GoToMeeting-integrated realm, and **/restart.aspx**, e.g. **https://secureauth.company.com/secureauth2/restart.aspx**
6. Set the **Identity Provider Entity ID** to the same Unique Name set in the SecureAuth IdP Web Admin (step 9)
7. Paste the contents of the **Assertion Signing Certificate** from the SecureAuth IdP Web Admin (step 13) into the **Verification certificate** field, or click **Upload certificate** to upload the certificate file
8. Click **Save**