INFORME DE ACTIVIDADES No. 1

Tipo de Informe: Final [X] Parcial [ ]	Pago No: [1] de [1]

Número del contrato: 217 del 2023	**Fecha del contrato:** 19 SEPTIEMBRE 2023	**Fecha de Iniciación:** 21 SEPTIEMBRE 2023	**Fecha de Terminación:** 29 DICIEMBRE DEL 2023
Nombre del Contratista: 2 SECURE S.A.S			
Objeto del contrato ADQUISICION DE UNA HERRAMIENTA DE ANALISIS DE VULNERABILIDADES POR EL PERIODO DE UN AÑO, PARA LA COMISION DE REGULACION DE AGUA POTABLE Y SANEAMIENTO BASICO - CRA, INCLUIDOS LOS SERVICIOS DE SOPORTE TÉCNICO, MANTENIMIENTO CONFIGURACIÓN Y AFINAMIENTO.			
Nombre del Supervisor: JUAN CARLOS VILLALBA CARDENAS		**Cargo del Supervisor:** PROFESIONAL ESPECIALIZADO	**Dependencia:** OFICINA ASESORA DE PLANEACION Y TIC
Valor del contrato: $16.869.530,94		**Certificado de disponibilidad presupuestal No. 35523, 4 SEPTIEMBRE 2023**	**Registro Presupuestal No. 61323, 19 SEPTIEMBRE 2023**

Obligaciones / Productos programados (según contrato, cronograma y/o asignaciones)	**Actividades / Productos desarrollados frente a lo programado**
El proponente deberá estar en capacidad, y en caso de ser seleccionado, de cumplir con las siguientes obligaciones: 1) Entregar suscripción de la herramienta de análisis de vulnerabilidades vigencia de mínimo un (1 año), para 85 Host. 2) Realizar la configuración y puesta funcionamiento de la herramienta de análisis de vulnerabilidades y del soporte técnico especializado, conforme a las indicaciones de la supervisión del contrato. Incluida prestación de servicios conexos, práctica de pruebas funcionales y técnicas, y verificación de correcto funcionamiento. 3) Realizar transferencia de conocimiento y documentación asociada a la instalación y uso de la herramienta según personalización para la CRA, para un total de mínimo de 12 Hrs. 4) Entregar documento que acredite titularidad y soporte técnico especializado por parte del fabricante, y en caso de aplicar, entregar los medios magnéticos y documentos técnicos respectivos. 5) Suministrar el personal idóneo y debidamente capacitado, para la ejecución de las actividades requeridas tanto	Se recibe suscripción de herramienta de vulnerabilidades para 85 hosts, así como demás condiciones técnicas del contrato. Manuales actualizados: https://docs.tenable.com/vulnerability-management.htm

técnicas como funcionales, sin importar el número de profesionales que se requieran.

6) Entregar GARANTIA, por un (1 año), así:
   a) Garantía suministrada directamente por el fabricante de la solución, sin costo adicional para la CRA.
   b) Incluye soporte técnico y mantenimiento.

7) SOPORTE TÉCNICO Y MANTENIMIENTO,

   a) Soporte técnico por medio de línea de contacto telefónico, correo electrónico, con SLA con las siguientes prioridades: Prioridad 1-Criticas: < 2 hr, Prioridad 2- Alta: < 4 hr, Prioridad 3-Medio: < 12 hr, P4-Informativas: < 24 hr.
   b) Asistencia remota para soporte telefónico, o en caso de requerirse, asistencia en sitio con el fabricante 24*7 e integrador 8*5.
   c) Actualizaciones de software por la vigencia de la renovación, a versiones mayores (upgrades) y mejoras (updates).
   d) La línea de contacto, debe permitir la apertura de tickets tanto de mantenimiento preventivo como correctivo, y el reporte de las posibles fallas que presenten, remplazo, actualizaciones, entre otras.
   e) Se entenderá como falla el inadecuado funcionamiento del bien o servicio adquirido.

8) PROCEDIMIENTO DETECCION FALLAS: Ante cualquier falla, el proveedor debe adelantar como mínimo las siguientes actividades:

a) Un diagnóstico inicial por medio de una conexión remota.
b) El ingeniero de soporte a cargo del caso debe realizar todo el protocolo de pruebas necesario para validar cuál es el origen de la falla reportada y si es posible proceder a dar solución de manera remota.
c) Brindar soporte en sitio si las condiciones lo ameritan, con la finalidad de garantizar la adecuada y normal operación de la plataforma instalada

JUAN CARLOS VILLALBA C.

JUAN CARLOS VILLALBA CARDENAS
Supervisor

INFORME DE SEGUIMIENTO TÉCNICO ADMINISTRATIVO Y FINANCIERO SUPERVISIÓN E INTERVENTORÍA:

En calidad de supervisor del contrato anotado, manifiesto que el Contratista ha cumplido a satisfacción y dentro de los términos contractuales con todas las obligaciones establecidas de acuerdo al siguiente cuadro – informe:

Aspectos de supervisión	No. de informe (s)	1	2	3	4	5	6	7	8	9	10	11	12
Aspecto técnico	Porcentaje de avance físico (entrega bienes, suministros o servicios prestados) (De 0 a 100%)	100%											
	No. de Pago (s)	1	2	3	4	5	6	7	8	9	10	11	12
Aspecto Financiero	Porcentaje de Ejecución Financiera (de 0 a 100%)	100%											
	Pagos	1	2	3	4	5	6	7	8	9	10	11	12
	Pagos frente al valor Total	$16.869.530,94											
	Valor a pagar					$16.869.530,03							
	Valor total ejecutado					$16.869.530,94							
	Saldo pendiente por ejecutar					0.91							
Fecha de Informe						8 Noviembre 2023							

Igualmente, certifico que el Contratista acreditó los pagos relacionados con aportes al Régimen de Seguridad Social integral.

*Certificación Representante Legal o Revisor Fiscal (personas Jurídicas) SI _X_ NO ____
*Planilla de aportes pagada mes de: Octubre 2023

Por lo anterior, se puede proceder a efectuar el pago correspondiente, conforme se señala en la cláusula de valor y forma de pago del contrato.

JUAN CARLOS VILLALBA C.

JUAN CARLOS VILLALBA CARDENAS
Supervisor

CUFE: 7bdb2a16c2cca7edaf1a4b843926756080b47ab5b287f960b115d5ba6aaf384d3749662b260d42eeaed32929fe133f30--Expedición:03/11/2023 04:41 PM

Inspiring Security

Documento Oficial de Autorización de Numeración Facturación Electrónica No. 18764040601860 que habilita desde 2SE 1001 hasta 2SE 5000. Vence 2023-12-01

Fecha Resolución: 01/12/2022

Actividad principal 6202. Tarifa 6.9 por mil

Bogotá D.C. Cr 11A 144-36 Of 301E (+57)1 7357655/ 3585415

www.2secure.co

2SECURE SAS

Nit 900372621 - 4

IVA Régimen Común

CLIENTE: COMISION DE REGULACION DE AGUA POTABLE Y SANEAMIENTO BASICO
NIT: 830000212 6
DIRECCION: CR 12 97 80 P 2 Bogota D.C.
TELEFONO: 4373820
FORMA DE PAGO: CREDITO 30 DIAS

Factura Electrónica de Venta No. 2SE 1652

FECHA FACTURA 03 de noviembre de 2023
FECHA VENCIMIENTO 03 de diciembre de 2023

Código		Item	Cant.	Valor Unitario	IVA %	Valor IVA	Total Renglón
LICEN	LICENCIA SUSCRIPCION LICENCIAMIENTO TENABLE IO - 85 LICENCIAS (1 AÑO) - SOPORTE ADVANCE TENABLE	1	1,00	13.731.794	0,00%	0	13.731.793,90
1006 3	HORAS CONSULTORIA SERVICIO DE IMPLEMENTACIÓN Y TRANSFERENCIA DE CONOCIMIENTO 12 HORAS	2	1,00	2.636.753	19,00%	500.983	2.636.753,05

Total Items 2

Valor en Letras

DIECISEIS MILLONES CIENTO OCHENTA Y TRES MIL SEISCIENTOS OCHENTA Y OCHO PESOS M/CTE

Lugar de prestación del servicio o compra: BOGOTÁ D.C.

SUBTOTAL	**16.368.546,95**
IVA	**500.983,08**
RETEFUENTE	572.899
RETEIVA	0
RETEICA	112.943
TOTAL FACTURA	**16.183.687,90**

OBSERVACIONES:

FAVOR HACER RETENCIÓN EN LA FUENTE DEL 3.5%. DECRETO 2499 DE 06/12/2012

NOTA IMPORTANTE

FAVOR CONSIGNAR EN BANCO DAVIVIENDA A LA CUENTA DE AHORROS No.006270560599 A NOMBRE DE 2SECURE S.A.S. La no cancelación al vencimiento causa interés a la tasa máxima legal vigente.

Fecha y Hora de Registro: 03/11/2023 16:26:37

CERTIFICACIÓN APORTES PARAFISCALES

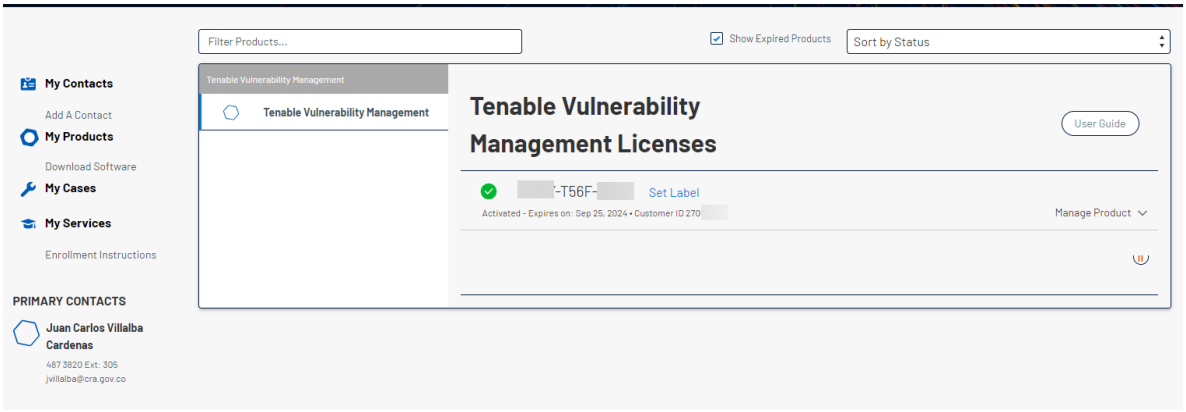
En mi calidad de revisor fiscal de la sociedad 2SECURE S.A.S., identificada con NIT 900.372.621-4, he efectuado los procedimientos de revisión, con el propósito de verificar el pago efectuado por la Compañía por concepto de aportes a los sistemas de salud, pensiones y riesgos profesionales y a las cajas de compensación familiar, Instituto Colombiano de Bienestar Familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA), durante el período de seis (6) meses, comprendido entre el 1 de mayo y el 31 de octubre del año 2023. El pago de dichos aportes es responsabilidad de la Administración de la Compañía como parte de su gestión. Mi responsabilidad de acuerdo con lo establecido en el artículo 50 de la Ley 789 del 27 de diciembre de 2002, es emitir un informe, certificando el cumplimiento de tales obligaciones.

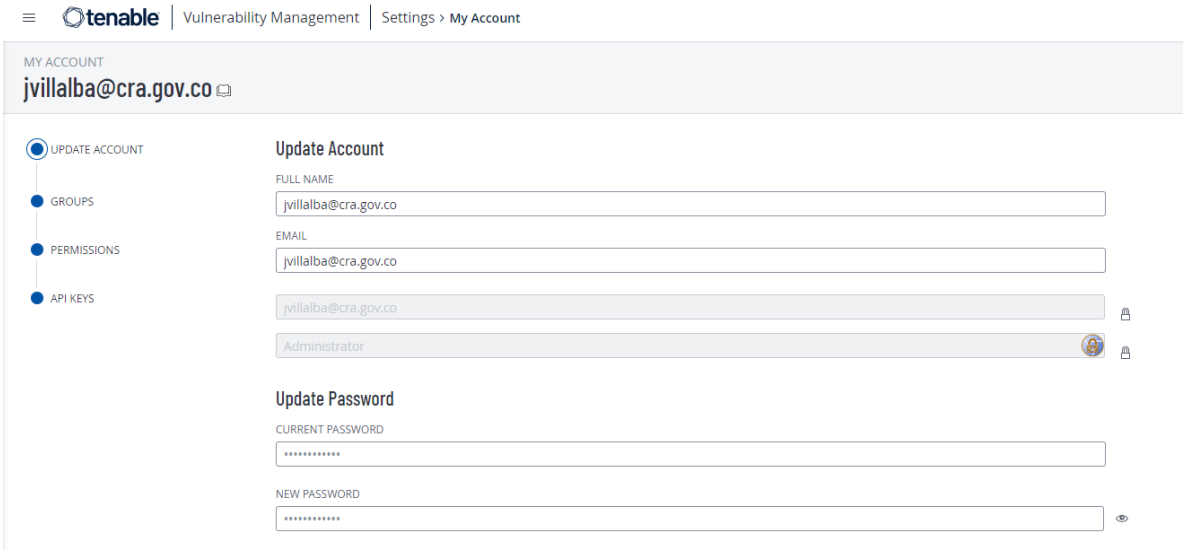
Con base en el resultado de mi revisión, certifico que la Compañía durante el período comprendido descrito en párrafo anterior, pagó los aportes a los sistemas de salud, pensiones y riesgos profesionales y a las cajas de compensación familiar. Instituto Colombiano de Bienestar Familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA).”

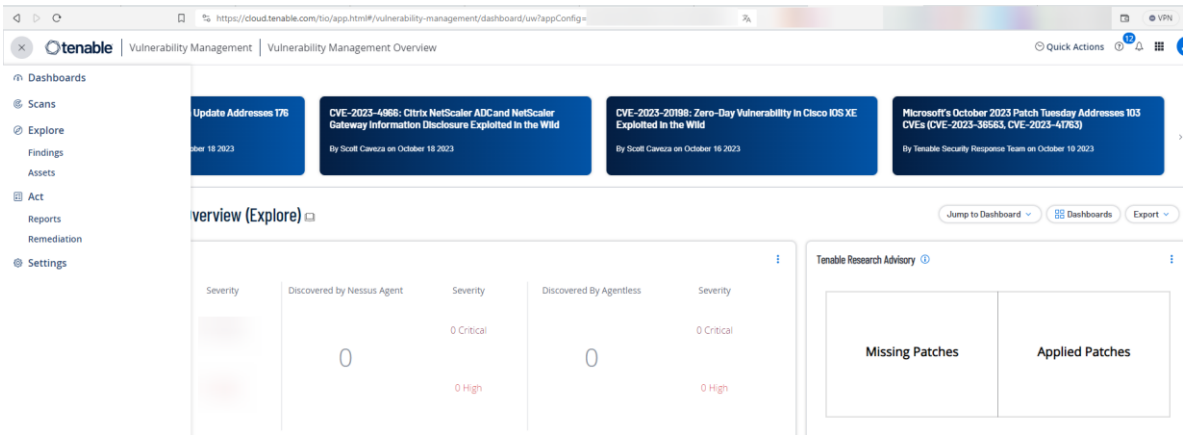
La presente certificación, es para uso exclusivo de la administración de la Compañía dentro del proceso de licitación y no debe ser utilizado para ningún otro propósito. Se expide a los 6 días del mes de octubre del año 2023, en Bogotá D.C.

Cordialmente,

Marlon Pardo Villalba
Revisor Fiscal Principal
Tarjeta Profesional 42648-T
Designado por GP&A SAS (TR 1731)


Filter Products...
Show Expired Products
Sort by Status
My Contacts
Add A Contact
My Products
Download Software
My Cases
My Services
Enrollment Instructions
PRIMARY CONTACTS
Juan Carlos Villalba Cardenas
487 3820 Ext. 305
jvillalba@cra.gov.co
Tenable Vulnerability Management
Tenable Vulnerability Management
Tenable Vulnerability Management Licenses
User Guide
-T56F-
Set Label
Activated - Expires on: Sep 25, 2024 • Customer ID 270
Manage Product


tenable | Vulnerability Management | Settings > My Account
MY ACCOUNT
jvillalba@cra.gov.co
UPDATE ACCOUNT
GROUPS
PERMISSIONS
API KEYS
Update Account
FULL NAME
jvillalba@cra.gov.co
EMAIL
jvillalba@cra.gov.co
jvillalba@cra.gov.co
Administrator
Update Password
CURRENT PASSWORD
NEW PASSWORD


tenable | Vulnerability Management | Vulnerability Management Overview
Quick Actions
Dashboards
Scans
Explore
Findings
Assets
Act
Reports
Remediation
Settings
CVE-2023-4966: Citrix NetScaler ADC and NetScaler Gateway Information Disclosure Exploited in the Wild
By Scott Caveza on October 18 2023
CVE-2023-20198: Zero-Day Vulnerability in Cisco IOS XE Exploited in the Wild
By Scott Caveza on October 16 2023
Microsoft's October 2023 Patch Tuesday Addresses 103 CVEs (CVE-2023-36563, CVE-2023-41763)
By Tenable Security Response Team on October 10 2023
verview (Explore)
Jump to Dashboard
Dashboards
Export
Severity
Discovered by Nessus Agent
Severity
Discovered By Agentless
Severity
0 Critical
0
0 High
0 Critical
0
0 High
Tenable Research Advisory
Missing Patches
Applied Patches

ACTA DE INICIO

En la ciudad de Bogotá, D.C. hoy 21 de septiembre 2023 las partes, representadas por **JUAN CARLOS VILLALBA CARDENAS** en calidad del supervisor del contrato designado por la CRA y **DAYANA VICTORIA WEVER LARA** con C.E. 822.562 en calidad de representante legal de la firma **2SECURE S.A.S** se ponen de acuerdo para suscribir la presente acta de inicio del contrato que se describe a continuación:

CONTRATO No.: 217 de 2023	
NOMBRE DEL CONTRATISTA: 2SECURE S.A.S	
IDENTIFICACIÓN: 900.372.621-4	**PLAZO FIJADO:** 29 DICIEMBRE DEL 2023
VALOR DEL CONTRATO: $16.869.530,94	**FECHA DE INICIACIÓN DEL CONTRATO:** 21 SEPTIEMBRE 2023
SUPERVISOR DEL CONTRATO: JUAN CARLOS VILLALBA CARDENAS	
OBJETO: ADQUISICION DE LA SUSCRIPCIÓN POR UN (1) AÑO A UNA HERRAMIENTA DE ANALISIS DE VULNERABILIDADES, PARA LA COMISION DE REGULACION DE AGUA POTABLE Y SANEAMIENTO BASICO - CRA, INCLUIDOS LOS SERVICIOS DE SOPORTE TÉCNICO, MANTENIMIENTO CONFIGURACIÓN Y AFINAMIENTO.	
REGISTRO PRESUPUESTAL No. 35523	**FECHA:** 19 SEPTIEMBRE 2023
PÓLIZA No: SGPL-111389047-1	**FECHA:** 20 SEPTIEMBRE 2023
FECHA DE SUSCRIPCIÓN DEL CONTRATO: 19 SEPTIEMBRE 2023	
FECHA DE APROBACIÓN DE PÓLIZA: 21 SEPTIEMBRE 2023	

JUAN CARLOS VILLALBA C.

Supervisor
Juan Carlos Villalba Cardenas
Profesional Especializado

Contratista:
DAYANA VICTORIA WEVER LARA
C.E. 822.562
Representante legal
2SECURE S.A.S

Tenable MSSP User Guide

Last Revised: October 26, 2023

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Table of Contents

Welcome to Tenable MSSP **5**

Get Started with Tenable MSSP **8**

Log in to Tenable MSSP 10

Tenable MSSP Dashboard Overview 11

View Tenable MSSP License Information 14

Tenable Licenses 15

Access the User Account Menu 16

My Account 17

Update Your User Account 18

Change Your Password 19

Configure Two-Factor Authentication 21

View Groups 24

View Permissions 25

Generate Your API Keys 26

About Settings 28

General Settings 29

Enforce Two-Factor Authentication for All Users 30

Remove Two-Factor Authentication for All Users 31

SAML 32

View SAML Configurations 34

Add a SAML Configuration 36

Edit a SAML Configuration 46

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Disable a SAML Configuration 50
Enable a SAML Configuration 51
Enable Automatic Account Provisioning 52
Disable Automatic Account Provisioning 54
Delete SAML Configuration 55
Access the Resource Center 56
Interact with Tenable MSSP Table 57
Log out of Tenable MSSP 60
Accounts **61**
Create an Eval Account 63
Create an Evaluation Account 64
View Details for a Customer Account 66
Account Details 67
Edit a Customer Account 69
Assign a Logo to an Account 70
Remove a Logo from an Account 71
Unlink an Account from the Tenable MSSP 72
Add Resource Links 73
Modify Resource Links 75
Remove Resource Links 77
Filter a Table 79
Domains **82**
View Domains 83
Add a Secondary Domain to your Account 85

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Set a Domain as Primary or Secondary 87
Disable a Domain 89
Enable a Domain 90
Scans **91**
View Scans 92
Logos **93**
Add a Logo 94
Edit a Logo 95
Delete a Logo 96
Users **97**
Create a Tenable MSSP User 98
Assign a Tenable MSSP User to an Account 100
Remove a Tenable MSSP User from an Account 101
Edit a Tenable MSSP User 102
Generate API Keys for another Tenable MSSP User 104
Disable a Tenable MSSP User 105
Enable a Tenable MSSP User 106
Delete a Tenable MSSP User 107
Instances **109**
Use Single Sign-On to Access a Customer Instance 110

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Welcome to Tenable MSSP

Tenable MSSP 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 Tenable MSSP for more information.

Managing Customer Accounts

Maintaining spreadsheets full of customer product data can be tedious, inaccurate, and difficult to track. Tenable MSSP features the default **Accounts** page, which displays all the Tenable Vulnerability Management customers that you maintain in one easily accessible location. In Tenable MSSP, you can add Tenable Vulnerability Management 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 Vulnerability Management Instance

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

Other Tenable Vulnerability Management Products

Tenable Vulnerability Management Vulnerability Management

See the User Guide

Tenable Vulnerability Management® allows security and audit teams to share multiple Nessus, Nessus Agent, and Nessus Network Monitor scanners, scan schedules, scan policies and scan

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

results among an unlimited set of users or groups. By making different resources available for sharing among users and groups, Tenable Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management API

See the API

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

Tenable Vulnerability Management Container Security

See the User Guide

Tenable Vulnerability Management 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 Vulnerability Management Container Security ensures every container reaching production is secure and compliant with enterprise policy.

Tenable Vulnerability Management Web Application Scanning

See the User Guide

Tenable Vulnerability Management 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 Vulnerability Management Web Application Scanning provides comprehensive vulnerability scanning for modern web applications. Tenable Vulnerability Management Web Application Scanning's accurate vulnerability coverage minimizes false positives and false negatives, ensuring

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.



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.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Get Started with Tenable MSSP

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

1. Prepare
2. Create Tenable MSSP Users
3. Configure Tenable MSSP Customer Accounts
4. Use Single Sign-On to Access a Customer Tenable Vulnerability Management Instance

Prepare

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

To plan your use case for Tenable MSSP:

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

Create Tenable MSSP Users

Create users for any administrators you want to have access to Tenable MSSP.

Configure Tenable MSSP Customer Accounts

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

Use Single Sign-On to Access a Customer Tenable Vulnerability Management Instance

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Use Tenable MSSP's single sign-on capabilities to access the Tenable Vulnerability Management instances associated with your configured customer accounts.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Log in to Tenable MSSP

Required Tenable Vulnerability Management User Role: Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

Before you begin:

- Obtain credentials for your Tenable MSSP account.

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

- Review the Tenable Vulnerability Management System Requirements in the *General Requirements User Guide* and confirm that your computer and browser meet the requirements.

To log in to Tenable MSSP:

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

   The Tenable Vulnerability Management 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, Tenable MSSP logs you out after a period of inactivity.

5. Click **Sign In**.

   Tenable MSSP appears. By default, the portal displays the Accounts page.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Tenable MSSP Dashboard Overview

Tenable MSSP Portal Dashboard visualizes key insights about your customer licenses and scan results.

To access the **Dashboard** page in Tenable MSSP, do the following:

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

   The left navigation plane appears.

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

   The Tenable MSSP Dashboard appears.

You can roll over individual items to reveal additional information or click on items to drill down into details behind the data.

In the **Tenable MSSP Overview** dashboard, you can interact with the following widgets:

Widget	Description
Cyber Exposure	This widget highlights the most recent Tenable blog posts related to Cyber Exposure incidents. • Click on a tile to navigate to the Tenable blog post. • Click the ⌄ or ⌃ button to collapse or expand the feed. • Click the ‹ or › button to scroll through the tiles.
Accounts	This widget displays the total number of customer accounts within the last 14 days. A green arrow indicates an increase in the number of customer accounts. A red arrow indicates a decrease in the number of customer accounts. To export the data in the widget, click the ⋮ button and select a format.
License Over Utilized	This widget displays the number of customer accounts with license utilization above 100% within the last 14 days. To export the data in the widget, click the ⋮ button and select a format.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

High License Utilized	This widget displays the number of customers with license utilization above 90% within the last 14 days. To export the data in the widget, click the ⋮ button and select a format.
Normal License Utilized	This widget displays the number of customer accounts with license utilization between 30% and 90% within the last 14 days. To export the data in the widget, click the ⋮ button and select a format.
License Under Utilized	This widget displays the number of customer accounts with license utilization under 30% within the last 14 days. A green arrow indicates an increase in the number of customer accounts with underutilized licenses. A red arrow indicates a decrease in the number of customer accounts with underutilized licenses. To export the data in the widget, click the ⋮ button and select a format.
License Expiring	This widget displays the number of licenses that age out in the next 90 days. A red arrow indicates the number of licenses nearing expiration. To export the data in the widget, click the ⋮ button and select a format.
Licensing Data	This widget displays a list of customer accounts, the basic details of their licenses, and their license utilization percentage. You can view the following information: • **Account Name** — The name of the customer account. • **Assets Licenses** — The number of asset licenses that the customer owns. • **Licenses Utilized** — The number of utilized licenses. This can be more than or less than the number of **Asset Licenses**. • **Utilization** — The utilization percentage of licenses.
Scan Results	This widget displays a list of customer accounts and the scan status for each customer account. You can view the following information:

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

	• **Account Name** — The name of the customer account.
	  • To view the customer account details, click one of the customer names.
	  The **Accounts** page appears. For more information, see Accounts.
	• **Running** — The number of currently running scans.
	• **Completed** — The number of completed scans.
	• **Aborted** — The number of aborted scans.
	• **Canceled** — The number of canceled scans.
	You can use the ▽ filter icon to filter results by 7 days, 30 days, 90 days, 180 days, or 1 year.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

View Tenable MSSP License Information

Required User Role: Administrator

The **License** page contains information about your Tenable MSSP instance, including license and environment details.

To view Tenable MSSP license information:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click **License**.

   The **License** page appears.

Widget	Description
License Overview	Information about your license utilization. The ring chart visualizes the percentage of Tenable MSSP licenses distributed compared to your total number of purchased licenses. The counts to the right of the chart show the total number of licenses used, and the total number of licenses purchased.
Environment Information	Information about your Tenable MSSP site. This includes the site name, the region in which your Tenable MSSP container resides, and its container ID. **Tip:** Your site is a geographical location that corresponds with your region. You can provide this information directly to Tenable Support when reporting a potential issue.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Tenable Licenses

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

- Vulnerability Management Licensing

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Access the User Account Menu

Required Tenable Vulnerability Management User Role: Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

To access the user account menu in Tenable MSSP:

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 Vulnerability Management.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

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
- View Groups
- View Permissions
- Generate Your API Keys

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Update Your User Account

Required Tenable Vulnerability Management User Role: Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

To update your user account in Tenable MSSP:

1. Access the **My Account** page:
    - In the upper-right corner, click the button.

      The user account menu appears.

      -or-

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

       The left navigation plane appears.

    b. In the left navigation plane, click **Settings**.

       The **Settings** page 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.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Change Your Password

Required Tenable Vulnerability Management User Role: Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

Note: To change another user's password, see Edit a Tenable MSSP User.

To change your password in Tenable MSSP:

1. Access the **My Account** page:
   - In the upper-right corner, click the button.

     The user account menu appears.

     -or-

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

      The left navigation plane appears.

   b. In the left navigation plane, click **Settings**.

      The **Settings** page appears.
2. Click **My Account**.

   The **My Account** page appears.
3. In the **Update Password** section, 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

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

5. Click the **Save** button.

   Tenable MSSP saves the new password.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Configure Two-Factor Authentication

Required Tenable Vulnerability Management 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 Tenable MSSP:

1. Access the **My Account** page:
    - In the upper-right corner, click the button.

      The user account menu appears.

      -or-

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

       The left navigation plane appears.

    b. In the left navigation plane, click **Settings**.

       The **Settings** page 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 Tenable MSSP sends a text message with a verification code to the phone number.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

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**.

   Tenable MSSP displays a success message confirming that you have configured two-factor authentication

   for your account.
9. (Optional) To configure whether Tenable MSSP 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 MSSP updates your backup email settings.

To disable two-factor authentication in Tenable MSSP:

1. Access the **My Account** page:
   - In the upper-right corner, click the button.

     The user account menu appears.

     -or-

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

      The left navigation plane appears.

   b. In the left navigation plane, click **Settings**.

      The **Settings** page appears.
2. Click **My Account**.

   The **My Account** page appears.
3. Under **Enable Two Factor Authentication**, click **Disable**.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

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

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

   Tenable MSSP disables two-factor authentication for your account.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

View Groups

The **Groups** page in the **My Account** section of Tenable MSSP shows the user groups in Tenable MSSP.

To view the **Groups** page:

1. Access the **My Account** page:
    - In the upper-right corner, click the button.

      The user account menu appears.

      -or-

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

      The left navigation plane appears.

    b. In the left navigation plane, click **Settings**.

      The **Settings** page appears.
2. Click **My Account**.

    The **My Account** page appears.
3. In the left navigation plane, click the **Groups** tab.

    The **Groups** page appears,

    On the **Groups** 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.
        2. Click the button.

            Tenable MSSP filters the table by your search criteria.
    - View the groups in the Tenable MSSP portal.
    - View the number of users in each group.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

View Permissions

The **Permissions** page in the **My Account** section of Tenable MSSP shows the permissions assigned to any Tenable MSSP accounts. An account's permissions determines their ability to view, edit, scan, or use one or more assets in their organization's account.

To view the **Permissions** page:

1. Access the **My Account** page:
    - In the upper-right corner, click the button.

      The user account menu appears.

      -or-

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

       The left navigation plane appears.

    b. In the left navigation plane, click **Settings**.

       The **Settings** page appears.
2. Click **My Account**.

   The **My Account** page appears.
3. In the left navigation plane, click the **Permissions** tab.

   The **Permissions** page appears,

   On the **Permissions** 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.
        2. Click the button.

           Tenable MSSP filters the table by your search criteria.
    - View the permissions assigned to each account in the Tenable MSSP portal.
    - View the objects to which the permissions apply.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Generate Your API Keys

Required Tenable Vulnerability Management User Role: Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

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

Note: Tenable Vulnerability Management API Access and Secret keys are required to use the Tenable Vulnerability Management API.

For information on generating API keys for another user, see Generate API Keys for another Tenable MSSP User.

To generate API keys for your own account in Tenable MSSP:

1. Access the **My Account** page:
   - In the upper-right corner, click the button.

     The user account menu appears.

     -or-

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

      The left navigation plane appears.

   b. In the left navigation plane, click **Settings**.

      The **Settings** page appears.
2. Click **My Account**.

   The **My Account** page appears.
3. In the left navigation plane, click the **API Keys** tab.

   The **API Keys** section appears.
4. Click **Generate**.

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

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

> **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**.

   Tenable MSSP generates access and secret keys for the account. These keys must be used to authenticate with Tenable MSSP 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 Vulnerability Management.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

About Settings

Required Tenable Vulnerability Management User Role: Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

To access the **Settings** page in Tenable MSSP:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

You can access the following pages from the **Settings** page:

Settings Page	Description
General	Manage your general settings.
My Account	Manage your account settings.
License	View license and environment details about your Tenable MSSP instance.
SAML	Configure Tenable MSSP to accept credentials from your SAML identity provider.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

General Settings

Required User Role: Administrator

On the **General** page, you can configure general settings for your Tenable MSSP instance.

To access the **General** settings page in Tenable MSSP:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click **General**.

   The **General** page appears.

From the **General** page, you can do the following:

- Enforce Two-Factor Authentication for All Users
- Remove Two-Factor Authentication for All Users

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Enforce Two-Factor Authentication for All Users

Required User Role: Administrator

To enforce two-factor authentication for all users:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click **General**.

   The **General** page appears.

4. Click **Enforce Two-Factor Authentication**.

   A confirmation window appears.

5. Click **Yes** to continue.

   Tenable MSSP enforces two-factor authentication for all users.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Remove Two-Factor Authentication for All Users

Required User Role: Administrator

To remove two-factor authentication for all users:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click **General**.

   The **General** page appears.

4. Click **Remove Two-Factor Authentication**.

   A confirmation window appears.

5. Click **Yes** to continue.

   Tenable MSSP removes two-factor authentication for all users.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

SAML

You can configure Tenable MSSP to accept credentials from your SAML identity provider (for example, Okta). This allows for an additional layer of security, where the SAML credentials are certified for use within Tenable MSSP. Once you enable SAML for a user, they can log in to Tenable MSSP directly through their identity provider, which automatically signs them in and redirects them to the Tenable MSSP landing page.

On the **SAML** page, you can view and manage your SAML credentials. You can also enable, disable, and add new configurations for users within your Tenable MSSP instance.

> **Note**: Tenable MSSP supports SAML 2.0 configurations.

SAML Details

On the **SAML** page, you can view a table that includes the following details about your SAML configurations:

Column	Description
UUID	The UUID that Tenable MSSP automatically generates when you create a new SAML configuration.
Description	A description for the SAML configuration.
Last Login	The date and time on which a user on your instance last successfully logged in via the SAML configuration. **Note**: The **Last Login** column shows a value only if Tenable MSSP has login data for the SAML identity provider.
Last Attempted Login	The date and time on which a user on your instance last attempted to log in via the SAML configuration. **Note**: The **Last Attempted Login** column shows a value only if Tenable MSSP has attempted login data for the SAML identity provider.
Certificate	The certificate for the SAML configuration.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

	In the certificate column, you can complete the following tasks. • Click the button to copy the certificate to your clipboard. • Hover over the button to view the certificate expiration date. **Note**: Your identity provider determines the expiration date for your certificate.
Actions	An interactive column from which you can download the metadata.xml file that contains one or more security certificates for the configuration. To download the metadata.xml file: a. In the **Actions** column for the configuration from which you want to download a metadata.xml file, click the button. An options menu appears. b. In the menu, click **Download SP Metadata**. Tenable MSSP downloads the metadata.xml file to your computer.

On the **SAML** page, you can perform the following tasks:

- View SAML Configurations
- Add a New SAML Configuration
- Edit a SAML Configuration
- Disable a SAML Configuration
- Enable a SAML Configuration
- Disable Automatic Account Provisioning
- Enable Automatic Account Creation
- Delete a SAML Configuration

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

View SAML Configurations

Required User Role: Administrator

To view your SAML configurations:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **SAML** tile.

   The **SAML** page appears.

4. (Optional) Refine the table data.

   The **SAML** table contains the following columns:

Column	Description
UUID	The UUID that Tenable MSSP automatically generates when you create a new SAML configuration.
Description	A description for the SAML configuration.
Last Login	The date and time on which a user on your instance last successfully logged in via the SAML configuration. **Note**: The **Last Login** column displays a value only if Tenable MSSP has login data for the SAML identity provider.
Last Attempted Login	The date and time on which a user on your instance last attempted to log in via the SAML configuration. **Note**: The **Last Attempted Login** column displays a value only if Tenable MSSP has attempted login data for the SAML identity provider.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Certificate	The certificate for the SAML configuration. In the certificate column, you can complete the following tasks. • Click the button to copy the certificate to your clipboard. • Hover over the button to view the certificate expiration date. **Note**: Your identity provider determines the expiration date for your certificate.
Actions	An interactive column from which you can download the metadata.xml file that contains one or more security certificates for the configuration. To download the metadata.xml file: 1. In the **Actions** column for the configuration from which you want to download a metadata.xml file, click the button. An options menu appears. 2. In the menu, click **Download SP Metadata**. Tenable MSSP downloads the metadata.xml file to your computer.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Add a SAML Configuration

Required User Role: Administrator

You can manually enter the details for your SAML configuration or you can upload a metadata.xml file that you download from your identity provider (IdP).

Before you begin:

- Follow the steps described in your IdP's documentation to set up a SAML application for Tenable MSSP on your IdP account. Your IdP requires an entity ID and a reply URL for Tenable MSSP to set up the SAML application:
    - Entity ID — `TENABLE_IO_PLACEHOLDER`.
    - ACS/Single Sign On URL — `https://cloud.tenable.com/SAML/login/placeholder.com`.
- In your IdP account, download your metadata.xml file.

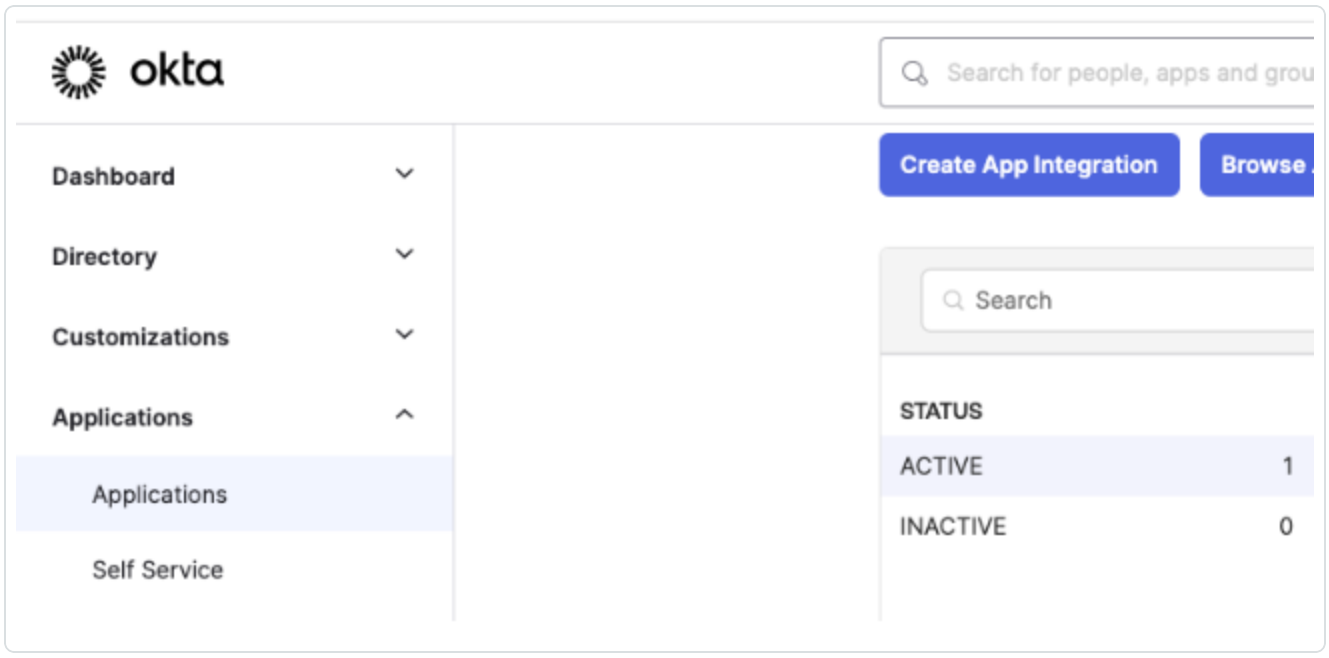
Example IdP configuration: Okta

To configure the initial IDP setup in Okta:

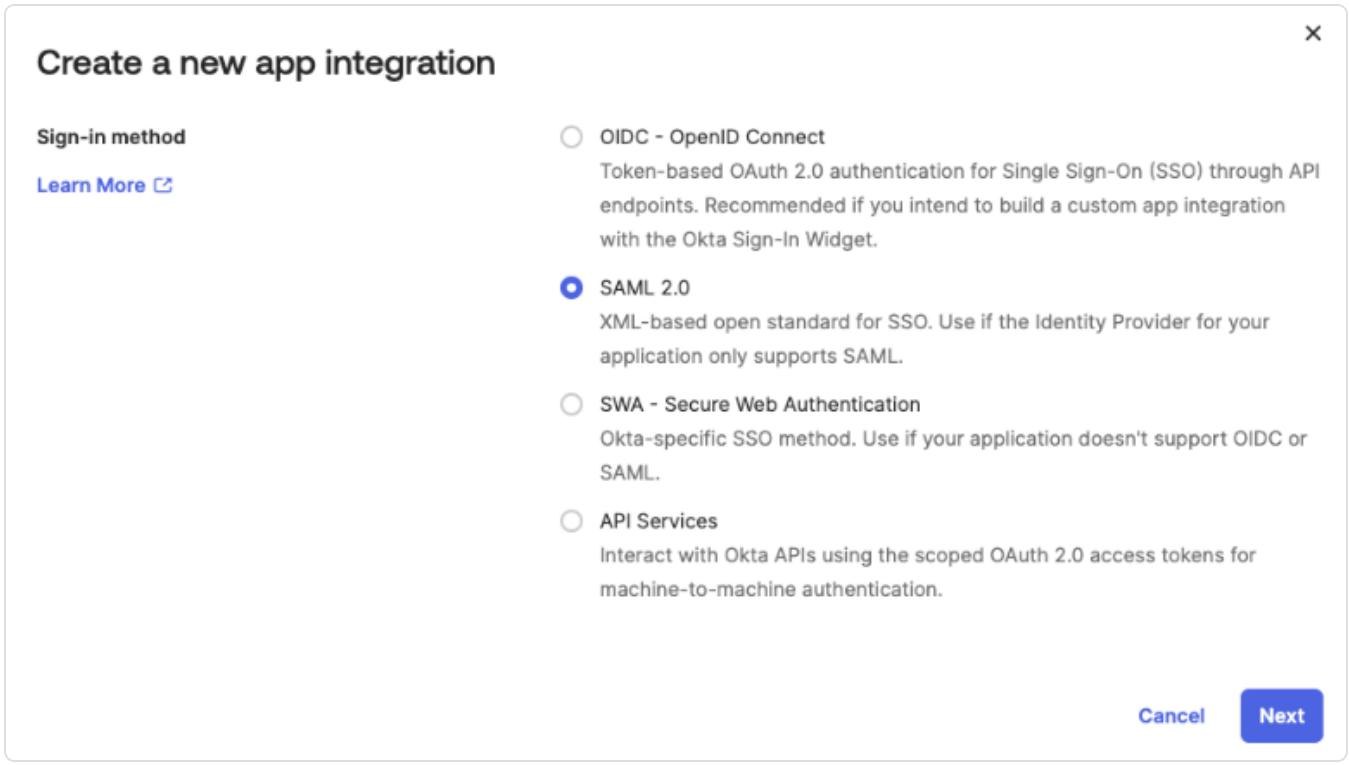
1. In your browser, navigate to the Okta Admin portal.
2. In the left navigation menu, click **Applications** > **Applications**.
3. Click **Create App Integration**.

   The **Create a new app integration** window appears.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.



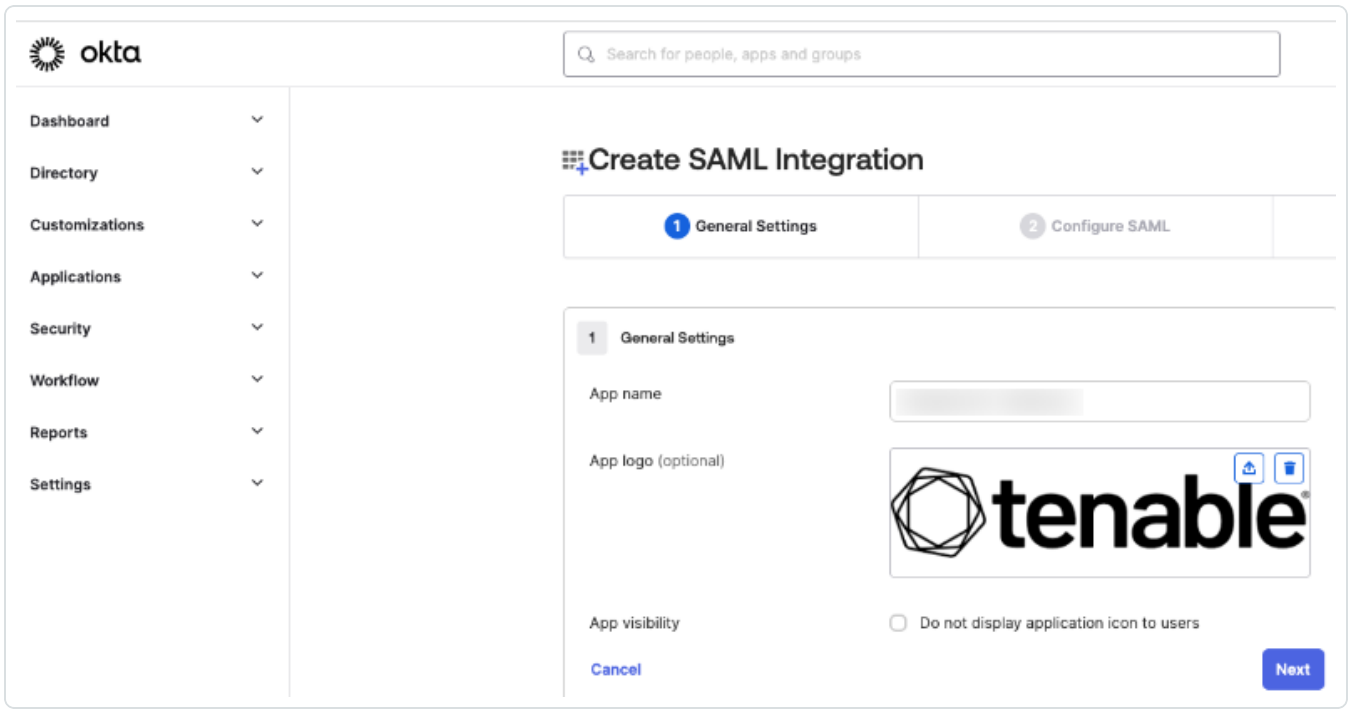
4. Select the **SAML 2.0** radio button.



5. Click **Next**.

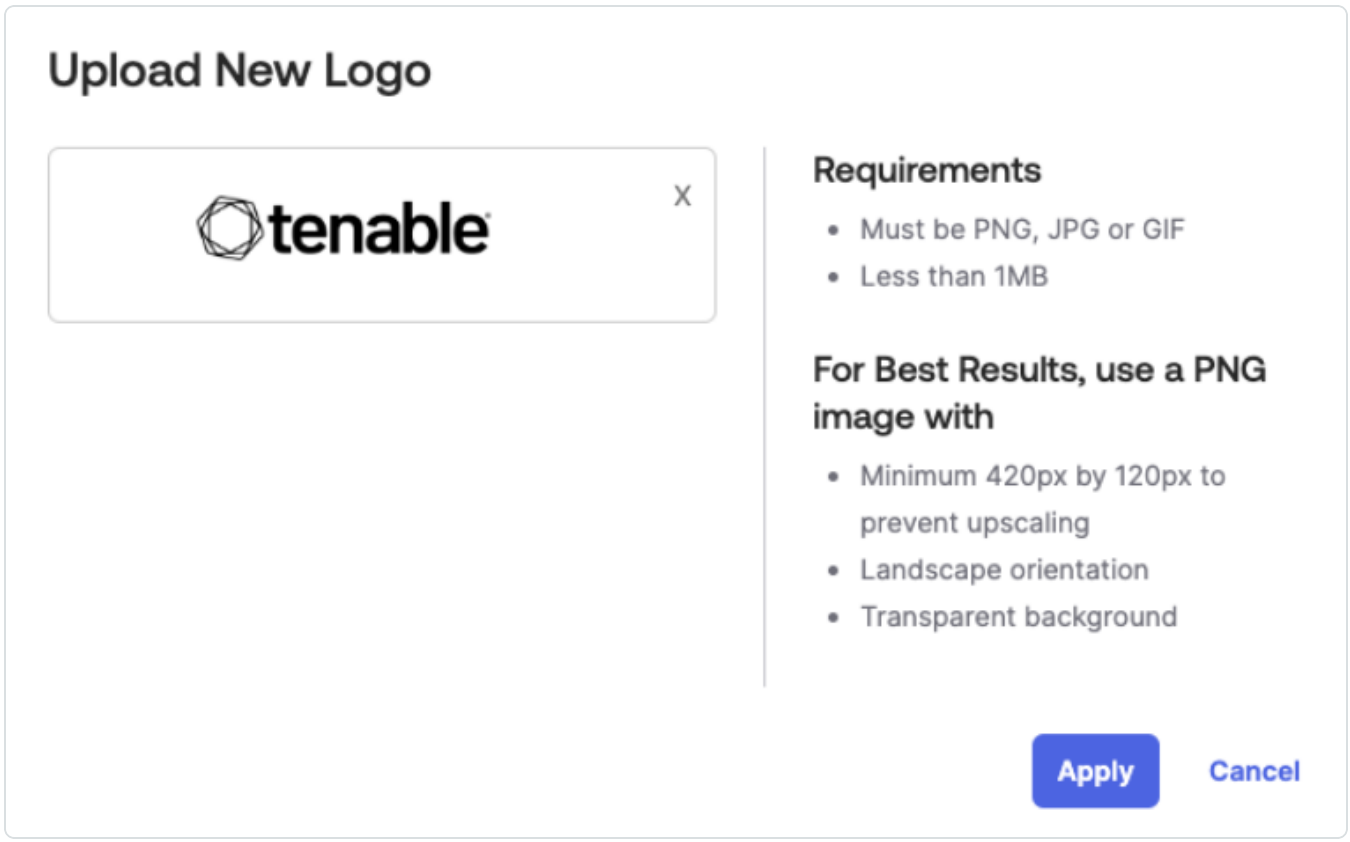
   The **General Settings** options appear.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.



6. In the **App name** text box, type a name for your application.
7. (Optional) To add a custom logo for the application, in the **App logo** section, upload a .png, .jpeg, or .gif file and click **Apply**.

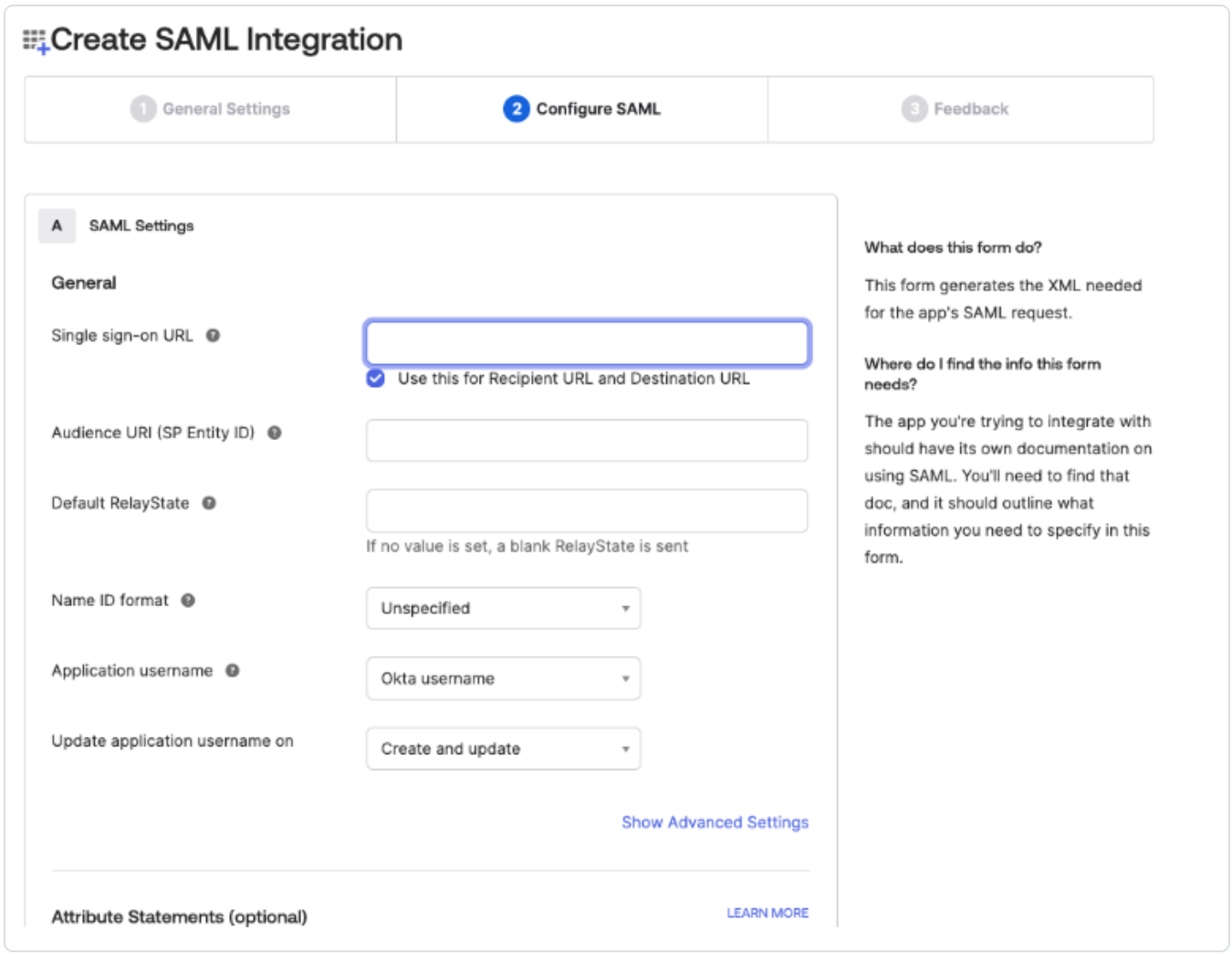
Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.



8. Click **Next**.

   The **Configure SAML** options appear.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.



9. In the **Single sign-on URL** text box, type the following placeholder URL:

```
https://cloud.tenable.com/saml/login/PLACEHOLDER
```

> **Note:** You will later replace *PLACEHOLDER* with a unique UUID for the SAML configuration. This link is case-sensitive.

10. Select the **Use this for Recipient URL and Destination URL** check box.

11. In the **Audience URI (SP Identity ID)** text box, type the following placeholder text:

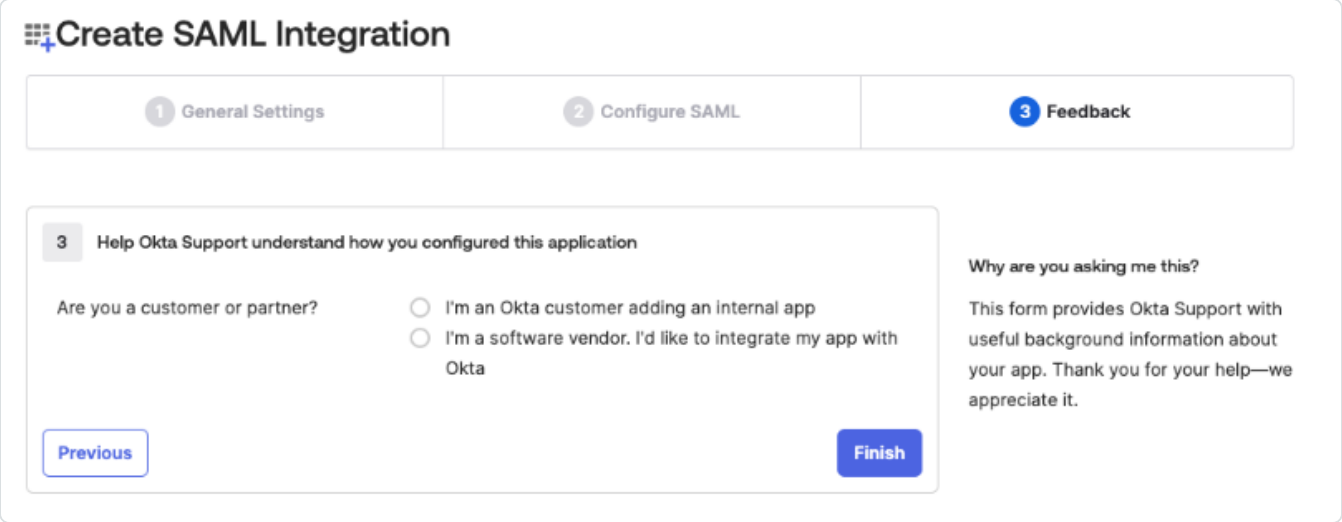
```
TENABLE_IO_PLACEHOLDER
```

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Note: You will later replace *PLACEHOLDER* with a unique UUID for the SAML configuration.

12. Ensure the **Default RelayState** text box is blank.
13. In the **Name ID format** drop-down, select **Unspecified**.
14. In the **Application username** drop-down, select **Email**.
15. In the **Update application username on** drop-down, select **Create and update**.
16. Do not change any other configuration options.
17. Click **Next**.

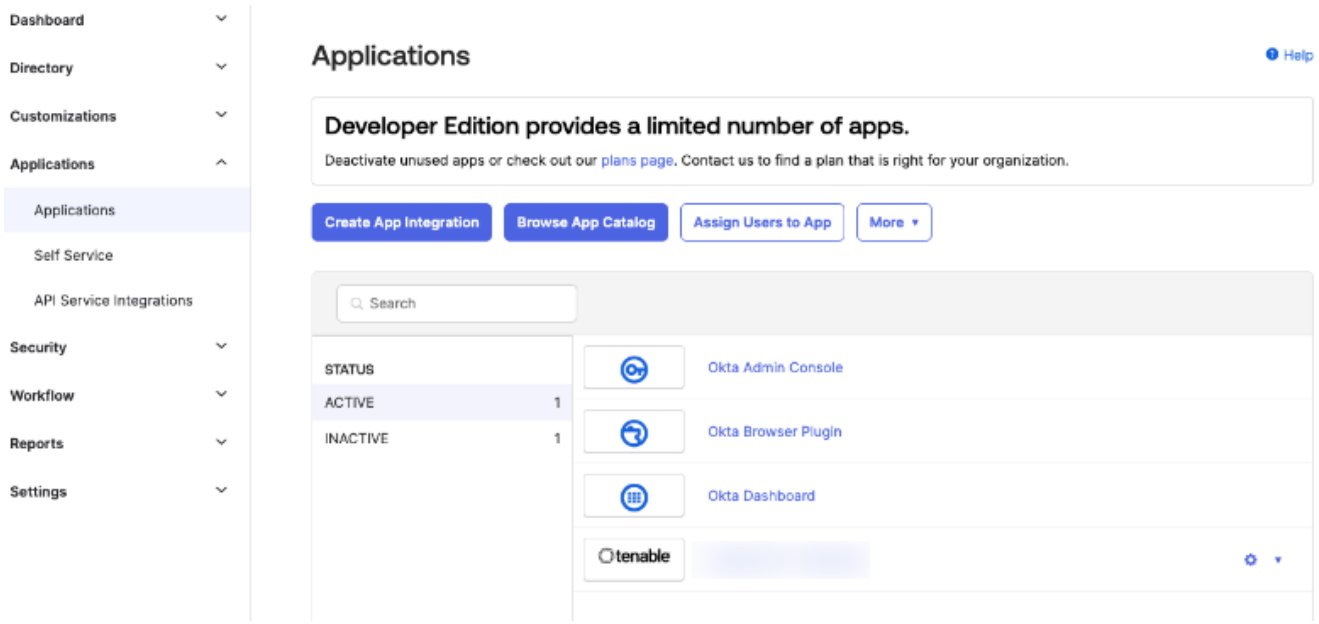
    The **Feedback** options appear.



18. (Optional) Provide any feedback you want to include.
19. Click **Finish**.

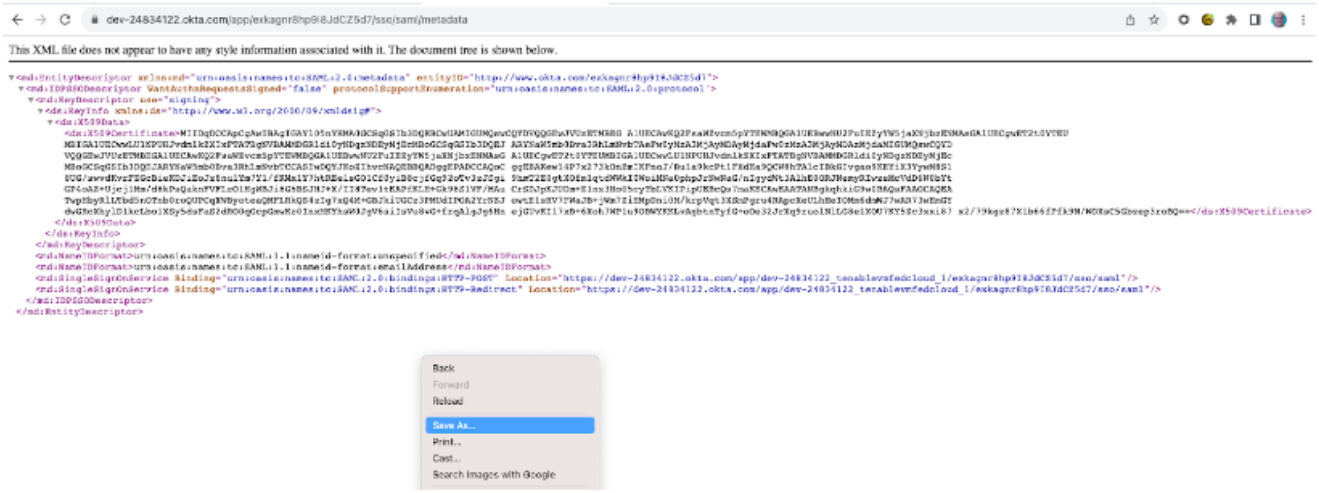
    Okta saves your application configuration.
20. In the applications list, select the newly added application configuration.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.



Application details appear.

21. In your browser, paste the URL and save the resulting file as *metadata.xml*.



Note: Tenable does not currently support a SP-Initiated SAML flow. Because it must be initiated from the Identity Provider side, navigating directly to https://cloud.tenable.com does not allow SSO.

Important! All users must have an account configured in Tenable MSSP that matches their SSO login. You must ensure the SSO login matches the FULL Tenable account name (i.e., user@tenable.com).

To add a new SAML configuration:

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **SAML** tile.

   The **SAML** page appears.

4. In the action bar, click ⊕ **Create**.

   The **SAML Settings** page appears.

5. Do one of the following:

   To provide configuration details by uploading the metadata.xml file from your IdP:

   a. In the first drop-down box, select **Import XML**.

   > **Note**: **Import XML** is selected by default.

   b. The **Type** drop-down box specifies the type of identity provider you are using. Tenable MSSP supports SAML 2.0 (for example, Okta, OneLogin, etc.).
   This option is read-only.

   c. Under **Import**, click **Add File**.

      A file manager window appears.

   d. Select the metadata.xml file.

      The metadata.xml file is uploaded.

   To manually create your SAML configuration using data from the metadata.xml file from your IdP:

   a. In the first drop-down box, select **Manual Entry**.

      A **SAML** configuration form appears.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

b. Configure the settings described in the following table:

Settings	Description
Enabled toggle	A toggle in the upper-right corner that indicates whether the SAML configuration is enabled or disabled. By default, the **Enable** setting is set to **Enabled**. Click the toggle to disable SAML configuration.
Type	Specifies the type of identity provider you are using. Tenable MSSP supports SAML 2.0 (for example, Okta, OneLogin, etc.). This option is read-only.
Description	A description for the SAML configuration.
IdP Entity ID	The unique entity ID that your IdP provides. **Note**: If you want to configure multiple IdPs for a user account, create a new configuration for each identity provider with separate identity provider URLs, entity IDs, and signing certificates.
IdP URL	The SAML URL for your IdP.
Certificate	Your IdP security certificate or certificates. **Note**: Security certificates are found in a metadata.xml file that your identity provider provides. You can copy the content of the file and paste it in the **Certificate** box.
User Auto Provisioning Enabled	A toggle that indicates whether automatic user account creation is enabled or disabled.
IdP Assigns User Role at Provisioning	To assign a user role during provisioning, enable this toggle. In your SAML identity provider, add an attribute statement with **userRoleUuid** as the attribute name and the user role UUID as

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

	the attribute value. To obtain the UUID for a user role, go to **Settings** > **Access Control** > **Roles**.
IdP Resets User Role at Each Login	To assign a role each time a user logs in, overwriting the current role with the one chosen in your IdP, enable this toggle. In your SAML identity provider, add an attribute statement with **userRoleUuid** as the attribute name and the user role UUID as the attribute value. To obtain the UUID for a user role, go to **Settings** > **Access Control** > **Roles**.

6. Click **Save**.

   Tenable MSSP saves your SAML configuration.

What to do next:

- Download the metadata.xml from Tenable MSSP using the **Download SP Metadata** option in the SAML Configurations table.
- Upload this file to the SAML application you created for Tenable MSSP with your SAML provider.

Tip: If you are having trouble configuring SAML, Tenable recommends trying one of the various third-party SAML debugging tools available online. You can also reach out to Tenable Support for further troubleshooting assistance.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Edit a SAML Configuration

Required User Role: Administrator

You can edit a SAML configuration on the **SAML** page.

To edit a SAML configuration:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **SAML** tile.

   The **SAML** page appears.

4. In the SAML table, click the SAML configuration that you want to edit.

   The **SAML Settings** page appears.

5. (Optional) In the first drop-down box, select a different method to provide basic configuration details.

   - **Import XML** — Configure SAML authentication by uploading the metadata file your IdP provided, as described in Add a New SAML Configuration.
   - Manual Entry — Configure SAML authentication by manually configuring SAML options using data from the metadat.xml file your IdP provides as described in Add a New SAML Configuration.

     Tenable MSSP updates the configuration options based on your selected source.

6. Update any of the configurable SAML settings described in the following table.

   Note: Some settings are read-only and cannot be modified.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Note: The configuration options you can update depend on the source you select in the first drop-down box.

Settings	Source	Description
Enabled toggle	**Manual Entry**	Indicates whether the SAML configuration is or disabled. By default, the **Enable** setting is set to **Enabled**. In the upper-right corner, click the toggle to disable SAML configuration.
Type	**Manual Entry** , **Import XML**	Specifies the type of identity provider you are using. Tenable MSSP supports SAML 2.0 (e.g., Okta, OneLogin, etc.).
UUID	**Entry**, **Import XML**	A unique identifier for your identity provider that Tenable MSSP automatically generates when you create a new SAML configuration. This box is read-only.
URL	**Manual Entry** , **Import XML**	The login URL that Tenable MSSP generates when you create a configuration. This box is read-only.
Entity ID	**Manual Entry** , **Import XML**	A unique identifier that Tenable MSSP generates when you create a configuration. This box is read-only.
Created	**Manual Entry** , **Import**	The time and date on which an administrator user created the configuration. This box is read-only.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

	XML	
Last Updated	**Manual Entry** , **Import XML**	The time and date on which an administrator user last updated the configuration. This box is read-only.
Description	**Manual Entry**	A description for the SAML configuration.
IdP Entity ID	**Manual Entry**	Your identity provider's unique entity ID. **Note**: If you want to configure multiple IdPs for a user account, create a new configuration for each identity provider, with separate identity provider URLs, entity IDs, and signing certificates.
IdP URL	**Manual Entry**	The SAML URL for your identity provider.
Certificate	**Manual Entry**	Your identity provider's security certificate or certificates. **Note**: Security certificates are found in a metadata.xml file that your identity provider provides. You can copy the content of the file and paste it in the **Certificate** box.
User Autoprovisioning Enabled	**Manual Entry**	A toggle that indicates whether automatic account user creation is enabled or disabled
IdP Assigns User Role at Provisioning	**Manual Entry**	To assign a user role during provisioning, enable this toggle. In your SAML identity provider, add an attribute statement with **userRoleUuid** as the attribute name and the user role UUID as the attribute value.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

		To obtain the UUID for a user role, go to **Settings** > **Access Control** > **Roles**.
IdP Resets User Role at Each Login	**Manual Entry**	To assign a role each time a user logs in, overwriting the current role with the one chosen in your IdP, enable this toggle. In your SAML identity provider, add an attribute statement with **userRoleUuid** as the attribute name and the user role UUID as the attribute value. To obtain the UUID for a user role, go to **Settings** > **Access Control** > **Roles**.
Import	**Import XML**	A metadata.xml file from your identity provider that contains one or more SAML certificates. To import a new metadata.xml file from your identity provider: a. Under **Import**, click **Add File**. A file explorer window appears. b. Select the metadata.xml file. The metadata.xml file is uploaded. **Note**: If your metadata.xml file contains multiple certificates, only the first one appears in the **Certificate** column for the configuration on the **SAML** page.

7. Click **Save**.

   Tenable MSSP saves the configuration.

   The **SAML** page appears with the updated configuration.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Disable a SAML Configuration

Required User Role: Administrator

Disabling a SAML configuration prevents users on your instance from using the SAML credentials in the configurations to log in to Tenable MSSP. You can enable a disabled SAML configuration as described in Enable a SAML Configuration.

Caution: When you disable a SAML configuration, users can no longer log in to Tenable MSSP using their SAML credentials. Make sure all users on your instance have an alternative method to log in to Tenable MSSP before you disable a SAML configuration.

To disable a SAML configuration:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **SAML** tile.

   The **SAML** page appears.

4. In the SAML table, click the SAML configuration that you want to disable.

   The **SAML Settings** page appears.

5. At the bottom of the page, click the **SAML Enable** toggle to disable the configuration.

6. Click **Save**.

   Tenable MSSP disables the SAML configuration. On the **SAML** page, the disabled configuration appears in light gray.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Enable a SAML Configuration

Required User Role: Administrator

You can enable a disabled a SAML configuration. For more information about SAML authentication in Tenable MSSP, see SAML.

To enable a SAML configuration:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **SAML** tile.

   The **SAML** page appears.

4. In the SAML table, click the SAML configuration that you want to enable.

   Tip: Disabled configurations appear in light gray.

   The **SAML Settings** page appears.

5. At the bottom of the page, click the **SAML Enable** toggle to enable the configuration.

6. Click **Save**.

   Tenable MSSP enables the SAML configuration. On the **SAML** page, the enabled configuration appears in black.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Enable Automatic Account Provisioning

Required User Role: Administrator

When you manually configure or edit a SAML configuration, you can enable automatic user account provisioning. Automatic account provisioning allows users with credentials for the IdP named in the SAML configuration to create a Tenable MSSP account the first time they log in via the IdP.

Tenable MSSP creates automatically provisioned accounts with the following defaults:

- **Full name** — NameID
- **Username** — NameID
- **Email** — NameID
- **User role** — Basic

Tenable MSSP does not currently support any other claim types.

To enable automatic user account provisioning:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **SAML** tile.

   The **SAML** page appears.

4. In the SAML table, click the SAML configuration for which you want to enable automatic account provisioning.

   The **SAML Settings** page appears.

5. At the bottom of the page, click the **User Autoprovisioning Enabled** toggle to enable automatic account provisioning.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

6. Click **Save**.

   Tenable MSSP enables automatic account provisioning in the SAML configuration.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Disable Automatic Account Provisioning

Required User Role: Administrator

Disabling automatic account provisioning prevents users from automatically creating Tenable MSSP account the first time they access the platform via their IdP. You can enable automatic account provisioning on a SAML configuration, as described in Enable Automatic Account Creation.

To disable automatic user account provisioning:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **SAML** tile.

   The **SAML** page appears.

4. In the SAML table, click the SAML configuration for which you want to disable automatic account provisioning.

5. The **SAML Settings** page appears.

6. At the bottom of the page, click the **User Autoprovisioning Enabled** toggle to disable automatic account provisioning.

7. Click **Save**.

   Tenable MSSP disables automatic account provisioning in the SAML configuration.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Delete SAML Configuration

Required User Role: Administrator

You can delete a SAML configuration on the **SAML** page. For more information about SAML authentication in Tenable MSSP, see SAML SAML.

To enable a SAML configuration:

Before you begin:

- Disable the SAML configuration you want to delete.

To delete a SAML configuration:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **SAML** tile.

   The **SAML** page appears.

4. In the SAML table, select the check box for the SAML configuration that you want to delete.

5. In the action bar, click the 🗑 **Delete** button.

   Tenable MSSP deletes the SAML configuration.

   Note: Ensure that when you delete a SAML configuration, you also remove the related configuration in your IdP.

What to do next:

- Remove the related configuration from your identity provider's application.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Access the Resource Center

Required Tenable Vulnerability Management User Role: Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

The **Resource Center** displays a list of Tenable Vulnerability Management informational resources including product announcements, Tenable blog posts, and Tenable Vulnerability Management 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.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Interact with Tenable MSSP Table

Required Tenable Vulnerability Management User Role: Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

Note: Customizable tables also include the ability to access the actions buttons by right-clicking a table row. To access your browser menu, press the Ctrl key and right-click.

To interact with an Tenable MSSP table:

1. View a customizable table.
2. Do any of the following:

    - Navigate the table:

        - To adjust the sort order, click a column title.

          Tenable MSSP sorts all pages of the table by the data in the column you selected.

        - To increase or decrease the number of rows displayed per page, click **Results per page** and select a number.

          Tenable MSSP refreshes the table.

        - To view all action buttons available in a table row, click the button.

          This button appears instead of individual action buttons if 5 or more actions are possible for the row.

        - To navigate to another page of the table, click the arrows:

Button	Action
	Navigate to the first page of the table.
	Navigate to the previous or next page of the table.
	Navigate to the last page of the table.

    - Search the table:

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

In Tenable MSSP, a search box appears above individual tables in various pages and planes. In some cases, the search box appears next to the **Filters** box.

a. In the **Search** box, type your search criteria.

   Your search criteria depends on the type of data in the table you want to search.

b. Click the 🔍 button.

   Tenable MSSP filters the table by your search criteria.

- To change the column order, drag and drop a column header to another position in the table.
- Remove or add columns:

  a. Roll over any column.

     The ☰ button appears in the header.

  b. Click the ☰ button.

     A column selection box appears.

  c. Select or clear the check box for any column you want to show or hide in the table.

     > **Tip:** Use the search box to quickly find a column name.

     The table updates based on your selection.

- Adjust column width:

  a. Roll over the header between two columns until the resize cursor appears.

     Click and drag the column width to the desired width.

     > **Tip:** To automatically resize a column to the width of its content, double-click the right side of the column header.

- To sort data in the table, click a column header.

  Tenable MSSP sorts all pages of the table by the data in the column you selected.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

- To sort data in the table by multiple columns, press **Shift** and click one or more column headers.

  > **Note:** Not all tables or columns support sorting by multiple columns.

  Tenable MSSP sorts all pages of the table in the order in which you selected the columns.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Log out of Tenable MSSP

Required Tenable Vulnerability Management User Role: Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

To log out of Tenable MSSP:

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

   The user account menu appears.

2. Click **Sign Out**.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Accounts

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

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

- View information about each account in the table:
  - **Name** — The account name.
  - **Custom Name** — Where applicable, the custom name of the account.
  - **Licenses Provisioned** — The number of licenses provisioned for the account.
  - **Licenses Limit** — The license limit for the account.
  - **Utilization %** — The percentage of licenses provisioned within the license limit.
  - **Licensed Apps** — The list of applications for which the account has subscriptions.
  - **Region** — The region in which the account resides.
  - **Logo** — Where applicable, the logo added to the account. For more information, see Logos.
  - **Notes** — Where applicable, notes about the account.
  - **Actions** — The list of actions that you can take:
    - **Assign Logo to Accounts** — Allows you to assign a logo to the customer accounts. For more information, see Assign a Logo to an Account.
    - **Detail** — Allows you to view the details of a customer account. For more information, see View Details for a Customer Account.
    - **Edit** — Allows you to edit a customer account. For more information, see Edit a Customer Account.
    - **Sign In** — Allows you to log in via SSO to an account. For more information, see Use Single Sign-On to Access a Customer Instance.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

- **Unlink** — Allows you to unlink an account from the accounts list. For more information, see Unlink an Account from the Tenable MSSP.

- Use the **Search** box to filter the customer accounts in the table:

  1. In the **Search** box, type the criteria by which you want to search the accounts table.
  2. Click the 🔎 button.

     Tenable MSSP filters the table by your search criteria.

- Use the **Filters** box to filter your search. For more information, see Filter a Table.
- Create an Eval Account
- Use Single Sign-On to Access a Customer Instance
- Assign a Logo to an Account
- Remove a Logo from an Account
- Edit a Customer Account

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Create an Eval Account

Required User Role: Administrator

In Tenable MSSP, you can create an eval account to give a customer 30 days of Tenable MSSP trial access.

Note: You might not see this if your evaluation account creation feature has upgraded to the new workflow. Refer to the updated the Create Evaluation Account page documentation for more information.

To create an eval account in Tenable MSSP:

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

   The left navigation plane appears.

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

   The **Accounts** page appears.

3. In the upper-right corner of the page, click ⊕ **Create Eval Account**.

   The **Create Eval Account** plane appears.

4. In the **Email** box, type the primary contact's email.

5. In the **Region** drop-down, select the region in which the eval account is used.

6. Click **Save**.

   Tenable MSSP saves the account. It can take up to 5 minutes for the account to activate within Tenable MSSP.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Create an Evaluation Account

Required User Role: Administrator

In Tenable MSSP, you can create an evaluation or trial account to give a customer 30 days of Tenable MSSP trial access.

To create an evaluation account in Tenable MSSP:

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

   The left navigation plane appears.

2. Click **Accounts**.

   The **Accounts** page appears.

3. In the upper-right corner of the page, click ⊕ **Create Evaluation Account**.

   The **Create Evaluation Account** window appears.

4. In the **Customer Name** box, type the name of the customer who requested the account. For example: <*customer_organization_name*>.

5. In the **Region** drop-down box, select the region in which the evaluation account is used.

6. In the **Admin Username** box, type the username for the evaluation account. Username is unique and must have this format: *customer@partner.com*.

7. In the **Contact Email** box, type the email address of the primary contact for this evaluation account designated by the Tenable MSSP partner.

   Note: The primary email address is populated by default and you can modify it as needed.

8. In the **Grant Access to** section, select at least one application to which you want to provide access for the evaluation account. Options available are:

   - Tenable Vulnerability Management
   - Tenable Web App Scanning

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

- Identity Exposure
- Tenable One
- Lumin Exposure View
- Tenable Attack Surface Management

> **Note**: When you select Tenable One, all applications are selected except Tenable Attack Surface Management.

9. Click **Save**.

   Tenable MSSP saves the account. It can take up to 5 minutes for the account to activate within Tenable MSSP.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

View Details for a Customer Account

Required User Role: Administrator

When creating support tickets for customer accounts, administrators must include the related customer account information. In the Tenable MSSP portal, you can view and copy these details to easily add them to support tickets.

To view details for a customer account in the Tenable MSSP:

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

   The left navigation plane appears.

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

   The **Accounts** page appears.

3. In the table, in the row for the account for which you want to view details, click the ⋮ button.

   A menu appears.

4. Click **Detail**.

   The **Account Details** plane appears and displays information about the customer account. For more information, see Account Details.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Account Details

On the **Account Details** plane, you can view the following information for a customer account:

Section	Action
Edit Account	• Click **Edit Account** to modify the customer account details. For more information, see Edit a Customer Account.
Client Data	• **Name** — The customer account name. • **Custom Name** — The custom name of the account. • **Region** — The region in which the account resides.
Logo	The logo of the customer account.
License Data	• **License Expiration Date** — The date on which the license for the customer account expires. • **Licensed Application** — The list of applications for which the account has subscriptions. • **Licenses Limit** — The license limit for the account. • **License Utilized** — The license utilization of the account. • **Utilization %** — The percentage of licenses provisioned within the license limit.
Scan Data	• **Running** — The number of running scans. • **Completed** — The number of completed scans. • **Aborted** — The number of aborted scans. • **Canceled** — The number of canceled scans.
Account Details For Support Ticket	• **Site** — The location where your container resides. • **Account UUID** — The container ID. • **Account Name** — The customer account name.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

	• **Account Admin Email** — The email address of the customer account administrator. • **LMS ID** — The customer ID. **Tip**: To copy the information, in the upper-right corner of the section, click the button.
Sign In	• Click **Sign In** to sign in to the Tenable Vulnerability Management interface. For more information, see Use Single Sign-On to Access a Customer Instance.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Edit a Customer Account

Required User Role: Administrator

To edit a customer account in the Tenable MSSP:

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

   The left navigation plane appears.

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

   The **Accounts** page appears.

3. In the table, in the row for the account you want to edit, click the ⋮ button.

   A menu appears.

4. Click **Edit**.

   The **Edit Account** plane appears.

5. (Optional) In the **Custom Name** box, type a descriptive name for the account. Any changes to the custom name are recorded in the **Custom Name Update History** table at the bottom of the plane.

6. (Optional) In the **Notes** box, type any notes you want to make about the account.

7. Click **Submit**.

   Tenable MSSP saves your changes to the account.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Assign a Logo to an Account

Required User Role: Administrator

Before you begin:

- Add a Logo

To assign a logo to a customer account in the Tenable MSSP:

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

   The left navigation plane appears.

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

   The **Accounts** page appears.

3. Do one of the following:

   - In the table, in the row for the account to which you want to assign a logo, click the ⋮ button.

     A menu appears.

   - Select the check box(es) next to the account(s) to which you want to assign a logo.

     A **Selected** bar appears at the top of the page.

4. Click ☆ **Assign Logo to Accounts**.

   The **Assign Logo to Accounts** plane appears.

5. In the **Logo** drop-down box, select the logo you want to assign to the selected account(s).

6. Click **Save**.

   A **Logo assigned to all selected accounts** confirmation message appears, and the Tenable MSSP assigns the logo to the appropriate customer Tenable Vulnerability Management accounts.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Remove a Logo from an Account

Required User Role: Administrator

To remove a logo from an account in the Tenable MSSP:

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

   The left navigation plane appears.

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

   The **Accounts** page appears.

3. Do one of the following:

   - In the table, in the row for the account to which you want to assign a logo, click the ⋮ button.

     A menu appears.

   - Select the check box(es) next to the account(s) to which you want to assign a logo.

     A **Selected** bar appears at the top of the page.

4. Click ☆ **Assign Logo to Accounts**.

   The **Assign Logo to Accounts** plane appears.

5. In the **Logo** drop-down box, select **(No Logo)**.

6. Click **Save**.

   A **Logo assigned to all selected accounts** confirmation message appears, and the Tenable MSSP removes the logo from the appropriate accounts.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Unlink an Account from the Tenable MSSP

Required User Role: Administrator

To unlink a customer account from the Tenable MSSP:

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

   The left navigation plane appears.

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

   The **Accounts** page appears.

3. Do one of the following:

   - In the table, in the row for the account you want to unlink, click the ⋮ button.

     A menu appears.

   - Select the check box(es) next to the account(s) you want to unlink.

     A **Selected** bar appears at the top of the page.

4. Click **Unlink**.

   A confirmation message appears.

5. Click **Unlink**.

   An **Account Unlinked** message appears and Tenable MSSP unlinks the account from the Tenable MSSP.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Add Resource Links

Resource links are URLs of tools and services that you want your Tenable Vulnerability Management user accounts to access. Tenable MSSP allows you to add Resource Links to your accounts, which are accessible to your user accounts from the Tenable MSSP portal.

To add resource links:

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

   The left navigation plane appears.

2. Click **Accounts**.

   The **Accounts** page appears.

3. Do one of the following:

Scope	Action
To add resource links to multiple accounts	In the accounts table, do the following: 1. Select one or more accounts for which you want to add resource links. Tenable MSSP enables **Add Resource Links** in the action bar. 2. Click **Add Resource Links**. The **Add Resource Links** window appears.
To add resource links to a single account	1. Do one of the following: • Select the check box next to the account for which you want to add resource links. Tenable MSSP enables **More** > **Add Resource Links** in the action bar. • In the row of the account for which you want to add resource links, click the ⋮ button.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

	The action options appear in the row. • Right-click the account for which you want to add resource links. • The action options appear in the row. 2. Click **Add Resource Links**. The **Add Resource Links** window appears.

4. Click **Add**.
5. Provide the following information:
    a. In the **Resource Name** box, type a name for the URL.
    b. In the **Resource Link** box, type the URL (`http://` or `https://`) that you want to add as a resource link.
    c. Click **Add** to add more resource links.
6. Click **Save**.

    Tenable MSSP adds your resource links and the accounts to which these resource links are added can now view them from the **Resource Center** > **My Links** section. To access **Resource Center** in your Tenable Vulnerability Management account, in the upper-right corner, click the ⓘ icon.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Modify Resource Links

You can modify a resource link or add new resource links to an account.

To modify resource links:

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

   The left navigation plane appears.

2. Click **Accounts**.

   The **Accounts** page appears.

3. Edit the account for which you want to modify the resource links:

   - Do one of the following:

     - Select the check box next to the account for which you want to add the resource link.

       Tenable MSSP enables **More** > **Edit** in the action bar.

     - In the row of the account for which you want to add the resource link, click the ⋮ button.

       The action options appear in the row.

     - Right-click the account for which you want to add the resource link.

     - The action options appear in the row.

4. Click **Edit**.

   The **Edit Account** window appears.

5. In the left pane, click **Resource Links**.

   The **Resource Links** page appears.

6. Modify the resource links as needed.

7. (Optional) Click **Add** to add additional resource links.

8. Click **Save**.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Tenable MSSP saves the list and the modified resource links appear in the **My Links** section in **Resource Center** of the customer account.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Remove Resource Links

You can remove resource links that are no longer needed.

To remove resource links:

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

   The left navigation plane appears.

2. Click **Accounts**.

   The **Accounts** page appears.

3. Edit the account from which you want to remove the resource links:

   - Do one of the following:

     - Select the check box next to the account from which you want to remove the resource link.

       Tenable MSSP enables **More** > **Edit** in the action bar.

     - In the row of the account from which you want to remove the resource link, click the ⋮ button.

       The action options appear in the row.

     - Right-click the account from which you want to remove the resource link.

     - The action options appear in the row.

4. Click **Edit**.

   The **Edit Account** window appears.

5. In the left pane, click **Resource Links**.

   The **Resource Links** page appears.

6. To remove a resource link, click ✕ next to the resource link that you want to remove.

   Tenable MSSP removes the resource link from the list.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

7. Click **Save**.

   Tenable MSSP removes the resource link and saves **Resource Links** list.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Filter a Table

Use the **Filters** box in the **Accounts** page to filter the accounts in your table.

To filter the **Accounts** table:

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

   The left navigation plane appears.

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

   The **Accounts** page appears.

3. Next to **Filters**, click the ⌄ button.

   The filter settings appear.

4. In the **Match** drop-down box, select one of the following:

   - **Match Any** — View results that match any of the filters you create.
   - **Match All** — View results that match all the filters you create.

5. In the **Select Category** drop-down box, select an attribute.

   For example, in Tenable MSSP, you might select **Account** if filtering customer accounts or **Licenses Utilized** if filtering the number of licenses utilized.

6. In the **Select Operator** drop-down box, select an operator.

   Note: When using the **contains** or **does not contain** operators, use the following best practices:

   - For the most accurate and complete search results, use full words in your search value.
   - Do not use periods in your search value.
   - Where applicable, Tenable recommends using the **contains** or **does not contain** instead of the **is equal to** or **is not equal to** operators.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

7. In the **Select Value** box, do one of the following:

Value Type	Action
Text	Type the value on which you want to filter. An example of the expected input is present in the box until you start typing. If what you type is invalid for the attribute, a red outline appears around the text box.
Single valid value	If a default value is associated with the attribute, Tenable MSSP selects the default value automatically. To change the default value, or if there is no associated default value: a. Click the box to display the drop-down list. b. Search for and select one of the listed values.
Multiple valid values	To select one or more values: a. Click the box to display the drop-down list. b. Search for and select a value. The selected value appears in the box. c. Repeat until you have selected all appropriate values d. Click outside the drop-down list to close it. To deselect values: a. Roll over the value you want to remove. The ✕ button appears over the value. b. Click the ✕ button. The value disappears from the box.

8. (Optional) In the lower-right corner of the filter section:

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

- To add another filter, click **Add**.
- To clear all filters, click **Reset Filters**.

9. Click **Apply**.

   Tenable MSSP applies your filter or filters to the table.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Domains

Required User Role: Administrator

A primary domain is associated with an account when you initially create an account. You can create multiple secondary domains that you can associate with your partner Tenable Vulnerability Management accounts, which allows you to track and manage your Tenable Vulnerability Management accounts.

The free version of Tenable Attack Surface Management uses the data from the primary domains to populate its Attack Surface Management (ASM) data. Any domain that you set as primary cannot be disabled. This ensures that you do not delete that domain by mistake.

For more information about creating secondary domains, see the following:

- View Domains
- Add a Secondary Domain
- Change a Domain to Primary or Secondary
- Disable a Domain
- Enable a Domain

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

View Domains

Required User Role: Administrator

To view the associated primary and secondary domains for an account, do the following:

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

   The left navigation plane appears.

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

   The **Accounts** page appears.

3. To view the domains for an account, do one of the following:

   - In the table, in the row for the account for which you want to view the list of associated domains, click the ⋮ button.

     A menu appears.

   - Select the check box next to the account for which you want to view the associated domains.

     Tenable MSSP enables the **More** > **Edit** option in the action bar.

4. Click **Edit**.

   The **Edit Account** page appears.

5. On the left pane, click **Domains**.

   The **Domains** page appears with the list of primary and secondary domains for the account.

The Domains table shows the following details:

Column	Description
Domain name	The name of the domain.
Status	The status of the domain, whether **Active** or **Disabled**.
Date Added	The date on which the domain was created.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Actions	The following actions are available for a domain: • **Set as Primary** (for secondary domains) • **Set as Secondary** (for primary domains) • **Disable**

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Add a Secondary Domain to your Account

Required User Role: Administrator

You can add a secondary domain and associate it with your Tenable Vulnerability Management accounts. For security purposes, Tenable allows usernames to be created only under approved domains. After you add a secondary domain, you can create a username under that domain.

Note: Tenable MSSP does not allow personal or free email addresses, such as Gmail, Hotmail, Yahoo, and so on, as secondary domains.

To add a secondary domain to a customer account:

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

   The left navigation plane appears.

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

   The **Accounts** page appears.

3. To edit an account, do one of the following:

   - In the table, in the row for the account for which you want to add a domain, click the ⋮ button.

     A menu appears.

   - Select the check box next to the account for which you want to add a domain.

     Tenable MSSP enables the **More** > **Edit** option in the action bar.

4. Click ✎ **Edit**.

   The **Edit Account** page appears.

5. On the left pane, click **Domains**.

   The **Domains** page appears.

6. Click ⊕ **Add Domain**.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

The **Add Domain** window appears.

7. In the **Domain Name** box, type the domain name.
8. In the **Verification Email** box, type the email address to which you want to receive the verification email.
9. Click **Verify Domain**.

   Tenable MSSP sends a verification email with an activation code to the email address specified.
10. In the **Activation Code** box, type the activation code.

    > **Note**: Activation code expires after a period of 24 hours. To resend the activation code, click **Resend the code**.

11. Click **Activate Domain**.

    Tenable MSSP adds the new domain to the **Domains** page and displays a confirmation message.

    > **Note**: If you click **Cancel** on the **Activate Domain** window, Tenable MSSP still adds the new domain to the **Domains** page and shows the status as **Activation Pending**. To activate the domain, in the **Actions** column of the domain, click the ⋮ button, then select **Activate Domain**.

12. Click **Save**.

    Tenable MSSP saves your changes to the account.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Set a Domain as Primary or Secondary

Required User Role: Administrator

You can change a secondary domain to primary or a primary domain to a secondary domain. Tenable MSSP creates the primary domain when you initially create the account. To change the domain to primary or secondary, the domain must be in the active state.

Note: It is not mandatory to have a primary domain. All domains can be secondary domains.

To change a domain to secondary or primary, do the following:

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

   The left navigation plane appears.

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

   The **Accounts** page appears.

3. To edit an account, do one of the following:

   - In the table, in the row for the account for which you want to change the domain, click the ⋮ button.

     A menu appears.

   - Select the check box next to the account for which you want to change the domain.

     Tenable MSSP enables the **More** > **Edit** option in the action bar.

4. Click **Edit**.

   The **Edit Account** page appears.

5. On the left pane, click **Domains**.

   The **Domains** page appears.

6. In the **Domains** window, hover over the domain you want to change and click the ⋮ button.

   The action options appear in the row.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

7. Click **Set as Primary** or **Set as Secondary**, as needed.

   Tenable MSSP sets the selected domain as the primary or secondary domain.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Disable a Domain

Required User Role: Administrator

You can disable a domain that you no longer require.

To disable a domain:

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

   The left navigation plane appears.

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

   The **Accounts** page appears.

3. To disable the domain for an account, do one of the following:

   - In the table, in the row for the account for which you want to disable a domain, click the ⋮ button.

     A menu appears.

   - Select the check box next to the account for which you want to disable a domain.

     Tenable MSSP enables the **More** > **Edit** option in the action bar.

4. Click **Edit**.

   The **Edit Account** page appears.

5. On the left pane, click **Domains**.

   The **Domains** page appears.

6. In the **Domains** window, hover over the domain you want to disable and click the ⋮ button.

   The action options appear in the row.

7. Click **Disable**.

   Tenable MSSP disables the selected domain.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Enable a Domain

Required User Role: Administrator

You can enable a domain that is in the disabled state.

To activate a domain:

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

   The left navigation plane appears.

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

   The **Accounts** page appears.

3. To activate the domain for an account, do one of the following:

   - In the table, in the row for the account for which you want to activate a domain, click the ⋮ button.

     A menu appears.

   - Select the check box next to the account for which you want to activate a domain.

     Tenable MSSP enables the **More** > **Edit** option in the action bar.

4. Click **Edit**.

   The **Edit Account** page appears.

5. On the left pane, click **Domains**.

   The **Domains** page appears.

6. In the **Domains** window, hover over the domain you want to activate and click the ⋮ button.

   The action options appear in the row.

7. Click **Enable**.

   Tenable MSSP activates the selected domain.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Scans

The **Scans** page in the Tenable MSSP displays a high-level overview of the scan status for each customer account that have completed scans. You can customize the scan table and drill down to view the scan details of an account.

To access the **Scans** page in Tenable MSSP, in the left navigation plane, click **Scans**. For more information, see View Scans.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

View Scans

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

- View information about completed scans:
  - **Account** — The account name associated with the scan.
  - **Last Completed Scan — Assets Scanned (% Successful)** — The number of assets scanned during the last scan and percentage of successfully scanned assets.

    > **Note**: If this column shows a value of 0 (0%), it indicates that the corresponding scan is older than 35 days and is in the archived state.

  - **Last 90 days — Scan Count (% Successful)** — The number of Tenable Nessus and Tenable Nessus Agent scans within the last 90 days and the percentage of successful scans.
  - **Authenticated Scan Coverage** — The coverage percentage of authenticated scans. You can create authenticated scans, also known as credentialed scans, by adding access credentials to your assessment scan configuration.
- To view the scan details of an account:
  - In the table, click on a scan for which you want to view details.

    The **Scan Details** pane appears. The **Scan Details** pane displays details of the last completed scan, scans run in the last 90 days, and the scan coverage for authenticated and unauthenticated scans.
- Use the **Search** box to filter the scans in the table:
  1. In the **Search** box, type the criteria by which you want to search the scans table.
  2. Click the 🔍 button.

     Tenable MSSP filters the table by your search criteria.
- Customize the table. For more information, see Interact with an Tenable MSSP Table.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Logos

By default, the Tenable logo appears in the header of your customer's Tenable Vulnerability Management instances. In Tenable MSSP, you can replace the Tenable logo with a logo appropriate to a customer's business context. You can assign individual logos to each customer account.

To access the **Logos** page in Tenable MSSP, in the left navigation plane, click **Logos**.

The **Logos** page lists all logos available for use in Tenable MSSP.

> **Note:** Due to the white background of the user interface, light colored logos with transparent backgrounds may be difficult to view in the table on the **Logos** page.

On the **Logos** page, you can:

- Add a Logo
- Edit a Logo
- Delete a Logo

> **Note:** You can Assign a Logo to an Account or Remove a Logo from an Account via the **Accounts** page.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Add a Logo

Required User Role: Administrator

To add a logo in the Tenable MSSP:

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

   The left navigation plane appears.

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

   The **Logos** page appears.

3. Click ⊕ **Add Logo**.

   The **Add Logo** plane appears.

4. In the **Name** box, type a name for the logo.

5. Click **Add File**.

   Your file manager appears.

6. Select the .png file you want to upload.

   Note: The Tenable MSSP does not accept any .png files larger than 246 x 52 pixels.

7. Click **Save**.

   A **Logo created successfully** message appears, and the Tenable MSSP adds the logo to the table on the **Logos** page.

   Note: Due to the white background of the user interface, light colored logos with transparent backgrounds may be difficult to view in the table on the **Logos** page.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Edit a Logo

Required User Role: Administrator

To edit a logo in the Tenable MSSP:

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

   The left navigation plane appears.

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

   The **Logos** page appears.

3. In the table, in the row for the logo you want to edit, click the ⋮ button.

   A menu appears.

4. Click **Edit**.

   The **Edit Logo** plane appears.

5. (Optional) Edit the logo name.

6. (Optional) Upload a different .png file:

   a. Next to the .png file, click the ✕ button.

   b. Click **Add File**.

      Your file manager appears.

   c. Select the .png file you want to upload.

      Note: The Tenable MSSP does not accept any .png files larger than 246 x 52 pixels.

7. Click **Save**.

   A **Logo changes saved successfully** message appears, and the Tenable MSSP updates the logo.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Delete a Logo

Required User Role: Administrator

To delete a logo in the Tenable MSSP:

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

   The left navigation plane appears.

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

   The **Logos** page appears.

3. In the table, in the row for the logo you want to delete, click the ⋮ button.

   A menu appears.

4. Click **Delete**.

   A confirmation message appears.

5. Click **Delete**.

   The Tenable MSSP deletes the logo and removes it from any accounts to which it was applied.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Users

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

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

The **Users** page displays a table of all Tenable MSSP 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 MSSP User
- Assign a Tenable MSSP User to an Account
- Remove a Tenable MSSP User from an Account
- Edit a Tenable MSSP User
- Generate API Keys for another Tenable MSSP User
- Disable a Tenable MSSP User
- Enable a Tenable MSSP User
- Delete a Tenable MSSP User

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Create a Tenable MSSP User

Required User Role: Administrator

A Tenable MSSP user can manage customer accounts and access Tenable Vulnerability Management customer instances.

To create a user in Tenable MSSP:

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** page 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 follow the format: *name@domain*, where *domain* corresponds to a domain approved for your Tenable MSSP instance.

   During initial setup, Tenable configures approved domains for your Tenable MSSP 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 contain at least 8 characters and at least three of the following:

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

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

8. In the **Verify Password** box, re-type the password.
9. 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.

10. In the **Authentication** section, select or deselect the available security setting options as required:

    - **API** — Allows the user to generate API keys.

      > **Tip**: You can select only this setting to create an API-only user account.

    - **SAML** — Allows the user to log in to their account using a SAML single sign-on (SSO).
    - **Username/Password** — Allows the user to log in to their account using a username and password.

      > **Note**: If you deselect this option, you cannot select the **Two-Factor** option.

    - **Two-Factor Required** — Requires the user to provide two-factor authentication to log in to their account.

11. (Optional) Assign the user to one or more accounts.
12. Click **Create**.

    Tenable MSSP saves the user and assigns them to the specified accounts. The **Users** page appears and you can view the new user listed in the users table.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Assign a Tenable MSSP User to an Account

Required User Role: Administrator

In Tenable MSSP, you can assign newly created users or existing users to one or more accounts. This allows you to control user access based on your business needs. For example, you may want to allow administrators or supervisors to access all accounts, while limiting the accounts to which an analyst has access based on their geographical location or their market specialization.

Note: You can only assign non-administrator users to accounts.

To assign a Tenable MSSP user to an account:

1. Do one of the following:

   - Create a user.

     The **Create User** page appears.

   - Edit an existing user.

     The **Edit User** page appears.

2. In the left panel, click the **Accounts** tab.

   The **Accounts** page appears, which displays a list of all accounts to which the user is assigned.

3. In the top right corner of the page, click the ⊕ **Assign Accounts** button.

   The **Assign Accounts** panel appears.

4. Select the check box(es) next to the account or Accounts to which you want to assign the user.

5. Click **Save**.

   Upon saving the user or changes to the user, Tenable MSSP assigns the user to the designated account(s).

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Remove a Tenable MSSP User from an Account

Once a user is assigned to an account, you can remove the user from the account at any time.

To remove a Tenable MSSP user from an account:

1. Edit an existing user.

   The **Edit User** page appears.

2. In the left panel, click the **Accounts** tab.

   The **Accounts** page appears, which displays a list of all accounts to which the user is assigned.

3. In the users table, roll over the account(s) from which you want to remove the user.

   The action buttons appear in the row.

4. In the row, click the ✕ button.

5. Click **Save**.

   The Tenable MSSP removes the user from the designated account(s).

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Edit a Tenable MSSP User

Required User Role: Administrator

To edit a user in Tenable MSSP:

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) In the **Authentication** section, select or deselect the available security setting options as required:

   - **API** — Allows the user to generate API keys.

     Tip: You can select only this setting to create an API-only user account.

   - **SAML** — Allows the user to log in to their account using a SAML single sign-on (SSO).

   - **Username/Password** — Allows the user to log in to their account using a username and password.

     Note: If you deselect this option, you cannot select the **Two-Factor** option.

   - **Two-Factor Required** — Requires the user to provide two-factor authentication to log in to their account.

6. (Optional) Assign the user to one or more accounts.

7. (Optional) If the user has one or more assigned accounts, unassign the user from the accounts.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

8. (Optional) Generate API keys for the user.
9. Click **Save**.

   Tenable MSSP saves the changes for the user.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Generate API Keys for another Tenable MSSP User

Required User Role: Administrator

Administrators can generate API keys for any Tenable MSSP user.

To generate API keys for another user in Tenable MSSP:

1. Edit a user.

   The **Edit User** plane appears.

2. In the left navigation plane, click the **API Keys** tab.

   The **API Keys** options appear.

3. 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.

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

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

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Disable a Tenable MSSP User

Required User Role: Administrator

Disabling a user account prevents the user from logging in to Tenable MSSP. You can enable a disabled user account as described in Enable a Tenable MSSP User.

To disable a user in Tenable MSSP:

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, in the row of the user you want to disable, click the ⋮ button.

   A menu appears.

4. Click ⊘ **Disable**.

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

5. Click **Disable**.

6. Click **Continue**.

   A success message appears.

   Tenable MSSP 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.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Enable a Tenable MSSP 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 Tenable MSSP:

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, in the row of the user you want to enable, click the ⋮ button.

   A menu appears.

4. Click ✓ **Enable**.

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

5. Click **Enable**.

6. Click **Continue**.

   A success message appears.

   Tenable MSSP enables the user account.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Delete a Tenable MSSP 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 (**Created By** value displays as **null**)
Tags	No	Retained (**Created By** value displays as **null**)
Recast/Accept Rules	No	Retained (**Owner** value displays as **Unknown User**)
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:

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Users** tile.

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

4. On the **Users** page, in the users table, in the row of the user you want to delete, click the ⋮ button.

   A menu appears.

5. Click 🗑 **Delete**.

   > **Note**: If a user is not disabled, then the 🗑 button does not appear. Disable the user before deleting them.

   The delete plane appears.

6. In the 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**.

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

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Instances

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

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

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Use Single Sign-On to Access a Customer Instance

Required Tenable Vulnerability Management User Role: Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

To sign in to a customer's Tenable Vulnerability Management instance in Tenable MSSP:

1. On the **Accounts** page, in the table, in the row for the customer account to which you want to sign in, click the ⋮ button.

   A menu appears.

2. Click **Sign In**.

3. If the customer has more than one domain associated with their instance, in the **Choose a Domain** window, select the domain you want to log in to.

4. Click **Sign in**.

   Tenable MSSP loads the appropriate Tenable Vulnerability Management interface according to the customer's licenses. For example, if the account is licensed for Tenable Web App Scanning only, the Tenable Web App Scanning interface appears.

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

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

   For more information about navigating Tenable Vulnerability Management interfaces, see the Tenable Vulnerability Management User Guide

To return to Tenable MSSP:

- From the new Tenable Vulnerability Management interface:

  1. At the top of any page, in the blue Tenable MSSP overlay, click ×.

     Tenable MSSP appears.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

- From the classic Tenable Vulnerability Management interface:

    1. In the upper-right corner of the top navigation bar, click the Tenable Vulnerability Management username.
    2. Click **Leave User**.

       Tenable MSSP appears.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.