Mandiant

FEDERATED ACCESS FOR THE MANAGED DEFENSE PORTAL

The Managed Defense Portal can be integrated with other identity providers for authentication. There are two main types of federation: identity provider (IdP) initiated and service provider (SP) initiated. The Managed Defense Portal supports IdP initiated sign in.

An integration with identity federation only provides authentication. User roles still need to be managed within the Managed Defense Portal by Team Admins.

- Customers can have more than one IdP that is federated with the Managed Defense Portal.
- Local accounts are not supported when using a federated IdP.

Configure identity federation

To request federated access to the Managed Defense Portal, follow these steps:

1. Configure your connection based on the following information and generate a metadata file (including a signing certificate and the details for the IdP):

   entityid: auth.mandiant.com
   ACS endpoint:
   https://auth.mandiant.com/sp/ACS.saml2
   attribute contract information:
   SAML_SUBJECT = user's email
   first_name = given name of user
   last_name = family name of user

   For a successful setup of federated access, make sure these SAML attribute names are configured exactly as shown, including spelling and case. If the SAML attributes don't match exactly, signing into the Managed Defense Portal won't work.

2. Provide the metadata file to the Provision Engineering team or contact them if you need additional assistance.
3. Upon confirmation that Mandiant has established your connection, test your IdP initiated federation using the tile or link within your IdP single sign-on dashboard.

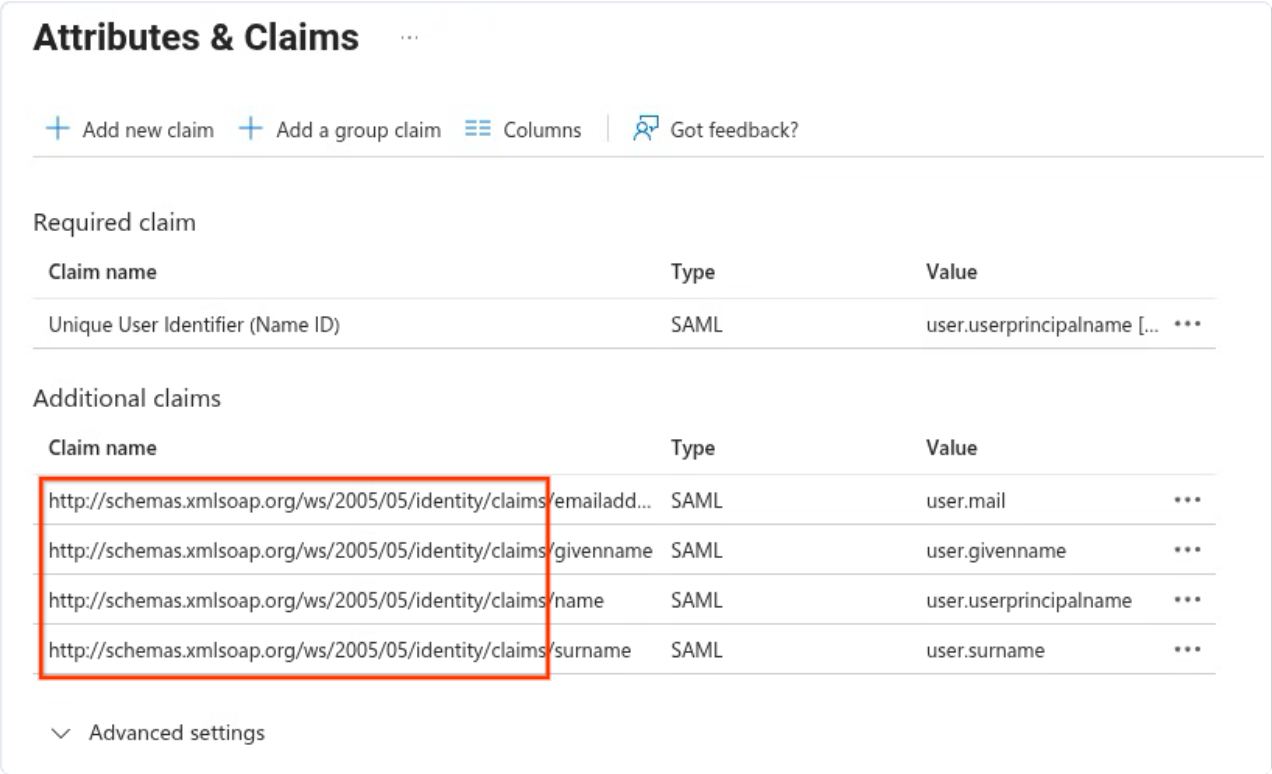
IdP initiated sign in

Once federated access for the Managed Defense Portal has been established, the user must sign into their IdP and select the Managed Defense application to initiate a sign in. That process is as follows:

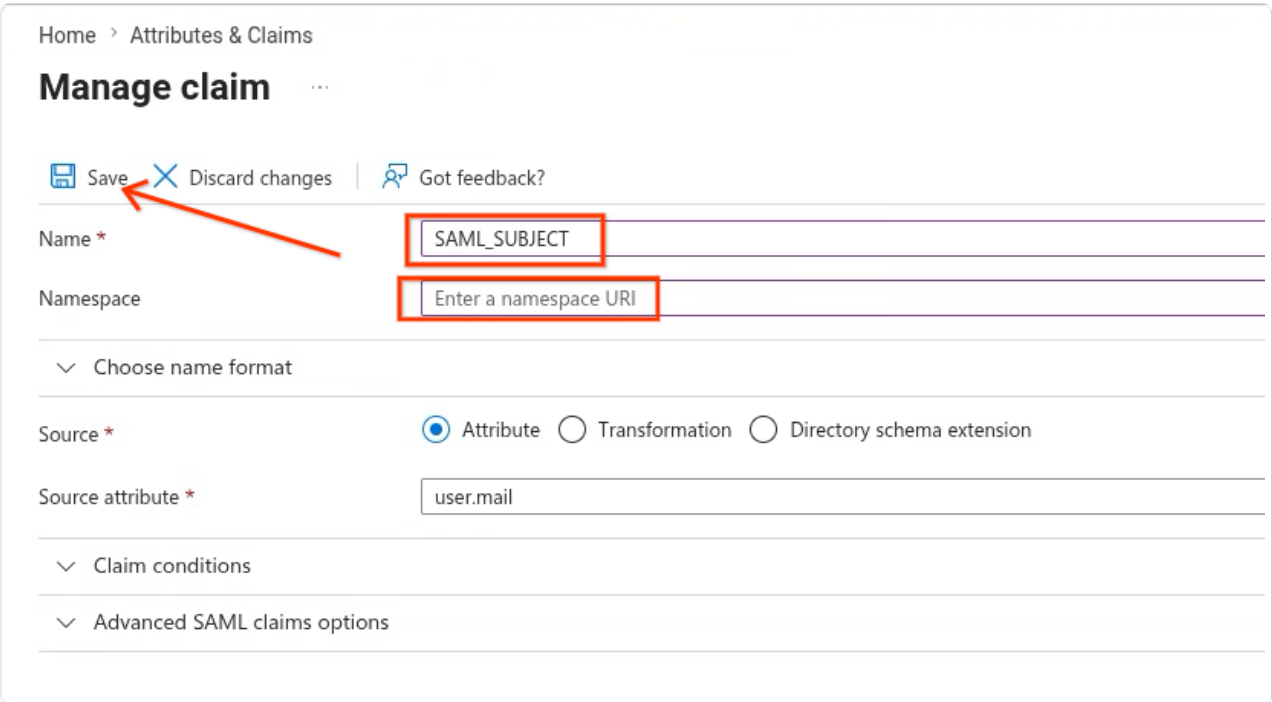
1. The user signs into their IdP, rather than the application they want to access.
2. The user is signed into the application using a **security assertion markup language (SAML) (https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language)** response from the IdP.

Microsoft Entra specifications

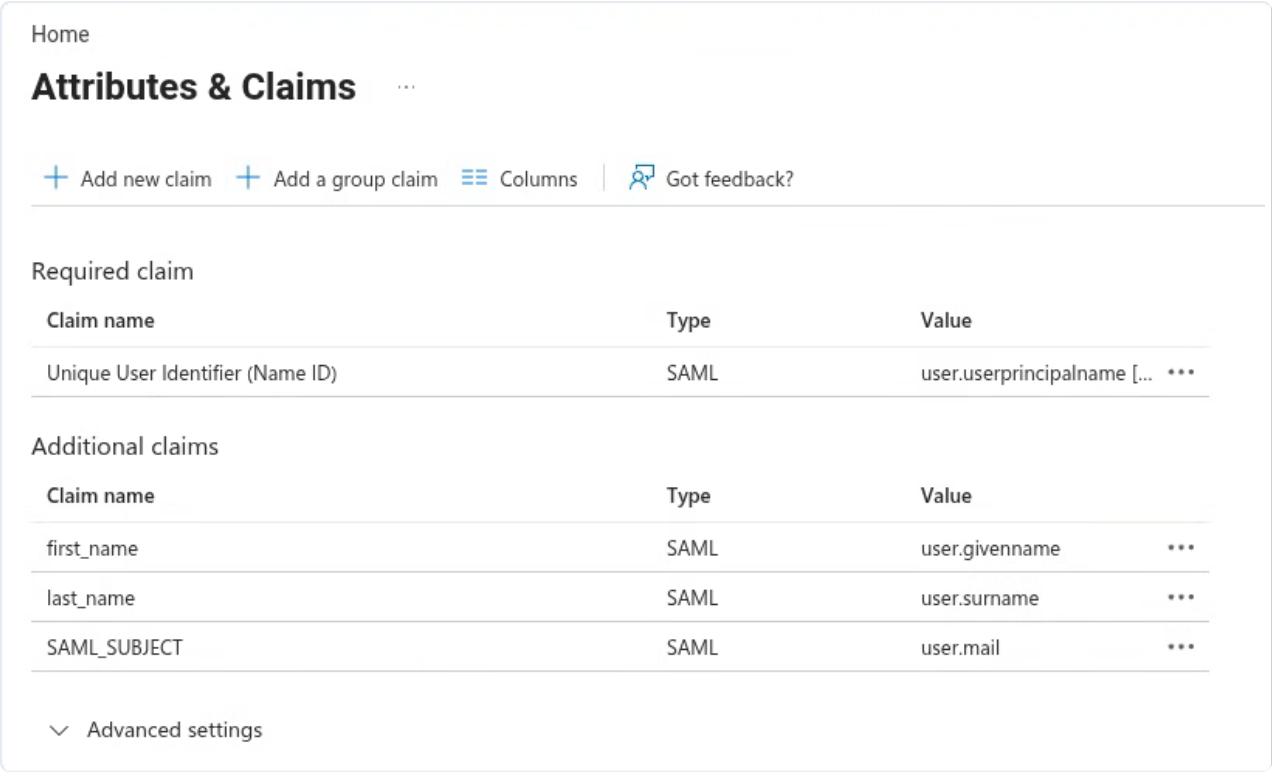
By default, Microsoft Entra sets up the SAML attributes with a Namespace. Because of the way that Mandiant configures the integrations, having the Namespace configured on the claims causes the federation request to fail. When you create a new application, Entra adds the default claims that are shown in the following screenshot. The highlighted part shows the Namespace configured.



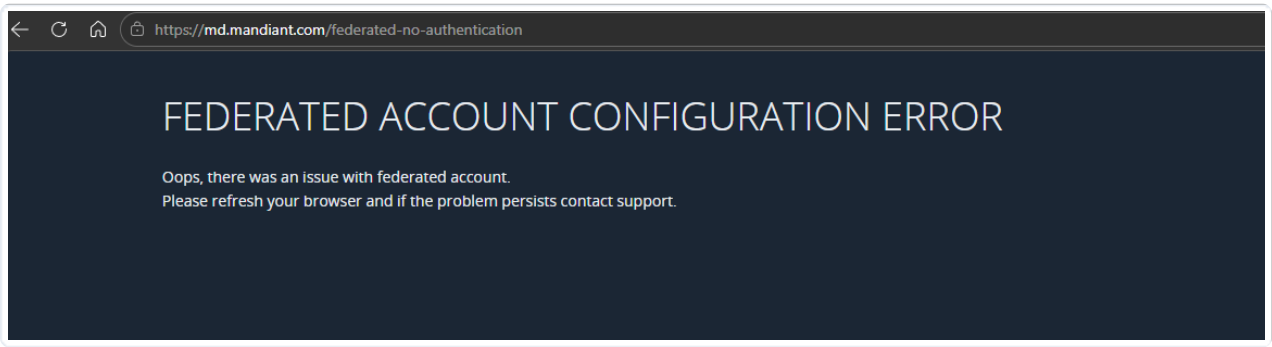
For the three claims that Mandiant requires (mail, givenname and surname), click the row for each claim to edit them. Update the **Name** parameter to the appropriate name from the preceding step, clear the **Namespace** value to ensure it's blank, then save your changes.



Once all three have been edited, your claims should look like the following screenshot. The fourth default claim has also been deleted since it isn't needed by Mandiant, but this is not required.



If you are getting an error message that looks like the following screenshot, then likely these claims have not been configured correctly and that should be the first thing to check.



Deactivate users with federated access

To deactivate and remove a user's access to the Managed Defense Portal when using federated access, two actions are required:

- Remove the user from the federated group in the IdP
- Deactivate the user in the Managed Defense Portal organization

> Removing a user from a group on the IdP only prevents the user from signing in and does not deactivate an account. A user might still receive notifications from the Managed Defense Portal if their account is active.

Remove user from the federated group in the IdP

To remove user access to the Managed Defense Portal, an administrator for your IdP (for example, Azure AD or Okta)

must remove the user from the groups that grant access. Because authentication is federated, the IdP controls application access.

Deactivate the user in the Managed Defense Portal

After the user is removed from the federated group in the IdP, a user with the Team Admin role within the Managed Defense Portal must perform the following steps to deactivate the user account.

1. Sign in to the Managed Defense Portal.
2. Navigate to **Settings > MD Users**.
3. Find and select the user account that needs to be deactivated.
4. From the **Edit** menu for that user, select **Deactivate User**.

Deactivating the user directly in the Managed Defense Portal ensures their account is immediately inactive within the Mandiant system. This can help terminate existing sessions (depending on session management) and remove the user from active user lists, reports, and access within the Managed Defense Portal interface.

When to contact support

Open a **Support (https://docs.mandiant.com/home/customer-support)** ticket if:

- You are unable to find any user with Team Admin privileges to perform the deactivation in the Managed Defense Portal.
- The user deactivation option does not work as expected.
- A user needs to be removed from the system, not just deactivated.