

Configure SAML Authentication

You can configure your Organization to utilize a SAML Identity Provider for quick and secure access. In this documentation we will show how to configure with EvolveIP's Identity and Access Management. Other vendors can be configured with the same general settings, however their support team might need involved if there are issues during the setup.

Configuring SAML is comprised of these steps:

1. [Configure your Service Provider \(in this case, EvolveIP's Identity and Access Management / ClearLogin\) for your vCloud Organization.](#)
2. [Configure your vCloud Organization with the configuration metadata XML from your service provider.](#)
3. [Configure your vCloud Organization with the user accounts to allow access.](#)
4. [Bypass SAML if there is an issue.](#)

When an imported user attempts to log in, the system extracts the following attributes from the SAML token, if available, and uses them for interpreting the corresponding pieces of information about the user:

- email address = "EmailAddress"
- user name = "UserName"
- user's groups = "Groups"
- user's roles = "Roles" (this attribute is configurable)

Group information is used if the user is not directly imported but is expected to log in by being a member of an imported group. A user can belong to multiple groups, so can have multiple roles during a session.

If an imported user or group is assigned the Defer to Identity Provider role, the roles are assigned based on the information gathered from the Roles attribute in the token. If a different attribute is used, this attribute name can be configured using API and only the Roles attribute is configurable. If the Defer to Identity Provider role is used, but no role information can be extracted, the user can log in but has no rights to perform any activities. With that information, we typically recommend against importing users or groups using the Defer to Identity Provider role.



Local User Account

You should keep an enabled local Org Admin account in case you need to bypass SAML.

If you subscribe to Self-Service BaaS, SAML credentials cannot be used to log into your Self-Service portal. You will **NEED** to use a local (non-SAML) Org Admin account when logging into your BaaS Self-Service portal.

Prerequisites

This operation requires the rights included in the predefined Organization Administrator role or an equivalent set of rights.

This operation requires you have administrative rights to create SAML applications within your Identity Provider.

Procedure

Configure your Identity Provider

1. Navigate within your Identity Provider (IDP) to create a new SAML App.
 - a. **Display Name:** Provide a display name
 - b. **Login URL (ACS):** This is the login URL for your vCloud Director tenant. This can be found by downloading the XML info from your vCloud Organization.
 - i. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore.
 - ii. From the main menu select **Administration**.
 - iii. In the right panel under **Identity Providers**, click **SAML**.
 1. Click on the **Metadata** link and download the .xml
 - a. The Login URL will be towards the bottom under the section "<md:AssertionConsumerService Location" and will be in this format:
 - i. **`https:// (vCloud URL) /login/org/ (Organization Name) /saml/SSO/alias/vcd`**
 - ii. For example, if your vCloud URL is `https://vcloud.evolveip.net` and your Organization Name is "Test" the Login URL would be:
 1. **`https://vcloud.evolveip.net/login/org/test/saml/SSO/alias/vcd`**
 - c. **Logout URL (ACS):** This is the logout URL for your vCloud Director tenant. This can be found by downloading the XML info from your vCloud Organization.
 - i. On the **Virtual Datacenters** dashboard screen, click the card of the virtual data center you want to explore.
 - ii. From the main menu select **Administration**.
 - iii. In the right panel under **Identity Providers**, click **SAML**.
 1. Click on the **Metadata** link and download the .xml
 - a. The Logout URL will be towards the bottom under the section "<md:SingleLogoutService Location" and will be in this format:
 - i. **`https:// (vCloud URL) /login/org/ (Organization Name) /saml/SingleLogout/alias/vcd`**

Import Groups

Source: SAML

Enter the group names

vcloudorgadmin

Group names must be in the same identifier format supported by the SAML identity provider configured for the organization. Use a new line for each group name.

Assign Role: Organization Administrator

DISCARD SAVE

ii.

- c. Click **Save** to complete the process of importing groups for SAML authentication.

You should now be able to authenticate utilizing your SAML IDP into vCloud. If you run into any issues please [contact EvolveIP Support](#).

Bypass SAML

In the event that there is an issue with either the IDP or Service Provider preventing sign in via SAML authentication, you can bypass SAML authentication.

To do this, manually enter the tenant URL of your vCloud Organization adding "/login" to the end of the URL.

For example, if your vCloud URL is `https://vcloud.evolveip.net` and your Organization Name is "Test".

The URL used to bypass SAML would be ***https://vcloud.evolveip.net/tenant/test/login***

You will then be presented with the local username and password prompt. You will need to provide local credentials in order to access the system.