AVANAN

A Check Point Company

03 March 2026

AVANAN

Administration Guide

CHECK POINT™

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback

Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments.

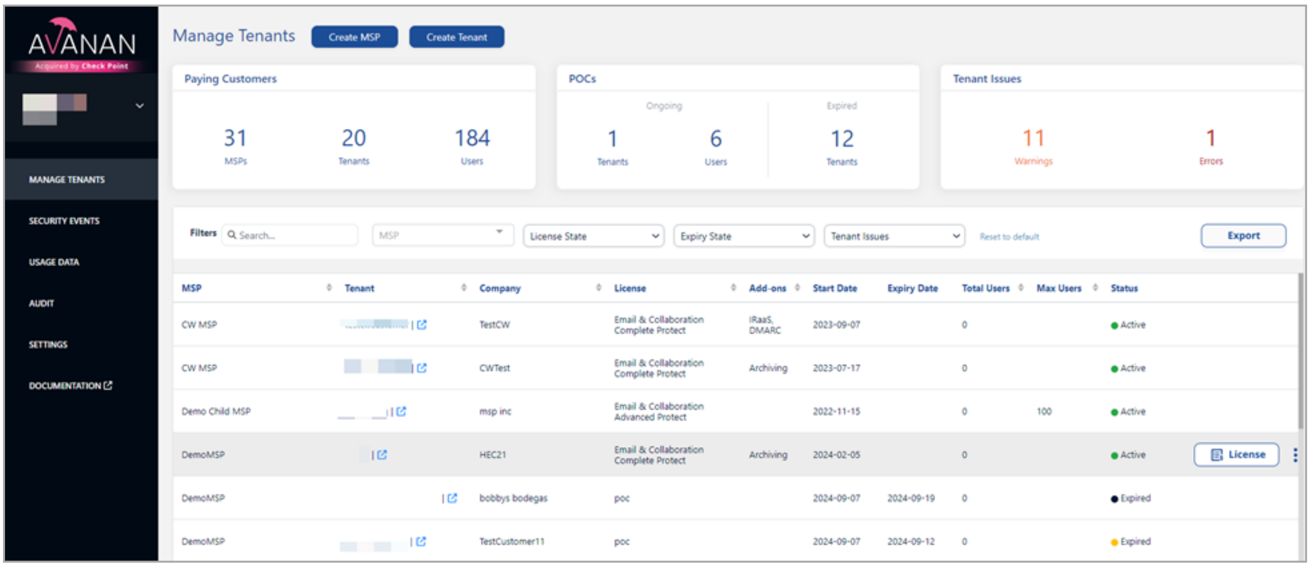
Related Documents

Document Title	Description
Avanan Administration Guide	Avanan offers an administration guide for the administrators. For more details, see Avanan Administration Guide.
Avanan User Guide	Avanan offers an user guide for the end users. For more details, see Avanan User Guide.
Avanan API Reference Guide	Avanan offers a rich set of REST API to manage and act on detected security events. For more details, see Avanan API Reference Guide.
Avanan MSP API Reference Guide	Avanan offers a API for MSSP to mange there child MSSP and customer accounts. For more details, see Avanan MSP API Reference Guide.

Table of Contents

Introduction

The Avanan Managed Service Provider (MSP) Management Portal gives MSP customers access to the data needed to manage their direct clients. The multi-tenancy view provides global visibility that allows to run the business efficiently.



Paying Customers: 31 MSPs, 20 Tenants, 184 Users

POCs: Ongoing 1 Tenants, 6 Users; Expired 12 Tenants

Tenant Issues: 11 Warnings, 1 Errors

MSP	Tenant	Company	License	Add-ons	Start Date	Expiry Date	Total Users	Max Users	Status
CW MSP	[redacted]	TestCW	Email & Collaboration Complete Protect	IRaaS, DMARC	2023-09-07		0		● Active
CW MSP	[redacted]	CWTest	Email & Collaboration Complete Protect	Archiving	2023-07-17		0		● Active
Demo Child MSP	[redacted]	msp inc	Email & Collaboration Advanced Protect		2022-11-15		0	100	● Active
DemoMSP	[redacted]	HEC21	Email & Collaboration Complete Protect	Archiving	2024-02-05		0		● Active
DemoMSP		bobbys bodegas	poc		2024-09-07	2024-09-19	0		● Expired
DemoMSP	[redacted]	TestCustomer11	poc		2024-09-07	2024-09-12	0		● Expired

Managed Service Provider (MSP) Portal Capabilities

The Avanan MSP Administrator Portal offers these capabilities:

Capability	Description
Manage Tenants	MSP can generate and manage an Avanan tenant for each client. The tenant is a regular Avanan portal that supports all the Avanan features and capabilities. For information about managing tenants and MSPs, see *"Managing Tenants and MSPs" on page 16*. For information about managing licenses, see *"License Management" on page 9*.
Unified Security Events View	Unified view allows MSP Security Administrators to view the security events status from all the managed tenants in a single, unified view, and drill down to the tenant events to investigation, remediation or configuration process. For information about managing security events, see Avanan Administration Guide.

Capability	Description
View Usage Data	View and export the usage information from each tenant. For information about usage data, see *"Viewing Customer Usage Data" on page 10*. **Note** - This feature is not available for child MSPs under large MSPs.

Smart APIs for MSPs

Base (Tenant)

- *Avanan API Reference Guide*
- Related files
  - SmartAPI Swagger File V1.40 (YAML)
  - SmartAPI Client (PY)

Managed Service Providers (MSP)

- Avanan MSP SmartAPI Reference Guide (HTML)
- Related files
  - Parent MSP
    - Parent MSP API (JSON)
    - Parent MSP swagger (JSON)
    - SmartAPI Client (PY)
  - Child MSPs
    - Child MSP API (JSON)
    - SmartAPI Client (PY)

Avanan Smart API Documentation Master Sets

- SmartAPI Documentation 1.40 Master (ZIP)
- SmartAPI Documentation 1.30 Master (ZIP)

License Management

Pay-as-you-Go Billing

In the **Pay-as-you-Go** license model, MSPs are billed monthly based on the number of users for each of their customers protected applications that month and the license package assigned to that customer. To assign licenses, see [Managing Tenant License](#).

Calculating the Monthly Bill of an MSP

The amount an MSP is billed for at the end of a month is calculated using this logic:

$$\sum_{Customer\ 1}^{Customer\ n} \sum_{Day\ 1}^{\substack{Last\ day\ of \\ the\ month}} (\boldsymbol{Daily\ User\ Count * Daily\ Package\ Price})$$

i.e, for every customer under the MSP, for every day of the month, multiply the Daily User Count by the Daily Package Price and sum up all the results.

Daily User Count

The **Daily User Count** is the number of unique email addresses of all licensed (active) users across all of the customer's protected applications on a given day.

Example: Customer A protects Office 365 Mail and Microsoft One Drive SaaS applications.

On Day 1:

- For Office 365 Mail, User1 (`user1@customerA.com`) and User2 (`user2@customerA.com`) are licensed.
- For Microsoft OneDrive, User1 (`user1@customerA.com`) and User3 (`user3@customerA.com`) are licensed.

So, the **Daily User Count** for Day 1 will be 3.

Users Included in the Daily User Count

- Avanan protects only user accounts with a valid Microsoft / Google license.
- Every user account with Microsoft/Google/other license to any protected SaaS application consumes a license from the quota.

- If both the Google and Microsoft applications are protected, every user associated with a licensed email address is counted so that the same person can consume two licenses.
- Avanan protects Shared mailboxes, Group mailboxes, and other aliases but will not count them for licensing purposes.

  Note - You are not billed for these accounts/mailboxes.

- Avanan sync the users every 24 hours with Microsoft and Google accounts. So, deleting or adding a user might take up to 24 hours to affect the license count.
- At the moment, only users from the Office 365 Mail, Microsoft OneDrive, Google Drive, and Gmail applications are billed.
- If a customer has users licensed for other applications, such as Microsoft Teams, these users get protection without billing.

  Note - In future, this changes , and the MSP bills for it.

To set the limit on the number of licenses for a tenant, see Setting a limit for licenses on a tenant.

Daily Package Price

The **Daily Package Price** of the license package assigned to the customer is calculated as:

$$\text{Daily Package Price} = \frac{monthly\ package\ price\ *\ 12}{365}$$

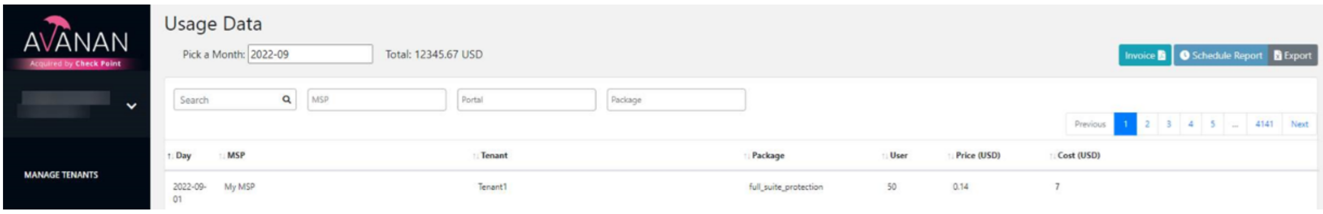
Example: Let us assume that on 01 January 2022, Customer A was licensed for the Advanced Protect package with a monthly package price of $4 per user per month.

So, the **Daily Package Price** for 01 January 2022 will be (4 * 12)/365 = $0.131

Viewing Customer Usage Data

In the Avanan MSP Administrator Portal, under the **Usage Data** tab, you can see the daily usage data in a table for each day of the month for every customer.

MSPs can select the month for which to see the usage data using the **Pick a Month** field at the top-left corner.



Usage Data

Pick a Month: 2022-09 Total: 12345.67 USD

Day	MSP	Tenant	Package	User	Price (USD)	Cost (USD)
2022-09-01	My MSP	Tenant1	full_suite_protection	50	0.14	7

Column Name	Description
Day	Reported date.
MSP[1]	Name of the MSP.
Tenant	Name of the customer.
Package	License package name.
User	Daily User Count.
Price (USD)	Daily Package Price.
Cost (USD)	Result of (Daily User Count * Daily Package Price).

[1] Applicable only for Master Distributor MSPs that manage other MSPs.

Exporting Usage Data

You can export the usage data for a specific month.

To export for an specific month:

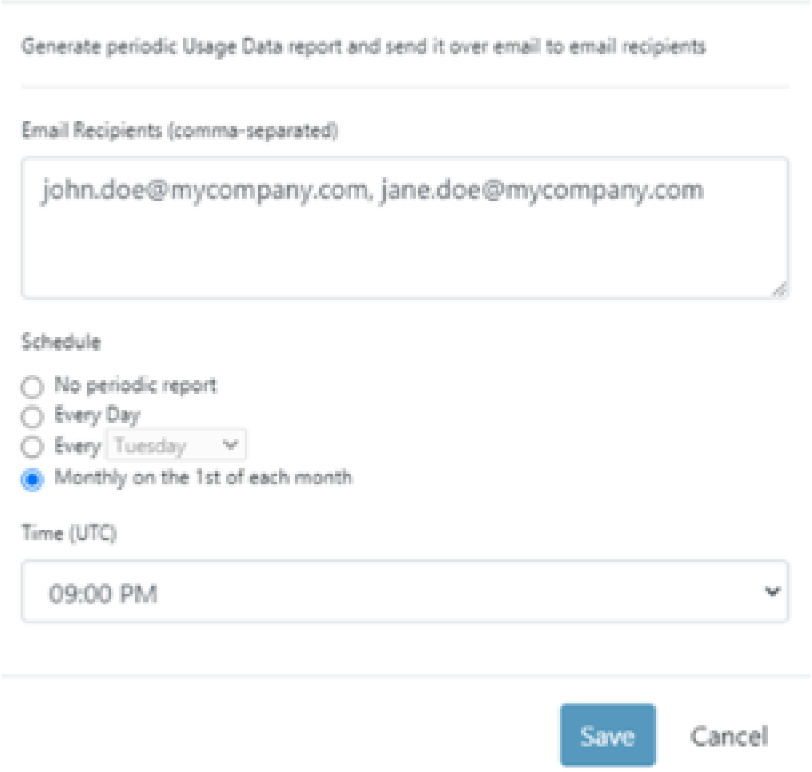
1. Go to the **Usage Data** tab.
2. In the **Pick a Month** field, select the month for which you want to export the data.
3. Click **Export**.

In some cases, a detailed list of users consuming a license for a specific day is required. To get the details, contact *Avanan Support*.

Scheduling Usage Data Report

You can generate periodic Usage Data report and send it over email to email recipient.

1. Go to the **Usage Data** tab.
2. Click **Schedule Report**.



Generate periodic Usage Data report and send it over email to email recipients

Email Recipients (comma-separated)

john.doe@mycompany.com, jane.doe@mycompany.com

Schedule

○ No periodic report
○ Every Day
○ Every Tuesday
● Monthly on the 1st of each month

Time (UTC)

09:00 PM

3. In the **Email Recipients (comma-separated)** field, enter the email address(es) to which you want to send the email.
4. In the **Schedule** list, select the frequency of the email:
   - **No periodic report**
   - **Every Day**
   - **Every** and from the list, select the day
   - **Monthly on the 1st of every month**
5. From the Time (UTC) list, select the time at which the report has to be sent.
6. Click **Save**.

For example, if the report is scheduled to be sent on a weekly basis every Tuesday, the report will include the usage data for the 7 days ending on every Tuesday.

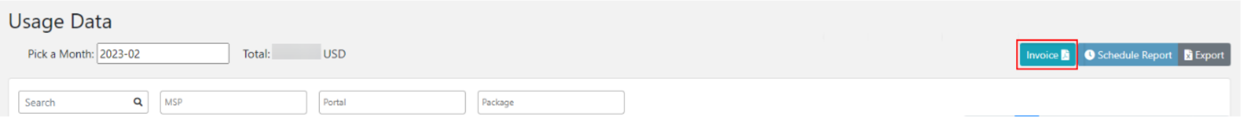
Viewing Monthly Invoices

Every month, you will be emailed the monthly invoice.

To view the monthly invoice through the MSP Portal:

1. Go to the **Usage Data** tab.
2. In the **Pick a Month** field, select the required month.

3. From the top right corner, click **Invoice** to download the Invoice PDF.



Usage Data

Pick a Month: 2023-02 Total: [redacted] USD

Note - Invoices are available only for completed months.

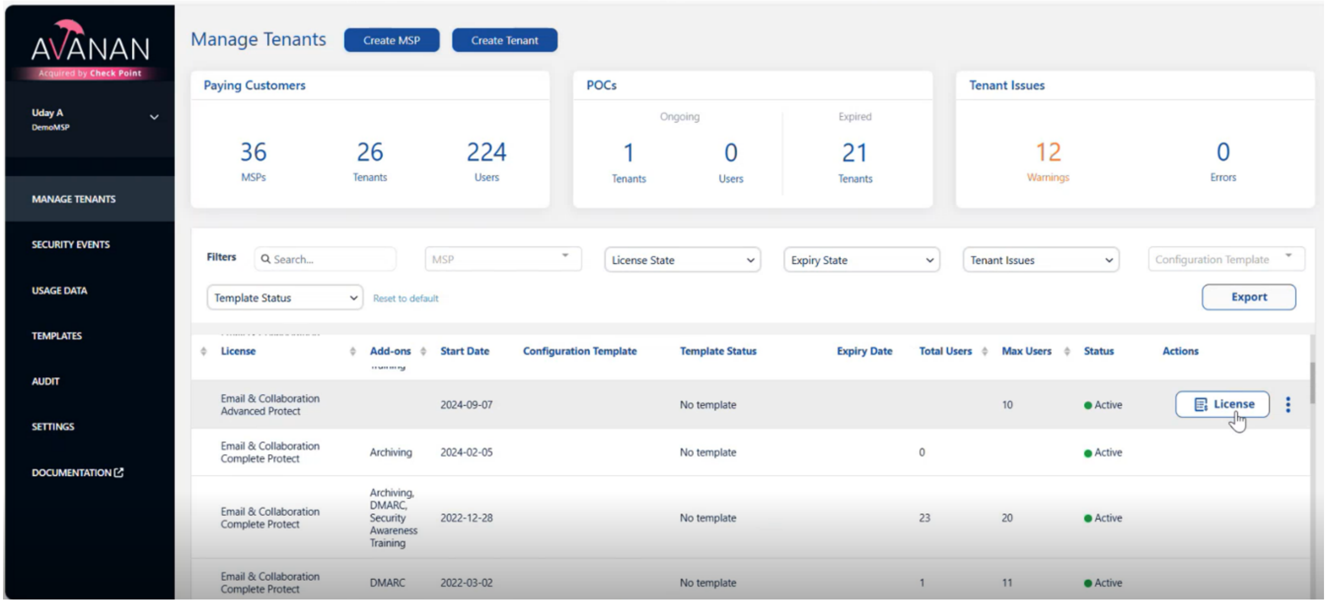
For example, on 20 February 2022, the Invoice for February month will not be available, while the invoice for January 2022 will be available.

Restricting License Usage

Avanan MSP Administrator Portal allows an MSP to set a limit on the number of protected users for each tenant.

Setting a limit to the number of licensed users in a tenant allows the MSP to enforce the license policy on each tenant. A tenant with a limited number of licensed users presents a screen that allows the portal administrator to select the protected users. Only the selected list of users are protected by Avanan. The users that are not selected in the list are not protected by Avanan - both inbound and outbound emails are not scanned by Avanan.

Note - After limiting the license usage for a specific customer, new employees are not protected without manually assigning a license to them.



Manage Tenants

Paying Customers: 36 MSPs, 26 Tenants, 224 Users

POCs: Ongoing 1 Tenants, 0 Users; Expired 21 Tenants

Tenant Issues: 12 Warnings, 0 Errors

License	Add-ons	Start Date	Configuration Template	Template Status	Expiry Date	Total Users	Max Users	Status	Actions
Email & Collaboration Advanced Protect		2024-09-07		No template			10	● Active	License
Email & Collaboration Complete Protect	Archiving	2024-02-05		No template		0		● Active	
Email & Collaboration Complete Protect	Archiving, DMARC, Security Awareness Training	2022-12-28		No template		23	20	● Active	
Email & Collaboration Complete Protect	DMARC	2022-03-02		No template		1	11	● Active	

To activate Licensed Users Management on your Avanan MSP Administrator Portal, contact *Avanan Support*.

Benefits

Offer additional pricing models, such as price tiers and Pay as you Go.

Use Cases

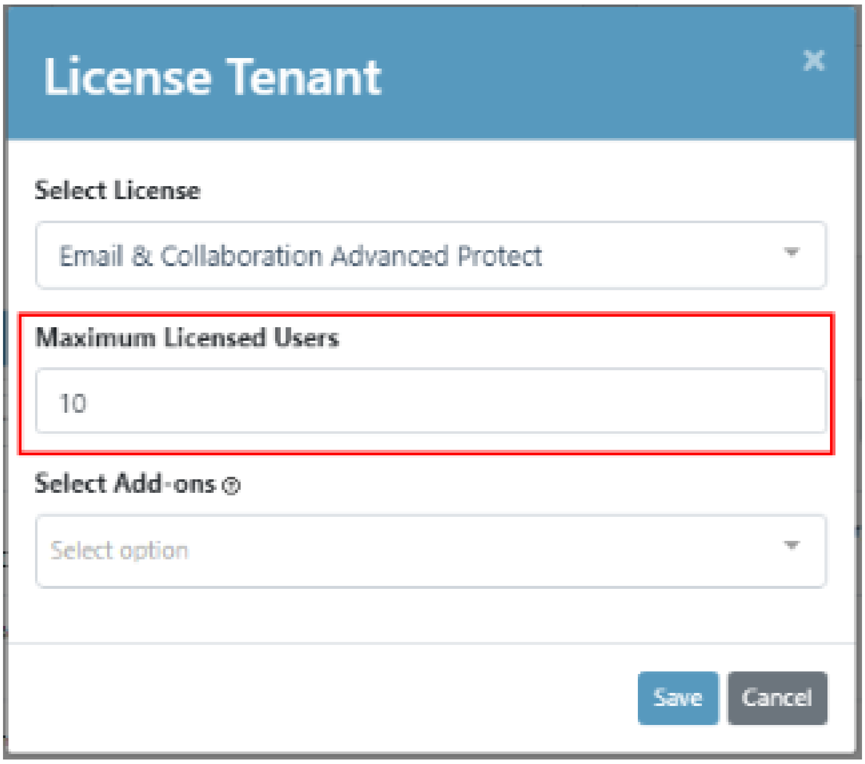
- Enforcing a pricing model that bills for a fixed number of users (compared to Pay as you Go model).
- Allow customers to protect only a subset of their users.
- Avoid protection on service inboxes (For example, printers).

Setting a Limit on the Maximum Number of Users for a Tenant

To set a limit on the maximum number of users for a specific tenant:

1. Go to **Manage Tenants**.
2. In the table, click **License** in the **Actions** column for the tenant you want to set a limit.

   The **License Tenant** pop-up appears.



License Tenant

Select License: Email & Collaboration Advanced Protect

Maximum Licensed Users: 10

Select Add-ons: Select option

3. In the **Maximum Licenses Users** field, enter the maximum number of users that need to be protected.
4. Click **Save**.

Selecting the Protected Users

You can select the list of protected users only for the tenants that have Maximum Licensed Users limit configured. See Setting a limit on a tenant.

1. Go to the Avanan Administrator Portal that has the Maximum Licensed Users limit configured.
2. From the left navigation pane, go to **Configuration** > **Licenses**.
3. Select the list of users to Assign (protect).
4. Select the list of users to Un-assign (unprotect).
5. Click **Save**.

Groups Filter

Groups Filter is an alternate method for limiting coverage to specific users or groups. You can configure these settings from Mail settings. Once configured, any changes to the group will be automatically synced for licensing and coverage purposes. All the policies can use the **All Users and Groups** setting as the only users that will be identified are those in the defined group.

Supported groups:

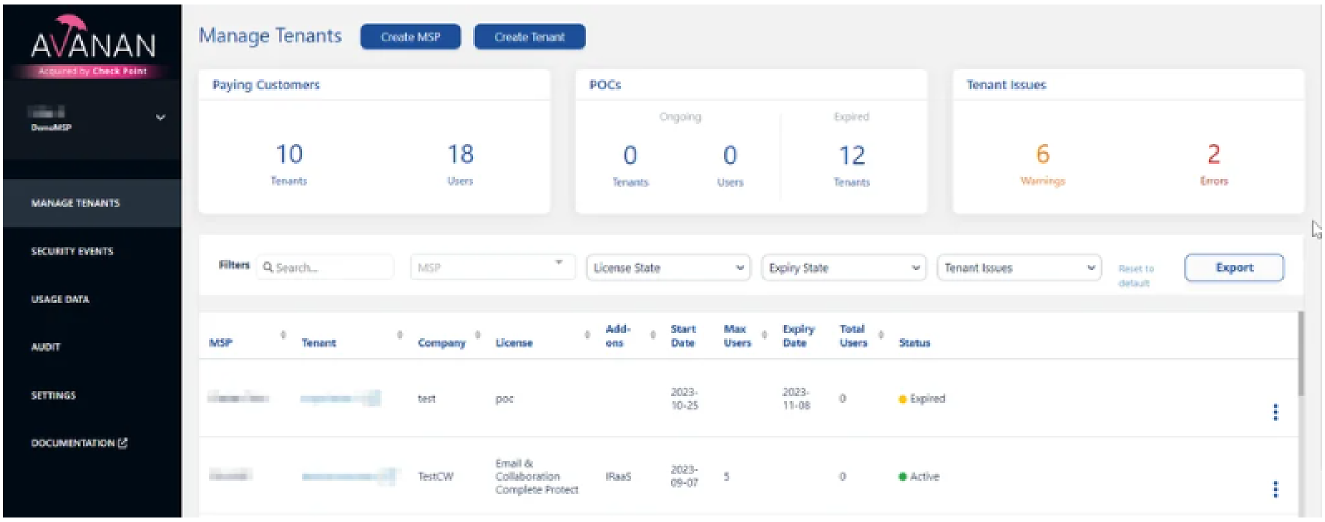
- Office 365: Office 365 Mail Group, Distribution List, or Mail Enabled Security Group.
- Gmail: Gmail Group Distribution List or Mail Enabled Security Group.

To configure groups filter, see Limiting License Consumption to a Specific Group.

Managing Tenants and MSPs

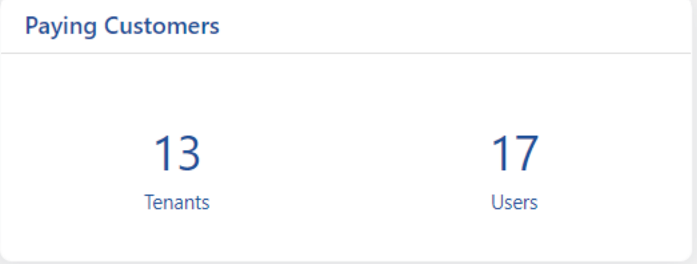
The MSP Portal allows Managed Service Providers (MSP) to manage customer portals (tenants).

In the **Manage Tenants** page, you can create new tenants and set their license package, and perform license add-ons. For Top-level MSP,you can add child-MSP tenants (sub-tenant) that allows smaller service providers to manage their customers.



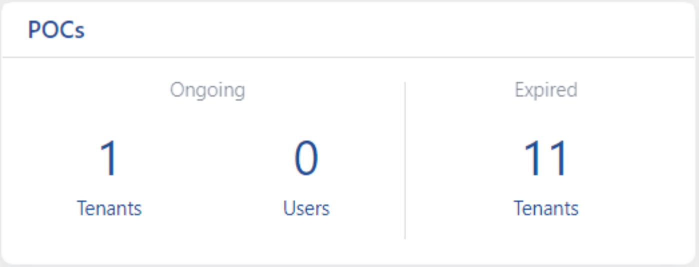
MSP	Tenant	Company	License	Add-ons	Start Date	Max Users	Expiry Date	Total Users	Status
[redacted]	[redacted]	test	poc		2023-10-25		2023-11-08	0	● Expired
[redacted]	[redacted]	TestCW	Email & Collaboration Complete Protect	IRaaS	2023-09-07	5		0	● Active

Paying Customers



The **Paying Customers** widget shows the number of tenants and users that have a valid license.

POCs

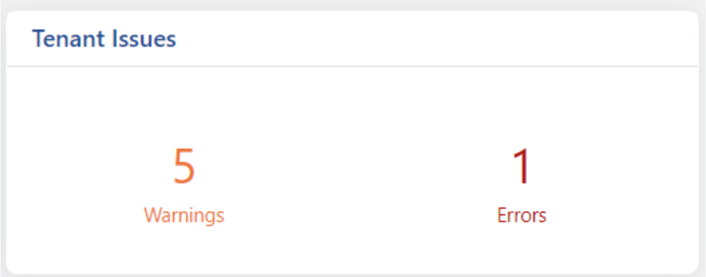


The **POCs** widget shows the number of ongoing (along with the number of users) and expired POCs.

Avanan supports POCs with a full license that allows testing all the features except IRaaS and Archiving add-ons. This license lasts for 14 days, beginning at the time of the tenant's creation. If you need to extend the trial period, contact your Sales representative.

Note - Deleting a tenant permanently removes it, prevents recovery, and prohibits reusing its name.

Tenant Issues

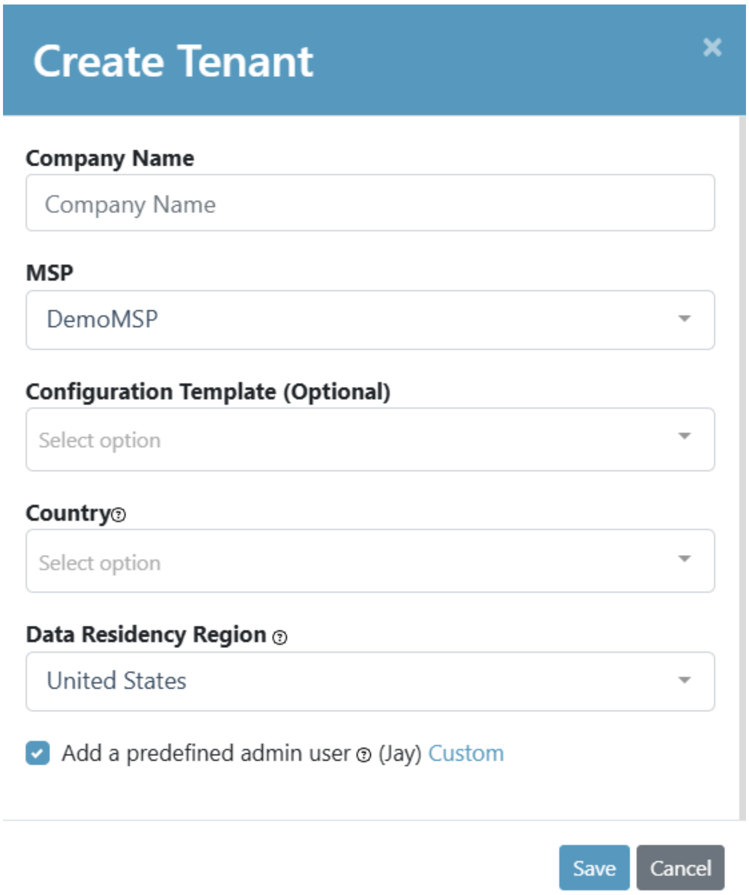


The **Tenant Issues** widget shows the number of warnings and errors related to the tenant.

Creating a New Tenant

1. Go to **Manage Tenants**.
2. Click **Create Tenant** at the top of the page.

   The **Create Tenant** Pop-up appears.



Create Tenant

Company Name: Company Name

MSP: DemoMSP

Configuration Template (Optional): Select option

Country: Select option

Data Residency Region: United States

☑ Add a predefined admin user (Jay) Custom

3. In the **Company Name** field, enter the name of the tenant.

4. In the **MSP** field, select the required MSP under which you create the tenant.

5. (Optional) In the **Configuration Templat**e field, select the required configuration template.

   Note - If you already set the configuration template as default, the system automatically selects it. See *"Setting a Template as a Default Template " on page 32*.

6. In the **Country** list, select the country.

7. In the **Data Residency Region** list, select the data region.

8. To add an admin user, select the **Add a predefined admin user** checkbox.

9. (Optional) To customize the predefined admin user, click **Custom** next to the **Add a predefined admin user**.

   a. In the **Name** field, enter the name of the tenant admin.

   b. In the **Email Address** field, enter the email address of the tenant admin.

   c. In the **Phone** field, enter the phone number of the tenant admin.

d. To use this admin as default for all the new tenants you create, select the **Use as default for future tenants** checkbox.

10. Click **Save**.

    A new tenant gets created. By default, the tenant will be set to trial mode (POC) with an expiry date.

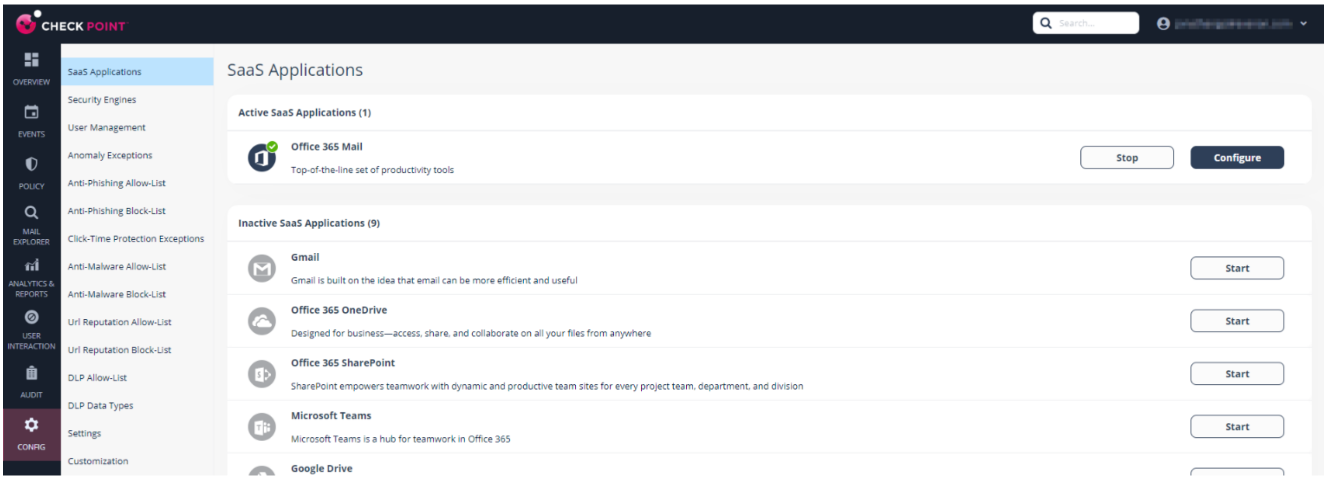
Tenants in the Australian and Indian Region

The tenants (customer portals) added to the Australian and Indian regions look different from those added to other regions.

Note - These regions are relevant only for tenants created using the Avanan MSP Administrator Portal.

By default, the tenants (customer portals) added to the Australian and Indian region have these changes:

1. Check Point logo is presented in the top left corner.
2. Notifications and web pages have the Check Point logo.
3. Notification's default text and name of some configuration items show the company name as Check Point instead of Avanan.



SaaS Applications

Active SaaS Applications (1)

Office 365 Mail
Top-of-the-line set of productivity tools

Inactive SaaS Applications (9)

Gmail
Gmail is built on the idea that email can be more efficient and useful

Office 365 OneDrive
Designed for business—access, share, and collaborate on all your files from anywhere

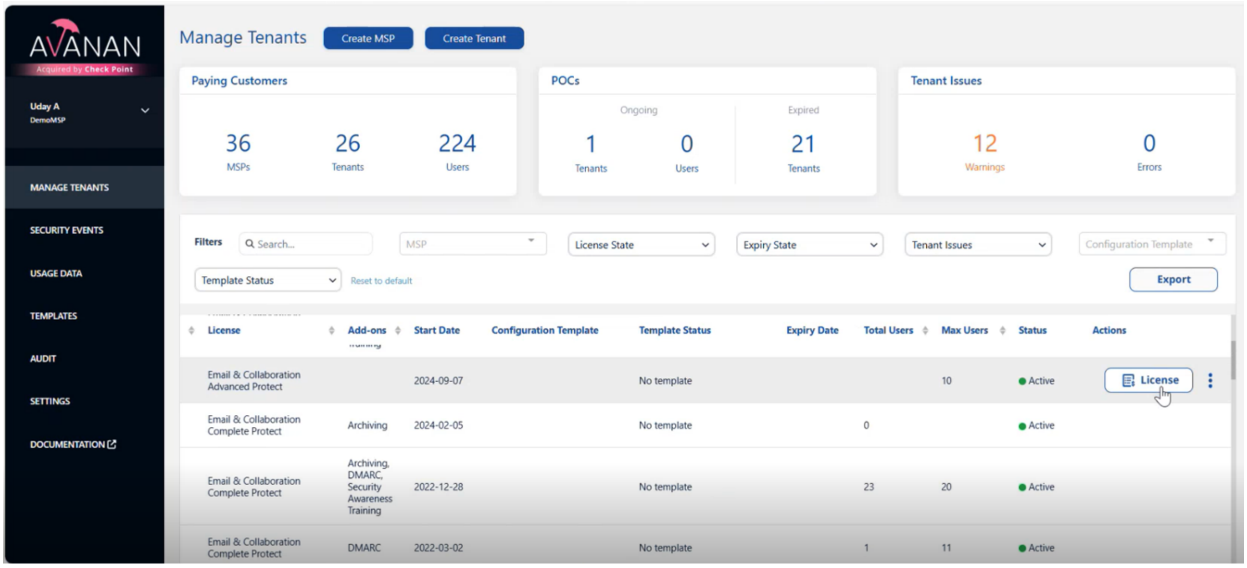
Office 365 SharePoint
SharePoint empowers teamwork with dynamic and productive team sites for every project team, department, and division

Microsoft Teams
Microsoft Teams is a hub for teamwork in Office 365

Google Drive

Managing Tenant License

1. Go to **Manage Tenants**.
2. In the table, click **License** in the **Actions** column for the tenant you want to set a limit.

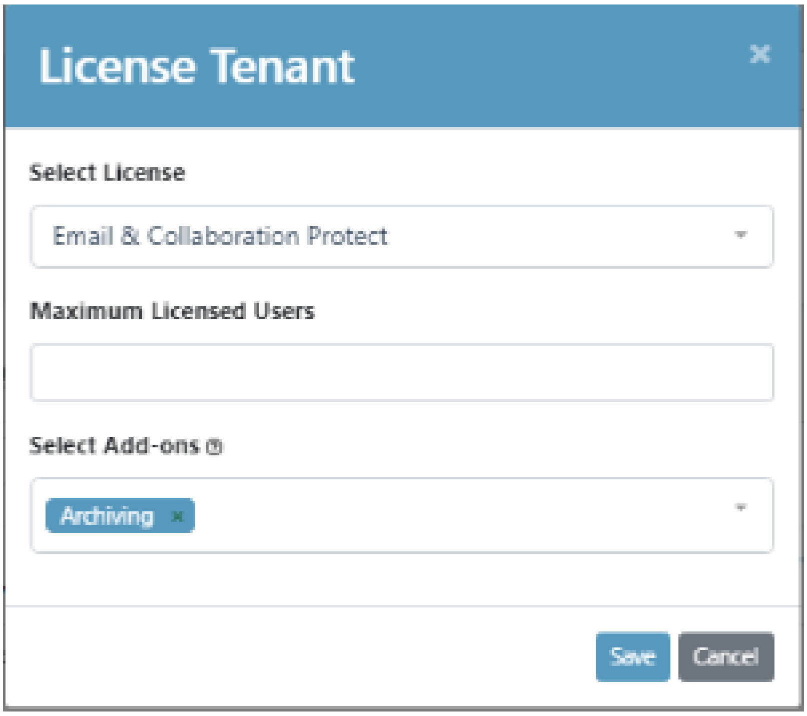


Manage Tenants

Paying Customers			POCs			Tenant Issues	
			Ongoing		Expired		
36 MSPs	26 Tenants	224 Users	1 Tenants	0 Users	21 Tenants	12 Warnings	0 Errors

License	Add-ons	Start Date	Configuration Template	Template Status	Expiry Date	Total Users	Max Users	Status	Actions
Email & Collaboration Advanced Protect		2024-09-07		No template			10	● Active	License ⋮
Email & Collaboration Complete Protect	Archiving	2024-02-05		No template		0		● Active	
Email & Collaboration Complete Protect	Archiving, DMARC, Security Awareness Training	2022-12-28		No template		23	20	● Active	
Email & Collaboration Complete Protect	DMARC	2022-03-02		No template		1	11	● Active	

The **License Tenant** pop-up appears.



License Tenant

Select License

Email & Collaboration Protect

Maximum Licensed Users

Select Add-ons

Archiving ×

3. From the **Select License** drop-down list, select the required license.

4. In the **Maximum Licensed Users**field, enter the maximum number of users to be protected.

5. (Optional) From the **Select Add-ons** field, select the required add-ons for the tenant.

   Note - Add-ons are optional features that require additional licenses. The selected add-ons are billed automatically by Avanan.

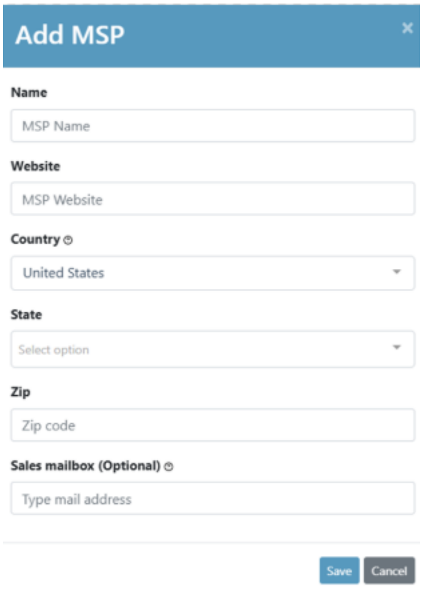
6. Click **Save**.

Creating a New MSP

Top-Level MSPs can manage Child MSPs. Each Child MSP is a fully functional MSP that can create and manage its tenants. Top-Level MSPs can manage both direct tenants and Child MSP tenants.

To create a new MSP:

1. Go to **Manage Tenants**.
2. Click **Create MSP**.
3. In the **Name** field, enter the MSP name.



4. In the **Website** field, enter the website associated with the MSP.
5. From the **Country** drop-down list, select the country the MSP is located in.
6. From the **State** drop-down list, select the state the MSP is located in.

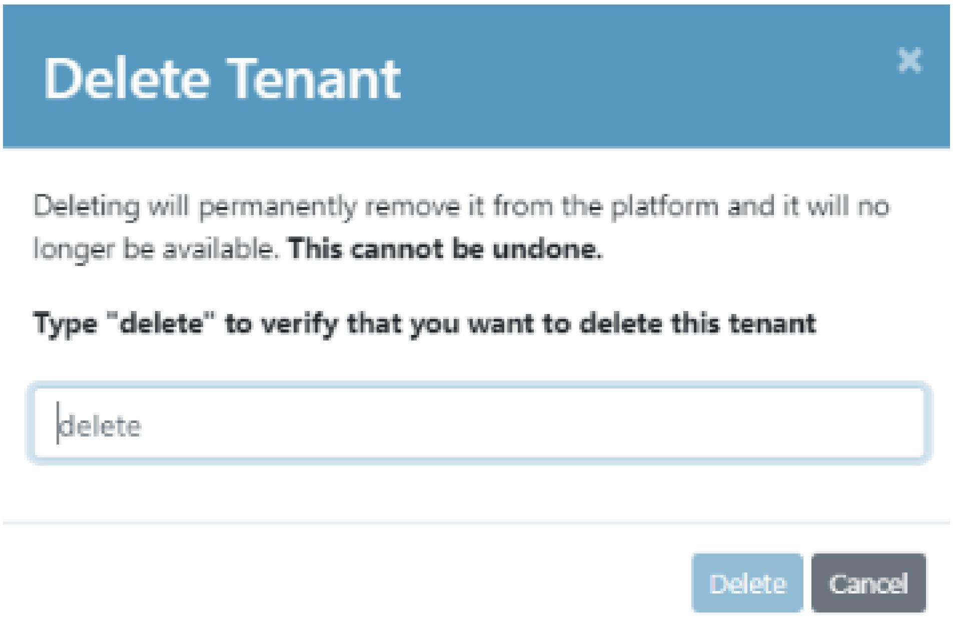
   Note - This option is available only if the MSP is created in the United States.

7. In the **Zip** field, enter the zip code of the area where the MSP is located.
8. Click **Save**.

Deleting a Tenant

1. Go to **Manage Tenants**.
2. Hover over the tenant and click ⋮.
3. Select **Delete**.

   The **Delete Tenant** window appears.



Delete Tenant

Deleting will permanently remove it from the platform and it will no longer be available. **This cannot be undone.**

Type "delete" to verify that you want to delete this tenant

delete

4. In the **delete** field, enter your justification.
5. Click **Delete**.

Templates for MSSPs

Overview

A Template is a structured collection of configuration settings designed to help Managed Security Service Providers (MSSPs) efficiently onboard and manage multiple tenants. By using reusable templates, MSSPs can streamline administrative workflows, ensure consistency across tenants, and accelerate customer onboarding.

Templates are derived from a Base Tenant, and they enable MSSPs to apply consistent security and operational policies in bulk with the following key characteristics:

- Provides a consistent set of predefined settings that can be applied across multiple tenants.
- Built using the configuration of an existing, designated tenant to simplify setup and ensure uniformity.

This functionality empowers MSSPs to maintain high standards of security and operational control across their tenant ecosystem.

Base Tenant: A Base Tenant is the source tenant from which a template is created. It serves as the reference point for copying configuration settings.

The base tenant’s configurations define the structure and content of the template, and enables MSSPs to apply consistent settings across multiple tenants.

Parent MSSPs: Parent MSSPs can create configuration templates and push them to:

- Tenants they manage directly.
- Tenants managed by MSSPs that they have created.

Benefits

- **Faster Customer Acquisition**: MSSPs can quickly apply predefined configurations to new customers.
- **Consistency Across Tenants**: Ensures aligned security and email configurations across all managed tenants.
- **Ease of Management**: Simplifies updates and propagates changes across multiple tenants efficiently.
- **Audit and Control:** Monitors configuration status and identifies deviations across tenants.

Template Lifecycle

The lifecycle of a template includes the following key steps:

1. **Create**: Create a new template based on a selected tenant's configuration. See *"Creating a Configuration Template" on page 27*.
2. **Assign**: Assign the template to one or more tenants. See *"Assigning Configuration Templates" on page 29*.
3. **Push**: Apply the template settings to the assigned tenants. See *"Pushing a Template to Tenants" on page 30*.
4. **Edit**: If required, update the base tenant or modify the template settings. See *"Editing a Configuration Template" on page 30*.
5. **Push Again**: If you made any changes to the template, reapply the updated template manually to keep assigned tenants aligned. See *"Pushing a Template to Tenants" on page 30*.

What Settings are Copied from the Template to the Tenant

When a configuration template is pushed to a tenant, the system copies the settings from the template to the tenant, depending on whether Office 365 Mail or Google Gmail is onboarded in the tenant.

Office 365 Mail

- Threat Detection policies
- Click-Time Protection policies
- Collaboration application settings and policies (for example, Office 365 OneDrive, Google Drive, Microsoft Teams, and more)
- Security Awareness Training settings include policies that are assigned to all users and custom phishing simulation templates
- DLP policies and Data Types

Notes:

- Policies applied to **All users and Groups** in the base tenant will be copied as **All Users and Groups**.
- Policies applied to specific users/groups in the base tenant will not be copied.

- Security Engine Settings (**Security Settings** > **Security Engines**)
  - Anti-Phishing
  - Anomalies

    Note - The system does not sync the Click-Time Protection engine settings.

- Office 365 Mail Notification Templates (**Security Settings** > **SaaS Applications** > **Office 365 Mail** > **Advanced**)
- **Exceptions**
  - Anti-Phishing
  - Anti-Spam (trusted senders, applied to all recipients)

    Notes:
    - The entries will not be modified when applying a template.
    - In the recipient tenant, all currently listed trusted senders remains unchanged.
  - URL Reputation
  - Anti-Malware
- User Interaction Settings (**Security Settings** > **User Interaction**)
  - End User Portal

    Note - If the End User Portal in the base tenant is activated for some users, it is enabled for all users in the tenants assigned to the template.
  - Daily Quarantine Digest
  - Automatic handling of restore requests and phishing reports
  - Automatic restore from Microsoft quarantine

Google Gmail

- Collaboration application settings and policies (for example, Office 365 OneDrive, Google Drive, Microsoft Teams, and more)
- Security Awareness Training settings
- **Exceptions**
  - Anti-Phishing
  - URL Reputation

  - Click-Time Protection
  - Anti-Malware
- User Interaction Settings (**Security Settings** > **User Interaction**)
  - End User Portal

    Note - If the End User Portal in the base tenant is activated for some users, it is enabled for all users in the tenants assigned to the template.
  - Daily Quarantine Digest
  - Automatic handling of restore requests and phishing reports
- Security Engine Settings (**Security Settings** > **Security Engines**)
  - Anti-Phishing
  - Anomalies

    Note - The system does not sync the Click-Time Protection engine settings.

What Settings are Not Copied from the Template to the Tenant

When a configuration template is pushed to a tenant, the system does not copy the following settings and data:

- DMARC management settings
- Smart Banners
- Archiving settings
- Security Checkup report scheduling
- Customers' personal data (for example, trusted senders for individual users')

  Note - The system copies the global trusted senders defined by administrators for all users.

Required Permissions

- Only Managed Service Security Provider (MSSP) Portal administrators can create and manage templates. See *"Creating a New Tenant" on page 17*.
- Help Desk Users can view template assignments but cannot modify them.

Creating a Configuration Template

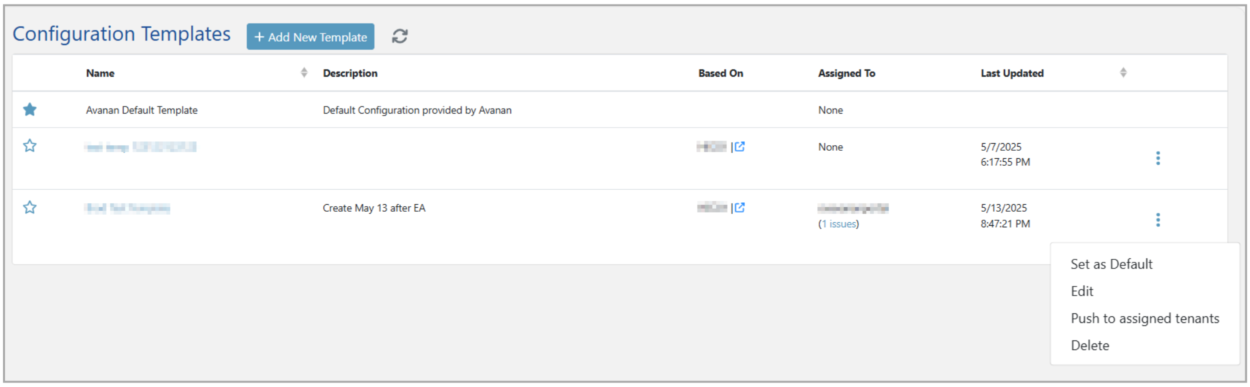
The Configuration Templates page allows administrators to:

- Create, edit, and delete configuration templates.
- Assign templates to tenants.
- View the assignment status of templates.
- Check the **Assigned To** column for the number of tenants using each template.
- Push updates to tenants. See *"Pushing a Template to Tenants" on page 30*.

Note - When a template is assigned but not pushed, the status for the tenant shows as **Not Aligned**.

To create a configuration template:

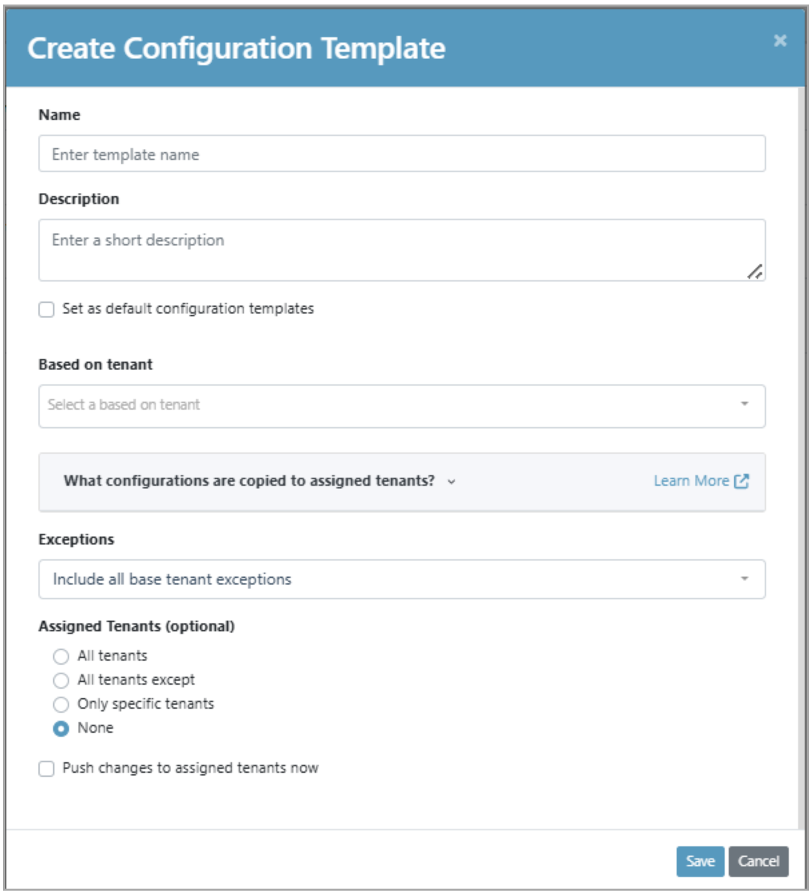
1. Go to **Templates**.
2. In the **Configuration Templates** page that appears, click **Add New Template** at the top of the page.



Configuration Templates

	Name	Description	Based On	Assigned To	Last Updated	
★	Avanan Default Template	Default Configuration provided by Avanan		None		
☆	[redacted]		[redacted]	None	5/7/2025 6:17:55 PM	⋮
☆	[redacted]	Create May 13 after EA	[redacted]	[redacted] (1 issues)	5/13/2025 8:47:21 PM	⋮

The **Create Configuration Template** pop-up appears.



Create Configuration Template

Name

Enter template name

Description

Enter a short description

□ Set as default configuration templates

Based on tenant

Select a based on tenant

What configurations are copied to assigned tenants? ⌄ Learn More

Exceptions

Include all base tenant exceptions

Assigned Tenants (optional)

○ All tenants
○ All tenants except
○ Only specific tenants
● None

□ Push changes to assigned tenants now

3. In the **Name** field, enter a name for the template.

4. In the **Description** field, describe the purpose or contents of the template.

5. (Optional) To make the template default for new tenants that you create, select **Set as default configuration templates** checkbox. See *"Creating a New MSP" on page 21*.

6. In the **Based on Tenant** section, select an existing tenant to use as the basis for the configuration.

7. From the **Exceptions** dropdown, select the required option:

   - **Include all base tenant exceptions (Default)**: Copies all exception configurations (such as allow-lists and block lists) from the base tenant into the template.
   - **Exclude all base tenant exceptions**: Excludes all exception configurations from being copied into the template.
   - **Include only base tenant block lists**: Copies only block-list exception entries from the base tenant into the template.
   - **Include only base tenant allow-lists**: Copies only allow-list exception entries from the base tenant into the template.

Note - If the **Exclude all base tenant exceptions** option is selected, the tooltip **[i]** for the **Exceptions** section will not display the word **Exceptions**.

8. (Optional) In the **Assigned Tenants** section, select the required tenants to assign the template:

    - All tenants
    - All tenants except
    - Only specific tenants
    - None (default)

    Note -You can assign tenants to the template even after creating it. See *"Assigning Configuration Templates" below*.

9. (Optional) To apply the template to the selected tenants immediately, select **Push changes to assigned tenants now** checkbox.

10. Click **Save**.

Assigning Configuration Templates

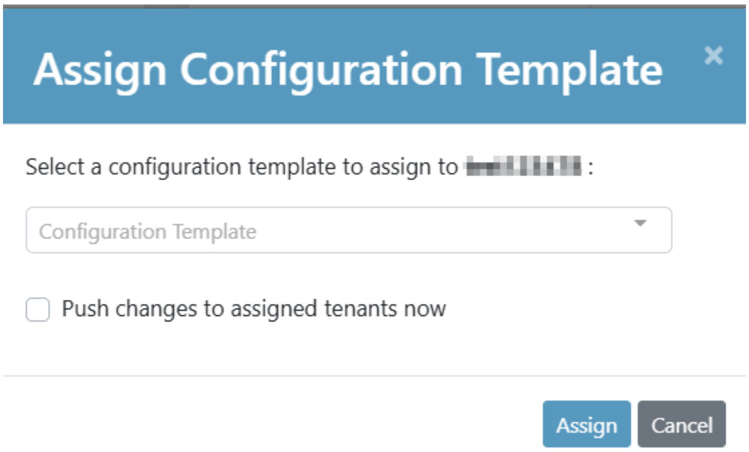
To assign a configuration template to the tenant:

1. Go to **Manage Tenants**.

2. In the table, click the ⋮ icon next to the **Actions** column for the tenant you want to assign a configuration template.

3. Click **Assign Template**.

    The **Assign Configuration Template** pop-up appears.



Assign Configuration Template ×

Select a configuration template to assign to [redacted] :

Configuration Template ▾

□ Push changes to assigned tenants now

4. In the **Select a configuration template to assign to** section, select the required configuration template.

5. (Optional) To apply the template to the selected tenant immediately, select **Push changes to assigned tenants now** checkbox.

6. Click **Assign**.

Finding a Tenant's Template Assignment State

1. Go to **Manage Tenants**.

2. The **Configuration Template** column shows the assigned template for each tenant.

3. To view a specific tenant's assigned template, use the available filtering and sorting options. See, *"Managing Tenants and MSPs" on page 16*.

Editing a Configuration Template

To edit a configuration template:

1. Go to **Templates**.

2. In the **Configuration Template** page that appears, click the ⋮ icon for the template you want to edit.

3. Click **Edit**.

4. In the **Edit Configuration Template** pop-up that appears, make the required changes.

5. Click **Save**.

Pushing a Template to Tenants

To push a configuration template to tenants through the Manage Tenants page:

1. Go to **Manage Tenants**.

2. In the table, click the ⋮ icon next to the **Actions** column for the tenant you want to push a template.

3. Click **Push Template**.

4. In the **Push Template** confirmation pop-up that appears, click **Push**.

To push a configuration template to tenants through the Templates page:

1. Go to **Templates**.
2. In the **Configuration Template** page that appears, click the ⋮ icon for the template you want to push to the tenant.
3. Click **Push to assigned tenants**.
4. In the **Push Template** confirmation pop-up that appears, click **Push**.

Handling Deviations

If a tenant deviates from its assigned template, it no longer reflects the full set of configurations intended by the MSSP, which may result in missing critical security or operational settings.

Template Status Indicators

The **Manage Tenants** page displays the deviation status in the **Template Status** column with the following states:

- **No Template**: The tenant does not have a configuration template assigned.
- **Aligned**: The tenant's configuration matches the assigned template.
- **Blank**: The tenant is edited and deviates from the assigned template.
- **Failed to Push**: An error occurred while applying the template to the tenant.
- **Updating**: The template is currently being applied to the tenant.

Note - Administrators can resolve the tenant deviations by clicking **Push Template**. To do that, see *"Pushing a Template to Tenants" on the previous page*.

Error Handling

In the **Configuration Templates** Page:

- Errors appear alongside tenant counts in the **Assigned to** column.
- Hover over errors to view detailed breakdown of it.
- Click the error count to open **Tenant Management** with applied filters.

Note - Administrators can resolve the tenant deviations by clicking **Pushed to assigned tenants**. To do that, see *"Pushing a Template to Tenants" on the previous page*.

Deleting Templates and Base Tenants

- **Template Deletion**: When a template is deleted, assigned tenants retain their configuration settings but lose the association with the template.

  To delete a configuration template:

  1. Go to **Templates**.
  2. In the **Configuration Template** page that appears, click the ⋮ icon for the template you want to delete.
  3. Click **Delete**.
  4. In the **Delete Deployment Template** confirmation pop-up that appears, click **Delete**.

- **Base Tenant Deletion**: The system blocks deletion of a base tenant if a template is based on it. You must assign the template to another tenant before deleting it.

  To delete a base tenant:

  1. Go to **Manage Tenants**.
  2. In the table, click the ⋮ icon next to the **Actions** column for the tenant you want to delete.
  3. Click **Delete**.
  4. In the **Delete Deployment Template** confirmation pop-up that appears, click **Delete**.

Setting a Template as a Default Template

Administrators can set any template as the default template. When creating new tenants, the system automatically pre-fills the default template. See *"Creating a New Tenant" on page 17*.

To make a Template the default template after creating it:

1. Go to **Templates**.
2. In the **Configuration Template** page that appears, click the ⋮ icon for the template you want to make default template.

3. Click **Set as Default**.

   The system sets the selected configuration template as the default template.

Settings

Authentication

The Managed Service Provider (MSP) Portal Authentication controls the authentication settings, with these configurations:

- Multi-Factor Authentication
- Enabling MFA
- SAML Authentication

Multi-Factor Authentication

Multi-Factor Authentication (MFA) allows to force login with a two-factor authentication platform, such as Google Authenticator.

Enabling MFA

1. Log in to the Avanan MSP Administrator Portal:
2. Go to **Settings**.
3. Expand **Authentication Settings** and click **Configure MFA**.
4. Scan the QR code using an authenticator software, such as Google Authenticator.
5. Enter the generated token.
6. Click **Continue**.

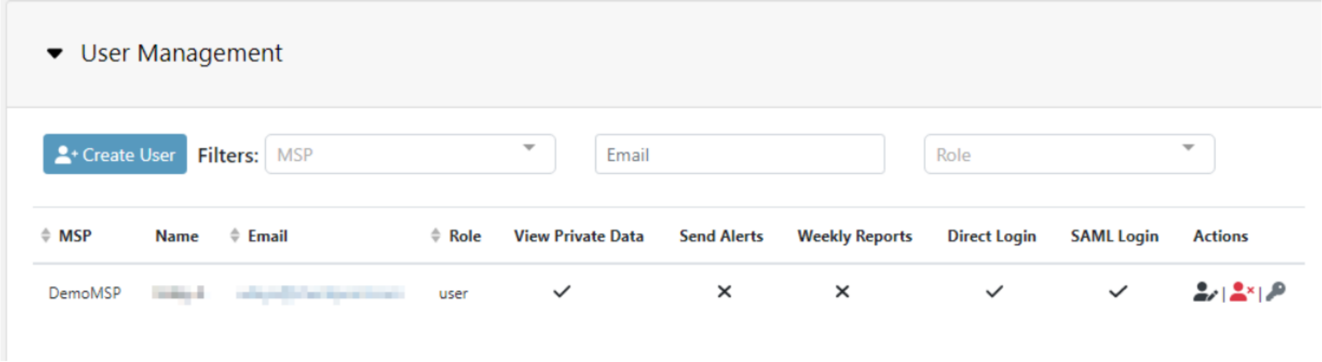
SAML Authentication

For information on how to configure SAML authentication, see *"SAML SSO Integration" on page 48*.

User Management

User management allows MSPs to control their MSP Portal users. It is possible to add, remove and edit users according to needs. Top-Level MSPs can also manage Child MSP users.

All users are portal administrators and gain access to the managed tenants. Each user can be configured to log in with a password or with SAML (if available).



MSP	Name	Email	Role	View Private Data	Send Alerts	Weekly Reports	Direct Login	SAML Login	Actions
DemoMSP	[redacted]	[redacted]	user	✓	✕	✕	✓	✓	

MSP Portal User Roles

MSP portal users can be assigned a role in the MSP Portal to view and control the customer portals they have access to.

There are two MSP Portal roles:

- **MSP Admin** - Can access all the customer portals and have full access to the MSP portal settings and reporting.
- **MSP Help Desk** - Can access only a set of customer portals and are not allowed to change the MSP portal settings.

Permissions for the different MSP Portal roles:

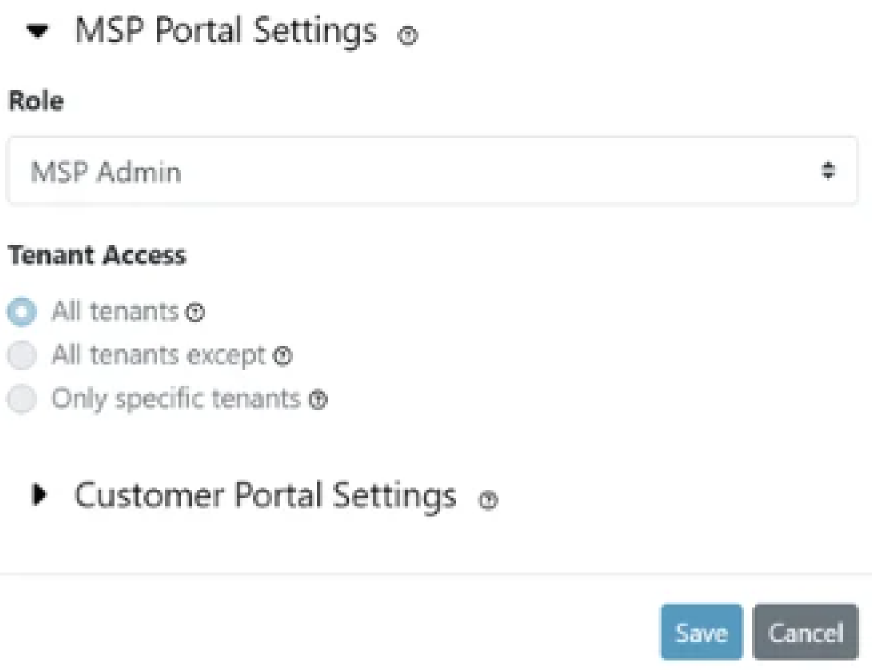
Feature		MSP Admin	MSP Help Desk
Managing MSP Portal	User Management	Can view and edit	Cannot view
	Branding	Can view and edit	Cannot view
	Authentication Settings	Can view and edit	Cannot view
	Other Settings	Can view and edit	Cannot view
Tenant Information	Security Settings	Can view for all the tenants	Can view only for the assigned tenants
	Usage Report	Can view for all the tenants	Cannot view
	MSP Portal Notifications (if enabled)	Can receive for all the tenants	Can receive only for the assigned tenants

Feature		MSP Admin	MSP Help Desk
Tenant Actions	Child MSP Actions	Can do	Cannot do
	Create Child MSP	Can do	Cannot do
	Delete Tenant	Can do	Cannot do
	License Tenant	Can do	Cannot do
	Configuration Template	Can view and edit	Can view only for the assigned tenants
Audit	View Audit Logs	Can view	Cannot view

Assigning Customer Tenants to MSP Help Desk Users

To assign the customer tenants to a Help Desk user:

1. Log in to the Avanan MSP Administrator Portal:
2. Go to **Settings** > **User Management**.
3. For the user you want to assign customer tenants, click **Edit**.
4. Expand **MSP Portal Settings**.



▾ MSP Portal Settings

Role

MSP Admin

Tenant Access

● All tenants
○ All tenants except
○ Only specific tenants

▸ Customer Portal Settings

5. From the **Role** list, select **MSP Help Desk**.
6. From the **Tenant Access** options, select one of these:

- To allow access to all the tenants, select **All tenants**.
- To allow access to all the tenants except some tenants, select **All tenants except** and then select the tenants that need to be excluded.
- To allow access only to some tenants, select **Only specific tenants** and then select the tenants you need to include.

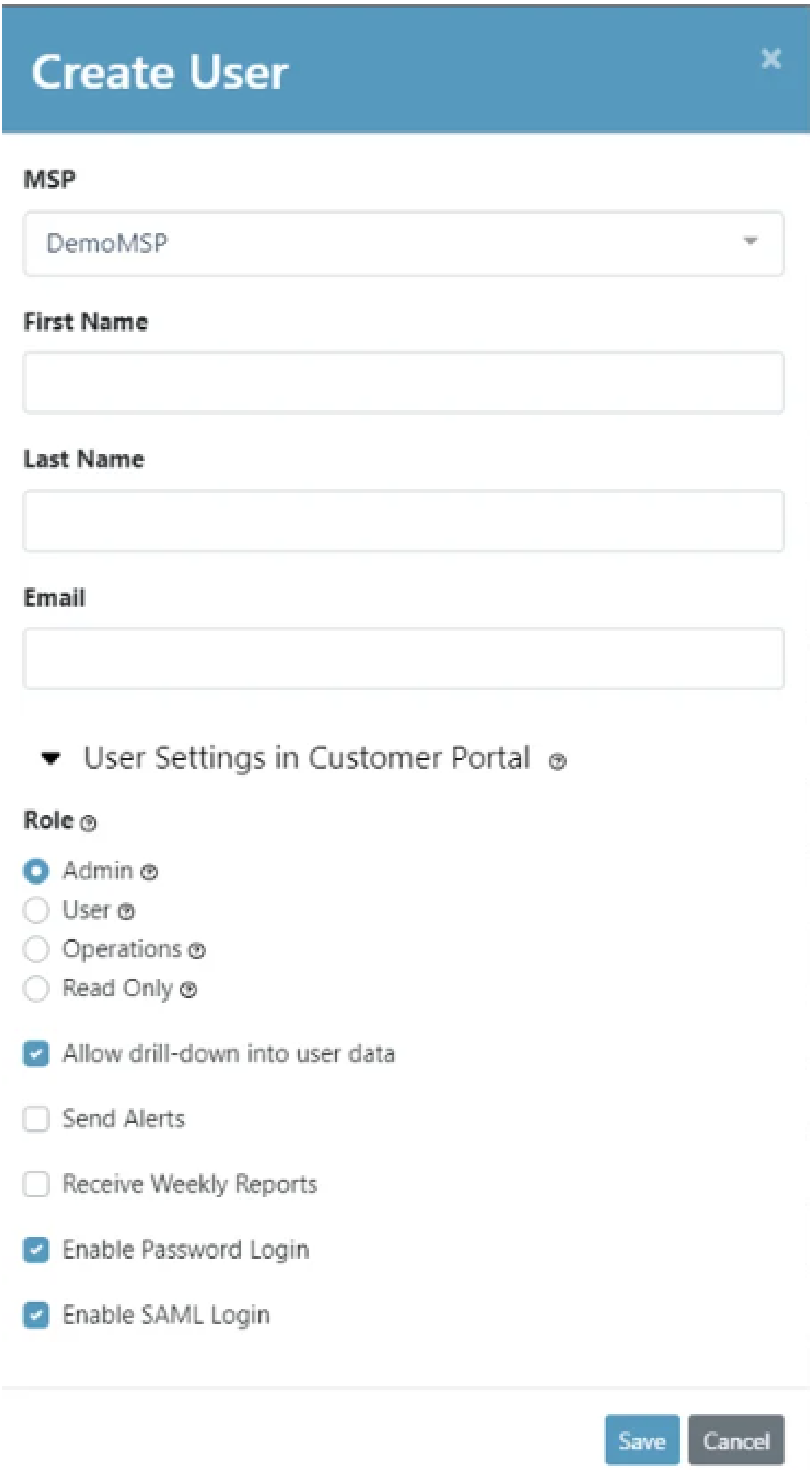
7. Click **Save**.

Creating and Managing User

1. Log in to the Avanan MSP Administrator Portal:
2. Go to **Settings**.
3. Expand **User Management** and click **Create User**.

   The **Create User** window appears.
4. Specify these:
   a. **MSP** - Associate user with Child MSP (available for Top-Level MSP only).
   b. **First Name**
   c. **Last Name**

d. **Email address**



Create User

MSP

DemoMSP

First Name

Last Name

Email

User Settings in Customer Portal

Role

● Admin
○ User
○ Operations
○ Read Only

☑ Allow drill-down into user data

□ Send Alerts

□ Receive Weekly Reports

☑ Enable Password Login

☑ Enable SAML Login

5. Expand **User Settings in Customer Portal** and from the **Role** list, select the role associated with the user in the managed tenants:
   a. **Admin**
   b. **User**
   c. **Operations**
   d. **Read Only**
6. Select the checkbox:
   a. **Allow drill-down into user data** - To allow admin to view email content (on tenant portal). Viewing email content is audited.
   b. **Send Alerts** - To allow admin to resend alerts to users.
   c. **Receive Weekly Reports** - For admins to receive weekly admin reports from each tenant.
   d. **Enable Password Login** - For password authentication method.
   e. **Enable SAML Login** - For SAML authentication method.
7. Click **Save**.
8. To edit a user, from the actions column, click 👤✎.

   The **Edit User** window appears.
9. Make the required changes and click **Save**.
10. To delete a user, from the actions column, click 👤✕ .
11. To reset the password, from the actions column, click 🔑 .

Notifications

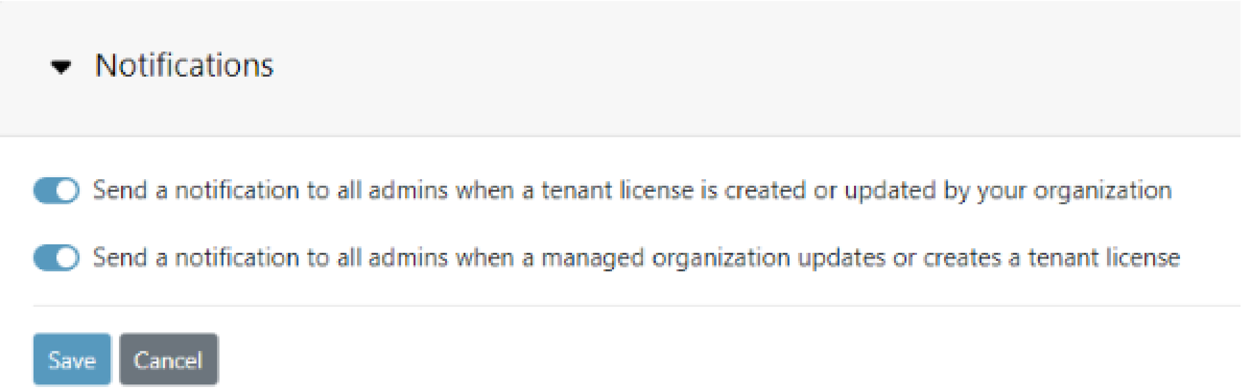
Avanan MSP Administrator Portal allows sending email notifications when there are updates to the tenant license and managed organization updates.

To update notifications:

1. Log in to the Avanan MSP Administrator Portal:
2. Go to **Settings**.
3. Expand Notifications and click **Create User**.

   The **Create User** window appears.
4. Enable the appropriate toggle button:

- **Send a notification to all admins when a tenant license is created or updated by your organization**
- **Send a notification to all admins when a managed organization updates or creates a tenant license**



Notifications

Send a notification to all admins when a tenant license is created or updated by your organization

Send a notification to all admins when a managed organization updates or creates a tenant license

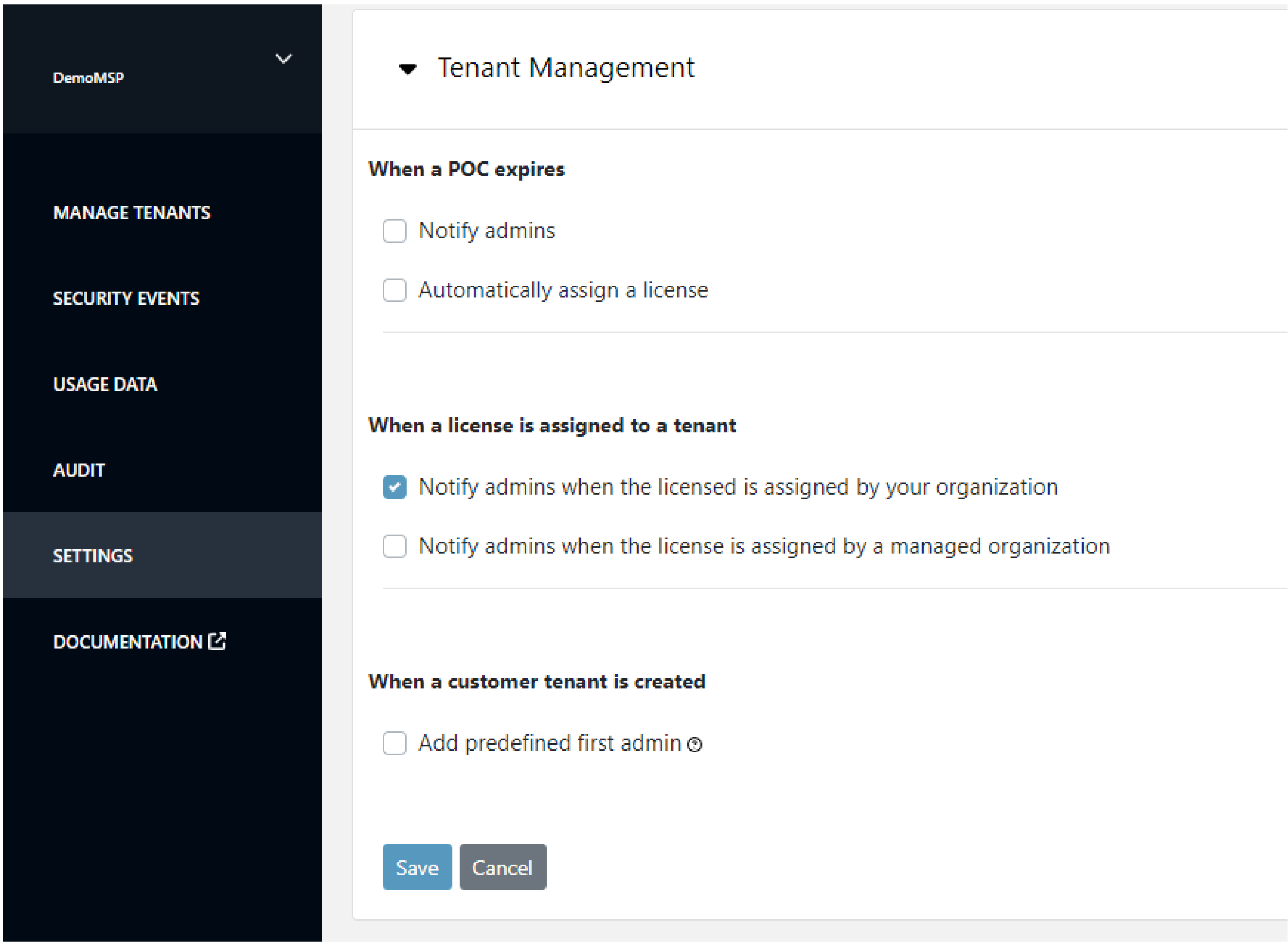
5. Click **Save**.

Tenant Management

Managed Service Providers (MSP) onboard customers on a daily basis and need to keep track of the customer acquisition lifecycle. After the POC (trial period) ends, Avanan stops protecting users without a license.

The **Tenant Management** page allows administrators to configure automatic actions when a POC expires.

To view the **Tenant Management** page, go to **Settings** > **Tenant Management**.



Tenant Management

When a POC expires

□ Notify admins

□ Automatically assign a license

When a license is assigned to a tenant

☑ Notify admins when the licensed is assigned by your organization

□ Notify admins when the license is assigned by a managed organization

When a customer tenant is created

□ Add predefined first admin

When a POC expires:

1. Go to the **When a POC Expires** section.
2. To send email notifications to administrators when a POC expires, select the **Notify Admins** toggle button.
3. To assign a license automatically after the POC expires, do these:
   a. From the **License** list, select the license.
   b. From the **Add-ons** list, select the add-ons.

      Note - You can select multiple add-ons.

   c. In the **Maximum licensed users** field, enter the number of licenses.
4. Click **Save**.

When a license is assigned to a tenant:

1. To send email notifications to administrators when a license is assigned to a tenant, select the **Notify admins when the license is assigned by your organization** toggle button.
2. To send email notifications to administrators when a license is assigned to a tenant, select the **Notify admins when the license is assigned by a managed organization** toggle button.
3. Click **Save**.

Customize Branding

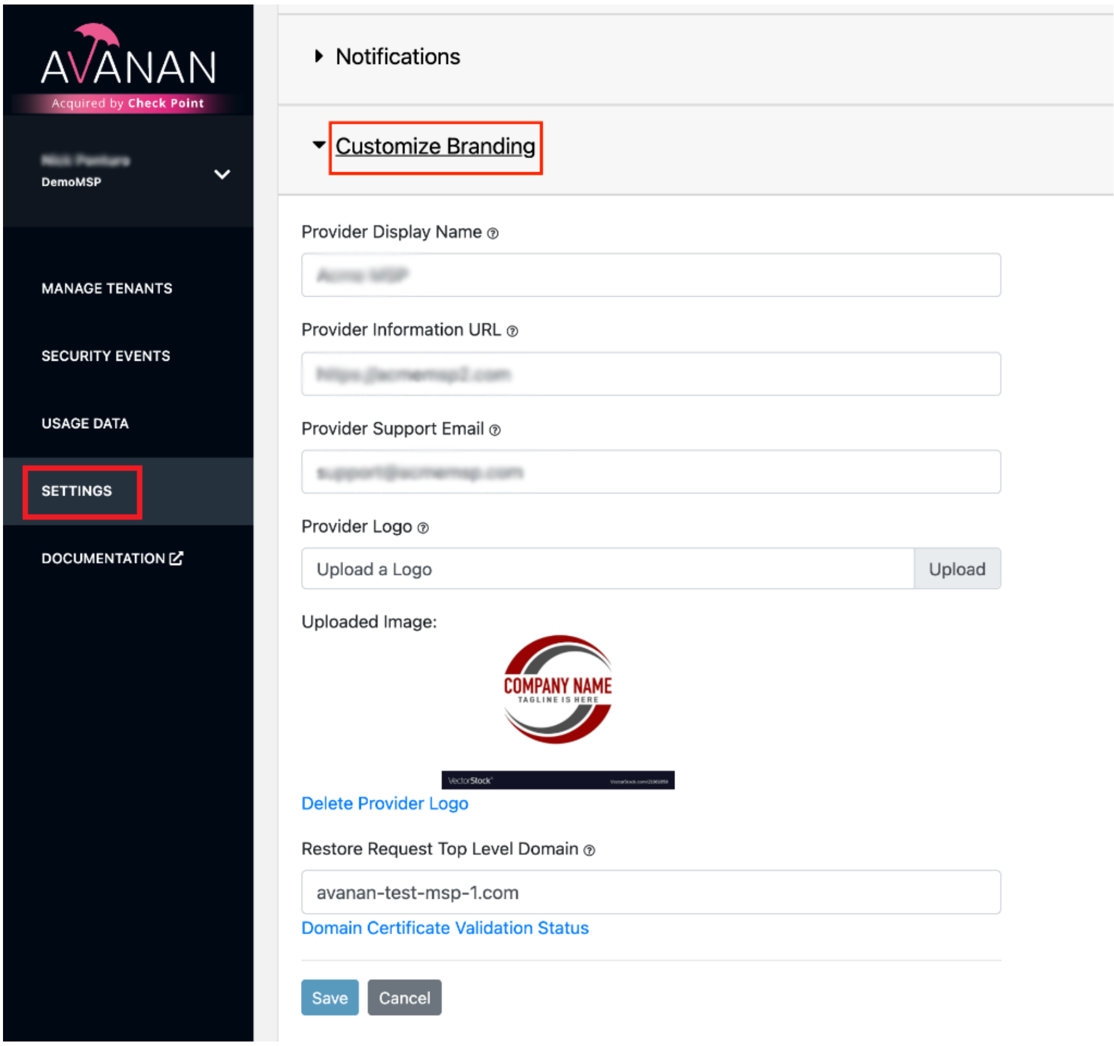
As part of customized branding, you can replace the name and logo of Avanan with the name of your MSP. The name of your MSP appears in the restore requests and email notifications to Office 365 and gmail end-users.

The fields for customized MSP branding:

Customizable Field	Description
Provide Display Name	MSP name to use instead of Avanan as the display name for emails to end-users.
Provide Information URL	MSP website or MSP documentation site URL.
Provider Support Email	MSP support email address.
Provider Logo	MSP logo.
Restore Request Top Level Domain	Link used to submit restore requests to release emails from quarantine. For example, if the default link is *https://CompanyName.avanan.net/email_restore...*, you can customize it to *https://CompanyName.ProviderDomain.suffix/emai_restore...*. For more information, see Configuring Request Top Level Domain. For each customer tenant, a `CNAME` with the new custom URL needs to be created pointing at the original customer URL.

Configuring Customized Branding

1. Log in to the https://portal.avanan.net.
2. Click **Settings**.
3. Expand **Customize Branding** and enter these:



Provider Display Name: [redacted]

Provider Information URL: [redacted]

Provider Support Email: [redacted]

Provider Logo: Upload a Logo | Upload

Uploaded Image:

Delete Provider Logo

Restore Request Top Level Domain: avanan-test-msp-1.com

Domain Certificate Validation Status

   a. In the **Provider Display Name** field, enter the MSP display name.

   b. In the **Provider Information URL** field, enter the MSP information URL.

   c. In the **Provider Support Email** field, enter the MSP support email.

   d. From the **Provider Logo** field, select the MSP logo and click **Upload**.

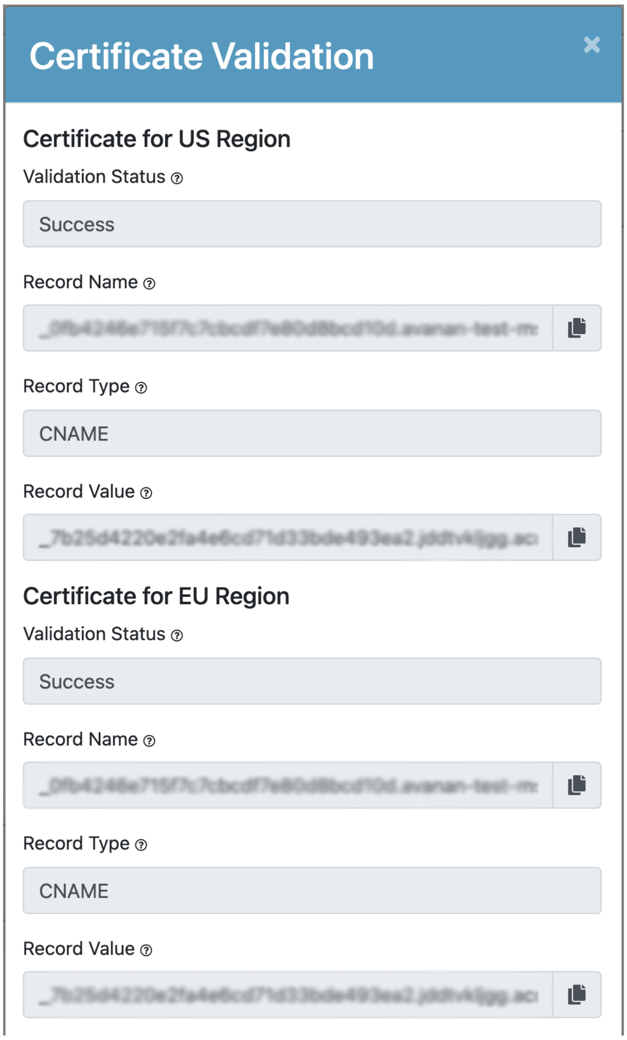
   e. In the **Restore Request Top Level Domain** field, enter the MSP top-level domain name.

4. Click **Save**.

Configuring Restore Request Top-Level Domain

Once you save the domain name in the **Retore Request Top Level Domain**, Avanan requests a certificate from AWS Certificate Manager for the domain to serve.

A validation DNS record is automatically generated in the **Domain Certificate Validation Status** modal. The modal shows the details of **Certificate Validation Status**, **Record Name**, **Record Type**, and **Record Value**.



Certificate Validation

Certificate for US Region

Validation Status: Success

Record Name: [redacted]

Record Type: CNAME

Record Value: [redacted]

Certificate for EU Region

Validation Status: Success

Record Name: [redacted]

Record Type: CNAME

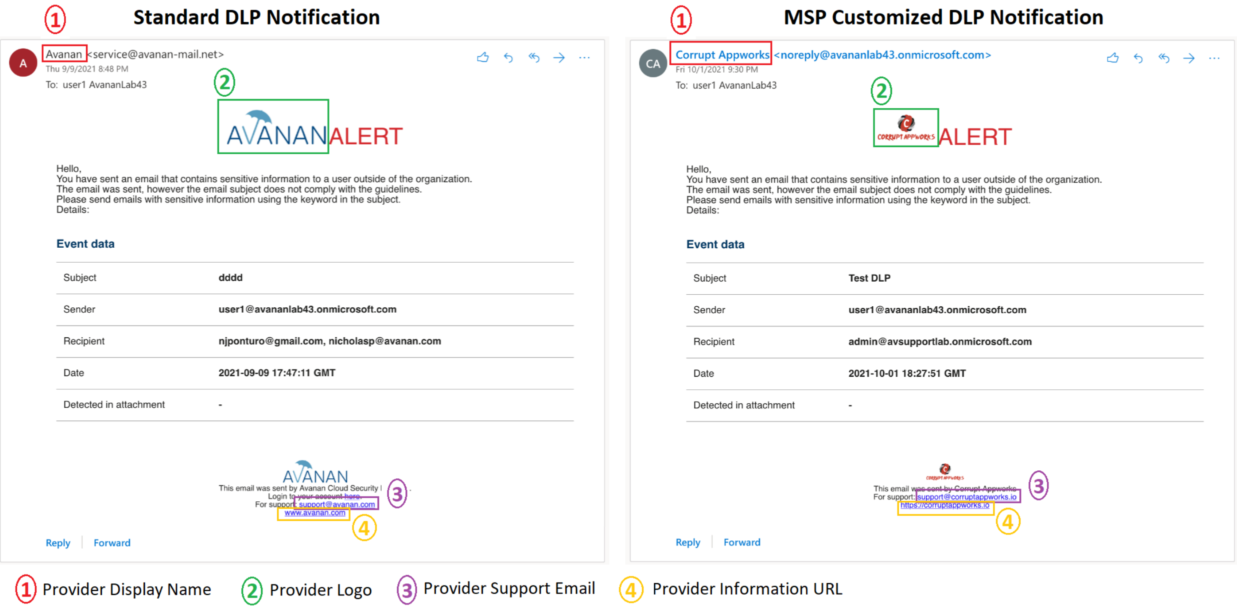
Record Value: [redacted]

Notes:

- The MSP has to go to the DNS provider and create a record with the generated **Record Name**, **Record Type**, and **Record Value** from the modal. Once the record is completed, Avanan uses the custom domain in the notifications for end-user emails.
- The MSP must add a record to their DNS provider for each of their Avanan tenants. The record should be a `cname` with the Avanan tenant domain name as the first part.
  For example, Avanan tenant `abccompany.avanan.net` should have a `cname` record `abccompany.restorerequestdomain.com` pointing to `abccompany.avanan.net` where `restorerequestdomain.com` is the MSPs custom restore request ID.

Examples

- Customized DLP notification to end-users.



Standard DLP Notification

Avanan <service@avanan-mail.net>
Thu 9/9/2021 8:48 PM
To: user1 AvananLab43

AVANAN ALERT

Hello,
You have sent an email that contains sensitive information to a user outside of the organization.
The email was sent, however the email subject does not comply with the guidelines.
Please send emails with sensitive information using the keyword in the subject.
Details:

Event data

Subject	**dddd**
Sender	**user1@avananlab43.onmicrosoft.com**
Recipient	**njponturo@gmail.com, nicholasp@avanan.com**
Date	**2021-09-09 17:47:11 GMT**
Detected in attachment	-

AVANAN
This email was sent by Avanan Cloud Security |
Login to your account here.
For support: support@avanan.com
www.avanan.com

Reply | Forward

MSP Customized DLP Notification

Corrupt Appworks <noreply@avananlab43.onmicrosoft.com>
Fri 10/1/2021 9:30 PM
To: user1 AvananLab43

CORRUPT APPWORKS ALERT

Hello,
You have sent an email that contains sensitive information to a user outside of the organization.
The email was sent, however the email subject does not comply with the guidelines.
Please send emails with sensitive information using the keyword in the subject.
Details:

Event data

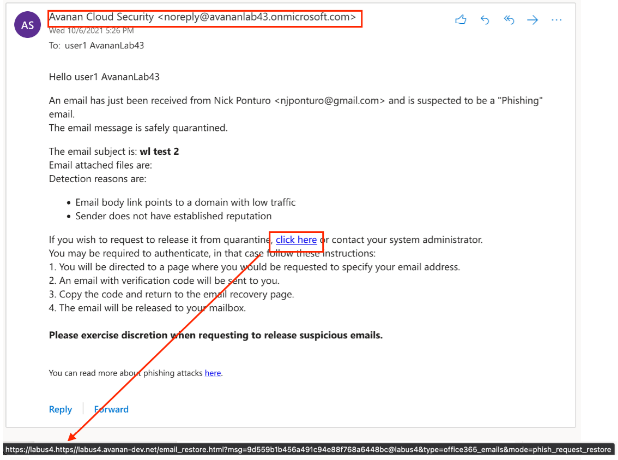
Subject	**Test DLP**
Sender	**user1@avananlab43.onmicrosoft.com**
Recipient	**admin@avsupportlab.onmicrosoft.com**
Date	**2021-10-01 18:27:51 GMT**
Detected in attachment	-

CORRUPT APPWORKS
This email was sent by Corrupt Appworks
For support: support@corruptappworks.io
https://corruptappworks.io

Reply | Forward

- Customized link to request release from quarantine by end-users.

Standard Restore Notification



Avanan Cloud Security <noreply@avananlab43.onmicrosoft.com>
Wed 10/6/2021 5:26 PM
To: user1 AvananLab43

Hello user1 AvananLab43

An email has just been received from Nick Ponturo <njponturo@gmail.com> and is suspected to be a "Phishing" email.
The email message is safely quarantined.

The email subject is: **wl test 2**
Email attached files are:
Detection reasons are:

- Email body link points to a domain with low traffic
- Sender does not have established reputation

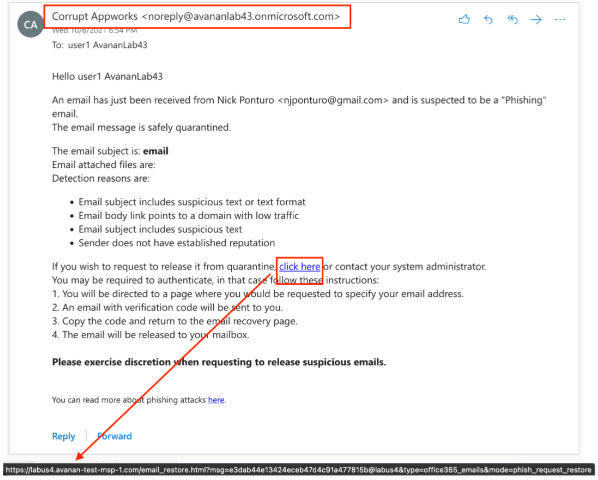
If you wish to request to release it from quarantine, click here or contact your system administrator.
You may be required to authenticate, in that case follow these instructions:
1. You will be directed to a page where you would be requested to specify your email address.
2. An email with verification code will be sent to you.
3. Copy the code and return to the email recovery page.
4. The email will be released to your mailbox.

Please exercise discretion when requesting to release suspicious emails.

You can read more about phishing attacks here.

https://labus4.https//labus4.avanan-dev.net/email_restore.html?msg=9d559b1b456a491c94e88f768a6448bc@labus4&type=office365_emails&mode=phish_request_restore

Customized Restore Notification



Corrupt Appworks <noreply@avananlab43.onmicrosoft.com>
Wed 10/6/2021 6:54 PM
To: user1 AvananLab43

Hello user1 AvananLab43

An email has just been received from Nick Ponturo <njponturo@gmail.com> and is suspected to be a "Phishing" email.
The email message is safely quarantined.

The email subject is: **email**
Email attached files are:
Detection reasons are:

- Email subject includes suspicious text or text format
- Email body link points to a domain with low traffic
- Email subject includes suspicious text
- Sender does not have established reputation

If you wish to request to release it from quarantine, click here or contact your system administrator.
You may be required to authenticate, in that case follow these instructions:
1. You will be directed to a page where you would be requested to specify your email address.
2. An email with verification code will be sent to you.
3. Copy the code and return to the email recovery page.
4. The email will be released to your mailbox.

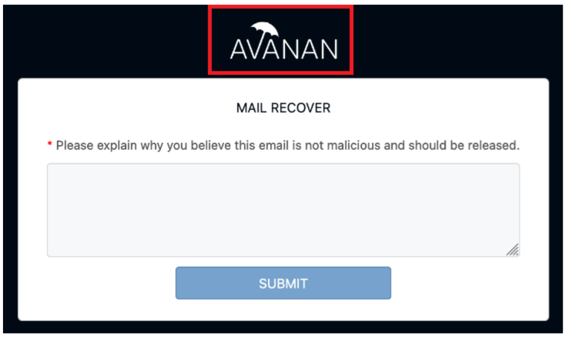
Please exercise discretion when requesting to release suspicious emails.

You can read more about phishing attacks here.

https://labus4.avanan-test-msp-1.com/email_restore.html?msg=e3dab44e13424eceb47d4c91a477815b@labus4&type=office365_emails&mode=phish_request_restore

- Customized restore request.

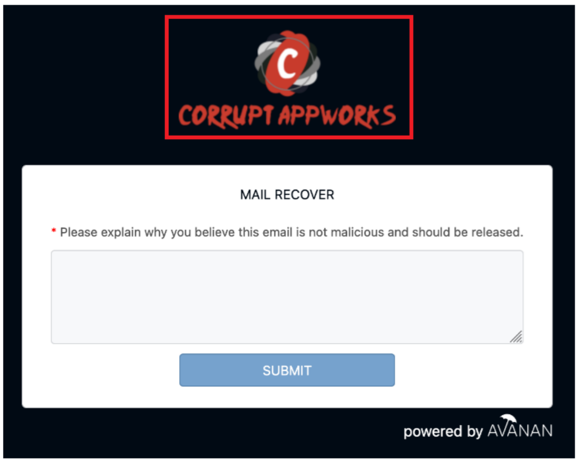
Avanan Restore Request Page



MAIL RECOVER

* Please explain why you believe this email is not malicious and should be released.

MSP Customized Restore Request Page



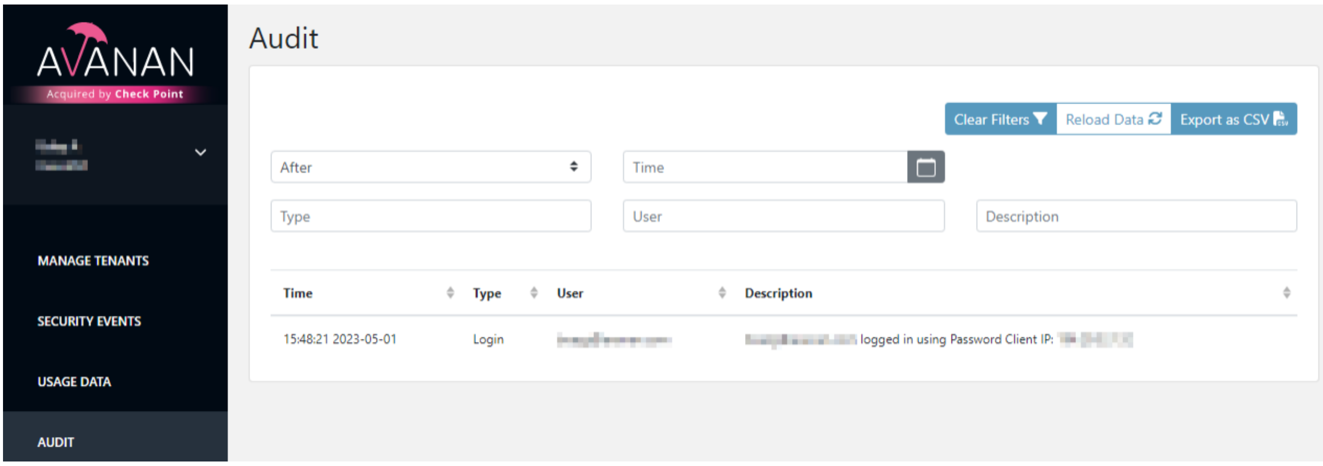
MAIL RECOVER

* Please explain why you believe this email is not malicious and should be released.

Audit

Avanan audits all the user actions performed in the MSP portal and adds them to the Audit page for forensic and auditing purposes.

The Audit page shows the user actions (onboarding new customers, assigning licenses, and so on) taken only in the MSP portal. It do not show the actions taken on the individual customer portals.



Time	Type	User	Description
15:48:21 2023-05-01	Login	[redacted]	[redacted] logged in using Password Client IP: [redacted]

Item	Description
Time	Date and time the action was started.
Type	Type of action performed.
User	Email address of the user who initiated the action.
Description	Action description.

You can filter logs by date, type of event, user, or description.

To export the results to an excel file, click **Export as CSV** in the top-right corner.

SAML SSO Integration

Avanan Managed Service Provider (MSP) Portal supports Single Sign-On (SSO) with various providers using SAML. Once SAML integration is enabled on the portal, each portal user can be configured to log in with either SAML or credentials (or both).

Configuring SAML Integration

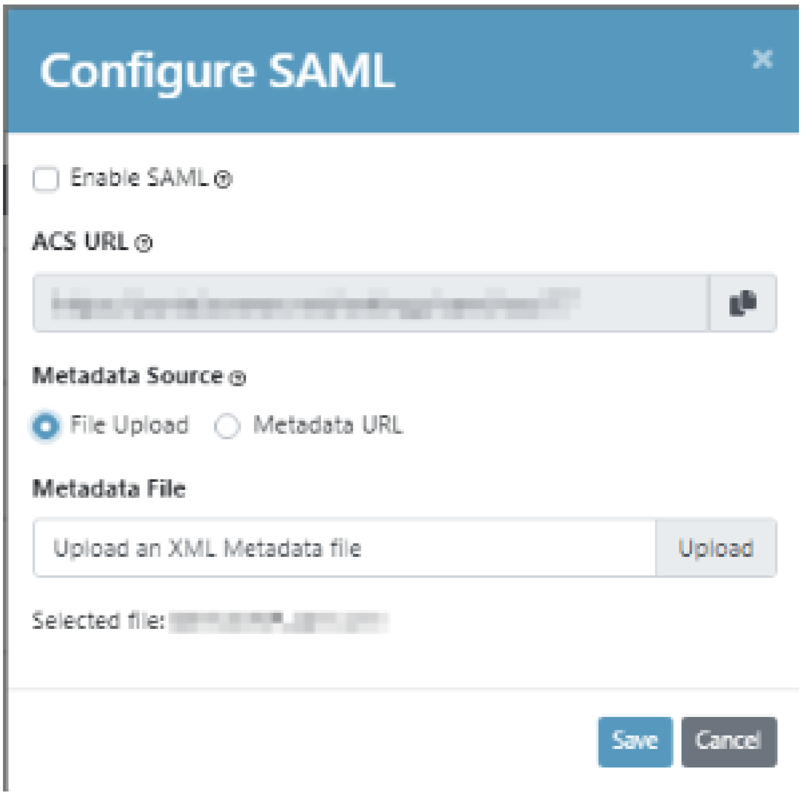
SAML Identity providers require:

- Assertion Consumer Service (ACS) URL (Single Sign-On URL) or the Entity ID of the service provider (Audience URI).
- Metadata Source, either in Metadata File in .xml format, or a Metadata URL, both can be obtained from the Identity Provider.

To configure SAML integration:

1. Go to **Settings**.
2. Expand **Authentication Settings** and click **Configure SAML**.

   The **Configure SAML** window appears.



Configure SAML

□ Enable SAML

ACS URL

[redacted]

Metadata Source

● File Upload ○ Metadata URL

Metadata File

Upload an XML Metadata file

Selected file: [redacted]

3. Select the **Enable SAML** checkbox.

4. To copy the ACS URL value, in the **ACS URL** field, click ⧉.

   Note - You must provide this URL to your Identity Provider.

5. Do these:

Action	Metadata Source	Metadata File
To add a local file	File Upload	Enter the path of the file.
To add a file from a URL	Metadata URL	Select the required file and click **Upload**.

6. Click **Save**.

User Authentication with SAML

For each user in the MSP portal, it is possible to set the allowed authentication method. When SAML integration is enabled, users can use SSO for their log in. Each user can log in with SAML, credentials, or both. It is advised that at least one of the administrator would be allowed to log in with credentials in case of an error in the SSO login or the SAML integration.

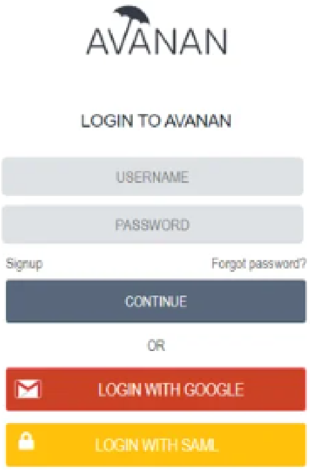
To set the authentication method for a user:

1. Go to **Settings**.
2. Expand **User Management**.
3. Select the user you want to edit, and under **Action**, click 👤.
4. Select the required options:
   - **Enable Password Login**

    - **Enable SAML Login**

5. Click **Save**.

Note - To log in using SSO to the Avanan MSP Administrator Portal, select Login with SAML.



SAML SSO Integration with Microsoft Azure

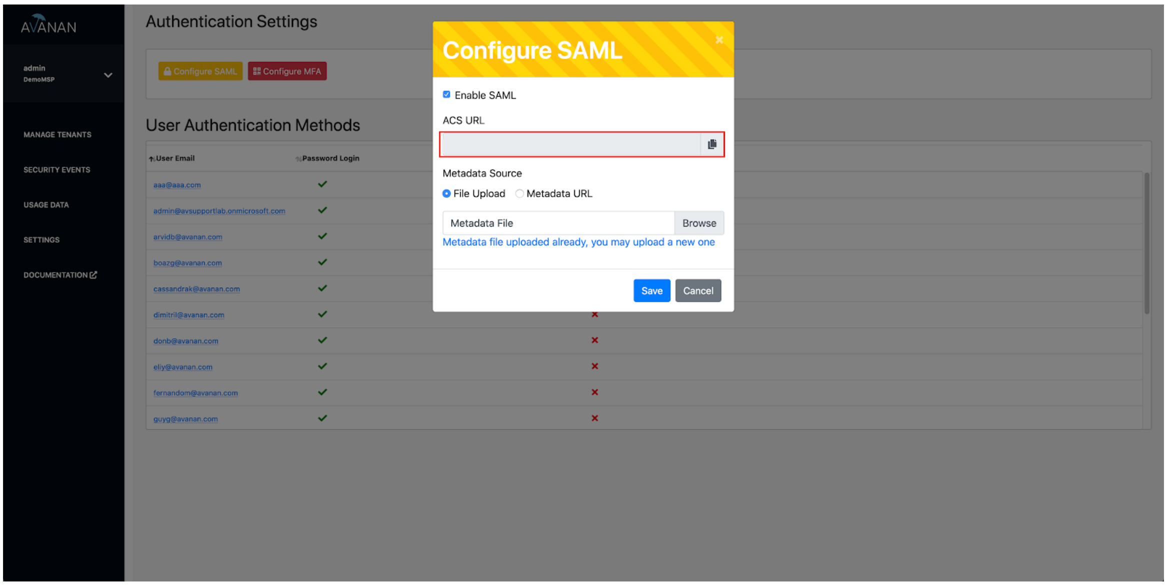
To configure Microsoft Azure as SAML Provider for the Avanan MSP Portal:

1. Log in to the Avanan MSP Administrator Portal:

   a. Go to **Settings**.

   b. Expand **Authentication Settings** and click **Configure SAML**.

   The **Configure SAML** window appears.



Authentication Settings

User Authentication Methods

User Email	Password Login	
aaa@aaa.com	✓	
admin@avsupportlab.onmicrosoft.com	✓	
arvidb@avanan.com	✓	
boazg@avanan.com	✓	
cassandrak@avanan.com	✓	
dimitril@avanan.com	✓	✗
donb@avanan.com	✓	✗
eliy@avanan.com	✓	✗
fernandom@avanan.com	✓	✗
guyg@avanan.com	✓	✗

Configure SAML

☑ Enable SAML

ACS URL

Metadata Source

● File Upload ○ Metadata URL

Metadata File

Metadata file uploaded already, you may upload a new one

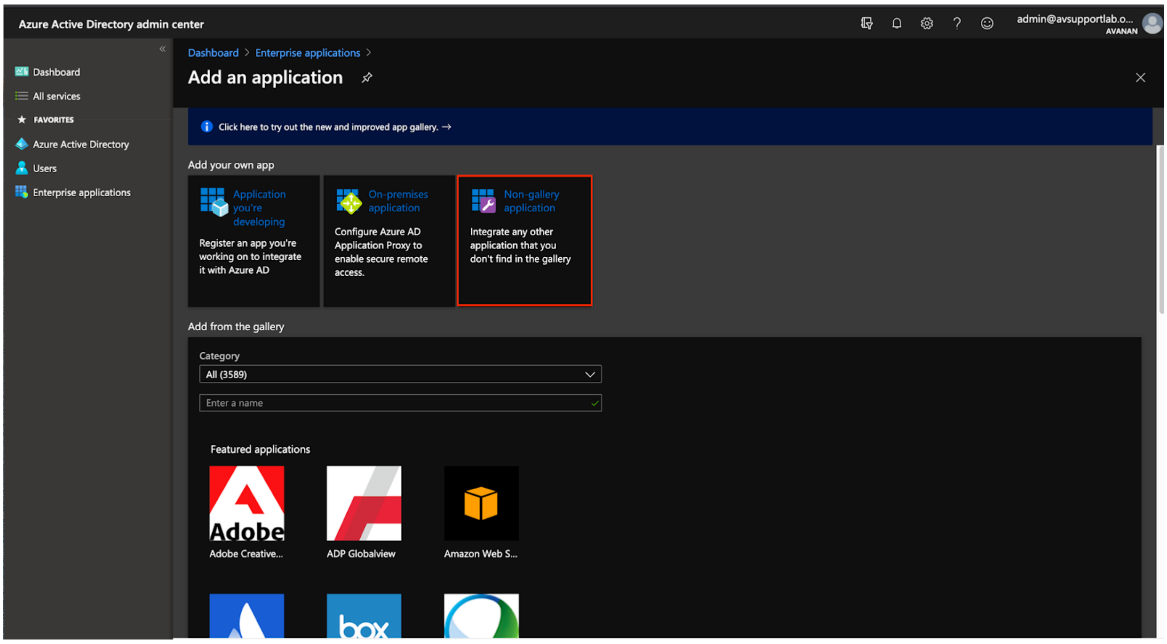
   c. To copy the ACS URL value, in the **ACS URL** field, click 📋.

   d. Click **Cancel**.

2. Sign in to the Microsoft Azure portal:

   a. Navigate to **Enterprise Applications** > **New Application**.

   b. Select **Non-gallery application**.



Azure Active Directory admin center

admin@avsupportlab.o... AVANAN

Dashboard > Enterprise applications >

Add an application

Click here to try out the new and improved app gallery. →

Add your own app

Application you're developing — Register an app you're working on to integrate it with Azure AD

On-premises application — Configure Azure AD Application Proxy to enable secure remote access.

Non-gallery application — Integrate any other application that you don't find in the gallery

Add from the gallery

Category: All (3589)

Enter a name

Featured applications

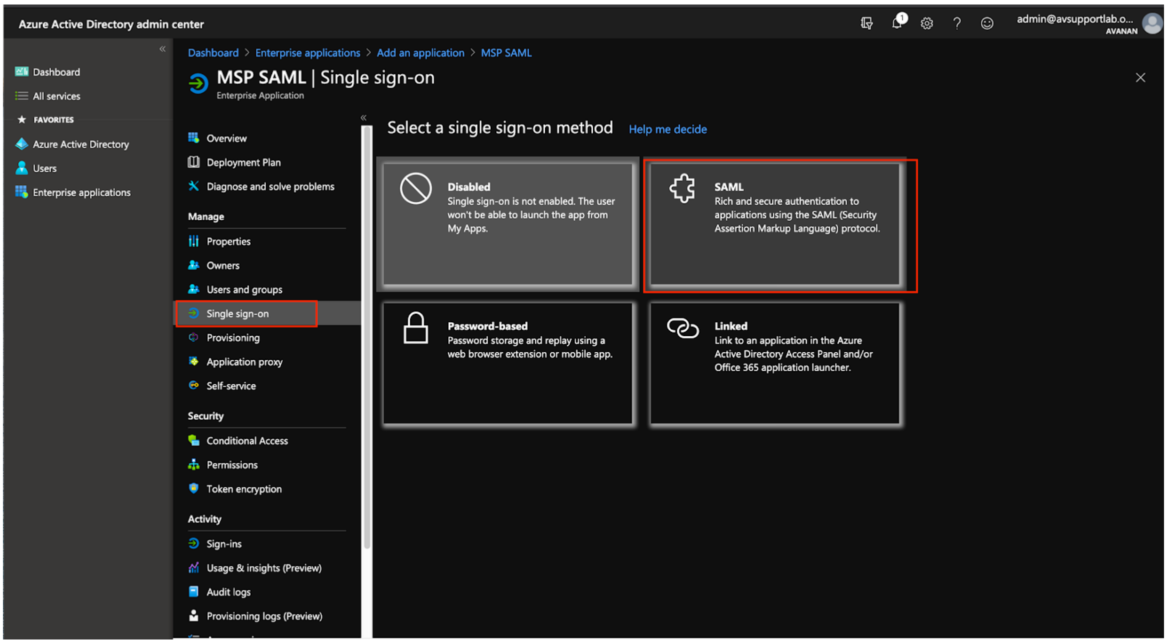
Adobe Creative... | ADP Globalview | Amazon Web S...

   c. In the **Enter a name** field, enter a name for the new application.

   d. Click **Add**.

   e. Go to **Manage** > **Single sign-on**.

   f. Select **SAML**.



Azure Active Directory admin center

admin@avsupportlab.o... AVANAN

Dashboard > Enterprise applications > Add an application > MSP SAML

MSP SAML | Single sign-on

Enterprise Application

Select a single sign-on method   Help me decide

Disabled — Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

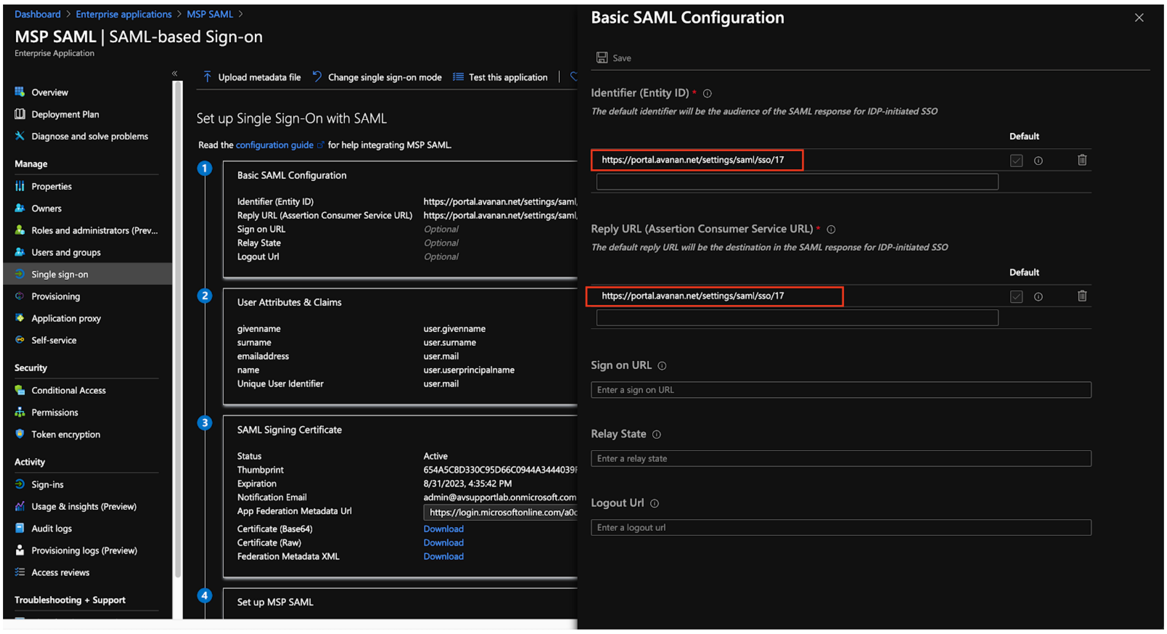
SAML — Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based — Password storage and replay using a web browser extension or mobile app.

Linked — Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

   g. In the **Basic SAML Configuration** section, click **Edit**.

h. In the **Identifier (Entity ID)** and **Reply URL (Assertion Consumer Service URL)** field, paste the ACS URL value copied in step **1.c**.



Set up Single Sign-On with SAML

Read the configuration guide for help integrating MSP SAML.

1 Basic SAML Configuration

Identifier (Entity ID)	https://portal.avanan.net/settings/saml
Reply URL (Assertion Consumer Service URL)	https://portal.avanan.net/settings/saml
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

2 User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.mail

3 SAML Signing Certificate

Status	Active
Thumbprint	654A5C8D330C95D66C0944A3444039F
Expiration	8/31/2023, 4:35:42 PM
Notification Email	admin@avsupportlab.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/a0c
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up MSP SAML

Basic SAML Configuration

Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

https://portal.avanan.net/settings/saml/sso/17

Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

https://portal.avanan.net/settings/saml/sso/17

Sign on URL

Enter a sign on URL

Relay State

Enter a relay state

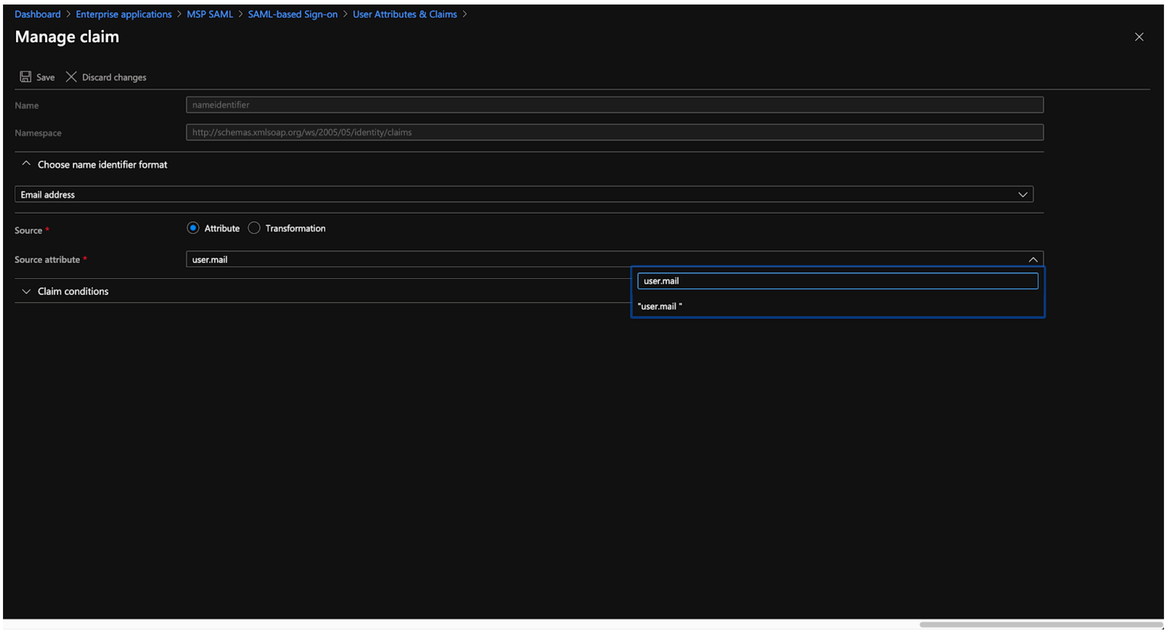
Logout Url

Enter a logout url

i. Click **Save**.

j. In the **User Attributes & Claims** section, click **Edit**.

The **Manage claims** page appears.


Dashboard > Enterprise applications > MSP SAML > SAML-based Sign-on > User Attributes & Claims >
Manage claim
Save
Discard changes
Choose name identifier format
Claim conditions

Name: nameidentifier

Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Email address

Source * ● Attribute ○ Transformation

Source attribute * user.mail

user.mail

"user.mail "

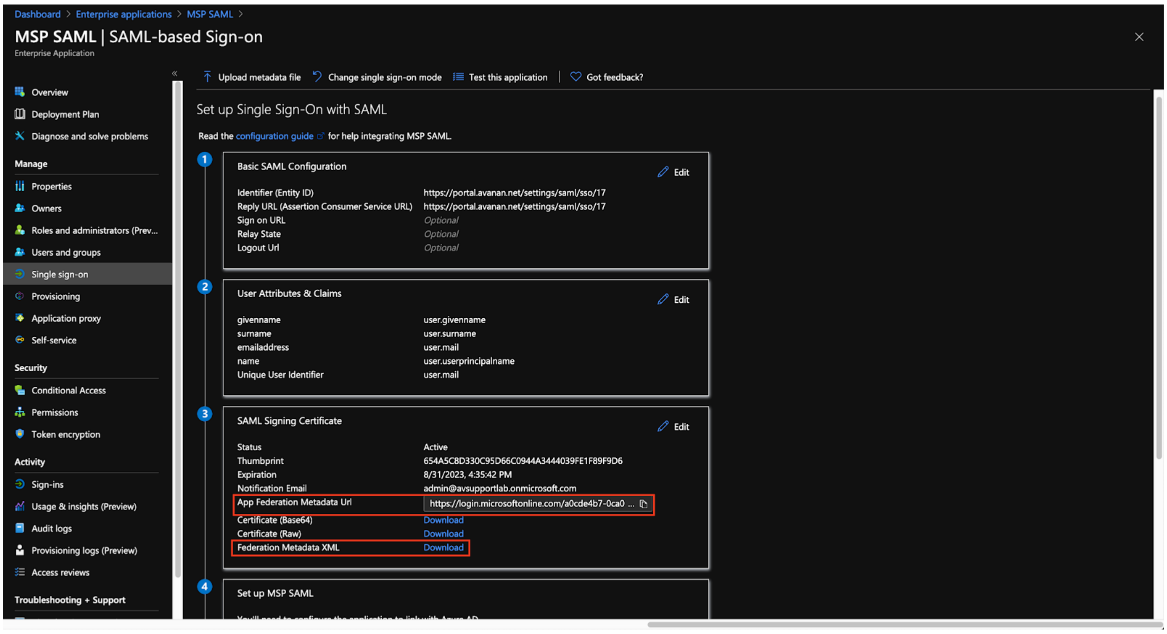
k. Expand **Choose name Identifier Format** and from the list, select **Email address**.

l. In the **Source** field, select **Attribute**.

m. From the **Source attribute** list, select **user.mail**.

n. Click **Save**.

o. In the **SAML Signing Certificate** section, do one of these:



Dashboard > Enterprise applications > MSP SAML >

MSP SAML | SAML-based Sign-on

Enterprise Application

Set up Single Sign-On with SAML

Read the configuration guide for help integrating MSP SAML.

1 Basic SAML Configuration

Identifier (Entity ID)	https://portal.avanan.net/settings/saml/sso/17
Reply URL (Assertion Consumer Service URL)	https://portal.avanan.net/settings/saml/sso/17
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

2 User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.mail

3 SAML Signing Certificate

Status	Active
Thumbprint	654A5C8D330C95D66C0944A3444039FE1F89F9D6
Expiration	8/31/2023, 4:35:42 PM
Notification Email	admin@avsupportlab.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/a0cde4b7-0ca0 ...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up MSP SAML

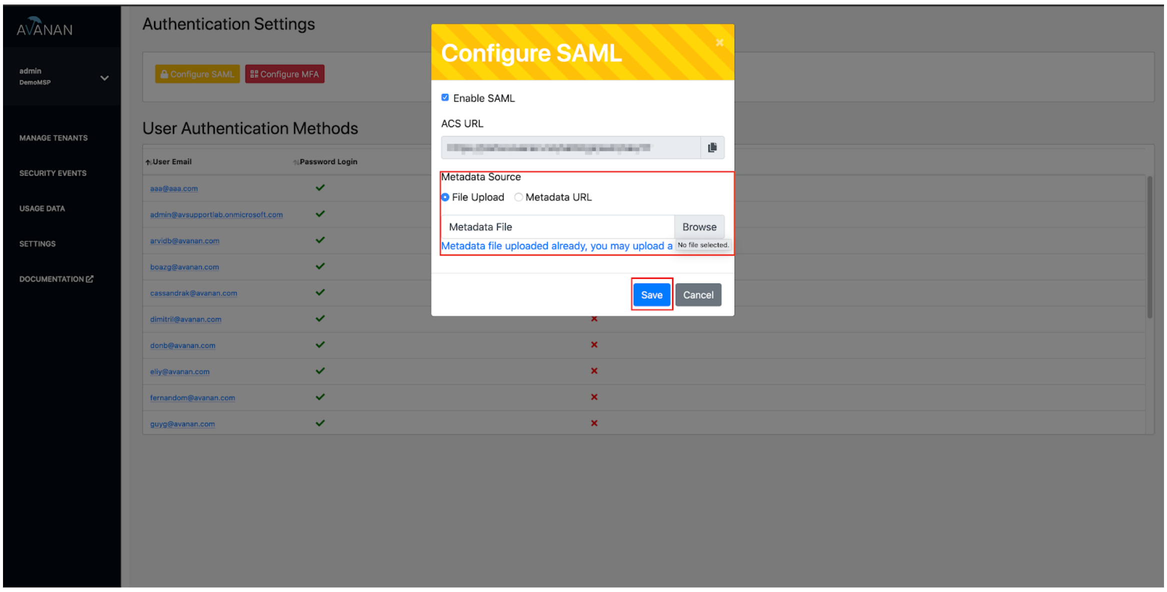
- In the **App Federation Metadata Url** field, click ⧉.
- In the **Federation Metadata XML** field, click **Download**.

3. Log in to the Avanan MSP Administrator Portal:

   a. Go to **Settings**.

   b. Expand **Authentication Settings** and click **Configure SAML**.

   The **Configure SAML** window appears.



User Email	Password Login	
aaa@aaa.com	✓	
admin@avsupportlab.onmicrosoft.com	✓	
arvidb@avanan.com	✓	
boazg@avanan.com	✓	
cassandrak@avanan.com	✓	
dimitril@avanan.com	✓	✗
donb@avanan.com	✓	✗
eliy@avanan.com	✓	✗
fernandom@avanan.com	✓	✗
guyg@avanan.com	✓	✗

Configure SAML

☑ Enable SAML

ACS URL

[redacted]

Metadata Source

● File Upload ○ Metadata URL

Metadata File

Metadata file uploaded already, you may upload a No file selected.

   c. Make sure the **Enable SAML** checkbox is selected.

d. In the **Metadata Source** section:

- To paste the Metadata url, select **Metadata URL** and paste the URL copied in step **2.o**.
- To upload the Metadata XML, select **File Upload** and upload the XML downloaded in step **2.o**.

e. Click **Save**.

Make sure to add users to the SAML application in your Microsoft Azure Portal and enable **SAML Login** under **User Authentication Methods** for the relevant users.

SAML SSO Integration with Okta

To configure Okta as SAML Provider for the Avanan MSP Administrator Portal:

1. Follow the instructions in Okta documentation portal.
2. The Okta configuration requires the ACS URL from the SAML Configuration window in the MSP portal, it also serve as the SP Entity ID.
3. Once you have configured the SSO application in Okta, copy the Identity Provider Metadata URL from Okta and paste it in the Metadata URL field of the SAML Configuration window in the MSP portal.
4. You can run the application from Okta directly from `https://{domain}.oktapreview.com/app/UserHome`

Tenant Videos

See Video Tutorials.

Check Point Copyright Notice