



## **MSSP 1.0.x User Guide**

---

Last Revised: April 30, 2021



# Table of Contents

<b>Welcome to the Tenable.io MSSP Portal</b> .....	<b>4</b>
<b>Get Started with the Tenable.io MSSP Portal</b> .....	<b>6</b>
Log in to the Tenable.io MSSP Portal .....	8
Tenable Licenses .....	9
Access the User Account Menu .....	10
My Account .....	11
Update Your User Account .....	12
Change Your Password .....	13
Configure Two-Factor Authentication .....	14
Generate Your API Keys .....	16
Access the Resource Center .....	17
Log out of the Tenable.io MSSP Portal .....	18
<b>Accounts</b> .....	<b>19</b>
<b>Users</b> .....	<b>20</b>
Create a Tenable.io MSSP Portal User .....	21
Edit a Tenable.io MSSP Portal User .....	23
Assist a Tenable.io MSSP Portal User with Their Account .....	24
Generate API Keys for another Tenable.io MSSP Portal User .....	25
Disable a Tenable.io MSSP Portal User .....	26
Enable a Tenable.io MSSP Portal User .....	27
Delete a Tenable.io MSSP Portal User .....	28
<b>Instances</b> .....	<b>30</b>



---

Use Single Sign-On to Access a Customer Instance .....	31
--	----



---

# Welcome to the Tenable.io MSSP Portal

---

The Tenable.io MSSP Portal 1.0.x provides secure and accessible ways for Managed Security Service Provider (MSSP) administrators to manage and maintain multiple customer instances of Tenable products in a single interface.

See [Get Started with the Tenable.io MSSP Portal](#) for more information.

## Managing Customer Accounts

Maintaining spreadsheets full of customer product data can be tedious, inaccurate, and difficult to track. The Tenable.io MSSP Portal features the default **Accounts** page, which displays all the Tenable.io customers that you maintain in one easily accessible location. In the Tenable.io MSSP Portal, you can add Tenable.io instances, view relevant customer information about the instances, and add customized notes that include valuable internal tracking or customer contact information. For more information, see [Accounts](#).

## Single Sign on to a Customer Tenable.io Instance

Tenable recognizes that each Tenable.io customer instance needs unique login credentials for security. Maintaining these credentials in spreadsheets can be difficult and unsafe. Using the Tenable.io MSSP Portal's Single Sign-on feature, you can access any customer's Tenable.io instance and navigate the user interface with your assigned permissions. When finished, you can then seamlessly pivot back to the Tenable.io MSSP Portal. This approach allows you to sign in once to the Tenable.io MSSP Portal and administer separate customer accounts and instances. For more information, see [Instances](#).

## Other Tenable.io Products

### Tenable.io Vulnerability Management

[See the User Guide](#)

Tenable.io® allows security and audit teams to share multiple Nessus, Nessus Agent, and Nessus Network Monitor scanners, scan schedules, scan policies and scan results among an unlimited set of users or groups. By making different resources available for sharing among users and groups, Tenable.io provides endless possibilities for creating customized workflows for vulnerability management



programs, regardless of any of the numerous regulatory or compliance drivers that demand keeping your business secure.

Tenable.io can schedule scans, push policies, view scan findings, and control multiple Nessus scanners from the cloud. This enables the deployment of Nessus scanners throughout networks to both public and private clouds as well as multiple physical locations.

## **Tenable.io API**

[See the API](#)

The Tenable.io API can be leveraged to develop your own applications using various features of the Tenable.io platform, including scanning, creating policies, and user management.

## **Tenable.io Container Security**

[See the User Guide](#)

Tenable.io Container Security stores and scans container images as the images are built, before production. It provides vulnerability and malware detection, along with continuous monitoring of container images. By integrating with the continuous integration and continuous deployment (CI/CD) systems that build container images, Tenable.io Container Security ensures every container reaching production is secure and compliant with enterprise policy.

## **Tenable.io Web Application Scanning**

[See the User Guide](#)

Tenable.io Web Application Scanning offers significant improvements over the existing **Web Application Tests** policy template provided by the Nessus scanner, which is incompatible with modern web applications that rely on Javascript and are built on HTML5. This leaves you with an incomplete understanding of your web application security posture.

Tenable.io Web Application Scanning provides comprehensive vulnerability scanning for modern web applications. Tenable.io Web Application Scanning's accurate vulnerability coverage minimizes false positives and false negatives, ensuring that security teams understand the true security risks in their web applications. The product offers safe external scanning that ensures production web applications are not disrupted or delayed, including those built using HTML5 and AJAX frameworks.



---

# Get Started with the Tenable.io MSSP Portal

---

Use the following getting started sequence to configure and mature your Tenable.io MSSP Portal deployment.

1. [Prepare](#)
2. [Create Tenable.io MSSP Portal Users](#)
3. [Configure Tenable.io MSSP Portal Customer Accounts](#)
4. [Use Single Sign-On to Access a Customer Tenable.io Instance](#)

## Prepare

Before you begin, prepare your use case for the Tenable.io MSSP Portal.

To plan your use case for the Tenable.io MSSP Portal:

1. Get your Tenable.io MSSP Portal access information and starter account credentials from your Tenable representative.
2. Identify the users in your organization that you want to have access to the Tenable.io MSSP Portal, and gather appropriate information (e.g., email address, appropriate user permissions).
3. Compile a list of Tenable.io customer accounts you want to monitor through the Tenable.io MSSP Portal, and gather appropriate information (e.g., email address, company name, and address).

## Create Tenable.io MSSP Portal Users

[Create](#) users for any administrators you want to have access to the Tenable.io MSSP Portal.

## Configure Tenable.io MSSP Portal Customer Accounts

Configure accounts for the customers you want to monitor through the Tenable.io MSSP Portal.

## Use Single Sign-On to Access a Customer Tenable.io Instance



[Use](#) the Tenable.io MSSP Portal's single sign-on capabilities to access the Tenable.io instances associated with your configured customer accounts.



# Log in to the Tenable.io MSSP Portal

**Required User Role:** Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

Before you begin:

- Obtain credentials for your Tenable.io MSSP Portal account.

**Note:** If you are logging in to the Tenable.io MSSP Portal for the first time, click **Forgot Password**. You are directed to reset the password for the account.

- Review the [Tenable.io System Requirements](#) in the *General Requirements User Guide* and confirm that your computer and browser meet the requirements.

To log in to the Tenable.io MSSP Portal:

1. In a supported browser, navigate to <https://cloud.tenable.com>.

The Tenable.io login page appears.

2. In the username box, type your username.
3. In the password box, type your password.
4. (Optional) To remain logged in until you sign out or close the browser, select the **Remember Me** check box. Otherwise, the Tenable.io MSSP Portal logs you out after a period of inactivity.
5. Click **Sign In**.

The Tenable.io MSSP Portal appears. By default, the portal displays the [Accounts](#) page.





## Tenable Licenses

---

When you use the Tenable.io MSSP Portal to access a customer's Tenable.io instance, the customer's Tenable.io licenses apply, as described in the following:

- [Tenable.io Vulnerability Management Licensing](#)



---

## Access the User Account Menu

---

**Required User Role:** Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

To access the user account menu in the Tenable.io MSSP Portal:

1. In the upper-right corner, click the  button.

The user account menu appears.

2. Do one of the following:
  - Click **My Account** to make changes to your own user account.
  - [Log out](#) of Tenable.io.



---

# My Account

---

From the **My Account** page, you can make changes to your own user account.

For more information, see the following topics:

- [Update Your User Account](#)
- [Change Your Password](#)
- [Configure Two-Factor Authentication](#)
- [Generate Your API Keys](#)



# Update Your User Account

**Required User Role:** Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

To update your user account in the Tenable.io MSSP Portal:

1. In the upper-right corner, click the  button.

The user account menu appears.

2. Click **My Account**.

The **My Account** page appears.

3. (Optional) Make any of the following changes:

- Edit your **Name**.
- Edit your **Email**.
- [Change](#) your password.

4. Click **Save**.

5. (Optional) [Configure](#) two-factor authentication.

6. (Optional) [Generate](#) API keys.



# Change Your Password

**Required User Role:** Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

**Note:** To change another user's password, see [Edit a Tenable.io MSSP Portal User](#).

To change your password in the Tenable.io MSSP Portal:

1. In the upper-right corner, click the  button.

The user account menu appears.

2. Click **My Account**.

The **My Account** page appears.

3. In the **Current Password** box, type your current password.

4. In the **New Password** box, type a new password.

**Note:** Passwords must be at least 12 characters long and contain the following:

- An uppercase letter
- A lowercase letter
- A number
- A special character

5. Click the **Save** button.

The Tenable.io MSSP Portal saves the new password.



# Configure Two-Factor Authentication

**Required User Role:** Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

You can configure two-factor authentication for your user account. Administrators cannot configure two-factor authentication for other users.

To add or modify two-factor authentication in the Tenable.io MSSP Portal:

1. In the upper-right corner, click the  button.

The user account menu appears.

2. Click **My Account**.

The **My Account** page appears.

3. Under **Enable Two Factor Authentication**:

- If you are enabling two-factor authentication for the first time, click **Enable**.
- If you are modifying an existing configuration, click **Edit**.

The **Two-Factor Setup** plane appears.

4. Type your mobile phone number in the box.

5. Click **Next**.

The **Verification Code** screen appears and the Tenable.io MSSP Portal sends a text message with a verification code to the phone number.

6. (Optional) If you have not received the verification code after several minutes, click **Resend Code**.

7. Type the verification code in the box.

8. Click **Next**.

The Tenable.io MSSP Portal displays a success message confirming that you have configured two-factor authentication

for your account.



9. (Optional) To configure whether the Tenable.io MSSP Portal sends a verification code to the email associated with your user account:
  - a. Select or clear the **Send backup email** check box.
  - b. Click **Save**.

The Tenable.io MSSP Portal updates your backup email settings.

## To disable two-factor authentication in the Tenable.io MSSP Portal:

1. In the upper-right corner, click the  button.

The user account menu appears.

2. Click **My Account**.

The **My Account** page appears.

3. Under **Enable Two Factor Authentication**, click **Disable**.

The **Disable Two-Factor** window appears and a warning message indicates that if you disable this feature for the account, the Tenable.io MSSP Portal deletes the mobile phone number and other settings associated with the feature.

4. Read the warning message, then click **Continue**.

The Tenable.io MSSP Portal disables two-factor authentication for your account.



# Generate Your API Keys

**Required User Role:** Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

API keys generated in the Tenable.io MSSP Portal can access the portal only, and cannot access any of the customer Tenable.io instances.

**Note:** Tenable.io API Access and Secret keys are required to use the [Tenable.io API](#).

For information on generating API keys for another user, see [Generate API Keys for another Tenable.io MSSP Portal User](#).

To generate API keys for your own account in the Tenable.io MSSP Portal:

1. In the upper-right corner, click the  button.

The user account menu appears.

2. Click **My Account**.

The **My Account** page appears.

3. Click the **API Keys** tab.

The **API Keys** section appears.

4. Click **Generate**.

The **Generate API Keys** window appears with a warning.

**Caution:** Any existing API keys are replaced when you click the **Generate** button. You must update the applications where the previous API keys were used.

5. Review the warning and click **Generate**.

The Tenable.io MSSP Portal generates access and secret keys for the account. These keys must be used to authenticate with the Tenable.io MSSP Portal REST API.

**Caution:** After you generate your API keys, copy and save the key to a safe location. Without saving the keys, you cannot retrieve the keys from Tenable.io.





---

## Access the Resource Center

---

**Required User Role:** Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

The **Resource Center** displays a list of (missing or bad snippet) informational resources including product announcements, Tenable blog posts, and Tenable.io user guide documentation.

To access the Resource Center:

1. In the upper-right corner, click the button.

The **Resource Center** menu appears.

2. Click a resource link to navigate to that resource.



## Log out of the Tenable.io MSSP Portal

**Required User Role:** Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

To log out of the Tenable.io MSSP Portal:

1. In the upper-right corner, click the  button.

The user account menu appears.

2. Click **Sign Out**.




---

# Accounts

---

The **Accounts** page in the Tenable.io MSSP Portal is the main dashboard through which you can view and manage your MSSP customer accounts.

On the **Accounts** page, you can do the following:

- Use the **Search** box to filter the customer accounts in the table:
  1. In the **Search** box, type your search based on one of the following criteria:
    - **Customer Name**
    - **Licensed Apps**
    - **Site Identifier**
    - **Notes**
  2. Click the  button.

The Tenable.io MSSP Portal filters the table by your search criteria.

- [Use Single Sign-On to Access a Customer Instance](#)
- Assign a Logo to an Account
- Remove a Logo from an Account
- Edit an Account



# Users

---

In the Tenable.io MSSP Portal, you can manage access to the portal for users from your organization.

To access the **Users** page in the Tenable.io MSSP Portal, in the left navigation plane, click **Users**.

The **Users** page displays a table of all Tenable.io MSSP Portal users. This documentation refers to that table as the *users table*.

Each row of the users table includes the username, the dates of the last login and last failed login attempt, the total number of failed attempts, and the role assigned to the account.

On the **Users** page, you can do the following:

- [Create a Tenable.io MSSP Portal User](#)
- Assign a Tenable.io MSSP Portal User to an Account
- Remove a Tenable.io MSSP Portal User from an Account
- [Edit a Tenable.io MSSP Portal User](#)
- [Assist a Tenable.io MSSP Portal User with Their Account](#)
- [Generate API Keys for another Tenable.io MSSP Portal User](#)
- [Disable a Tenable.io MSSP Portal User](#)
- [Enable a Tenable.io MSSP Portal User](#)
- [Delete a Tenable.io MSSP Portal User](#)



# Create a Tenable.io MSSP Portal User

**Required User Role:** Administrator

A Tenable.io MSSP Portal user can manage customer accounts and access Tenable.io customer instances.

To create a user in the Tenable.io MSSP Portal:

1. In the upper left corner, click the ☰ button.

The left navigation plane appears.

2. In the left navigation plane, click **Users**.

The **Users** page appears.

3. In the top right corner of the page, click the ⊕ **Create User** button.

The **Create User** plane appears.

4. In the **Full Name** box, type the full name of the user.

5. In the **Username** box, type a valid username. A valid username must be in the format, *name@domain*, where *domain* corresponds to a domain approved for your Tenable.io MSSP Portal instance.

**Note:** During initial setup, Tenable configures approved domains for your Tenable.io MSSP Portal instance. To add domains to your instance, contact Tenable Support.

6. (Optional) In the **Email** box, type the email address of the user.

7. In the **Password** box, type a password.

**Note:** Passwords must be at least 8 characters long and contain at least three of the following:

- An uppercase letter
- A lowercase letter
- A number
- A special character



8. In the **Role** drop-down box, select the role that you want to assign to the user.

**Tip:** For more information on role permissions, click [View guide to Role Permissions](#). The **Role Permissions** plane appears.

9. Click **Create**.

The Tenable.io MSSP Portal saves the user . The **Users** page appears, where you can view the new user listed in the users table.



## Edit a Tenable.io MSSP Portal User

**Required User Role:** Administrator

To edit a user in the Tenable.io MSSP Portal:

1. In the upper left corner, click the ☰ button.

The left navigation plane appears.

2. In the left navigation plane, click **Users**.

The **Users** page appears.

3. In the table, click the name of the user you want to edit.

The **Edit User** page appears.

4. (Optional) Edit the user **Full Name**, **Email**, **Password**, and/or **Role**.

5. (Optional) [Generate](#) API keys for the user.

6. Click **Save**.

The Tenable.io MSSP Portal saves the changes to the user.



## Assist a Tenable.io MSSP Portal User with Their Account

**Required User Role:** Administrator

As an administrator, you can use the user assist functionality to simulate being logged in as another account. While assisting a user account, you can perform operations in the Tenable.io MSSP Portal as that user without needing to obtain their password or having to log out of your administrator account.

To assist a user with their account in the Tenable.io MSSP Portal:

1. In the upper left corner, click the  button.

The left navigation plane appears.

2. In the left navigation plane, click **Users**.

The **Users** page appears.


3. In the users table, roll over the user you want to assist.

The action buttons appear at the end of the row.

4. In the row, click the  button.

The Tenable.io MSSP Portal refreshes and displays the default MSSP **Accounts** page. While you are assisting the user, the Tenable.io MSSP Portal displays a blue overlay at the top of each page with the role of the user you are assisting.

To stop assisting a user with their account:

- At the top of any page, in the overlay that displays the role of the user account you are assisting, click the  button.





## Generate API Keys for another Tenable.io MSSP Portal User

**Required User Role:** Administrator

Administrators can generate API keys for any MSSP user.

To generate API keys for another user in the Tenable.io MSSP Portal:

1. [Edit](#) a user.

The **Edit User** plane appears.

2. In the **API Keys** section, click **Generate API Keys**.

**Caution:** Any existing API keys are replaced when you generate new API keys. You must update the applications where the previous API keys were used.

3. Review the warning and click **Replace & Generate**.

Tenable.io generates access and secret keys for the account. These keys must be used to authenticate with the Tenable.io MSSP Portal REST API.



# Disable a Tenable.io MSSP Portal User

**Required User Role:** Administrator

Disabling a user account prevents the user from logging in to the Tenable.io MSSP Portal. You can enable a disabled user account as described in [Enable a Tenable.io MSSP Portal User](#).

To disable a user in the Tenable.io MSSP Portal:

1. In the upper left corner, click the ☰ button.

The left navigation plane appears.

2. In the left navigation plane, click **Users**.

The **Users** page appears.

3. On the **Users** page, in the users table, roll over the user you want to edit.

The action buttons appear at the end of the row.

4. In the row, click the ⓧ button.

The **Disable User** window appears and prompts you to confirm that you want to disable the selected user.

5. To confirm, click **Disable**.

6. Click **Continue**.

A success message appears.

The Tenable.io MSSP Portal disables the user account and tags it as **Disabled** in the users table.

**Note:** If the user being disabled has a session in progress, they may continue to have limited access. However, once they log out, they cannot log back in.



## Enable a Tenable.io MSSP Portal User

**Required User Role:** Administrator

If you [disable](#) a user, you can enable an account again to restore a user's access.

To enable a user in the Tenable.io MSSP Portal:

1. In the upper left corner, click the ☰ button.

The left navigation plane appears.

2. In the left navigation plane, click **Users**.

The **Users** page appears.

3. On the **Users** page, in the table, roll over the user you want to enable.

The action buttons appear at the end of the row.

4. In the row, click the ✓ button.

The **Enable User** window appears and prompts you to confirm that you want to enable the selected user.

5. To confirm, click **Enable**.

6. Click **Continue**.

A success message appears.

The Tenable.io MSSP Portal enables the user account.



## Delete a Tenable.io MSSP Portal User

**Required User Role:** Administrator

Before you delete a user account, you must first [disable](#) the user account.

**Caution:** Once you delete a user account, the account cannot be recovered and the action cannot be reversed.

The following table describes what objects are migrated, retained, or permanently deleted upon user deletion:

Object Type	Deleted	Notes
Scan Schedules	No	Migrated to the new object owner
Historical Scan Results	No	Migrated to the new object owner
Scan Templates	No	Migrated to the new object owner
Custom Dashboards/Widgets	Yes	Permanently deleted
Managed Credentials	No	Retained ( <b>Created By</b> value displays as <b>null</b> )
Tags	No	Retained ( <b>Created By</b> value displays as <b>null</b> )
Recast/Accept Rules	No	Retained ( <b>Owner</b> value displays as <b>Unknown User</b> )
Exclusions	No	Retained
System Target Groups	No	Retained
User Target Groups	Yes	Permanently deleted
Saved Searches	Yes	Permanently deleted
Connectors	No	Retained
Sensors	No	Retained

To delete a user account in the new interface:



1. In the upper-left corner, click the ☰ button.

The left navigation plane appears.

2. (missing or bad snippet)

3. Click the **Users** tile.

The **Users** page appears. This page contains a table that lists all users for your MSSP instance.

In the users table, roll over the user account you want to delete.

4. (missing or bad snippet)

5. In the row, click the 🗑 button.

**Note:** If a user is not disabled, then the 🗑 button does not appear. [Disable](#) the user before deleting them.

The **Delete User** page appears.

6. In the **Transfer User Objects** section, from the **Select New Object Owner** drop-down box, select the user to which you want to transfer any of the user's objects (e.g., scans, user-defined templates).

7. Click 🗑 **Delete**.

A confirmation message appears.

8. Click **Delete**.

MSSP deletes the user and transfers any user objects to the user you designated.



---

## Instances

---

In the Tenable.io MSSP Portal, you can use single sign-on capabilities to access the Tenable.io instances associated with your configured customer accounts.


You can access the Tenable.io MSSP Portal single sign-on capabilities via the [Accounts](#) page. For more information, see [Use Single Sign-On to Access a Customer Instance](#).



## Use Single Sign-On to Access a Customer Instance

**Required User Role:** Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

To sign in to a customer's Tenable.io instance in the Tenable.io MSSP Portal:

1. On the **Accounts** page, in the table, roll over the customer account where you want to sign in.  
The action buttons appear at the end of the row.
2. In the row, click the  button.

The Tenable.io MSSP Portal loads the appropriate Tenable.io interface according to the customer's licenses. For example, if the account is licensed for Tenable.io Web Application Scanning only, the Tenable.io Web Application Scanning interface appears.


Additionally, a blue MSSP overlay appears along the outside edges of the page. This indicates that you are actively signed in to that instance of Tenable.io as a user.

**Note:** When you sign in to a customer's Tenable.io instance, you retain the permissions assigned to you in the Tenable.io MSSP Portal.

For more information about navigating Tenable.io interfaces, see the following documentation:

- [Tenable.io Vulnerability Management User Guide](#)
- [Tenable.io Container Security User Guide](#)
- [Tenable.io Web Application Scanning User Guide](#)

To return to the Tenable.io MSSP Portal:

- From the new Tenable.io interface:
  1. At the top of any page, in the blue MSSP overlay, click .

The Tenable.io MSSP Portal appears.



- From the classic Tenable.io interface:
  1. In the upper-right corner of the top navigation bar, click the Tenable.io username.
  2. Click **Leave User**.

The Tenable.io MSSP Portal appears.