# **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.

#### A 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
        - 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

- 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/SingleLogout/alias/vcd
- d. App URL Override: This is the tenant URL you would use to log into vCloud Director.
  - i. 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/tenant/test

- e. NameID Value: This is the main username attribute that will be sent. This attribute is what vCloud will validate against when signing
- in. We typically recommend using {{Idap.sAMAccountName}} as the value. f. Attributes: These are the attributes that will populate the imported user account upon first sign in. Att

ibutes	
UserName	{{ldap.sAMAccountName}}
EmailAddress	((ldap.mail))
FullName	{{ldap.sn}}

- g. Attribute Format: Use the following: urn:oasis:names:tc:SAML:2.0:attrname-format:basic
- h. Digest Method: SHA256

i.

2. The configured system should look like this:

VLAND SHOEL NULESS		0
on		
Theorem Bills   the Distances		
Accepted Access Tags		
v #Cloud Test		
house the access tags that you no	ald like to allow access to this App Connection. If none are selected then all users will be given access.	
/EA Access Tags		
thoose the access tags that you no	ald like to trigger an MMA prompt. If name are selected, there will be no restrictions.	
/FA bureton Forever?		
24 Hours		
he leigh of line to wait after a use	r has laurched as app to prompt for MPA.	
ogin URL (ACS)		
https://voload.evolveip.net/fo	pin/org/test/semi/550/alos/vod	
he of used to solved the SAM, Pier	pani, Tesporae.	
opeut URL (SLO) (Optional)		
https://scload.exolveip.net/lo	pin/org/text/sami/SingleLogoLt/allas/vod	
optional ari used to logisut from the	ordernal application.	
op URL Overvice (Optional)		
https://voload.evolvetp.net/te	nan(/test	
phonal art used for an 3P initiated I	lan.	
Adence Restriction		
the second second second		
KometD Volue		
(gap.tAMAccountName)		
tomo D Comme		
Line Report Format		
SAML Nomespace		
SAML Nomespace soni Tecomespace to are on the same	erf daarnen.	
GAML Nonrespace sonil the namespace to use on the signed	sof duarwet.	
SAML Nomespace sole) tenamespace to use on the signed Windowles	eri duarwet	
SAML Nomespace seni tenanespace to use on the topic tenbutes Userbane	ert horvest.	
SAM, Nerrespace sent teraneque to un or te spec terbores Usedhare	en bornet. [Bits stMhoovertrent]	•
SAM, Nerrespace sent tenanequarito use on the signal Ministres UseName EmailAddress	(1975) (1990) (1	-
AML Nerrospace sant Terrorepace to use on the topic Arributes UseName EmalAdores FullName	nel increas.	
SAML Namespace Sam Terranequice to an or the topic United to an or the topic EnsetAddress FullName	nel harvest   [blas addass.vflwrei]   [blas add]   [blas ad]	
ANE, Nonespece sant Tenansepece Sciences to the signed Weblane DealAddress FullName FullName	nel accent [Bits allocardine]] [Bits enfit [Bits enfit	
AML Nonespece Sent Intervention to use on the segred Mitholes UseRisere EmailAddress FullName Ambuse Fornat	al horses ) [Bite Million Allow] ] [Bite well ] [Bite well	IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
KMR, Norrespace soni Interampiane to see on the topped Mithodes UseNance FullNance FullNance Mithodes Format um pasile namestic SAML 2.0.	on Hannes [Balag Makhours Hanne] [Balag Makhours Hanne] [Balag Makhours Hanne] Stephen Annes Stephen Annes	- E D Mar Antone -
XML, Menepooe sand the menepole to one on the topole Methodes Deskilddees Faiblane Faiblane Attribute Forent wareautionameets SAML2.0 he forent operated for any addition	or House ( Day Milosoftward) ( Darwell ( Darwell ( Darwell Milosoftward) Arrowska Marka Arrowska Marka Arrowska Marka Arrowska Marka Arrowska Marka Arrowska Marka Arrowska Marka Arrowska Marka Arrowska Marka Arrowska Marka Arrowsk	- - - - - - -
Add, Nemispace Add Testingtace to cer of the types Add UseRane Fullikane Exclusive Format annowed format Medy Add Cer and Add Cer Add Cer and Cer Mark Status	on laws.	a a Maria and Anno Anno Anno Anno Anno Anno Anno Anno
UAN, Nempore See To an impact to an of the lapso darbotics UserNarke EmailAddress FullName Exablate Format an south comments (SAUL2.0 In the horn operated for any addition Methy 304.7	of howse (Bay with summary) (Bay with Section 2) Section 2) Se	-
VAM, Nempore Seri Internet and Series of Series United Series Ser	of laws	a B Markatar -
VAIA, Nempore Self Teramonasti Li vili vi Teragon Usefurio Emalitàdoses Fullisme Establisto fonuti umasteramento: SAML2.2 In Inno appundo fu un addito Mello destinon Mello destinon	on Hannes (Bala Addisour Shared) (Bala Addisour Shared) (Bala Addi Shared) Stream Control Addisour Shared Shared Market Shared Shared Shared Shared Market Shared Shared Shared Shared Shared Shared Shared Share	-
VAM, Nempson Soort	or Houses	
Adda, Nempore Seri Teramonan to and on the legan UseRenze DuralAddess Fullecrea Fullecrea Instance Series Instance Se	In iteration	-
Add, Hempsone Self Hommonyan Li ani vi his lagen Arbitras Userbare Userbare Fuldkense Fuldkense Kriskade Format In salaka Format	In the second se	
Adda, Nemrepore Seri Formanipues to carl or the topic UseRearce EurostAddess Euro	In House I Be Allowarteng Bernet Be	-
Adda, Hennysone Badf Mananopus II. and an Yes Lapon Architek Danaladores Danaladores Fuldbane Architek Architek Architek Architek Architek Architek Marky SAK7 Malk Comments Marky SAK7	In the second se	
Add, Hermpool Self Hommonyan Louis V for Lipse Archives (UseRives Fuelkines Fuelkines Archives Arc	In the second se	
Adda, Hennyanoe and Hanamapan Ku, and Khang Hanamapan Harbura Danakhadowa Kathara Kathara Kathara Kathara Kathara Kathara Kathara Mala Casthora Mala Casthor	In Florent	
UAL Harroyse MI Marine and Marine and Karan Marine and Marine Marine and Marine Mari	In Hannes	-
UAL Networkson	In the second s	
UAL Networks	In the set of the set	
UAS Harrowski and Starter Star	Windows	
MAX Humper Home Service and Annual A	With Names	
UAA Humper Mit Carl and the second s	In House In the second	• • • • • • •
MAX Humper Homes Termination of the second	Implementation Implementation   Implementation Implementation   Implementation Implementation	•
UAR Historyen and The second and a second and the second	With Name.	

3. Export the SAML XML configuration for import into vCloud.

### Configure your vCloud Organization (Service Provider)

1. On the Virtual Datacenters dashboard screen, click the card of the virtual data center you want to explore.

DISCARD SAVE

- 2. From the main menu select Administration.
- 3. In the right panel under Identity Providers, click SAML.
- 4. In the left pane click Edit.

a.

ervice Provider	Identity Provider	
Entity ID		
	Your survive previoler entity 33. Once you set it is lickly if cannot for sharped least in anyly-	
Certificate Explicition	12/05/2021, 08:38:34 AM	INCOMPANY.

a. b. Service Provider

i. Entity ID: This field does not require any data, and is not utilized with EvolvelP's Identity and Access Management system. If something is entered here, it cannot be changed back to empty.

ii. Certificate Expiration: The Service Provider certificate expires after 1 year. You will need to navigate to this location and click Regenerate to prevent the certificate from expiring. We recommend clicking Regenerate when configuring SAML to reset the expiration timer.

1. If you configured notifications for your Organization you will be notified when the certificate is about to expire.



- . User SAML Identity Provider: Enable the slider button to enable SAML authentication for your Organization. ii. Metadata XML: Copy or upload your metadata XML from your Service Provider
- e. Click Save to complete this step of the process.

## Import Users or Groups for SAML Authentication

- 1. On the Virtual Datacenters dashboard screen, click the card of the virtual data center you want to explore.
- 2. From the main menu select Administration.

C.

- 3. Users: Import individual users for SAML access.
  - a. On the left pane under Access Control and click Users.
    - b. Click Import Users. (This option is only available if SAML is enabled as outlined above.)
      - i. Enter the user names one per line in the Import Users window.
        - 1. User names must be in the format configured in the IDP setup, in this example we specified sAMAccountName in the IDP configuration.
        - ii. Click the drop-down and assign a role for the users.
          - 1. The role will be assigned to all users. If you want to import multiple users with different roles they need to be imported in batches based on their group access.

Ender the user names *	heed
	User remain must be in the same identifier formal supported by the SAMI identify provider scribpand for this reparimities
Annalase Danks 1	Use a new line for each user name.

- c. Click Save to complete the process of importing users for SAML authentication.
- 4. Groups: Specify which groups should be allowed to log in via SAML. Users will be created as they successfully log into the system. a. On the left pane under Access Control click Groups.
  - b. Click Import Groups. (This option is only available if SAML is enabled as outlined above.)
    - i. Enter the group names one per line in the Import Groups window.
      - 1. The group names must match the format configured in the IDP setup.

Import Groups	×
Source	SAML
Enter the group names 1	sclassfinadesd
Assign Role -	Cross names must be in the name dentifier formal supported by the 2444, storing proved in the ingeneration the organization. We as new inter to call or goal areas. Corganization Administrator *
Auguran -	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.