VERCARA
a digicert® company

UltraDNS Managed Services Portal – SAML Quick Start Guide

Customer Guide

Version 1.3 (May 2025)

Find more information at:

vercara.com

Call USA: +1 (844) 929 - 0808
Call EMEA: +44 808 175 1189

Table of Contents

Overview

Security Assertion Markup Language (SAML) provides the solution for providing both authentication and authorization services for UltraDNS customers. By sharing security credentials between customers and our Security teams, we can transition your user's internal login credentials to an UltraDNS Managed Services Portal (UI Portal) username, thereby creating a Single Sign On (SSO) relationship between our services and systems.

Account Owners and Admins please note the disclaimer prior to submitting your SAML request.

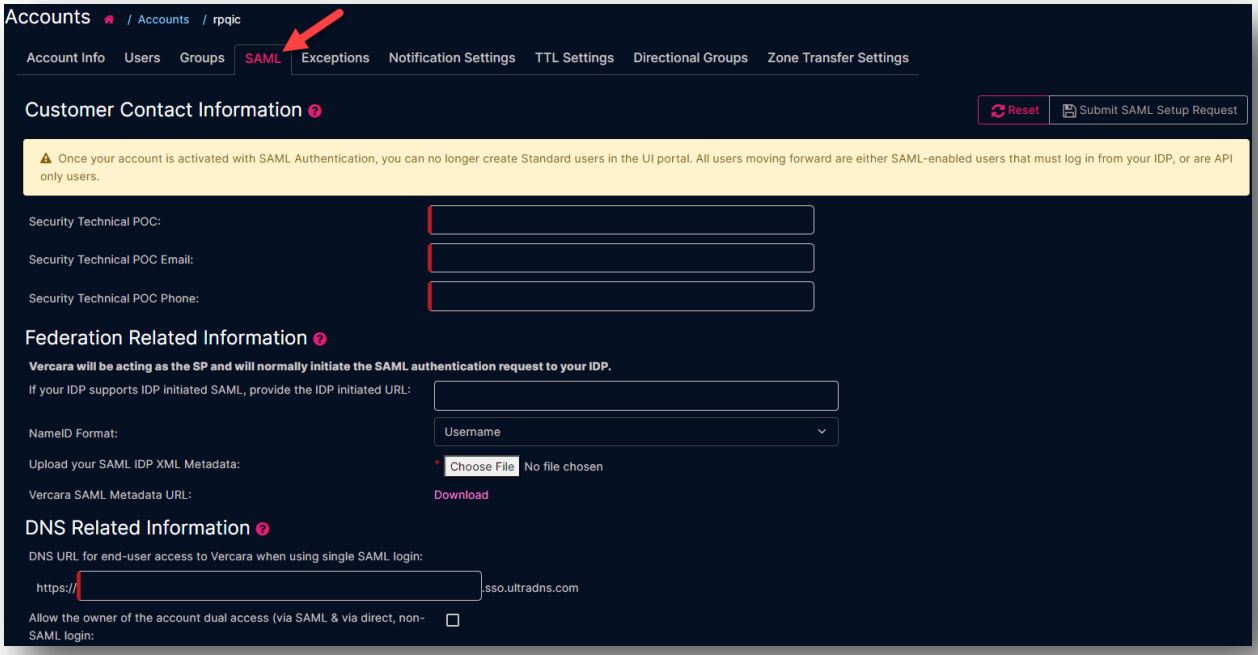
Once SAML is enabled on your UltraDNS account, (creating) New Users will only be able to be created as API Only users. If new users will need to access the UltraDNS Portal, they will need to be created from your IDP.

How to Enable SAML from the UI Portal

The following steps are for the Account Administrator to complete when logged in to the UI Portal.

> SAML and **Multi-Factor Authentication** (MFA) cannot be enabled together. MFA must be disabled at the Account Level and User Level before SAML can be configured and utilized by users.

1. Click on **Accounts** from the left-hand navigation pane.
2. Select the Account Name that you want to enable SAML for.
3. Click the **SAML** link from the header.
4. Complete the required fields (indicated by a red bar in the field).
    - Download the sample XML metadata file so that you can copy the format correctly.
5. Click **Submit SAML Setup Request** when finished.



Required SAML Details

Below are the sections you need to complete before submitting your SAML request, with additional details about the required fields.

Customer Contact Information

- **Security Technical Point of Contact** (POC) – Provide the first and last name for the primary point of contact.
- **Security Technical POC Email** – Provide a valid email address for the primary point of contact using the addr-spec format. (i.e., John@email.com)
- **Security Technical POC Phone** – Provide a valid phone number (without dashes) beginning with the country code for the primary point of contact.

Federation Related Information

- **IDP Initiated URL** - If your Identity Provider (IDP) supports initiated SAML, provide the IDP initiated URL.
- **NameID Format** – Select either **Username** or **Email** from the drop-down menu depending on how your internal login IDs are currently formatted (as an email address or not).
- **Upload your SAML IDP XML Metadata** – Click on the **Choose File** button and upload your XML Metadata file.
    - Click the **Download** option to get the UltraDNS XML Metadata to match the configuration requirements before submitting your own XML Metadata file.

DNS Related Information

- **DNS URL for end-user Access** – Provide your company's uniquely identifiable company name. This will also be used as a domain tag for the UDNS usernames, if the NameID Format type selection is Username.
- **Allow the owner of the account dual access** – If you (as the Admin) need to retain access to the UI Portal, as well as getting access via SAML (SSO), check the box for dual access.
    - **I**f you opt not to check the box, you will no longer be able to log in directly to the UltraDNS Managed Services Portal.

Submitting Your SAML Request

Verify that all the information you have provided in the previous sections is accurate before clicking the **Submit SAML Setup Request** button.

Once submitted, changes cannot be made to your SAML request content without reaching out to our Customer Support department.

Upon the successful completion of your SAML request, a confirmation email will be sent to the Customer Security Technical POC Email that you provided. This email will contain the URL (vanity URL) you will use to access the UI portal moving forward.

Please wait a few minutes before trying to log in using the vanity URL that has been emailed to you. While you wait for the email confirmation, please continue through this guide for the final steps of setup.

After your submission has been processed, the **UltraDNS Users Details** section will appear with the list of your users currently found on the UltraDNS UI Portal. Your users' details will be displayed in one of two different formats, which is determined by the **NameID Format** type that you selected.

IDP Provisioning

As previously stated, once the request for SAML has been submitted, our Customer Support team will send an email to the Primary Point of Contact that was listed. This email contains the following information to assist with the provisioning of the UltraDNS setup from within your IDP.

When setting up your system, please ensure that the NameID and SAML attributes match the assertion as specified below.

If the NameID is a Username

Your SAML XML metadata must contain the NameID Format as unspecified:
urn:oasis:names:tc:SAML:1.1:**nameid-format**:unspecified

If the NameID is an Email

Your SAML XML metadata must contain the NameID Format as emailAddress:
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

The Mandatory attribute statements required by UltraDNS in the SAML assertion are:

Given Name	<saml:Attribute Name="givenname"NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
Surname	<saml:Attribute Name="sn"NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
Mail - The Email address (not postal)	<saml:Attribute Name="mail" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">

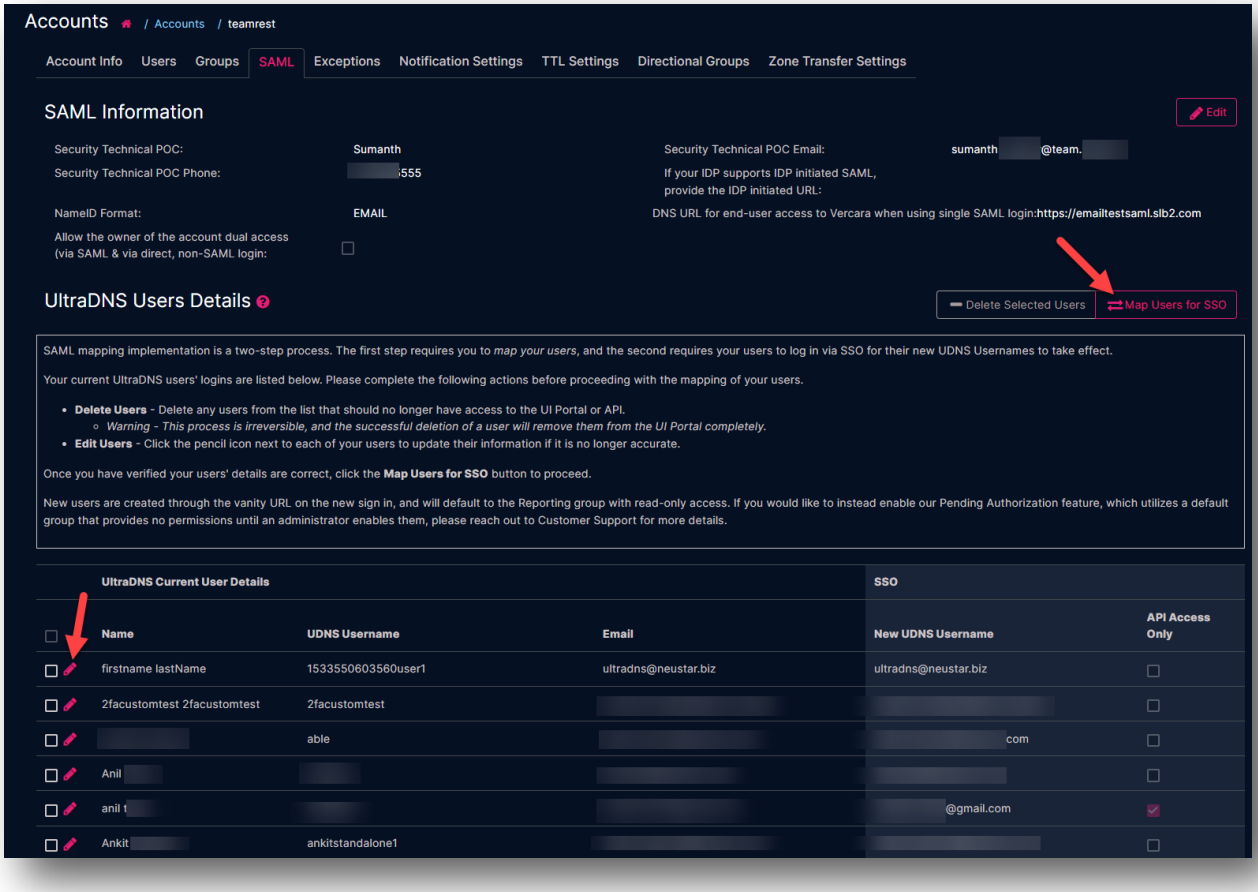
The above listed formats are MANDATORY.

Upon full implementation of SAML / SSO with UltraDNS, your existing UltraDNS login ids will be renamed to the persistent NameID value that was passed, and direct login access via the UltraDNS portal http://portal.ultradns.com/ will be blocked. Any logins used to access REST API will continue to be supported as is."

UltraDNS Users Details

The UltraDNS Users Details section displays the SAML features for your users based upon existing UI Portal details, and the NameID Format field type that you selected during the initial SAML setup request.

The significant difference is the addition of the **SSO Login** column for NameID Format **Username** (Non-Email) selection.



The following table denotes each column from the UltraDNS User Details section, along with an additional explanation of each field, and what content (if any) needs to be updated or provided.

Table 1 UltraDNS User's Details by NameID Format

Column Header	Details	Additional Actions Required?
Name	The first and last name of the user taken from the My Profile section of user's UI Portal account.	**None**
Current UDNS Login	The current username used by the user to access the UI Portal.	**None**
Email	The current email address taken from the My Profile section of the user's UI Portal account. Click the pencil icon to update the email address if it is invalid.	**Yes. Update if invalid.** **Will become part of the SSO Login if NameID Format Email was selected.**
SSO Login	**Only present when NameID Format is Username (non-email).** Click the pencil icon to update the SSO Login for the user, so that it is aligned with your current SSO username format.	**Yes. Update if invalid. Only available when NameID Format is Username.**
Upon Implementation UDNS Username	Displays what the new username will be after successfully logging in via SSO. **When NameID Format is Email**: ▪ Username is a combination of the Email address and the DNS URL provided during SAML setup. **When NameID Format is Username (non-email)**: Username is a combination of the SSO Login field, and the DNS URL provided during the SAML setup.	**None**
API Access Only	If selected, the associated user will ONLY have access to the REST API. The user will retain all their current API permissions. However, the selected user will no longer be able to access the UI Portal directly, or via SSO login.	**Yes. Selected when editing user details.**

If you forget to check the box for **API Access Only**, and you have already selected the **Map Users for SSO** button, your selected user will lose the ability to log in to the API if they use the vanity URL. However, if the user never logs in using the vanity URL, they can continue to access the REST API and retain their access and permissions.

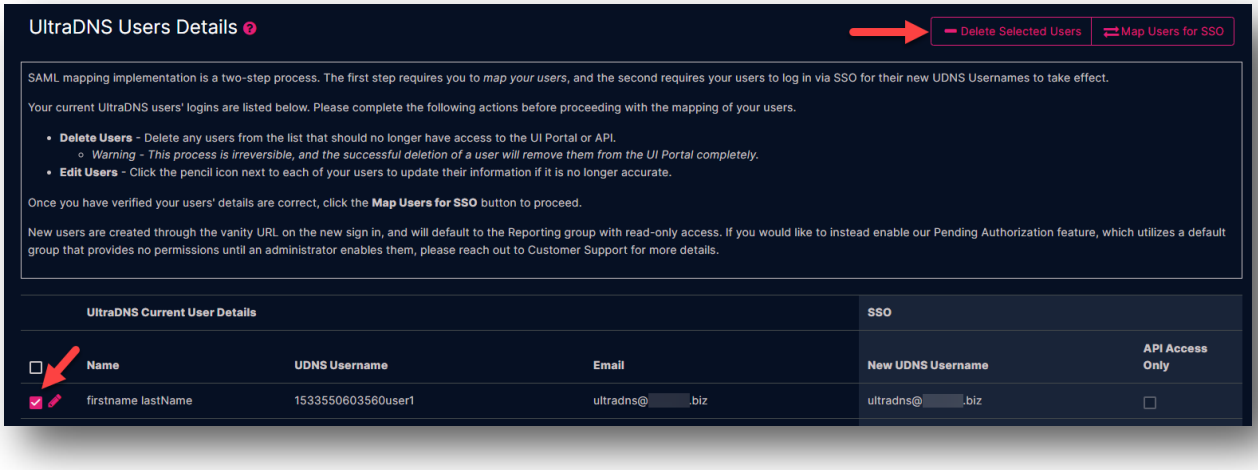
Delete Users

The **Delete Selected Users** option provides the ability to clean up your list of UltraDNS Users.

For those users that should not have access to the UI Portal (or API), or are no longer affiliated with your company, it is the Account Owner's responsibility to delete these users.

Click the checkbox next to each of the users that should be deleted and click the **Delete Selected Users** button. A confirmation window will appear displaying the selected user(s) for deletion. Click the **Delete** button to confirm the user's deletion from the system.

> **WARNING** – *Deleting a user is irreversible. Please be sure you confirm that the user does in fact need to be deleted before completing the action.*

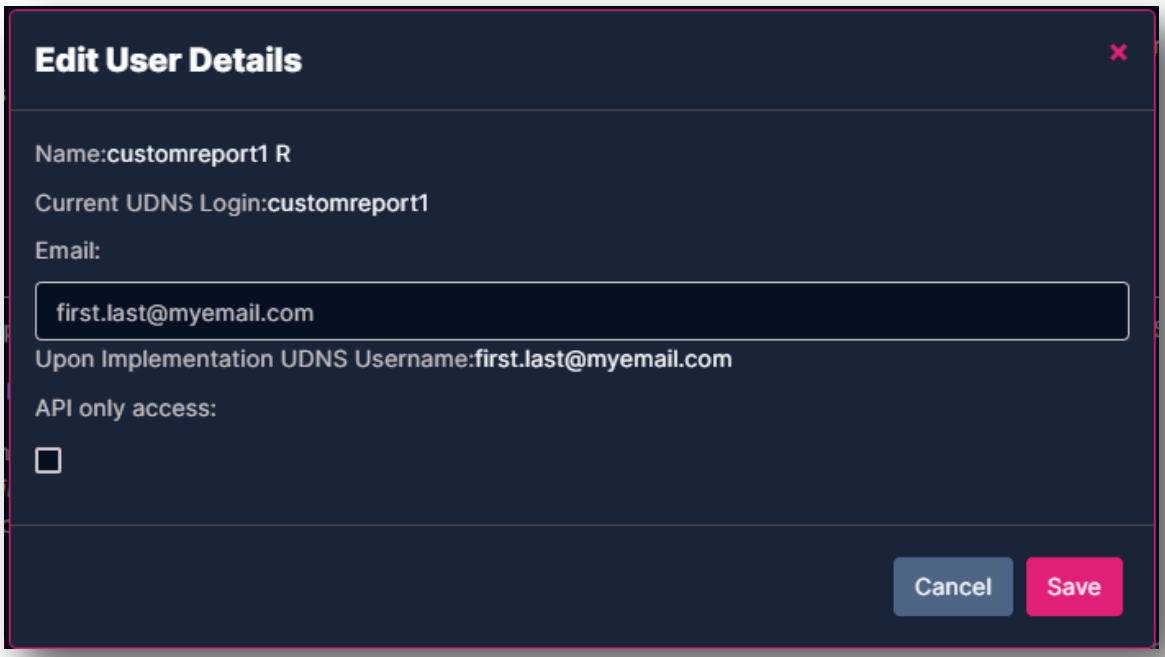


Edit Users

We highly encourage you to review and update your users' details before continuing with the mapping process. Click the **pencil icon** to edit each individual user.

For SAML requests that were submitted with the NameID Format type as **Email**, you can:

- Edit the user's **Email** address.
  - *Only unique email addresses are allowed. If duplicate email addresses are detected, an error will occur and the SAML Mapping process will be cancelled.*
  - The email address will directly update the *Upon Implementation UDNS Username* (the future SSO login credential) field for the user.
- Check the box to determine if the selected user should ONLY have access to the API or not.



For SAML requests that were submitted with the NameID Format type as **Username** (Non_Email), you can:

- Edit the user's **Email** address.
- Edit the **SSO Login** so that it is aligned with your current SSO login credentials.
    - The SSO Login field will directly update the *Upon Implementation UDNS Username* (the future SSO login credential) field for the user.
- Check the box to determine if the selected user should ONLY have access to the API or not.

To further elaborate on why we highly recommend you update the email address for each user, below is an example of why your mapping may not correctly work.

Example: Company ABC has the following listed under their Ultra DNS User Details section:

Name	Current UDNS Login	Email	Upon Implementation UDNS Username
John Dykes	John235	John.d235@gmail.com	John.d235@gmail.com

However, this user's credentials in their customer IDP are John.Dykes, or John.Dykes@abc.com

If John is mapped as is, the mapping will complete with an error when John tries to log in via SSO, because his credentials will not be recognized by his IDP. If his email address is updated however to John.Dykes@abc.com, then the mapping will complete without error, and John will

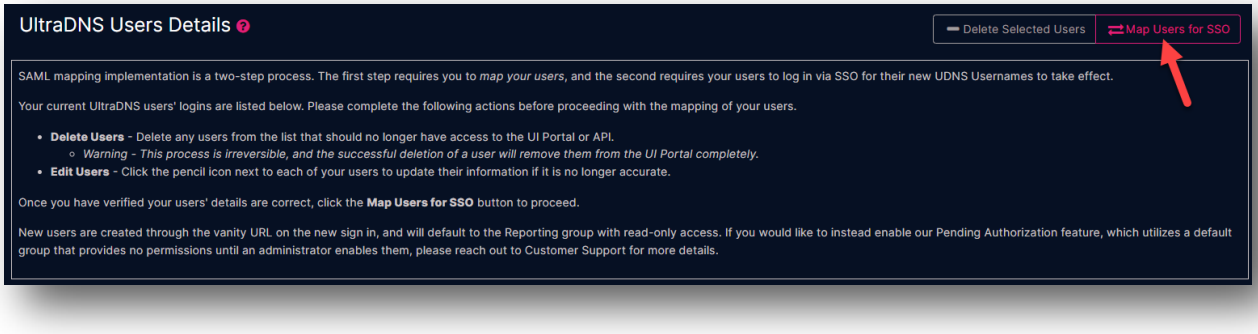
be able to login via SSO without any issue.

Map Users for SSO

Once you have verified that all your users' information is accurate, click the **Map Users for SSO** button. **Every user from the list will be selected automatically**, which is why it is important for the account owner to review the initial list of users and use the **Delete Selected Users** option to remove any obsolete users.

A confirmation screen will appear listing the total number of users that are being mapped for SAML, along with the details their details and login credentials. Click the **Confirm Map Users** button to complete the SAML setup process.

Please only click the **Confirm Map Users** button once, as doing so multiple times could cause issues with your submission.



Once the confirmation of the SAML submission appears, your request will be processed. At this point, you can log in using the SAML credentials and vanity URL that have been emailed to you.

The SAML process will work around a trial period. Once you have become familiar and comfortable using SAML login to access the UI Portal and manage your users, UltraDNS will remove all your user's direct access to the UDNS Portal. Our Customer Support team will reach out to you directly to confirm your readiness to begin using SAML and have your access to the Portal removed.

For further assistance on the SAML submission process, or with using SAML, you can open a support ticket at https://www.ultraproducts.support.

User Access and Permissions

For existing users on the UltraDNS Portal, your permissions will remain once your Account Administrator completes the Setup Users for SSO step (before you attempt to log in using the

vanity URL).

If the **Setup Users for SSO** step has not been completed, and you log in using the vanity URL, your account will inherit the Reporter Role permissions upon logging in. The Reporter Role provides only Read Access. Your Account Administrator will need to log in and change your permissions from the UltraDNS Portal.

Please note that if you have configured Account Level Allowed IP (ranges) for your account, these do not currently apply to SAML users, as the IP authentication check is done by the Identity Provider (IDP), not UltraDNS.

Creating New Users

Once you have completed the SAML setup, new users are dynamically provisioned from your end. Once you have established a new user's credentials, they will automatically be enabled for SAML and have the **Reporter Role** access, which gives them Read Only access. You can change their access, if necessary, through the UI.

The Invite User feature will only be for granting API access to a user.

Pending Authorization

For an additional security measure for your account, contact Customer Support and request to have **Pending Authorization** enabled on your account. With this optional feature enabled, any newly created users will be placed into the default system Pending Authorization security group, where the user does not have any permissions to access the Managed Services Portal until an account administrator moves them to a designated security group.