# Tenable OT Security 4.6 Benutzerhandbuch

Letzte Überarbeitung: 11. Mai 2026

# Inhalt

# Willkommen bei Tenable OT Security

Tenable OT Security (OT Security) (vormals Tenable.ot) schützt industrielle Netzwerke vor Cyberbedrohungen, böswilligen Insidern und menschlichen Fehlern. Von der Erkennung und Eindämmung von Bedrohungen bis hin zu Asset-Verfolgung, Schwachstellen-Management, Konfigurationskontrolle und Active Query-Überprüfungen – die ICS-Sicherheitsfunktionen von OT Security maximieren die Transparenz, Sicherheit und Kontrolle Ihrer Betriebsumgebung.

OT Security bietet umfassende Sicherheitstools und Berichte für IT-Sicherheitspersonal und OT-Ingenieure. Es bietet einen Einblick in konvergente IT/OT-Segmente und ICS-Aktivitäten und macht auf Situationen an allen Sites und bei ihren jeweiligen OT-Assets aufmerksam – von Windows-Servern bis hin zu SPS-Backplanes – in einer zentralen, einheitlichen Ansicht.

OT Security weist die folgenden wichtigen Leistungsmerkmale auf:

- 360-Grad-Sichtbarkeit – Angriffe können sich in einer IT/OT-Infrastruktur leicht ausbreiten. Mit einer einzigen Plattform zur Verwaltung und Messung des Cyberrisikos für Ihre OT- und IT-Systeme erhalten Sie einen vollständigen Einblick in Ihre konvergente Angriffsoberfläche. OT Security lässt sich auch nativ in IT-Sicherheits- und Betriebstools integrieren, wie z. B. Ihre Security Information and Event Management (SIEM)-Lösung, Protokollverwaltungstools, Next-Generation-Firewalls und Ticketing-Systeme. Zusammen entsteht dadurch ein Ökosystem, in dem all Ihre Sicherheitsprodukte als Einheit zusammenarbeiten können, um Ihre Umgebung zu schützen.
- Bedrohungserkennung und -entschärfung – OT Security nutzt eine Multi-Detection Engine, um hochriskante Ereignisse und Verhaltensweisen zu finden, die sich auf den OT-Betrieb auswirken können. Diese Engines umfassen richtlinien-, verhaltens- und signaturbasierte Erkennung.

- Asset-Inventarisierung und aktive Erkennung – OT Security nutzt patentierte Technologie und bietet einen Einblick in Ihre Infrastruktur – nicht nur auf Netzwerkebene, sondern bis hinunter auf die Geräteebene. Es verwendet native Kommunikationsprotokolle, um sowohl IT- als auch OT-Geräte in Ihrer ICS-Umgebung abzufragen und alle Aktivitäten und Aktionen zu identifizieren, die in Ihrem Netzwerk ausgeführt werden.
- Risikobasiertes Schwachstellen-Management – Auf der Grundlage umfassender und detaillierter Funktionen zur Verfolgung von IT- und OT- Assets generiert OT Security mithilfe von Predictive Prioritization Schwachstellen- und Risikostufen für jedes Asset in Ihrem ICS-Netzwerk (Industrial Control Systems, industrielle Steuerungssysteme). Diese Berichte enthalten Risikobewertungen und detaillierte Einblicke sowie Vorschläge zur Risikominderung.
- Konfigurationskontrolle – OT Security bietet einen detaillierten Verlauf der Änderungen an der Gerätekonfiguration im Zeitverlauf, einschließlich spezifischer Kontaktplan-Segmente, Diagnosepuffer, Tag-Tabellen und mehr. Auf diese Weise können Administratoren einen Backup-Snapshot mit dem „letzten als funktionierend bekannten Zustand“ für eine schnellere Wiederherstellung und Einhaltung von Branchenvorschriften erstellen.

> Tipp: Das *Tenable OT Security-Benutzerhandbuch* und die Benutzeroberfläche sind auf Englisch, Japanisch, Deutsch, Französisch und vereinfachtem Chinesisch verfügbar. Informationen zum Ändern der Sprache der Benutzeroberfläche finden Sie unter Lokale Einstellungen.

Weitere Informationen zu Tenable OT Security finden Sie in den folgenden Materialien für Kundenschulungen:

- Einführung in Tenable OT Security (Tenable University)

## Erste Schritte mit OT Security

Befolgen Sie die unter Erste Schritte mit OT Security genannten Schritte, um mit OT Security zu beginnen.

# OT Security-Technologien

Die umfassende OT Security-Lösung umfasst zwei zentrale Erfassungstechnologien:

- Netzwerkerkennung – Die Netzwerkerkennungstechnologie von OT Security ist eine passive Deep-Packet Inspection Engine, die für die einzigartigen Eigenschaften und Anforderungen industrieller Steuerungssysteme entwickelt wurde. Die Netzwerkerkennung bietet detaillierte Echtzeit-Einblicke in alle Aktivitäten, die über das Betriebsnetzwerk durchgeführt werden, mit einem einzigartigen Fokus auf Engineering-Aktivitäten. Dazu gehören Firmware-Downloads/-Uploads, Code-Updates und Konfigurationsänderungen, die über proprietäre, anbieterspezifische Kommunikationsprotokolle stattfinden. Die Netzwerkerkennung warnt in Echtzeit vor verdächtigen/nicht autorisierten Aktivitäten und erstellt ein umfassendes Ereignisprotokoll mit forensischen Daten. Die Netzwerkerkennung generiert drei Arten von Warnungen:

    - Richtlinienbasiert – Sie können vordefinierte Richtlinien aktivieren oder benutzerdefinierte Richtlinien erstellen, die bestimmte granulare Aktivitäten, die auf Cyberbedrohungen oder Betriebsfehler hinweisen, auf die Zulassungsliste und/oder Sperrliste setzen, um Warnungen auszulösen. Es können auch Richtlinien festgelegt werden, um Prüfungen aktiver Abfragen für vordefinierte Situationen auszulösen.

    - Verhaltensanomalien – Das System erkennt Abweichungen von einer Baseline für den Netzwerk-Traffic, die basierend auf Traffic-Mustern während eines bestimmten Zeitraums festgelegt wurde. Außerdem erkennt es verdächtige Scans, die auf Malware und Auskundschaftsverhalten hinweisen.

    - Signaturerkennungsrichtlinien – Diese Richtlinien verwenden signaturbasierte OT- und IT-Bedrohungserkennung, um Netzwerk-Traffic zu identifizieren, der auf Bedrohungen durch Eindringlinge hinweist. Die Erkennung basiert auf Regeln, die in der Threats-Engine von Suricata katalogisiert wurden.

- Aktive Abfrage – Die patentierte Abfragetechnologie von OT Security überwacht Geräte im Netzwerk, indem sie regelmäßig die Metadaten von Kontrollgeräten im ICS-Netzwerk abfragt. Diese Funktionalität verbessert die Fähigkeit von OT Security, alle ICS-Ressourcen, einschließlich untergeordneter Geräte wie SPS und RTUs, automatisch zu erkennen und zu klassifizieren, selbst wenn sie nicht im Netzwerk aktiv sind. Sie identifiziert außerdem lokal implementierte Änderungen in den Metadaten des Geräts (z. B. Firmware-Version, Konfigurationsdetails und Status) sowie Änderungen in jedem Code-/Funktionsblock der Gerätelogik. Da sie schreibgeschützte Abfragen in den nativen Controller-Kommunikationsprotokollen verwendet, ist sie sicher und hat keine Auswirkungen auf die Geräte. Abfragen können regelmäßig nach einem vordefinierten Zeitplan oder nach Bedarf durch den Benutzer ausgeführt werden.

# Lösungsarchitektur

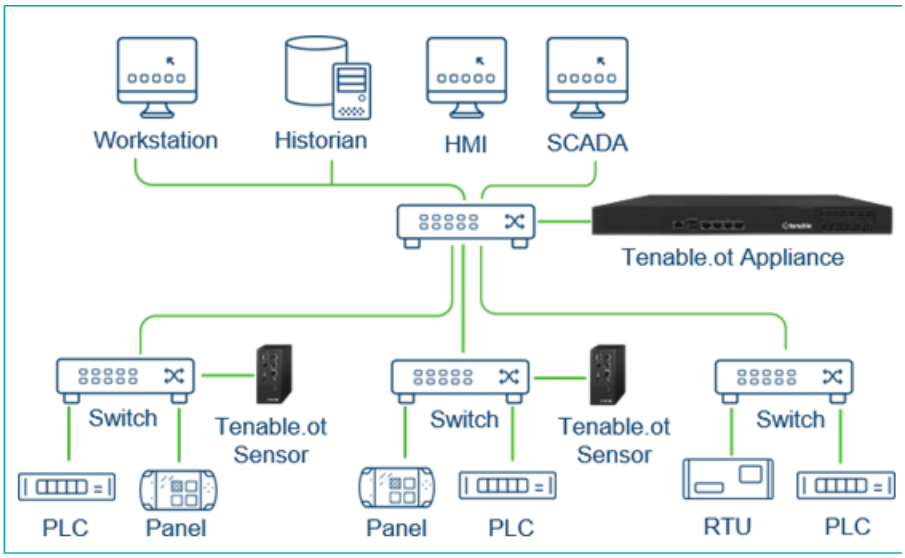
## Komponenten der OT Security-Plattform

> Hinweis: In diesem Dokument wird die OT Security Appliance als ICP (Industrial Core Platform) bezeichnet.

Die OT Security-Lösung setzt sich aus diesen Komponenten zusammen:

- ICP (**OT Security** Appliance) – Diese Komponente erfasst und analysiert den Netzwerk-Traffic direkt aus dem Netzwerk (über einen Span-Port oder Netzwerk-Tap) und/oder mithilfe eines Datenfeeds vom Tenable OT Security Sensor (OT Security Sensor). Die ICP-Appliance führt sowohl die Netzwerkerkennung als auch aktive Abfragen aus.
- **OT Security** Sensoren – Hierbei handelt es sich um kleine Geräte, die in Netzwerksegmenten von Interesse bereitgestellt werden, bis zu einem Sensor pro Managed Switch. OT Security Sensoren bieten einen vollständigen Einblick in diese Netzwerksegmente, indem sie den

gesamten Traffic erfassen, die Daten komprimieren und die Informationen dann an die OT Security Appliance übermitteln. Sie können Sensoren der Version 3.14 und höher auch so konfigurieren, dass sie aktive Abfragen an die Netzwerksegmente senden, in denen sie bereitgestellt werden.




## Netzwerkkomponenten

OT Security unterstützt die Interaktion mit den folgenden Netzwerkkomponenten:

- OT Security-Benutzer (Verwaltung) – Sie können Benutzerkonten erstellen, um den Zugriff auf die OT Security-Verwaltungskonsole zu steuern. Sie können mit einem Browser (Google Chrome) über Secure Socket-Layer-Authentifizierung (HTTPS) auf die Verwaltungskonsole zugreifen.

> Hinweis: Der Zugriff auf die OT Security-Benutzeroberfläche ist nur mit der neuesten Version von Chrome möglich.

- Active Directory-Server – Die Zugangsdaten der Benutzer können optional über einen LDAP-Server wie beispielsweise Active Directory zugewiesen werden. In diesem Fall werden die Benutzerrechte in Active Directory verwaltet.

- SIEM – Senden Sie OT Security-Ereignisprotokolle mithilfe des Syslog-Protokolls an ein SIEM-System.
- SMTP-Server – OT Security sendet Ereignisbenachrichtigungen per E-Mail über einen SMTP-Server an bestimmte Mitarbeitergruppen.
- DNS-Server – Integrieren Sie DNS-Server in OT Security, um bei der Auflösung von Asset-Namen zu helfen.
- Anwendungen von Drittanbietern – Externe Anwendungen können mit OT Security über dessen REST-API interagieren oder über andere spezifische Integrationen auf Daten zugreifen[1].

[1]Beispielsweise unterstützt OT Security die Integration mit Palo Alto Networks Next Generation Firewall (NGFW) und Aruba ClearPass, wodurch OT Security Asset-Inventarisierungsdaten mit diesen Systemen austauschen kann. OT Security kann auch mit anderen Tenable-Plattformen wie Tenable Vulnerability Management und Tenable Security Center integriert werden. Integrationen werden unter Lokale Einstellungen > Integrationen konfiguriert, siehe Integrationen.

# Tenable OT Security – Hardwarespezifikationen

## ICP- und Sensorspezifikationen

Im Folgenden finden Sie die Spezifikationen für die OT Security Hardware-Appliances für die Industrial Core Platform (ICP):

### Reguläre ICP

| Kategorie | Reguläre ICP |
|---|---|
| **CPU** | Intel® Xeon™ D-218dIT, 2,0 GHz |
| **Kerne** | 14 |

| | |
|---|---|
| **RAM** | 64 GB |
| **Speicher** | 256 GB SSD<br>800 GB NVMe<br>2 TB HDD |
| **Netzwerk (Kupfer-Ethernet)** | 4 x 1 Gbit/s |
| **Netzwerk (Glasfaser-Ethernet)** | N/A |
| **Stromversorgung** | 110-220 V, einphasig |
| **Formfaktor** | 1 HE, halbe Tiefe |
| **Abmessungen (LxBxH)** | 209 x 43 x 376 mm<br>8,2 x 1,7 x 14,8 in |
| **Gewicht** | 3,6 kg |
| **Betriebstemperatur** | 5 bis 45 °C (41 bis 113 °F) |
| **Relative Luftfeuchtigkeit** | 8 % bis 90 %, nicht kondensierend |
| **Max. SPAN-Durchsatz** | 500 Mbit/s |

XL-ICP

| Kategorie | XL-ICP |
|---|---|
| **CPU** | 2 x Xeon® Silver 4314 |
| **Kerne** | 2 x 16 |
| **RAM** | 256 GB |

| | |
|---|---|
| **Speicher** | 960 GB SSD SAS FIPS-140 SED<br><br>960 GB SSD SAS FIPS-140 SED<br><br>2 x 2,4 TB SAS HDD FIPS-140 SED<br><br>> Hinweis: Die Hardware unterstützt eine vollständige Verschlüsselung und ist FIPS-140-konform. |
| **Netzwerk (Kupfer)** | 6 x 1 Gbit/s |
| **Netzwerk (Glasfaser)** | 2 x 10 Gbit/s SFP+ |
| **Stromversorgung** | Redundant, 110-220 V, 165 W |
| **Formfaktor** | 1 HE, volle Tiefe |
| **Abmessungen (BxHxT)** | Breite*: 482,0 mm (18,98 in) x Höhe: 42,8 mm (1,69 in) x Tiefe*: 698 mm (27,5 in)<br><br>* Maße einschließlich Blende. |
| **Gewicht** | 22 kg |
| **Betriebstemperatur** | 0 bis 40 °C (32 bis 104 °F) |
| **Lagertemperatur** | -10 bis 50 °C (14 bis 122 °F) |
| **Relative Luftfeuchtigkeit** | 5 % bis 90 %, nicht kondensierend |
| **Zertifizierungen** | CE/FCC/RoHS<br><br>CB, CCC, UL, RCM, NOM |
| **Max. SPAN-Durchsatz** | 1 Gbit/s |

ICP-Mini

| Kategorie | ICP-Mini |
|---|---|
| **CPU** | Intel® Core™ i7-1185G7E, 1,8 GHz |
| **Kerne** | 4 |
| **RAM** | 32 GB |
| **Speicher** | 480 GB SSD |
| **Netzwerk (Kupfer)** | 4 x 2,5 Gbit/s |
| **Netzwerk (Glasfaser)** | N/A |
| **Stromversorgung** | Klemmleiste, 12-28 VDC |
| **Formfaktor** | DIN-Schiene |
| **Abmessungen (mm)** | 150 x 190 x 81 mm |
| **Gewicht** | 1,9 kg |
| **Betriebstemperatur** | 0 bis 40 °C (32 bis 104 °F) |
| **Lagertemperatur** | -10 bis 50 °C (14 bis 122 °F) |
| **Relative Luftfeuchtigkeit** | 10 % bis 95 %, nicht kondensierend |
| **Zertifizierung** | CE/FCC/RoHS, Klasse A<br><br>CB, CCC, UL, RCM, NOM |
| **Max. SPAN-Durchsatz** | 150 Mbit/s |

Sensor

| Kategorie | Sensor |
|---|---|

| | |
|---|---|
| **CPU** | Intel® Core™ 13-8145UE, 2,2 GHz |
| **Kerne** | 2 |
| **RAM** | 4 GB |
| **Speicher** | 128 GB SATA M.2 |
| **Netzwerk (Kupfer)** | 2 x 1 Gbit/s |
| **Netzwerk (Glasfaser)** | N/A |
| **Stromversorgung** | Klemmleiste, 12-28 VDC |
| **Formfaktor** | Extra kleiner Formfaktor (ESFF) |
| **Abmessungen (BxHxT)** | 179 x 88 x 34,5 mm<br>7,05 x 3,46 x 1,36 in |
| **Gewicht** | 0,72 kg |
| **Betriebstemperatur** | 0 bis 50 °C (32 bis 122 °F) |
| **Lagertemperatur** | -40 bis 60 °C (-40 bis 140 °F) |
| **Relative Luftfeuchtigkeit** | 20 % bis 80 %, nicht kondensierend |
| **Max. SPAN-Durchsatz** | N/A |

## Systemelemente

### Assets

Assets sind die Hardwarekomponenten in Ihrem Netzwerk, wie beispielsweise Controller, Engineering-Stationen und Server. Die automatisierte Asset-Erfassung, -Klassifizierung und -Verwaltung von OT Security bietet eine genaue Asset-Inventarisierung, indem alle Änderungen an Geräten kontinuierlich verfolgt werden. Dies vereinfacht die Aufrechterhaltung der betrieblichen Kontinuität, Zuverlässigkeit und Sicherheit. Es spielt außerdem eine wichtige Rolle bei der Planung von Wartungsprojekten, der Priorisierung von Upgrades, der Bereitstellung von Patches sowie bei der Vorfallsreaktion und Risikominderungsmaßnahmen.

## Risikobewertung

OT Security wendet hochentwickelte Algorithmen an, um den Grad des Risikos zu bewerten, dem jedes Asset im Netzwerk ausgesetzt ist. Für jedes Asset im Netzwerk wird ein Risikowert (von 0 bis 100) vergeben. Der Risikowert basiert auf den folgenden Faktoren:

- Ereignisse – Ereignisse im Netzwerk, die sich auf das Gerät ausgewirkt haben (gewichtet nach dem Schweregrad des Ereignisses und und wie lange das Ereignis zurückliegt).

  > Hinweis: Ereignisse werden nach Aktualität gewichtet, sodass neuere Ereignisse einen größeren Einfluss auf den Risikowert haben als ältere Ereignisse.

- Schwachstellen – CVEs, die Assets in Ihrem Netzwerk betreffen, sowie andere Bedrohungen, die in Ihrem Netzwerk identifiziert wurden (z. B. veraltete Betriebssysteme, Verwendung anfälliger Protokolle und anfällige offene Ports). In OT Security werden diese als Plugin-Treffer auf Ihren Assets erkannt.

- Asset-Kritikalität – Ein Messwert, der die Wichtigkeit des Geräts für das ordnungsgemäße Funktionieren des Systems angibt.

  > Hinweis: Bei SPS, die an eine Backplane angeschlossen sind, wirkt sich der Risikowert anderer Module, die die Backplane gemeinsam nutzen, auf den Risikowert der SPS aus.

### Richtlinien und Ereignisse

Richtlinien definieren bestimmte Arten von Ereignissen, die verdächtig, nicht autorisiert, anormal oder anderweitig auffällig sind und im Netzwerk stattfinden. Wenn ein Ereignis eintritt, das alle Bedingungen der Richtliniendefinition für eine bestimmte Richtlinie erfüllt, generiert OT Security ein Ereignis. OT Security protokolliert das Ereignis und sendet Benachrichtigungen gemäß den für die Richtlinien konfigurierten Richtlinienaktionen.

Es gibt zwei Arten von Richtlinienereignissen:

- Richtlinienbasierte Erkennung – Löst Ereignisse aus, wenn die genauen Bedingungen der Richtlinie, wie durch eine Reihe von Ereignisdeskriptoren definiert, erfüllt sind.
- Anomalie-Erkennung – Löst Ereignisse aus, wenn anomale oder verdächtige Aktivitäten im Netzwerk identifiziert werden.

Das System verfügt über eine Reihe vordefinierter (sofort einsetzbarer) Richtlinien. Darüber hinaus bietet das System die Möglichkeit, die vordefinierten Richtlinien zu bearbeiten oder neue benutzerdefinierte Richtlinien zu definieren.

## Richtlinienbasierte Erkennung

Für die richtlinienbasierte Erkennung konfigurieren Sie die spezifischen Bedingungen dafür, welche Ereignisse im System Ereignisbenachrichtigungen auslösen. Richtlinienbasierte Ereignisse werden nur ausgelöst, wenn die genauen Bedingungen der Richtlinie erfüllt sind. Dies stellt sicher, dass keine Fehlalarme auftreten, da das System bei tatsächlichen Ereignissen warnt, die im ICS-Netzwerk stattfinden, und gleichzeitig aussagekräftige detaillierte Informationen über das „Wer“, „Was“, „Wann“, „Wo“ und „Wie“ liefert. Die Richtlinien können auf verschiedenen Ereignistypen und -deskriptoren basieren.

Im Folgenden finden Sie einige Beispiele für mögliche Richtlinienkonfigurationen:

- Anomale oder nicht autorisierte ICS-Steuerungsebenenaktivität (Engineering) – Eine HMI sollte die Firmwareversion eines Controllers nicht abfragen (kann auf Auskundschaftung

hinweisen) und ein Controller sollte nicht während der Betriebszeiten programmiert werden (kann auf nicht autorisierte, potenziell böswillige Aktivität hinweisen).

- Änderung am Code des Controllers – Es wurde eine Änderung an der Controller-Logik festgestellt („Snapshot-Konflikt“).
- Anomale oder nicht autorisierte Netzwerkkommunikation – Zwischen zwei Netzwerk-Assets wurde ein unzulässiges Kommunikationsprotokoll verwendet oder es fand eine Kommunikation zwischen zwei Assets statt, die noch nie zuvor kommuniziert haben.
- Anomale oder nicht autorisierte Änderungen an der Asset-Inventarisierung – Es wurde ein neues Asset entdeckt oder ein Asset kommuniziert nicht mehr im Netzwerk.
- Anomale oder nicht autorisierte Änderungen an Asset-Eigenschaften – Die Firmware oder der Status eines Assets haben sich geändert.
- Abnormales Schreiben von Sollwerten – Ereignisse werden für Änderungen an bestimmten Parametern generiert. Der Benutzer kann die zulässigen Bereiche für einen Parameter definieren und Ereignisse für Abweichungen von diesem Bereich generieren.

## Anomalie-Erkennung

Richtlinien zur Anomalie-Erkennung erkennen verdächtiges Verhalten im Netzwerk basierend auf den integrierten Funktionen des Systems zur Erkennung von Abweichungen von „normalen“ Aktivitäten. Die folgenden Richtlinien für die Anomalie-Erkennung sind verfügbar:

- Abweichungen von einer Baseline für den Netzwerk-Traffic: Der Benutzer definiert eine Baseline für „normalen“ Netzwerk-Traffic basierend auf der Traffic-Karte während eines bestimmten Zeitraums und generiert Warnungen für Abweichungen von der Baseline. Die Baseline kann jederzeit aktualisiert werden.
- Spitze im Netzwerk-Traffic: Es wird ein drastischer Anstieg des Netzwerk-Traffic-Volumens oder der Anzahl von Konversationen festgestellt.

- Potenzielle Netzwerkaufklärungs-/Cyberangriffsaktivität: Ereignisse werden für Aktivitäten generiert, die auf Aktivitäten in Zusammenhang mit Auskundschaftung oder Cyberangriffen im Netzwerk hinweisen, wie z. B. IP-Konflikte, TCP-Port-Scans und ARP-Scans.

## Richtlinienkategorien

Die Richtlinien sind nach folgenden Kategorien geordnet:

- Richtlinien für Konfigurationsereignisse – Diese Richtlinien beziehen sich auf die Aktivitäten, die im Netzwerk stattfinden. Es gibt zwei Unterkategorien von Richtlinien für Konfigurationsereignise:
    - Controller-Validierung – Diese Richtlinien beziehen sich auf Änderungen, die in den Controllern im Netzwerk stattfinden. Dabei kann es sich um Statusänderungen eines Controllers, aber auch um Änderungen an Firmware, Asset-Eigenschaften oder Codeblöcken handeln. Die Richtlinien können auf bestimmte Zeitpläne (z. B. Firmware-Upgrade während eines Arbeitstages) und/oder bestimmte Controller beschränkt werden.
    - Controller-Aktivitäten – Diese Richtlinien beziehen sich auf bestimmte Engineering-Befehle, die sich auf den Status und die Konfiguration von Controllern auswirken. Es ist möglich, bestimmte Aktivitäten zu definieren, die immer Ereignisse generieren, oder eine Reihe von Kriterien zum Generieren von Ereignissen festzulegen. Zum Beispiel, wenn bestimmte Aktivitäten zu bestimmten Zeiten und/oder auf bestimmten Controllern ausgeführt werden. Assets, Aktivitäten und Zeitpläne können sowohl auf Sperrlisten als auch auf Zulassungslisten gesetzt werden.
- Richtlinien für Netzwerkereignisse – Diese Richtlinien beziehen sich auf die Assets im Netzwerk und die Kommunikationsströme zwischen Assets. Dies schließt Assets ein, die dem Netzwerk hinzugefügt oder daraus entfernt wurden. Es enthält auch Traffic-Muster, die für das Netzwerk ungewöhnlich sind oder die als besonders besorgniserregend gekennzeichnet

wurden. Wenn beispielsweise eine Engineering-Station mit einem Controller über ein Protokoll kommuniziert, das nicht Teil eines vorkonfigurierten Satzes von Protokollen ist (z. B. Protokolle, die von Controllern verwendet werden, die von einem bestimmten Anbieter hergestellt werden), wird ein Ereignis ausgelöst. Diese Richtlinien können auf bestimmte Zeitpläne und/oder bestimmte Assets beschränkt werden. Anbieterspezifische Protokolle werden der Einfachheit halber nach Anbieter organisiert, während jedes Protokoll in einer Richtliniendefinition verwendet werden kann.

- SCADA-Ereignisrichtlinien – Diese Richtlinien erkennen Änderungen der Sollwerte, die den industriellen Prozess beeinträchtigen können. Diese Änderungen können aus einem Cyberangriff oder menschlichem Fehlverhalten resultieren.
- Netzwerkbedrohungsrichtlinien – Diese Richtlinien verwenden signaturbasierte OT- und IT-Bedrohungserkennung, um Netzwerk-Traffic zu identifizieren, der auf Bedrohungen durch Eindringlinge hinweist. Die Erkennung basiert auf Regeln, die in der Threats-Engine von Suricata katalogisiert wurden.

## Gruppen

Eine wesentliche Komponente bei der Definition von Richtlinien in OT Security ist die Verwendung von Gruppen. Bei der Konfiguration einer Richtlinie wird jeder der Parameter durch eine Gruppe und nicht durch einzelne Entitäten bestimmt. Dadurch wird der Prozess für die Richtlinienkonfiguration erheblich optimiert.

## Ereignisse

Wenn ein Ereignis eintritt, das die Bedingungen einer Richtlinie erfüllt, wird im System ein Ereignis generiert. Alle Ereignisse werden im Bildschirm „Ereignisse“ angezeigt und können auch über die entsprechenden Bildschirme „Inventar“ und „Richtlinie“ aufgerufen werden. Jedes Ereignis ist mit einem Schweregrad gekennzeichnet, der den Grad des Risikos angibt, das von dem Ereignis ausgeht. Benachrichtigungen können automatisch an E-Mail-Empfänger und SIEMs gesendet werden, wie in den Richtlinienaktionen der Richtlinie angegeben, die das Ereignis generiert hat.

Ein Ereignis kann von einem autorisierten Benutzer als gelöst markiert und mit einem Kommentar versehen werden.

# Lizenzkomponenten von OT Security

In diesem Thema wird das Verfahren zur Lizenzierung von Tenable OT Security als eigenständiges Produkt beschrieben. Außerdem wird erläutert, wie Assets gezählt werden, welche Add-On-Komponenten Sie erwerben können, wie Lizenzen zurückgefordert werden und was geschieht, wenn Lizenzen überschritten werden oder ablaufen.

Wichtig! Um Tenable-Produkte zu erwerben, wenden Sie sich an Ihren Tenable-Vertriebsmitarbeiter.

Tipp: Informationen zur Aktualisierung oder erneuten Initialisierung Ihrer Lizenz finden Sie unter OT Security - Lizenz-Workflow.

## Lizenzierung von Tenable OT Security

Sie können Tenable OT Security als Subscription oder als unbefristete Version/Wartungsversion erwerben.

Um Tenable OT Security zu lizenzieren, erwerben Sie Lizenzen, die auf den Anforderungen Ihres Unternehmens und den Umgebungsdetails basieren. Tenable OT Security weist diese Lizenzen dann Ihren *Assets* zu: allen erkannten Geräten mit IP-Adressen, eine Lizenz für jede IP-Adresse.

## Zählung von Assets

In Tenable OT Security basiert die Anzahl Ihrer Lizenzen auf der Anzahl eindeutiger IP-Adressen in Ihrer Umgebung. Assets werden ab dem Zeitpunkt lizenziert, zu dem sie erkannt werden.

Hinweis: Assets in internen Netzwerken hinter Live-IP-Adressen werden nicht auf Ihre Lizenz angerechnet. Beispielsweise werden in einem redundant verbundenen PLC-Chassis (speicherprogrammierbare Steuerung) mit zwei Live-IP-Adressen und zehn Modulen dahinter nur die beiden Live-IP-Adressen auf Ihre Lizenz angerechnet.

Hinweis: Sie können zwar eine separat erworbene Version von OT Security mit Ihrer Instanz von Tenable Oneverbinden, dies hat jedoch keinen Einfluss auf die Lizenzierung dieser Assets. Tenable One-Kunden verfügen über eine Vielzahl von Tenable-Lösungen, die für sie lizenziert sind, einschließlich OT Security. Die Lizenzen müssen jedoch zuerst Teil der Tenable One-Lizenz sein. Sie können das Konto gemeinsam mit Ihren CSMs (Customer Success Manager) aktualisieren.

## Komponenten von Tenable OT Security

Sie können Tenable OT Security an Ihren Anwendungsfall anpassen, indem Sie Komponenten hinzufügen. Bei einigen Komponenten handelt es sich um Add-ons, die Sie erwerben müssen.

| Im Lieferumfang enthalten | Add-on-Komponente |
|---|---|
| • Virtual Core Appliance<br>• Tenable Security Center. | • Tenable OT Security Enterprise Manager.<br>• Tenable OT Security – Konfigurierbarer Sensor<br>• Tenable OT Security – Zertifizierter konfigurierbarer Sensor<br>• Tenable OT Security – Zertifizierte Core-Plattform<br>• Tenable OT Security – Core-Plattform<br>• Tenable OT Security – XL Core-Plattform |

## Lizenzen zurückfordern

Wenn Sie Lizenzen erwerben, bleibt die Gesamtzahl Ihrer Lizenzen für die Dauer Ihres Vertrags unverändert, es sei denn, Sie erwerben weitere Lizenzen. Tenable OT Security fordert jedoch Lizenzen in Echtzeit zurück, wenn sich die Anzahl Ihrer Assets ändert.

Die folgenden Assets werden von Tenable OT Security zurückgefordert:

- Ausgeblendete Assets
- Assets, die länger als 30 Tage offline waren
- Assets, die Sie in der Benutzeroberfläche entfernen oder ausblenden

## Überschreitung der maximalen Lizenzanzahl

In Tenable OT Security können Sie nur die Ihnen zugeteilte Anzahl an Lizenzen verwenden, es sei denn, Sie erwerben weitere Lizenzen.

Die Überschreitung der maximalen Lizenzanzahl bewirkt Folgendes:

- Benutzer ohne Administratorrechte können nicht mehr auf Tenable OT Security zugreifen.
- In der Benutzeroberfläche wird eine Meldung angezeigt, dass Ihre Lizenzanzahl überschritten wurde.
- Sie können Assets nicht mehr über die Tenable OT Security-Einstellungen wiederherstellen.
- Sie können Schwachstellen-Plugins oder IDS-Signaturen (Feed-Updates) nicht mehr aktualisieren.

> Hinweis: Wenn Sie Ihre maximale Lizenzanzahl überschreiten, kann Tenable OT Security weiterhin neue Assets erkennen und hinzufügen.

## Abgelaufene Lizenzen

Die von Ihnen erworbenen Tenable OT Security-Lizenzen sind für die Dauer Ihres Vertrags gültig. 30 Tage vor Ablauf Ihrer Lizenz wird eine Warnung in der Benutzeroberfläche angezeigt. Setzen Sie

sich während dieses Verlängerungszeitraums mit dem für Sie zuständigen Tenable-Mitarbeiter in Verbindung, um Produkte hinzuzufügen oder zu entfernen oder die Anzahl Ihrer Lizenzen zu ändern.

Nach Ablauf Ihrer Lizenz wird Tenable OT Security deaktiviert und Sie können das Tool nicht verwenden.

## Operational Playbooks

Operational Playbooks sind Handbücher, die Ihnen dabei helfen sollen, mithilfe umsetzbarer Workflows bestimmte Sicherheitsergebnisse zu erzielen. Unabhängig von Ihrer Rolle in der OT-Organisation bieten diese Playbooks standardisierte Verfahren zur Absicherung Ihrer Umgebungen für industrielle Steuerungssysteme (ICS) und SCADA (Supervisory Control and Data Acquisition).

Diese Playbooks nutzen die Multi-Engine-Erkennungsfunktionen von OT Security, einschließlich Asset-Inventarisierung, Schwachstellenmanagement und Bedrohungserkennung, um Ihnen zu helfen, resilient zu bleiben.

Jeder Workflow umfasst Folgendes:

- Eine Zielsetzung oder ein spezifisches Ziel, die bzw. das Sie erreichen möchten.
- Die genauen Pfade innerhalb der OT Security-Oberfläche.
- Das messbare Ergebnis nach Ausführung des Workflows.

### Voraussetzungen

Bevor Sie diese Playbooks ausführen, stellen Sie sicher, dass Ihr Netzwerk über Folgendes verfügt:

- Asset-Erkennung: Stellen Sie sicher, dass OT Security mindestens ein Netzwerksegment mithilfe passiver Erfassung oder aktiver Abfragen überwacht, um das Inventar zu füllen.

- Benutzerberechtigungen: Stellen Sie sicher, dass Sie über die erforderlichen Benutzerrollen verfügen, um Dashboards anzuzeigen und Scans zu initiieren.

## Operative Workflows

Um loszulegen, sehen Sie sich diese Workflows an:

- Schwachstellen priorisieren und entschärfen – Priorisieren Sie Behebungsmaßnahmen auf der Grundlage der tatsächlichen Bedrohungsstufen (VPR) und nicht nur basierend auf CVSS-Bewertungen
- Netzwerkbedrohungen untersuchen und darauf reagieren – Erkennen und untersuchen Sie Anomalien, Malware und nicht autorisierte Netzwerkscans.

## Schwachstellen priorisieren und entschärfen

OT Security identifiziert Bedrohungen, einschließlich CVEs, anfällige Protokolle und offene Ports. Es verwendet Vulnerability Priority Rating (VPR), um Risikowerte für jede Schwachstelle zu generieren. So können sich Teams auf Schwachstellen mit hohem Risiko konzentrieren, die aktiv ausgenutzt werden können, und nicht nur auf solche mit hohen CVSS-Werten (Common Vulnerability Scoring System).

VPR ist der von Tenable berechnete Wert, der auf den technischen Auswirkungen und der Threat-Intelligence für eine Schwachstelle basiert. Weitere Informationen zu VPR und dazu, wie es sich von CVSS unterscheidet, finden Sie in diesem Blog.

### Ziel

Wechseln Sie von einem reaktiven „Alles patchen“-Ansatz zu einer risikobasierten Strategie, indem Sie die Schwachstellen identifizieren und beheben, die die größte tatsächliche Bedrohung für die Betriebsumgebung darstellen.

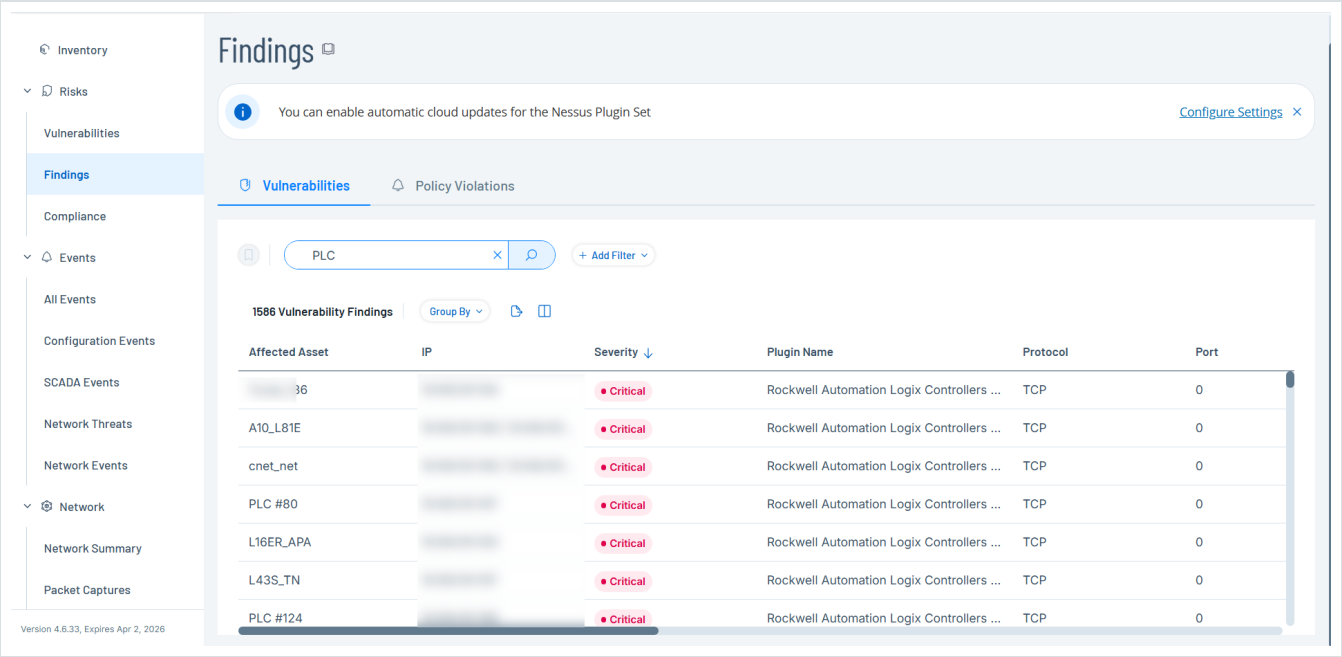
### Voraussetzungen

- OT Security muss Assets durch passive oder aktive Erfassung identifiziert haben.
- (Optional) Integration mit Tenable Vulnerability Management oder Tenable Security Center für eine einheitliche Bewertung.

## Schritt 1: Risiko-Dashboard anzeigen

1. Loggen Sie sich bei OT Security ein.
2. Klicken Sie im linken Navigationsmenü auf Risiken > Feststellungen.

   Die Seite Feststellungen wird mit der Standardregisterkarte Schwachstellen angezeigt, die alle Netzwerkbedrohungen enthält, einschließlich CVEs und anfälliger Protokolle.



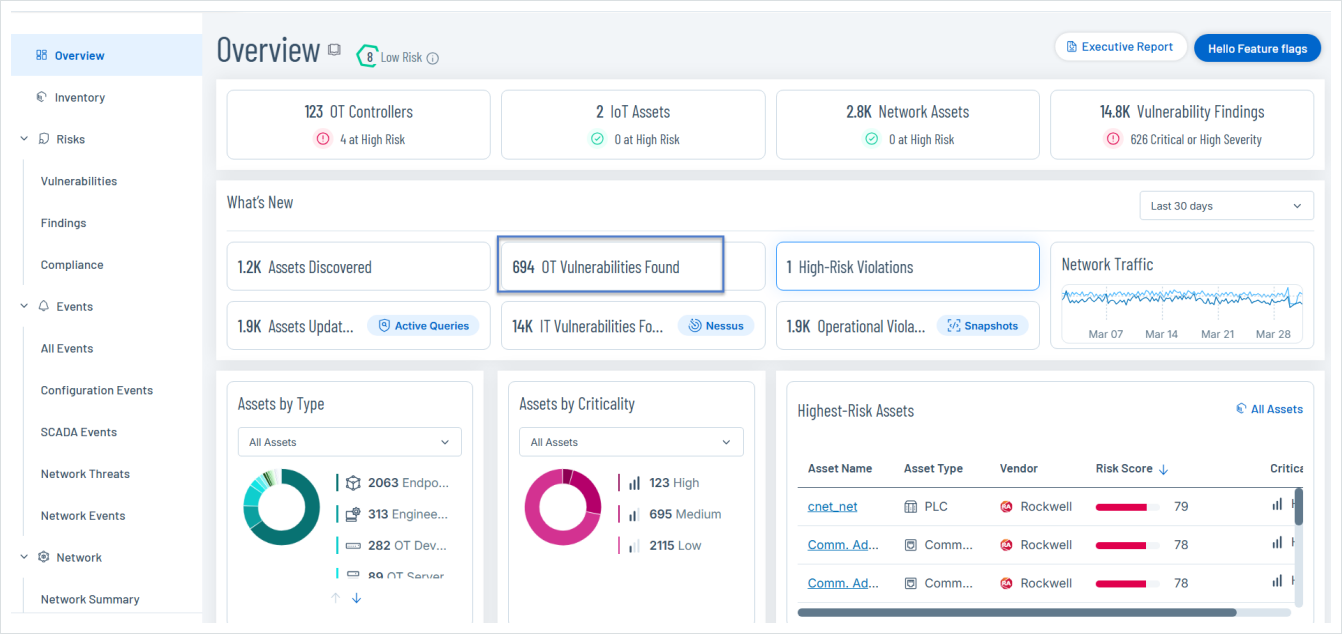

## Schritt 2: Nach Schweregrad und Asset-Kritikalität priorisieren

1. Sortieren Sie die Schwachstellenliste nach VPR oder Schweregrad (Kritisch oder Hoch), um die wichtigsten Bedrohungen zu identifizieren.

2. Verwenden Sie die Schaltfläche Filter hinzufügen, um die Ansicht so zu filtern, dass kritische Asset-Kategorien wie Controller (SPS) oder Engineering-Stationen angezeigt werden.

   Die Liste „Schwachstellen“ zeigt die gefilterten Ergebnisse an.

3. Alternativ können Sie sich das Widget Schwachstellen im Dashboard Übersicht ansehen, um die Schweregradverteilung auf die Asset-Typen anzuzeigen.

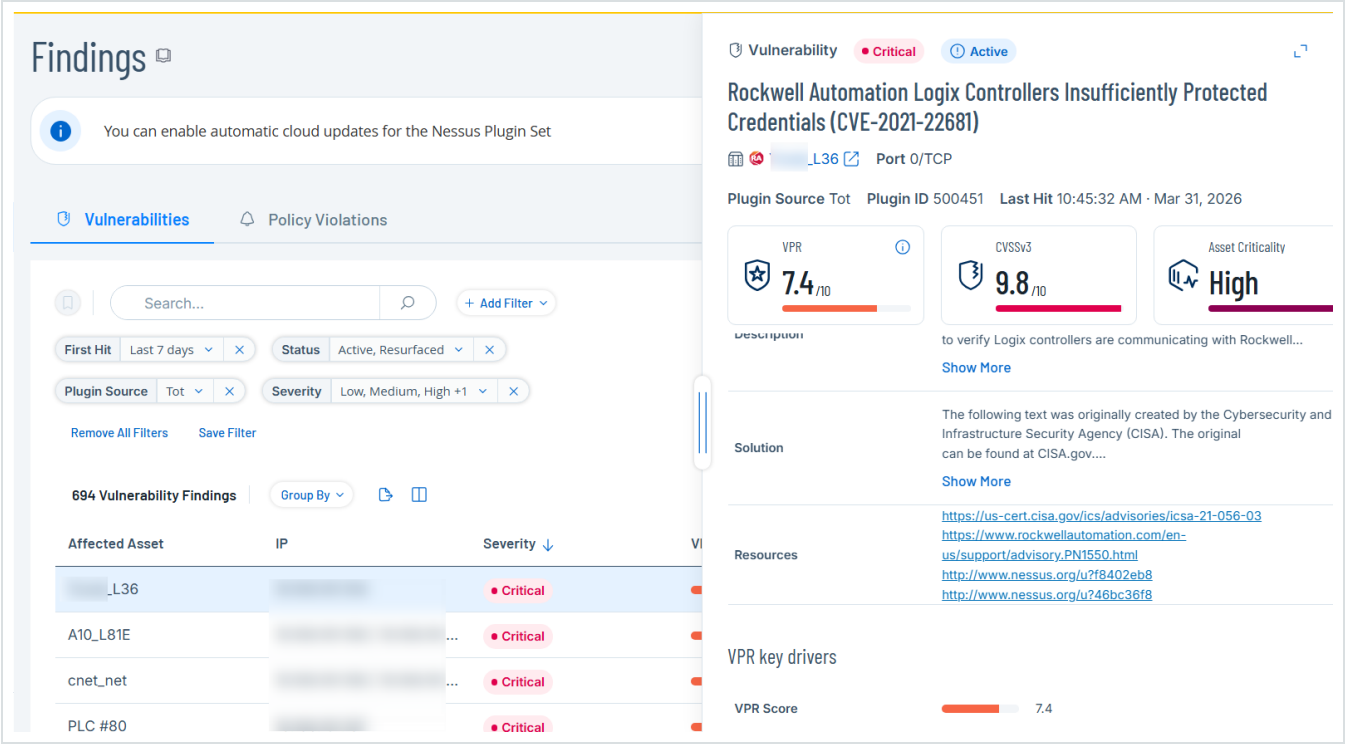



   - Klicken Sie auf das Widget OT-Schwachstellen, um die Seite Feststellungen aufzuschlüsseln.

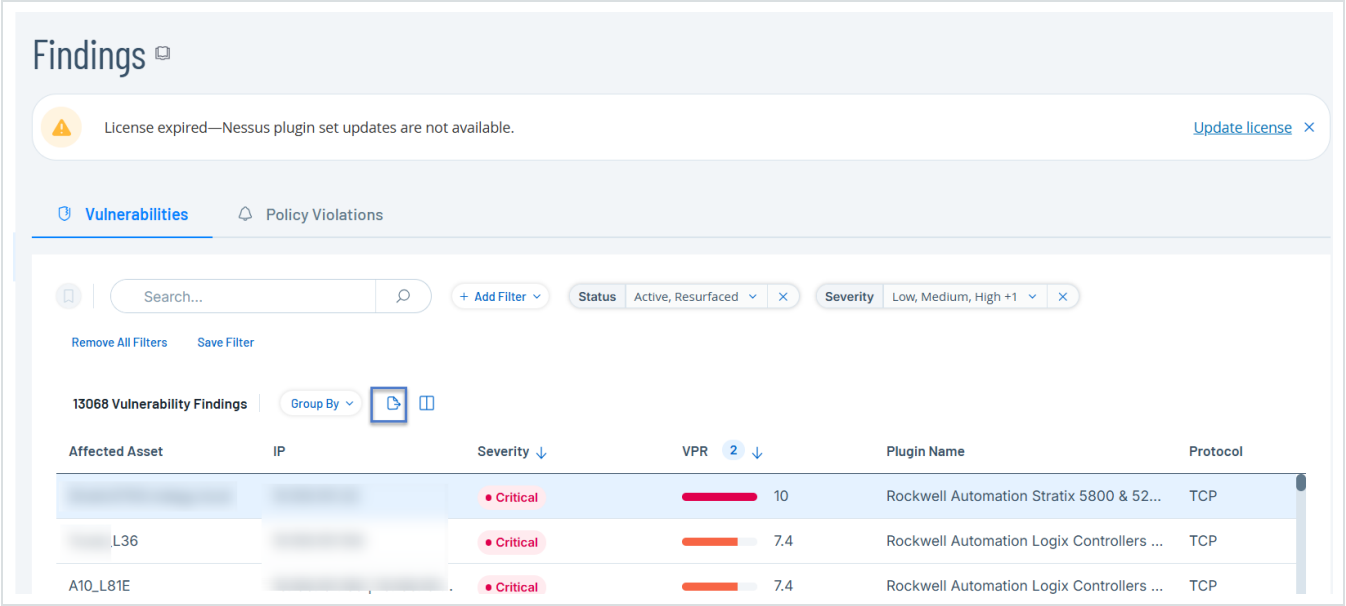
## Schritt 3: Behebungsoptionen analysieren

1. Klicken Sie auf der Seite „Feststellungen“ auf ein bestimmtes Asset, um den Bereich Asset-Details zu öffnen.

2. Klicken Sie auf eine bestimmte Schwachstelle, um die detaillierten Erkenntnisse und Behebungsvorschläge zu überprüfen, die für das spezifische CVE oder die Schwachstelle bereitgestellt werden.




3. Klicken Sie auf der Seite Feststellungen auf die Schaltfläche Exportieren , um die Daten zu exportieren und mit anderen Teams und Stakeholdern zu teilen.



Tipp: Wenn Sie OT Security mit Tenable One oder Tenable Security Center integriert haben, können Sie die Ergebnisse in diesen Anwendungen weiter analysieren. Weitere Informationen zur Integration von Tenable One oder Tenable Security Center finden Sie unter Integrationen.

### Ergebnis

Sie verfügen über eine priorisierte Liste von Schwachstellen, die für Ihre Umgebung relevant sind, und können so Wartungsressourcen effizient zuteilen, um das größte Risiko zu reduzieren.

## Netzwerkbedrohungen untersuchen und darauf reagieren

OT Security verwendet mehrere Erkennungs-Engines, darunter Verhaltensanomalien, signaturbasierte Erkennung (Suricata) und richtlinienbasierte Regeln, um Traffic zu identifizieren, der auf Cyberangriffe hinweist.

### Ziel

Erkennen und untersuchen Sie verdächtige Netzwerkaktivitäten, wie z. B. nicht autorisierte Scans, Malware-Verbreitung oder Protokollanomalien, um Betriebsunterbrechungen zu verhindern.

### Voraussetzungen

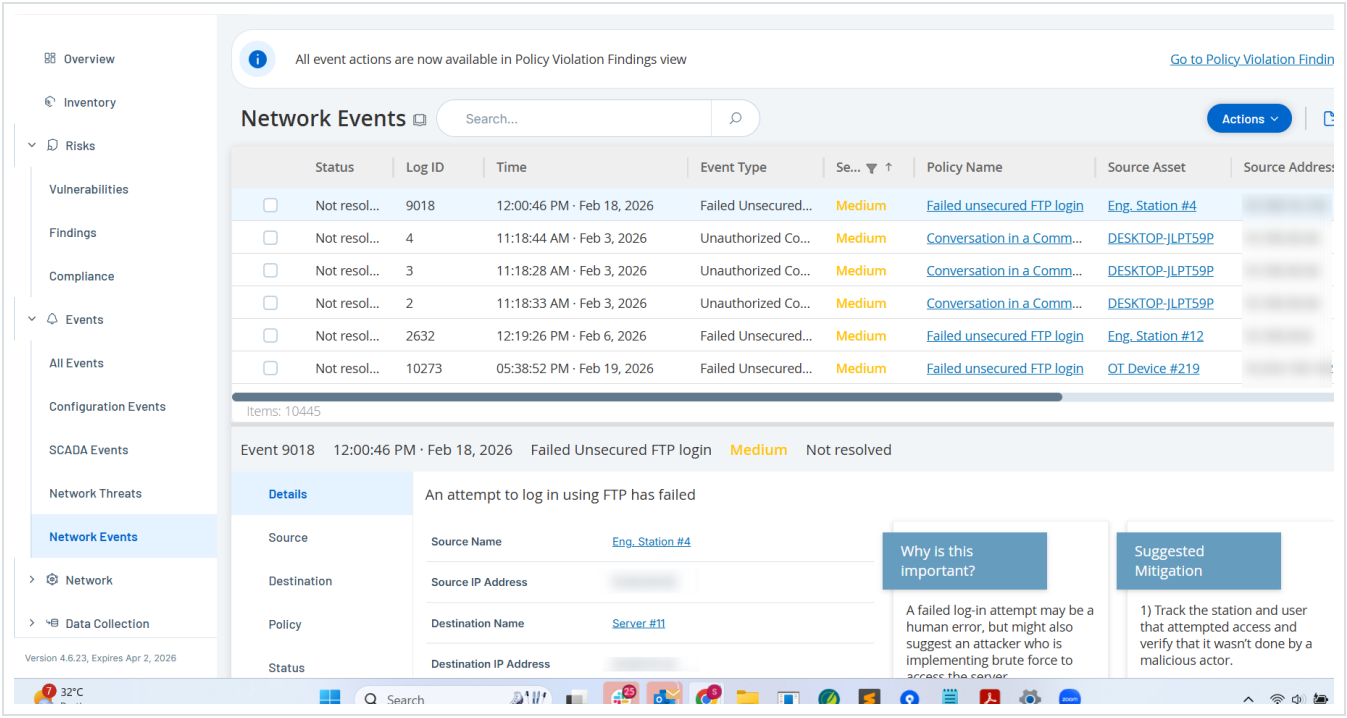
Sie müssen über die erforderlichen Berechtigungen verfügen, um Ereignisse anzuzeigen.

Konfigurieren Sie Folgendes:

- Konfigurieren Sie das Netzwerk-Monitoring. Siehe Überwachte Netzwerke.
- Aktivieren Sie Erkennungsrichtlinien. Siehe Richtlinien aktivieren oder deaktivieren.
- (Optional) Aktivieren Sie die PCAP-Erfassung für forensische Analysen. Siehe Einzelne Erfassungsdateien herunterladen.

### Schritt 1: Ereigniswarnungen überwachen

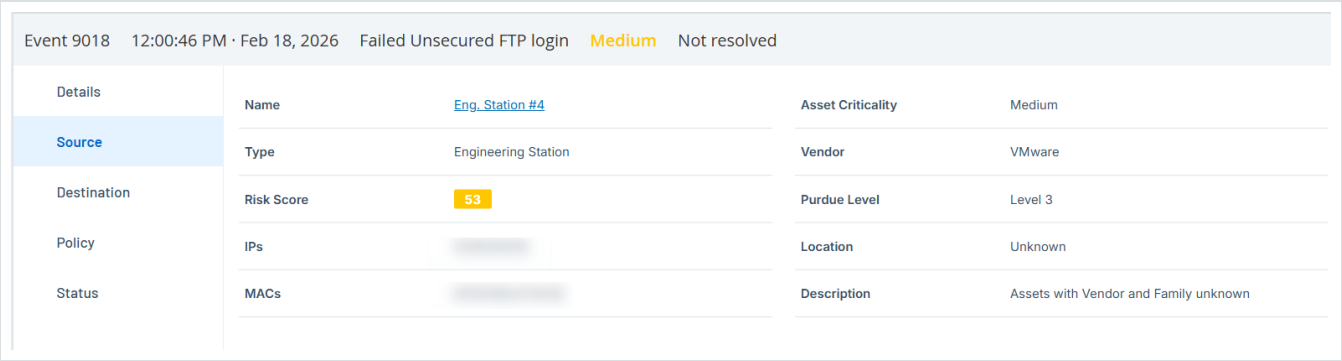
1. Loggen Sie sich bei OT Security ein.
2. Klicken Sie im linken Navigationsmenü auf Ereignisse.
3. Wählen Sie Netzwerkbedrohungen oder Netzwerkereignisse aus, um Warnungen im Zusammenhang mit Eindringungsversuchen oder anormalem Traffic anzuzeigen.



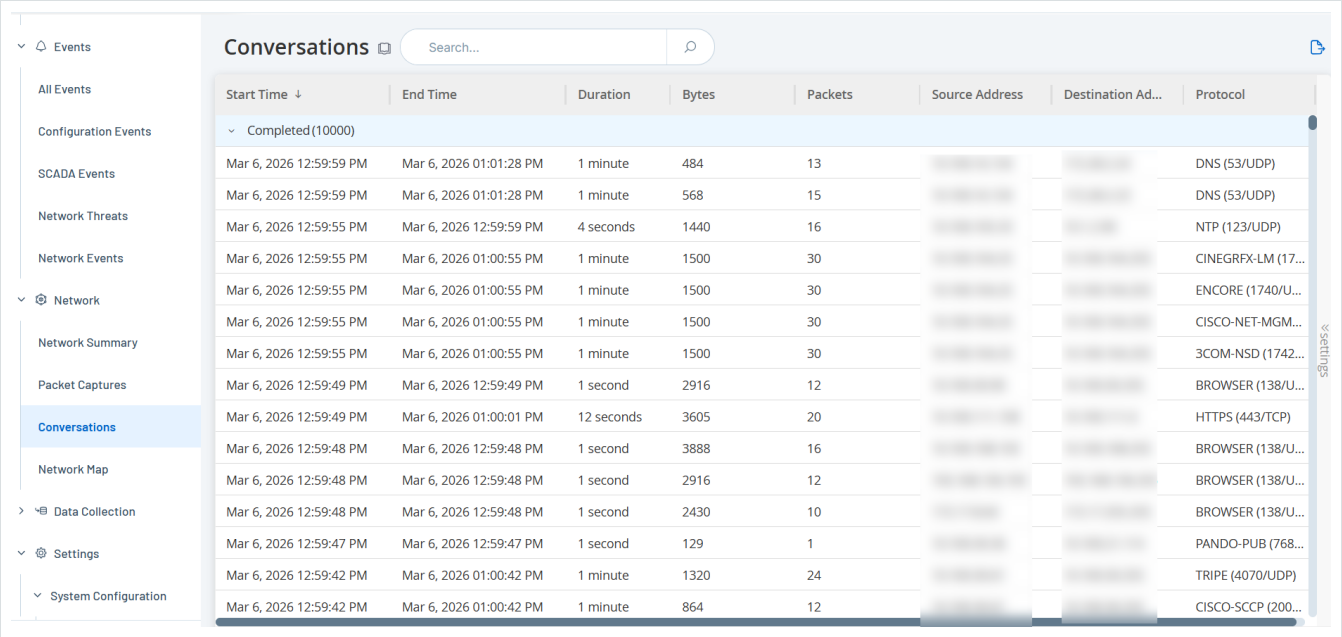

4. Sortieren Sie Ereignisse nach Schweregrad (Hoch oder Kritisch), um unmittelbare Bedrohungen einzuordnen.

## Schritt 2: Konversationsdaten analysieren

1. Wählen Sie ein bestimmtes Ereignis aus, um den Bereich Ereignisdetails anzuzeigen.
2. Identifizieren Sie die Quell- und Ziel-Assets, die an der verdächtigen Aktivität beteiligt sind.




3. Navigieren Sie zur Seite Netzwerk > Konversationen, um die spezifischen Traffic-Flüsse zwischen diesen Assets anzuzeigen.




4. Sofern verfügbar, verwenden Sie die Ansicht Paketerfassungen (PCAP), um die rohen Traffic-Daten auf forensische Beweise zu analysieren. Siehe Einzelne Erfassungsdateien herunterladen.

## Schritt 3: Reaktion einleiten

- Sehen Sie sich Empfohlene Maßnahmen im Abschnitt „Ereignisdetails“ an und ergreifen Sie Maßnahmen (z. B. das kompromittierte Asset isolieren).

- Wenn das Ereignis falsch positiv ist, passen Sie die Richtlinienkonfiguration an, um die Erkennung zu optimieren und Störungen zu reduzieren. Siehe Richtlinien.
- Markieren Sie das Ereignis unter Feststellungen > Richtlinienverstöße als Aufgelöst, um es aus der aktiven Warteschlange zu löschen. Siehe Richtlinienverstöße.

Ergebnis

Sie können schnell das „Wer, Was, Wo und Wann“ eines Sicherheitsvorfalls identifizieren und so die mittlere Reaktionszeit (MTTR) minimieren.

## Fehlermeldungen

In der folgenden Tabelle werden die Fehlermeldungen beschrieben, die in Tenable OT Security angezeigt werden können.

| Kategorie | Name der Fehlerkategorie | Fehlerbeschreibung | Meldung in der Benutzeroberfläche | Empfohlene Aktion |
|---|---|---|---|---|
| Verwaltung aktiver Abfragen | NoRoutesForClient | Für eine Abfrage wurde ein Routing-Fehler vom Netzwerk empfangen. | Möglicherweise liegt ein Problem mit der Netzwerkkonnektivität vor. Bitte überprüfen Sie die Netzwerkkonnektivität und wiederholen Sie die Abfrage. | Überprüfen Sie die Netzwerkkonnektivität und wiederholen Sie die aktive Abfrage. |

| | | | | |
|---|---|---|---|---|
| Verwaltung aktiver Abfragen | InternalError | Beim Abfrageversuch ist ein interner Fehler aufgetreten. | Es ist ein unerwarteter Fehler aufgetreten. Versuchen Sie es später noch einmal. Falls das Problem weiterhin besteht, wenden Sie sich an den technischen Support. | Wiederholen Sie die Abfrage nach einiger Zeit. Wenn das Problem weiterhin besteht, wenden Sie sich an Tenable Support. |
| Verwaltung aktiver Abfragen | DnsError | Für die Ziel-IP wurde kein DNS-Hostname gefunden. | Für die Ziel-IP konnte kein DNS-Hostname gefunden werden. Stellen Sie sicher, dass Reverse DNS aktiviert und ein PTR-Eintrag für die IP definiert ist. | Überprüfen Sie, ob die Reverse DNS-Suche aktiviert und der DNS Pointer Record (PTR) für die IP definiert ist. |
| Verwaltung aktiver Abfragen | HostUnreachableError | Ein Abfrageziel kann nicht erreicht werden. Überprüfen Sie | Das Gerät konnte nicht erreicht werden. Dies könnte an einem Problem | Überprüfen Sie die Netzwerkkonnektivität und die Firewall- |

| | | | | |
|---|---|---|---|---|
| | | das Routing. | mit der Netzwerkkonnektivität liegen. Bitte überprüfen Sie Ihre Netzwerk- oder Firewalleinstellungen und versuchen Sie es erneut. | Einstellungen und wiederholen Sie die aktive Abfrage. |
| Verwaltung aktiver Abfragen | TimeoutError | Eine Abfrage hat keine Antwort vom Ziel empfangen und eine Zeitüberschreitung ist aufgetreten. | Zeitüberschreitung im Netzwerk. Dies könnte an vorübergehenden Netzwerkproblemen liegen oder daran, dass das Gerät langsam reagiert. Bitte wiederholen Sie die Abfrage zu einem späteren Zeitpunkt. | Wiederholen Sie die Abfrage nach einiger Zeit. |
| Verwaltung aktiver Abfragen | NetworkError | Für eine Abfrage wurde eine Fehlerantwort vom Netzwerk | Es ist ein Netzwerkfehler aufgetreten. Dies könnte auf vorübergehende | Überprüfen Sie die Netzwerkkonnektivität und wiederholen |

| | | | | |
|---|---|---|---|---|
| | | empfangen. | Netzwerkprobleme oder Firewall-Einschränkungen zurückzuführen sein. Bitte überprüfen Sie die Netzwerkkonnektivität und wiederholen Sie die Abfrage. | Sie die Abfrage. |
| Verwaltung aktiver Abfragen | ProtocolError | Eine Abfrage hat eine unerwartete Antwort vom Ziel empfangen. | Nicht unterstütztes Antwortformat vom Ziel. Dies könnte an einer nicht kompatiblen Protokollversion auf dem Gerät oder an einem vorübergehenden Netzwerkproblem liegen. Bitte überprüfen Sie die Gerätekompatibilität oder wiederholen Sie | Überprüfen Sie, ob das Zielgerät kompatibel ist, oder wiederholen Sie die Abfrage nach einiger Zeit. |

| | | | | |
|---|---|---|---|---|
| | | | die Abfrage zu einem späteren Zeitpunkt. | |
| Verwaltung aktiver Abfragen | AuthenticationError | In der Abfrage wurden ungültige Authentifizierungsdaten verwendet. | Die Authentifizierung beim Gerät ist fehlgeschlagen. Dies könnte an falschen oder fehlenden Zugangsdaten liegen. Überprüfen Sie Ihre Zugangsdaten. | Überprüfen Sie Ihre Zugangsdaten und wiederholen Sie die Abfrage. |
| Verwaltung aktiver Abfragen | LimitExceededError | OT Security hat den Grenzwert für fehlgeschlagene Abfragen des Ziels erreicht. | Aktive Abfragen dieses Geräts werden aufgrund zu vieler fehlgeschlagener Abfragen angehalten. Versuchen Sie es später noch einmal. Wenn das Problem weiterhin besteht, wenden Sie sich an den | Es liegen mehrere fehlgeschlagene Abfragen für das Gerät vor. Wiederholen Sie die Abfrage nach einiger Zeit. Wenn das Problem weiterhin besteht, |

| | | | | |
|---|---|---|---|---|
| | | | Support. | wenden Sie sich an den technischen Support. |
| Verwaltung aktiver Abfragen | NoPotentialClients | Im Ziel-Abfragebereich (CIDR-Block, Asset-Liste oder IP-Bereich) sind keine gültigen Clients vorhanden. | Die aktive Abfrage konnte keine zugänglichen Geräte im Zielbereich finden. Einige Geräte (CIDR-Block, Asset-Liste oder IP-Bereich) werden möglicherweise durch Einschränkungen blockiert, die von Benutzern angewendet wurden. Bitte überprüfen Sie Ihre Auswahl und die Zugriffskontrollen. | Auf die Zielgeräte kann möglicherweise aufgrund von Einschränkungen, die von Benutzern angewendet wurden, nicht zugegriffen werden. Überprüfen Sie Ihre Einstellungen für die Zugriffskontrolle und wiederholen Sie die Abfrage. |
| Verwaltung aktiver | NoAllowedClients | Im Ziel-Abfragebereich | Die aktive Abfrage konnte | Die Zielgeräte sind |

| | | | | |
|---|---|---|---|---|
| Abfragen | | (CIDR-Block, Asset-Liste oder IP-Bereich) sind keine zulässigen Clients vorhanden. | im Zielbereich keine kompatiblen Geräte finden (CIDR-Block, Asset-Liste oder IP-Bereich). Bitte überprüfen Sie Ihre Auswahl und die Zugriffskontrollen. | möglicherweise nicht mit den OT Security-Einstellungen kompatibel. Überprüfen Sie Ihre Einstellungen für die Zugriffskontrolle und wiederholen Sie die Abfrage. |
| IoT | ServiceUnavailable | Der Dienst ist nicht verfügbar, möglicherweise liegt ein Problem beim Systemstart oder nach dem Zurücksetzen vor. | Der IoT Connector-Dienst ist vorübergehend nicht verfügbar oder weist ein Problem auf. Versuchen Sie es später noch einmal. Wenn das Problem weiterhin besteht, wenden Sie sich an den Support. | Wiederholen Sie die Abfrage nach einiger Zeit, da der IoT Connector-Dienst möglicherweise vorübergehend inaktiv ist. Wenn das Problem weiterhin besteht, wenden Sie |

| | | | | |
|---|---|---|---|---|
| | | | | sich an den technischen Support. |
| IoT | IotConnectorSecureModeError | Der IoT-Connector kann keine Verbindung zu einem remote installierten IoT-Agent herstellen. | Fehler im sicheren Modus des IoT-Connectors. Der IoT-Agent auf dem Remote-System muss neu installiert werden, damit wieder Verbindungen zulässig sind. | Installieren Sie den IoT-Agent auf dem Remote-System neu und wiederholen Sie den Verbindungsversuch. |
| IoT | IotConnectorIpAlreadyExists | Der Benutzer versucht, einen Connector mit einer bereits vorhandenen IP-Adresse hinzuzufügen. | Die Erstellung des Connectors ist fehlgeschlagen. Die angegebene IP-Adresse wird bereits von einem anderen Connector verwendet. Bitte geben Sie eine eindeutige IP-Adresse an und versuchen Sie es | Geben Sie eine eindeutige IP-Adresse an und versuchen Sie, den Connector hinzuzufügen. |

| | | | | |
|---|---|---|---|---|
| | | | erneut. | |
| Serverkopplung: (Enterprise Manager (EM), externer Server, FW) | WrongCertificate | Der Benutzer versucht, die ICP mit einem ungültigen Zertifikat mit dem EM zu koppeln. | Die Kopplungsserver hat ein ungültiges Sicherheitszertifikat vorgelegt. Bitte überprüfen Sie das Serverzertifikat und versuchen Sie es erneut. Wenn dieses Problem weiterhin besteht, wenden Sie sich an den Serveradministrator. | Generieren Sie ein neues Sicherheitszertifikat und versuchen Sie, die ICP mit dem EM zu koppeln. Wenn das Problem weiterhin besteht, wenden Sie sich an den Serveradministrator. |
| Serverkopplung: (EM, externer Server, FW) | MissingEmAddress | Nur über API | Es wurde keine Serveradresse für die Kopplung angegeben. Bitte geben Sie die IP-Adresse oder den Hostnamen des Servers an, zu dem Sie eine Verbindung | Geben Sie die IP-Adresse oder den Hostnamen des Servers an, zu dem Sie eine Verbindung herstellen möchten, und |

| | | | | |
|---|---|---|---|---|
| | | | herstellen möchten, und versuchen Sie es erneut. | versuchen Sie es erneut. |
| Serverkopplung: (EM, externer Server, FW) | MissingPassword | Nur über API | Die angegebenen Zugangsdaten sind unvollständig. Bitte geben Sie das Passwort für den Kopplungsserver ein und versuchen Sie es erneut. | Geben Sie einen Benutzernamen und ein Passwort für den Server an und versuchen Sie es erneut. |
| Serverkopplung: (EM, externer Server, FW) | MissingCredentials | Nur über API | Die Zugangsdaten zum Herstellen einer Verbindung zum Kopplungsserver fehlen. Geben Sie die erforderlichen Zugangsdaten an (z. B. Benutzername und Passwort) | Geben Sie gültige Zugangsdaten für den Server an und versuchen Sie es erneut. |

| | | | | |
|---|---|---|---|---|
| | | | und versuchen Sie es erneut. | |
| Serverkopplung: (EM, externer Server, FW) | BothApiKeyAndUserCredentials | Nur über API | Für die Kopplung mit diesem Server ist nur eine Authentifizierungsmethode zulässig. Entfernen Sie entweder den API-Schlüssel oder die Benutzer-Zugangsdaten und versuchen Sie es erneut. | Verwenden Sie für die Kopplung entweder einen API-Schlüssel oder Benutzer-Zugangsdaten. |
| OT-Feeds: PII/Suricata/Nessus | NessusNotReady | Der Dienst ist nicht verfügbar, möglicherweise liegt ein Problem beim Systemstart oder nach dem Zurücksetzen vor. | Der Nessus-Dienst ist vorübergehend nicht verfügbar oder weist ein Problem auf. Versuchen Sie es später noch einmal. Wenn das Problem weiterhin besteht, wenden | Der Nessus-Dienst ist möglicherweise inaktiv. Versuchen Sie nach einiger Zeit erneut, den Dienst zu erreichen. Wenn das Problem |

| | | | | |
|---|---|---|---|---|
| | | | Sie sich an den Support. | weiterhin besteht, wenden Sie sich an Tenable-Support. |
| OT-Feeds: PII/Suricata/ Nessus | MissingFile | Nur über API | Keine Konfigurationsdatei angehängt. Bitte laden Sie eine gültige Konfigurationsdatei im unterstützten Format hoch, um fortzufahren. | Laden Sie eine gültige Konfigurationsdatei hoch. |
| OT-Feeds: PII/Suricata/ Nessus | InvalidFile | Die hochgeladene Datei ist ungültig. | Die hochgeladene Datei ist ungültig. Möglicherweise weist die Datei ein nicht unterstütztes Format auf oder es fehlen Versionsinformationen. Bitte informieren Sie sich in der | Überprüfen Sie, ob das Format oder die Version der hochgeladenen Datei gültig ist, bevor Sie die Datei hochladen. |

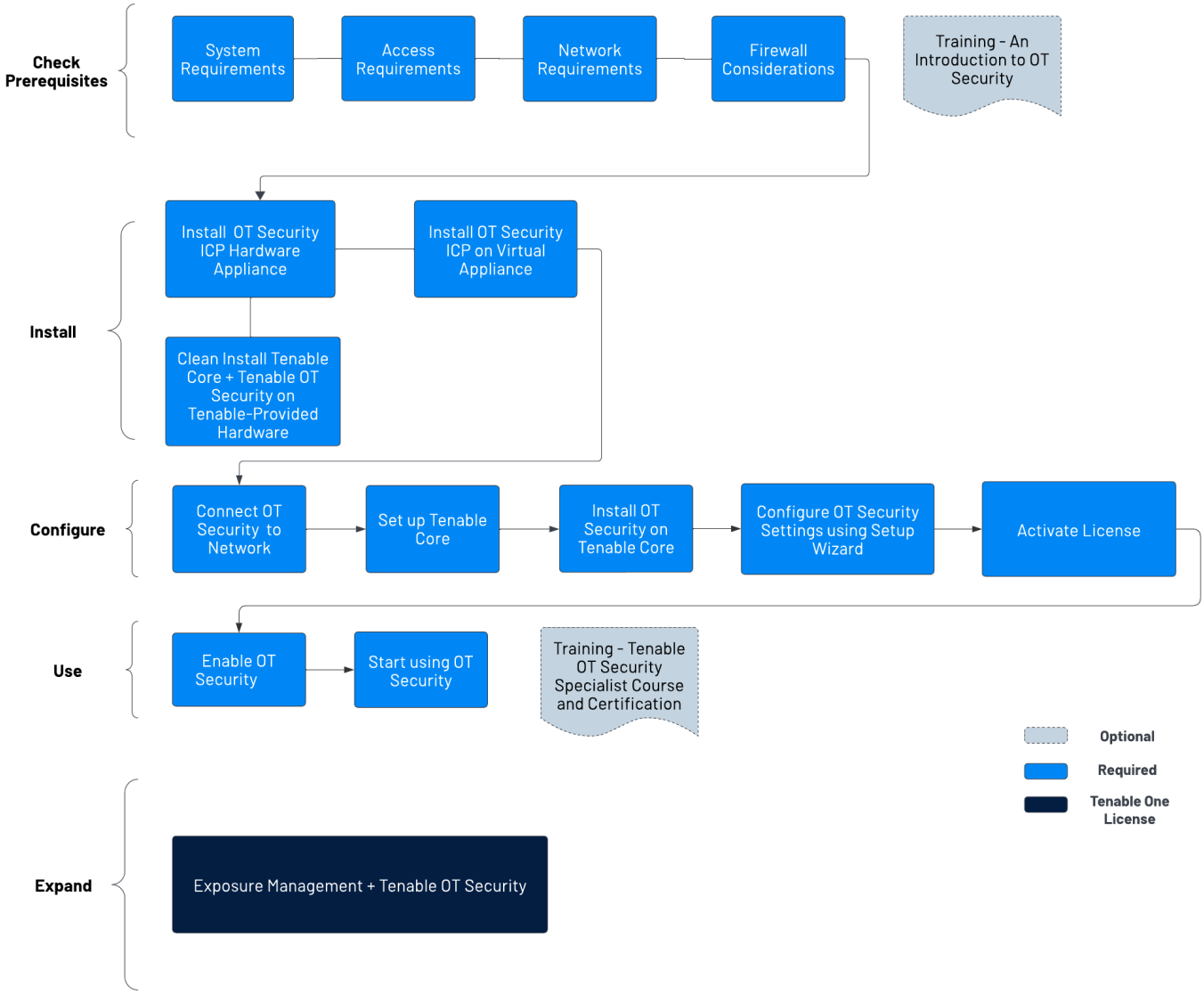
| | | | | |
|---|---|---|---|---|
| | | | Dokumentation über die unterstützten Formate sowie die erforderlichen Felder und versuchen Sie es erneut. | |
| OT-Feeds: PII/Suricata/ Nessus | NoSpaceLeftOnDevice | Es wird eine Datei im Online- oder Offline-Modus hochgeladen, auf dem Gerät ist jedoch kein Platz für die neue Datei vorhanden. | Die neue Konfigurationsdatei konnte nicht gespeichert werden, da nicht genügend Speicherplatz verfügbar ist. Bitte geben Sie Speicherplatz auf dem Gerät frei und versuchen Sie es erneut. | Geben Sie Speicherplatz auf dem Gerät frei und versuchen Sie, die Konfigurationsdatei hochzuladen. |
| OT-Feeds: PII/Suricata/ Nessus | OldLicense | Der Benutzer verwendet eine Lizenz ohne gültige Zugangsdaten. | Die Aktion ist aufgrund eines veralteten Versionsformats nicht zulässig. Bitte beziehen Sie eine neue Lizenz in dem | Führen Sie für Ihre OT Security-Lizenz ein Upgrade auf das unterstützte Format durch. |

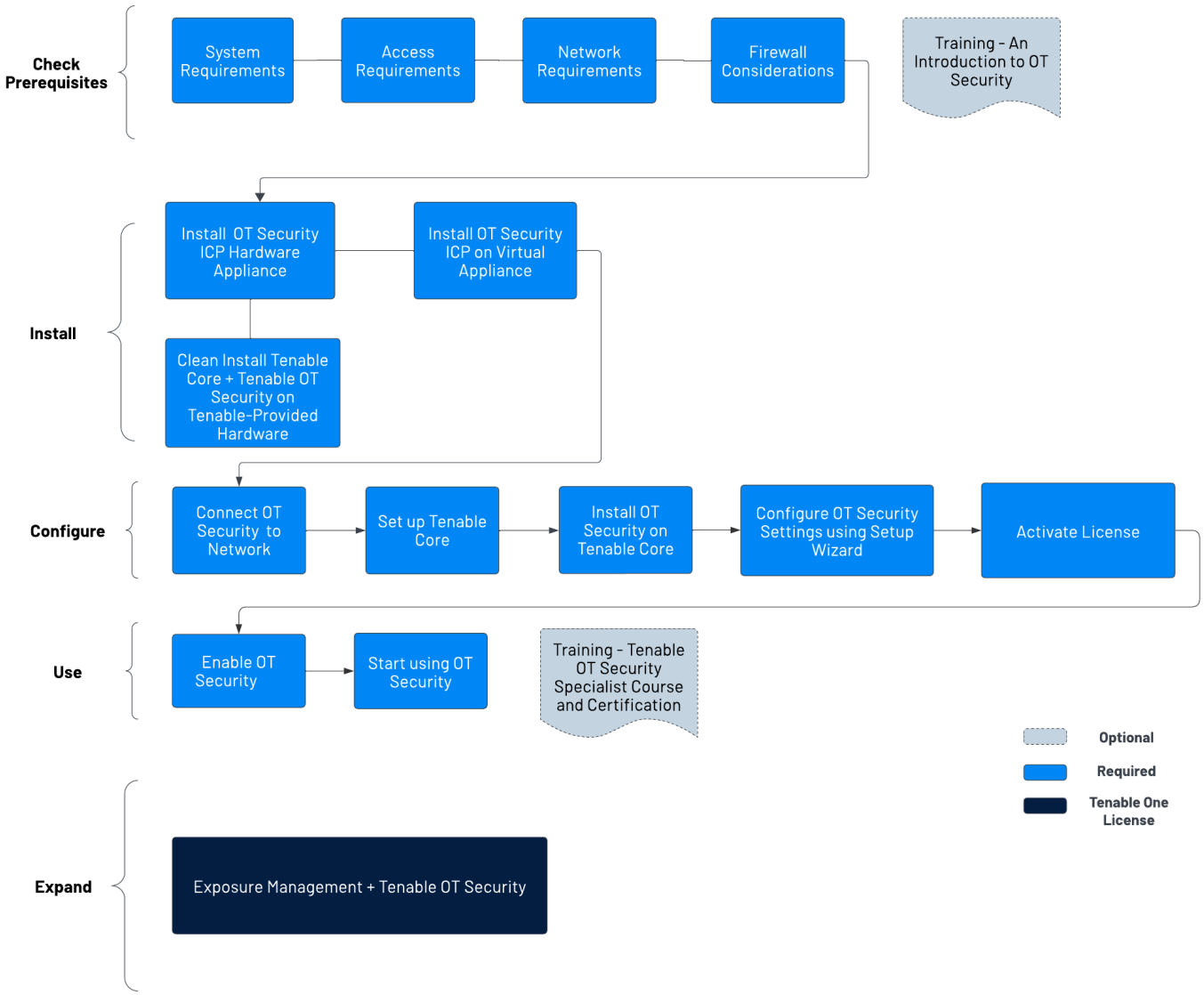
| | | | | |
|---|---|---|---|---|
| | | | unterstützten Format und versuchen Sie es erneut. | |
| OT-Feeds: PII/Suricata/ Nessus | UpdateAlreadyInProgress | Der Benutzer führt derzeit ein Update durch, während bereits ein Auftrag ausgeführt wird. Es kann jedoch jeweils nur ein Update ausgeführt werden. | Für dieses Gerät wird gerade ein Update durchgeführt. Bitte warten Sie auf den Abschluss des aktuellen Updates, bevor Sie ein weiteres Update starten. | Warten Sie, bis das aktuelle Update abgeschlossen ist, bevor Sie es erneut versuchen. |
| OT-Feeds: PII/Suricata/ Nessus | OlderVersionUpdateAttempt | Der Benutzer versucht, ein Downgrade auf eine frühere Version durchzuführen. | Die Datei konnte nicht hochgeladen werden, weil eine neuere Version aktiv ist. Vergewissern Sie sich, dass Sie über die neueste aktualisierte Datei verfügen und versuchen | Vergewissern Sie sich, dass es sich bei der Datei, die Sie hochladen möchten, um die neueste Version handelt. |

| | | | | |
|---|---|---|---|---|
| | | | Sie erneut, die Datei hochzuladen. | |

## Erste Schritte mit OT Security

Verwenden Sie die folgende Einstiegssequenz, um die Installation zu starten und OT Security zu verwenden.


Check Prerequisites
System Requirements
Access Requirements
Network Requirements
Firewall Considerations
Training - An Introduction to OT Security
Install
Install OT Security ICP Hardware Appliance
Install OT Security ICP on Virtual Appliance
Clean Install Tenable Core + Tenable OT Security on Tenable-Provided Hardware
Configure
Connect OT Security to Network
Set up Tenable Core
Install OT Security on Tenable Core
Configure OT Security Settings using Setup Wizard
Activate License
Use
Enable OT Security
Start using OT Security
Training - Tenable OT Security Specialist Course and Certification
Optional
Required
Tenable One License
Expand
Exposure Management + Tenable OT Security




# Voraussetzungen überprüfen

- Voraussetzungen – Informieren Sie sich über die System-, Hardware-, virtuellen und Lizenzanforderungen für OT Security.
    - Systemanforderungen – Informieren Sie sich über die Anforderungen für die Installation und Ausführung von Tenable Core + OT Security.

- Zugriffsanforderungen – Informieren Sie sich über die Internet- und Portanforderungen für die Ausführung von Tenable Core + OT Security.
- Überlegungen zum Netzwerk – Informieren Sie sich über die Netzwerkschnittstellen, die zum Verbinden von OT Security benötigt werden.
- Überlegungen zur Firewall – Informieren Sie sich über die Ports, die offen sein müssen, damit OT Security ordnungsgemäß funktioniert.
- Einführung in Tenable OT Security – Gehen Sie das Schulungsmaterial durch, um detaillierte Informationen zu OT Security zu erhalten.

## OT Security ICP installieren

OT Security ist eine Anwendung, die auf dem Betriebssystem Tenable Core ausgeführt wird und den Basisanforderungen von Tenable Core unterliegt. Beachten Sie die folgenden Richtlinien, um Tenable Core + OT Security zu installieren und zu konfigurieren.

So installieren Sie OT Security:

1. OT Security ICP installieren
    - OT Security ICP-Hardware-Appliance installieren – Richten Sie OT Security als Hardware-Appliance ein.

      > Hinweis: Auf der von Tenable bereitgestellten Tenable Core-Hardware ist Tenable Core + OT Security vorinstalliert. Wenn Sie eine ältere oder veraltete Appliance installieren, sollten Sie sich möglicherweise für eine Neuinstallation entscheiden. Weitere Informationen finden Sie unter Neuinstallation von Tenable Core + Tenable OT Security auf von Tenable bereitgestellter Hardware.

    - Virtuelle OT Security ICP-Appliance installieren – Stellen Sie Tenable Core + OT Security als virtuelle Maschine bereit, indem Sie die vorkonfigurierte `OVA`-Datei mit der

Standardkonfiguration der virtuellen Maschine verwenden, oder passen Sie Ihre Appliance mit der `ISO`-Installationsdatei an.

2. OT Security mit dem Netzwerk verbinden – Verbinden Sie die OT Security Hardware- und virtuelle Appliance mit dem Netzwerk.
3. OT Security ICP konfigurieren
    a. Tenable Core einrichten – Konfigurieren Sie Tenable Core über die CLI oder die Benutzeroberfläche.
    b. OT Security unter Tenable Core installieren – Schließen Sie die Installation von Tenable OT Security in Tenable Core manuell ab.
    c. Einstellungen von OT Security mit dem Setup-Assistenten konfigurieren – Konfigurieren Sie die grundlegenden Einstellungen in OT Security mit dem Setup-Assistenten.
        - Loggen Sie sich bei der OT Security-Konsole ein und konfigurieren Sie die Einstellungen für Benutzerinformationen, Gerät, System Time und Port-Trennung.
4. OT Security-Lizenz aktivieren – Aktivieren Sie Ihre Lizenz, nachdem Sie die Installation von OT Security abgeschlossen haben.

## OT Security verwenden

Starten OT Security

1. OT Security aktivieren – Aktivieren Sie OT Security, nachdem Sie Ihre Lizenz aktiviert haben.
2. verwendenOT Security – Konfigurieren Sie Ihre überwachten Netzwerke, die Port-Trennung, Benutzer, Gruppen und Authentifizierungsserver so, dass sie OT Security verwenden.

> Tipp: Um praktische Erfahrungen zu sammeln und die Tenable OT Security Specialist-Zertifizierung zu erhalten, absolvieren Sie den Tenable OT Security Specialist-Kurs.

# OT Security zu Tenable One erweitern

> Hinweis: Hierzu ist eine Tenable One-Lizenz erforderlich. Weitere Informationen zum Testen von Tenable One finden Sie unter Tenable One.

Integrieren Sie OT Security mit Tenable One und nutzen Sie die folgenden Funktionen:

- Rufen Sie die Seite **Exposure View** auf, auf der Sie konvergierende Risikostufen anzeigen und versteckte Schwächen über die IT-OT-Grenze hinweg aufdecken können. Mithilfe von erweiterten OT-Daten können Sie potenzielle Schwachstellen kontinuierlich überwachen und verfolgen:
    - Sie können Cyber Exposure-Karten anzeigen und verwalten.
    - Sie können CES- und CES-Trenddaten für die Exposure-Karten „Global“ und Operative Technologien anzeigen.
    - Zeigen Sie Daten zu Service Level Agreements (SLA) für Behebungsmaßnahmen an.
    - Zeigen Sie Daten zur Tag-Performance an.
- Rufen Sie die Seite **Exposure Signals** auf, auf der Sie Exposure Signals generieren können, die mithilfe von Abfragen nach Asset-*Verstößen* suchen. Einfach ausgedrückt: Wenn ein Asset von einer Schwäche im Zusammenhang mit der Abfrage betroffen ist, wird das Asset als *Verstoß* angesehen. Auf dieser Grundlage können Sie Einblick in Ihre kritischsten Risikoszenarien erhalten.
    - Mit aktuellen Feeds von Tenable Research finden Sie die wichtigsten aktiven Bedrohungen in Ihrer Umgebung.
    - Sie können die Daten aus Abfragen und den betroffenen Asset-Verstößen anzeigen, generieren und mit ihnen interagieren.

- Erstellen Sie benutzerdefinierte Exposure Signals, um unternehmensspezifische Risiken und Schwächen anzuzeigen.

- Rufen Sie die Seite **Inventar** auf und reichern Sie die Asset-Erfassung mit OT-spezifischen Informationen an, wie z. B. Firmware-Versionen, Anbieter, Modelle und Betriebsstatus. Rufen Sie OT-Informationen ab, die Standard-IT-Sicherheitstools nicht bieten können:
  - Zeigen Sie die Daten auf der Registerkarte **Assets** an und arbeiten Sie mit ihnen:
    - Überprüfen Sie Ihre AD-Assets, um die strategischen Aspekte der Benutzeroberfläche zu verstehen. Dies sollte Ihnen eine Vorstellung davon vermitteln, welche Funktionen Sie in Tenable Exposure Management wann verwenden können.
    - Machen Sie sich mit der Global Asset Search und ihren Objekten und Eigenschaften vertraut. Versehen Sie benutzerdefinierte Abfragen für die spätere Verwendung mit Lesezeichen.
    - Suchen Sie nach Geräten, Benutzerkonten, Software, Cloud-Assets, SaaS-Anwendungen, Netzwerken und deren Schwächen.
    - Schlüsseln Sie die Seite mit **Asset-Details** auf, um Asset-Eigenschaften und alle zugehörigen Kontextansichten anzuzeigen.
  - Zeigen Sie die Daten auf der Registerkarte **Schwächen** an und arbeiten Sie mit ihnen:
    - Zeigen Sie wichtigen Kontext zu Schwachstellen und Fehlkonfigurationen an, um wirkungsvolle Entscheidungen über Behebungsmaßnahmen zu treffen.
  - Zeigen Sie die Daten auf der Registerkarte **Software** an und arbeiten Sie mit ihnen:
    - Verschaffen Sie sich einen vollständigen Überblick über die in Ihrem Unternehmen bereitgestellte Software und und gewinnen Sie ein besseres Verständnis für die damit verbundenen Risiken.

        - Ermitteln Sie, welche Software möglicherweise veraltet ist und welche Softwareteile bald das Ende des Lebenszyklus (End of Life, EoL) erreichen.
    - Zeigen Sie die Daten auf der Registerkarte **Feststellungen** an und arbeiten Sie mit ihnen:
        - Zeigen Sie Instanzen von Schwächen (Schwachstellen oder Fehlkonfigurationen) an, die auf einem Asset auftreten und eindeutig durch Plugin-ID, Port und Protokoll identifiziert werden.
        - Überprüfen Sie die Erkenntnisse zu diesen Feststellungen, einschließlich Beschreibungen, betroffener Assets, Kritikalität und mehr, um potenzielle Sicherheitsrisiken zu identifizieren, Einblick in nicht ausgelastete Ressourcen zu erhalten und Compliance-Maßnahmen zu unterstützen..
- Rufen Sie die Seite **Angriffspfad** auf, auf der Sie die Risikopriorisierung optimieren können, indem Sie riskante Angriffspfade aufdecken, die die Angriffsfläche durchqueren (z. B. Web-Apps, IT, OT, IoT, Identitäten, ASM), und schwerwiegende Auswirkungen verhindern können. Optimieren Sie Risikominderungsmaßnahmen, indem Sie kritische Knotenpunkte identifizieren, um Angriffspfade mithilfe von Anleitungen zur Risikominderung zu unterbrechen, und erwerben Sie fundiertes Fachwissen durch KI-gestützte Erkenntnisse (wird in FedRAMP-Umgebungen nicht unterstützt).
    - Auf der Registerkarte **Dashboard** erhalten Sie einen Überblick über Ihre gefährdeten Assets, z  B. die Anzahl der Angriffspfade, die zu diesen kritischen Assets führen, die Anzahl der offenen Angriffstechniken und deren Schweregrad, eine Matrix zur Anzeige von Pfaden mit unterschiedlichen Kombinationen aus Quellknoten-Exposure-Score und ACR-Zielwert sowie eine Liste der häufigsten Angriffspfade.
        - Sehen Sie sich die Top Attack Path Matrix an und klicken Sie auf die Kachel Top Attack Paths, um weitere Informationen zu Pfaden, die zu Ihren wertvollsten Daten führen, oder Assets mit einem ACR von 7 oder höher anzuzeigen.

Sie können diese bei Bedarf anpassen, um sicherzustellen, dass Daten zu den kritischsten Angriffspfaden angezeigt werden.

- Zeigen Sie auf der Seite **Top Attack Techniques** alle Angriffstechniken an, die in einem oder mehreren Angriffspfaden, die zu einem oder mehreren kritischen Assets führen, verwendet werden. Kombinieren Sie dazu Ihre Daten mit fortschrittlichen Diagrammanalysen und dem MITRE ATT&CK®-Framework, um Angriffstechniken zu generieren, mit deren Hilfe Sie die unbekannten Faktoren verstehen können, die dazu führen, dass Bedrohungen Auswirkungen auf Ihre Assets und Informationen haben und die diese Auswirkungen verstärken. Diese Feststellungen ermöglichen Ihnen außerdem die Bestimmung und Einleitung geeigneter Korrekturmaßnahmen.
- Generieren Sie auf der Registerkarte **Top Attack Paths** Angriffspfad-Abfragen, um Ihre Assets als Teil potenzieller Angriffspfade anzuzeigen:
  - Angriffspfad mit einer integrierten Abfrage generieren
  - Angriffspfad-Abfrage mit dem Attack Path Query Builder generieren
  - Asset-Abfrage mit dem Asset Query Builder generieren

  Anschließend können Sie die Daten der Attack Path Query und der Asset Query über die Abfrageergebnis-Liste und das interaktive Diagramm anzeigen und mit ihnen interagieren.
- Wählen Sie auf der Registerkarte **MITRE ATT&CK Heatmap** die ICS-Heatmap-Option aus, um sich auf die Taktiken und Techniken für industrielle Steuerungssysteme (ICS) zu konzentrieren.

- Zeigen Sie die Daten auf der Seite **Tags** an und arbeiten Sie mit ihnen:

- Erstellen Sie ein neues dynamisches Tag für Ihre OT-Assets. Dabei gilt:
  - Operator = Typ des Hostsystems
  - Wert = SPS
- Erstellen und verwalten Sie Tags, um verschiedene Asset-Klassen hervorzuheben oder zu kombinieren.
- Auf der Seite **Tag-Details** erhalten Sie weitere Informationen zu den Tags, die Ihren Assets zugeordnet sind.

## Voraussetzungen

> Ziel: Sicherstellen, dass Sie alles für eine erfolgreiche ICP-Installation besitzen.

Tenable OT Security ist eine Anwendung, die auf dem Betriebssystem Tenable Core ausgeführt wird und den Basisanforderungen von Tenable Core unterliegt.

Tenable Core + Tenable OT Security ist für die Bereitstellung sowohl auf Hardware als auch als VM-Appliance verfügbar. Für eine Bereitstellung als virtuelle Maschine müssen die in Hardwareanforderungen genannten Mindestanforderungen erfüllt sein.

### Hardwareanforderungen

Dedizierte Tenable Core + Tenable OT Security Hardware-Appliances sind in mehreren Größen verfügbar (separat erhältlich). Hardwarespezifikationen finden Sie im Tenable OT Security-Datenblatt zu physischer Hardware.

Das Betriebssystem Tenable Core und die Anwendung Tenable OT Security sind auf allen verfügbaren Hardware-Appliances vorinstalliert.

Sie können Tenable Core + Tenable OT Security auch auf benutzerdefinierter Hardware installieren, die die Anforderungen erfüllt. Wenden Sie sich an Tenable Support oder Ihren Customer Success Manager, um Anweisungen zu erhalten.

Informationen zu den Anforderungen für Tenable Core + Tenable OT Security finden Sie in folgenden Ressourcen:

- Systemanforderungen
- Zugriffsanforderungen

## Virtuelle Appliance – Anforderungen

Tenable Core + Tenable OT Security kann auf folgende Weise bereitgestellt werden:

- Mithilfe der `OVA`-Datei – Diese Datei kann sofort bereitgestellt werden und enthält die gesamte standardmäßige und unterstützte Konfiguration der virtuellen Maschine.
- Mithilfe der `ISO`-Datei – Dies ist ein universelles Image des Installationsdatenträgers. Stellen Sie diese Datei auf einer ordnungsgemäß konfigurierten virtuellen Maschine bereit, die die Anforderungen erfüllt.

## Lizenzanforderungen

Allgemeine Informationen zur Lizenzierung für OT Security finden Sie unter Lizenzkomponenten von OT Security.

Informationen zum Lizenzierungs-Workflow finden Sie unter Lizenzaktivierung für OT Security.

## Systemanforderungen

Tenable OT Security ist eine Anwendung, die auf dem Betriebssystem Tenable Core ausgeführt wird und den Basisanforderungen von Tenable Core unterliegt.

Um Tenable Core + OT Security oder OT Security Sensor zu installieren und auszuführen, müssen die Anwendung und das System die folgenden Anforderungen erfüllen.

Tipp: OT Security bietet einsatzfertige Appliances an, die direkt mit vorinstalliertem Image geliefert werden. Diese Option ist viel einfacher zu verwenden und bereitzustellen und bietet eine kürzere Amortisationszeit. Sie können jedoch auch Ihre eigene Hardware beschaffen und unser ISO-Image darauf anwenden. Wenn Sie Ihre eigene Hardware bereitstellen oder unsere Hardware verwenden möchten, finden Sie Anleitungen und bewährte Methoden in unseren Tenable OT-Hardwarespezifikationen. Alle Komponenten von OT Security, der ICP-EM und der Sensor können auf jeder Hardware ausgeführt werden, die die Spezifikationen erfüllt.

Hinweis: Tenable rät davon ab, mehrere Anwendungen auf einer einzigen Instanz von Tenable Core bereitzustellen. Wenn Sie mehrere Anwendungen auf Tenable Core bereitstellen möchten, stellen Sie für jede Anwendung eine eigene Instanz bereit.

Hinweis: Tenable-Support bietet keine Unterstützung bei Problemen im Zusammenhang mit dem Host-Betriebssystem, selbst wenn diese während der Installation oder Bereitstellung auftreten.

| Umgebung | | Tenable Core-Dateiformat | Weitere Informationen |
|---|---|---|---|
| Virtuelle Maschine | VMware | `OVA`-Datei | Tenable Core in VMware bereitstellen |
| | Microsoft Hyper-V | `ZIP`-Datei | |
| Hardware<br><br>Von Tenable bereitgestellte Hardware | | `ISO`-Image | Tenable Core auf Hardware installieren |

Hinweis: Sie könnten die Pakete verwenden, um Tenable Core in anderen Umgebungen auszuführen, Tenable bietet jedoch keine Dokumentation für diese Verfahren.

## OT Security – Hardwareanforderungen

Weitere Informationen zu spezifischen Hardwareanforderungen für OT Security oder OT Security Sensor finden Sie unter Tenable OT Security Hardware Specifications im Leitfaden *General Requirements*.

## OT Security – Anforderungen an virtuelle Hardware

Unternehmensnetzwerke können in puncto Leistung, Kapazität, Protokollen und Gesamtaktivität variieren. Für Bereitstellungen müssen unter anderem folgende Ressourcenanforderungen berücksichtigt werden: reale Netzwerkgeschwindigkeit, Größe des zu überwachenden Netzwerks und Konfiguration der Anwendung.

Die folgende Tabelle enthält grundlegende Richtlinien für den Einsatz von Tenable Core + OT Security in einer virtuellen Umgebung.

Tenable Core + OT Security erfordert CPUs mit AVX und AVX2 (z. B. Intel Haswell oder neuer).

| Installationsszenario | CPU-Kerne | Arbeitsspeicher | Festplattenspeicher |
|---|---|---|---|
| Virtuelle Maschine | 8 Kerne | 16 GB RAM | 205 GB |

## Anforderungen an virtuelle OT Security-Sensoren

| Installationsszenario | CPU | Arbeitsspeicher | Festplattenspeicher |
|---|---|---|---|
| Sensor | 2 virtuelle CPUs | 4 GB RAM | 60 GB HDD |

## Speicheranforderungen

Tenable empfiehlt, OT Security auf DAS-Geräten (Direct Attached Storage) zu installieren, vorzugsweise auf Solid-State-Laufwerken (SSD), um eine optimale Leistung zu erzielen. Tenable empfiehlt nachdrücklich die Verwendung von Solid-State-Speicher (SSS), der über eine hohe

DWPD-Rate (Laufwerksschreibvorgänge pro Tag) verfügt, um eine lange Lebensdauer zu gewährleisten.

Die Installation von OT Security auf NAS-Geräten (Network-Attached Storage) wird von Tenable nicht unterstützt. In diesen Fällen sind Speichernetzwerke (SAN) mit einer Speicherlatenz von maximal 10 Millisekunden oder Tenable Hardware-Appliances eine gute Alternative.

### Anforderungen an den Festplattenspeicher

Unternehmensnetzwerke können in puncto Leistung, Kapazität, Protokollen und Gesamtaktivität variieren. Für Bereitstellungen müssen unter anderem folgende Ressourcenanforderungen berücksichtigt werden: reale Netzwerkgeschwindigkeit, Größe des zu überwachenden Netzwerks und Konfiguration der Anwendung. Die Auswahl von Prozessoren, Arbeitsspeicher und Netzwerkkarte hängt stark von diesen Bereitstellungskonfigurationen ab. Die Anforderungen an den Festplattenspeicher hängen von der Nutzung auf Basis der Datenmenge und der Dauer der Datenspeicherung im System ab.

OT Security muss vollständige Paketerfassungen des überwachten Traffics durchführen, und die Größe der von OT Security gespeicherten Richtlinienereignisdaten hängt von der Anzahl der Geräte und dem Typ der Umgebung ab.

Sie können die Speicheranforderungen pro Tag (GB/Tag) berechnen, indem Sie die Traffic-Rate (Mbps) * 2,7 multiplizieren – basierend auf einem Komprimierungsfaktor von 0,25.

In einem Beispiel mit zwei Sensoren, die jeweils 23 Mbps SPAN-Traffic empfangen, wird der Speicherbedarf pro Tag (GB/Tag) berechnet als (23*2)*2,7=124 GB Speicherplatz pro Tag für die Traffic-Speicherung.

> Hinweis: Wenn Sie gemäß Compliance- oder Sicherheitsvorschriften Traffic von bis zu 30 Tagen speichern müssen, benötigen Sie ein PCAP-Speicherlaufwerk (Paketerfassung) mit 3,75 TB, um diese Anforderung zu erfüllen. Sobald die gespeicherten Traffic-Daten die maximale Größe erreicht haben, überschreibt OT Security die ältesten PCAP-Daten und ersetzt sie durch neuen Traffic.

### Richtlinien für ICP-Systemanforderungen

| Maximaler SPAN/TAP-Durchsatz (Mbit/s) | CPU-Kerne[1] | Arbeitsspeicher (DDR4) | Speicheranforderungen | Netzwerkschnittstellen |
|---|---|---|---|---|
| 50 Mbit/s oder weniger | 4 | 16 GB RAM | Mindestens 205 GB | Mindestens zwei Netzwerkschnittstellen |
| 50–150 Mbit/s | 16 | 32 GB RAM | Mindestens 205 GB | Mindestens zwei Netzwerkschnittstellen |
| 150–300 Mbit/s | 32 | 64 GB RAM | Mindestens 205 GB | Mindestens zwei Netzwerkschnittstellen |
| 300 Mbit/s bis 1 GB | 32-64 | 128 GB RAM oder mehr | Mindestens 205 GB | Mindestens zwei Netzwerkschnittstellen |

### Anforderungen an Festplattenpartitionen

OT Security verwendet die folgenden bereitgestellten Partitionen:

| Partition | Inhalt |
|---|---|
| / | Betriebssystem |
| /opt | Anwendungs- und Datenbankdateien |
| /var/pcap | Paketerfassungen (vollständige Paketerfassung, Ereignis, Abfrage) |

Im Standardinstallationsprozess werden diese Partitionen auf demselben Datenträger abgelegt. Tenable empfiehlt, diese zu Partitionen auf separaten Festplatten zu verschieben, um den Durchsatz zu erhöhen. OT Security ist eine festplattenintensive Anwendung. Die Verwendung von Festplatten mit hohen Lese-/Schreibgeschwindigkeiten, wie z. B. SSDs, ermöglicht die beste Leistung. Tenable empfiehlt, eine SSD mit hohen DWPD-Raten auf vom Kunden bereitgestellter Hardware zu verwenden, wenn die Paketerfassungsfunktion in OT Security genutzt wird.

> Tipp: Durch die Bereitstellung von OT Security auf einer Hardwareplattform, die mit einem redundanten Array unabhängiger Festplatten (RAID 0) konfiguriert ist, kann die Leistung erheblich verbessert werden.

> Tipp: Tenable erfordert selbst für unsere größten Kunden keine RAID-Laufwerke. In einem Fall änderten sich jedoch für einen Kunden mit mehr als einer Million verwalteter Schwachstellen die Antwortzeiten für Abfragen mit einer schnelleren RAID-Festplatte von einigen Sekunden auf weniger als eine Sekunde.

### Anforderungen an Netzwerkschnittstellen

Bevor Sie OT Security installieren, müssen zwei (oder mehr) Netzwerkschnittstellen auf Ihrem Gerät vorhanden sein. Tenable empfiehlt die Verwendung von Gigabit-Schnittstellen. Die VMWare OVA-Datei erstellt diese Schnittstellen automatisch. Erstellen Sie diese Schnittstellen manuell, wenn Sie die ISO-Datei installieren (z. B. Hyper-V).

> Hinweis: Tenable bietet keine SR-IOV-Unterstützung für die Verwendung von 10-G-Netzwerkkarten und garantiert bei Verwendung von 10-G-Netzwerkkarten keine 10-G-Geschwindigkeiten.

### Anforderungen an Netzwerkschnittstellen-Controller

- OT Security erfordert nur eine NIC für EM.
- OT Security erfordert mindestens zwei NICs für die ICP und die Sensoren.
- OT Security erfordert die Verwendung statischer IP-Adressen für ICP/EM/Sensoren.

- Sowohl der Sensor als auch die ICP können so konfiguriert werden, dass sie mehrere SPAN-Schnittstellen überwachen.

> Hinweis: Ab OT Security 4.1 lauten die Profilnamen für Netzwerkschnittstellen wie folgt:
>
> - nic0 – Systemport 1
> - nic1 – Systemport 2
> - nic2 – Systemport 3
> - nic3 – Systemport 4

nic0 oder Systemport 1 (192.168.1.5) und nic3 oder Systemport 4 (192.168.3.3) haben statische IP-Adressen, wenn Sie Tenable Core + OT Security in einer Hardware- oder virtuellen Umgebung installieren. Andere Netzwerkschnittstellen-Controller (Network Interface Controllers, NICs) verwenden DHCP.

nic3 oder Systemport 4 (192.168.3.3) hat eine statische IP-Adresse, wenn Sie Tenable Core + OT Security auf VMware bereitstellen. Andere NICs verwenden DHCP. Bestätigen Sie, dass die MAC-Adresse von nic1 oder Systemport 2 in Tenable Core + OT Security mit der MAC-Adresse des NIC in Ihrer VMware-Konfiguration für passives Scannen übereinstimmt. Ändern Sie bei Bedarf Ihre VMware-Konfiguration so, dass sie mit Ihrer MAC-Adresse in Tenable Core übereinstimmt.

Weitere Informationen finden Sie unter Manually Configure a Static IP Address, Manage System Networking und in der *VMware-Dokumentation*.

[1]„CPU-Kerne“ bezieht sich auf PHYSISCHE Kerne und setzt CPUs der Serverklasse voraus (Xeon, Opteron).

## Zugriffsanforderungen

Ihre Bereitstellung von Tenable Core und OT Security Sensor muss die folgenden Anforderungen erfüllen.

- Internetanforderungen
- Portanforderungen

## Internetanforderungen

Sie müssen über Internetzugriff verfügen, um Tenable Core-Dateien herunterzuladen und Online-Installationen durchzuführen.

Nachdem Sie eine Datei auf Ihren Computer übertragen haben, variieren die Internetzugriffsanforderungen zum Bereitstellen oder Aktualisieren von Tenable Core je nach Umgebung.

> Hinweis: Sie müssen `appliance.cloud.tenable.com` erreichen können, um die Online-ISOs für Installationen verwenden zu können (und um Online-Updates zu erhalten), und `sensor.cloud.tenable.com`, um Scan-Jobs auszuwählen.

| Umgebung | | Tenable Core-Format | Internetanforderungen |
|---|---|---|---|
| Virtuelle Maschine | VMware | `OVA`-Datei | Sie benötigen für die Bereitstellung oder Aktualisierung von Tenable Core keinen Internetzugriff. |
| | Microsoft Hyper-V | `ZIP`-Datei | |
| Cloud | Amazon Web Services (AWS) | N/A | Für die Bereitstellung oder Aktualisierung von Tenable Core ist Internetzugriff erforderlich. |
| Cloud | Microsoft Azure | N/A | |
| Hardware | | `ISO`-Image | Für die Installation und Aktualisierung von Tenable Core ist Internetzugriff erforderlich. |

Tipp: Sie benötigen keinen Zugriff auf das Internet, wenn Sie Updates für Tenable Core und Tenable OT Security Sensor über eine Offline-`ISO`-Datei installieren. Weitere Informationen finden Sie unter Update Tenable Core Offline.

## Portanforderungen

Ihre Tenable Core-Bereitstellung erfordert Zugriff auf bestimmte Ports für ein- und ausgehenden Traffic. OT Security erfordert außerdem anwendungsspezifischen Portzugriff. Weitere Informationen finden Sie unter Überlegungen zur Firewall.

### Eingehender Traffic

Lassen Sie eingehenden Traffic zu folgenden aufgeführten Ports zu.

Hinweis: Eingehender Traffic bezieht sich auf Traffic von Benutzern, die Tenable Core konfigurieren.

| Port | Traffic |
|---|---|
| TCP 22 | Eingehende SSH-Verbindungen. |
| TCP 443 | Eingehende Kommunikation an die OT Security-Schnittstelle. |
| TCP 8000 | (Standard) Eingehende HTTPS-Kommunikation an die Tenable Core-Schnittstelle. |
| TCP 8090 | Eingehende HTTPS-Kommunikation zur Wiederherstellung von Sicherungen.<br><br>Eingehende Kommunikation mit dem Datei-Upload-Server. |

### Ausgehender Traffic

Lassen Sie ausgehenden Traffic zu folgenden aufgeführten Ports zu.

| Port | Traffic |
|---|---|

| | |
|---|---|
| TCP 22 | Ausgehende SSH-Verbindungen, einschließlich Remotespeicher-Verbindungen. |
| TCP 443 | Ausgehende Kommunikation an die Server `appliance.cloud.tenable.com` und `sensor.cloud.tenable.com` für System-Updates. |
| UDP 53 | Ausgehende DNS-Kommunikation für OT Security und Tenable Core. |

## Überlegungen zum Netzwerk

Die OT Security-Appliance (sowohl physisch als auch virtuell) erfordert einige Netzwerkverbindungen, die als Schnittstellenrollen bezeichnet werden.

### Schnittstelle für Verwaltung und aktive Abfragen

Das ist eine Schnittstelle, die mit einer IP-Adresse konfiguriert ist, über die das Netzwerk erreicht werden kann, um die Appliance zu verwalten und zu konfigurieren. Über diese Schnittstelle kann das Gerät auf Assets im Netzwerk zugreifen, um aktive Abfragen durchzuführen (empfohlen, aber optional).

### Trennung der Rollen für Verwaltung und aktive Abfragen (Split-Port)

Sie können die Rollen für Verwaltung und aktive Abfragen auf zwei separate Schnittstellen aufteilen. So können Sie beispielsweise zu Verwaltungszwecken eine Verbindung zu einem IT-Netzwerk herstellen und eine separate Verbindung zu einem OT-Netzwerk, um über aktive Abfragen auf die OT-Assets zuzugreifen.

Bereiten Sie zu diesem Zweck zwei separate Schnittstellen vor, die jeweils einer der Rollen zugeordnet sind, und verbinden Sie sie.

Eine grundlegende Verwaltungskonnektivität zur ICP über die Schnittstelle für aktive Abfragen ist zulässig und funktionsfähig, sofern das ICP-System Netzwerkkonnektivität zulässt.

Um das Setup von OT Security abzuschließen, benötigen Sie Verwaltungskonnektivität. Die Konnektivität für Split-Port und aktive Abfragen können Sie später konfigurieren.

Auf von Tenable bereitgestellten Hardware-Appliances wird OT Security automatisch mit den Standardschnittstellenrollen (kombinierte Rollen für Verwaltung und aktive Abfragen) installiert.

> Hinweis: Bei der Konfiguration der IP-Adresse für beide Schnittstellen empfiehlt Tenable, nur ein Standard-Gateway für die Schnittstelle zu konfigurieren, der die Verwaltungsrolle zugeordnet ist. Bei der Konfiguration von Split-Port können Sie ein dediziertes Gateway für aktive Abfragen angeben.

### Monitoring-Schnittstellen

Für das passive Netzwerk-Monitoring können eine oder mehrere Netzwerkschnittstellen verwendet werden. Schnittstellen für passives Monitoring (SPAN):

- überwachen und erfassen Traffic zu Analysezwecken
- müssen mit einer Spiegelungs-, Switch Port Analyzer (SPAN)- oder Remote Switch Port Analyzer (RSPAN)-Zielschnittstelle eines Switch verbunden sein.

> Hinweis: Traffic, der nicht direkt von den Appliance-Schnittstellen überwacht werden kann, kann mithilfe von OT-Sensoren oder ERSPAN-Konfiguration erfasst werden.

## Überlegungen zur Firewall

Beim Einrichten Ihres OT Security-Systems ist es wichtig, die offenen Ports zu bestimmen, damit das Tenable-System ordnungsgemäß funktioniert. Die folgenden Tabellen geben die Ports an, die für die Verwendung mit OT Security ICP und den OT Security Sensoren reserviert werden müssen, sowie die Ports, die für die Ausführung von aktiven Abfragen und für die Integration mit Tenable Vulnerability Management und Tenable Security Center benötigt werden.

> Hinweis: Informationen zur Liste der Tenable-Websites und -Domänen, die Sie in der Firewall zulassen müssen, finden Sie im Wissensdatenbankartikel.

### OT Security Core-Plattform

Die folgenden Ports sollten für die Kommunikation mit der OT Security Core-Plattform offen bleiben.

> Hinweis: Damit die zentralisierten EM-Updates funktionieren, muss der ICP die Ports 28305 und 8000 (TCP) erreichen können.

| Flussrichtung | Port | Kommuniziert mit | Zweck |
|---|---|---|---|
| Eingehend | TCP 443 | Weboberfläche für die OT Security Appliance | Browserzugriff auf OT Security |
| Eingehend | TCP 8000 | Weboberfläche für Tenable Core | Browserzugriff auf Tenable Core |
| Eingehend | TCP 443 und TCP 28304 | OT-Sensor | Sensorauthentifizierung, Kopplung und Empfang von Sensorinformationen. |
| Ausgehend | TCP 443 und TCP 28305 | OT Security EM | ICP- und EM-Kopplung |
| Eingehend | TCP 22 | Appliance für SSH-Zugriff | Befehlszeilenzugriff auf Betriebssystem oder Appliance |
| Ausgehend | TCP 443 | Tenable Security Center | Sendet Daten zur Integration |
| Ausgehend* | TCP 443 | cloud.tenable.com | Sendet Daten zur Integration |
| Ausgehend* | Verschiedene Industrieprotokolle | SPS/Steuerungen | Aktive Abfrage |
| Ausgehend* | TCP 25 oder 587 | E-Mail-Server für | SMTP (Warn-E-Mails, |

| Flussrichtung | Port | Kommuniziert mit | Zweck |
|---|---|---|---|
| | | Warnmeldungen | Berichte) |
| Ausgehend* | UDP 514 | Syslog-Server | Sendet Richtlinien-Ereigniswarnungen und Syslog-Meldungen |
| Ausgehend* | UDP 53 | DNS-Server | Namensauflösung |
| Ausgehend* | UDP 123 | NTP-Server | Zeitdienst |
| Ausgehend* | TCP 389 oder 636 | AD-Server | AD-LDAP-Authentifizierung |
| Ausgehend* | TCP 443 | SAML-Anbieter | Single Sign-On (SSO) |
| Ausgehend* | UDP 161 | SNMP-Server | SNMP-Überwachung an Tenable Core |
| Ausgehend* | TCP 443 | *.tenable.com<br>*.nessus.org | Automatische Plugin-, Anwendungs- und Betriebssystem-Updates** |
| Ausgehend | TCP 10146 (sicherer Port) | IoT-Connector | Verbindet ICP mit dem IoT-Connector-Agent |

* Optionale Dienste

** Offline-Verfahren verfügbar

## OT Security Sensoren

Die folgenden Ports sollten für die Kommunikation mit OT Security Sensoren offen bleiben.

| Flussrichtung | Port | Kommuniziert mit | Zweck |
|---|---|---|---|
| Eingehend | TCP 8000 | Weboberfläche | Browserzugriff auf Benutzer-GUI |
| Eingehend | TCP 22 | Appliance für SSH-Zugriff | Befehlszeilenzugriff auf Betriebssystem oder Appliance |
| Ausgehend* | TCP 25 | E-Mail-Server für Warnmeldungen | SMTP (Warn-E-Mails, Berichte) |
| Ausgehend* | UDP 53 | DNS-Server | Namensauflösung |
| Ausgehend* | UDP 123 | NTP-Server | Zeitdienst |
| Ausgehend* | UDP 161 | SNMP-Server | SNMP-Überwachung an Tenable Core |
| Ausgehend | TCP 28303 | ICP/OT Security Sendet Kommunikation vom Sensor, empfängt auf ICP/OT Security | Nicht authentifizierte/nur passive Sensorverbindung |
| Ausgehend | TCP 28304 (SSH)<br>TCP 443 (HTTPS) | ICP/OT Security<br>SSH-Verbindungen für die Sensorkopplung. Sendet Kommunikation vom Sensor, empfängt auf ICP/OT Security | Authentifizierter/sicherer Tunnel zwischen Sensor und ICP |

* Optionale Dienste

## Aktive Abfrage

Die folgenden Ports müssen offen bleiben, um die aktiven Abfragen nutzen zu können.

> Hinweis: OT Security unterstützt Abfragen in diesen Protokollen, jedoch gelten möglicherweise nicht alle für Ihre Umgebung. Um optimale Ergebnisse zu erzielen, öffnen Sie so viele der aufgeführten Ports wie möglich zwischen OT Security (oder den OT Security-Sensoren) und den nahegelegenen Remote-Geräten. Dies ermöglicht eine genaue Identifizierung und Abfrage.

| Protokoll | Port | Kommuniziert mit | Zweck |
|---|---|---|---|
| ICMP | | Generisch/Verschiedene | Asset-Erfassung/Ping auf Netzwerkebene |
| TCP | 21 | Generisch/Verschiedene | FTP-Dateiübertragung |
| TCP/UDP | 53 | DNS-Server | Abfragen für die DNS-Auflösung |
| TCP | 80 | Generisch/Verschiedene | HTTP-Fingerprinting und Zugriff auf die Weboberfläche |
| TCP | 102 | Siemens-Geräte | Manufacturing Message Specification (MMS), überlappt IEC 61850 |
| TCP | 102 | Siemens-Geräte | IEC 61850/MMS für Unterstationen und SCADA-Geräte |
| TCP | 102 | Siemens-Geräte | S7/S7+-/MMS-Kommunikation für Automatisierungsgeräte |
| UDP | 111 | Emerson Ovation-Geräte | Registrierung/Erfassung des RPC-Diensts für Ovation |
| TCP | 135 | Windows-Geräte | WMI-Abfragen für die System- und |

| Protokoll | Port | Kommuniziert mit | Zweck |
|---|---|---|---|
| | | | Netzwerkverwaltung |
| UDP | 137 | Generisch/Verschiedene | NetBIOS Name Service (NBNS) für Windows-Netzwerkerfassung |
| UDP | 138 | Generisch/Verschiedene | NetBIOS Datagram Service (NBT) für Datei-/Druckerfreigabe unter Windows |
| UDP | 161 | Generisch/Verschiedene | SNMP-Abfrage und -Trap-Kommunikation |
| TCP | 443 | Generisch/Verschiedene | HTTPS-Fingerprinting und sichere Webdienste |
| TCP | 445 | Windows-Geräte | WMI/SMB-Abfragen für die Systemverwaltung (ersetzt in einigen Fällen 135) |
| TCP | 502 | OT-Geräte | Modbus TCP-Kommunikation mit SPS und Zählern |
| UDP | 1069 | Cognex-Kameras | Erfassungsprotokoll für Cognex Vision-System |
| TCP | 1911 | BMS-Controller | Unverschlüsseltes Niagara FOX-Protokoll |
| TCP | 1962 | Phoenix Contact-Geräte | PC Worx-Engineering und -Steuerungskommunikation |
| TCP/UDP | 2001 | Profinet-Geräte | Profinet-Gerätekommunikation für |

| Protokoll | Port | Kommuniziert mit | Zweck |
|---|---|---|---|
| | | | Controller und E/A-Module |
| TCP | 2001 | Siemens-Geräte | SICAM/PROFINET (ältere Geräte und Unterstationen) |
| TCP | 2222 | Rockwell-Geräte | PCCC-Protokoll für die ControlLogix/SPS-Kommunikation |
| TCP | 2404 | SCADA-Geräte | IEC 60870-5-104 für RTU- und Unterstationskommunikation |
| TCP | 3389 | Windows-Geräte | RDP (Remote Desktop Protocol) |
| TCP | 3500 | Bachmann M1-Geräte | Bachmann M1-Controller-Kommunikation |
| TCP | 4000 | Emerson-Geräte | Daten/Steuerung des Emerson ROC 4000-Controllers |
| TCP | 4444 | Schneider Electric | SmartX-Controller (EcoStruxure Building Operation) |
| UDP | 4800 | Moxa-Geräte | Moxa-Geräteerfassungsprotokoll |
| TCP | 4911 | BMS-Controller | Niagara FOX Secure-Protokoll (TLS/SSL) |
| TCP | 5001 | Bosch-Geräte | Bosch PSI (Programmable System Interface) |
| TCP | 5002 | Mitsubishi-Geräte | MELSEC-SPS-MC-Protokoll über TCP |

| Protokoll | Port | Kommuniziert mit | Zweck |
|---|---|---|---|
| TCP | 5007 | Mitsubishi-Geräte | Zusätzlicher Kommunikationsport der MELSEC SPS |
| UDP | 5009 | Mitsubishi-Geräte | MELSEC-Finder-Broadcast (Geräteerfassung) |
| TCP | 5033 | Siemens-Geräte | P2-Protokoll (in älteren Siemens-Automatisierungssystemen verwendet) |
| TCP | 5050 | Saia-Burgess-Geräte | Saia PCD-Controller-Kommunikation |
| TCP | 5094 | HART-IP | HART-IP über TCP für intelligente Instrumentierung |
| TCP | 5313 | Yokogawa DCS | CENTUM DCS-Engineering-Oberfläche |
| TCP | 5432 | SEL-Geräte (Schweitzer) | Zugriff auf die PostgreSQL-Datenbank für Energiegeräte |
| TCP | 6626 | WAGO-Geräte | WAGO-E/A-Kommunikation und -Programmierung |
| TCP | 7700 | Schneider Electric | ION-Stromzähler und -Energiemanagementsysteme |
| TCP | 8000, 8008, 8080, | Generisch/Verschiedene | Gängige alternative HTTP/HTTPS-Ports |

| Protokoll | Port | Kommuniziert mit | Zweck |
|---|---|---|---|
| | 8443, 8800 | | |
| TCP | 9940 | Yokogawa DCS | CENTUM-Status und -Diagnose |
| UDP | 12321 | Honeywell-Geräte | Honeywell FTE UDP-Erfassung/Redundanz |
| TCP | 18245 | Schneider-Geräte | SRTP (Schneider Real-Time Protocol) für M340-/M580-SPS |
| TCP | 18507 | Emerson-Geräte | Emerson ROC/Mengenumwerter (FACE-Protokoll) |
| TCP | 18508 | Emerson-Geräte | Emerson-Firmware-Upgrade-Service (UPGD) |
| TCP | 20256 | GE-Geräte | PCOM-Protokoll für Proficy iFIX/CIMPLICITY SCADA |
| TCP | 20547 | Procon | PROCON OS-Remote-Verwaltungsoberfläche |
| TCP | 24576 | ABB-Geräte | ABB Network Control (ABB_NC)-Protokoll für die Automatisierung von Unterstationen |
| TCP | 34964 | Siemens-Geräte | PROFINET-Verbindungsverwaltung (PROFINET CM) |
| TCP | 39329 | Emerson-Geräte | Ovation-/VME-basierte |

| Protokoll | Port | Kommuniziert mit | Zweck |
|---|---|---|---|
| | | | Steuerungssysteme |
| TCP/UDP | 44818 | OT-Geräte | CIP (Common Industrial Protocol) für Rockwell-Geräte |
| UDP | 47808 | BMS-Controller | BACnet/IP-Kommunikation für Gebäudeautomatisierungsgeräte |
| TCP/UDP | 48898 | Beckhoff-Geräte | ADS/TwinCAT-Protokoll für die Controller- und Engineering-Kommunikation |
| UDP | 48899 | Beckhoff-Geräte | ADS/AMS-Erfassung (TwinCAT-/Beckhoff-IPCs) |
| TCP | 50000 | Siemens-Geräte | SIPROTEC 4-Relay-Kommunikation |
| TCP | 51966 | Honeywell-Geräte | Honeywell FTE-Kommunikation (Fault Tolerant Ethernet) |
| TCP | 55553 | Honeywell-Geräte | CEE-Kommunikation (Control Execution Environment) in Experion PKS |
| TCP | 55565 | Honeywell-Geräte | FTE-Kommunikation (Fault Tolerant Ethernet) für Redundanz in Experion PKS |

OT Security-Integrationen

Die folgenden Ports sollten für die Kommunikation mit der Tenable Vulnerability Management- und der Tenable Security Center-Integration offen bleiben.

| Flussrichtung | Port | Kommuniziert mit | Zweck |
|---|---|---|---|
| Ausgehend | TCP 443 | cloud.tenable.com | Tenable Vulnerability Management-Integration |
| Ausgehend | TCP 443 | Tenable Security Center | Tenable Security Center-Integration |

### OT-Agent

| Flussrichtung | Port | Kommuniziert mit | Zweck |
|---|---|---|---|
| Ausgehend | 443 | OT Security | Erstmalige Kopplung mit einem OT-Agent. |
| Ausgehend | 28306 | OT Security | Verbindung mit dem OT-Agent. |

### IoT-Connector-Agent

| Flussrichtung | Port | Kommuniziert mit | Zweck |
|---|---|---|---|
| Ausgehend | TCP 10146 (sicherer Port) | IoT-Connector | Verbindet ICP mit dem IoT-Connector-Agent |
| Ausgehend | TCP 10104 (unsicherer Port) | IoT-Connector | Verbindet ICP mit dem IoT-Connector-Agent |

| | | | |
|---|---|---|---|
| | | | |

# OT Security ICP installieren

Ziel: Installation und Betriebsbereitschaft des ICP für OT Security.

## Bevor Sie beginnen

- Siehe Voraussetzungen.

Führen Sie nach Bedarf diese Schritte aus, um OT Security ICP zu installieren und eine Verbindung mit dem Netzwerk herzustellen:

- OT Security ICP-Hardware-Appliance installieren

  Hinweis: Auf der von Tenable bereitgestellten Tenable Core-Hardware ist Tenable Core + OT Security vorinstalliert. Wenn Sie eine ältere oder veraltete Appliance installieren, sollten Sie sich möglicherweise für eine Neuinstallation entscheiden. Weitere Informationen finden Sie unter Neuinstallation von Tenable Core + Tenable OT Security auf von Tenable bereitgestellter Hardware.

- Virtuelle OT Security ICP-Appliance installieren

## Nächster Schritt

- OT Security mit dem Netzwerk verbinden

## OT Security ICP-Hardware-Appliance installieren

Sie können die OT Security Appliance entweder in einem Rack montieren oder einfach auf eine ebene Oberfläche wie einen Schreibtisch stellen.

Tipp: Tenable empfiehlt, dass Sie die unter Tenable Core einrichten beschriebene grundlegende Konfiguration und Einrichtung und den OT Security-Setup-Assistenten bequem von Ihrem

Schreibtisch aus ausführen, bevor Sie die Appliance in ein Rack oder an einen anderen Remote-Standort verschieben.

## Rack-Montage

So montieren Sie die OT Security Appliance in einem 19-Zoll-Standard-Rack:

1. Setzen Sie die Servereinheit in einen freien 1-HE-Steckplatz im Rack ein.

   Hinweis:
   - Stellen Sie sicher, dass das Rack geerdet ist.
   - Stellen Sie sicher, dass der Lufteinlass des Lüfters (in der Rückwand) und die Belüftungsöffnungen (an der Oberseite) nicht blockiert sind.

2. Sichern Sie das Gerät am Rack, indem Sie die Rack-Montage-Halterungen (mitgeliefert) am Rack-Rahmen befestigen. Verwenden Sie dabei geeignete Schrauben für die Rack-Montage (nicht mitgeliefert).

3. Stecken Sie das eine Ende des Wechselstromkabels (mitgeliefert) in den Stromversorgungsanschluss in der Rückwand und das andere Ende in die Wechselstromversorgung (Netz).

## Ebene Oberfläche

So installieren Sie die OT Security Appliance auf einer ebenen Oberfläche:

1. Stellen Sie die Geräteeinheit auf eine trockene, ebene Oberfläche (z. B. einen Schreibtisch).

   Hinweis:
   - Stellen Sie sicher, dass die Tischplatte eben und trocken ist.
   - Stellen Sie sicher, dass der Lufteinlass des Lüfters (in der Rückwand) und die Belüftungsöffnungen (an der Oberseite) nicht blockiert sind.
   - Wenn Sie ein Gerät zusammen mit anderen Elektrogeräten aufstellen, vergewissern Sie sich, dass hinter dem Lüfter (in der Rückwand) genügend Platz ist, um eine ausreichende Belüftung und Kühlung zu gewährleisten.

2. Stecken Sie das eine Ende des Wechselstromkabels (mitgeliefert) in den Stromversorgungsanschluss in der Rückwand und das andere Ende in die Wechselstromversorgung (Netz).

Weitere Informationen zur Konnektivität finden Sie unter Überlegungen zum Netzwerk.

### Nächste Schritte

OT Security mit dem Netzwerk verbinden

## Neuinstallation von Tenable Core + Tenable OT Security auf von Tenable bereitgestellter Hardware

Tenable Core + OT Security sind auf einsatzfertiger, offiziell von Tenable bereitgestellter Hardware vorinstalliert. In einigen Fällen wird eine Neuinstallation (auch als erneutes Flashen bezeichnet) empfohlen.

> Hinweis: Wenn Sie vor Kurzem eine neue Appliance erhalten haben, können Sie dieses Verfahren überspringen.

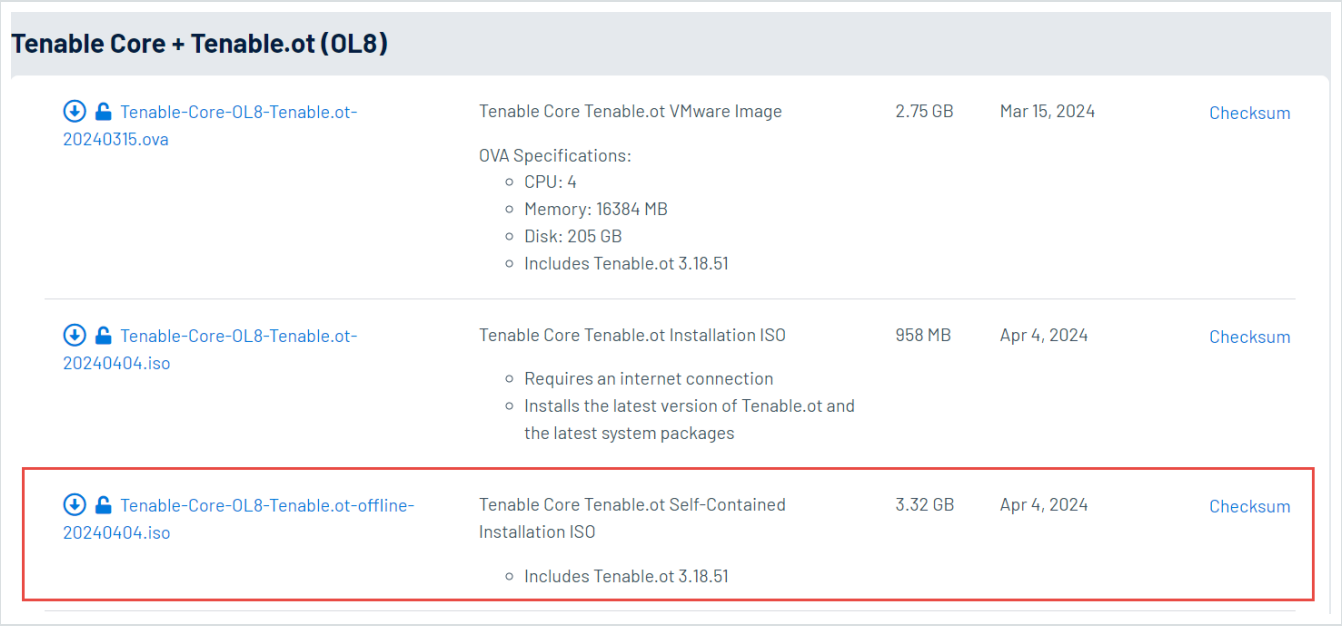
### Bevor Sie beginnen

Vergewissern Sie sich, dass Sie über Folgendes verfügen:

- Eine Anwendung zum Formatieren und Erstellen bootfähiger USB-Flash-Laufwerke wie Rufus.
- Ein serielles Kabel.
- Eine serielle Terminalanwendung, wie z. B. PuTTY.
- Einen USB-Speicherstick mit ca. 8 GB+.

### So installieren Sie die ISO-Datei von Tenable Core + OT Security:

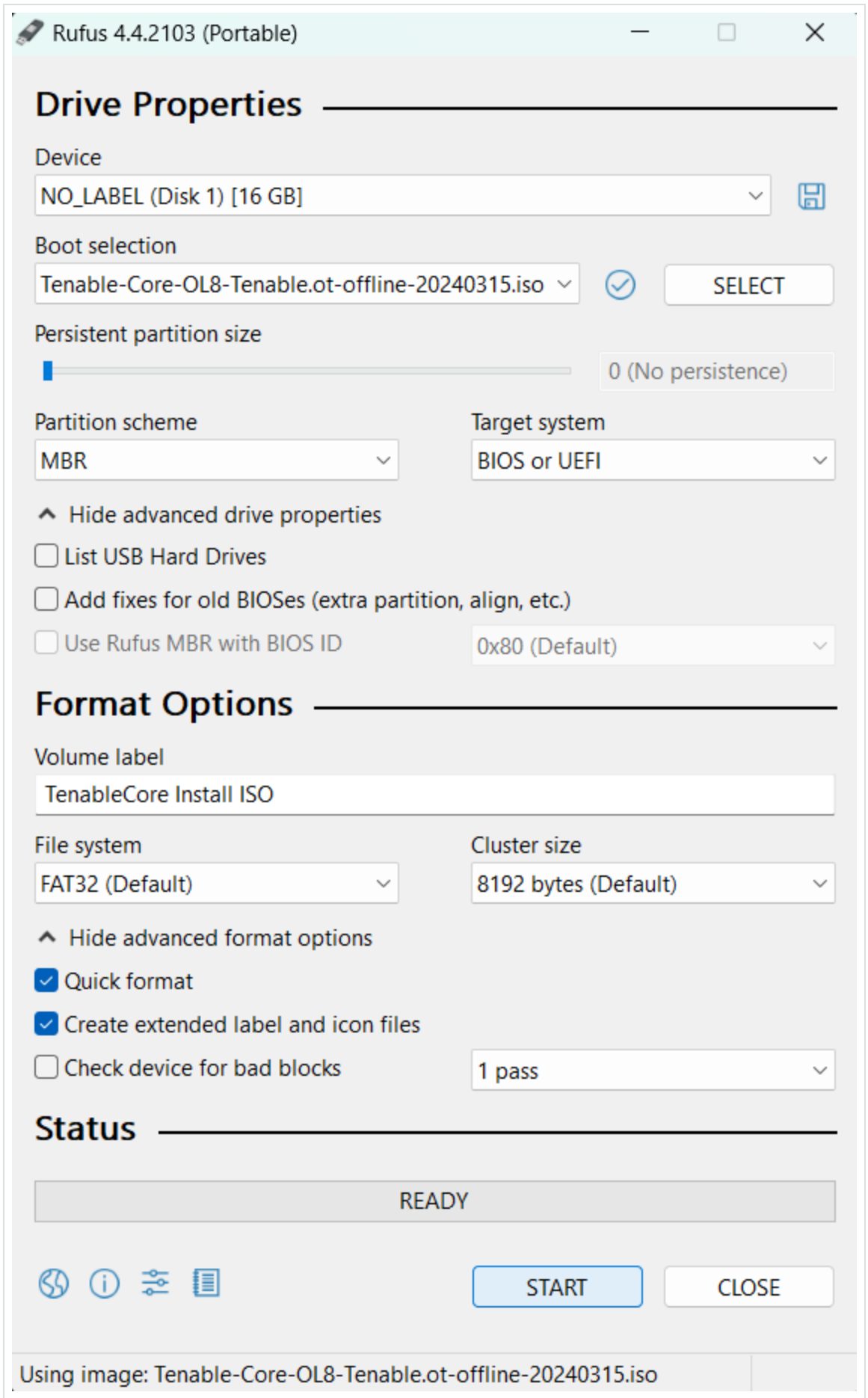
1. Laden Sie die neueste Offline-ISO-Datei unter Tenable Downloads herunter.

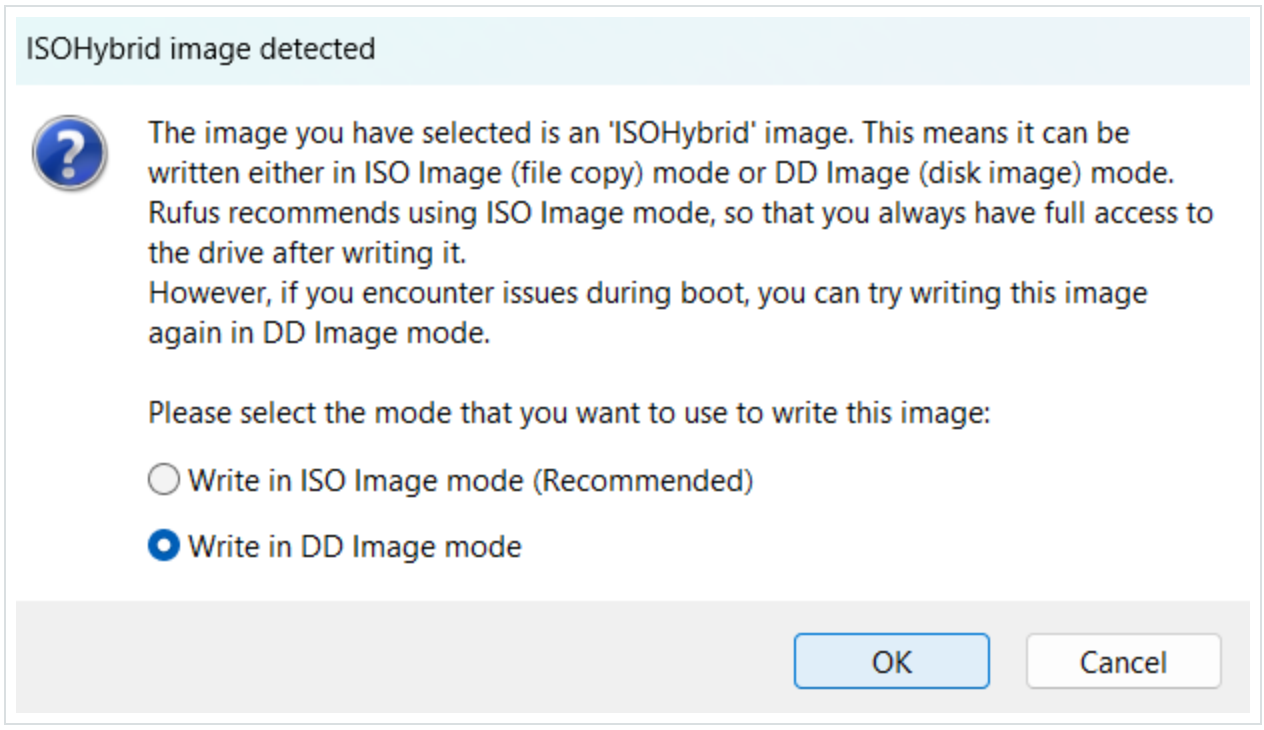


**Tenable Core + Tenable.ot (OL8)**

| | | | | |
|---|---|---|---|---|
| Tenable-Core-OL8-Tenable.ot-20240315.ova | Tenable Core Tenable.ot VMware Image<br>OVA Specifications:<br>○ CPU: 4<br>○ Memory: 16384 MB<br>○ Disk: 205 GB<br>○ Includes Tenable.ot 3.18.51 | 2.75 GB | Mar 15, 2024 | Checksum |
| Tenable-Core-OL8-Tenable.ot-20240404.iso | Tenable Core Tenable.ot Installation ISO<br>○ Requires an internet connection<br>○ Installs the latest version of Tenable.ot and the latest system packages | 958 MB | Apr 4, 2024 | Checksum |
| Tenable-Core-OL8-Tenable.ot-offline-20240404.iso | Tenable Core Tenable.ot Self-Contained Installation ISO<br>○ Includes Tenable.ot 3.18.51 | 3.32 GB | Apr 4, 2024 | Checksum |

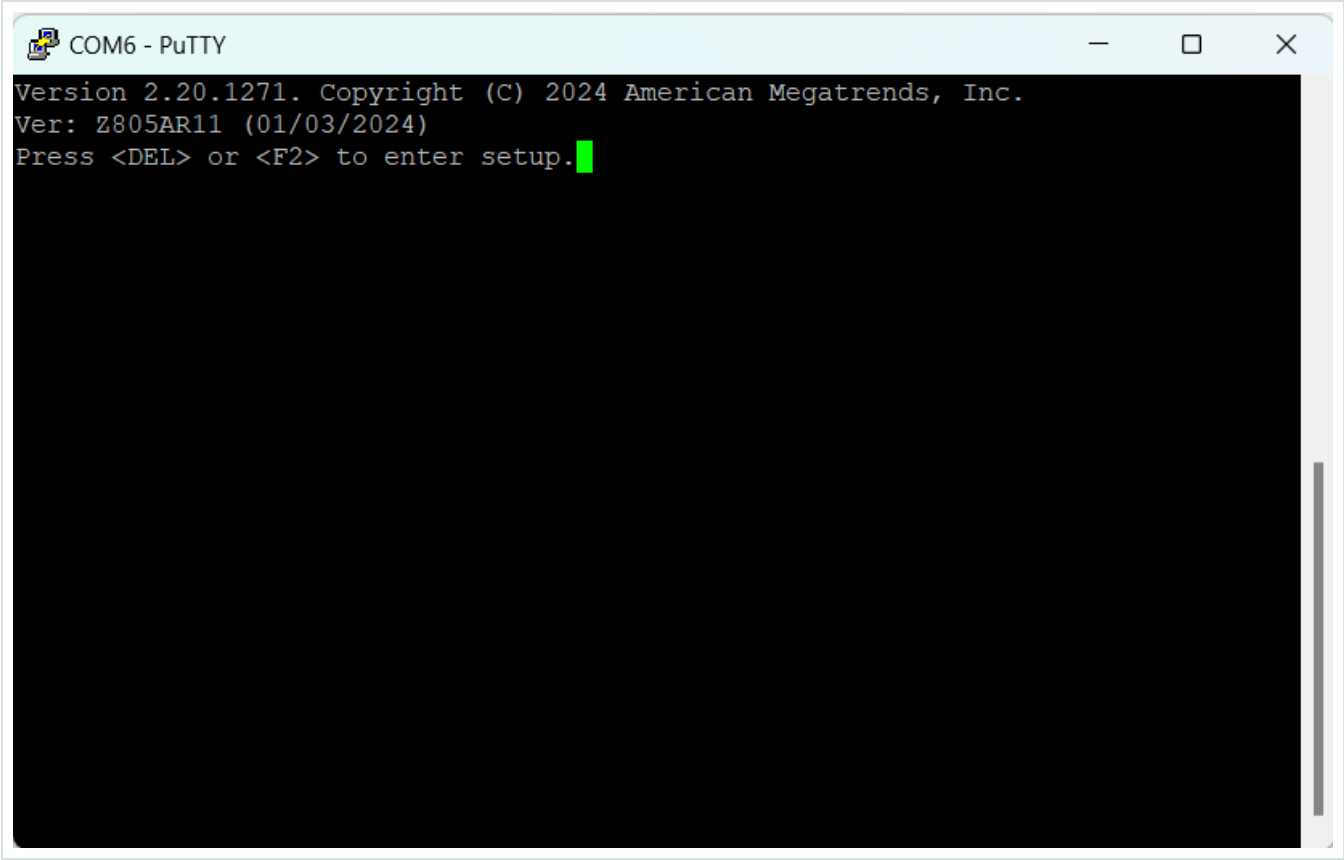
2. Stecken Sie den USB-Speicherstick in einen PC und flashen Sie die ISO im DD-Modus auf den Speicherstick.


Rufus 4.4.2103 (Portable)
Drive Properties
Device
NO_LABEL (Disk 1) [16 GB]
Boot selection
Tenable-Core-OL8-Tenable.ot-offline-20240315.iso
SELECT
Persistent partition size
0 (No persistence)
Partition scheme
MBR
Target system
BIOS or UEFI
Hide advanced drive properties
List USB Hard Drives
Add fixes for old BIOSes (extra partition, align, etc.)
Use Rufus MBR with BIOS ID
0x80 (Default)
Format Options
Volume label
TenableCore Install ISO
File system
FAT32 (Default)
Cluster size
8192 bytes (Default)
Hide advanced format options
Quick format
Create extended label and icon files
Check device for bad blocks
1 pass
Status
READY
START
CLOSE
Using image: Tenable-Core-OL8-Tenable.ot-offline-20240315.iso



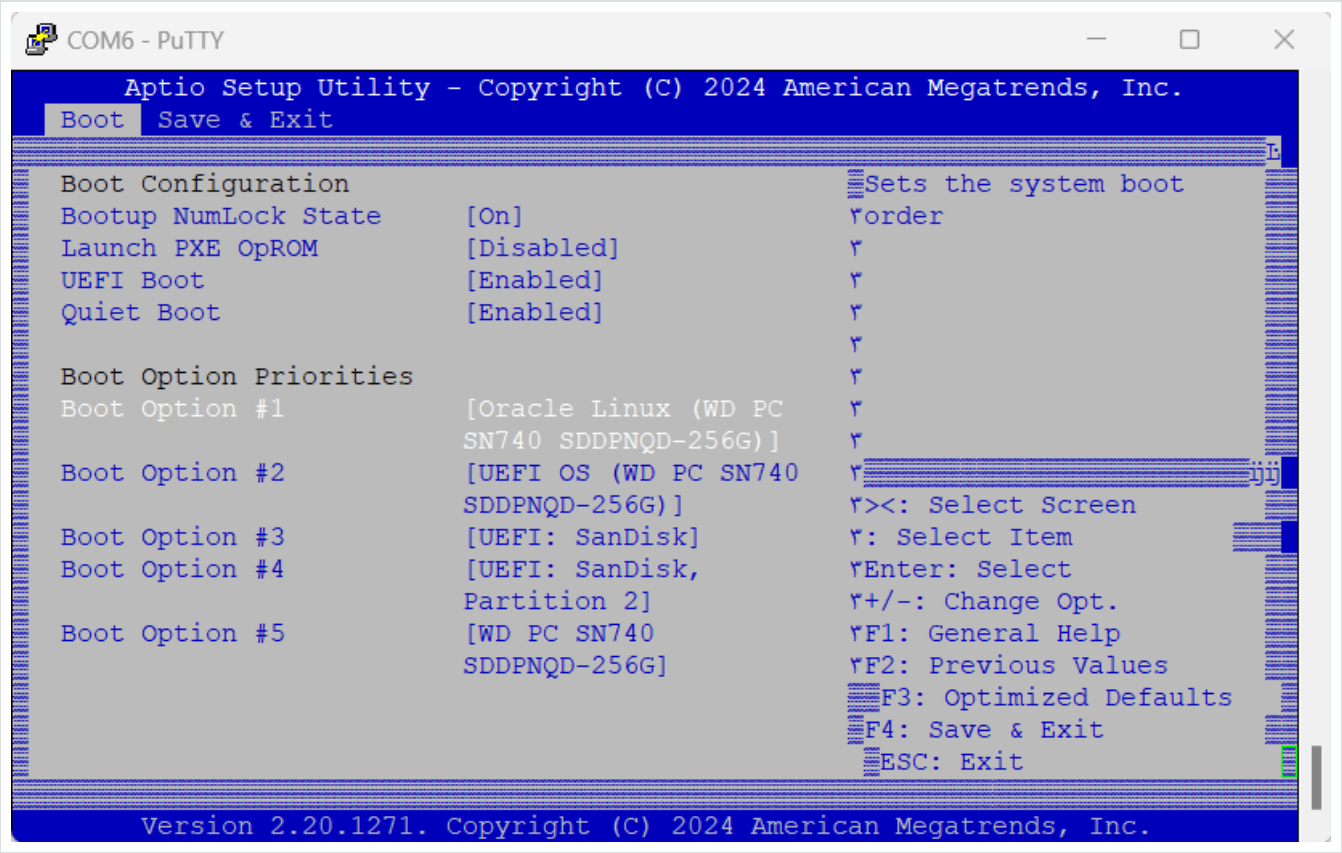

3. Wenn Sie fertig sind, stecken Sie den USB-Speicherstick in einen USB-Port der OT Security Appliance.

4. Stellen Sie über die serielle Schnittstelle der Konsole eine Verbindung zur Appliance her (Baudrate 115.200 Bit/s mit einer 8N1-Konfiguration) und schalten Sie die Appliance ein.



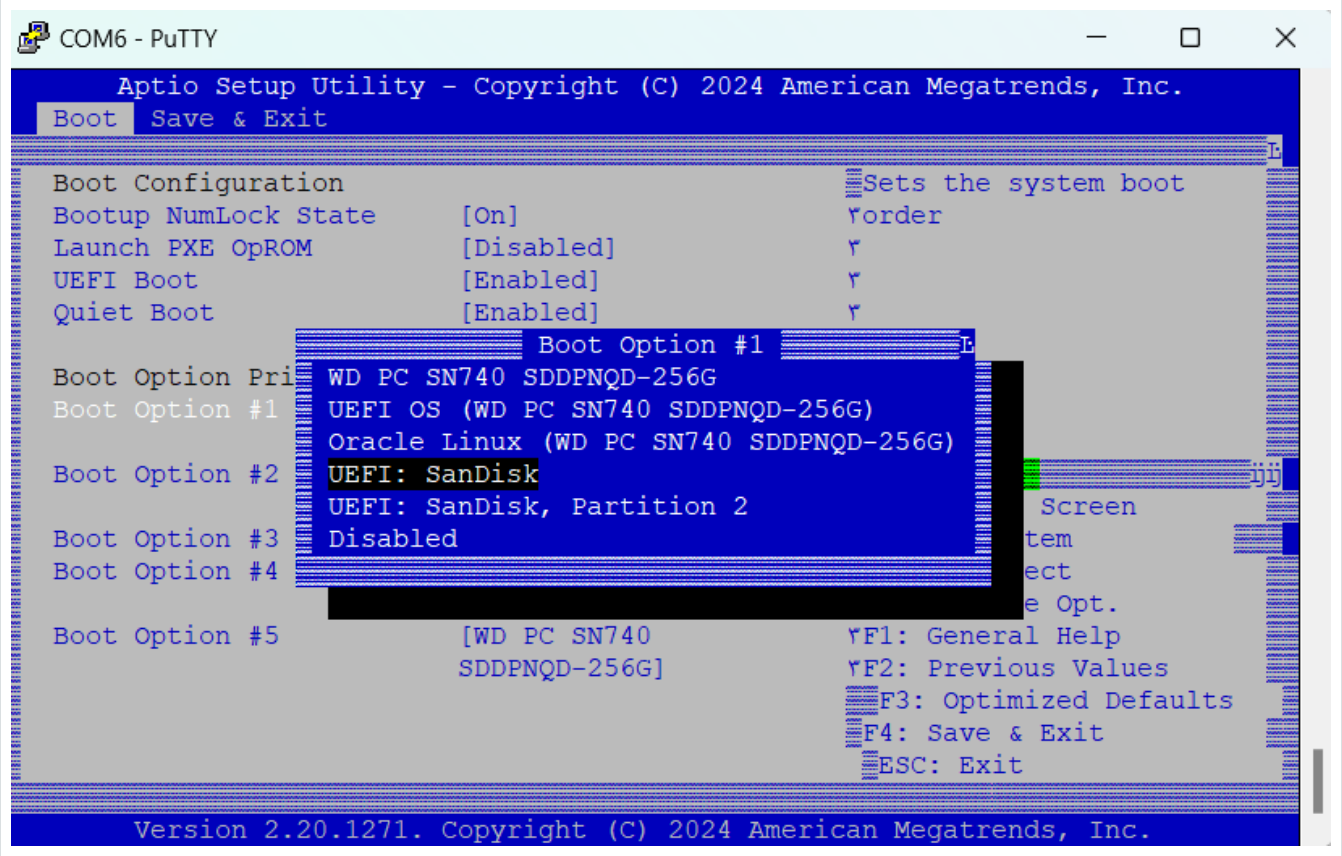

5. Wenn Sie dazu aufgefordert werden, drücken Sie <DEL>, um das Setup zu starten.

6. Navigieren Sie im System-Setup mit den Pfeiltasten zum Abschnitt Boot (Start).




7. Wählen Sie Boot-Option #1 (Startoption 1) aus und legen Sie sie auf Ihren USB-Speicherstick fest.

> Hinweis: Verwenden Sie die UEFI-Option (Unified Extensible Firmware Interface).

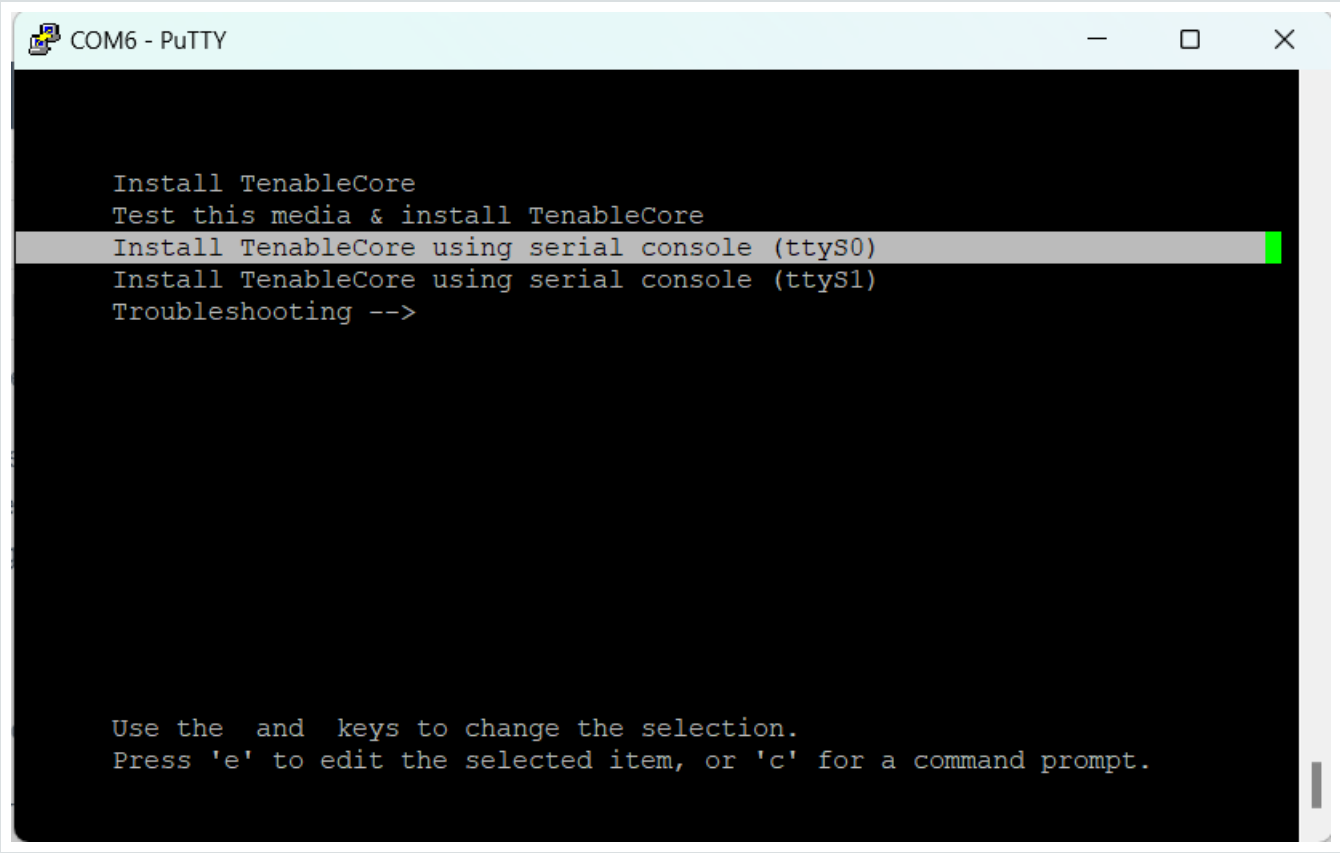



> Hinweis: Sie können „One-Shot-Boot“ auf Appliances verwenden, die die Funktion unterstützen.

8. Wählen Sie im Abschnitt Save & Exit (Speichern und beenden) die Option Save Changes and Reset (Änderungen speichern und zurücksetzen) aus.

9. Wählen Sie nach dem Neustart der Appliance an der Eingabeaufforderung die Option Install TenableCore using serial console (ttyS0) (TenableCore über serielle Konsole (ttyS0) installieren) aus. Dadurch wird sichergestellt, dass die Installationsausgabe in den seriellen Konsolenanschluss der Appliance verschoben wird.

> Hinweis: Wenn Ihre Hardware eine Monitorausgabe (VGA und HDMI) unterstützt, können Sie die Option Install TenableCore (TenableCore installieren) auswählen. In diesem Fall wird die Ausgabe der Installation auf Ihrem angeschlossenen Monitor angezeigt.




Warten Sie, bis die Appliance die Installation abgeschlossen hat. Das System wird möglicherweise mehrmals neu gestartet. Die Installation ist abgeschlossen, wenn eine Login-Eingabeaufforderung angezeigt wird. Auf einigen Appliances wird das System nach Abschluss der Installation möglicherweise standardmäßig heruntergefahren.

> Hinweis: Das System führt möglicherweise einige Installationsvorgänge durch, auch nachdem die Login-Eingabeaufforderung angezeigt wird. Tenable empfiehlt, einige Minuten zu warten, bevor Sie den Setup-Assistenten von Tenable Core starten.

10. Trennen Sie den USB-Speicherstick erst, wenn die Installation abgeschlossen ist.

### Nächste Schritte

OT Security mit dem Netzwerk verbinden

## Virtuelle OT Security ICP-Appliance installieren

Um Tenable Core + OT Security als virtuelle VMware-Maschine bereitzustellen, müssen Sie die OVA-Datei für Tenable Core + OT Security herunterladen und auf einem Hypervisor bereitstellen.

> Hinweis: Wenn Sie die ISO-Datei anstelle der vorkonfigurierten OVA-Datei bereitstellen:
>
> - Befolgen Sie die Systemanforderungen für Tenable Core + OT Security.
> - Wenn Sie aufgefordert werden, eine Setup-Methode auszuwählen, wählen Sie **Tenable Core** installieren aus. Siehe Neuinstallation von Tenable Core + Tenable OT Security.
> - Verfolgen und überwachen Sie den Installationsprozess über die Installationsbenutzeroberfläche auf der Konsole der virtuellen Maschine. Der Installationsprozess läuft vollständig automatisiert ab. Interagieren Sie daher nicht mit dem System, bis die Installation vollständig abgeschlossen ist.

Bevor Sie beginnen:

- Bestätigen Sie, dass Ihre Umgebung die beabsichtigte Verwendung der Instanz unterstützt, wie unter Systemanforderungen beschrieben.
- Vergewissern Sie sich, dass Ihr Internet- und Port-Zugang die von Ihnen beabsichtigte Nutzung der Instanz unterstützt, wie unter Zugriffsanforderungen beschrieben

So stellen Sie Tenable Core + OT Security als virtuelle Maschine bereit:

1. Laden Sie die OVA-Datei für Tenable Core + OT Security von der Tenable Downloads-Seite herunter.
2. Öffnen Sie Ihre virtuelle VMware-Maschine im Hypervisor.
3. Importieren Sie die OVA-Datei für Tenable Core + OT Security VMware von Ihrem Computer auf Ihre virtuelle Maschine.
   Informationen zum Konfigurieren Ihrer virtuellen Maschinen finden Sie in der VMware-Dokumentation.

4. Konfigurieren Sie an der Setup-Eingabeaufforderung die virtuelle Maschine so, dass sie den Speicherbedarf Ihres Unternehmens sowie die unter OT SecuritySystemanforderungen beschriebenen Anforderungen erfüllt.

5. Starten Sie Ihre Tenable Core + OT Security-Instanz.

   Der Startvorgang der virtuellen Maschine wird in einem Terminal-Fenster angezeigt. Der Startvorgang kann mehrere Minuten dauern.

   > Hinweis: Das System führt möglicherweise einige letzte Installationsvorgänge durch, auch nachdem die Login-Eingabeaufforderung angezeigt wird. Tenable empfiehlt, einige Minuten zu warten, bevor Sie den Setup-Assistenten von Tenable Core starten.

   > Tipp: Wenn Sie Ihren Festplattenspeicher vergrößern möchten, um den Datenspeicherbedarf Ihres Unternehmens zu decken, finden Sie weitere Informationen unter Disk Management.

### Nächste Schritte

OT Security mit dem Netzwerk verbinden

## OT Security mit dem Netzwerk verbinden

Sie können OT Security sowohl für die Netzwerküberwachung als auch für aktive Abfragen verwenden. Stellen Sie sicher, dass Sie Ihre Netzwerkinfrastruktur entsprechend vorbereiten. Weitere Informationen finden Sie unter Überlegungen zum Netzwerk.

### Verwaltung und aktive Abfragen

Verbinden Sie die ausgewählte Netzwerkschnittstelle mit einer Netzwerk-Switch-Schnittstelle, die so konfiguriert ist, dass bei Bedarf Verwaltungskonnektivität zur ICP hergestellt werden kann.

Konfigurieren Sie eine IP-Adresse und andere Konnektivitätseinstellungen in der ausgewählten OT Security-Appliance-Schnittstelle über Tenable Core.

Wenn Sie die Rollen für Verwaltung und aktive Abfragen trennen möchten, stellen Sie sicher, dass jede ausgewählte Schnittstelle mit der entsprechenden Switch-Schnittstelle verbunden ist. Weisen Sie jeweils eine IP-Adresse zu und konfigurieren Sie die Switch-Schnittstellen nach Bedarf, damit beide Funktionalitäten über das Netzwerk erreichbar sind.

Weitere Informationen finden Sie unter Trennung der Rollen für Verwaltung und aktive Abfragen (Split-Port).

### Netzwerk-Monitoring

Verbinden Sie eine oder mehrere der für passives Netzwerk-Monitoring ausgewählten Schnittstellen des Geräts mit einer konfigurierten Port-Spiegelungs-Zielschnittstelle (SPAN/RSPAN) auf einem Netzwerk-Switch. Sie müssen Port-Spiegelung konfigurieren, um eine ordnungsgemäße Sichtbarkeit der Protokolle und der Kommunikation des OT-Netzwerks zu gewährleisten.

> Hinweis: Mithilfe von OT-Sensoren oder ERSPAN können Sie Traffic erfassen, der nicht direkt von den Appliance-Schnittstellen überwacht werden kann.

### So verbinden Sie die OT Security Appliance mit dem Netzwerk:

#### Auf einer Hardware-Appliance:

Die von Tenable bereitgestellten Hardware-Appliances können eine unterschiedliche Anzahl und Art (RJ45 oder SFP) von Netzwerkschnittstellen aufweisen. Bei OT Security sind die für jede Rolle ausgewählten Standardschnittstellen vorinstalliert. Sie können diese Konfiguration zu einem späteren Zeitpunkt nach Bedarf ändern.

Auf nicht von Tenable bereitgestellter Hardware müssen Sie Schnittstellen für jede Rolle auswählen, bevor Sie den OT Security-Installationsprozess manuell initiieren. Achten Sie darauf, dass Sie die verfügbaren Schnittstellen für die einzelnen Rollen korrekt verwenden.

#### Auf einer virtuellen Appliance:

Wenn Sie die Appliance mithilfe der `.ova`-Datei bereitgestellt haben, wird die Appliance mit vier Netzwerkschnittstellen vorkonfiguriert geliefert. Sie können während der Bereitstellung oder zu einem späteren Zeitpunkt weitere Netzwerkadapter/-schnittstellen hinzufügen.

Wenn Sie eine benutzerdefinierte virtuelle Appliance mit der `.iso`- oder `.zip`-Datei (Hyper-V) bereitgestellt haben, konfigurieren Sie die erforderliche Anzahl von Netzwerkschnittstellen.

Achten Sie darauf, die virtuelle Maschine gemäß den in den Systemanforderungen beschriebenen Anforderungen zu konfigurieren. Weitere Informationen zum Konfigurieren des Netzwerks auf virtuellen Maschinen finden Sie in der VMware-Dokumentation oder der Hyper-V-Dokumentation.

## OT Security ICP konfigurieren

> Ziel: Vorbereitung der Software auf die Aktivierung.

Nachdem Sie OT Security ICP installiert haben, können Sie OT Security konfigurieren. Die Konfiguration umfasst die folgenden Schritte:

1. Tenable Core einrichten – Führen Sie die Ersteinrichtung für Tenable Core über die CLI oder die Benutzeroberfläche durch.
2. OT Security unter Tenable Core installieren – Installieren Sie OT Security unter Tenable Core.
3. Einstellungen von OT Security mit dem Setup-Assistenten konfigurieren – Konfigurieren Sie die grundlegenden Einstellungen Ihrer OT Security ICP mit dem Setup-Assistenten.

### Tenable Core einrichten

Sie können die Erstkonfiguration von Tenable Core sowohl über die CLI als auch über die Tenable Core-Benutzeroberfläche durchführen.

Die Verwendung der Tenable Core-Benutzeroberfläche ist obligatorisch, um die Konfiguration für die Bereitstellung virtueller Appliances abzuschließen.

Hinweis: Wenn Sie den Setup-Assistenten nicht innerhalb von etwa 30 Minuten abschließen, starten Sie die Appliance neu.

### Erstkonfiguration über die Tenable Core-Benutzeroberfläche

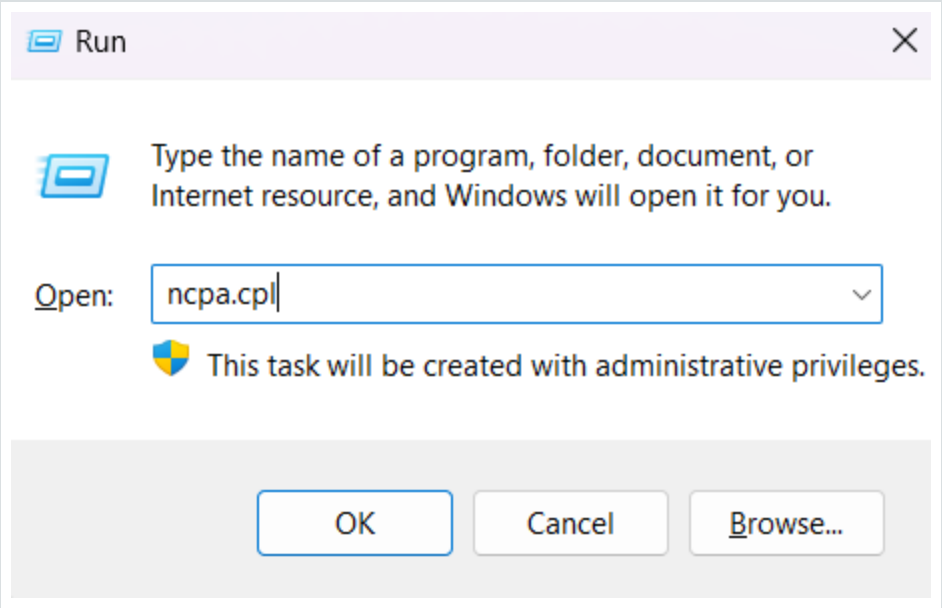
Um die Erstkonfiguration über die Tenable Core-Benutzeroberfläche (verfügbar unter https://<mgmt-IP>:8000) durchzuführen, benötigen Sie eine funktionierende Netzwerkverbindung zur Appliance.

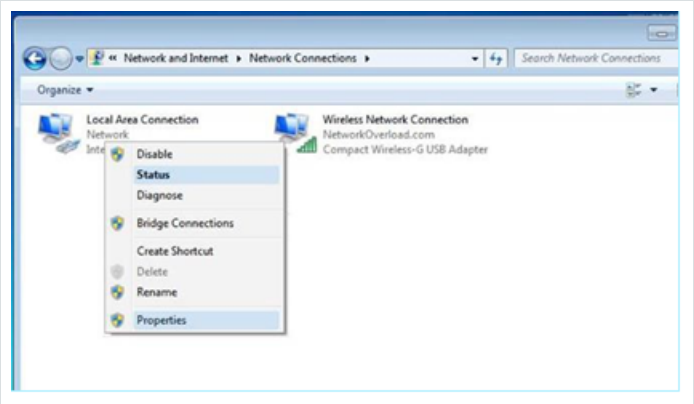
Wenn Sie die Verwaltungs-IP-Adresse nicht konfiguriert haben, können Sie entweder einen direkt verbundenen PC oder ein entsprechend konfiguriertes Netzwerk verwenden, um die Tenable Core-Benutzeroberfläche über eine der folgenden Schnittstellen zu erreichen:

- Systemport 1 – Standard-Verwaltungsschnittstelle, vorkonfiguriert mit IP-Adresse 192.168.1.5/24
- Systemport 4 – Engineering-Schnittstelle, vorkonfiguriert mit IP-Adresse 192.168.3.3/24
  Sofern keine Änderung erfolgt, kann diese Verbindung für Wiederherstellungsverfahren verwendet werden.

### So stellen Sie direkt über Ihren PC oder Laptop eine Verbindung zu Tenable Core her:

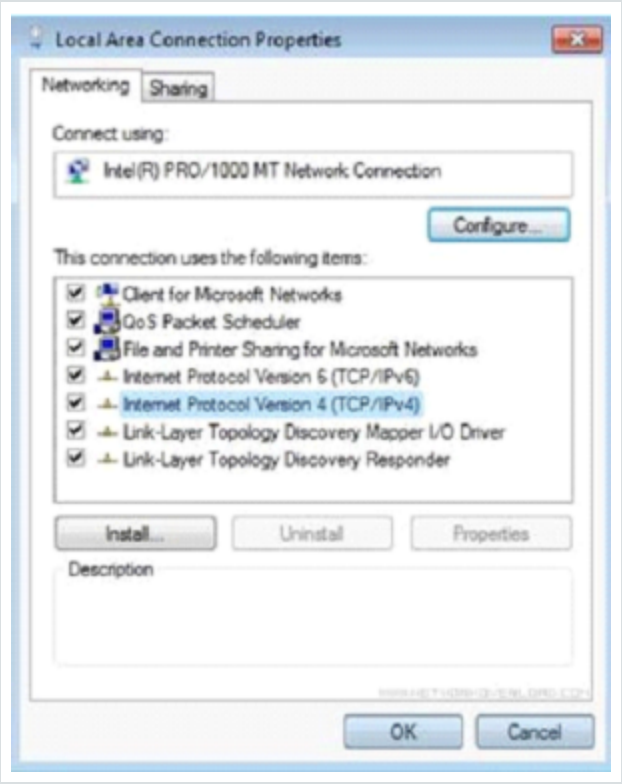
1. Schließen Sie ein Ethernet-Kabel zwischen Ihrem PC und einem der vorkonfigurierten Ports der OT Security Appliance an.
2. Verwenden Sie unter Windows win+R, um Ausführen zu öffnen, und geben Sie `ncpa.cpl` ein, um Netzwerkverbindungen zu öffnen.




3. Klicken Sie mit der rechten Maustaste auf Ihre Netzwerkverbindung (namens LAN-Verbindung) und wählen Sie Eigenschaften aus.

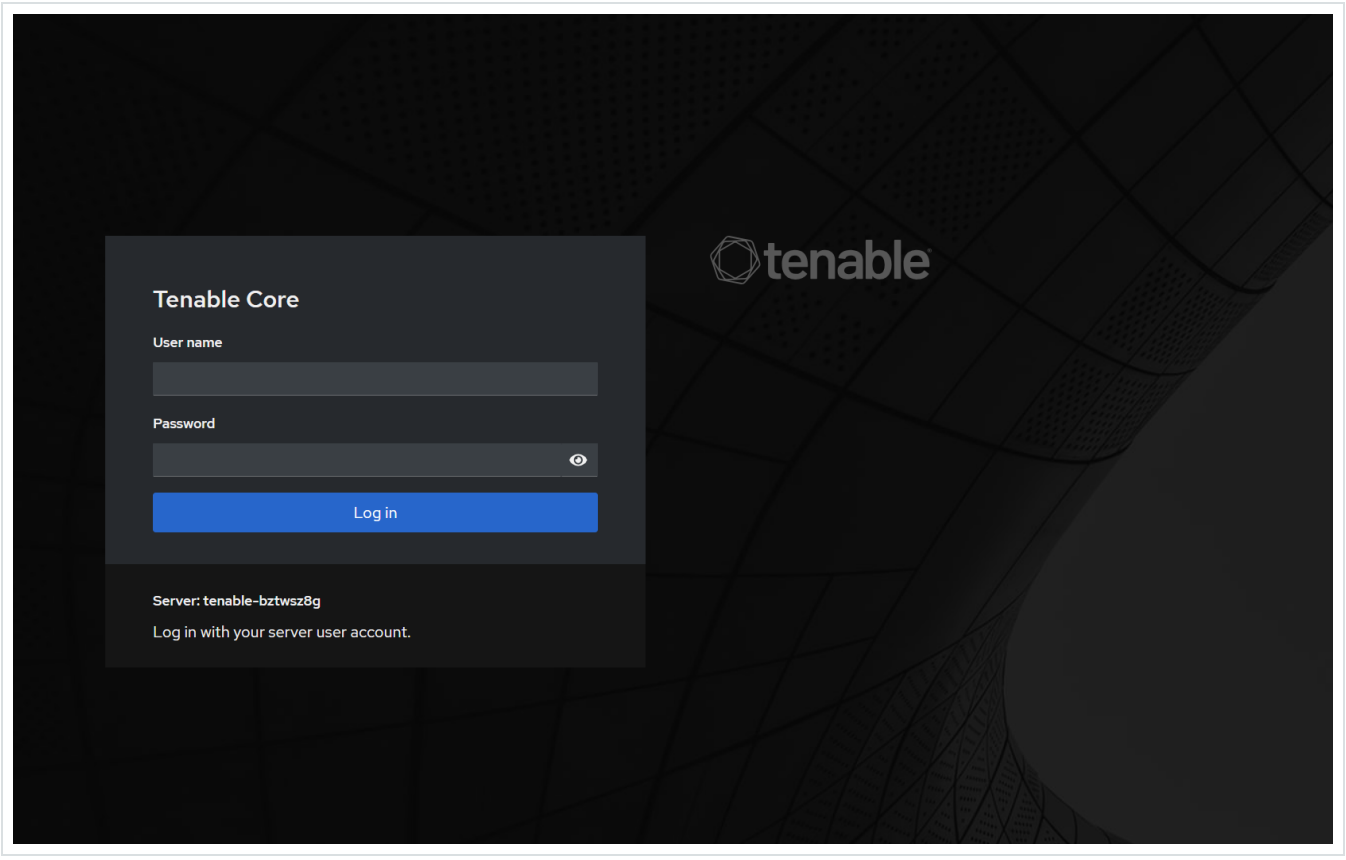
   Das Fenster Eigenschaften für LAN-Verbindung wird angezeigt.




4. Wählen Sie Internetprotokoll, Version 4 (TCP/IPv4) und klicken Sie auf Eigenschaften.

   Das Fenster mit den Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4) wird angezeigt.


5. Wählen Sie Folgende IP-Adresse verwenden aus.
6. Geben Sie im Feld IP-Adresse eine entsprechende IP-Adresse für die Schnittstelle ein, zu der Sie eine Verbindung herstellen. Zum Beispiel 192.168.1.10 als Standardadresse von Systemport 1 oder 192.1683.10 als Standardadresse von Systemport 4.
7. Geben Sie in das Feld Subnetzmaske 255.255.255.0 ein.
8. Klicken Sie auf OK.
9. Navigieren Sie im Chrome-Browser zu https://<mgmt-ip>:8000.




10. Wenn Sie das Administratorbenutzerkonto noch nicht konfiguriert haben, werden Sie vom System aufgefordert, dies jetzt zu tun und sich dann mit Ihrem neu erstellten Benutzer erneut einzuloggen. Weitere Informationen finden Sie unter Create an Initial Administrator User Account.

    Nach Erstellung des Administratorkontos empfiehlt Tenable, die Verwaltungs-IP-Adresse zu konfigurieren. Wenn Sie die Split-Port-Konfiguration verwenden möchten, stellen Sie sicher, dass die Schnittstellen die entsprechenden Netzwerke erreichen können. Weitere Informationen finden Sie unter Überlegungen zum Netzwerk.

    > Hinweis: Um die Verwaltungs-IP-Adresse zu konfigurieren oder zu ändern, loggen Sie sich bei Tenable Core ein, aktivieren Sie den Administratorzugriff und bearbeiten Sie die Netzwerkkonfiguration.

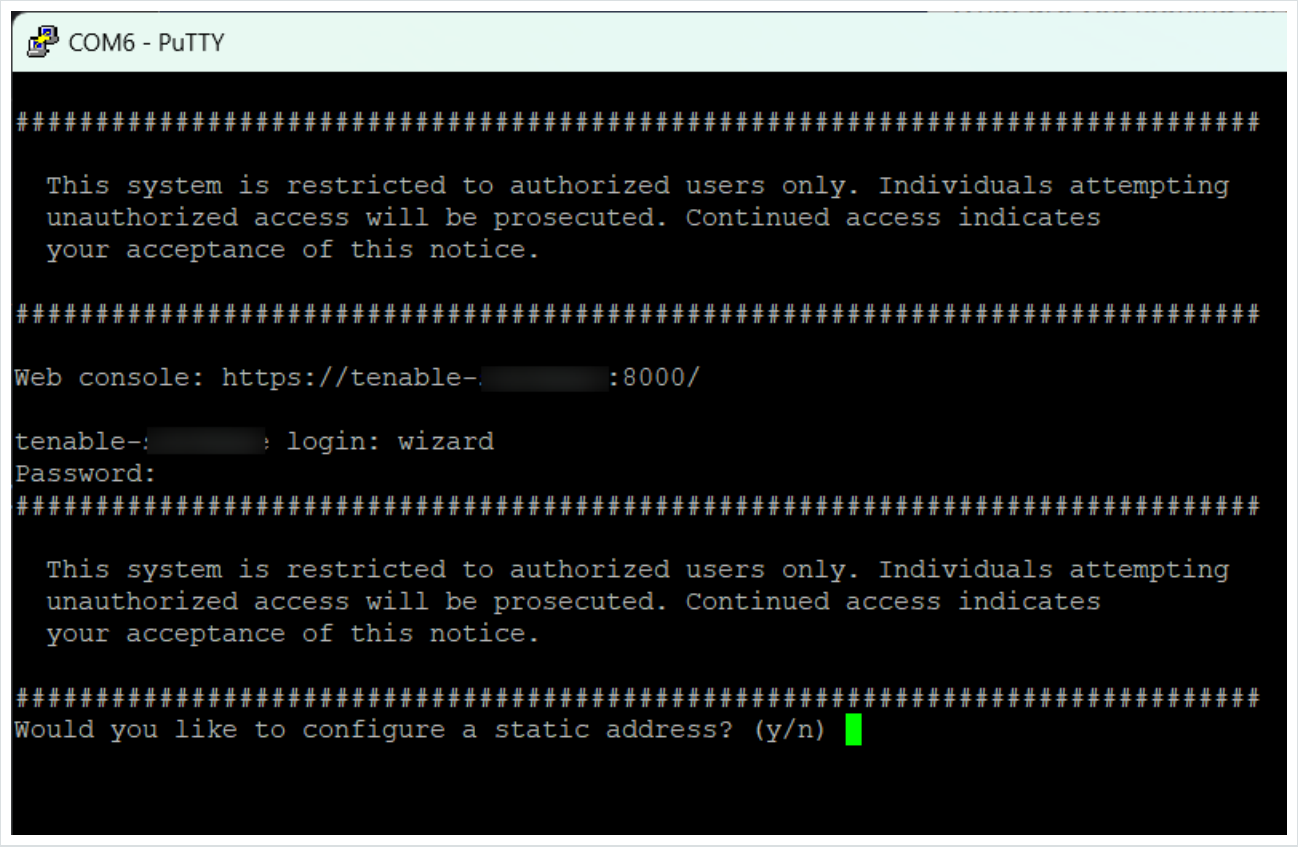
## Erstkonfiguration über die CLI (optional)

So konfigurieren Sie Tenable Core über die CLI:

1. Stellen Sie über die serielle Konsole eine Verbindung zur OT Security Appliance her, wie unter Neuinstallation von Tenable Core + OT Security beschrieben.

2. Loggen Sie sich mit dem Benutzernamen `wizard` und dem Passwort `admin` ein.

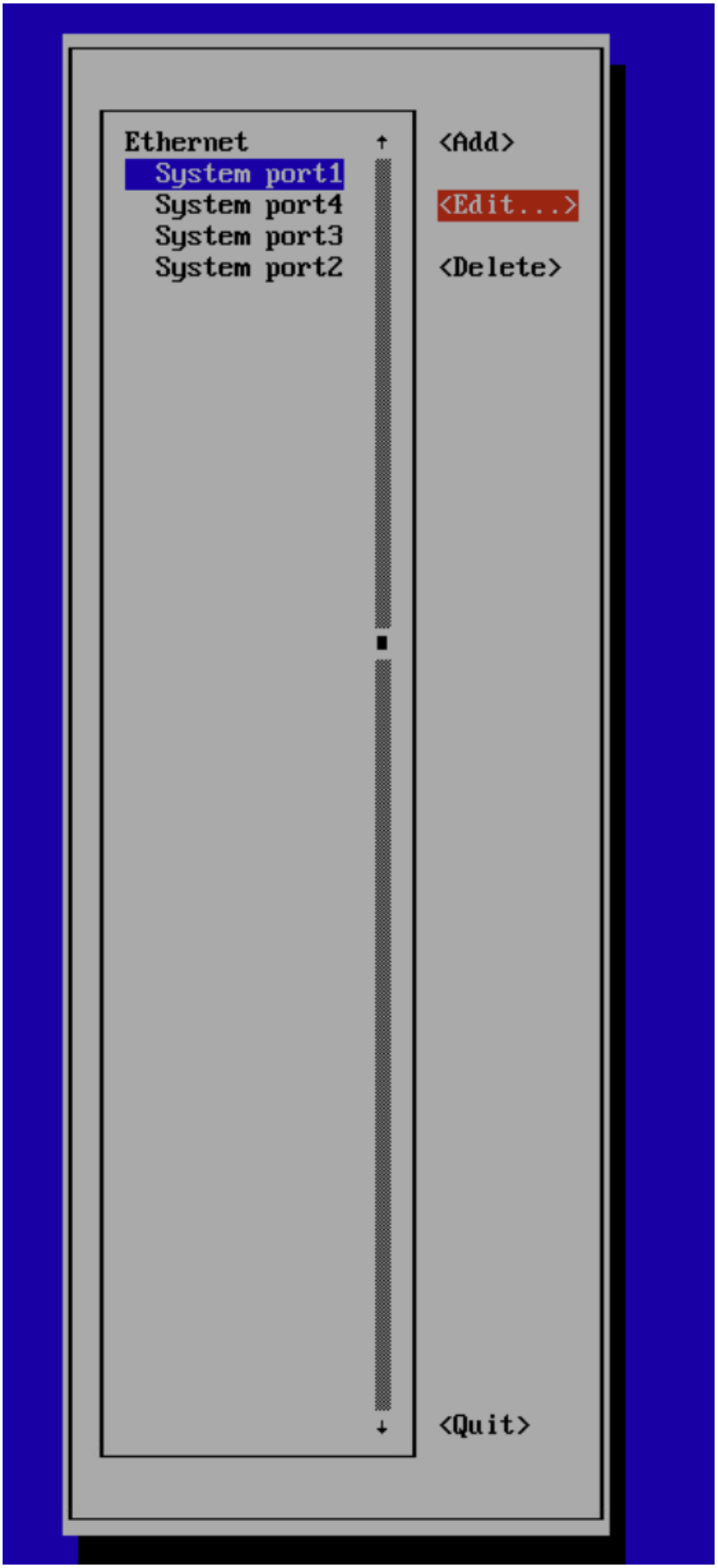
   Die Terminaloberfläche Network Manager (Netzwerk-Manager) wird angezeigt.




3. (Optional) Geben Sie **y** ein, um die Verwaltungs-IP-Adresse zu konfigurieren.

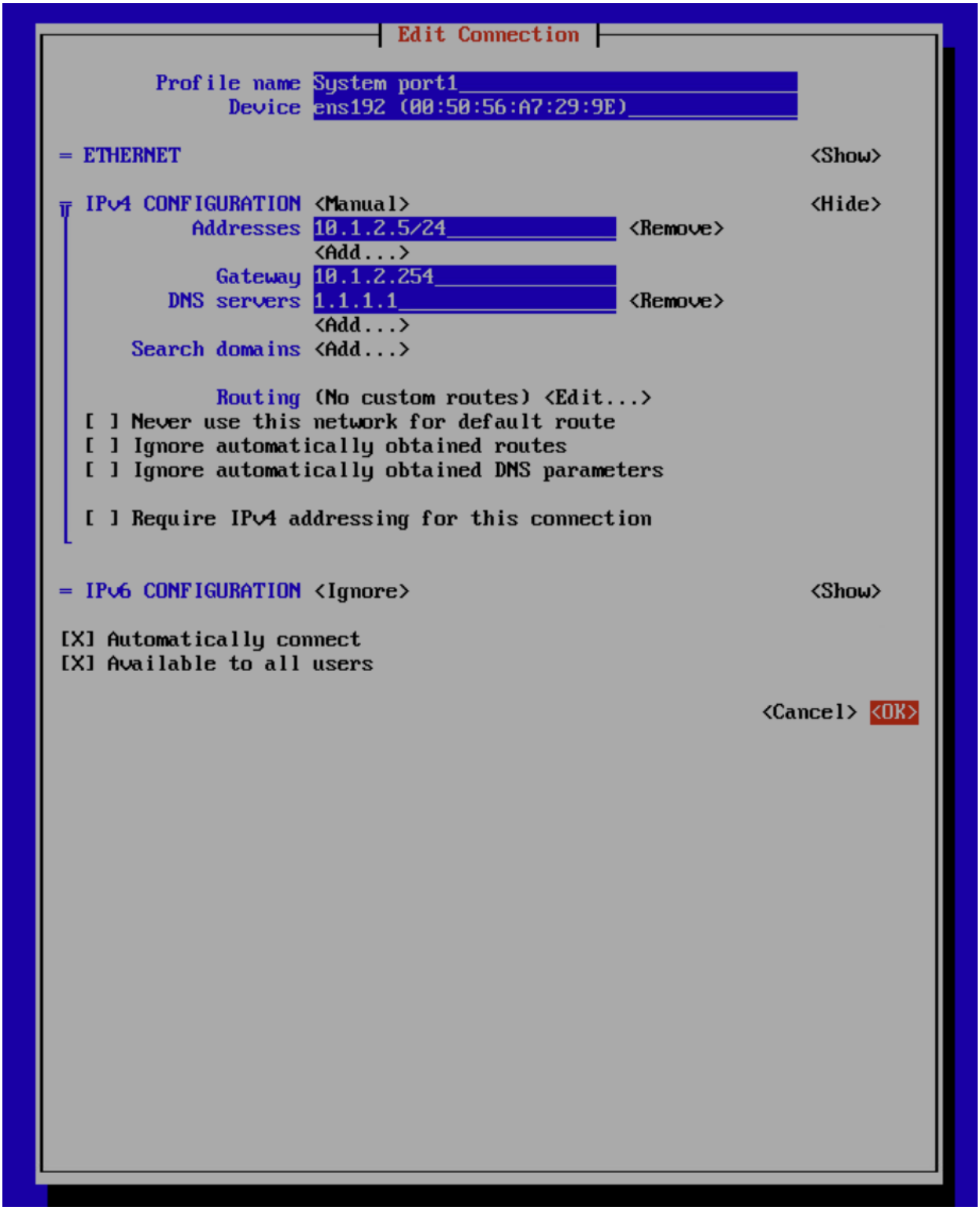
> Hinweis: Wenn Sie diesen Schritt überspringen möchten, können Sie jederzeit mit dem Befehl `sudo nmtui` auf diese Option zugreifen.

a. Wählen Sie System Port 1 (oder System Port 3, wenn Sie die Split-Port-Konfiguration verwenden).


Ethernet
System port1
System port4
System port3
System port2
<Add>
<Edit...>
<Delete>
<Quit>

b. Drücken Sie die Eingabetaste.

   Das Fenster Edit Connection (Verbindung bearbeiten) wird angezeigt.


Edit Connection
Profile name System port1
Device ens192 (00:50:56:A7:29:9E)
= ETHERNET <Show>
IPv4 CONFIGURATION <Manual> <Hide>
Addresses 10.1.2.5/24 <Remove>
<Add...>
Gateway 10.1.2.254
DNS servers 1.1.1.1 <Remove>
<Add...>
Search domains <Add...>
Routing (No custom routes) <Edit...>
[ ] Never use this network for default route
[ ] Ignore automatically obtained routes
[ ] Ignore automatically obtained DNS parameters
[ ] Require IPv4 addressing for this connection
= IPv6 CONFIGURATION <Ignore> <Show>
[X] Automatically connect
[X] Available to all users
<Cancel> <OK>

c. Ändern Sie im Feld IPV4 Configuration (IPV4-Konfiguration) die Option von <Automatic> (Automatisch) zu <Manual> (Manuell).

> Hinweis:
>
> - Auf virtuellen Maschinen und nicht von Tenable bereitgestellter Hardware ist Port 1 auf Automatic IPv4 configuration (Automatische IPv4-Konfiguration) (DHCP) voreingestellt.
> - Auf von Tenable bereitgestellten Appliances ist Port 1 auf „192.168.1.5/24“ voreingestellt. Sie können diesen Port verwenden, um die Appliance einzurichten und sie für die Erstkonfiguration direkt zu verbinden. Später können sie ihn über die Registerkarte Network (Netzwerk) in der Tenable Core-Benutzeroberfläche oder mit dem Befehl `sudo nmtui` über die CLI ändern.

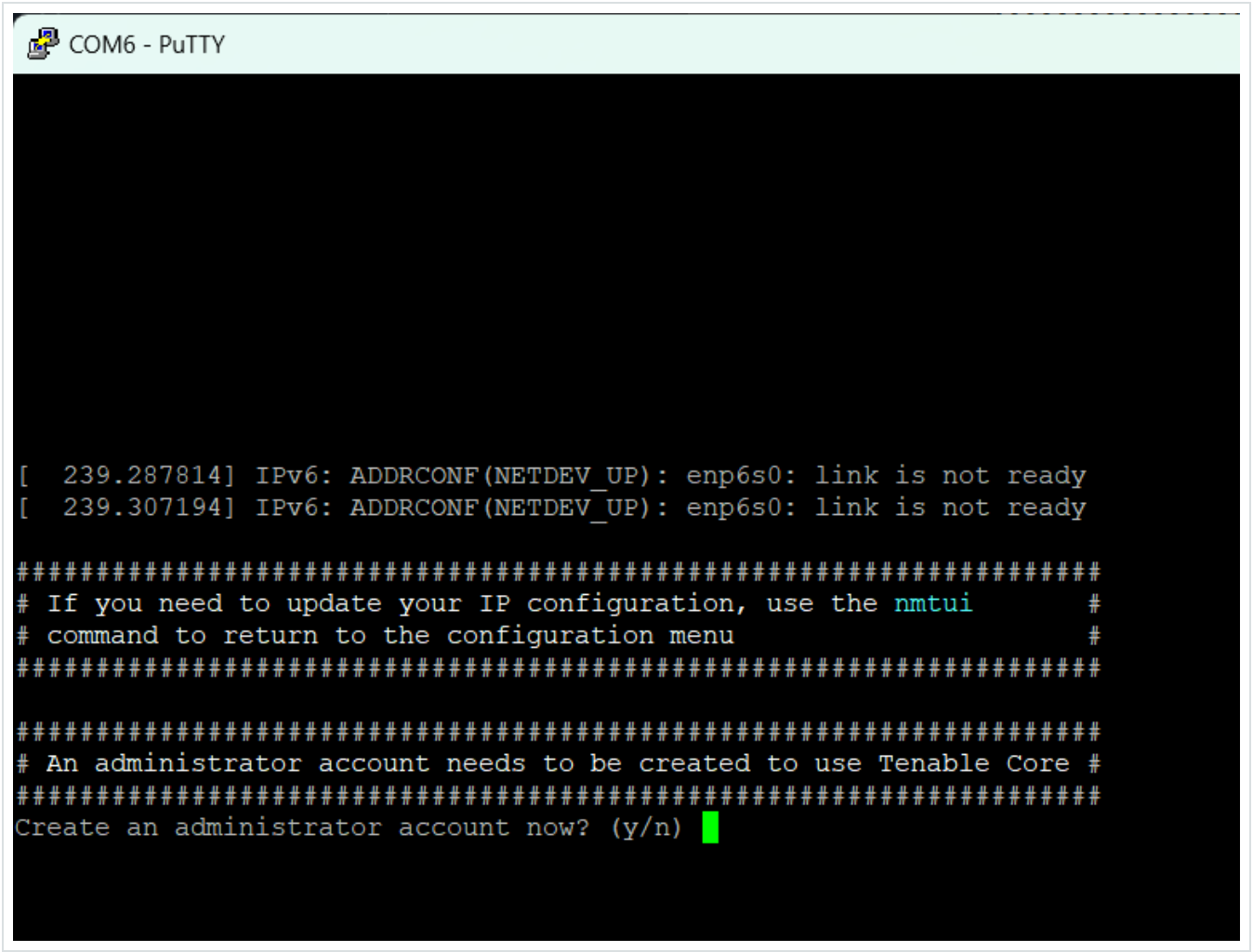
d. Navigieren Sie mit den Pfeiltasten und konfigurieren Sie die erforderliche IP-Adresse, das Standard-Gateway, die DNS-Server usw. Sie können diese Konfiguration später ändern.

e. Navigieren Sie mit dem Abwärtspfeil zum unteren Bildschirmrand und wählen Sie <OK> aus.

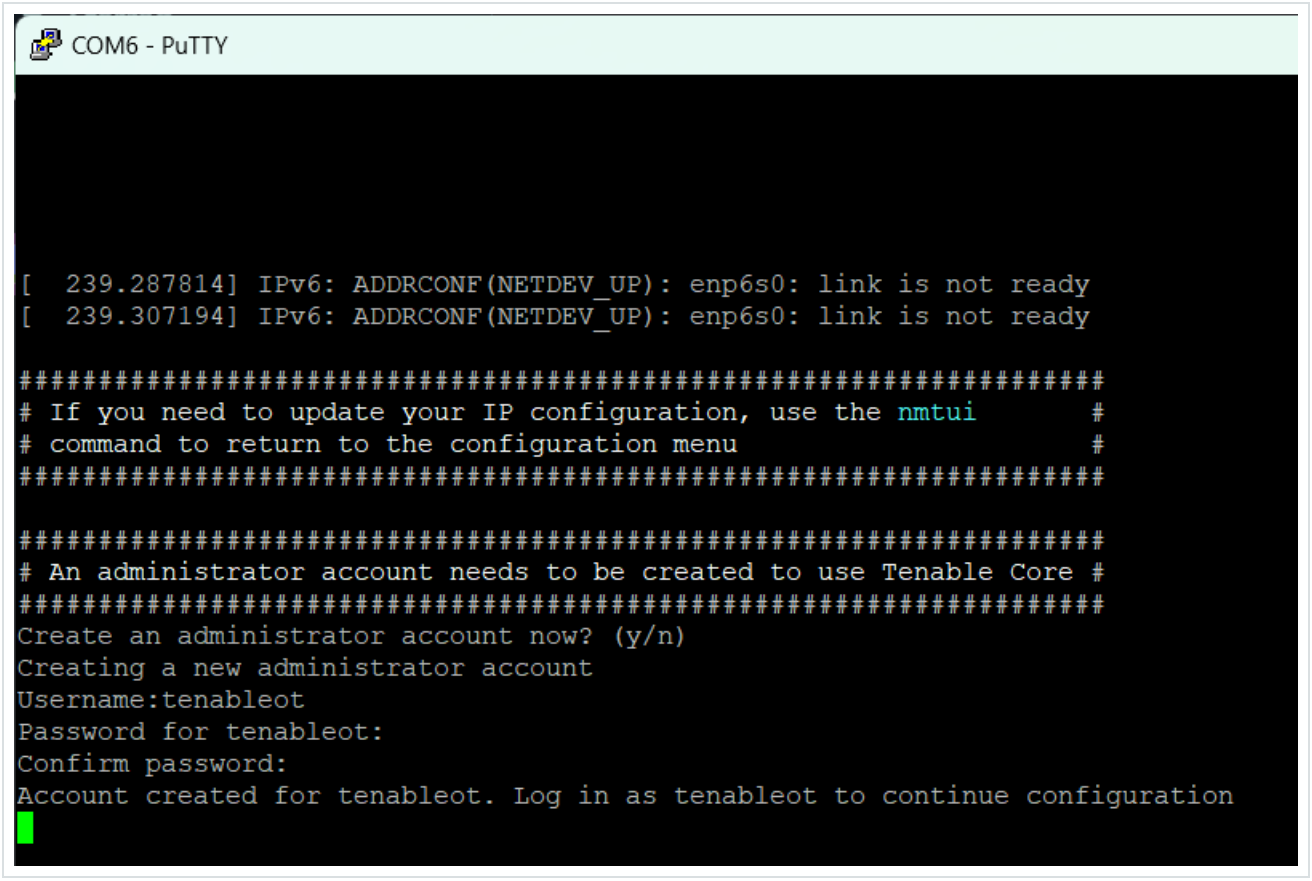
   Das Fenster Network Manager (Netzwerk-Manager) wird angezeigt.

4. Wählen Sie <Quit> (Beenden).

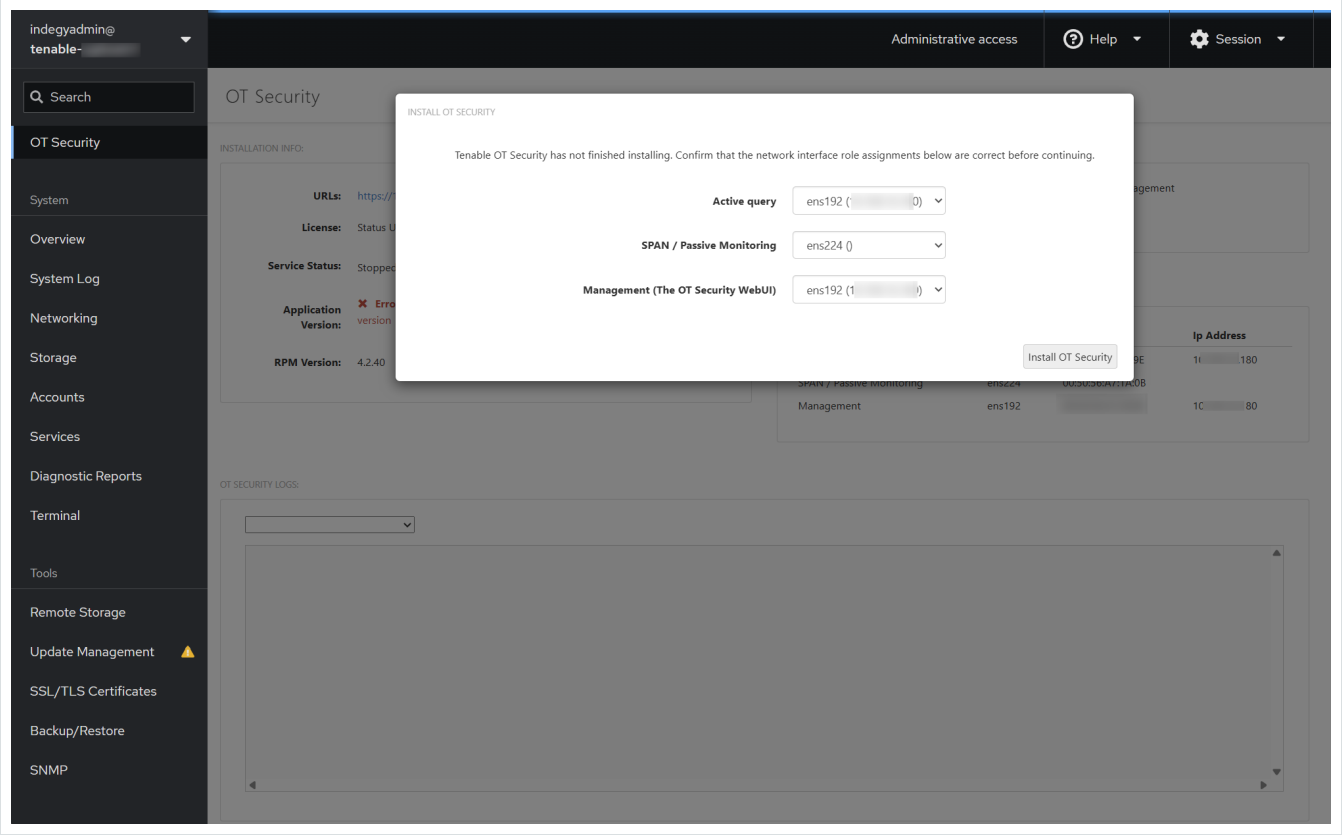
   Das Terminalfenster Network Manager (Netzwerk-Manager) wird mit der Aufforderung, ein Administratorkonto zu erstellen, angezeigt.




5. Geben Sie **y** ein und befolgen Sie die Anweisungen, um ein Administratorkonto zu erstellen. Verwenden Sie dieses Konto nur, um sich bei Tenable Core einzuloggen (Terminalkonsole, SSH und Tenable Core-Benutzeroberfläche). Verwenden Sie separate Konten für die OT Security-Anwendung.




6. Nachdem Sie das Konto erstellt haben, greifen Sie über die Konsole oder über eine Netzwerkverbindung auf den Terminal zu (über SSH oder die Tenable Core-Schnittstelle (https://<mgmt-IP>:8000)).




Auf virtuellen Maschinen und Hardware, die nicht von Tenable stammt, wird auf der Seite Tenable Core > **OT Security** eine Eingabeaufforderung zur Installation von OT Security angezeigt.

### Nächste Schritte

OT Security unter Tenable Core installieren

## OT Security unter Tenable Core installieren

Von Tenable bereitgestellte Hardware-Appliances werden mit der vorinstallierten OT Security-Anwendung geliefert. Bei der Bereitstellung von OT Security auf benutzerdefinierter Hardware oder virtuell muss der Installationsprozess manuell initiiert werden.

> Hinweis: Bevor Sie die Installation der OT Security-Anwendung initiieren, weisen Sie Rollen für jede Schnittstelle zu. Konfigurieren Sie die Schnittstellen in Tenable Core und achten Sie darauf, dass die Netzwerkinfrastruktur so vorbereitet ist, dass eine ordnungsgemäße Konnektivität möglich ist.

Weitere Informationen finden Sie unter Überlegungen zum Netzwerk und OT Security mit dem Netzwerk verbinden.

## Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie über Administratorzugriff verfügen.
- Stellen Sie sicher, dass Sie über SSH- oder Cockpit-Zugriff auf virtuellen und physischen Appliances von Tenable Core verfügen.

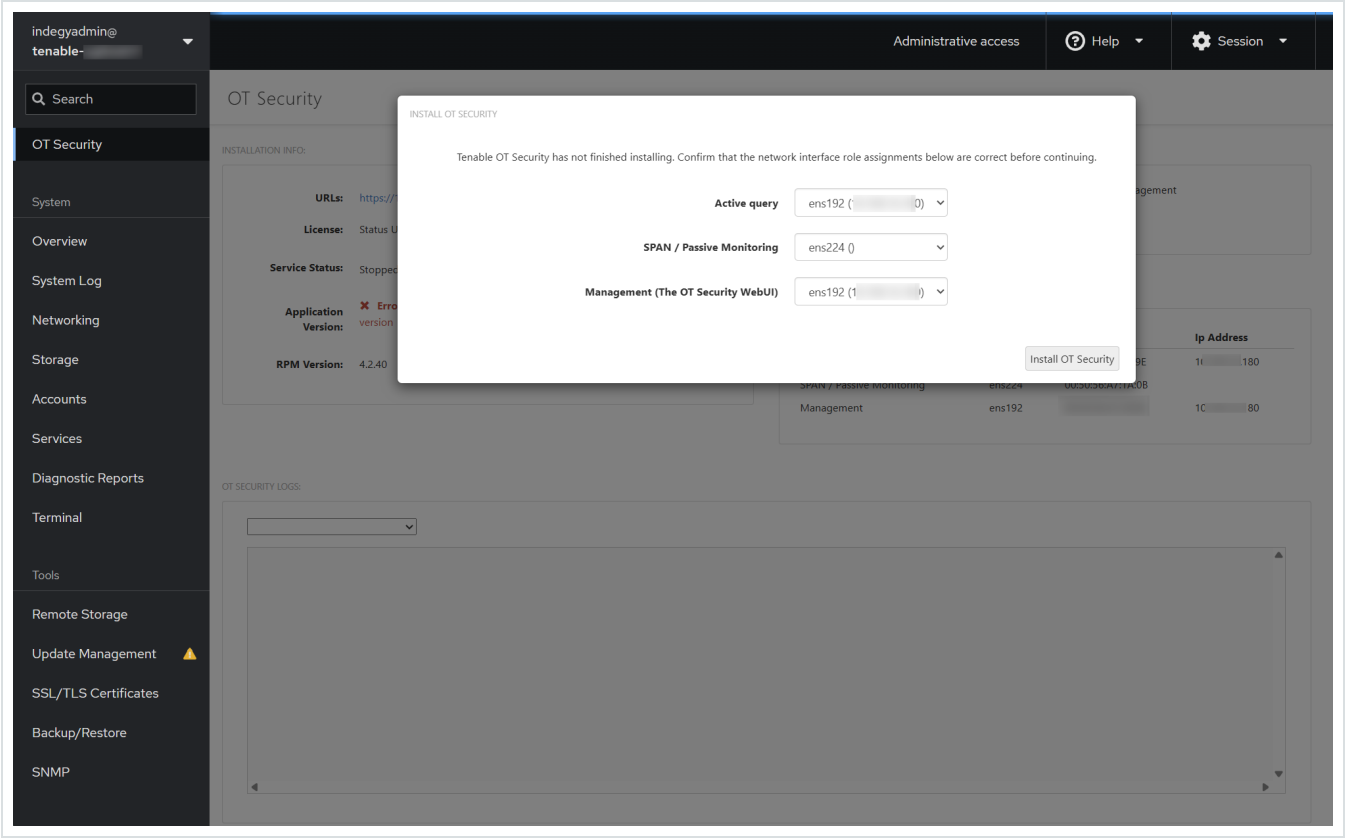
  Hinweis: Administrator-Konten können unzugänglich werden, wenn Sie sich nicht regelmäßig einloggen und Ihr Passwort aktualisieren. Wenn ein Administratorkonto gesperrt wird, weil das zugehörige Passwort abgelaufen ist, können Sie das Konto mit dem Dienstprogramm zum Remote-Entsperren entsperren. Mit diesem Dienstprogramm kann eine ICP ihre Sensoren und ein OT Security Enterprise Manager (EM) seine ICPs remote entsperren, falls das Konto gesperrt wird. Weitere Informationen zur Verwendung des Dienstprogramms finden Sie im Artikel Leveraging the Remote Unlock Feature in Tenable Core in der Wissensdatenbank.

## So installieren Sie OT Security unter Tenable Core:

1. Loggen Sie sich von Ihrem Chrome-Browser aus bei Tenable Core ein: `https://<mgmt-ip>:8000`.
2. Navigieren Sie zu **OT Security**.

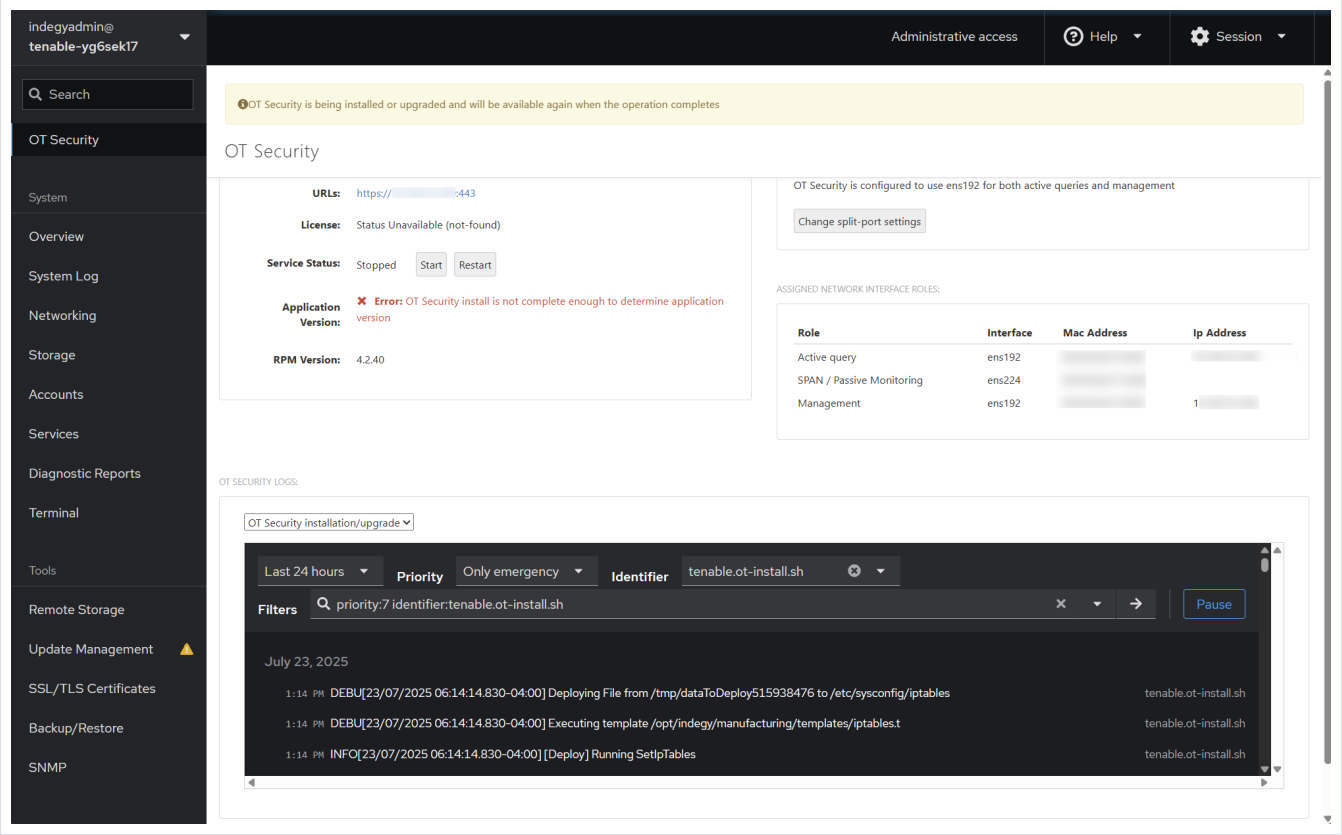
   Die Seite OT Security wird angezeigt.

   Hinweis: Bei virtuellen Maschinen und Hardware, die nicht von Tenable stammt, werden Sie aufgefordert, OT Security zu installieren.

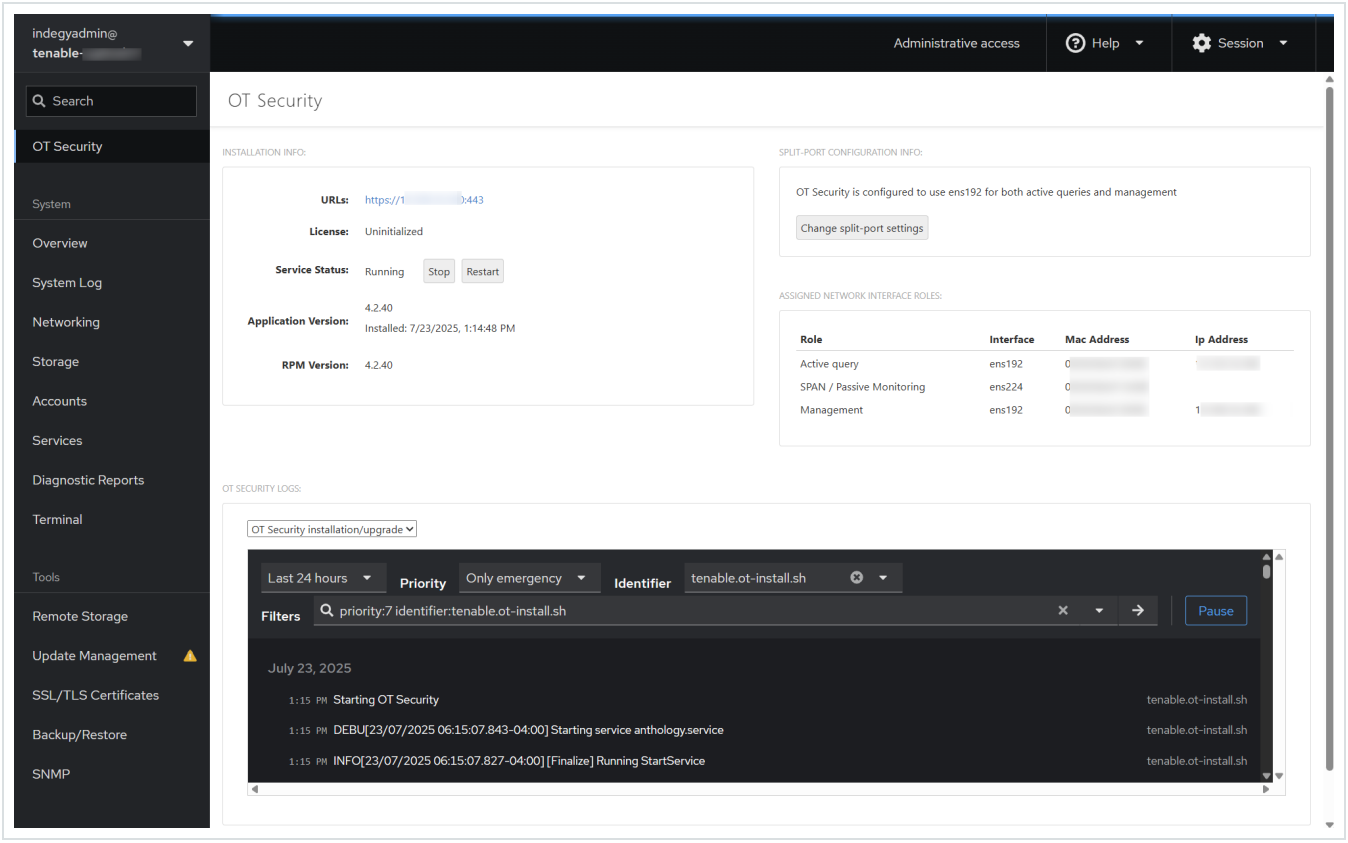



3. Klicken Sie auf Install **Tenable OT Security** (Tenable OT installieren).

   Tenable Core initiiert die Installation und zeigt ein gelbes Banner mit der folgenden Meldung an: `OT Security is being installed or upgraded and will be available again when the operation completes` (Tenable OT wird installiert oder aktualisiert und ist wieder verfügbar, wenn der Vorgang abgeschlossen ist).

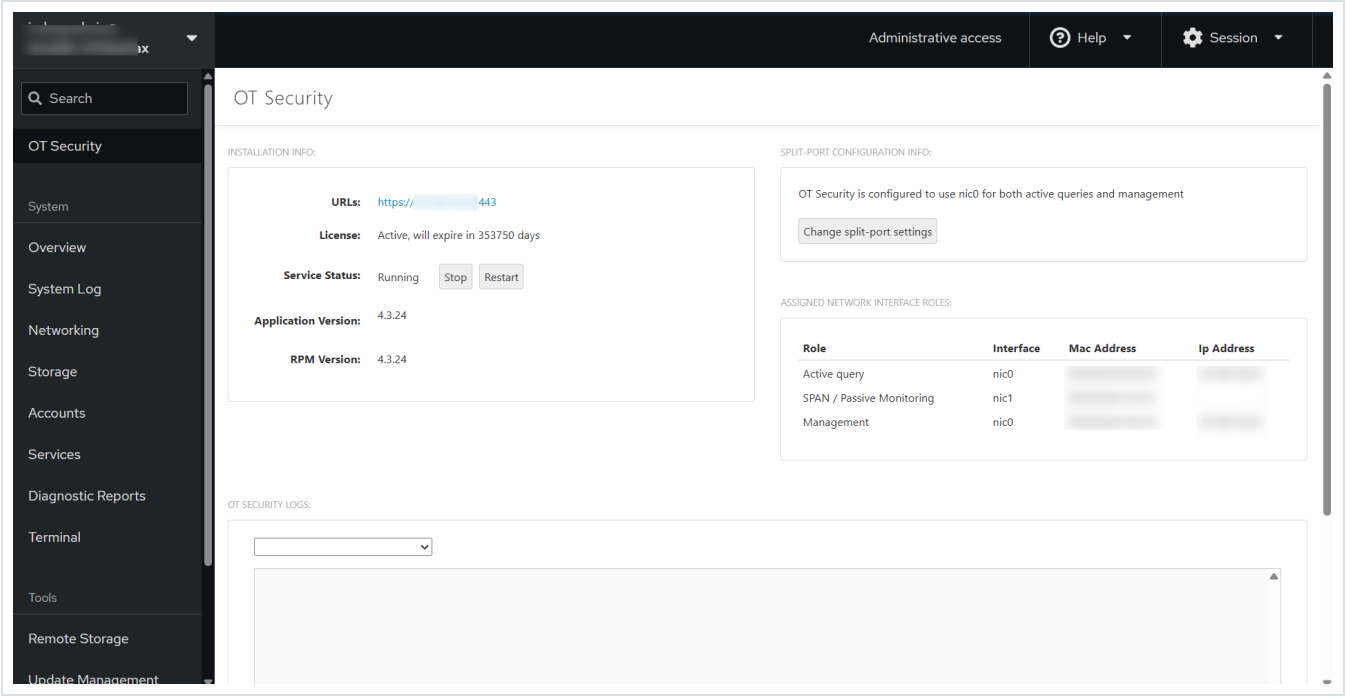



Wenn die Installation abgeschlossen ist, wird das gelbe Banner ausgeblendet und der Status der Lizenz ändert sich von Unavailable (Nicht verfügbar) in Uninitialized (Nicht initialisiert).



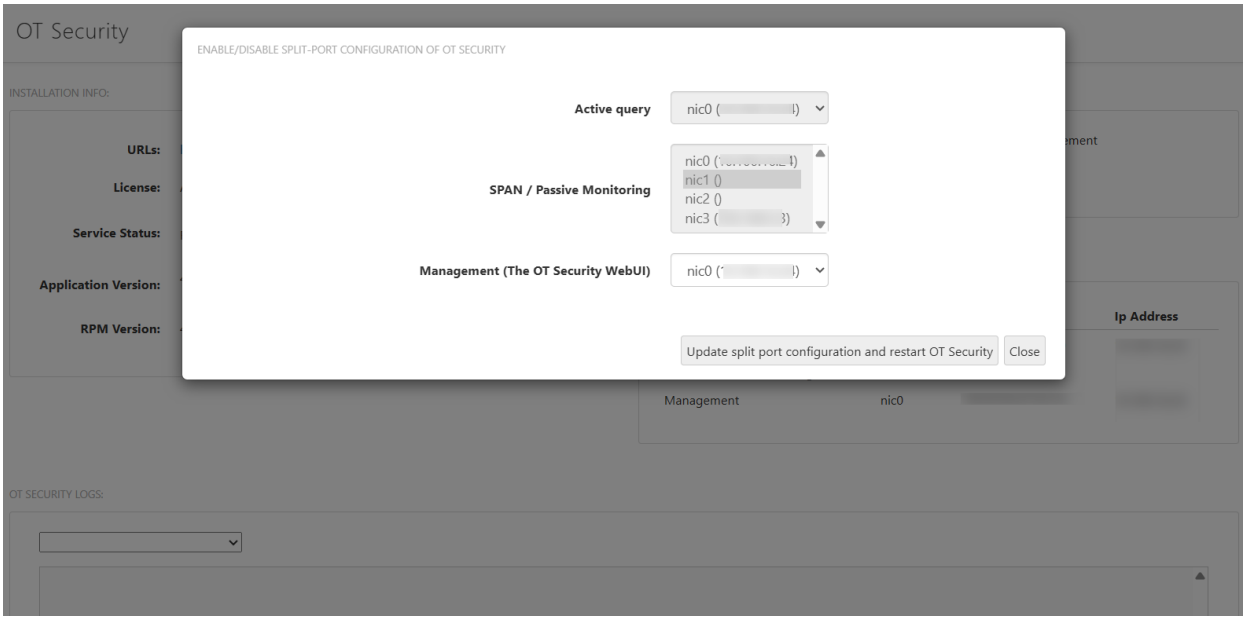

4. (Optional) Wählen Sie die Schnittstellenrollen aus.

> Hinweis: Sie können wählen, die Standardkonfiguration beizubehalten. Die Standardschnittstellenkonfiguration umfasst Port 1: Verwaltung + aktive Abfrage und Port 2: Passives Monitoring.

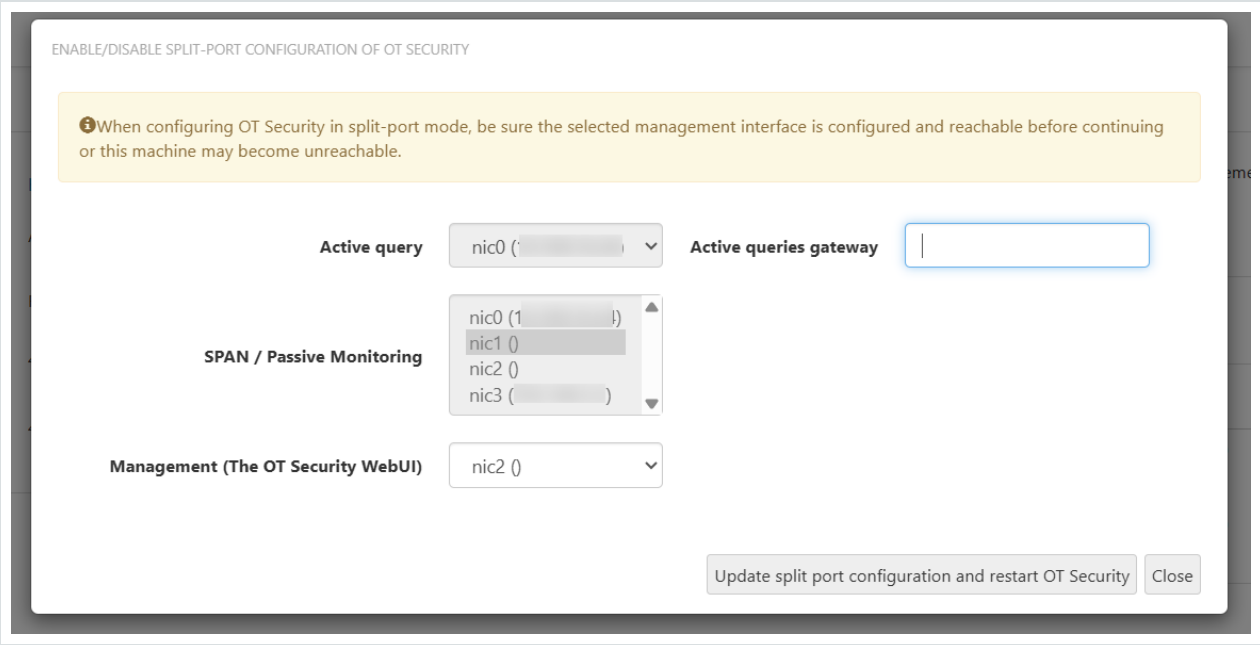



a. Klicken Sie im Abschnitt Split Port Configuration Info (Informationen zur Split-Port-Konfiguration) auf Change split-port settings (Split-Port-Einstellungen ändern).

   Das Fenster Enable/Disable Split Configuration of **OT Security** (Split-Konfiguration von Tenable OT aktivieren/deaktivieren) wird angezeigt.



b. Verschieben Sie im Feld Management (The **OT Security** Web UI) (Verwaltung (die OT Security-Web-Benutzeroberfläche)) den Verwaltungsport zu einer anderen Schnittstelle, z. B. Port 3.



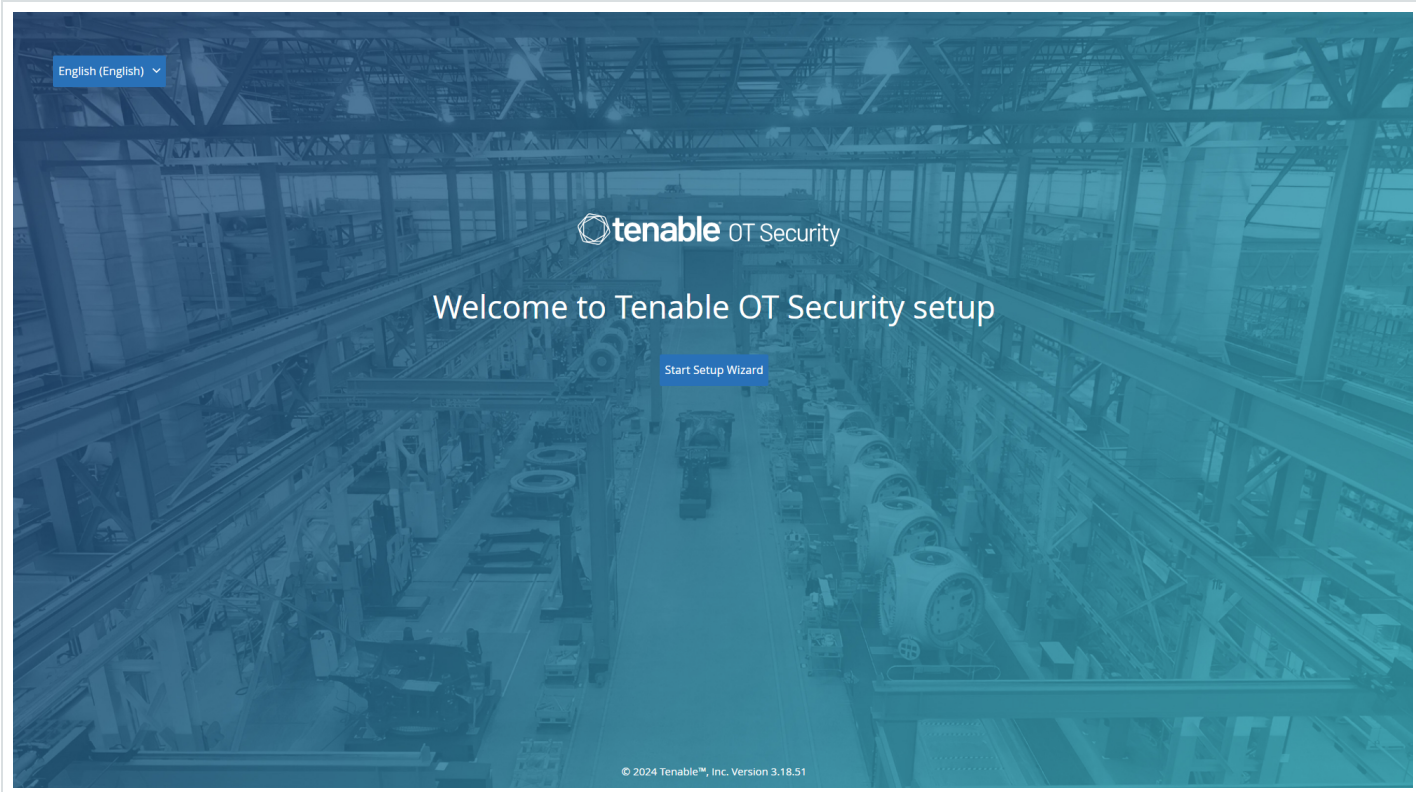

c. (Optional) Geben Sie im Feld Active queries gateway (Gateway für aktive Abfragen) die IP-Adresse des Gateways an.

d. Klicken Sie auf Update split-port configuration and restart OT Security (Split-Port-Konfiguration aktualisieren und OT Security neu starten).

Tenable Core initiiert je nach Bedarf einen Neustart oder die Installation.

> Achtung: Zu diesem Zeitpunkt dürfen Sie keine anderen Updates installieren oder neu starten. Der Installationsprozess kann einige Zeit dauern. Unterbrechen Sie den Installationsprozess nicht.

Wenn die Installation abgeschlossen ist, können Sie auf den Link im Feld URLs klicken, um sich bei der OT Security-Benutzeroberfläche einzuloggen.




### Nächste Schritte

Einstellungen von OT Security mit dem Setup-Assistenten konfigurieren

## Einstellungen von OT Security mit dem Setup-Assistenten konfigurieren

Der Setup-Assistent von OT Security führt Sie durch die Konfiguration der grundlegenden Systemeinstellungen.

> Hinweis: Sie können die Konfiguration bei Bedarf im Bildschirm Einstellungen in der Verwaltungskonsole (Benutzeroberfläche) ändern.

Um auf den Setup-Assistenten zuzugreifen, müssen Sie sich zuerst bei der OT Security Verwaltungskonsole einloggen. Informationen zum Einloggen bei der Verwaltungskonsole finden Sie unter Bei der OT Security-Verwaltungskonsole einloggen.

Konfigurieren Sie mit dem Setup-Assistenten Folgendes:

1. Benutzerinformationen
2. Gerät
3. Verbinden und Trennung der Ports für Verwaltung und aktive Abfragen konfigurieren

> Hinweis: Nachdem Sie den Setup-Assistenten abgeschlossen haben, werden Sie von OT Security aufgefordert, das System neu zu starten.

## Bei der OT Security-Verwaltungskonsole einloggen

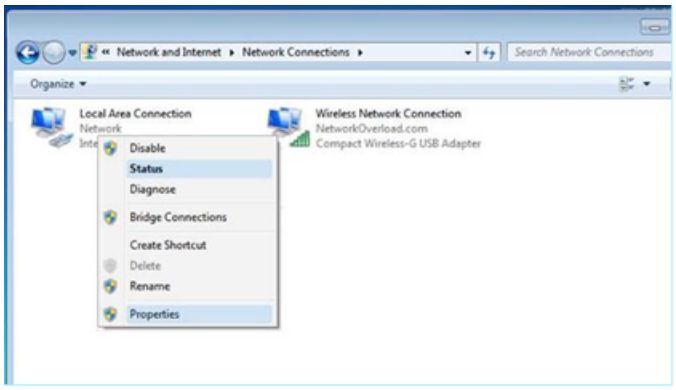
So loggen Sie sich bei der OT Security Verwaltungskonsole ein:

1. Führen Sie einen der folgenden Schritte aus:
   - Verbinden Sie die Workstation der Verwaltungskonsole (z. B. PC und Laptop) über das Ethernet-Kabel direkt mit Port 1 der OT Security Appliance.
   - Verbinden Sie die Workstation der Verwaltungskonsole mit dem Netzwerk-Switch.

   > Hinweis: Stellen Sie sicher, dass die Workstation der Verwaltungskonsole entweder Teil desselben Subnetzes ist wie die OT Security Appliance (192.168. 1.0/24) oder an das Gerät umgeleitet werden kann.

2. Richten Sie wie folgt eine statische IP ein, um eine Verbindung zur OT Security Appliance herzustellen:
   a. Gehen Sie zu Netzwerk und Internet > Netzwerk- und Freigabecenter > Adaptereinstellungen ändern.

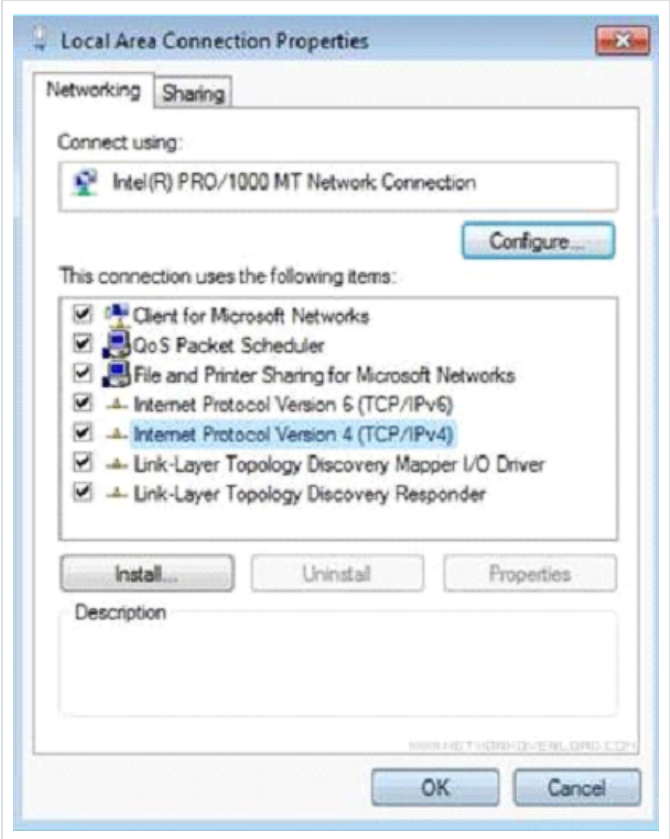
      Der Bildschirm Netzwerkverbindungen wird angezeigt.




> Hinweis: Die Navigation kann bei den verschiedenen Windows-Versionen leicht variieren.

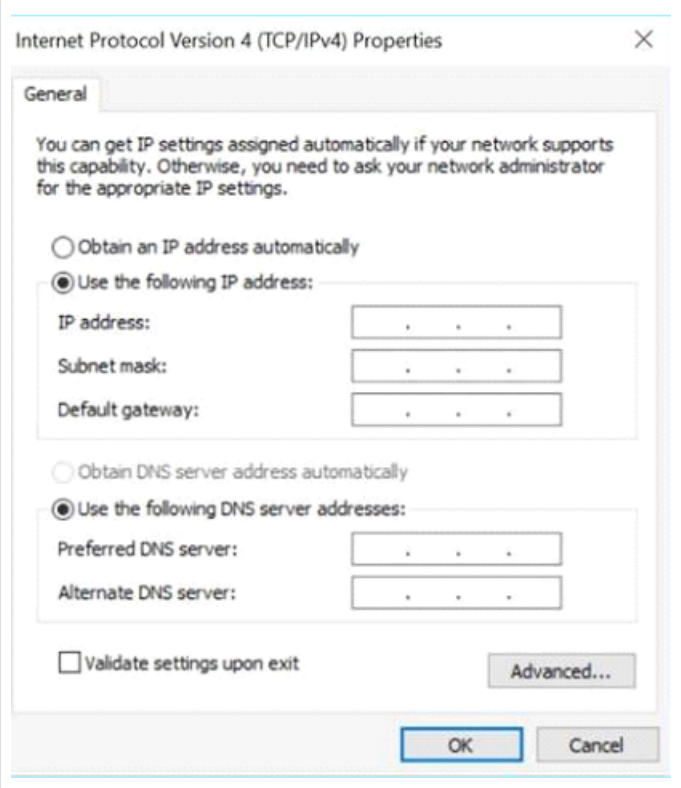
b. Klicken Sie mit der rechten Maustaste auf LAN-Verbindung und wählen Sie Eigenschaften aus.

Das Fenster LAN-Verbindung wird angezeigt.



c. Wählen Sie Internetprotokoll, Version 4 (TCP/IPv4) und klicken Sie auf Eigenschaften.

   Das Fenster mit den Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4) wird angezeigt.




d. Wählen Sie Folgende IP-Adresse verwenden aus.

e. Geben Sie in das Feld IP-Adresse 192.168.1.10 ein.

f. Geben Sie in das Feld Subnetzmaske 255.255.255.0 ein.

g. Klicken Sie auf OK.

   OT Security wendet die neuen Einstellungen an.

h. Navigieren Sie im Chrome-Browser zu https://192.168.1.5.

   Der Begrüßungsbildschirm des Setup-Assistenten wird geöffnet.


> Hinweis: Für den Zugriff auf die Benutzeroberfläche ist die neueste Version von Chrome erforderlich.

i. Klicken Sie auf Setup starten.

   Der Setup-Assistent wird geöffnet und zeigt die Seite Benutzerinformationen an.

### Nächste Schritte

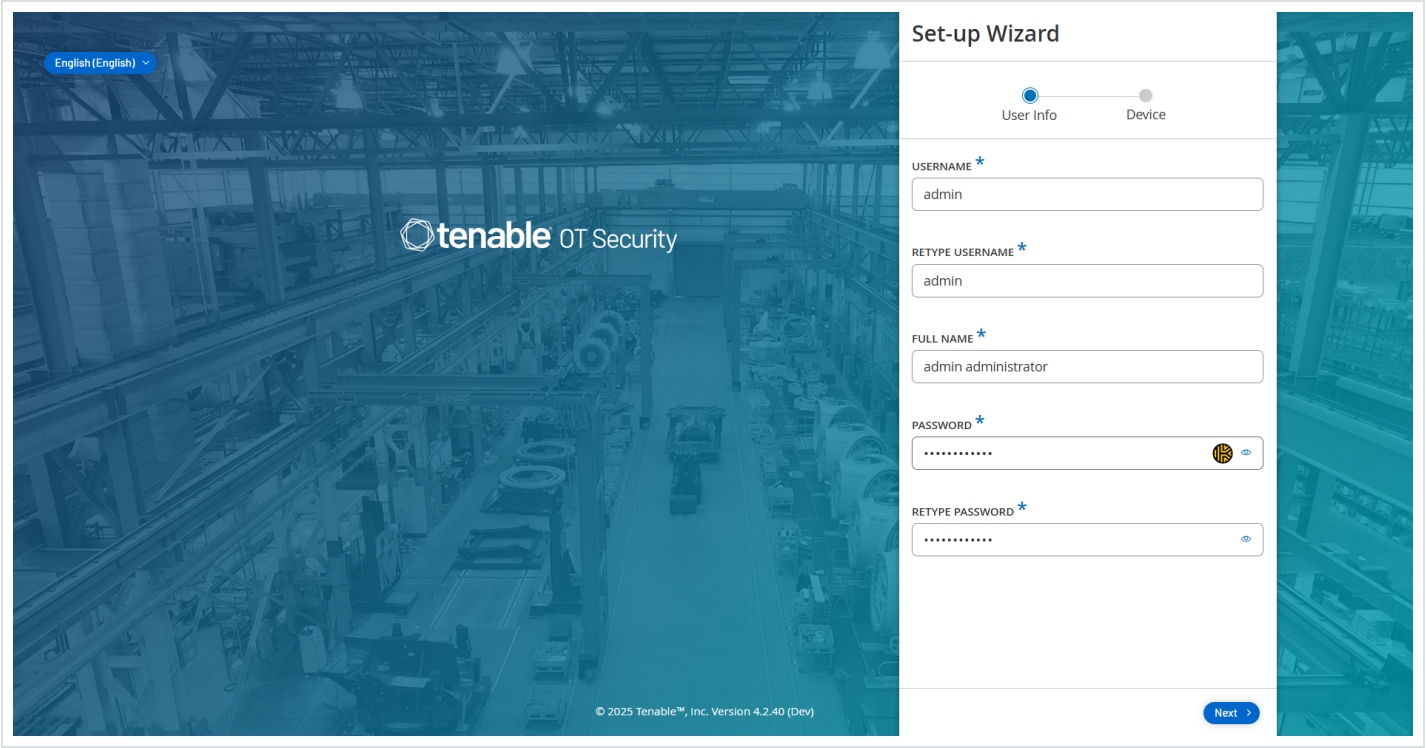
Benutzerinformationen

## Benutzerinformationen

Der Setup-Assistent von OT Security führt Sie durch die Konfiguration der grundlegenden Systemeinstellungen.

> Hinweis: Sie können die Konfiguration bei Bedarf im Bildschirm Einstellungen in der Verwaltungskonsole (Benutzeroberfläche) ändern.

Benutzerinformationen




Geben Sie auf der Seite Benutzerinformationen die Informationen zu Ihrem Benutzerkonto ein.

> Hinweis: Im Setup-Assistenten können Sie die Zugangsdaten für ein Administratorkonto konfigurieren. Nachdem Sie sich bei der Benutzeroberfläche eingeloggt haben, können Sie zusätzliche Benutzerkonten erstellen. Weitere Informationen zu Benutzerkonten finden Sie im Abschnitt Benutzer und Rollen.

1. Geben Sie im Feld Benutzername einen Benutzernamen zum Einloggen beim System ein.

   Der Benutzername kann bis zu 12 Zeichen lang sein und darf nur Kleinbuchstaben und Zahlen enthalten.

2. Geben Sie im Feld Benutzernamen erneut eingeben den Benutzernamen erneut ein.

3. Geben Sie im Abschnitt Vollständiger Name Ihren vollständigen Vor- und Nachnamen ein.

   > Hinweis: Dies ist der Name, der in der Kopfleiste und in Ihren Aktivitätsprotokollen im System angezeigt wird.

4. Geben Sie im Feld Passwort ein Passwort zum Einloggen beim System ein.
   Mindestanforderungen für Passwörter:
   - 12 Zeichen
   - Ein Großbuchstabe
   - Ein Kleinbuchstabe
   - Eine Zahl
   - Ein Sonderzeichen
5. Geben Sie im Feld Passwort erneut eingeben das Passwort erneut ein.
6. Klicken Sie auf Weiter.

   Die Seite Gerät des Setup-Assistenten wird geöffnet.

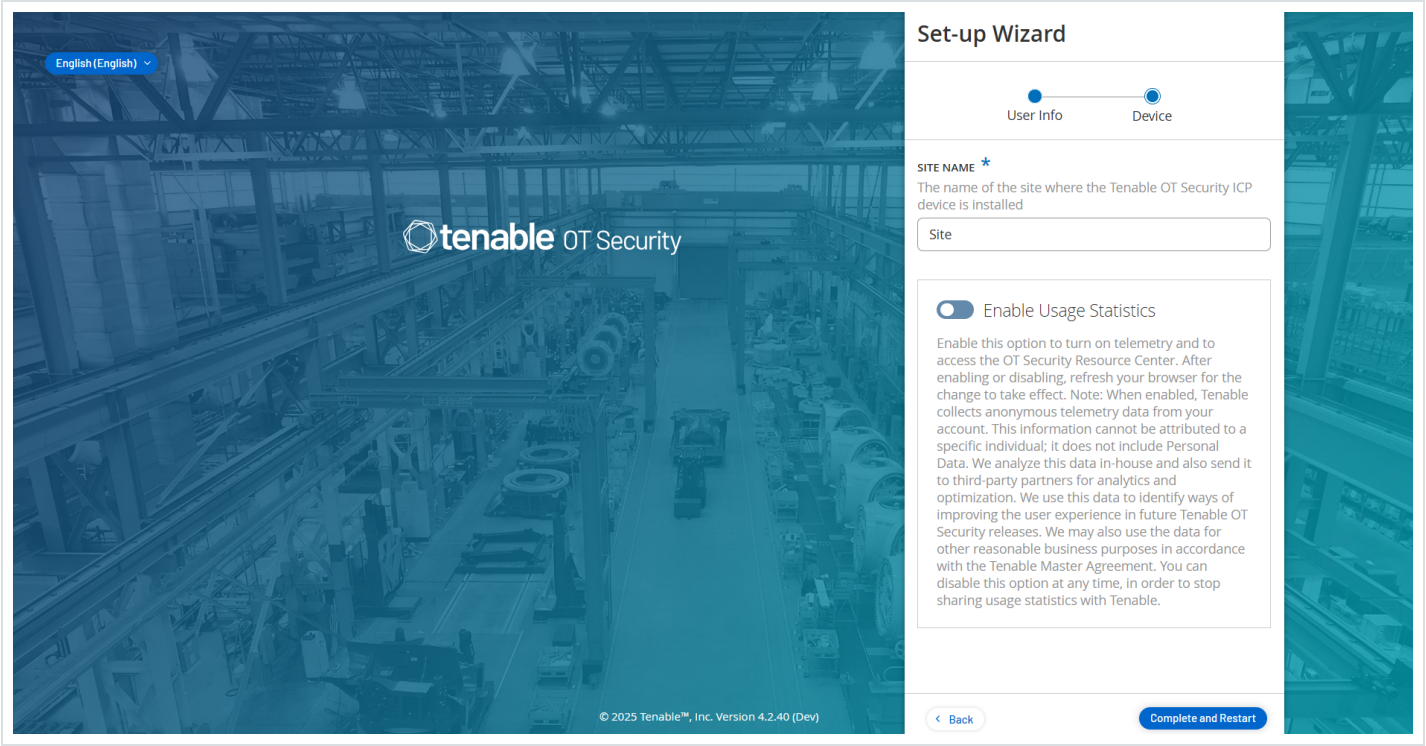
## Nächste Schritte

Gerät konfigurieren

## Gerät

Der Setup-Assistent von OT Security führt Sie durch die Konfiguration der grundlegenden Systemeinstellungen.

> Hinweis: Sie können die Konfiguration bei Bedarf im Bildschirm Einstellungen in der Verwaltungskonsole (Benutzeroberfläche) ändern.




Geben Sie auf der Seite Gerät Informationen zur OT Security-Plattform an:

1. Geben Sie im Feld Site-Name den Namen der Site an, auf der Sie OT Security installiert haben.
2. (Optional) Klicken Sie auf den Umschalter Nutzungsstatistiken aktivieren, damit OT Security Telemetriedaten erfassen und auf das Ressourcen-Center zugreifen kann.
3. Klicken Sie auf Abschließen und neu starten.

   OT Security wird neu gestartet.

## Nächste Schritte

- Verbinden und Trennung der Ports für Verwaltung und aktive Abfragen konfigurieren
- Lizenzaktivierung für OT Security

## Verbinden und Trennung der Ports für Verwaltung und aktive Abfragen konfigurieren

Dies ist ein optionaler Schritt. Wenn Sie die Split-Port-Option ausgewählt haben (um die Schnittstellenrolle für aktive Abfragen von der Verwaltungsrolle zu trennen), können Sie jetzt die sekundäre Schnittstelle der OT Security Appliance mit der entsprechenden Netzwerk-Switch-Schnittstelle verbinden, sofern Sie dies noch nicht in Tenable Core getan haben.

Weitere Informationen finden Sie unter Trennung der Rollen für Verwaltung und aktive Abfragen (Split-Port).

So verbinden Sie den Verwaltungsport:

1. Schließen Sie an der OT Security Appliance ein Ethernet-Kabel (mitgeliefert) an Port 3 an.
2. Schließen Sie das Kabel an einen Port an einem Netzwerk-Switch an.

## Lizenzaktivierung für OT Security

Erforderliche OT Security-Benutzerrolle: Administrator

Ziel: Freischaltung von Systemfunktionen durch Lizenzaktivierung.

Tenable berechnet Lizenzen basierend auf der Anzahl eindeutiger IP-Adressen im System. Jede IP-Adresse erfordert eine separate Lizenz. Beispiel: Tenable basiert die Lizenzierung auch dann auf der Anzahl eindeutiger IP-Adressen, wenn mehrere Geräte dieselbe IP-Adresse nutzen (mehrere Geräte, die mit derselben Backplane verbunden sind und dieselben drei IP-Adressen verwenden). Deshalb benötigen Sie drei Lizenzen, unabhängig von der Anzahl der Geräte.

Nachdem Sie die OT Security Appliance installiert haben, können Sie Ihre Lizenz aktivieren.

Hinweis: Um Ihre OT Security-Lizenz zu aktualisieren oder neu zu initialisieren, wenden Sie sich an Ihren Tenable Account Manager. Sobald Ihr Tenable Account Manager Ihre Lizenz aktualisiert hat, können Sie Ihre Lizenz aktualisieren oder neu initialisieren.

Informationen zur Bereitstellung und Lizenzierung von Tenable OT Security für Tenable One finden Sie im Tenable One Deployment Guide.

Bevor Sie beginnen

- Installieren Sie die OT Security Appliance.
- Vergewissern Sie sich, dass Ihnen der Lizenzcode (20 Buchstaben/Ziffern) vorliegt, den Sie bei der Bestellung des Geräts von Tenable erhalten haben.
- Vergewissern Sie sich, dass Sie Zugang zum Internet haben. Wenn Ihr OT Security-Gerät nicht mit dem Internet verbunden ist, können Sie die Lizenz von jedem PC aus registrieren.
- Vergewissern Sie sich, dass Sie Zugriff auf das Tenable Account Management-Portal haben. Wenden Sie sich an Ihren Tenable Customer Success Manager, um Zugriff zu erhalten.

## OT Security-Lizenz aktivieren

Sie können Ihre OT Security-Lizenz aktivieren und das Tenable Account Management-Portal zum Erstellen neuer Sites für die Verwaltung Ihrer Assets nutzen.

Weitere Informationen zum Account Management-Portal finden Sie in der Dokumentation zum Account Management-Portal.

### So aktivieren Sie Ihre OT Security-Lizenz:

1. Melden Sie sich mit Ihrem Community-Konto beim Tenable Account Management-Portal an.

   Die Seite Account (Konto) wird mit den Optionen angezeigt, für die Sie Anzeigeberechtigungen haben.

2. Klicken Sie auf die Tenable OT Security-Lizenz.

Die Seite Details für **Tenable OT Security** wird angezeigt. Die OT Security-Lizenzen werden mit Details wie Kaufdatum, Ablaufdatum und Anzahl der lizenzierten IP-Adressen und Sites angezeigt.

3. Kopieren Sie den 20-stelligen OT Security-Lizenzcode aus der Spalte für den Aktivierungscode.
4. Generieren Sie das Aktivierungszertifikat in OT Security:
    a. Gehen Sie in OT Security zur Seite Lizenzaktivierung.
    b. Klicken Sie in Schritt 1 auf Neuen Lizenzcode eingeben.

        Der Bereich Neuen Lizenzcode eingeben wird angezeigt.

    c. Fügen Sie im Feld Lizenzcode den Code (Aktivierungscode) ein, den Sie im Account Management-Portal kopiert haben.
    d. Klicken Sie auf Verifizieren.

        In OT Security wird der Abschnitt Aktivierungszertifikat generieren aktiviert.

    e. Klicken Sie auf Zertifikat generieren.

        Der Bereich Zertifikat generieren wird angezeigt.

    f. Klicken Sie auf Text in die Zwischenablage kopieren und dann auf Fertig.

        OT Security generiert das Zertifikat, das Sie im Tenable Account Management-Portal angeben müssen, um Ihre Sites hinzuzufügen.
5. Klicken Sie in Schritt 3 im Abschnitt Aktivierungscode eingeben auf den Link Self-Service, um das Tenable Account Management-Portal zu öffnen.

    Die Seite des Account Management-Portals wird angezeigt.

> Hinweis: Um den Evaluierungszeitraum zu aktivieren, klicken Sie auf den Link Click here (Hier klicken).

6. Klicken Sie im linken Navigationsbereich auf Produkte.

   Die Seite My Products (Meine Produkte) wird angezeigt.

7. Suchen Sie mit dem 20-stelligen Lizenzcode von OT Security nach Ihrem Produkt.

   Das OT Security-Produkt mit dem spezifischen Lizenzcode wird angezeigt.

8. Klicken Sie auf die Registerkarte Sites.

   Die Registerkarte Sites (Sites) wird angezeigt.

9. Um eine Site zu erstellen, klicken Sie auf Manage Sites (Sites verwalten) > Create Site (Site erstellen).

   Das Fenster Create New Site (Neue Site erstellen) wird angezeigt.

   a. (Optional) Geben Sie im Feld Label (Bezeichnung) einen Namen für die Site ein.

      > Tipp: Verwenden Sie das Feld Label (Bezeichnung), um den Namen des Geräts oder der ICP anzugeben, damit Sie die verschiedenen Sites besser unterscheiden können.

   b. Geben Sie in das Feld Size (Größe) die Anzahl der IP-Adressen ein, die Sie dieser Site zuweisen möchten.

      > Tipp: Um die Anzahl der IP-Adressen anzupassen, die der Lizenz zugewiesen sind, können Sie den Schieberegler unter dem Feld Size (Größe) verwenden.

   c. Fügen Sie im Feld Activation Certificate (Aktivierungszertifikat) das Zertifikat ein, das Sie aus OT Security kopiert haben. Siehe Schritt f.

   d. Klicken Sie auf Erstellen.

Daraufhin wird ein Dialogfeld mit einem Aktivierungscode angezeigt. Dies ist ein generierter Einmal-Code, den Sie in die OT Security-Instanz kopieren müssen.

e. Klicken Sie auf die Schaltfläche .

f. Klicken Sie auf Confirm (Bestätigen).

10. Navigieren Sie zurück zur OT Security-Instanz.
11. Klicken Sie in Schritt 3 im Abschnitt Aktivierungscode eingeben auf Aktivierungscode eingeben.

    Der Bereich Aktivierungscode eingeben wird auf der rechten Seite angezeigt.
12. Fügen Sie im Feld Aktivierungscode den generierten Einmal-Code ein, den Sie auf der Seite Tenable OT Security Account Management kopiert haben. Siehe Schritt 8e.
13. Klicken Sie auf Aktivieren.

    In OT Security wird die Bestätigungsmeldung angezeigt, dass das System erfolgreich aktiviert wurde, und die Benutzeroberfläche von OT Security wird angezeigt.
14. Klicken Sie auf Aktivieren.

    OT Security ist jetzt aktiviert und kann verwendet werden.
15. Navigieren Sie zurück zum Tenable Account Management-Portal und aktivieren Sie im Dialogfeld mit dem generierten Einmal-Aktivierungscode das Kontrollkästchen I confirm I have saved the activation license (Ich bestätige, dass ich die Aktivierungslizenz gespeichert habe).
16. Klicken Sie auf Confirm (Bestätigen).

    Die neu hinzugefügte Site wird auf der Registerkarte Sites (Sites) für OT Security angezeigt.

## Lizenz aktualisieren

Wenn Sie Ihr Asset-Limit erhöhen, Ihren Lizenzzeitraum verlängern oder Ihren Lizenztyp ändern, können Sie Ihre Lizenz aktualisieren. Wenn Sie Ihre Lizenz aktualisieren, verwenden Sie Ihren bestehenden 20-stelligen Lizenzcode.

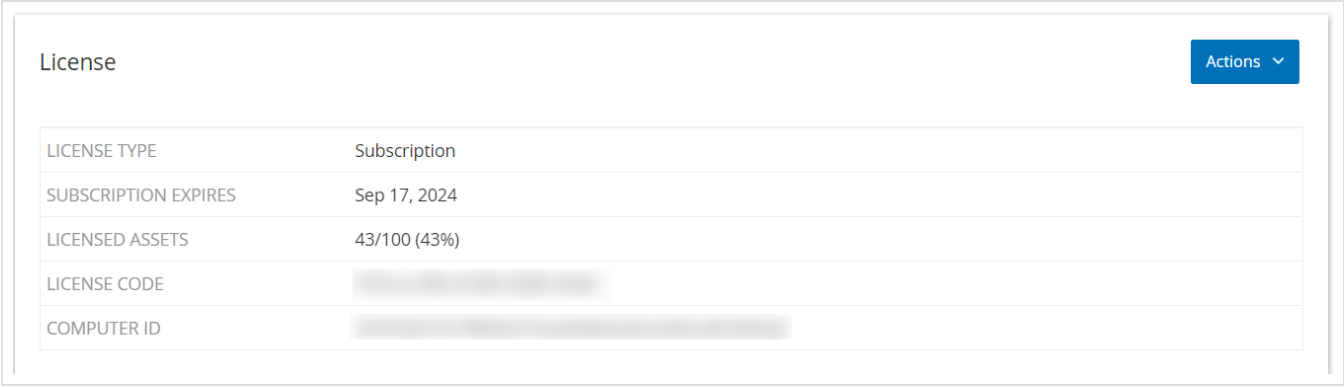
## Bevor Sie beginnen

- Ihr Tenable Account Manager muss Ihre Lizenzinformationen bereits in seinem System aktualisiert haben, bevor Sie Ihre Lizenz aktualisieren können.
- Sie benötigen Zugang zum Internet. Wenn Ihr OT Security-Gerät das Internet nicht erreichen kann, können Sie die Lizenz von jedem PC aus registrieren.

## So aktualisieren Sie Ihre Lizenz:

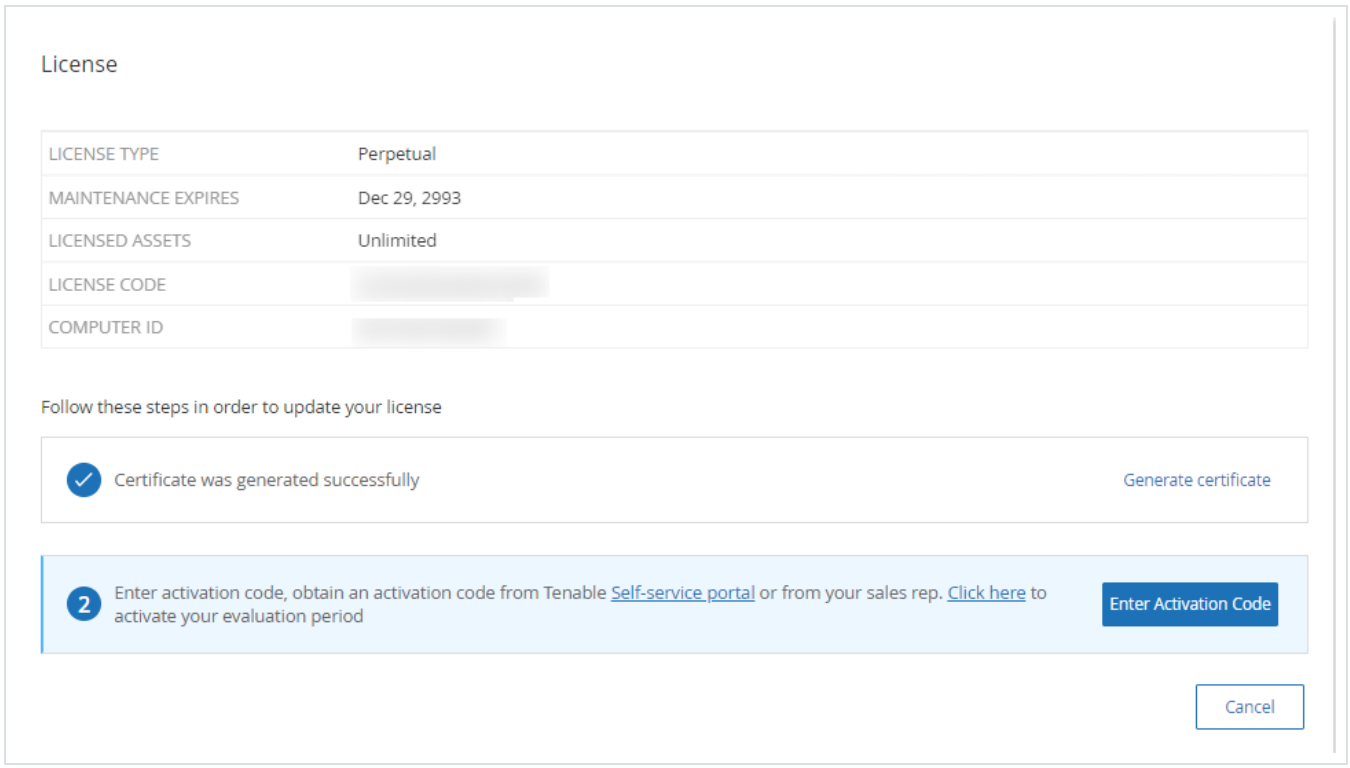
1. Gehen Sie zu  Einstellungen > Systemkonfiguration > Lizenz.

   Das Fenster Lizenz wird angezeigt.

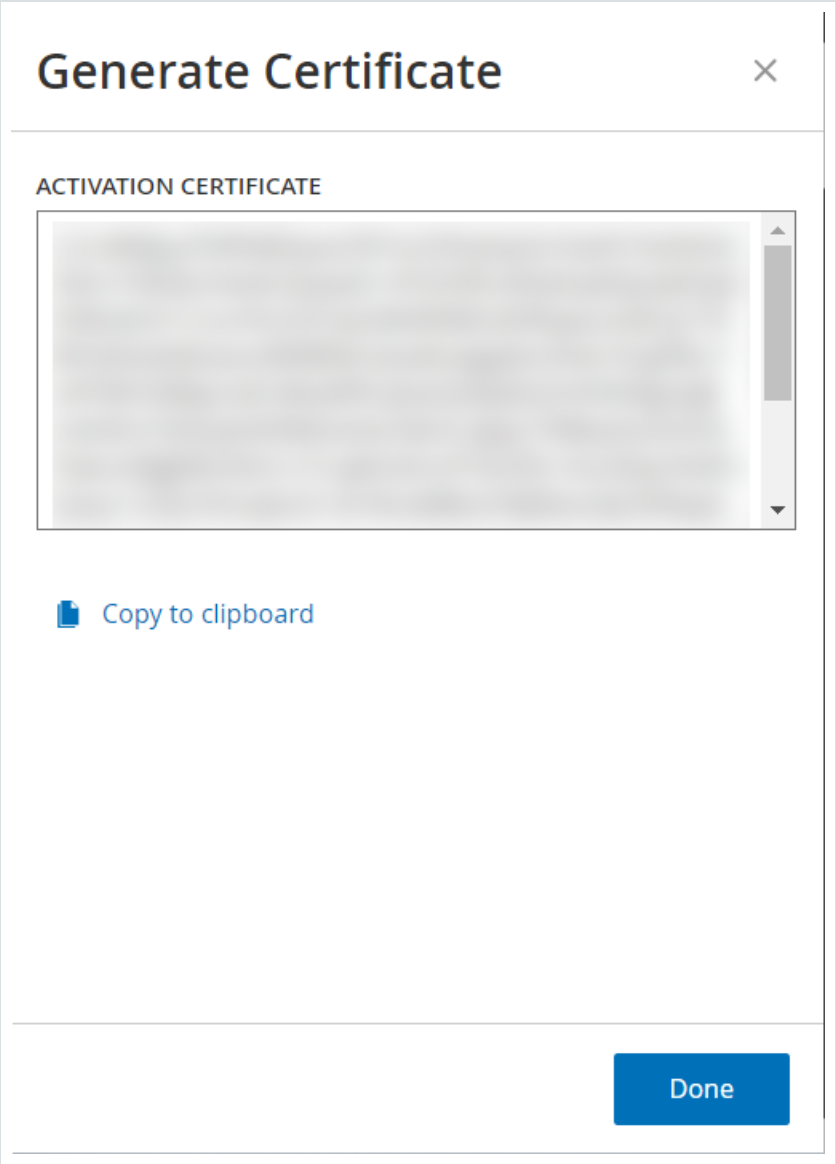
2. Wählen Sie im Menü Aktionen die Option Lizenz aktualisieren aus.

   Die Schritte Zertifikat generieren und Aktivierungscode eingeben werden angezeigt.




3. Klicken Sie im Feld (1) Aktivierungszertifikat generieren auf Zertifikat generieren.

   Der Bereich Zertifikat generieren wird mit dem Aktivierungszertifikat angezeigt.




4. Klicken Sie auf Text in die Zwischenablage kopieren und dann auf Fertig.

   Der Seitenbereich wird geschlossen.

5. Klicken Sie im Feld (2) Aktivierungscode eingeben auf den Link zum Self-Service-Portal.

   OT Security leitet Sie zur Seite My Account (Mein Konto) im Tenable Account Management-Portal weiter.

Hinweis: Wenn Sie sich im Evaluierungszeitraum befinden, klicken Sie auf den zweiten Link. Siehe Lizenz im Offline-Modus aktualisieren.

6. Bearbeiten Sie die Site-Details im Tenable Account Management-Portal:

   a. Klicken Sie im linken Navigationsbereich auf Produkte.

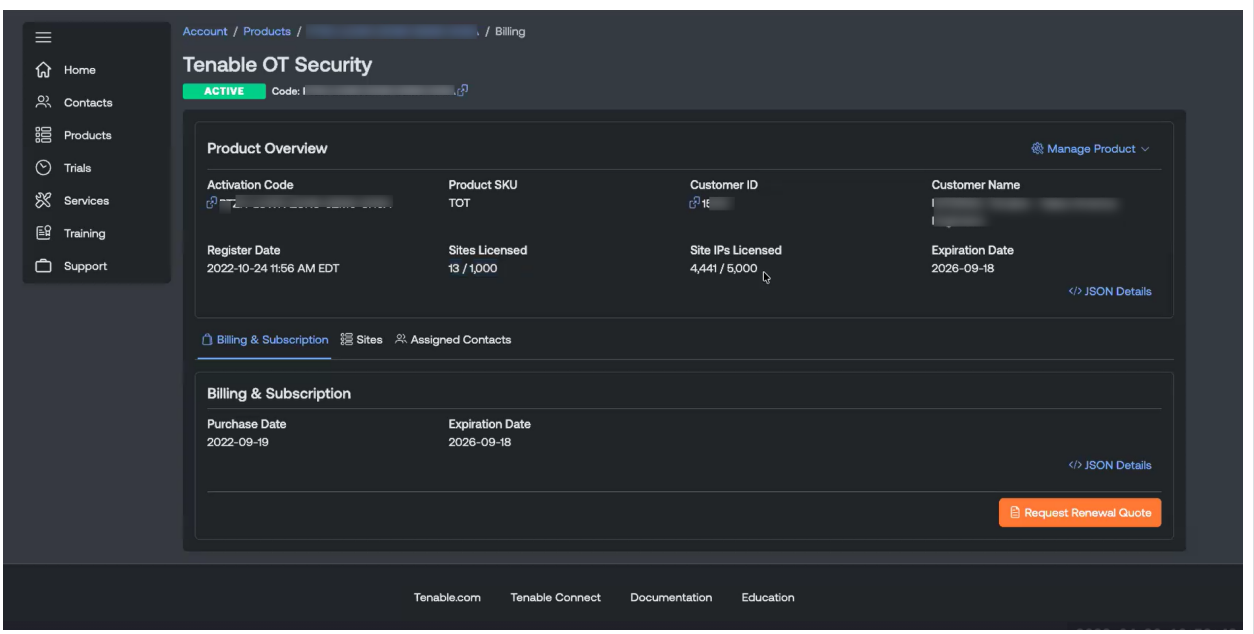
      Die Seite My Products (Meine Produkte) wird angezeigt.

   b. Suchen Sie mit dem 20-stelligen Lizenzcode von OT Security nach Ihrem Produkt.

      Das OT Security-Produkt mit dem spezifischen Lizenzcode wird angezeigt.

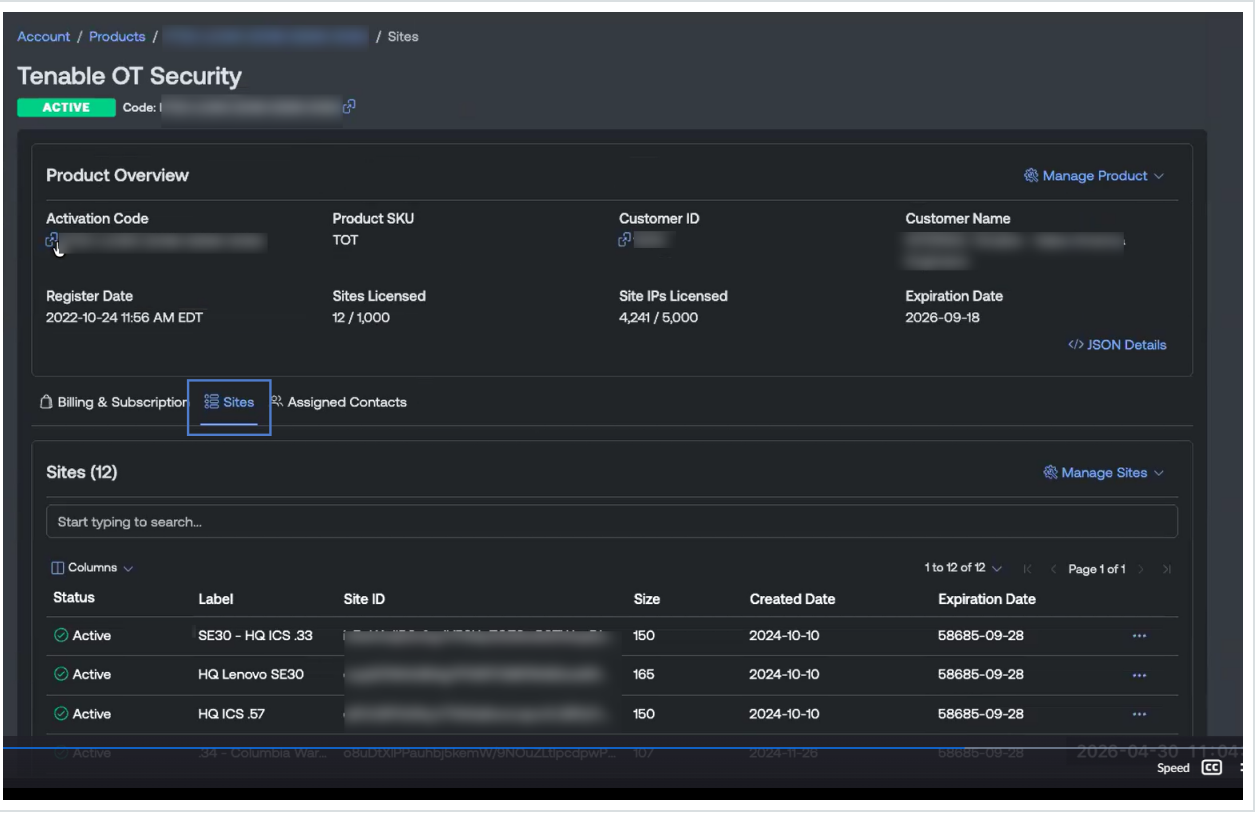
   c. Klicken Sie auf den Lizenzcode, um die Produktdetails anzuzeigen.

      Die Seite Tenable OT Security wird mit Details wie Produktübersicht, Abrechnung und Abonnement und Sites angezeigt.




   d. Klicken Sie auf die Registerkarte Sites.

      Der Abschnitt Sites (Sites) wird angezeigt.

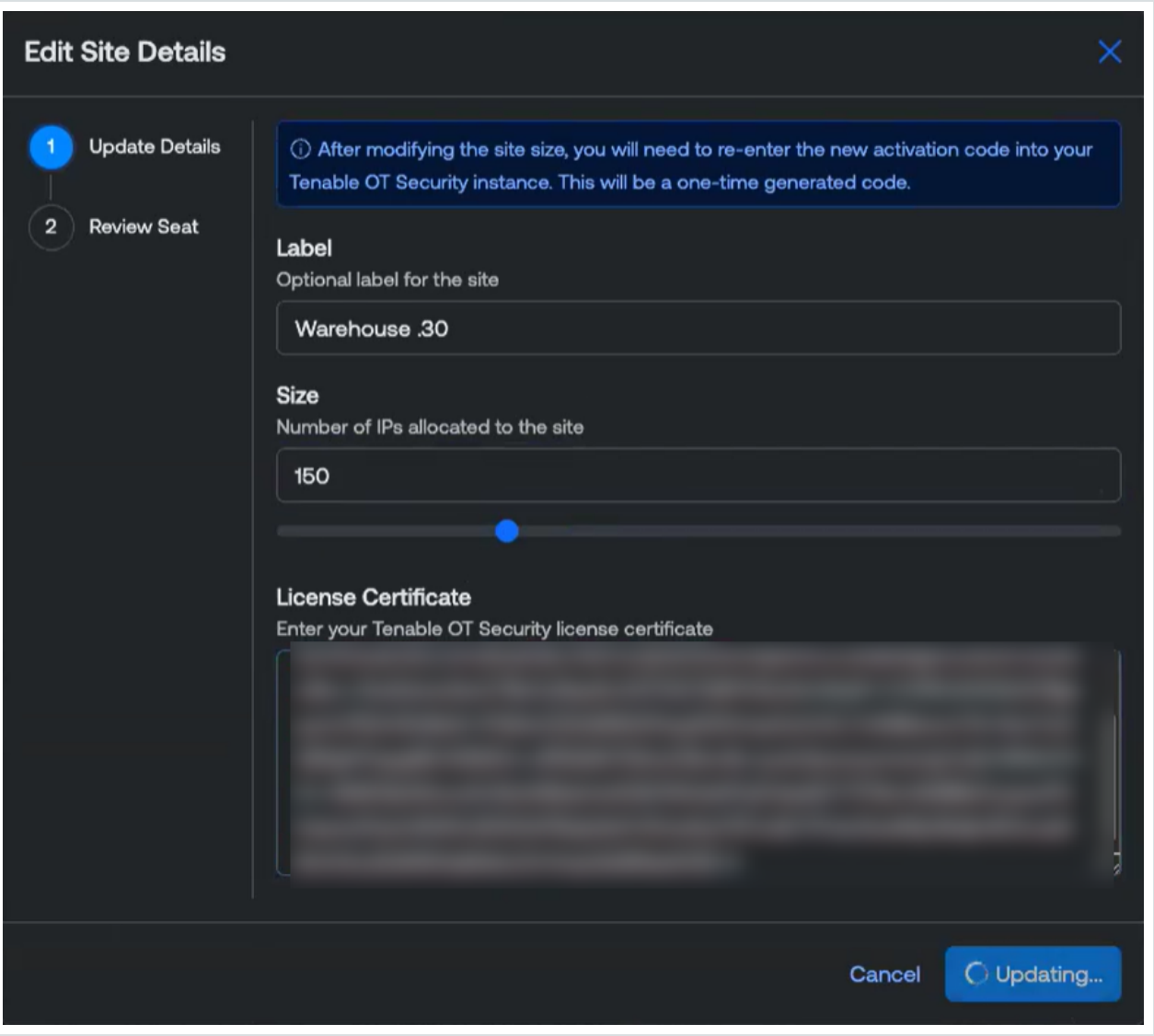



e. Klicken Sie in der Zeile der Site, die Sie bearbeiten möchten, auf die Schaltfläche ⋯.

   Ein Menü wird angezeigt.

f. Klicken Sie auf Edit Site (Site bearbeiten).

   Die Seite Edit Site Details (Site-Details bearbeiten) wird angezeigt.

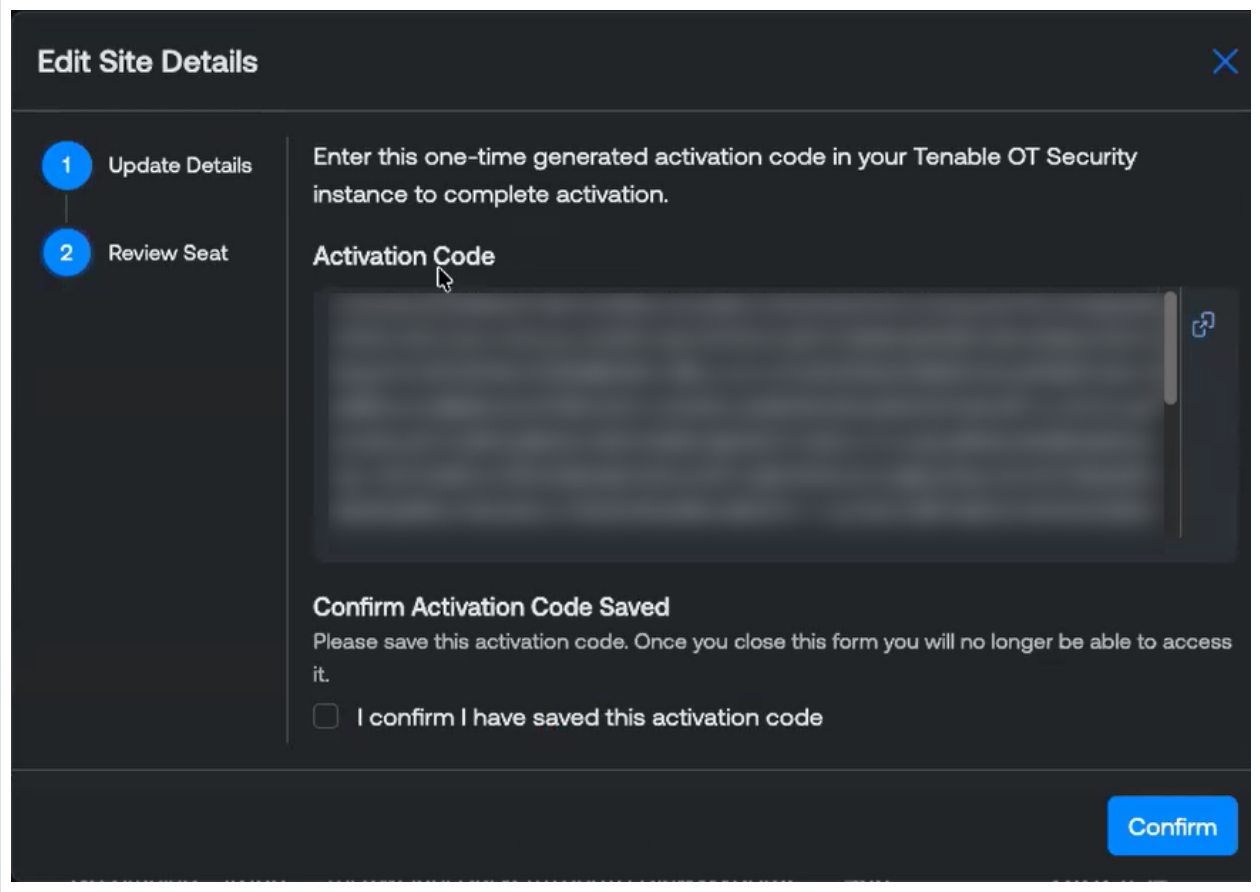



g. Passen Sie die Details nach Bedarf an.

h. Fügen Sie im Feld Activation Certificate (Aktivierungszertifikat) das Zertifikat ein, das Sie im Fenster Zertifikat generieren in OT Security kopiert haben.

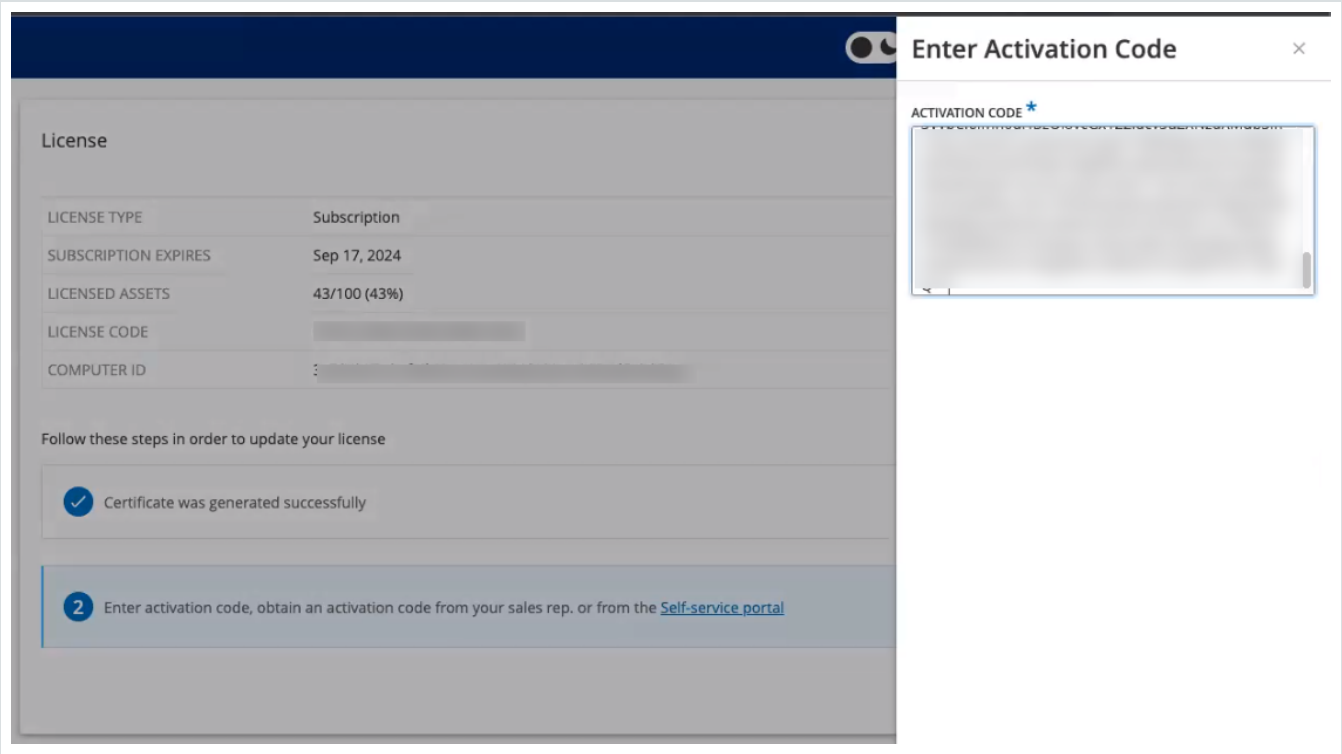
i. Klicken Sie auf Aktualisieren.

   Im Portal wird ein Dialogfeld mit einem Aktivierungscode angezeigt. Dies ist ein generierter Einmal-Code, den Sie in die OT Security-Instanz kopieren müssen.




j. Klicken Sie auf die Schaltfläche und dann auf Confirm (Bestätigen).

7. Navigieren Sie zurück zur OT Security-Instanz.
8. Klicken Sie im Feld (2) Aktivierungscode eingeben auf Aktivierungscode eingeben.
9. Fügen Sie im Feld Aktivierungscode den generierten Einmal-Code ein, den Sie auf der Seite Tenable OT Security Account Management kopiert haben.

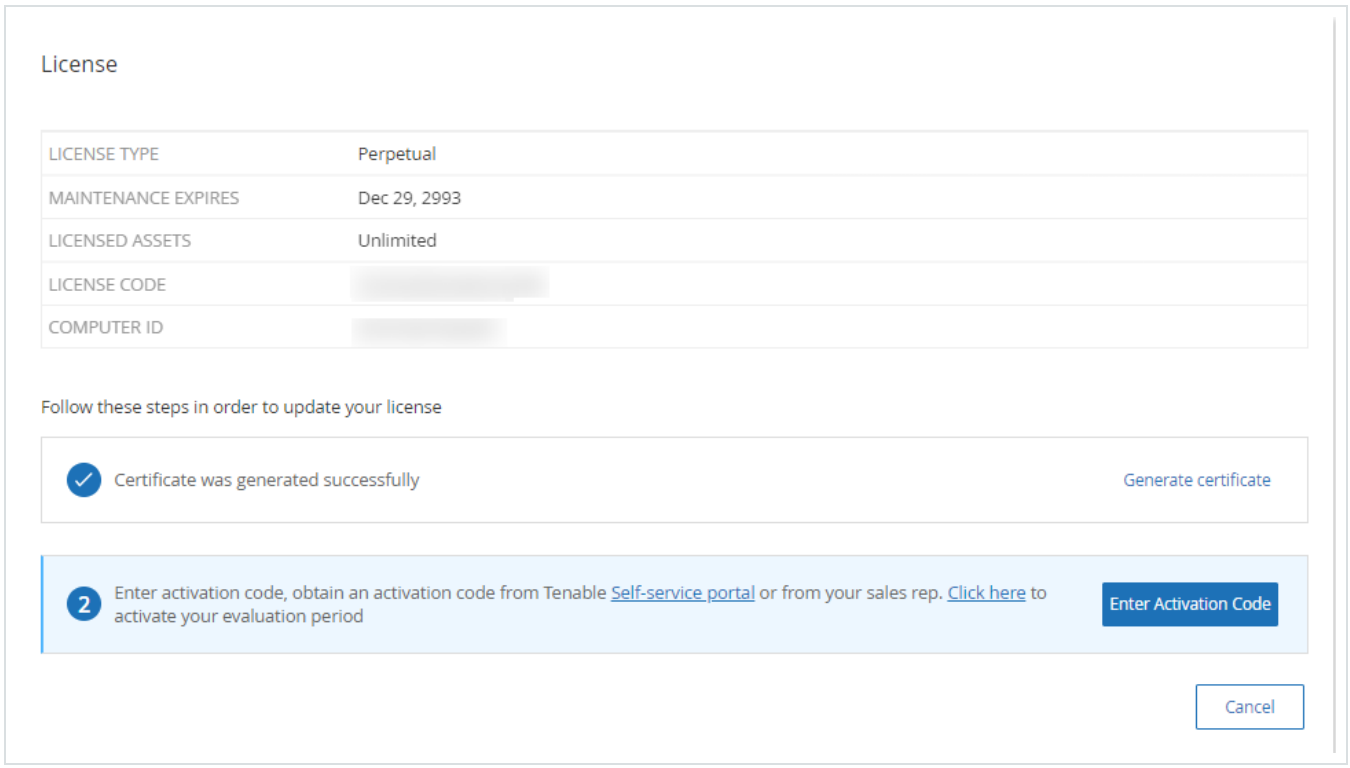



10. Klicken Sie auf Aktivieren.

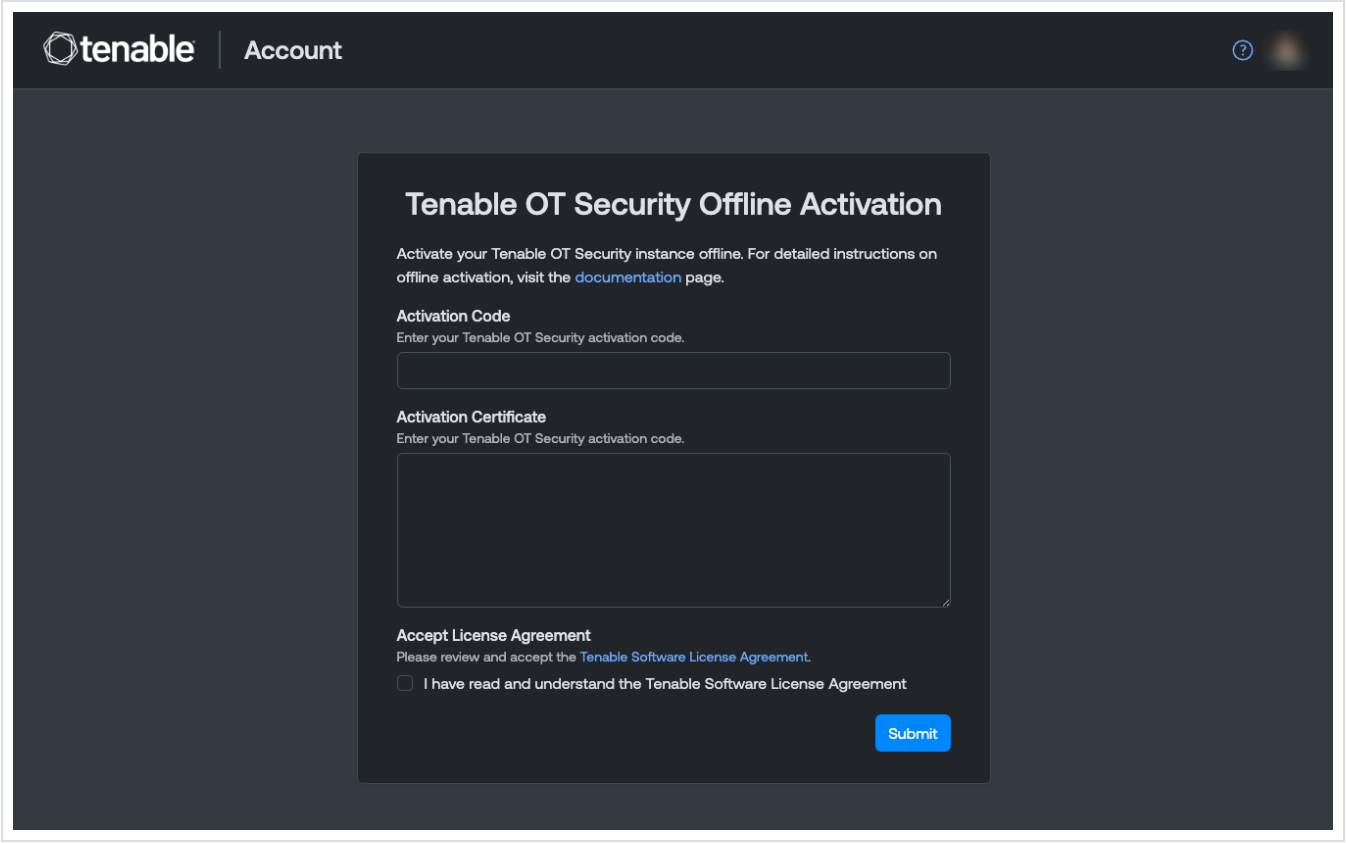
    In OT Security wird die Bestätigungsmeldung angezeigt, dass das System erfolgreich aktiviert wurde, und auf der Seite Lizenz werden die aktualisierten Lizenzdetails angezeigt.

## Lizenz im Offline-Modus aktualisieren

1. Führen Sie die Schritte 1 bis 4 wie im Abschnitt Lizenz aktualisieren beschrieben aus.
2. Klicken Sie im Feld (2) Aktivierungscode eingeben auf den Link zum Self-Service-Portal.




Das Fenster OT Security offline aktivieren wird auf einer neuen Registerkarte geöffnet.



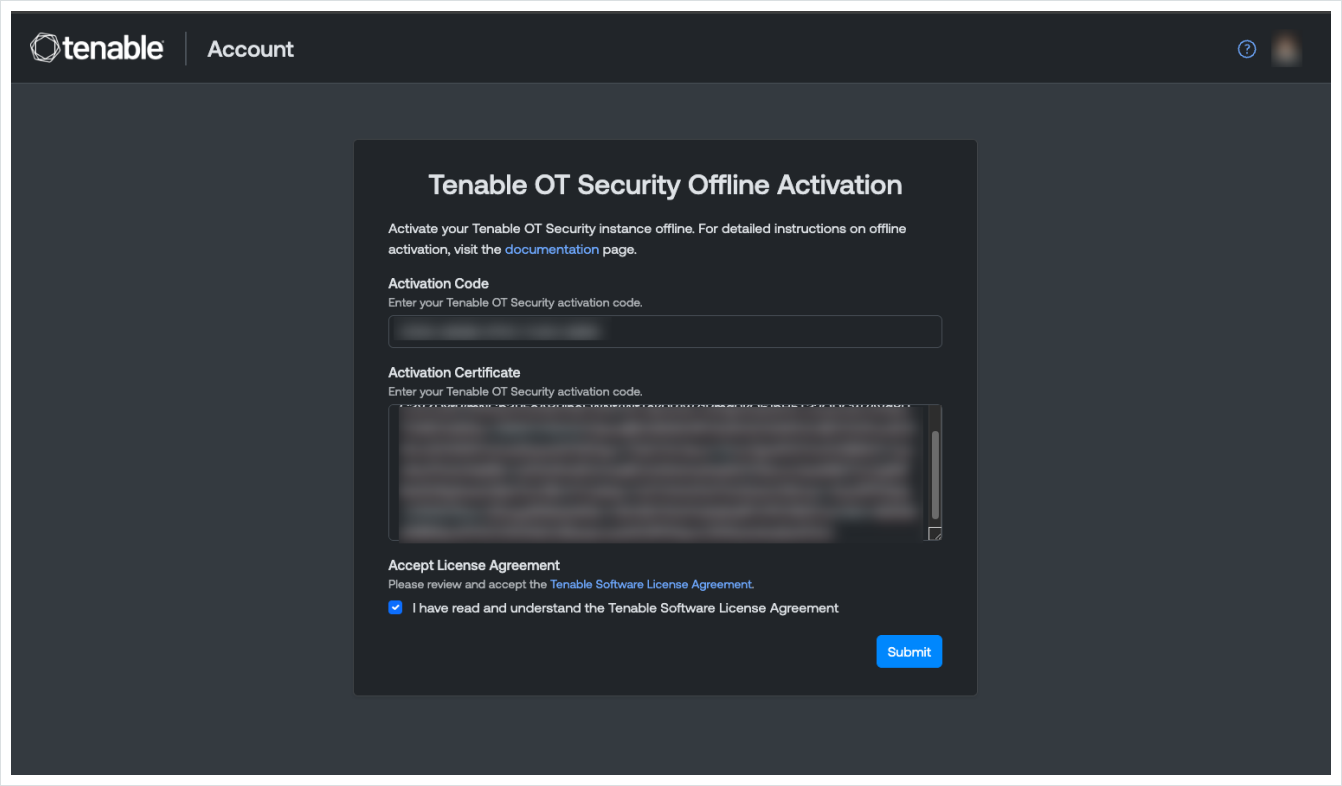

> Hinweis: Sie können den Bildschirm „OT Security offline aktivieren“ von einem mit dem Internet verbundenen Gerät über die folgende URL aufrufen: https://account.tenable.com/offline-activation/ot-security.

> Hinweis: Wenn Sie nicht bei tenable.com eingeloggt sind, können Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort einloggen. Verwenden Sie das E-Mail-Konto, über das Sie Ihren Lizenzcode erhalten haben. Wenn Sie keine Login-Zugangsdaten haben, können Sie entweder auf Passwort vergessen klicken (und den Anweisungen folgen) oder sich an Ihren Tenable Account Manager wenden.

3. Geben Sie im Feld Aktivierungscode Ihren 20-stelligen Lizenzcode ein (diesen können Sie im Fenster Lizenz kopieren und hier einfügen).

4. Fügen Sie im Feld Aktivierungszertifikat das Aktivierungszertifikat ein.

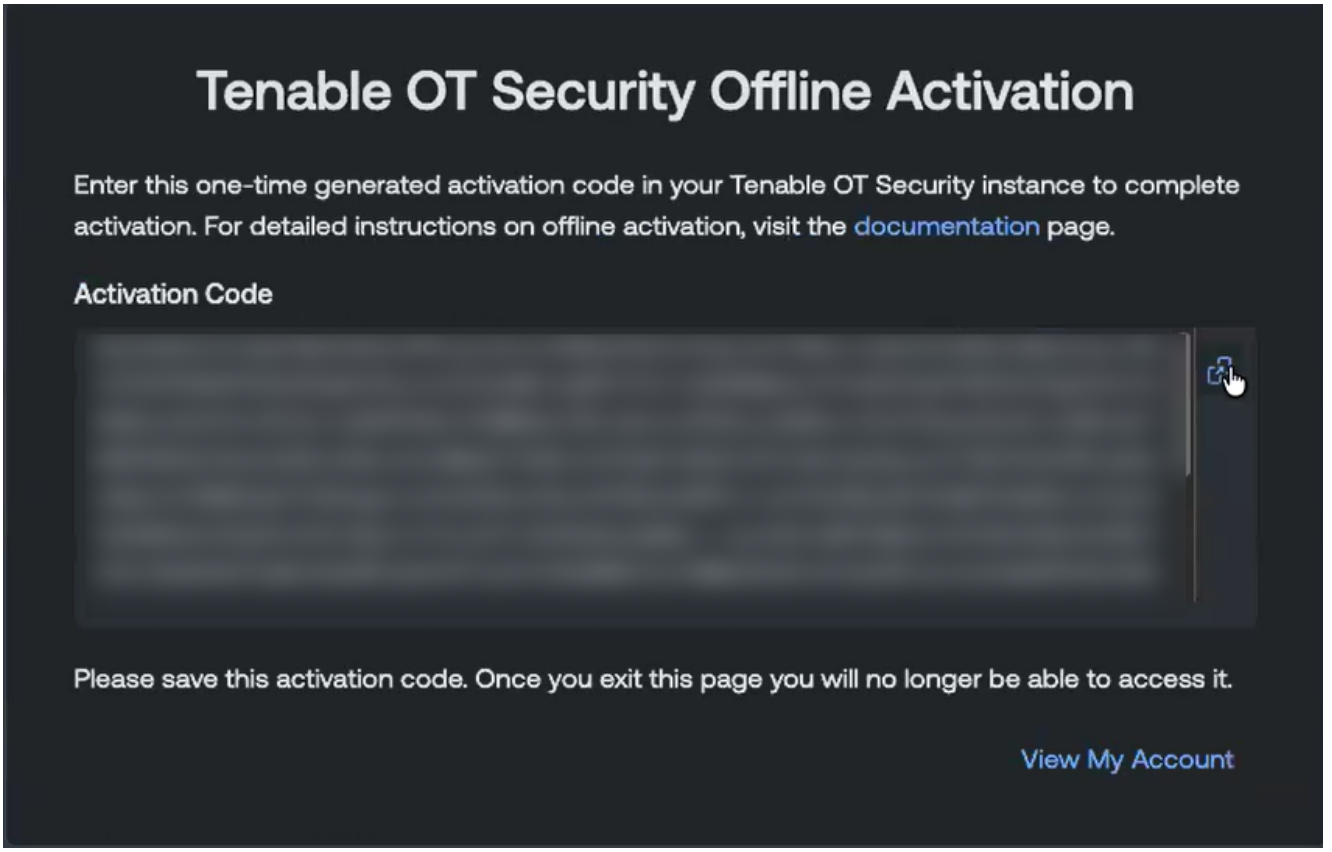
5. Aktivieren Sie das Kontrollkästchen Ich habe die Tenable-Softwarelizenzvereinbarung gelesen und verstanden.




> Hinweis: Um die Lizenzvereinbarung anzuzeigen, klicken Sie auf den Link Tenable-Softwarelizenzvereinbarung.

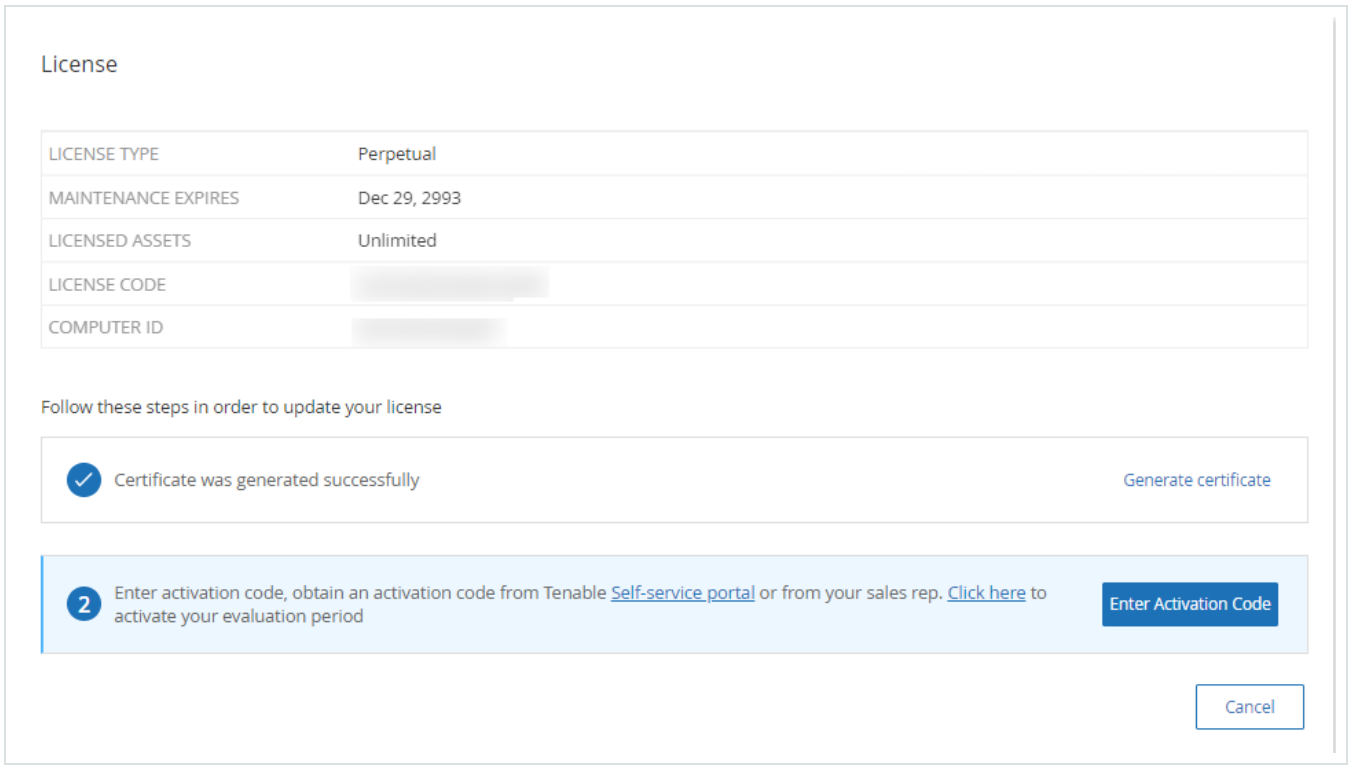
6. Klicken Sie auf Senden.

   OT Security generiert den Aktivierungscode.



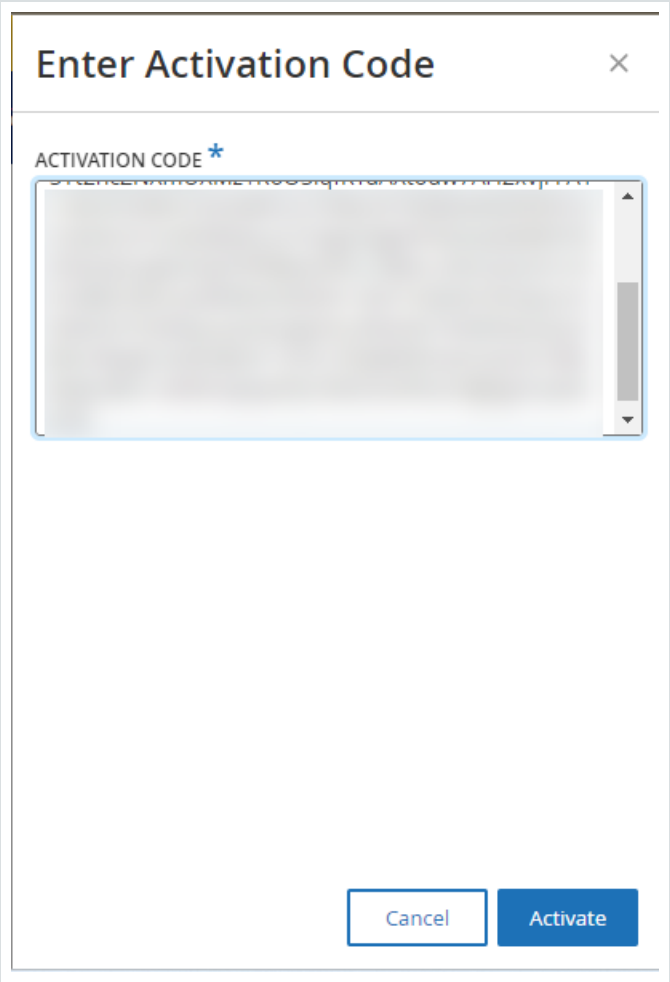

7. Um den Aktivierungscode zu kopieren, klicken Sie auf die Schaltfläche .

8. Navigieren Sie zurück zur Registerkarte Lizenz in OT Security und klicken Sie auf Aktivierungscode eingeben.




Der Seitenbereich Aktivierungscode eingeben wird angezeigt.

9. Fügen Sie Ihren Aktivierungscode in das Feld Aktivierungscode ein und klicken Sie auf die Schaltfläche Aktivieren.




Der Seitenbereich wird geschlossen und die Lizenz wird von OT Security aktualisiert.

## Lizenz neu initialisieren

Durch die Neuinitialisierung Ihrer Lizenz wird Ihre aktuelle Lizenz aus dem System entfernt und eine neue Lizenz aktiviert, ähnlich wie bei der Lizenzaktivierung während des Systemstarts. Wenn Sie Ihre Lizenz neu initialisieren müssen (d. h., wenn Sie eine neue Lizenz erhalten), verwenden Sie das folgende Verfahren.

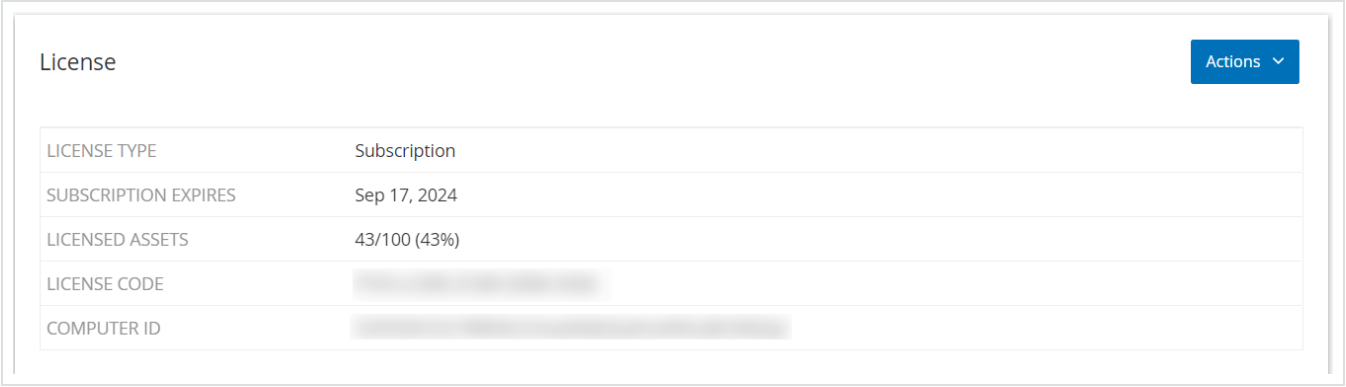
> Hinweis: Eine Evaluierungslizenz oder temporäre Lizenz hat immer einen eindeutigen Lizenzcode.

### Bevor Sie beginnen

- Ihr Tenable Account Manager muss Ihre neue Lizenz bereits in seinem System ausgestellt und Ihnen einen Lizenzcode (20 Buchstaben/Ziffern) bereitgestellt haben.
- Sie benötigen Zugang zum Internet. Wenn Ihr OT Security-Gerät nicht mit dem Internet verbunden werden kann, können Sie die Lizenz von jedem PC aus registrieren.

So initialisieren Sie Ihre Lizenz neu:

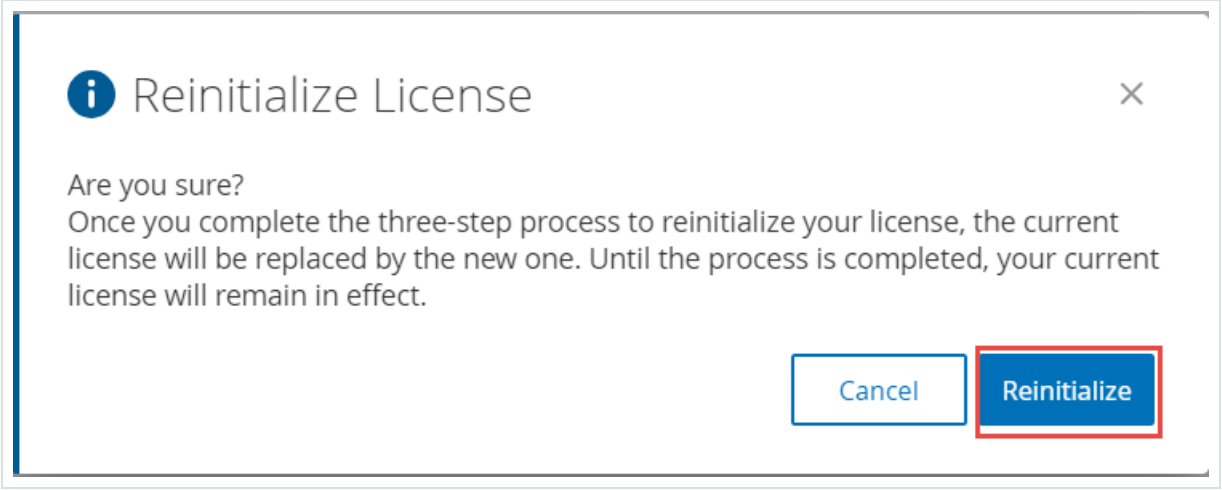
1. Gehen Sie zu Einstellungen > Systemkonfiguration > Lizenz.



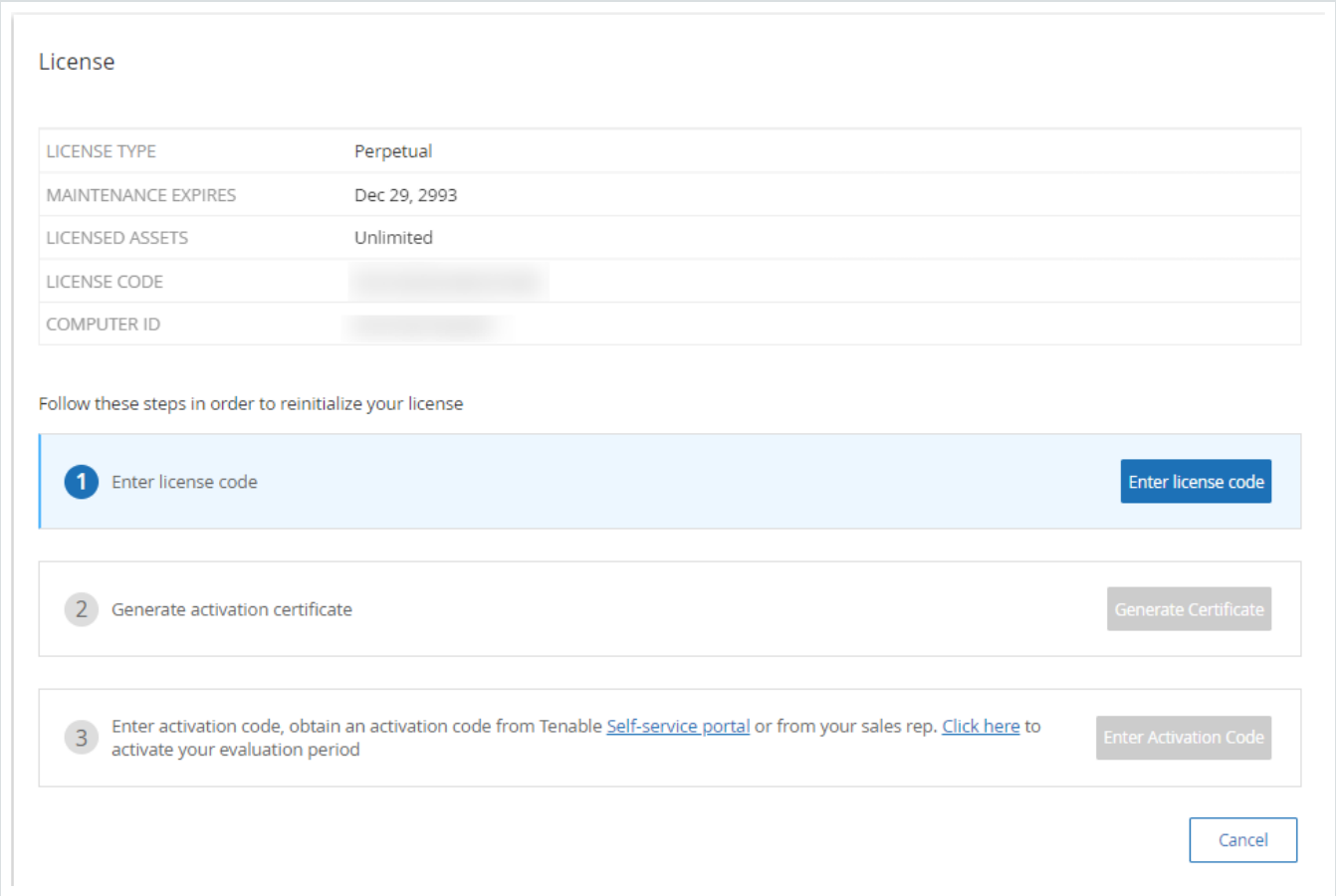

2. Wählen Sie im Menü Aktionen die Option Lizenz erneut initialisieren aus.

   Daraufhin wird ein Bestätigungsfenster angezeigt.

3. Klicken Sie auf Neu initialisieren.



Das Fenster Lizenz mit den drei Schritten zur Neuinitialisierung wird angezeigt.




4. Befolgen Sie die Schritte zum Systemstart ( Schritt 1 bis Schritt 17), um Ihre Lizenz im Abschnitt Lizenz aktivieren zu aktivieren.

   Nachdem Sie Ihren Aktivierungscode angegeben haben, wird Ihre aktuelle Lizenz durch Ihre neue Lizenz ersetzt.

### Nächste Schritte

Das OT Security-System aktivieren

## OT Security starten

Ziel: Start des Systems und seine Nutzung für Ihre OT-Sicherheitsbedürfnisse.

Nachdem Sie Tenable Core + OT Security konfiguriert haben, aktivieren Sie das System, um OT Security zu verwenden.

1. Das OT Security-System aktivieren – Aktivieren Sie das OT Security-System, nachdem Sie Ihre Lizenz aktiviert haben.
2. OT Security verwenden – Konfigurieren Sie Ihre überwachten Netzwerke, die Port-Trennung, Benutzer, Gruppen, Authentifizierungsserver so, dass sie OT Security verwenden.

## Das OT Security-System aktivieren

> Erforderliche OT Security-Benutzerrolle: Administrator

Nach Abschluss der Lizenzaktivierung zeigt OT Security die Schaltfläche Aktivieren an.


Aktivieren Sie OT Security, um die Kernfunktionen des Systems zu aktivieren, wie zum Beispiel:

- Identifizieren von Assets im Netzwerk
- Erfassen und Überwachen des gesamten Netzwerk-Traffic
- Protokollieren von „Konversationen“ im Netzwerk

Sie können alle zusammengestellten Daten und Analysen aus diesen Funktionalitäten in der Benutzeroberfläche einsehen.

> Hinweis: Dies sind laufende Prozesse, die sich über einen längeren Zeitraum erstrecken. Daher kann es einige Zeit dauern, bis in der Benutzeroberfläche vollständig aktualisierte Ergebnisse angezeigt werden.

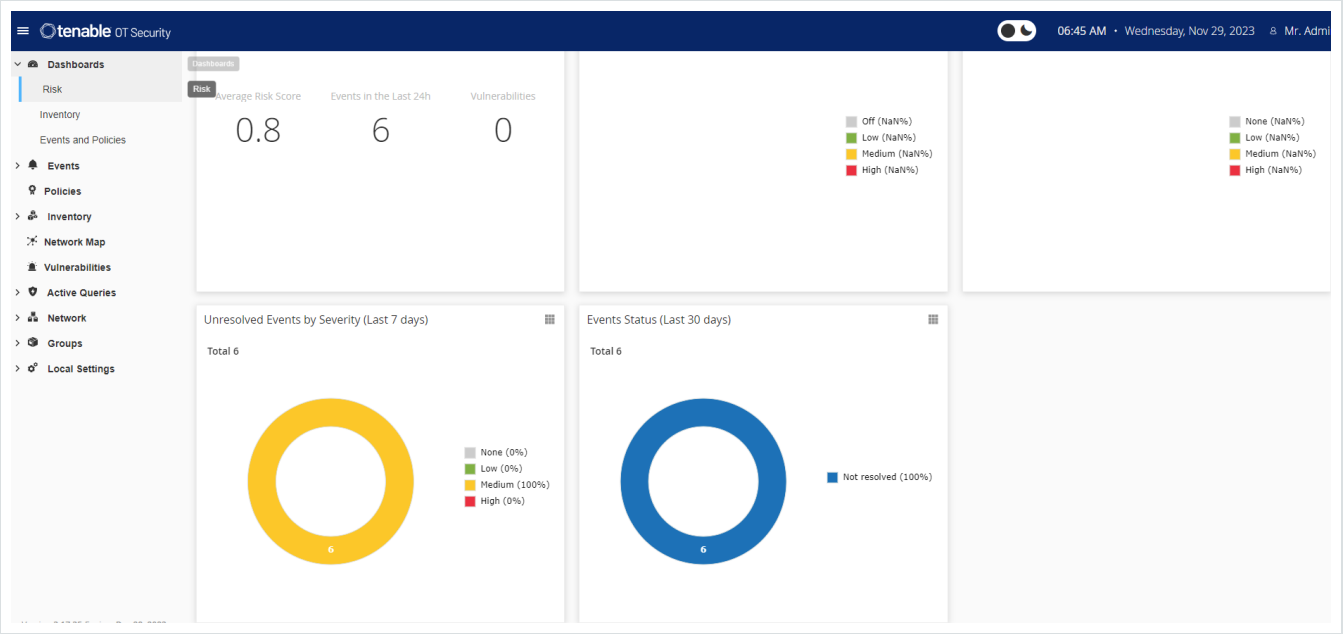
Sie können zusätzliche Funktionen wie aktive Abfragen im Fenster Einstellungen in der Verwaltungskonsole (Benutzeroberfläche) konfigurieren und aktivieren. Weitere Informationen finden Sie unter Aktive Abfragen.

> Wichtig: Ab Version 4.4 ist passives Monitoring standardmäßig deaktiviert, wenn Sie OT Security aktivieren, um übermäßige Warnungen zu reduzieren. Um das passive Monitoring zu aktivieren, navigieren Sie zur Seite Einstellungen > Netzwerkdefinitionen und aktivieren Sie den Umschalter Passives Monitoring. Das Symbol für passives Monitoring in der Kopfzeile zeigt an, ob das passive Monitoring aktiviert oder deaktiviert ist.

So aktivieren Sie OT Security:

1. Klicken Sie auf Aktivieren.

   OT Security aktiviert das System und zeigt das Fenster Dashboard > Risiko an.



Hinweis: Es dauert einige Minuten, bis das System Ihre Assets identifiziert hat. Möglicherweise müssen Sie die Seite aktualisieren, damit die Daten angezeigt werden.

## OT Security verwenden

Nach der Installation können Sie OT Security konfigurieren und verwenden.

### Überwachte Netzwerke konfigurieren

Konfigurieren Sie die Netzwerksegmente, die OT Security überwachen soll, und stellen Sie sicher, dass alle für Ihr Netzwerk relevanten Bereiche enthalten sind. Siehe Umgebungseinstellungen.

Hinweis: Entfernen Sie nicht benötigte überwachte Netzwerke. Sie können alle Assets ausblenden, die Sie aus diesen Netzwerken hinzugefügt haben. Weitere Informationen finden Sie unter Assets ausblenden.

### Ports überprüfen und konfigurieren

Sofern Sie dies noch nicht getan haben, können Sie die Ports für Verwaltung und aktive Abfragen trennen.

### Benutzer, Gruppen und Authentifizierungsserver konfigurieren

Legen Sie Ihre lokalen Benutzer und Benutzergruppen fest. Sie können externe Authentifizierungsserver konfigurieren oder SAML für ein einfacheres SSO-Login verwenden.

### Netzwerkdienste hinzufügen

Fügen Sie Ihre DNS- und NTP-Server hinzu. Sie können auch Syslog und E-Mail-Server so konfigurieren, dass alle kritischen Ereignisse abgerufen werden.

### Aktive Abfragen aktivieren

Aktive Abfragen stellen einen der Hauptvorteile von OT Security dar. Sie können darüber direkt auf Ihre Assets zugreifen, um möglichst genaue und zeitnahe Details und Einblick zu erhalten. Weitere Informationen finden Sie unter Aktive Abfragen.

Aktive Asset-Erfassung – Untersuchen und erfassen Sie proaktiv „stille“ Assets oder Assets, die durch passives Monitoring von Traffic nicht abgedeckt werden.

### Nessus-Scans erstellen

Konfigurieren Sie Nessus-Scans für IT-Geräte in Ihrem OT Security-Netzwerk. Tenable Nessus-Scans sind sicher und betreffen nur erfasste IT-Assets. Weitere Informationen finden Sie unter Nessus-Plugin-Scans erstellen.

### Sicherungen einrichten

Konfigurieren Sie regelmäßige Systemsicherungen und entscheiden Sie, ob Sie diese lokal speichern oder in einen Remote-Speicher exportieren möchten. Weitere Informationen finden Sie unter Application Data Backup and Restore.

### Updates abrufen

Achten Sie unbedingt darauf, Feed- und System-Updates zu überprüfen. Wenn Ihr System offline ist, sollten Sie regelmäßig ein manuelles Update durchführen. Weitere Informationen finden Sie unter Updates.

### Optimieren

Wenn OT Security eingerichtet ist und ausgeführt wird, sehen Sie sich die generierten Ereignisse an und optimieren Sie Ihre Richtlinien entsprechend den Anfoderungen Ihrer Umgebung.

### Integrieren

Integrieren Sie OT Security mit anderen Tenable-Produkten oder Drittanbieterdiensten. Weitere Informationen finden Sie unter Integrationen.

# OT Security Sensor installieren

Hinweis: Dieser Abschnitt beschreibt das Verfahren zur Konfiguration eines Sensors ab Version 3.14.

Die Installation des OT Security-Sensors umfasst die Kopplung der Sensoren mit der Industrial Core Platform (ICP). Um Sensoren mit der OT Security-ICP zu koppeln, verwenden Sie sowohl die ICP-Verwaltungskonsole als auch die Tenable Core-Benutzeroberfläche des Sensors.

Sie können entweder die automatische Genehmigung eingehender Kopplungsanfragen aktivieren oder die automatische Genehmigung deaktivieren und nur die manuelle Genehmigung für jede neue Kopplungsanfrage des Sensors zulassen.

## Bevor Sie beginnen

Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:

- Die Sensor-Hardware ist ordnungsgemäß installiert (siehe Sensor einrichten).
- Der Sensor ist mit Ihrem Netzwerk-Switch verbunden (siehe Sensor mit dem Netzwerk verbinden).
- Der Sensor hat seine eigene statische IPv4-Adresse (siehe Sensor-Setup-Assistenten aufrufen).
- Der Sensor ist mit der Tenable Core-Plattform verbunden und Sie verfügen über einen Benutzernamen und ein Passwort zum Einloggen bei der Core-Benutzeroberfläche. Weitere Informationen zur Verwendung der Benutzeroberfläche von Tenable Core finden Sie im Tenable Core + Tenable OT Security-Benutzerhandbuch.
- In der ICP-Konsole ist ein gültiges Zertifikat vorhanden (siehe Zertifikat).

Hinweis: Tenable empfiehlt, einen dedizierten ICP-Benutzer mit Administratorrolle für das Koppeln von Sensoren zuzuweisen, um Verbindungsunterbrechungen zu vermeiden (siehe Hinzufügen

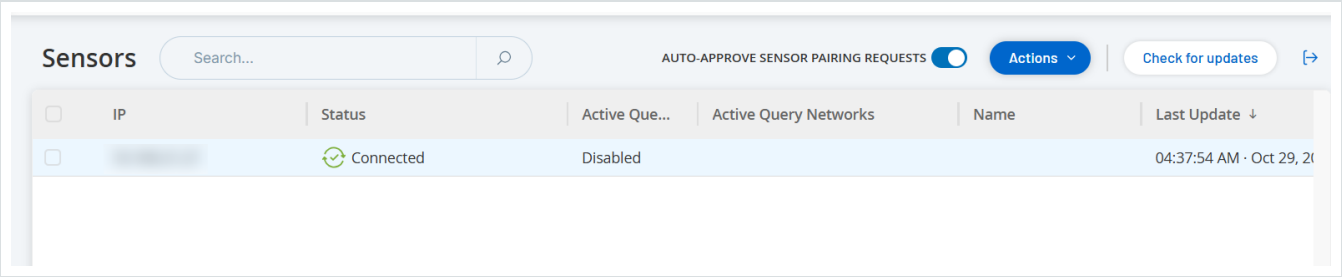
lokaler Benutzer). Sie können einen neuen Administratorbenutzer hinzufügen, um mehrere Sensoren zu koppeln.

Hinweis: Informationen zum Anwenden von Offline-Updates auf Ihren Tenable Core-Computer finden Sie unter Update Tenable Core Offline.

## Sensor koppeln

So koppeln Sie einen Sensor der Version 3.14 oder höher mit der ICP:

1. Navigieren Sie in der ICP-Verwaltungskonsole (Benutzeroberfläche) zum Bildschirm Einstellungen > Sensoren.

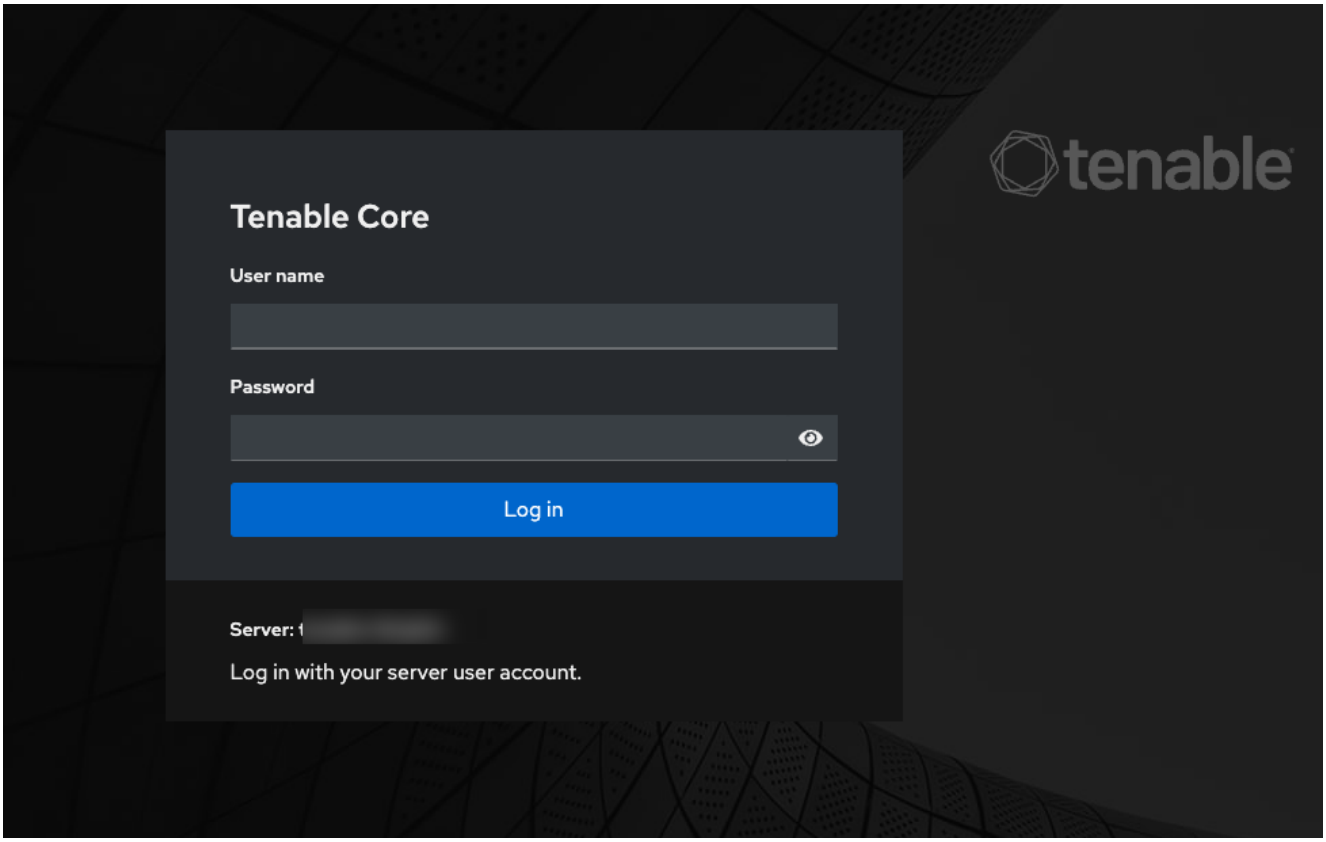



2. Um die automatische Genehmigung der Sensorkopplung zu aktivieren, stellen Sie sicher, dass der Umschalter Sensorkopplungsanforderungen automatisch genehmigen oben auf der Seite auf EIN gestellt ist. Wenn dies nicht der Fall ist, müssen alle Kopplungsanfragen manuell genehmigt werden.

3. Lassen Sie die ICP-Registerkarte geöffnet und öffnen Sie eine neue Registerkarte. Geben Sie <Sensor-IP>:8000 ein, um auf die Tenable Core-Benutzeroberfläche des Sensors zuzugreifen.

   Hinweis: Der Zugriff auf die Tenable Core-Benutzeroberfläche ist nur mit der neuesten Version von Chrome möglich.

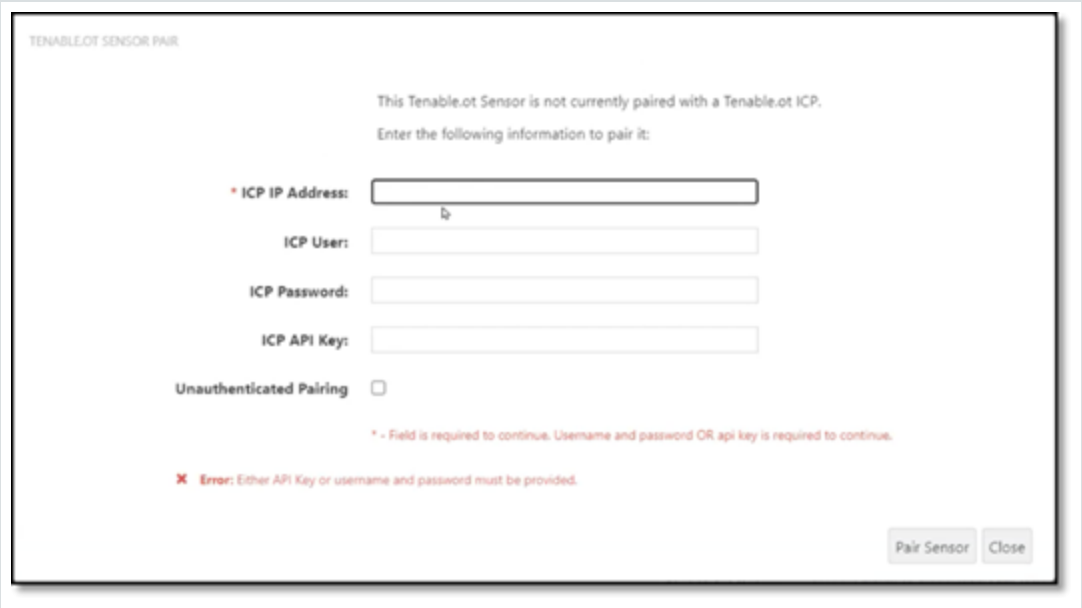
4. Geben Sie im Login-Fenster der Tenable Core-Konsole Ihren Benutzernamen und Ihr Passwort ein, aktivieren Sie das Kontrollkästchen Reuse my password for privileged tasks (Mein Passwort für privilegierte Aufgaben wiederverwenden) und klicken Sie auf Log In (Einloggen).




> Wichtig: Wenn Sie die Option Reuse my password for privileged tasks (Mein Passwort für privilegierte Aufgaben wiederverwenden) beim Login nicht aktivieren, können Sie den Sensor-Dienst nicht neu starten.

5. Klicken Sie in der Navigationsmenüleiste auf OT Security Sensor.

   Das Fenster OT Security Sensor Pair (Sensor Pair) wird angezeigt.




> Hinweis: Das Fenster **Tenable OT Security** Sensor Pair wird nur beim ersten Laden der Seite angezeigt. Wenn Sie das Fenster zu einem späteren Zeitpunkt öffnen möchten, klicken Sie auf die Schaltfläche im Abschnitt Pairing Info (Kopplungsinfo) der Tenable Core-Konsole.

6. Geben Sie im Feld ICP IP Address (ICP-IP-Adresse) die IPv4-Adresse der ICP ein, die mit diesem Sensor gekoppelt werden soll.

7. Um eine nicht authentifizierte (unverschlüsselte) Kopplung zu verwenden, wählen Sie die Option Unauthenticated Pairing (Nicht authentifizierte Kopplung) aus und fahren Sie mit Schritt 8 fort.

   > Hinweis: Sensoren, die die nicht authentifizierte Kopplung verwenden, können ihre Netzwerksegmente nur passiv scannen und können nicht von der ICP verwaltet werden, um aktive Abfragen zu senden.

8. Führen Sie einen der folgenden Schritte aus, um die Kopplung zu authentifizieren:

   - Geben Sie den ICP-Benutzernamen in das Feld ICP User (ICP-Benutzer) und das ICP-Passwort in das Feld ICP Password (ICP-Passwort) ein.

- Geben Sie im Feld ICP-API-Schlüssel (ICP API Key) einen API-Schlüssel für die ICP ein.

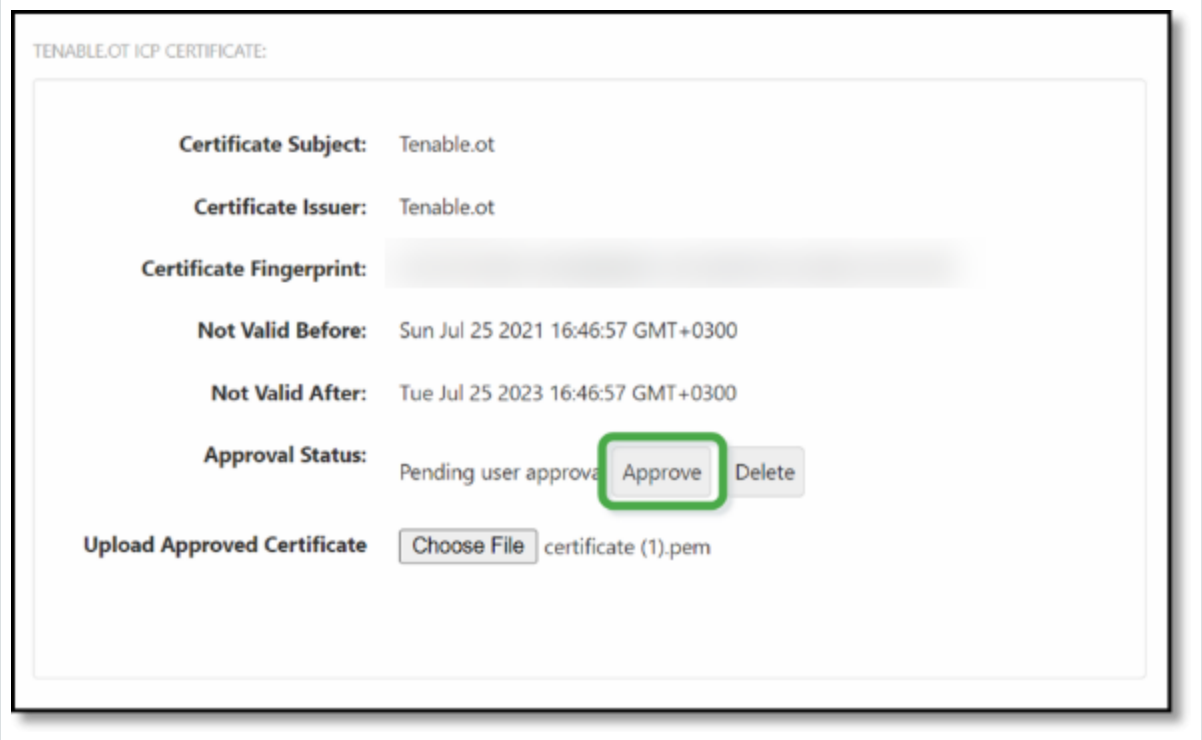
> Hinweis: Tenable empfiehlt, einen dedizierten ICP-Benutzer für das Koppeln von Sensoren zu erstellen, um Konnektivität während des Kopplungsvorgangs sicherzustellen (siehe Hinzufügen lokaler Benutzer).

> Hinweis: Die Authentifizierungsmethode mit Benutzername und Passwort bietet den Vorteil, dass die Zugangsdaten nicht ablaufen, im Gegensatz zu einem API-Schlüssel, der irgendwann abläuft.

9. Klicken Sie auf Pair Sensor (Sensor koppeln).

10. So nutzen Sie ein von der ICP angebotenes Zertifikat:

    a. Warten Sie in Tenable Core im Abschnitt Tenable ICP Certificate (Tenable ICP-Zertifikat) unter Approval Status (Genehmigungsstatus), bis die Zertifikatinformationen geladen wurden.



b. Klicken Sie auf Approve (Genehmigen), um das Zertifikat zu genehmigen.

c. Klicken Sie im Fenster Confirm Accept **Tenable OT Security** Server Certificate (Akzeptieren des Tenable.ot-Serverzertifikats bestätigen) auf Accept This Certificate (Dieses Zertifikat akzeptieren).

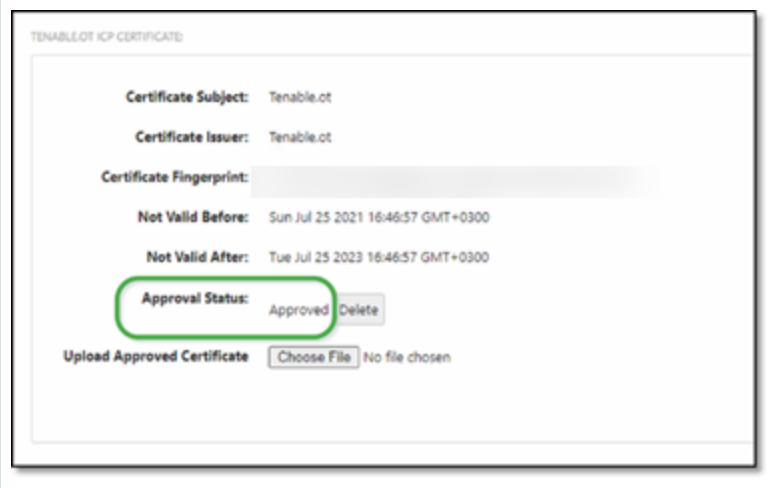
   Wenn Sie es vorziehen, ein Zertifikat manuell hochzuladen:

   a. Befolgen Sie in der **Tenable** ICP-Konsole das unter Generieren eines HTTPS-Zertifikats beschriebene Verfahren.

   b. Klicken Sie in Tenable Core im Abschnitt **Tenable** ICP Certificate (Tenable ICP-Zertifikat) unter Upload Approved Certificate (Genehmigtes Zertifikat hochladen) auf Choose File (Datei auswählen).

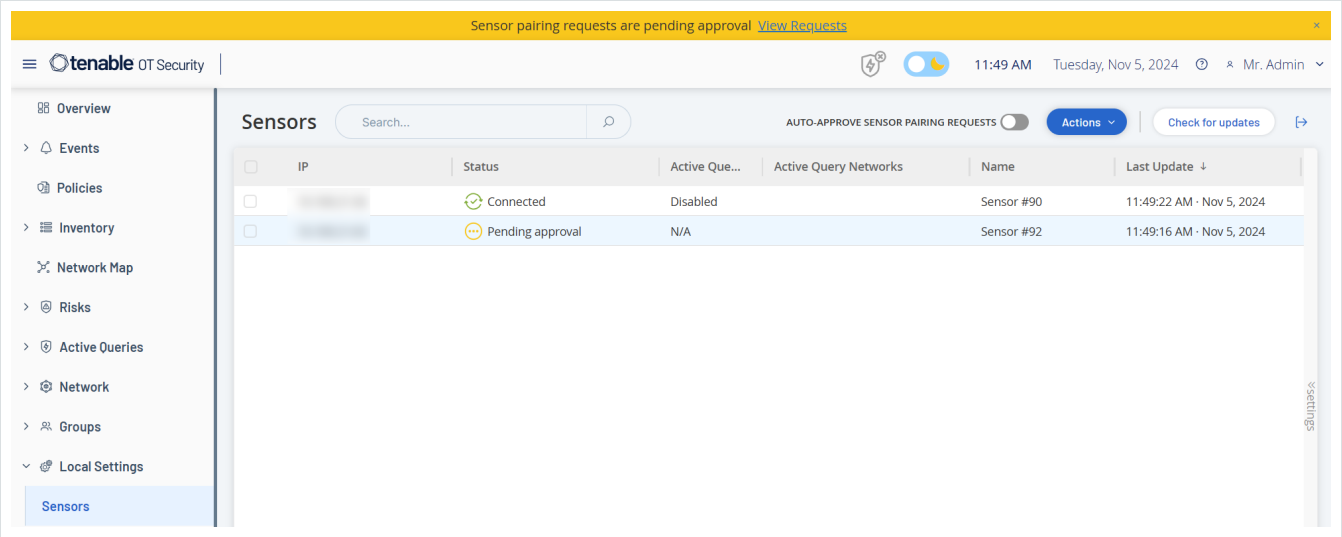
   c. Navigieren Sie zur hochzuladenden `.pem`-Zertifikatdatei.

      Sobald ein gültiges Zertifikat ordnungsgemäß geladen wurde, wird sein Approval State (Genehmigungsstatus) in der Tabelle OT Security-ICP Certificate (ICP-Zertifikat) als Approved (Genehmigt) angezeigt.

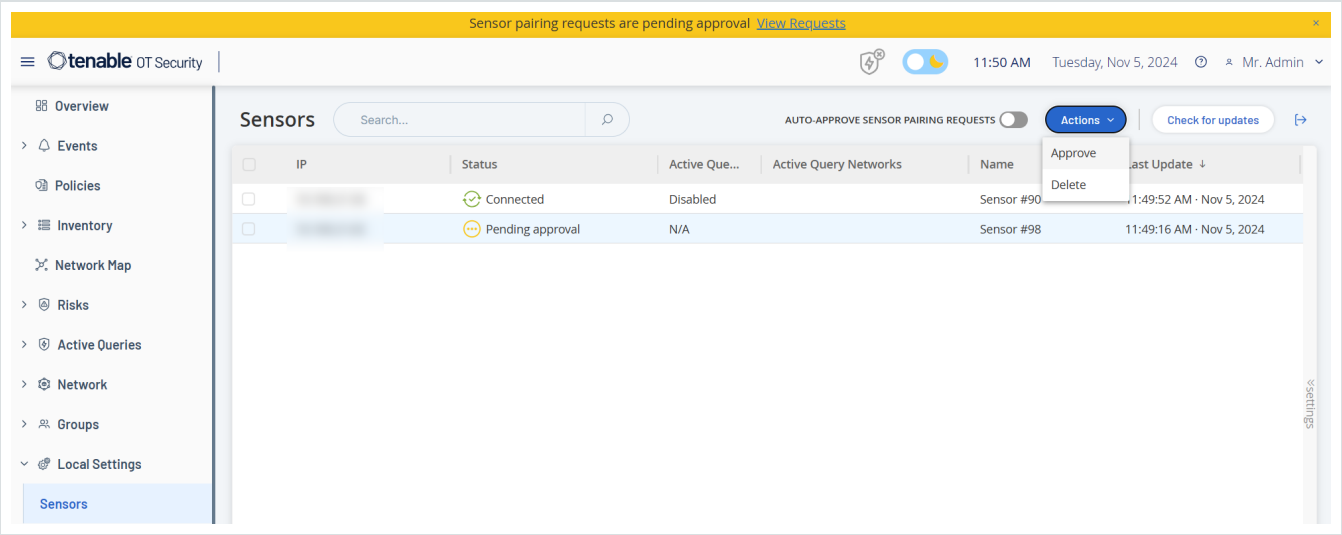



11. Navigieren Sie in der ICP-Benutzeroberfläche zu Lokale Einstellungen > Sensoren.

OT Security zeigt den neuen Sensor in der Tabelle angezeigt und der Status lautet Genehmigung ausstehend.




12. Klicken Sie auf die Zeile des Sensors, dann auf Aktionen (oder klicken Sie mit der rechten Maustaste auf die Zeile) und wählen Sie Genehmigen aus.




Der Status ändert sich in Verbunden, wodurch angezeigt wird, dass die Kopplung erfolgreich war. Andere mögliche Status sind:

- Verbunden (nicht authentifiziert) – Der Sensor ist im nicht authentifizierten Modus verbunden. Der Sensor kann nur eine passive Netzwerkerkennung durchführen.
- Angehalten – Der Sensor ist ordnungsgemäß verbunden, wurde jedoch angehalten.
- Getrennt – Der Sensor ist nicht verbunden. Bei einem authentifizierten Sensor kann dies auf einen Fehler bei der Kopplung zurückzuführen sein. Beispiele: Tunnelfehler und API-Problem.
- Verbunden (Tunnelfehler) – Die Kopplung war erfolgreich, aber die Kommunikation über den Tunnel funktioniert nicht. Überprüfen Sie die Konnektivität von Port 28304 vom Sensor zur ICP. Weitere Informationen finden Sie unter Überlegungen zur Firewall.

Sobald OT Security die Kopplung für einen authentifizierten Sensor abgeschlossen hat, können Sie aktive Abfragen zur Ausführung auf diesem Sensor konfigurieren. Siehe Aktive Abfragen verwalten.

> Hinweis: Sobald die Kopplung abgeschlossen ist, empfiehlt Tenable, den Sensor nur noch über die ICP-Seite zu verwalten und nicht mehr über die Tenable Core-Benutzeroberfläche.

## Sensor einrichten

Das konfigurierbare Modell kann auf einer DIN-Schiene installiert oder in einem standardmäßigen 19-Zoll-Rack montiert werden (unter Verwendung des Montagelaschen-Adapterkits).

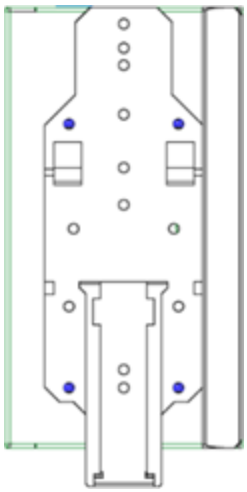
### Konfigurierbaren Sensor einrichten

Sie können den konfigurierbaren Sensor entweder auf einer DIN-Schiene oder in einem standardmäßigen 19-Zoll-Rack montieren (unter Verwendung des Montagelaschen-Adapterkits).

#### Montage auf DIN-Schiene

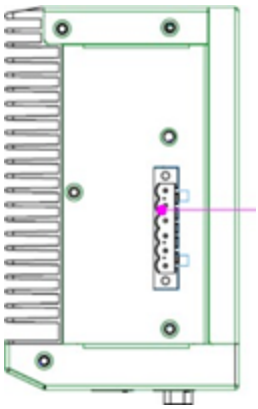
So montieren Sie den konfigurierbaren OT Security Sensor auf einer Standard-DIN-Schiene:

1. Verwenden Sie die Halterung auf der Rückseite des Sensors, um den Sensor auf einer DIN-Schiene zu montieren.



2. Schließen Sie die Stromversorgung mit einer der folgenden Methoden an:

    - Gleichstromversorgung – Schließen Sie das Gleichstromkabel an den Sensor an, indem Sie den 6-poligen 12-36-V-DC-Phoenix-Contact-Stecker in die Seite des Sensorgeräts stecken und die integrierten Schrauben oben und unten am Stecker festziehen. Schließen Sie dann das andere Ende des Kabels an eine Gleichstromquelle an.



    - Wechselstromversorgung – Schließen Sie die Wechselstromversorgung an den Sensor an, indem Sie den 6-poligen 12-36-V-DC-Phoenix-Contact-Stecker in die Seite des Sensorgeräts stecken und die integrierten Schrauben oben und unten am Stecker

festziehen.

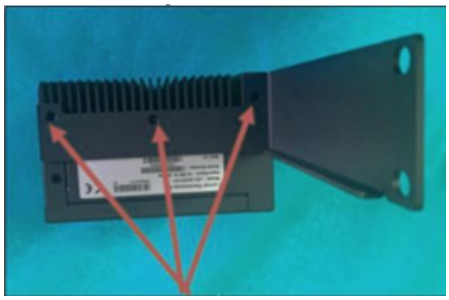
Stecken Sie dann das eine Ende des Wechselstromkabels (mitgeliefert) in das Netzteil und das andere Ende in eine Netzsteckdose.

## Rack-Montage (für konfigurierbares Modell)

Ein konfigurierbarer Sensor kann mit den mitgelieferten „Montagelaschen“ an einem Montage-Rack befestigt werden.

So montieren Sie den konfigurierbaren Sensor in einem Standard-Rack (19 Zoll):

1. Bereiten Sie das Gerät für die Rack-Montage vor:
    a. Entfernen Sie drei Schrauben auf jeder Seite des Geräts.
    b. Befestigen Sie die Montagelaschen mit neuen Schrauben (mitgeliefert) auf beiden Seiten des Geräts.



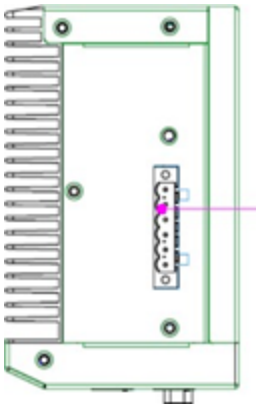
2. Setzen Sie die Servereinheit in einen freien 1-HE-Steckplatz im Rack ein.

> Hinweis:
> - Stellen Sie sicher, dass das Rack geerdet ist.
> - Stellen Sie sicher, dass der Lufteinlass des Lüfters (in der Rückwand) und die Belüftungsöffnungen (an der Oberseite) nicht blockiert sind.

3. Befestigen Sie das Gerät am Rack, indem Sie die „Montagelaschen“ mit den Montageschrauben (mitgeliefert) am Rack-Rahmen befestigen.

4. Schließen Sie die Stromversorgung mit einer der folgenden Methoden an:

   - Gleichstromversorgung – Schließen Sie das Gleichstromkabel an den Sensor an, indem Sie den 6-poligen 12-36-V-DC-Phoenix-Contact-Stecker in die Seite des Sensorgeräts stecken und die integrierten Schrauben oben und unten am Stecker festziehen. Schließen Sie dann das andere Ende des Kabels an eine Gleichstromquelle an.



   - Wechselstromversorgung – Schließen Sie die Wechselstromversorgung an den Sensor an, indem Sie den 6-poligen 12-36-V-DC-Phoenix-Contact-Stecker in die Seite des Sensorgeräts stecken und die integrierten Schrauben oben und unten am Stecker festziehen.

Stecken Sie dann das eine Ende des Wechselstromkabels (mitgeliefert) in das Netzteil und das andere Ende in eine Netzsteckdose.

## Sensor mit dem Netzwerk verbinden

Der OT Security Sensor wird verwendet, um Netzwerk-Traffic zu erfassen und an die OT Security Appliance weiterzuleiten. Um eine Netzwerküberwachung durchzuführen, schließen Sie das Gerät an einen Spiegelport am Netzwerk-Switch an, der mit den relevanten Controllern/SPS verbunden ist.

Um den Sensor zu verwalten, verbinden Sie das Gerät mit einem Netzwerk. Hierbei kann es sich um ein anderes Netzwerk handeln als dasjenige, das für die Netzwerküberwachung verwendet wird.

### So verbinden Sie den konfigurierbaren OT Security-Sensor mit dem Netzwerk:

1. Schließen Sie am OT Security Sensor das Ethernet-Kabel (mitgeliefert) an Port 1 an.
2. Schließen Sie das Kabel an einen regulären Anschluss am Netzwerk-Switch an.
3. Schließen Sie am Gerät ein weiteres Ethernet-Kabel (mitgeliefert) an Port 3 an.
4. Schließen Sie das Kabel an einen Spiegelport am Netzwerk-Switch an.

## Sensor-Setup-Assistenten aufrufen

So loggen Sie sich bei der Verwaltungskonsole ein:

1. Führen Sie einen der folgenden Schritte aus:

   - Verbinden Sie die Workstation der Verwaltungskonsole (z. B. PC und Laptop) über das Ethernet-Kabel direkt mit Port 1 des OT Security Sensor.
   - Verbinden Sie die Workstation der Verwaltungskonsole mit dem Netzwerk-Switch.

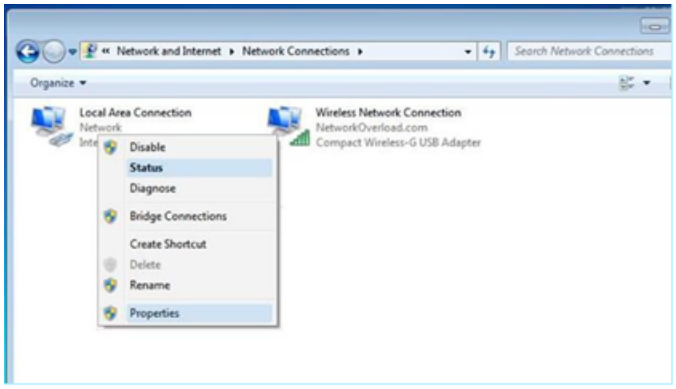
2. Stellen Sie sicher, dass die Workstation der Verwaltungskonsole Teil desselben Subnetzes ist wie der OT Security Sensor (d. h. 192.168.1.5) oder an das Gerät umgeleitet werden kann.

3. Verwenden Sie das folgende Verfahren, um eine statische IP-Adresse einzurichten (Sie müssen eine statische IP einrichten, um eine Verbindung zum OT Security Sensor herzustellen):

   a. Gehen Sie zu Netzwerk und Internet > Netzwerk- und Freigabecenter > Adaptereinstellungen ändern.

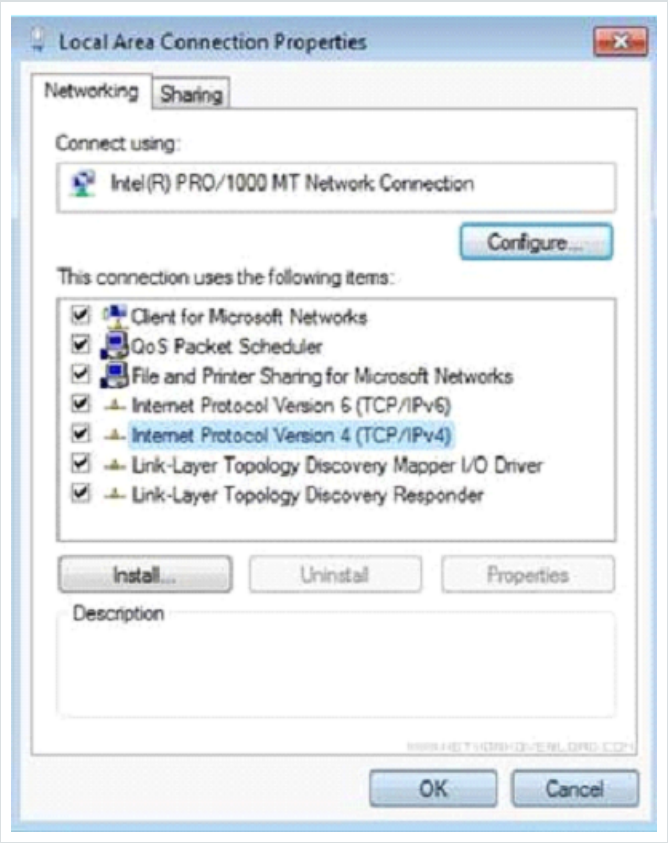
   > Hinweis: Die Navigation kann bei den verschiedenen Windows-Versionen leicht variieren.

   Das Fenster Netzwerkverbindungen wird angezeigt.



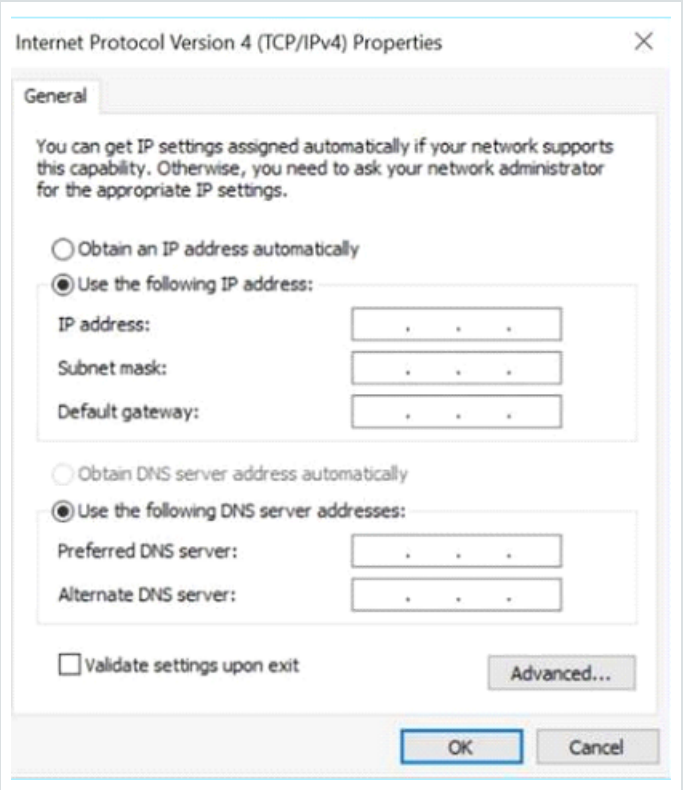

   b. Klicken Sie mit der rechten Maustaste auf LAN-Verbindung und wählen Sie Eigenschaften aus.

Das Fenster LAN-Verbindung wird angezeigt.




c. Wählen Sie Internetprotokoll, Version 4 (TCP/IPv4) und klicken Sie auf Eigenschaften.

Das Fenster mit den Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4) wird angezeigt.




d. Wählen Sie Folgende IP-Adresse verwenden aus.

e. Geben Sie in das Feld IP-Adresse 192.168.1.10 ein.

f. Geben Sie in das Feld Subnetzmaske 255.255.255.0 ein.

g. Klicken Sie auf OK.

   OT Security wendet die neuen Einstellungen an.

4. Navigieren Sie im Chrome-Browser zu https://192.168.1.5:8000.

   > Hinweis: Auf die Benutzeroberfläche kann nur über einen Chrome-Browser zugegriffen werden. Verwenden Sie die neueste Version von Chrome.

5. Koppeln Sie den Sensor.

## Konsolenverbindung herstellen und Ersteinrichtung vornehmen

In diesem Thema wird beschrieben, wie Sie eine lokale serielle Konsole mit Ihren OT Security-Appliances (ICP und Sensoren) verbinden. Verwenden Sie diese Verbindungsmethode für die Erstkonfiguration der IP-Adresse, die Fehlerbehebung im Netzwerk oder die Wiederherstellung des Zugriffs, wenn die Management-IP nicht erreichbar ist.

## Bevor Sie beginnen

Sie benötigen die folgende Software und Hardware:

Software

- Terminalemulator: Ein Dienstprogramm wie PuTTY, Tera Term, Serial oder Minicom.
- Treiber: Stellen Sie sicher, dass Sie die Treiber für Ihr spezifisches USB-Kabel oder Ihren Adapter (z. B. FTDI oder PL2303) installieren.

### Hardware- und Verkabelungsoptionen

Identifizieren Sie Ihren Appliance-Typ, um die richtige Verkabelungsmethode auszuwählen:

- **Tenable OT Security** oder **Tenable** ICP-Konsole (Industrial Core Platform)
    - Porttyp: RJ-45-Konsole.
    - Empfohlenes Kabel: USB-zu-RJ45-Konsolenkabel.

> Hinweis: Ein hellblaues Cisco-Konsolenkabel ist in der Regel im Lieferumfang der Appliance enthalten. Dies ist ein Standardkabel (ca. 10 USD), das häufig für Netzwerk-Switches verwendet wird.

- **Tenable Sensoren:** Sensoren gibt es in zwei Hardwarevariationen. Überprüfen Sie die physischen Ports auf Ihrem Gerät:
    - RJ-45-Konsolenport: Verwenden Sie ein USB-zu-RJ45-Konsolenkabel.
    - DB9-Port (seriell): Verwenden Sie ein serielles USB-zu-DB9-Kabel.

Tipp: Tenable empfiehlt die Verwendung von direkten USB-zu-DB9-Buchsenkabeln (einteilig) anstelle von mehrteiligen Adaptern, um Konnektivitätsprobleme zu minimieren.

Alternative Methode (ältere Adapter)

Wenn Sie anstelle eines direkten USB-zu-Konsole-Kabels einen handelsüblichen Seriell-zu-USB-Adapter verwenden, müssen Sie einen Nullmodem-Adapter oder -Koppler in die Verbindung einbauen.

Tipp: Viele Verbindungsfehler sind darauf zurückzuführen, dass serielle Standardadapter die Sende- oder Empfangsstifte ohne Nullmodem nicht korrekt kreuzen.

## Physische Verbindung

1. Verbinden Sie das USB-Ende des Kabels mit Ihrer Workstation.
2. Verbinden Sie das andere Ende (RJ-45 oder DB9) mit der Appliance.
    - Beschriftete Ports: Suchen Sie den Port mit der Konsolen-Beschriftung oder mit einem Monitor- oder IOIOI-Symbol.
    - Unbeschriftete Ports: Falls die Anschlüsse nicht beschriftet sind, schließen Sie das Gerät an den einzelnen RJ-45-Anschluss links neben den USB-Anschlüssen an.
3. Vergewissern Sie sich, dass das Kabel fest sitzt.

## COM-Port identifizieren (Windows)

Sie müssen den Kommunikationsport (COM) identifizieren, den Windows Ihrem Kabel zugewiesen hat.

1. Klicken Sie auf Ihrem Windows-Computer mit der rechten Maustaste auf Start und wählen Sie Device Manager aus.

    Das Fenster Device Manager wird angezeigt.

2. Erweitern Sie Ports (COM & LPT).
3. Suchen Sie Ihr Gerät (z. B. Serieller USB-Port) und notieren Sie sich die Nummer (z. B. COM3).

## Terminal konfigurieren (PuTTY)

Starten Sie Ihren Terminalemulator (z. B. PuTTY) und konfigurieren Sie die Sitzung mit den folgenden Tenable TTY-Einstellungen.

Gehen Sie in PuTTY zu Connection > Serial und konfigurieren Sie die folgenden Einstellungen:

| Einstellung | Wert |
|---|---|
| Connection Type | Serial |
| Serial Line: | Ihr COM-Port (z. B. COM3) |
| Speed (Baud) | 115200 |
| Datenbits | 8 |
| Stoppbits | 1 |
| Parität | Keine |
| Flow Control | Keine<br><br>Hinweis: Stellen Sie sicher, dass „Flow Control“ nicht auf `XON/XOFF` festgelegt ist. |

Tipp: Speichern Sie diese Einstellungen auf der Seite Sessions für die zukünftige Verwendung als „Tenable OT Console“.

## Verbindung herstellen

1. Klicken Sie auf Open, um die Sitzung zu starten.
2. Wenn das Terminalfenster angezeigt wird, drücken Sie zweimal die Eingabetaste, um die Konsole zu aktivieren.
3. Vergewissern Sie sich, dass die folgende Eingabeaufforderung angezeigt wird:

```
################################################################################

  This system is restricted to authorized users only. Individuals attempting
  unauthorized access will be prosecuted. Continued access indicates
  your acceptance of this notice.

################################################################################
```

4. Loggen Sie sich an der Eingabeaufforderung ein.

## Anfängliche Netzwerkkonfiguration

Die Verwaltungsschnittstelle erfordert eine statische IP. DHCP wird nicht unterstützt.

1. Führen Sie das Netzwerk-Manager-Tool aus:

```
sudo nmtui
```

2. Wählen Sie Edit a connection (Verbindung bearbeiten) aus.
3. Wählen Sie die Verwaltungsschnittstelle aus (in der Regel die erste Schnittstelle, z. B. nic0 oder eth0).

> Achtung: Konfigurieren Sie nicht die zweite Schnittstelle (oft nic1). Dies ist der SPAN- oder Spiegelport für passives Monitoring und erfordert keine IP-Adresse.

4. Legen Sie IPv4 Configuration auf `<Manual>` fest.

5. Wählen Sie `<Show>` und geben Sie Folgendes ein:
    - Adresses: Ihre statische IP oder Ihr CIDR (z. B. 192.168.1.50/24).
    - Gateway: Ihre Gateway-IP-Adresse.
    - DNS Servers: Ihre DNS-IP-Adressen.
6. Navigieren Sie nach unten und wählen Sie `<OK>`, um zu speichern.
7. Wählen Sie `Quit`.

### Benutzeroberfläche aufrufen

Gehen Sie nach der Konfiguration der IP wie folgt vor:

1. Schließen Sie ein Netzwerkkabel vom Verwaltungsport an den Netzwerk-Switch an.
2. Öffnen Sie einen Browser und navigieren Sie über Port 8000 zur IP-Adresse: `https://<IHRE_STATISCHE_IP> :8000`

    Die Login-Seite von OT Security wird angezeigt. Sie können jetzt mit dem Setup-Assistenten fortfahren. Siehe Einstellungen von OT Security mit dem Setup-Assistenten konfigurieren.

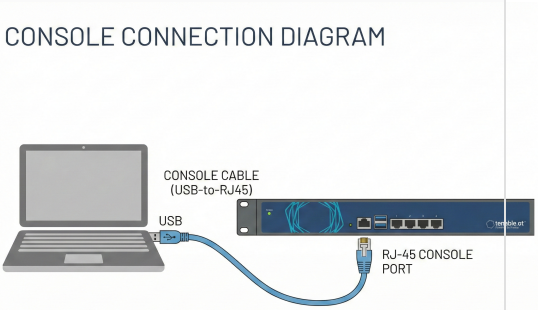
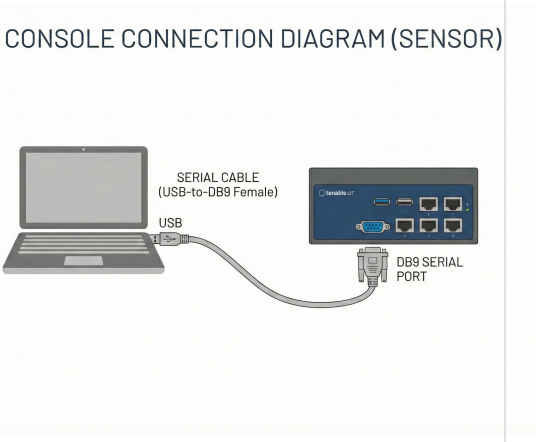
### Siehe auch

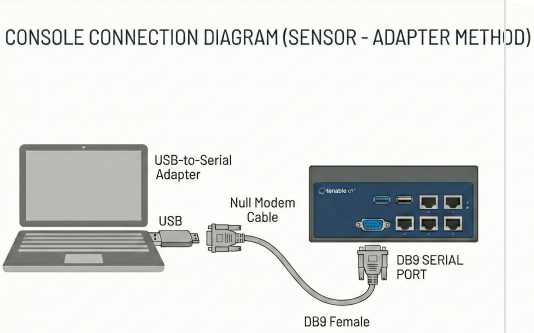
Konsolenkabel zum Anschließen an OT Security Sensor

## Konsolenkabel zum Anschließen an OT Security Sensor

Sie können die folgenden Kabel verwenden, um Ihren Laptop mit OT Security Sensor zu verbinden:

| Kabel | Bild | Grafik zur Konsolenverbindung |
|---|---|---|

| | | |
|---|---|---|
| Konsolenkabel (USB-zu-RJ45) |  |   |
| Serielles Kabel (USB-zu-DB9-Buchsenkabel) |  |   |

| | | |
|---|---|---|
| Nullmodemkabel |  |  |

## Sicherung mithilfe der CLI wiederherstellen

Sie können OT Security mithilfe der CLI oder über die Tenable Core-Oberfläche wiederherstellen. Weitere Informationen zur Wiederherstellung von Sicherungen über die Tenable Core-Benutzeroberfläche finden Sie unter Restore a Backup im Tenable Core + Tenable OT Security User Guide. Führen Sie für eine Wiederherstellung mithilfe der CLI die folgenden Schritte aus.

> Hinweis: Sie können nur Sicherungen wiederherstellen, die mit dem Sicherungsdienstprogramm von Tenable Core erstellt wurden. Ältere Sicherungen von OT Security vor Version 3.18 sind nicht kompatibel. Wenn Sie eine Sicherung wiederherstellen möchten, die mit einer älteren Version von OT Security (vor Version 3.18) erstellt wurde, wenden Sie sich an den Support, um die benötigten Anweisungen und Befehle zu erhalten.

### Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie über die wiederherzustellenden `TAR`-Sicherungsdateien verfügen.

> Hinweis: Sie können die OT Security-Sicherungsdateien von der Seite Backup/Restore (Sichern/Wiederherstellen) in Tenable Core herunterladen. Weitere Informationen finden Sie unter Restore a Backup im Tenable Core + Tenable OT Security User Guide.
> Beispiel für eine OT Security-Sicherungsdatei: `tenable-ot-tenable-s2cc78kg-2024-03-21T135648.tar`.

So stellen Sie Ihre OT Security-Sicherung mithilfe der CLI wieder her:

1. Führen Sie einen der folgenden Schritte aus, um auf das ICP-System zuzugreifen:
   - Loggen Sie sich bei Tenable Core ein und rufen Sie das Terminal auf.
   - Loggen Sie sich mit SSH ein.
2. Führen Sie im Terminal den folgenden Befehl aus:

```
sudo systemctl start tenablecore.restorelocal@$(systemd-escape /home/admin/my-tc-ot-backup.tar)
```

Dabei gilt:

- `/home/admin/my-tc-ot-backup.tar` ist der Speicherort der Sicherungsdateien.

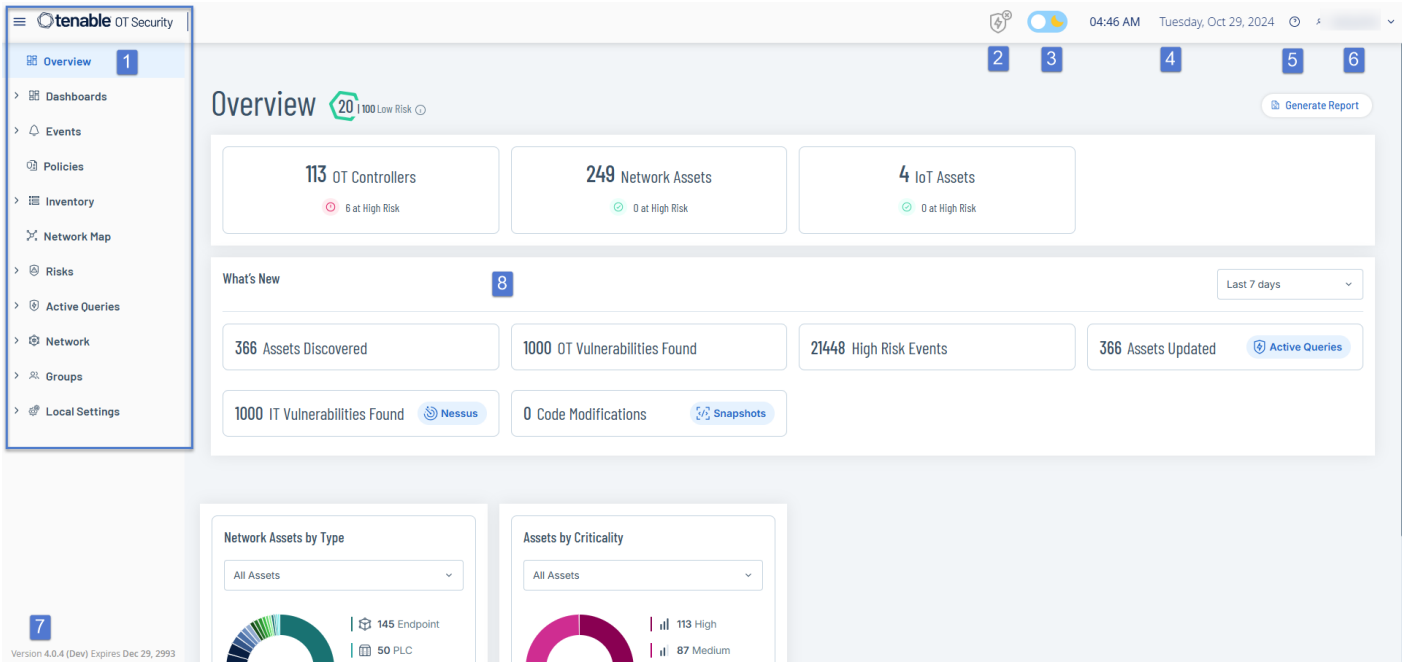
> Hinweis: Der Vorgang benötigt viel Zeit, da die Sicherung wiederhergestellt wird, bevor der Befehl abgeschlossen ist. Sie können den Wiederherstellungsfortschritt unter Backup/Restore (Sichern/Wiederherstellen) > Backup/Restore Logs (Protokolle sichern/wiederherstellen) > Restore Logs (Protokolle wiederherstellen) in der Benutzeroberfläche von Tenable Core einsehen oder den folgenden Befehl ausführen:
>
> `journalctl -xf tenablecore.restorelocal@$(systemd-escape /home/admin/my-tc-ot-backup.tar)`
>
> Dabei gilt: `/home/admin/my-tc-ot-backup.tar` ist der Speicherort der Sicherungsdateien.

OT Security wird wiederhergestellt und Sie können auf die Anwendung zugreifen. Um zu überprüfen, ob OT Security ausgeführt wird, loggen Sie sich mit Ihrem Browser über Port 443 (HTTPS) bei der OT Security-Benutzeroberfläche ein.

# Elemente in der Benutzeroberfläche der Verwaltungskonsole

Die Benutzeroberfläche der Verwaltungskonsole bietet einfachen Zugriff auf wichtige Daten in Bezug auf Asset-Management, Netzwerkaktivität und Sicherheitsereignisse, die von OT Security erfasst werden. Sie können die Benutzeroberfläche verwenden, um die Funktionen der OT Security-Plattform Ihren Anforderungen entsprechend zu konfigurieren.

## Hauptelemente der Benutzeroberfläche




In der folgenden Tabelle werden die Hauptelemente der Benutzeroberfläche beschrieben.

| Nr. | Element der Benutzeroberfläche | Beschreibung |
|---|---|---|
| 1 | Hauptnavigation | Hauptnavigationsmenü. Klicken Sie auf das Symbol ☰, um das Hauptnavigationsmenü anzuzeigen oder auszublenden. |
| 2 | Aktive Abfragen | Gibt an, ob die Funktion Aktive Abfragen aktiviert |

| | | |
|---|---|---|
| | | oder deaktiviert ist. |
| 3 | Dunkler Modus/Tageslichtmodus | Ändert das Farbschema der Anzeige in den dunklen Modus oder den Tageslichtmodus. |
| 4 | Aktuelle(s) Datum und Uhrzeit | Zeigt das aktuelle Datum und die Uhrzeit an, wie sie im System registriert sind. |
| 5 | Ressourcen-Center | Ressourcen-Center von OT Security |
| 6 | Aktueller Benutzername | Zeigt den Namen des Benutzers an, der derzeit beim System eingeloggt ist. Klicken Sie auf den Abwärtspfeil, um die Menüoptionen anzuzeigen: Info (zeigt Informationen zur Software an) und Ausloggen.<br><br>Nachdem Sie OT Security aktiviert haben, können Sie Ihre Tenable-Kunden-ID in der Ansicht Info einsehen. Diese Kunden-ID ist erforderlich, wenn Sie sich an den technischen Support oder das Customer Success-Team wenden. |
| 7 | Lizenzinformationen | Zeigt die Softwareversion von OT Security und das Ablaufdatum der Lizenz an. |
| 8 | Hauptbildschirm | Zeigt den Bildschirm an, der Sie in der Hauptnavigation ausgewählt haben. |

## Dunklen Modus aktivieren oder deaktivieren

Sie können das Farbschema Dunkler Modus in allen Bildschirmen verwenden, indem Sie den Umschalter für den dunklen Modus auf „Ein“ stellen.

So aktivieren oder deaktivieren Sie den dunklen Modus:

1. Klicken Sie oben im Fenster auf den Umschalter (Dunkler Modus).

   OT Security wendet die ausgewählte Einstellung auf alle Bildschirme an.

2. Um die Einstellung für den Tageslichtmodus wiederherzustellen, klicken Sie auf den Umschalter (Tageslichtmodus).

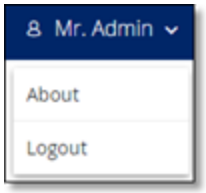
## Aktuelle Softwareversion überprüfen

Sie können die Version Ihrer Software über das Benutzerprofilsymbol in der oberen rechten Ecke der Kopfleiste überprüfen.

So zeigen Sie die aktuelle Softwareversion an:

1. Klicken Sie in der Hauptkopfleiste auf das Symbol in der oberen rechten Ecke.

   OT Security zeigt das Benutzermenü an.




2. Klicken Sie auf Info.

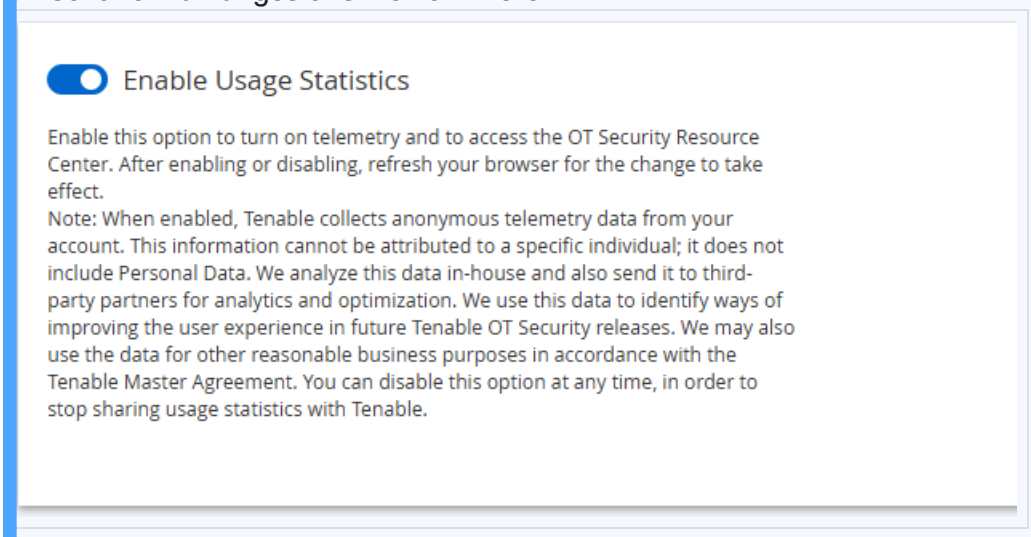
OT Security zeigt die aktuelle Softwareversion an.


## Auf das Ressourcen-Center zugreifen

Das Ressourcen-Center zeigt eine Liste mit Informationsressourcen an, einschließlich Produktankündigungen, Tenable-Blog-Beiträgen und Benutzerhandbüchern.

> Hinweis: Für den Zugriff auf das Ressourcen-Center ist eine Internetverbindung erforderlich. Das Ressourcen-Center ⓘ ist standardmäßig deaktiviert. Zum Aktivieren des Ressourcen-Center gehen Sie zu Einstellungen> Systemkonfiguration > Gerät und aktivieren den

UmschalterNutzungsstatistiken aktivieren.




So greifen Sie auf das Ressourcen-Center zu:

1. Klicken Sie in der oberen rechten Ecke auf die Schaltfläche ⓘ.

   Das Menü Ressourcen-Center wird angezeigt.

2. Klicken Sie auf einen Ressourcen-Link, um zu dieser Ressource zu navigieren. Die folgenden Ressourcen sind verfügbar:

   - Suche in der OT Security-Wissensdatenbank
   - Neue Funktions-Updates

## In OT Security navigieren

Sie können über die linke Navigationsleiste auf die folgenden Hauptseiten zugreifen:

- Übersicht – Zeigt Widgets an, die einen allgemeinen Überblick über das Inventar und die Sicherheitslage Ihres Netzwerks geben. Siehe OT Security – Übersicht.

- Ereignisse – Zeigt alle Ereignisse an, die als Folge von Richtlinienverletzungen aufgetreten sind. Die Seite Alle Ereignisse enthält separate Bildschirme für jeden spezifischen Ereignistyp. Beispiel: Konfigurationsereignisse, SCADA-Ereignisse, Netzwerkbedrohungen oder Netzwerkereignisse. Siehe Ereignisse.

- Richtlinien – Hier können Sie Richtlinien im System anzeigen, bearbeiten und aktivieren. Siehe Richtlinien.

- Inventar – Zeigt ein Inventar aller erfassten Assets an und ermöglicht so ein umfassendes Asset-Management, die Statusüberwachung der einzelnen Assets sowie die Anzeige der damit verbundenen Ereignisse. Die Seite Alle Assets enthält separate Ansichten für jeden spezifischen Asset-Typ (Controller und Module, Netzwerk-Assets und IoT). Siehe Inventar.

- Netzwerkübersicht – Zeigt eine visuelle Darstellung der Netzwerk-Assets und ihrer Verbindungen. Siehe Netzwerkübersicht.

- Risiken – Zeigt alle von OT Security erkannten Netzwerkbedrohungen an, z. B. CVEs, anfällige Protokolle, anfällige offene Ports und mehr, und nennt empfohlene Behebungsmaßnahmen. Siehe Schwachstellen.

- Aktive Abfragen – Ermöglicht es Ihnen, aktive Abfragen zu konfigurieren und zu aktivieren. Siehe Aktive Abfragen verwalten.

- Netzwerk – Bietet einen umfassenden Überblick über den Netzwerk-Traffic, indem Daten zu Konversationen angezeigt werden, die im Laufe der Zeit zwischen Assets im Netzwerk stattgefunden haben. Siehe Netzwerk.

  OT Security zeigt die Netzwerkinformationen in drei separaten Fenstern an:

  - Netzwerk – Zusammenfassung – Zeigt eine Übersicht über den Netzwerk-Traffic.

  - Paketerfassungen – Zeigt vollständige Paketerfassungen des Netzwerk-Traffic an.

- Konversationen – Zeigt eine Liste aller im Netzwerk erkannten Konversationen mit Details zum Zeitpunkt des Auftretens und den beteiligten Assets an.

- Gruppen – Hier können Sie Gruppen anzeigen, erstellen und bearbeiten, die bei der Richtlinienkonfiguration verwendet werden. Siehe Gruppen.
- Lokale Einstellungen – Hier können Sie die Systemeinstellungen anzeigen und konfigurieren. Siehe Einstellungen.

## Tabellen anpassen

Auf OT Security-Seiten werden Daten in einem Tabellenformat mit einer Liste für jedes Element angezeigt. Diese Tabellen verfügen über standardisierte Anpassungsfunktionen, die Ihnen einen einfachen Zugriff auf die relevanten Informationen ermöglichen.

Wichtig: In OT Security Version 4.0 und höher wurden mehrere Änderungen an der Benutzeroberfläche vorgenommen, aber nicht alle Seiten in der Anwendung wurden aktualisiert. In dieser Version wird nur auf den Seiten unter Inventar und Feststellungen von Schwachstellen die verbesserte Methode zum Anpassen, Filtern, Sortieren und Suchen verwendet. Diese Schritte sind in Abschnitten dokumentiert, in deren Überschriften explizit Version 4.0 angegeben ist. Beispiel: Spaltenanzeige anpassen in OT Security 4.0 und höher.

Hinweis: Die hier gezeigten Beispiele beziehen sich auf die Seiten Alle Ereignisse und Alle Assets, aber ähnliche Funktionen sind für die meisten Seiten verfügbar. Sie können jederzeit zu den standardmäßigen Anzeigeeinstellungen zurückkehren, indem Sie auf Einstellungen > Tabelle auf Standard zurücksetzen klicken. Für OT Security 4.0 und höher klicken Sie auf Angezeigte Spalten > Auf Standard zurücksetzen.

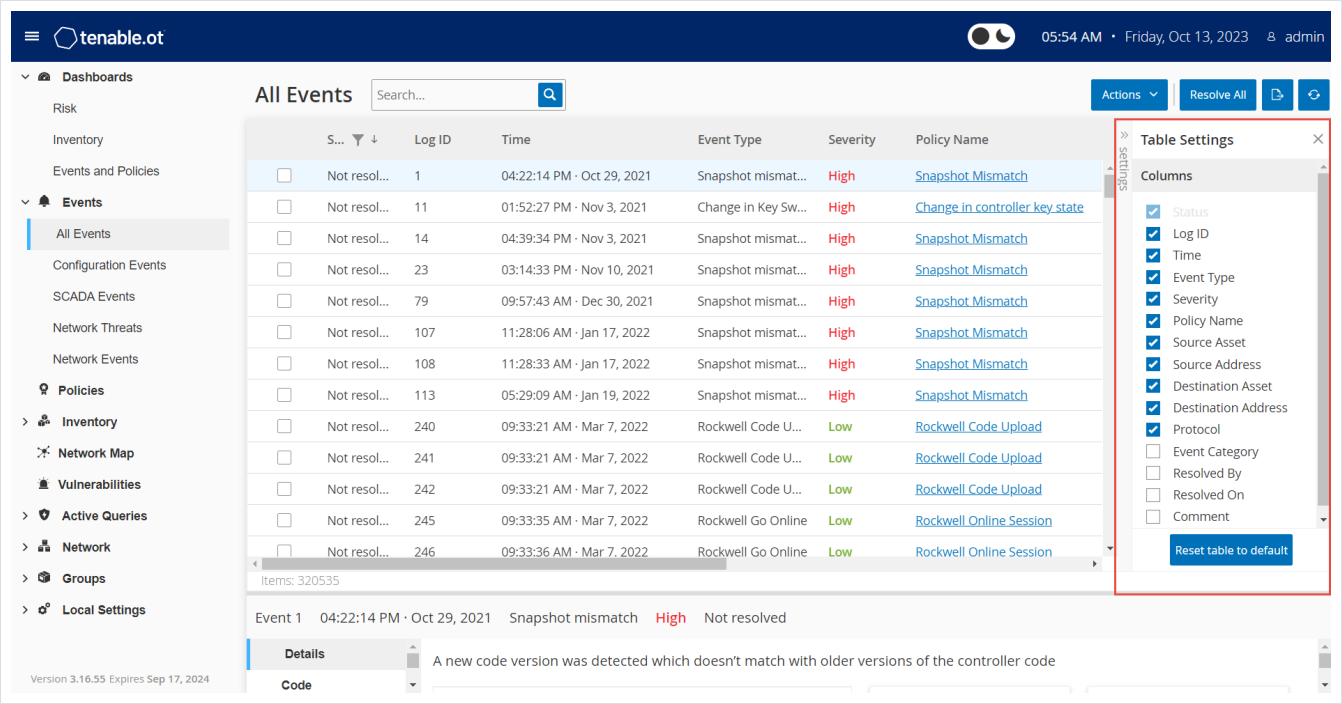
### Spaltenanzeige anpassen (3.19 und früher)

Sie können anpassen, welche Spalten angezeigt werden und wie sie organisiert sind.

So geben Sie an, welche Spalten angezeigt werden:

1. Klicken Sie rechts neben der Tabelle auf Einstellungen.

   Der Bereich Tabelleneinstellungen wird mit dem Abschnitt Spalten angezeigt.




2. Aktivieren Sie im Abschnitt Spalten das Kontrollkästchen neben den Spalten, die angezeigt werden sollen.

3. Deaktivieren Sie das Kontrollkästchen neben den Spalten, die Sie ausblenden möchten.

   OT Security zeigt nur die ausgewählten Spalten an.

4. Klicken Sie auf das x (oder auf die Registerkarte Einstellungen), um das Fenster Tabelleneinstellungen zu schließen.

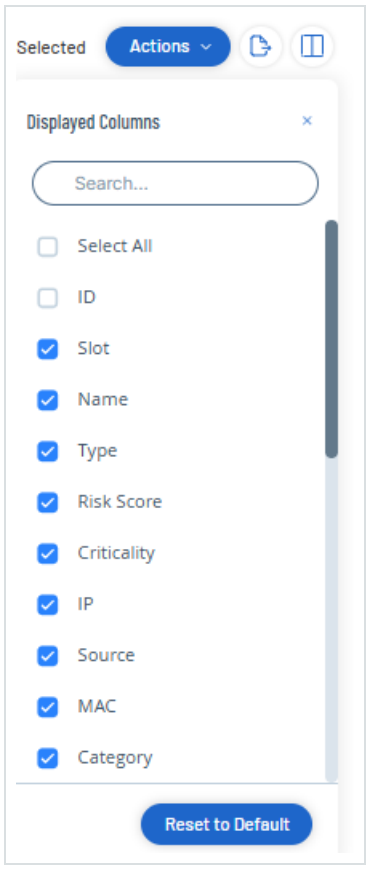
So passen Sie die Anzeigereihenfolge der Spalten an:

1. Klicken Sie auf eine Spaltenüberschrift und ziehen Sie die Spalte an die gewünschte Position.

## Spaltenanzeige anpassen (4.0 und höher)

1. Klicken Sie in der Kopfleiste auf die Schaltfläche .

   Das Fenster Angezeigte Spalten wird geöffnet.




2. Aktivieren Sie die Kontrollkästchen neben den Spalten, die angezeigt werden sollen.

   Hinweis: Deaktivieren Sie die Kontrollkästchen neben Spalten, die Sie ausblenden möchten.

   Tipp: Verwenden Sie das Suchfeld, um nach bestimmten Spalten zu suchen.

3. Klicken Sie auf die Schaltfläche , um den Bereich Angezeigte Spalten zu schließen.

   OT Security zeigt nur die ausgewählten Spalten an.

## Listen nach Kategorien gruppieren (3.19 und früher)

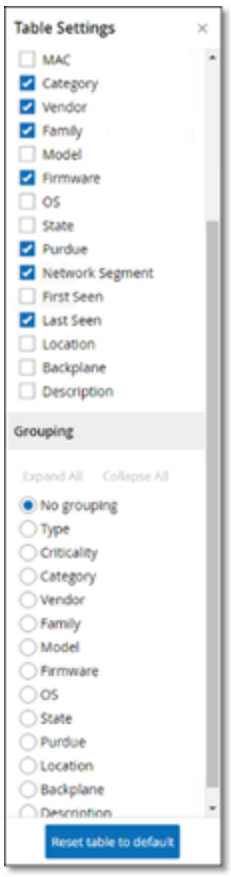
Für die Inventar-Seiten können Sie die Listen nach verschiedenen Parametern gruppieren, die für diesen bestimmten Bildschirm relevant sind.

So gruppieren Sie die Listen:

1. Klicken Sie am rechten Rand der Tabelle auf die Registerkarte Einstellungen.

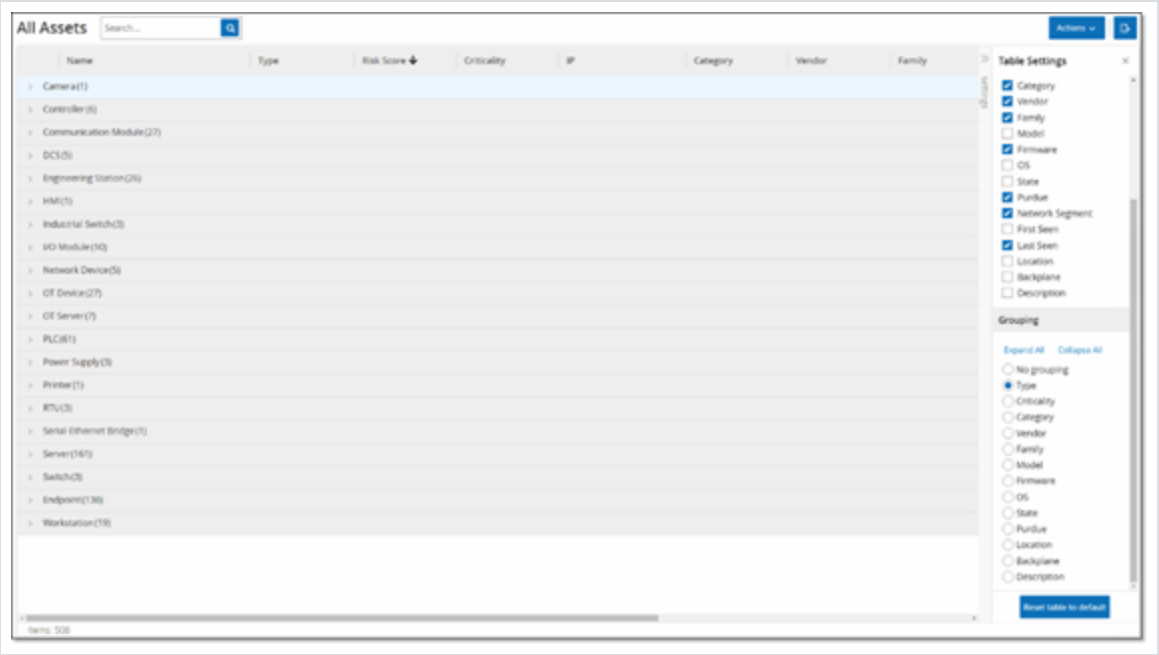
   Der Bereich Tabelleneinstellungen wird auf der rechten Seite mit den Abschnitten Spalten und Gruppierung angezeigt.

2. Scrollen Sie nach unten zum Abschnitt Gruppierung.



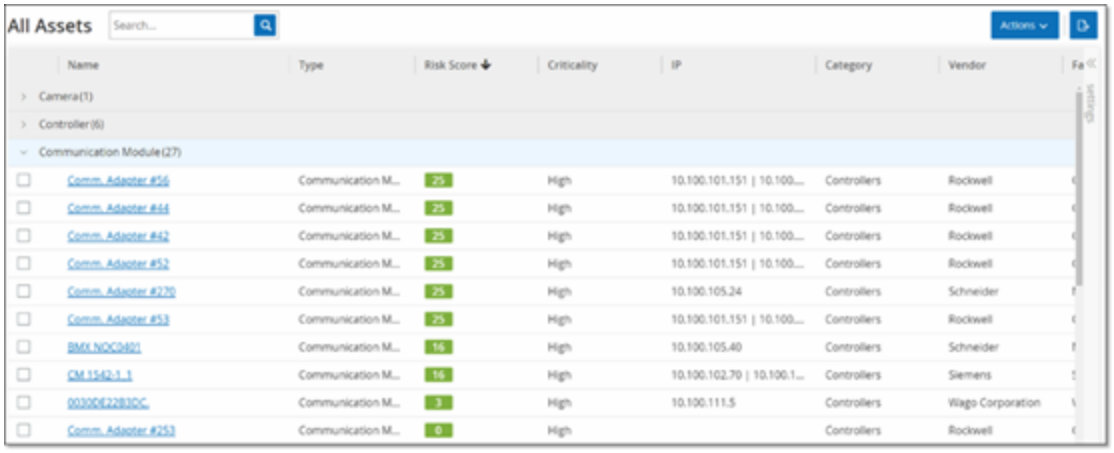

3. Wählen Sie den Parameter aus, nach dem die Listen gruppiert werden sollen. Beispiel: Typ.

   OT Security zeigt die gruppierten Kategorien an.



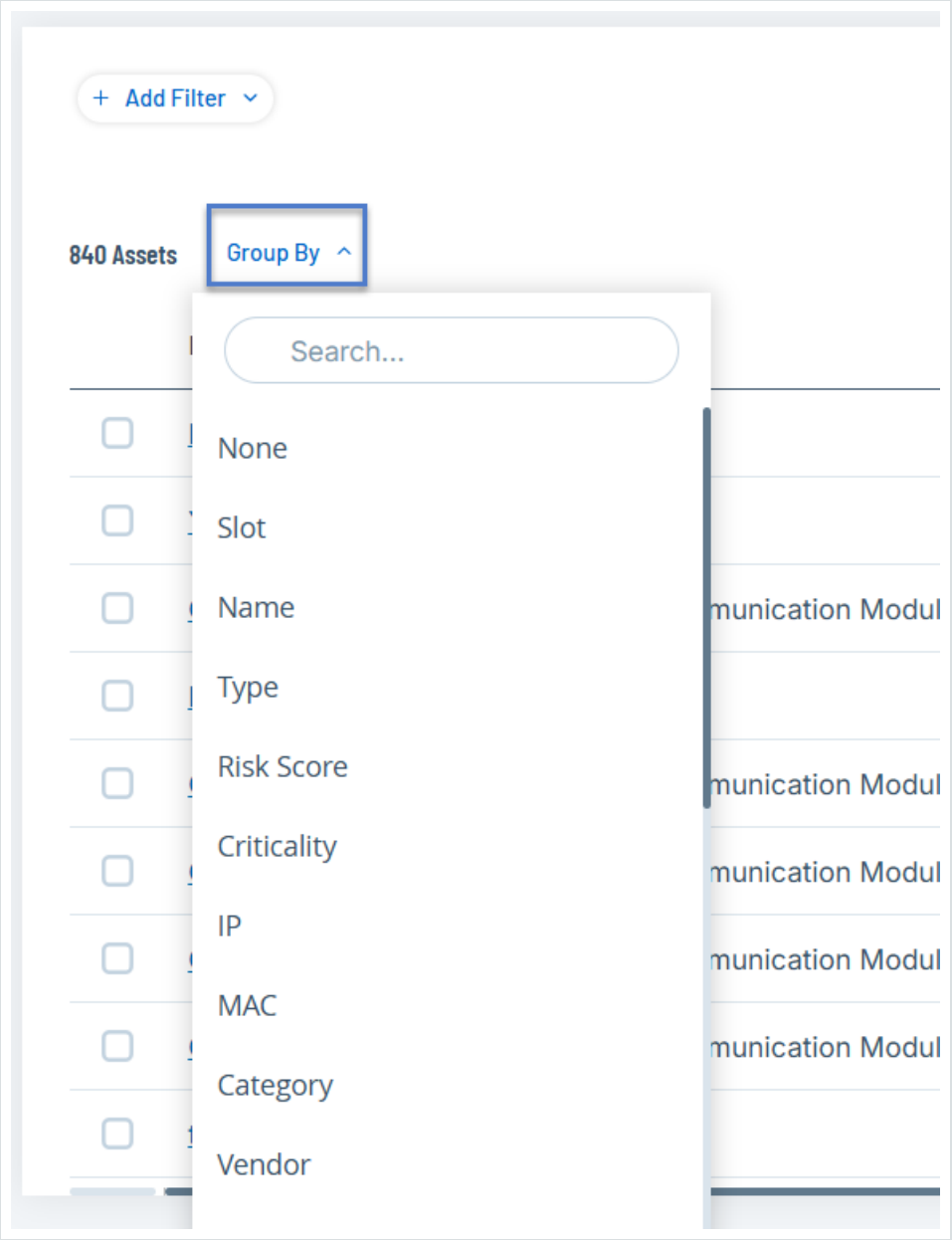

4. Klicken Sie auf das x (oder auf die Registerkarte Einstellungen), um das Fenster Tabelleneinstellungen zu schließen.

5. Klicken Sie auf den Pfeil neben einer Kategorie, um alle Instanzen für diese Kategorie anzuzeigen.




## Listen nach Kategorien gruppieren (4.0 und höher)

1. Klicken Sie in der Tabellenüberschrift auf die Dropdown-Liste Gruppieren nach.




2. Wählen Sie den Parameter aus, der zum Gruppieren der Liste verwendet werden soll. Beispiel: Name.

> Tipp: Verwenden Sie das Suchfeld, um nach einem bestimmten Parameter zu suchen.

OT Security gruppiert die Liste nach dem ausgewählten Parameter.

> Hinweis: Verwenden Sie die Schaltflächen Alle erweitern oder Alle reduzieren, um die Liste zu erweitern bzw. zu reduzieren.

## Spalten sortieren

### So sortieren Sie die Listen:

1. Klicken Sie auf eine Spaltenüberschrift, um die Assets nach diesem Parameter zu sortieren. Klicken Sie beispielsweise auf die Überschrift Name, um die Assets in alphabetischer Reihenfolge nach Namen anzuzeigen.
2. Klicken Sie erneut auf die Spaltenüberschrift, wenn Sie die Anzeigereihenfolge umkehren möchten (d. h. A→Z, Z→A).

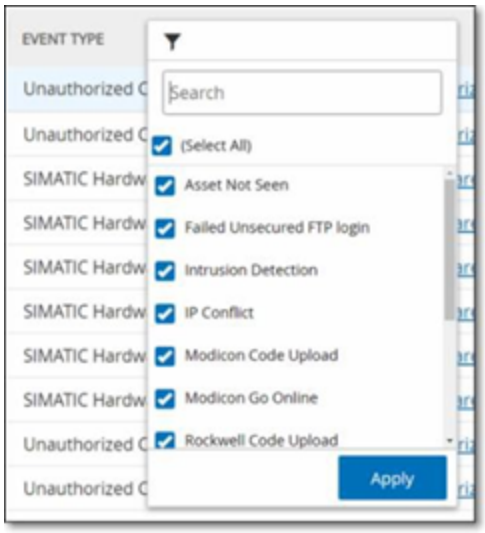
## Spalten filtern (3.19 und früher)

Sie können Filter für eine oder mehrere Spaltenüberschriften festlegen. Die Filter sind kumulativ, sodass nur Listen angezeigt werden, die allen Filterkriterien entsprechen. Die Filteroptionen sind für jede Spaltenüberschrift spezifisch. Jede Seite bietet eine Auswahl relevanter Filter. Im Bildschirm Controller-Inventar können Sie beispielsweise nach Name, Adressen, Typ, Backplane und Anbieter filtern.

### So filtern Sie die Listen:

1. Bewegen Sie den Mauszeiger über eine Spaltenüberschrift, um das Filtersymbol ▼ anzuzeigen.
2. Klicken Sie auf das Filtersymbol ▼.

   Eine Liste mit Filteroptionen wird angezeigt. Die Optionen sind für jeden Parameter spezifisch.




3. Wählen Sie die anzuzeigenden Elemente aus und deaktivieren Sie die Kontrollkästchen der Elemente, die ausgeblendet werden sollen.

   > Hinweis: Sie können zunächst das Kontrollkästchen Alle auswählen deaktivieren und dann die Kontrollkästchen der Elemente aktivieren, die Sie anzeigen möchten.

4. Sie können die Liste nach Filtern durchsuchen und diese aktivieren oder deaktivieren.

5. Klicken Sie auf Anwenden.

   OT Security filtert die Listen wie angegeben.

> Die Filterschaltfläche ▼ neben der Spaltenüberschrift zeigt an, dass die Ergebnisse nach diesem Parameter gefiltert werden.

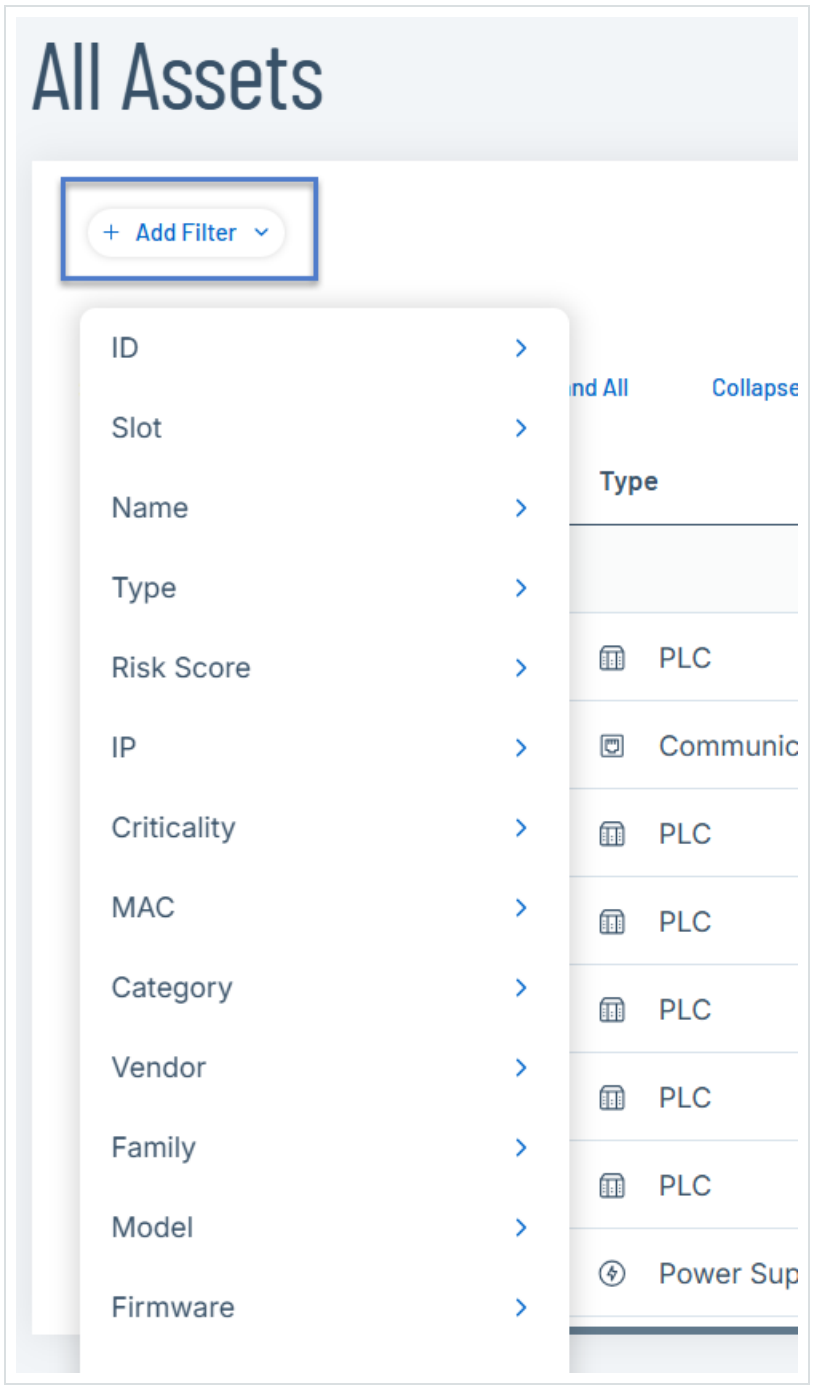
So entfernen Sie die Filter:

1. Klicken Sie auf die Filterschaltfläche ▼.
2. Klicken Sie auf das Kontrollkästchen Alle auswählen, um Ihre Auswahl aufzuheben.
3. Klicken Sie erneut auf das Kontrollkästchen Alle auswählen, um alle Elemente auszuwählen.
4. Klicken Sie auf Anwenden.

## Spalten filtern in (4.0 und höher)

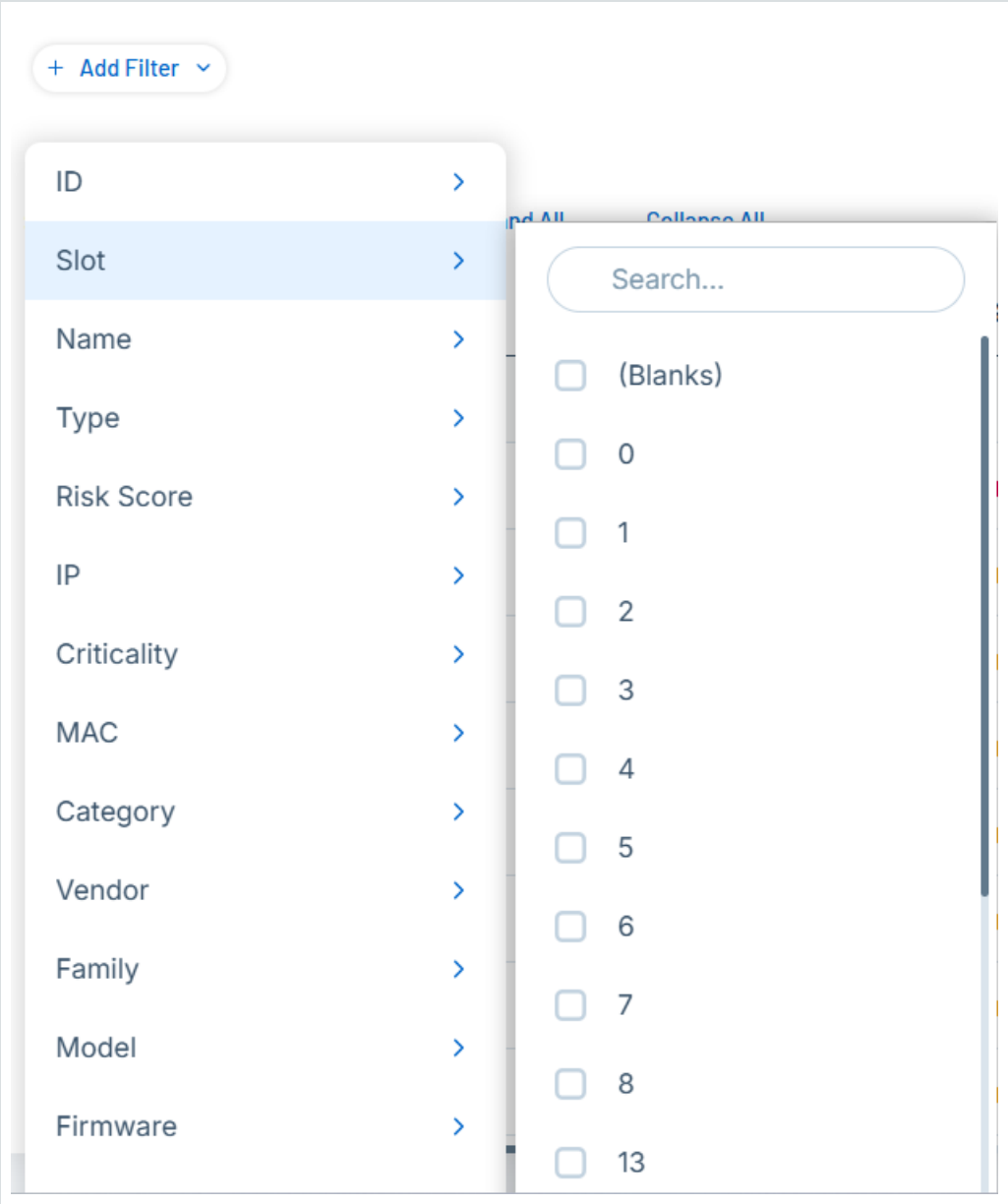
1. Klicken Sie in der Tabellenüberschrift auf die Dropdown-Liste + Filter hinzufügen.

   Es wird ein Dropdown-Menü mit verfügbaren Filterelementen angezeigt.




2. Wählen Sie das Element aus, nach dem Sie filtern möchten.

Eine Liste mit Filteroptionen wird angezeigt.

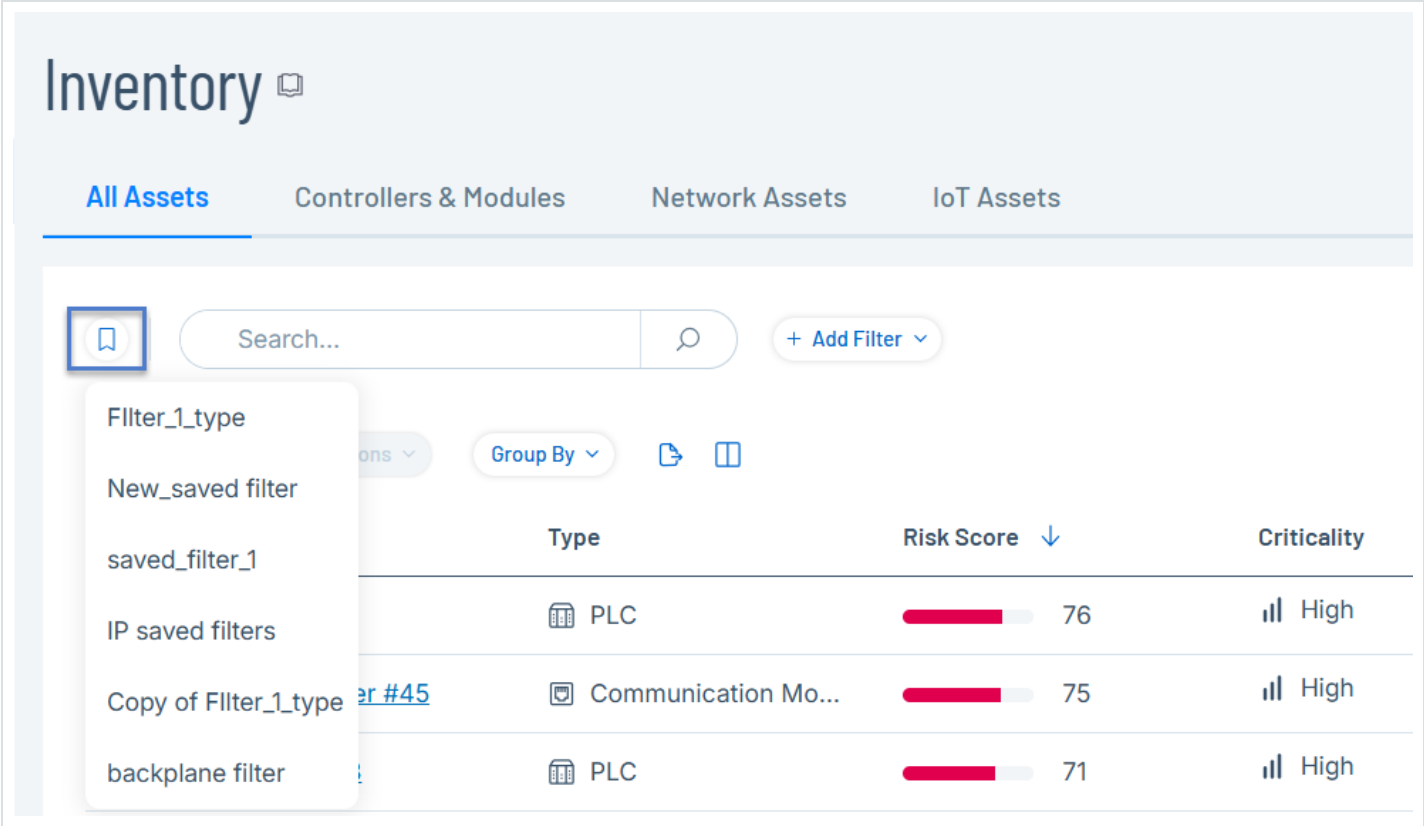



3. Aktivieren Sie die Kontrollkästchen neben den Optionen, nach denen Sie filtern möchten.

> Tipp: Verwenden Sie das Suchfeld, um nach bestimmten Filteroptionen zu suchen.

## Filter speichern

Sie können die häufig verwendeten Filter speichern und bei Bedarf über Gespeicherte Filter darauf zugreifen. So können Sie Ihre spezifischen gefilterten Ansichten speichern und schnell zu ihnen zurückkehren.




Hinweis: Die Funktion „Filter speichern“ finden Sie auf den Seiten Inventar, Feststellungen > Schwachstellen und Feststellungen > Richtlinienverstöße.

So speichern Sie einen häufig verwendeten Filter:

1. Klicken Sie in der Tabellenüberschrift auf die Dropdown-Liste + Filter hinzufügen.

   Es wird ein Dropdown-Menü mit verfügbaren Filterelementen angezeigt.

2. Wählen Sie die gewünschten Filterelemente aus.

3. Klicken Sie auf Filter anwenden.

   OT Security zeigt die gefilterten Ergebnisse an.

4. Um den Filter zu speichern, klicken Sie auf Filter speichern.

   Der Bereich Filter speichern wird angezeigt.

5. Geben Sie im Feld Name einen Namen für den Filter ein.

6. Klicken Sie auf Speichern.

   OT Security speichert den Filter.

7. Um auf die gespeicherten Filter zuzugreifen, klicken Sie auf die Schaltfläche .

   Die Liste der gespeicherten Filter wird angezeigt.

8. Klicken Sie auf den gewünschten Filter und sehen Sie sich die gefilterten Ergebnisse an.

### Gespeicherte Filter ändern

Sie können Änderungen an vorhandenen gespeicherten Filtern vornehmen.

#### So nehmen Sie Änderungen an vorhandenen gespeicherten Filtern vor:

1. Klicken Sie in der Tabellenüberschrift auf die Schaltfläche .

   Die Liste der gespeicherten Filter wird angezeigt.

2. Klicken Sie auf einen vorhandenen gespeicherten Filter, den Sie ändern möchten.

3. Fügen Sie nach Bedarf Filterelemente hinzu oder entfernen Sie sie.

4. Klicken Sie auf Filter speichern und wählen Sie Änderungen speichern aus.

   OT Security speichert die Änderungen am Filter.

### Kopie des gespeicherten Filters erstellen

Sie können ein Duplikat des gespeicherten Filters erstellen und ihn als neuen Filter speichern.

#### So duplizieren Sie einen gespeicherten Filter und speichern ihn unter einem neuen Namen:

1. Klicken Sie in der Tabellenüberschrift auf die Schaltfläche .

   Die Liste der gespeicherten Filter wird angezeigt.

2. Klicken Sie auf einen vorhandenen gespeicherten Filter, den Sie kopieren möchten.
3. Klicken Sie auf Filter speichern und wählen Sie Als Kopie speichern aus.

   Der Bereich Filter speichern wird angezeigt.

4. Ändern Sie im Feld Name den Filternamen.
5. Klicken Sie auf Speichern.

   OT Security speichert den Filter.

### Alle Filter entfernen

So löschen Sie alle angewendeten Filter und setzen die Tabelle in ihren ursprünglichen, ungefilterten Zustand zurück:

- Klicken Sie in der Tabellenüberschrift auf Alle Filter entfernen.

## Suchen (3.19 und früher)

Sie können auf jeder Seite nach bestimmten Datensätzen suchen.

### So durchsuchen Sie die Listen:

1. Geben Sie den Suchtext in das Suchfeld ein.
2. Klicken Sie auf die Schaltfläche .
3. Um den Suchtext zu löschen, klicken Sie auf die Schaltfläche x.

## Suchen (4.0 und höher)

Sie können auf jeder Seite nach bestimmten Datensätzen suchen.

So durchsuchen Sie die Listen:

1. Geben Sie den Suchtext in das Suchfeld ein.
2. Klicken Sie auf die Schaltfläche .
3. Um den Suchtext zu löschen, klicken Sie auf die Schaltfläche .

## Daten exportieren

Sie können Daten aus jeder der in der Benutzeroberfläche von OT Security angezeigten Listen (z. B. Ereignisse und Inventar) als CSV-Datei exportieren.

> Hinweis: Die exportierte Datei enthält alle Daten für diese Seite, selbst wenn Filter auf die aktuelle Anzeige angewendet wurden.

So exportieren Sie Daten:

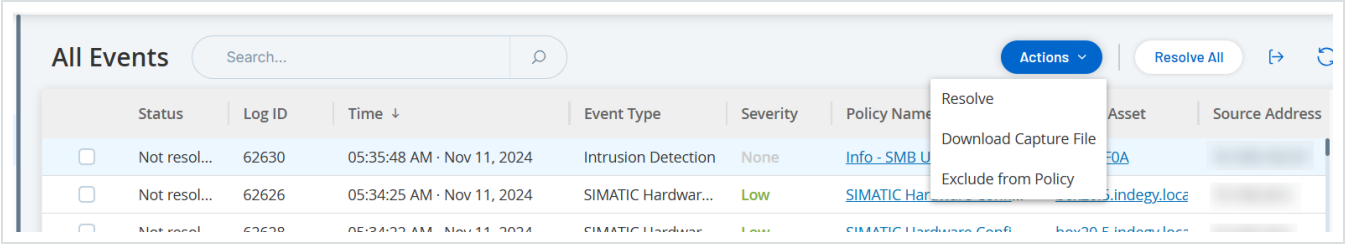
1. Gehen Sie zu der Seite, für die Sie Daten exportieren möchten.
2. Klicken Sie in der Kopfleiste auf die Schaltfläche .

   OT Security lädt ein CSV-Format der Daten herunter.

## Menü „Aktionen“

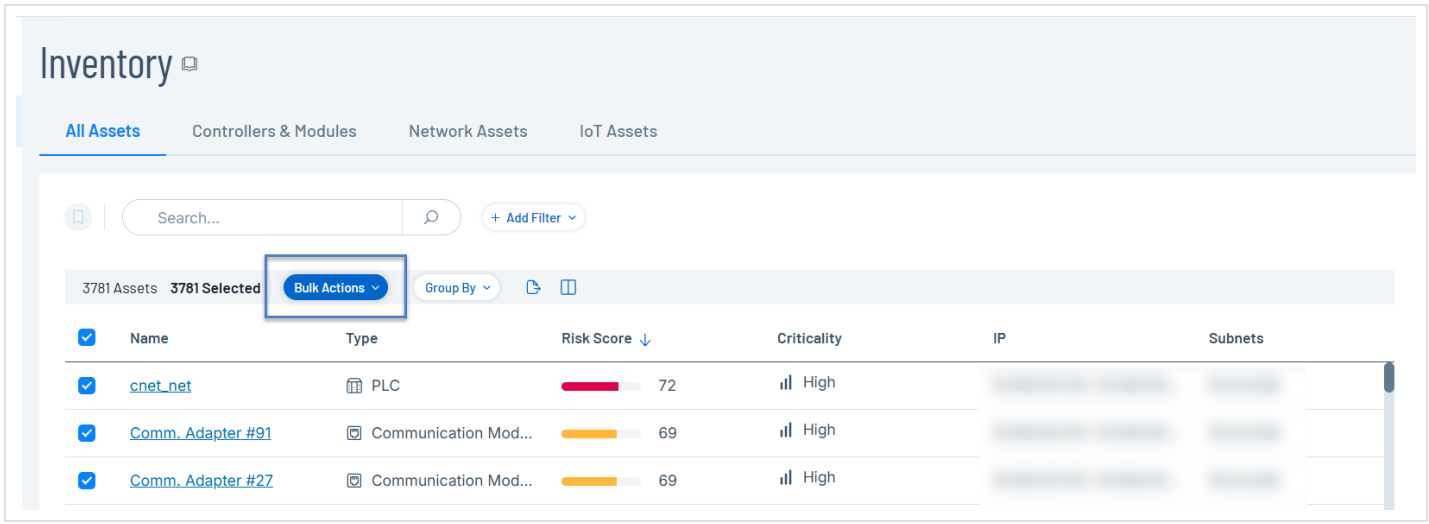
Jeder Bildschirm verfügt über eine Reihe von Aktionen, die Sie für die auf diesem Bildschirm aufgeführten Elemente ausführen können. Beispielsweise können Sie im Bildschirm Richtlinien die Aktionen **Anzeigen**, **Bearbeiten**, **Duplizieren** oder **Löschen** für eine Richtlinie ausführen. Im Bildschirm Ereignisse können Sie für ein Ereignis die Aktionen **Auflösen** oder **Erfassungsdatei herunterladen** ausführen.

So greifen Sie auf das Menü Aktionen zu:

- Wählen Sie ein Element aus und klicken Sie dann in der Kopfleiste auf Aktionen.
- 


## Massenaktionen

Wenn Sie mehrere Elemente auf einer Seite auswählen, aktiviert OT Security die Option Massenaktionen in der Kopfzeile.



# OT Security – Übersicht

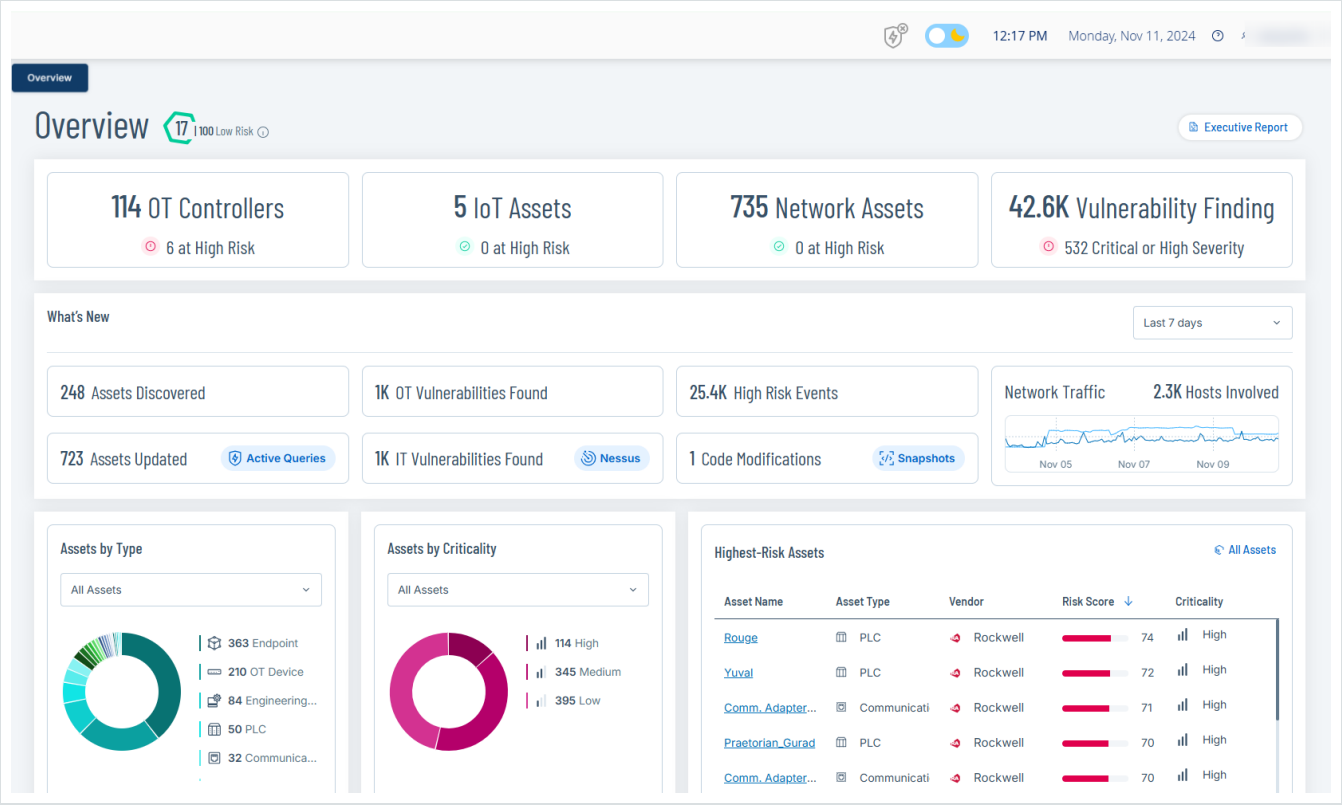
Auf der Seite Übersicht werden in interaktiven Widgets wichtige Informationen zu Ihrer OT-Umgebung angezeigt. Die Widgets auf dieser Seite bieten Echtzeit-Einblicke in Ihre Umgebung, beispielsweise:

- Informationen über die Sicherheitslage Ihrer Umgebung
- Eine Zusammenfassung der Änderungen seit Ihrem letzten Login
- Eine Aufschlüsselung der verschiedenen Arten von Assets in Ihrem Inventar
- Der aktuelle Status von Assets und Schwachstellen.
- Assets, die das höchste Risiko darstellen
- Zeitstempel Ihrer letzten Coderevision

So greifen Sie auf die Seite Übersicht zu:

1. Klicken Sie in der linken Navigationsleiste auf Übersicht.

   Die Seite Übersicht wird angezeigt.




Die Seite Übersicht enthält die folgenden Widgets:

| Widget | Beschreibung |
|---|---|
| Risikowert | Der durchschnittliche Risikowert ist der Durchschnitt aller Asset-Werte in Ihrer Umgebung. Um eine Aufschlüsselung dieses Werts anzuzeigen, bewegen Sie den Mauszeiger über den Wert.<br><br>Für den durchschnittlichen Risikowert werden die folgenden Farbcodes verwendet, um den Schweregrad des Risikos anzuzeigen:<br><br>• Gering (Grün):0-29<br><br>• Mittel (Gelb): 30-69 |

| | |
|---|---|
| | • Hoch (Rot): 70-100<br><br>OT Security berechnet die Asset-Werte auf der Grundlage der folgenden Faktoren, die sich im Laufe der Zeit ändern (verfallende Ereignisse, Firmware- und Statusänderungen):<br><br>• Kritikalität – Basierend auf Asset-Typ und Purdue-Level. Beispielsweise steuert eine SPS die Produktion und wird daher als kritisch angesehen, während eine Kamera in der Regel weniger kritisch ist.<br><br>• Schwachstellen – Basierend auf dem Vulnerability Priority Rating (VPR)-Asset.<br><br>• Ereignisse – Basierend auf den Ereignissen, die mit dem Asset verbunden sind. Richtlinien lösen Ereignisse aus und jede Richtlinie definiert einen Schweregrad. Der Schweregrad wird basierend auf der Anzahl der Ereignisse, ihrem Schweregrad und der Dauer ihres Bestehens berechnet. Ältere Ereignisse wirken sich weniger auf den Wert aus als kürzlich stattgefundene Ereignisse.<br><br>• Backplane – Ein Asset, das sich auf einer Backplane befindet, wirkt sich auf die Werte seiner Nachbar-Assets aus. Wenn beispielsweise ein Modul anfällig ist, ist auch die gesamte Backplane anfällig. |
| Assets und Schwachstellen | Der aktuelle Status von Assets und Schwachstellen in Ihrer Umgebung. Enthält separate Widgets für jeden Asset-Typ (OT-Controller, Netzwerk-Assets, IoT-Assets), die die Anzahl der Assets in der jeweiligen Kategorie und die Anzahl der Assets, die einem hohen Risiko ausgesetzt sind, anzeigen.<br><br>Hinweis: Assets mit einem Risikowert von 70 und höher werden als |

| | |
|---|---|
| | Assets mit hohem Risiko eingestuft. |
| Neuerungen | Eine Zusammenfassung der Änderungen seit Ihrem letzten Login, wie z. B. neue Assets, Schwachstellen und Ereignisse mit hohem Risiko. Führen Sie einen Drilldown durch, um die Seite der jeweiligen Assets, Ereignisse oder Schwachstellen zu öffnen und die gefilterten Assets, Schwachstellen oder Ereignisse anzuzeigen.<br><br>Eine Zusammenfassung der Änderungen seit Ihrem letzten Login, wie z. B. neue Assets, Schwachstellen, Verstöße mit hohem Risiko und Betriebsverstöße. Führen Sie einen Drilldown durch, um die Seite der jeweiligen Assets, Feststellungen oder Schwachstellen zu öffnen und die gefilterten Assets, Schwachstellen oder Ereignisse anzuzeigen.<br><br>Verwenden Sie die Dropdown-Liste mit Filtern, um die Ergebnisse nach Letzter Tag, Letzte 7 Tage (Standardeinstellung) oder Letzte 30 Tage zu filtern. |
| Assets nach Typ | Die Anzahl der Assets nach Typ, z. B. Endgerät, SPS und OT-Gerät. |
| Assets nach Kritikalität | Die Anzahl der Assets nach ihrer Kritikalität: Hoch, Mittel oder Gering. |
| Assets mit höchstem Risiko | Listet alle Assets mit hohem Risiko mit Details wie Asset-Name, Asset-Typ, Anbieter, Risikowert und Kritikalität auf. So rufen Sie die Seite Alle Assets auf: Klicken Sie in der oberen rechten Ecke auf den Link Alle Assets. |
| Kurzbericht | Generiert einen Risikobewertungsbericht Ihrer OT-Umgebung. Weitere Informationen finden Sie unter Kurzbericht generieren. |

## Kurzbericht generieren

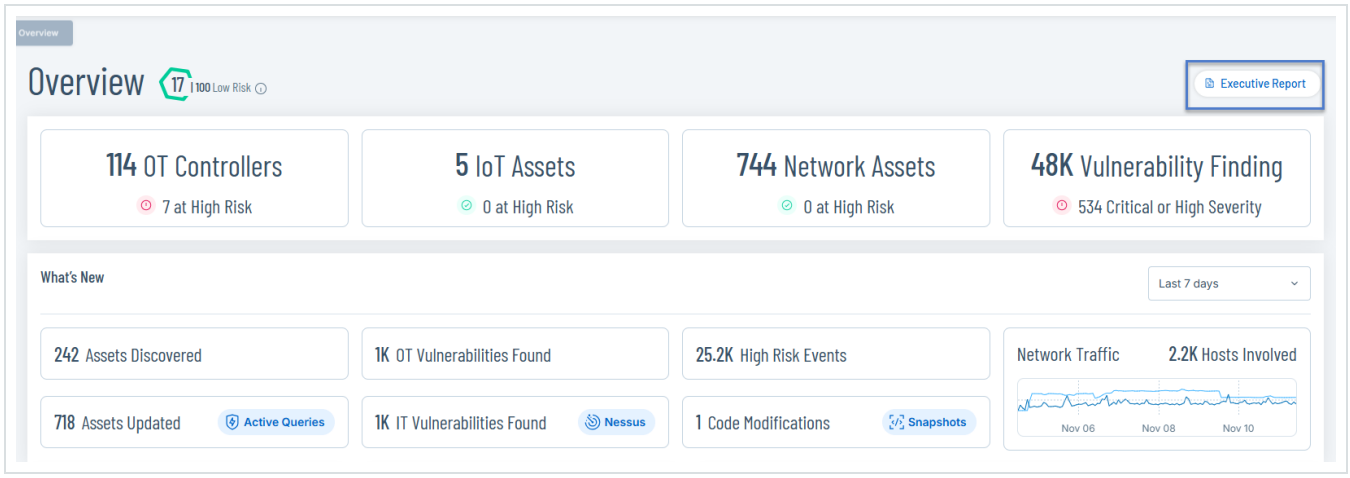
Sie können einen Risikobewertungsbericht für Ihre Umgebung generieren, der auf den Daten der letzten 30 Tage basiert. OT Security verwendet wichtige Widgets aus den Dashboards Risiko, Inventar sowie Ereignisse und Richtlinien, um eine allgemeine grafische Übersicht zu erstellen, die Assets mit hohem Risiko, kritische und häufige Schwachstellen, gängige Plugin-Familien und vor Kurzem erfasste Assets hervorhebt.

Verwenden Sie die Diagramme des Berichts, wie z. B. „Schwachstellen nach Schweregrad“, „Assets nach Risikowert“ und „Assets nach Kritikalität“, um kritische Assets und die schwerwiegendsten Schwachstellen in Ihrer Umgebung in den letzten 30 Tagen zu identifizieren.

## So generieren Sie einen monatlichen Bericht:

1. Gehen Sie in der linken Navigationsleiste zu Übersicht.

   Die Seite Übersicht wird angezeigt.




2. Klicken Sie in der oberen rechten Ecke auf Kurzbericht.

   OT Security öffnet den Bericht in Ihrem Browser.

3. Um den Bericht als PDF-Datei herunterzuladen, klicken Sie oben auf der Seite auf Als PDF speichern.

   Das Dialogfeld Drucken wird angezeigt.

4. Wählen Sie im Dropdown-Feld Ziel die Option Als PDF speichern aus.

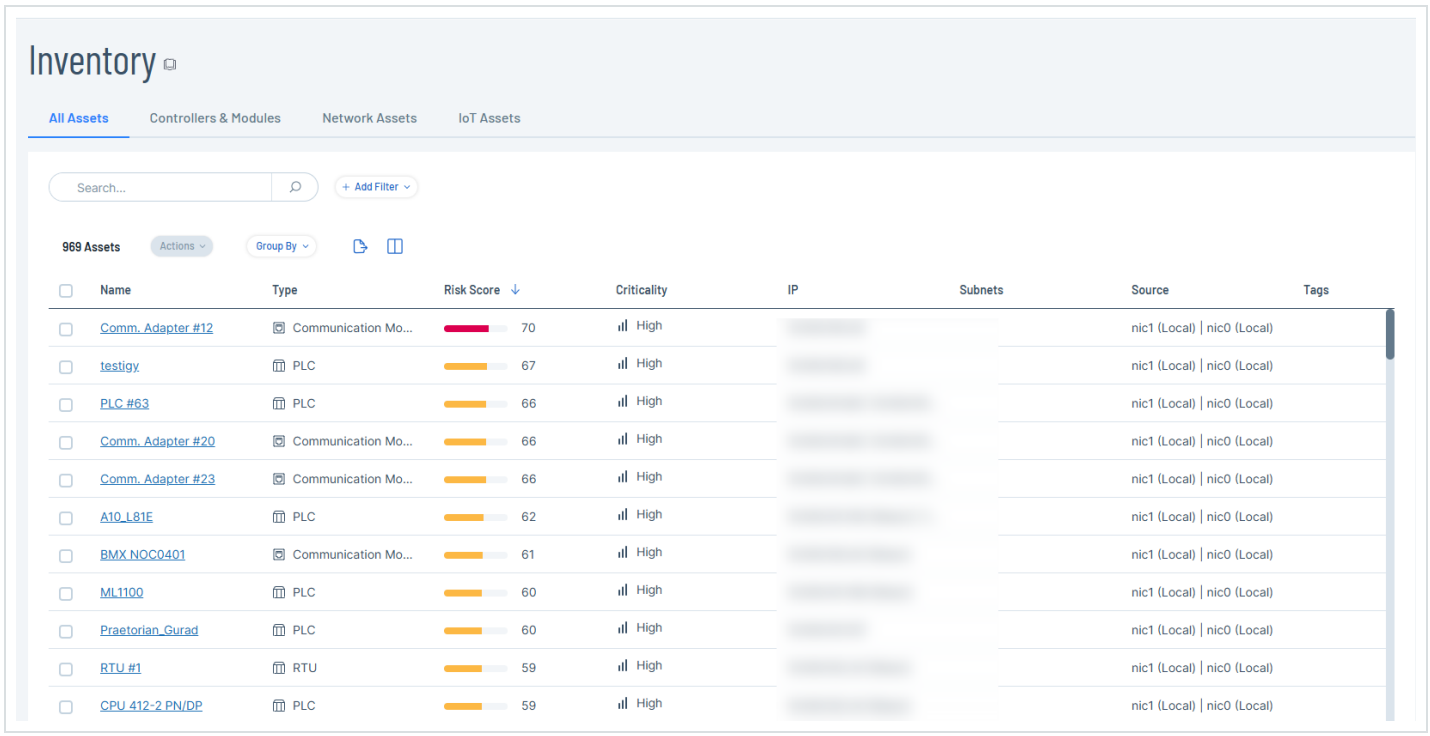
5. Navigieren Sie zu dem Pfad, in dem Sie den Bericht speichern möchten.
6. Klicken Sie auf Speichern.

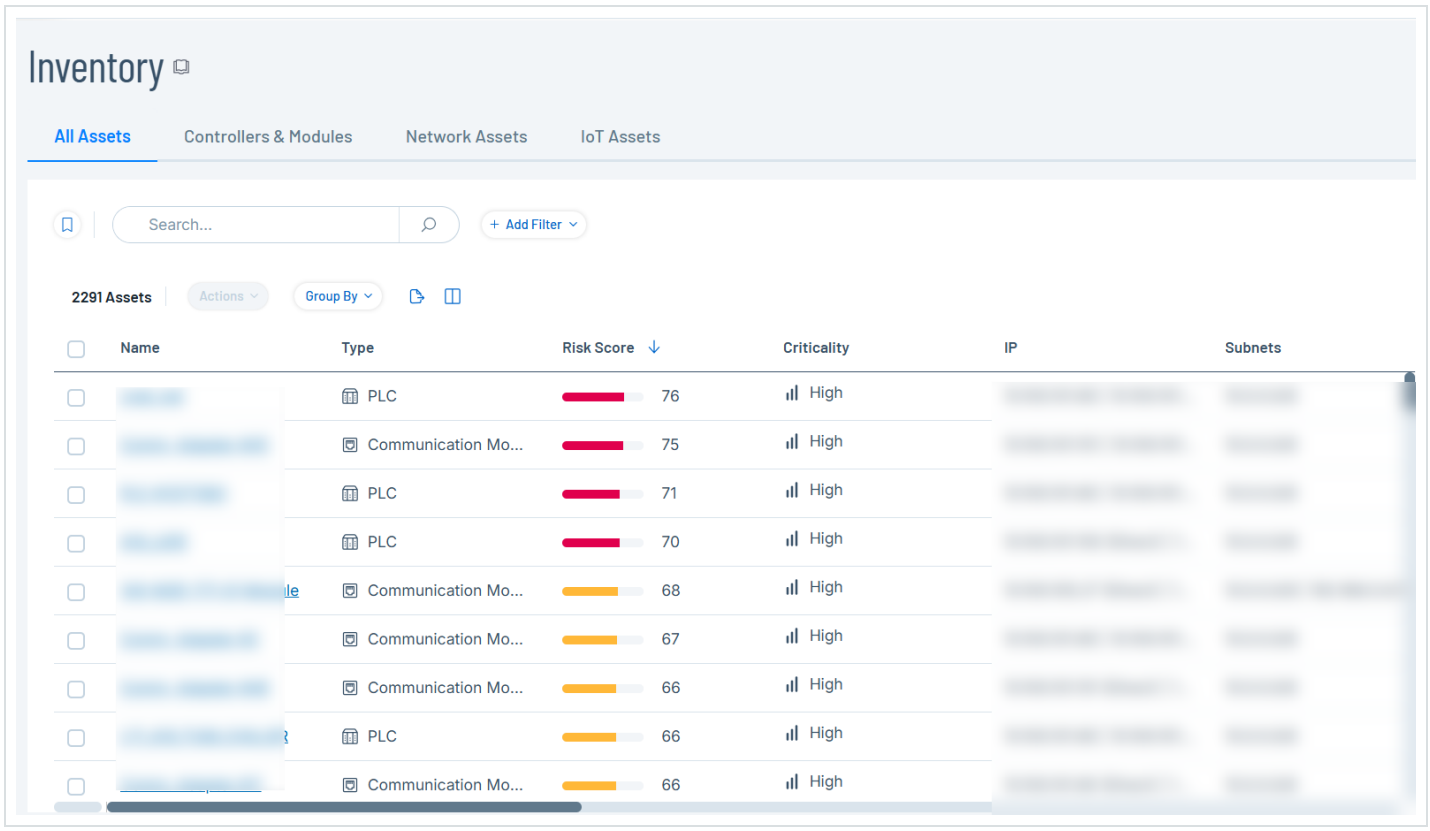
   OT Security speichert den Bericht im PDF-Format.

# Inventar

Die automatisierte Asset-Erfassung, -Klassifizierung und -Verwaltung von OT Security bietet eine genaue, aktuelle Asset-Inventarisierung, indem alle Änderungen an Geräten kontinuierlich verfolgt werden. Dies vereinfacht die Aufrechterhaltung der betrieblichen Kontinuität, Zuverlässigkeit und Sicherheit. Es spielt außerdem eine wichtige Rolle bei der Planung von Wartungsprojekten, der Priorisierung von Upgrades, der Bereitstellung von Patches sowie bei der Vorfallsreaktion und Risikominderungsmaßnahmen.

## Anzeigen von Assets




Alle Assets im Netzwerk werden auf den Inventar-Seiten angezeigt. Die Inventar-Seite enthält detaillierte Daten über Assets, was ein umfassendes Asset-Management sowie die Überwachung

des Status jedes Assets und der damit verbundenen Ereignisse ermöglicht. OT Security erfasst diese Daten mit den Funktionen zur Netzwerkerkennung und der aktiven Abfrage. Die Seite Alle zeigt Daten für alle Asset-Typen. Darüber hinaus werden spezifische Teilmengen der Assets für jeden der folgenden Asset-Typen auf separaten Bildschirmen angezeigt: Controller und Module, Netzwerk-Assets und IoT.

> Hinweis: Der Bildschirm „Netzwerk-Assets“ enthält alle Asset-Typen, die nicht in den Bildschirmen „Controller und Module“ oder „IoT“ enthalten sind.

Für jeden Asset-Bildschirm (Alle, Controller und Module, Netzwerk-Assets und IoT) können Sie die Anzeigeeinstellungen benutzerdefiniert einstellen, indem Sie anpassen, welche Spalten angezeigt werden und wo die einzelnen Spalten positioniert sind. Außerdem können Sie die Assets-Listen sortieren und filtern sowie eine Suche durchführen. Informationen zum Anpassen von Tabellen finden Sie unter Elemente in der Benutzeroberfläche der Verwaltungskonsole.

Die folgende Tabelle beschreibt Parameter, die auf den Inventar-Seiten angezeigt werden.

Mit einem * gekennzeichnete Parameter werden nur auf der Seite Controller angezeigt.

| Parameter | Beschreibung |
|---|---|
| Name | Der Name des Assets im Netzwerk. Klicken Sie auf den Namen des Assets, um den Bildschirm „Asset-Details“ für dieses Asset anzuzeigen (siehe Inventar). |
| IP | Die IP-Adresse des Assets.<br><br>Hinweis: Ein Asset kann mehrere IP-Adressen haben.<br><br>Hinweis: Als „Direkt“ ausgewiesene IP-Adressen sind diejenigen, zu denen Tenable eine direkte Verbindung hergestellt hat. Wenn keine Beschriftung vorhanden ist, bedeutet dies, dass Tenable die IP ohne direkte Kommunikation gefunden hat.<br><br>Hinweis: Assets können nach IP-Bereich gefiltert werden. Weitere |

| Parameter | Beschreibung |
|---|---|
| | Informationen zum Filtern finden Sie unter Elemente in der Benutzeroberfläche der Verwaltungskonsole. |
| Subnetze | Die Subnetze, die durch die Abfrage von Netzwerkgeräten über SNMP erfasst wurden. |
| Quelle | Der Name der Quelle. Zum Beispiel „nic1“ oder „nic2“ für eine lokale Quelle oder der Sensorname, wenn die Quelle ein Sensor ist. |
| MAC | Die MAC-Adresse des Assets. |
| Tags | Die Tags, die Sie für das Asset auf der Seite Asset-Gruppen und Tags erstellen. |
| Netzwerksegment | Das Netzwerksegment, dem die IPs dieses Assets zugewiesen sind. |
| Typ | Der Typ des Assets: Controller, E/A oder Kommunikation usw. (siehe Asset-Typen). |
| Backplane* | Die Backplane-Einheit, mit der das Asset verbunden ist. Weitere Details zur Backplane-Konfiguration werden im Bildschirm „Asset-Details“ angezeigt. |
| Slot* | Zeigt für Assets auf Backplanes die Nummer des Steckplatzes an, an dem das Asset angeschlossen ist. |
| Anbieter | Der Asset-Anbieter. |
| Familie* | Der vom Asset-Anbieter definierte Name der Produktfamilie. |
| Firmware | Die aktuell auf dem Asset installierte Firmware-Version. |
| Standort | Der Standort des Assets, wie vom Benutzer in den Asset-Details von OT Security eingegeben. Siehe Asset-Details bearbeiten. |

| Parameter | Beschreibung |
|---|---|
| Zuletzt gesehen | Der Zeitpunkt, zu dem das Gerät zuletzt von OT Security gesehen wurde. Dies ist das letzte Mal, dass das Gerät mit dem Netzwerk verbunden war oder eine Aktivität durchgeführt hat. |
| Betriebssystem | Das Betriebssystem, das auf dem Asset ausgeführt wird. |
| Modellname | Der Modellname des Assets. |
| Status* | Der Gerätestatus. Mögliche Werte:<br>• Backup – Der Controller wird als Backup für einen primären Controller ausgeführt.<br>• Fehler – Der Controller befindet sich im Fehlermodus.<br>• Keine Konfig. – Für den Controller wurde keine Konfiguration eingestellt.<br>• Läuft – Der Controller läuft.<br>• Angehalten – Der Controller läuft nicht.<br>• Unbekannt – Der Status ist unbekannt. |
| Beschreibung | Eine kurze Beschreibung des Assets, wie vom Benutzer in den Asset-Details von OT Security konfiguriert. Siehe Asset-Details bearbeiten. |
| Risiko | Ein Maß für das mit diesem Asset verbundene Risiko auf einer Skala von 0 (kein Risiko) bis 100 (extrem hohes Risiko). Eine Erläuterung, wie der Risikowert berechnet wird, finden Sie unter Risikobewertung. |
| Kritikalität | Ein Maß für die Bedeutung dieses Assets für das ordnungsgemäße Funktionieren des Systems. Jedem Asset wird basierend auf dem Asset-Typ automatisch ein Wert zugewiesen. Sie können den Wert |

| Parameter | Beschreibung |
| --- | --- |
| | manuell anpassen. |
| Purdue-Level | Das Purdue-Level des Assets (0=Physischer Prozess, 1=Intelligente Geräte, 2=Steuerungssysteme, 3=Betriebssysteme der Produktion, 4=Business-Logistiksysteme). |
| Benutzerdefiniertes Feld | Sie können benutzerdefinierte Felder erstellen, um Ihre Assets mit relevanten Informationen zu kennzeichnen. Das benutzerdefinierte Feld kann ein Link zu einer externen Ressource sein. |

## Asset-Typen

In der folgenden Tabelle werden die verschiedenen Arten von Assets beschrieben, die von OT Security identifiziert werden. Die Tabelle zeigt auch das Symbol, mit dem die einzelnen Asset-Typen in der OT Security-Verwaltungskonsole dargestellt werden (z. B. im Bildschirm „Netzwerkübersicht“).

| Kategorie | Standard-Kritikalitätsstufe/Purdue-Level | Beschreibung | Untertypen | |
| --- | --- | --- | --- | --- |
| Controller | Hoch/1 | Ein industrielles Computer-Steuerungssystem, das den Zustand von Eingabegeräten kontinuierlich überwacht und Entscheidungen auf der Grundlage eines |  | Controller |

| Kategorie | Standard-Kritikalitätsstufe/Purdue-Level | Beschreibung | Untertypen | |
|---|---|---|---|---|
| | | benutzerdefinierten Programms trifft, um den Zustand von Ausgabegeräten zu steuern. Diese Kategorie umfasst alle Arten von Controllern und ihre zugehörigen Komponenten. | | |

| Kategorie | Standard-Kritikalitätsstufe/Purdue-Level | Beschreibung | Untertypen | |
|---|---|---|---|---|
| | | |  | SPS |

| Kategorie | Standard-Kritikalitätsstufe/Purdue-Level | Beschreibung | Untertypen | |
|---|---|---|---|---|
| | | |  | DCS |
| | | |  | IED |
| | | |  | RTU |
| | | |  | BMS-Controller |
| | | |  | Roboter |
| | | |  | Kommunikationsmodul |
| | | |  | E/A-Modul |
| | | |  | CNC |
| | | |  | Stromversorgung |
| | | |  | Backplane-Modul |

| Kategorie | Standard-Kritikalitätsstufe/Purdue-Level | Beschreibung | Untertypen | |
|---|---|---|---|---|
| Feldgeräte | Hoch/1 | Ein industrielles Gerät (z. B. Sensor, Aktuator, Elektromotor), das Industrieprotokolle verwendet, um Informationen an ICS-Systeme zu senden. |  | Feldgerät |
| | | |  | Strommessgerät |
| | | |  | Remote-E/A |
| | | |  | Relay |
| | | |  | Wandler |
| | | |  | Industrieller Sensor |
| | | |  | Antrieb |
| | | |  | Aktuator |

| Kategorie | Standard-Kritikalitätsstufe/Purdue-Level | Beschreibung | Untertypen | |
|---|---|---|---|---|
| OT-Geräte | Mittel/2 | Diese Kategorie umfasst alle Arten von OT-Geräten. |  | OT-Gerät |
| | | |  | Industrieller Router |
| | | |  | Industrieller Switch |
| | | |  | Industrielles Gateway |
| | | |  | Industrielles Netzwerkgerät |
| | | |  | Industrieller Drucker |
| OT-Server | Mittel/2 | Ein Computer/Gerät, der/das für den Zugriff auf industrielle |  | OT-Server |

| Kategorie | Standard-Kritikalitätsstufe/Purdue-Level | Beschreibung | Untertypen | |
|---|---|---|---|---|
| | | Daten verwendet wird. Diese Kategorie umfasst alle Arten von OT-Servern und ihre zugehörigen Komponenten. | | |
| | | |  | Historian |
| | | |  | HMI |
| | | |  | Datenlogger |
| Netzwerkgeräte | Mittel/3 | Ein Netzwerkgerät (z. B. ein Switch oder ein Router). Diese Kategorie umfasst alle Arten von |  | Netzwerkgerät |

| Kategorie | Standard-Kritikalitätsstufe/Purdue-Level | Beschreibung | Untertypen | |
|---|---|---|---|---|
| | | Netzwerkgeräten und ihre zugehörigen Komponenten. | | |
| | | |  | Router |
| | | |  | Switch |
| | | |  | Serielle Ethernet-Brücke |
| | | |  | Gateway |
| | | |  | Hub |
| | | |  | Wireless Access Point |

| Kategorie | Standard-Kritikalitätsstufe/Purdue-Level | Beschreibung | Untertypen | |
|---|---|---|---|---|
| | | |  | Firewall |
| | | |  | Konverter |
| | | |  | Repeater |
| | | |  | Funksender |
| Workstations | Gering/3 | Ein Computer, der mit dem Netzwerk verbunden ist und zur Steuerung der SPS verwendet wird. Diese Kategorie umfasst alle Arten von Workstations |  | Workstation |

| Kategorie | Standard-Kritikalitätsstufe/Purdue-Level | Beschreibung | Untertypen | |
|---|---|---|---|---|
| | | und ihre zugehörigen Komponenten. | | |
| | | |  | OT-Workstation |
| | | |  | Engineering-Station |
| | | |  | Virtuelle Workstation |
| Server | Gering/3 | Diese Kategorie umfasst verschiedene Arten von IT-Servern. |  | Server |
| | | |  | Dateiserver |
| | | | | Webserver |

| Kategorie | Standard-Kritikalitätsstufe/Purdue-Level | Beschreibung | Untertypen | |
|---|---|---|---|---|
| | | |  | |

| Kategorie | Standard-Kritikalitätsstufe/Purdue-Level | Beschreibung | Untertypen | |
|---|---|---|---|---|
| | | |  | Virtueller Server |
| | | |  | Sicherheits-Appliance |
| | | |  | Tenable ICP |
| | | |  | Tenable EM |
| | | |  | Tenable Sensor |
| | | |  | Domänen controller |
| | | |  | IoT |

| Kategorie | Standard-Kritikalitätsstufe/Purdue-Level | Beschreibung | Untertypen | |
|---|---|---|---|---|
| IoTs | Gering/3 | Diese Kategorie umfasst verschiedene Arten von miteinander verbundenen Geräten. |  | Kamera |
| | | |  | Panel |
| | | |  | Beamer |
| | | |  | VOIP-Gerät |
| | | |  | 3D-Drucker |
| | | |  | Drucker |
| | | | | USV |

| Kategorie | Standard-Kritikalitätsstufe/Purdue-Level | Beschreibung | Untertypen | |
|---|---|---|---|---|
| | | |  | |

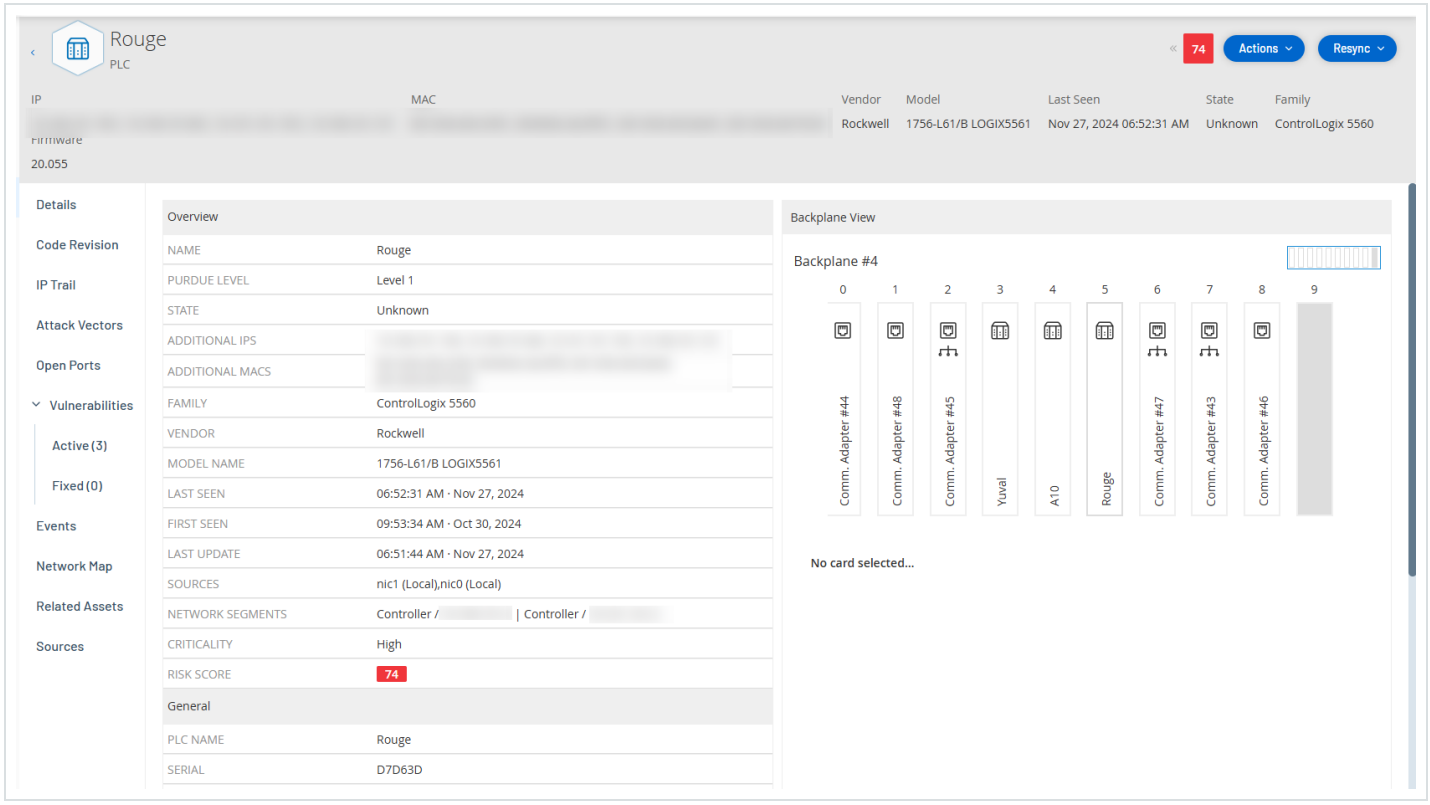
| Kategorie | Standard-Kritikalitätsstufe/Purdue-Level | Beschreibung | Untertypen | |
|---|---|---|---|---|
| | | |  | IP-Telefon |
| | | |  | Intelligenter Sensor |
| | | |  | Barcodescanner |
| | | |  | Zugangskontrollsystem |
| | | |  | Beleuchtungssteuerung |
| | | |  | HLK-Modul |
| | | |  | Intelligenter Hub |
| | | | | Smart-TV |

| Kategorie | Standard-Kritikalitätsstufe/Purdue-Level | Beschreibung | Untertypen | |
|---|---|---|---|---|
| | | |  | |
| | | |  | Medizinisches Gerät |
| | | |  | Tablet |
| | | |  | Mobilgerät |
| | | |  | Speichergerät |
| Endgeräte | Gering/3 | Eine nicht identifizierte IP-Adresse im Netzwerk. |  | Endgerät |

## Asset-Details anzeigen

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager, Sicherheitsanalyst, Site-Operator, Schreibgeschützt

Der Bildschirm Asset-Details zeigt umfassende Details zu allen Daten an, die von OT Security für ein ausgewähltes Asset erfasst wurden. Die Details werden in der Kopfleiste sowie in einer Reihe von Registerkarten und Unterabschnitten angezeigt. Einige Registerkarten und Unterabschnitte sind nur für bestimmte Asset-Typen relevant.




So greifen Sie auf die Seite Asset-Details für ein bestimmtes Asset zu:

1. Führen Sie einen der folgenden Schritte aus:

    - Klicken Sie auf einer dieser Seiten, auf der der Asset-Name als Link angezeigt wird, auf den Asset-Namen: Inventar, Ereignisse oder Netzwerk.

    - Klicken Sie auf der Seite Inventar auf Aktionen > Anzeigen.

Die folgenden Elemente sind im Fenster Asset-Details enthalten (für relevante Asset-Typen):

- Kopfleistenbereich – Zeigt einen Überblick der wichtigen Informationen über das Asset und seinen aktuellen Zustand an. Er enthält auch ein Menü Aktionen, mit dem Sie die Auflistung für

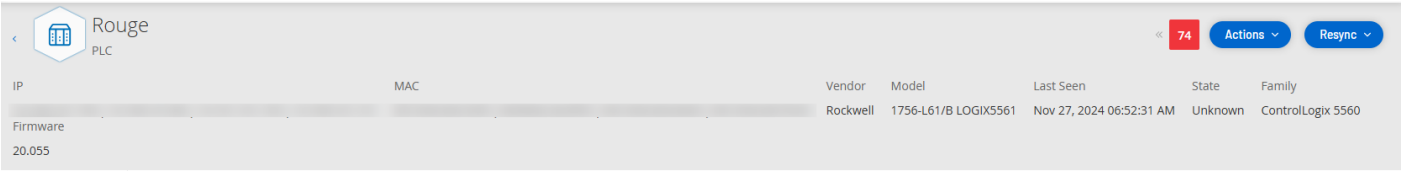
dieses Asset bearbeiten können.

- Details – Zeigt detaillierte Informationen an, die in Unterabschnitte mit spezifischen Daten unterteilt sind, die für verschiedene Asset-Typen relevant sind.
- Coderevisionen (nur für Controller) – Zeigt Informationen zu aktuellen sowie früheren Coderevisionen an, die von der „Snapshot“-Funktion von OT Security ermittelt wurden. Dazu gehören Einzelheiten zu allen spezifischen Änderungen, die am Code vorgenommen wurden, d. h. die Abschnitte (Codeblöcke/Zeilen), die hinzugefügt, gelöscht oder geändert wurden.
- IP-Trail – Zeigt alle aktuellen und historischen IPs an, die sich auf das Asset beziehen.
- Angriffsvektoren – Zeigt anfällige Angriffsvektoren an, d. h. die Routen, die ein Angreifer verwenden kann, um Zugriff auf dieses Asset zu erlangen. Sie können einen Angriffsvektor automatisch generieren, um den kritischsten Angriffsvektor anzuzeigen, oder Sie können Angriffsvektoren aus bestimmten Assets manuell generieren.
- Offene Ports – Zeigt Informationen zu offenen Ports auf dem Asset an.
- Schwachstellen – Zeigt die behobenen und aktiven Schwachstellen an, die das System für das ausgewählte Asset identifiziert hat, wie z. B. veraltete Windows-Betriebssysteme, die Verwendung anfälliger Protokolle und offene Kommunikationsports, die bekanntermaßen riskant oder für bestimmte Gerätetypen nicht wesentlich sind, siehe Schwachstellen.
- Ereignisse – Eine Liste von Ereignissen im Netzwerk, die das Asset betreffen.
- Netzwerkübersicht – Zeigt eine grafische Visualisierung der Netzwerkverbindungen des Assets an.
- Geräte-Ports (für Netzwerk-Switches) – Zeigt Informationen zu Ports auf dem Netzwerk-Switch an.
- Verwandte Assets – Zeigt die Liste aller verschachtelten Assets an.
- Quellen – Zeigt alle Informationen im Zusammenhang mit der Quelle des Assets an, wie z. B. Standort, Typ, die IP- und die MAC-Adresse des Assets sowie den Zeitpunkt der ersten und

der letzten Meldung.

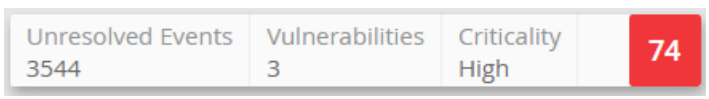
## Kopfleistenbereich

Der Kopfleistenbereich zeigt eine Übersicht über den aktuellen Status des Assets.




Die Anzeige umfasst die folgenden Elemente:

- Name – Der Name des Assets.
- ‹ Link „Zurück“ – Bringt Sie zurück zu dem Bildschirm, von dem aus Sie diesen Asset-Bildschirm aufgerufen haben.
- Asset-Typ – Zeigt das Symbol und den Namen des Asset-Typs an.
- Asset-Übersicht – Zeigt wichtige Informationen über das Asset, einschließlich IPs, Anbieter, Familie, Modell, Firmware und „Zuletzt gesehen“ (Datum und Uhrzeit).
- Risikowert-Widget – Zeigt den Risikowert für das Asset an. Der Risikowert ist eine Bewertung (von 1 bis 100) des Grades der Bedrohung, die für das Asset besteht Eine Erläuterung, wie der Wert bestimmt wird, finden Sie unter Risikobewertung. Klicken Sie auf den Risikowert-Indikator, um ein erweitertes Widget mit einer Aufschlüsselung der Faktoren anzuzeigen, die zur Bewertung der Risikostufe beitragen (nicht aufgelöste Ereignisse, Schwachstellen und Kritikalität). Einige der Elemente sind Links zum entsprechenden Bildschirm, der Details zu diesem Element anzeigt.



- Menü Aktionen – Ermöglicht es Ihnen, die Asset-Details zu bearbeiten oder einen Tenable Nessus-Scan auszuführen.
- Erneut synchronisieren – Klicken Sie auf diese Schaltfläche, um eine oder mehrere der Abfragen, die für dieses Asset verfügbar sind, manuell auszuführen. Siehe Erneute Synchronisierung durchführen.

## Details

Auf der Registerkarte Details werden zusätzliche Details zum ausgewählten Asset angezeigt. Die Informationen sind in Abschnitte unterteilt, die verschiedene Arten von System- und Konfigurationsdaten für das angegebene Asset zeigen. OT Security zeigt nur die Abschnitte an, die für das angegebene Asset relevant sind. Die folgende Liste enthält alle möglichen Abschnittskategorien für verschiedene Asset-Typen: Übersicht, Allgemein, Projekt, Speicher, Ethernet, Profinet, Betriebssystem, System, Hardware, Geräte und Laufwerke, USB-Geräte, Installierte Software, IEC 61850 und Schnittstellenstatus.

> Hinweis: OT Security zeigt nur die Details an, die aus dem Asset extrahiert werden. Möglicherweise werden nicht alle Abschnitte für alle Assets angezeigt. Zum Beispiel Allgemein, Nessus-Scan-Informationen.

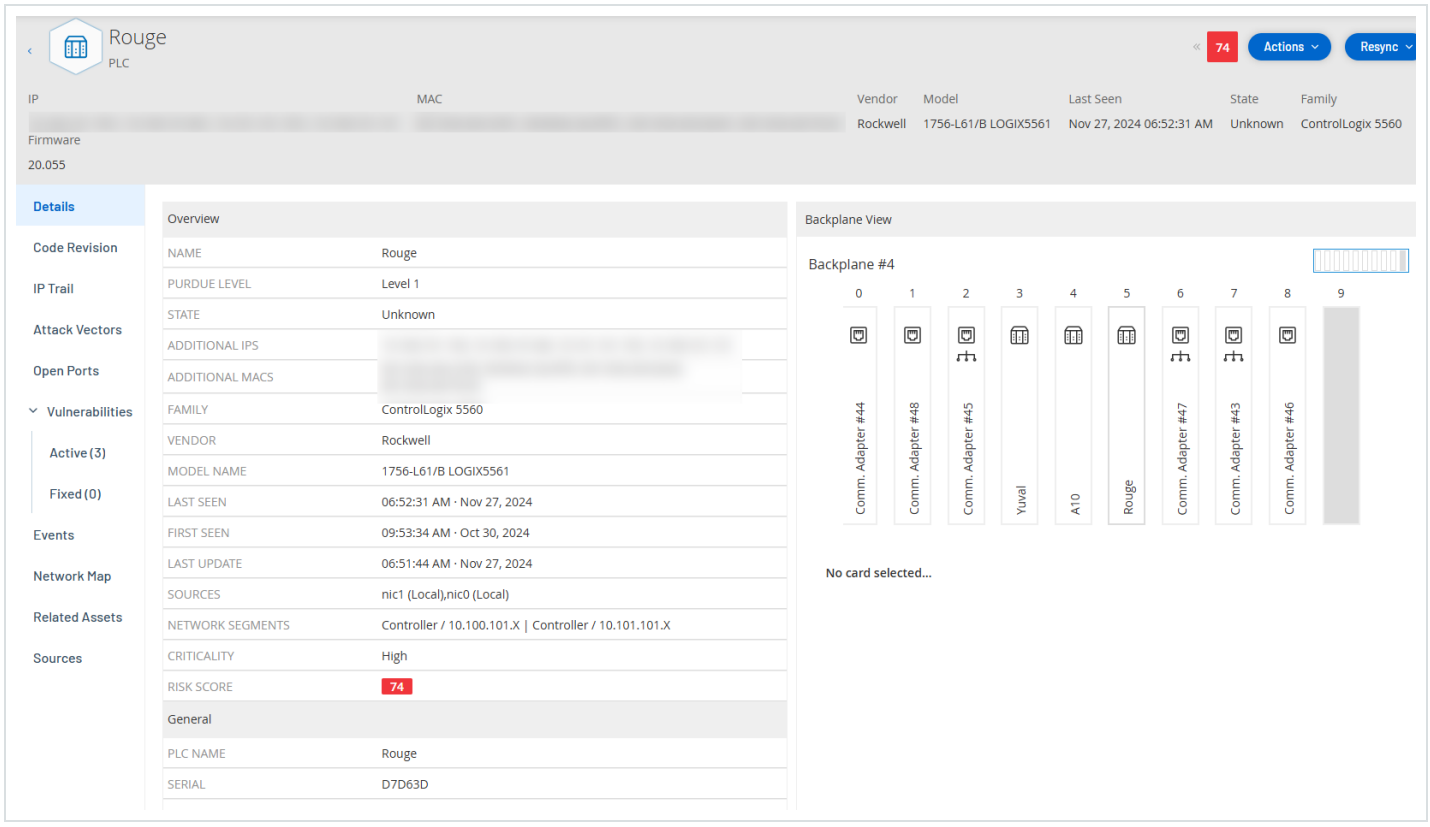
Die folgende Tabelle zeigt die Details im Abschnitt Übersicht:

| Abschnitt | Beschreibung |
|---|---|
| Name | Der Asset-Name, der entweder durch passives Monitoring oder aktives Abfragen erhalten oder automatisch unter Verwendung des Asset-Typs und eines eindeutigen Bezeichners generiert wird. |
| Beschreibung | Die Beschreibung des Assets vom Benutzer. |
| Purdue-Level | Das Purdue-Modell-Level, das dem Asset zugewiesen ist. |

| Abschnitt | Beschreibung |
| --- | --- |
| Status | Der aktuelle Betriebsstatus des Assets. Das Feld ist für bestimmte Asset-Typen relevant, in der Regel Controller. |
| Direkte IP | Die IP-Adresse, die auf diesem spezifischen Asset oder Modul vorhanden oder für dieses konfiguriert ist. |
| Direkte Mac | Die Mac-Adresse, die auf diesem spezifischen Asset oder Modul physisch vorhanden oder für dieses konfiguriert ist. |
| Zusätzliche IPs | IP-Adressen, die mit anderen Modulen verknüpft sind, die eine Backplane oder eine ähnliche Infrastruktur mit dem Asset gemeinsam nutzen, und für den indirekten Zugriff auf das Asset verwendet werden.<br><br>Beispielsweise verfügt eine SPS (Controller-Modul) möglicherweise nicht über eine eigene Netzwerkschnittstelle und der Zugriff erfolgt über eine IP-Adresse, die auf einem Kommunikationsmodul konfiguriert ist, das in einem anderen Steckplatz installiert ist. Beachten Sie, dass das Asset möglicherweise auch über andere Verbindungen als eine Backplane verfügt. |
| Zusätzliche Macs | Mac-Adressen, die mit anderen Modulen verknüpft sind, die eine Backplane oder eine ähnliche Infrastruktur gemeinsam nutzen, und für den indirekten Zugriff auf das Asset verwendet werden. |
| Familie | Die Gerätefamilie oder Produktreihe, zu der das Asset gehört. |
| Anbieter | Der Hersteller oder Anbieter des Assets. |
| Modellname | Die spezifische Modellnummer des Assets. |
| Zuletzt gesehen | Das Datum und die Uhrzeit, zu der OT Security das Asset zuletzt erfasst hat. |

| Abschnitt | Beschreibung |
|---|---|
| | OT Security kann dieses Feld aktualisieren, wenn eine PCAP-Datei (Traffic-Capture-Datei) wiedergegeben oder eine ähnliche Analyse durchgeführt wird. |
| Zum ersten Mal gesehen | Das Datum und die Uhrzeit, zu der das Asset zum ersten Mal erkannt wurde. Dies kann dem Wert Zuletzt gesehen entsprechen oder davor liegen. |
| Letzte Aktualisierung | Das Datum und die Uhrzeit der letzten Aktualisierung von Asset-Details.<br><br>Hinweis: Bei jeder manuellen Änderung an den Asset-Informationen, wie z. B. eine Aktualisierung der Beschreibung, wird dieser Wert aktualisiert, unabhängig davon, ob das Asset derzeit aktiv ist oder vor Kurzem erkannt wurde. |
| Quellen | Die Quellen (z. B. Sensoren, PCAPs, lokale Schnittstellen), die identifiziert wurden oder mit dem Asset verbunden sind. |
| Netzwerksegmente | Die Netzwerksegmente, die dem Asset zugewiesen oder mit ihm verknüpft sind. |
| Kritikalität | Die Wichtigkeit des Assets, die als hoch, mittel oder gering bewertet wird. |
| Risikowert | Spiegelt die potenziellen Auswirkungen des mit dem Asset verbundenen Risikos wider. Die Bewertung wird durch Faktoren wie Kritikalität, Schwachstellen, nicht aufgelöste Ereignisse (und ihre Dauer), zugehörige Assets (z. B. über Backplane) und andere relevante Überlegungen beeinflusst. |
| Tags | Die mit dem Asset verknüpften Tags. Siehe Asset-Gruppen und Tags. |

## Backplane-Ansicht




Für Assets, die mit einer Backplane verbunden sind, gibt es auch einen Abschnitt Backplane-Ansicht, der eine grafische Darstellung der Backplane-Konfiguration zeigt, einschließlich der Steckplatzposition jedes angeschlossenen Geräts. Wählen Sie ein Gerät aus, um seine Details im unteren Bereich anzuzeigen.

## Nessus-Scan-Informationen

Die Nessus-Scan-Informationen helfen Ihnen bei Folgendem:

- Bewertete und nicht bewertete Assets zu verstehen
- Nachzuvollziehen, ob auf Ihre Assets Credentialed-Scans oder Non-Credentialed-Scans angewendet werden

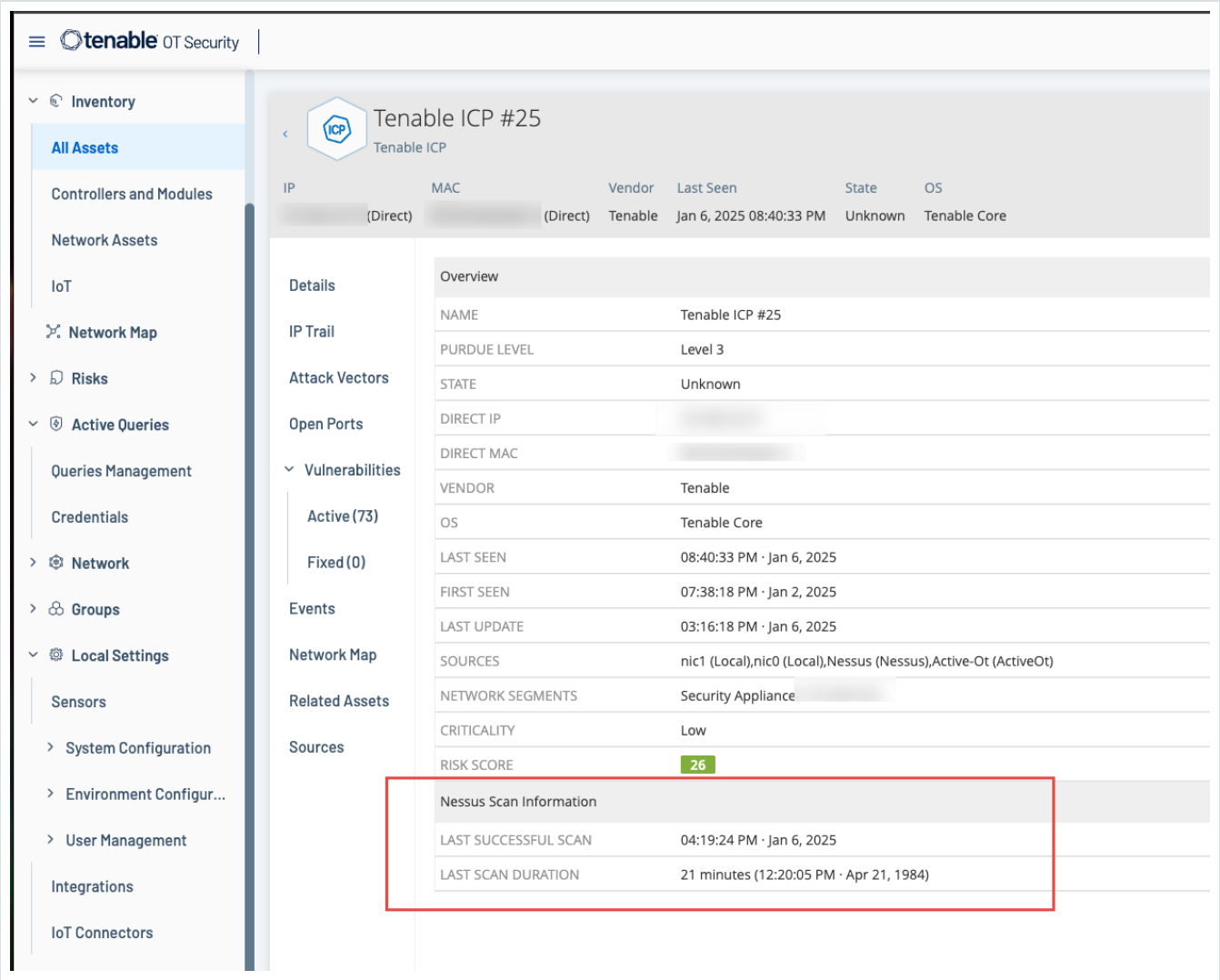
- Bei Scans und Schwachstellen-Management Best Practices anzuwenden. Beispielsweise können Sie Schwachstellenbewertungs-Scans für IT-Assets durchführen, auf denen Windows oder Linux ausgeführt wird. Scans, egal ob mit oder ohne Zugangsdaten, geben Aufschluss darüber, wie stark die Angriffsfläche Ihrer Organisation sowohl intern als auch extern gefährdet ist.

Weitere Informationen zu Nessus-Scans finden Sie unter Nessus-Plugin-Scans erstellen.

Im Abschnitt Nessus-Scan-Informationen auf der Seite Details werden die folgenden Details angezeigt:

- Letzter erfolgreicher Scan
- Letzter authentifizierter Scan

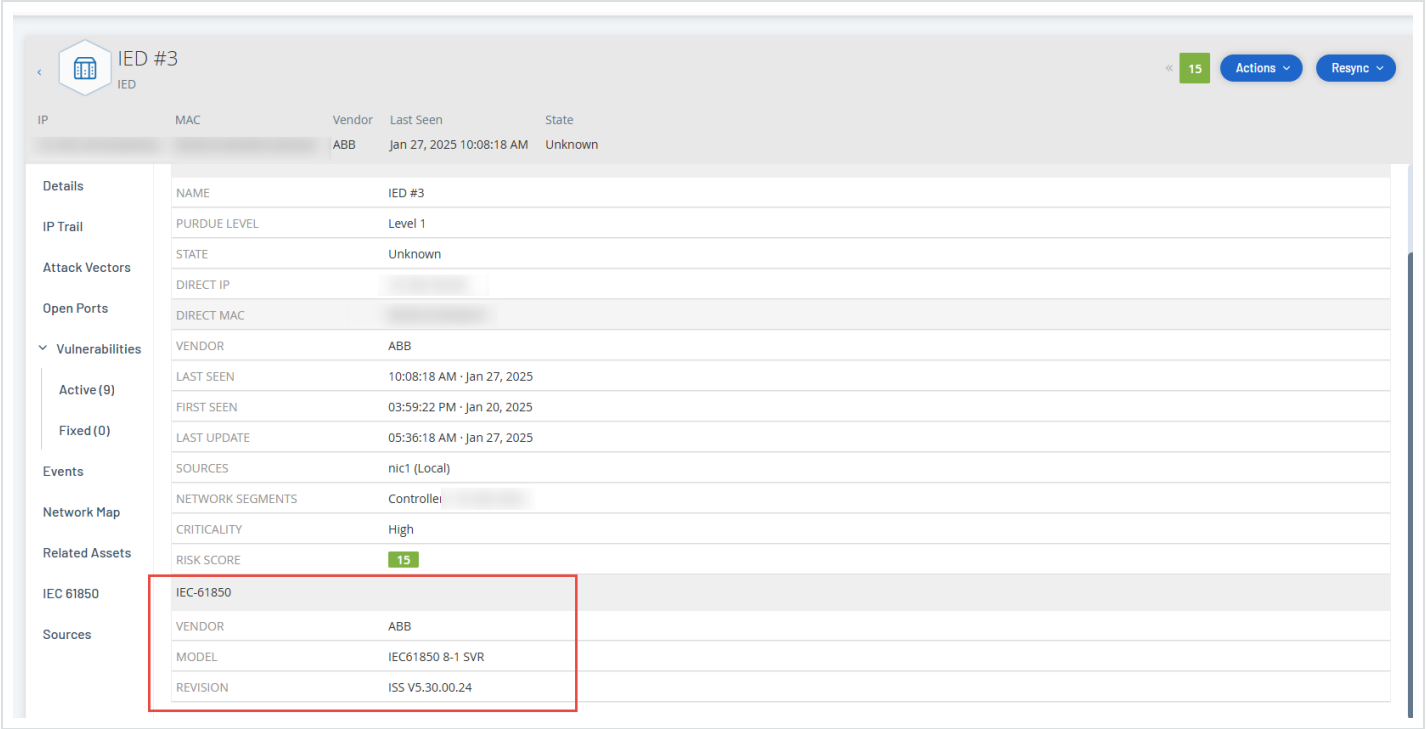
- Dauer des letzten Scans




## IEC 61850

Im Abschnitt „IEC 61850“ auf der Seite Details wird die folgende Konfiguration für das spezifische IED-Asset angezeigt.

- Anbieter
- Modell
- Revision

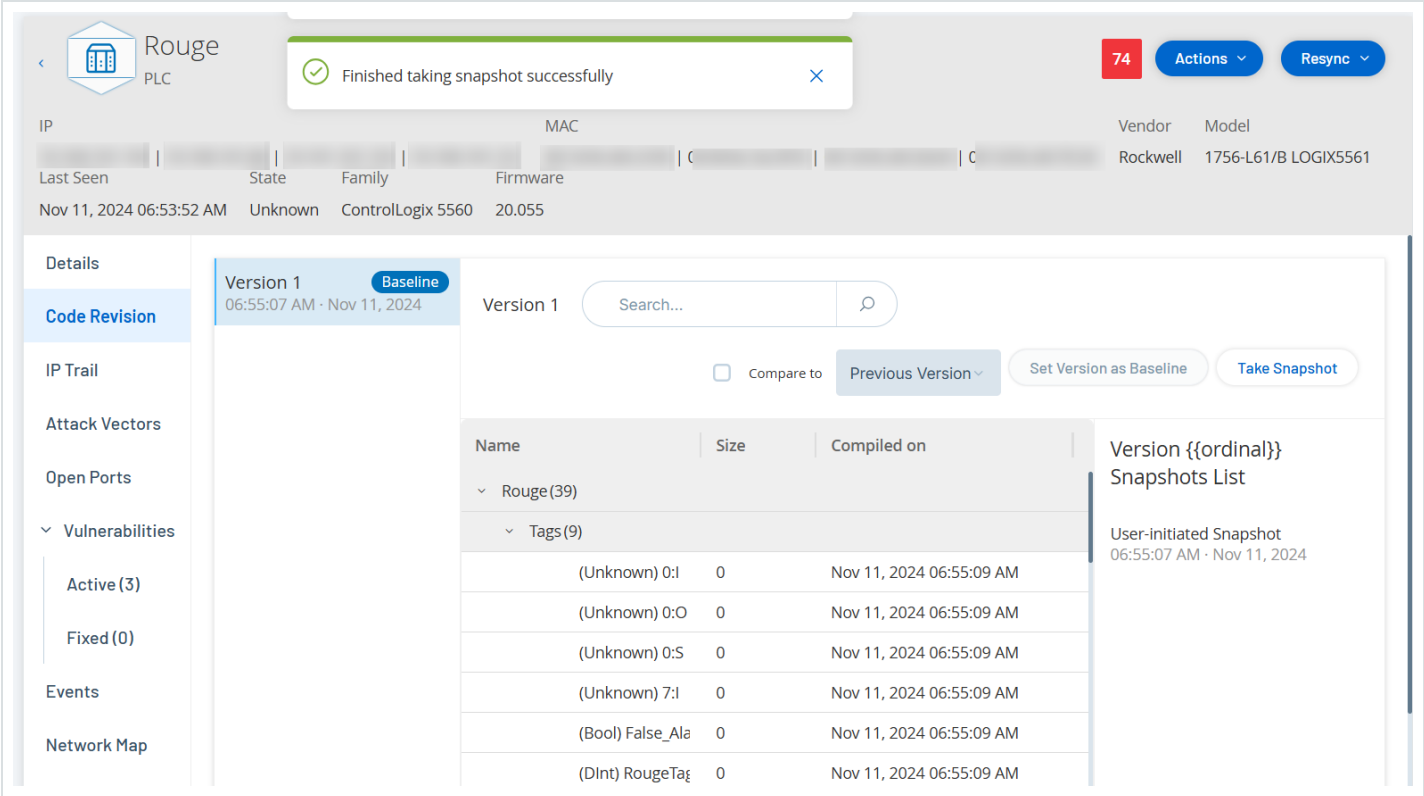



Weitere Informationen zu den SCD-Dateien finden Sie hier:

- SCD-Dateien
- IEC 61850

## Coderevisionen

Die Registerkarte Coderevision (nur für Controller) zeigt die verschiedenen Versionen des Controller-Codes, die von OT Security-„Snapshots“ erfasst wurden. Jede „Snapshot“-Version enthält Informationen über die Coderevision zum Zeitpunkt der Erstellung des Snapshot, einschließlich Details zu bestimmten Abschnitten (Codeblöcken/Zeilen) und Tags. Immer wenn ein Snapshot nicht mit dem vorherigen Snapshot dieses Controllers identisch ist, wird eine neue Version der Coderevision erstellt. Sie können die einzelnen Versionen miteinander vergleichen, um zu sehen, welche Änderungen am Controller-Code vorgenommen wurden.



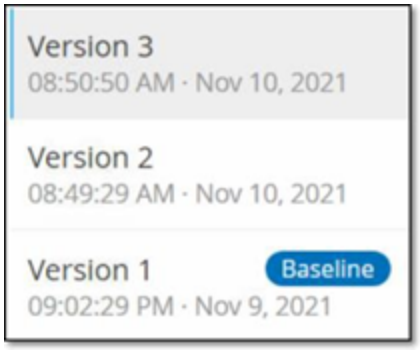

Ein Snapshot kann auf folgende Weise ausgelöst werden:

- Routine – Snapshots werden in regelmäßigen Abständen erstellt, wie vom Benutzer im Bildschirm mit Systemeinstellungen festgelegt.
- Durch Aktivität – Das System löst einen Snapshot aus, wenn eine bestimmte Code-Aktivität erkannt wird (z. B. ein Code-Download).
- Durch Benutzer – Der Benutzer kann einen Snapshot manuell auslösen, indem er auf die Schaltfläche „Snapshot erstellen“ für ein bestimmtes Asset klickt.

Sie können eine Richtlinie für Snapshot-Konflikte konfigurieren, um Ergänzungen, Löschungen oder Änderungen am Code eines Controllers zu erkennen, siehe Konfigurationsereignis – Typen von Controller-Aktivitätsereignissen.

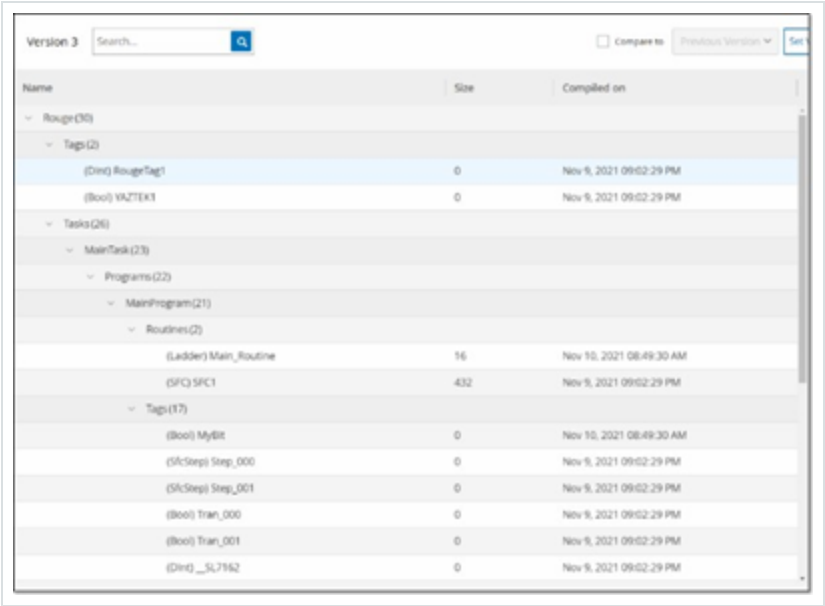
In den folgenden Abschnitten werden die verschiedenen Abschnitte der Coderevisionsanzeige sowie der Vergleich verschiedener „Snapshot“-Versionen beschrieben.

## Bereich „Versionsauswahl“



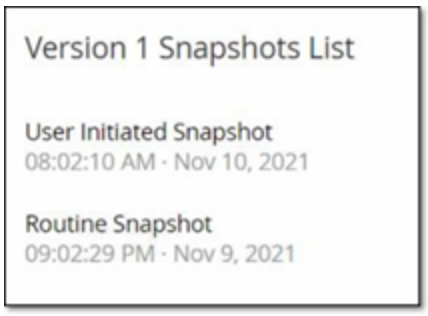

Dieser Bereich zeigt eine Liste aller verfügbaren Versionen der Coderevision für diesen Controller. Für jede Version wird die Startzeit angezeigt, zu der die Version nachweislich in Kraft war. Eine neue Version wird jedes Mal erstellt, wenn eine Änderung gegenüber dem vorherigen „Snapshot“ erkannt wird. Das Tag „Baseline“ gibt an, welche Version aktuell als Baseline-Version für Vergleichszwecke festgelegt ist. Wählen Sie eine Version aus, um ihre Coderevisionen im Bereich „Snapshot-Details“ anzuzeigen.

## Bereich „Snapshot-Details“



Der Detailbereich zeigt detaillierte Informationen zu den spezifischen Codeblöcken, Zeilen und Tags für die ausgewählte Snapshot-Version. Die Codeelemente werden in einer Baumstruktur mit Pfeilen zum Erweitern/Minimieren der angezeigten Details angezeigt. Für jedes Element werden der Name, die Größe und das Erstellungsdatum angezeigt. Sie können die ausgewählte Version mit der vorherigen Version oder mit der „Baseline“-Version vergleichen, um zu sehen, welche Änderungen vorgenommen wurden, siehe Snapshot-Versionen vergleichen.

### Bereich „Versionsverlauf“




Dieser Bereich zeigt Details über den Snapshot, mit dem die ausgewählte Version erfasst wurde, einschließlich der Methode, mit der er initiiert wurde, sowie Datum und Uhrzeit der Erfassung.

Wenn zwischen den Snapshots keine Änderungen vorgenommen wurden, werden mehrere Snapshots zu einer einzigen Version zusammengefasst. Alle identischen Snapshots werden im Bereich für den Snapshot-Verlauf für die betreffende Version aufgelistet.

### Snapshot-Versionen vergleichen

Sie können eine Snapshot-Version entweder mit der vorherigen Version oder mit der Baseline-Version vergleichen. Nachdem ein Vergleich ausgeführt wurde, zeigt der Bereich „Snapshot-Details“ die Änderungen an, die zwischen den beiden Snapshots am Code des Controllers vorgenommen wurden.

Änderungen werden wie folgt gekennzeichnet:

✚ Hinzugefügt – Neuer Code, der in der ausgewählten Version hinzugefügt wurde.

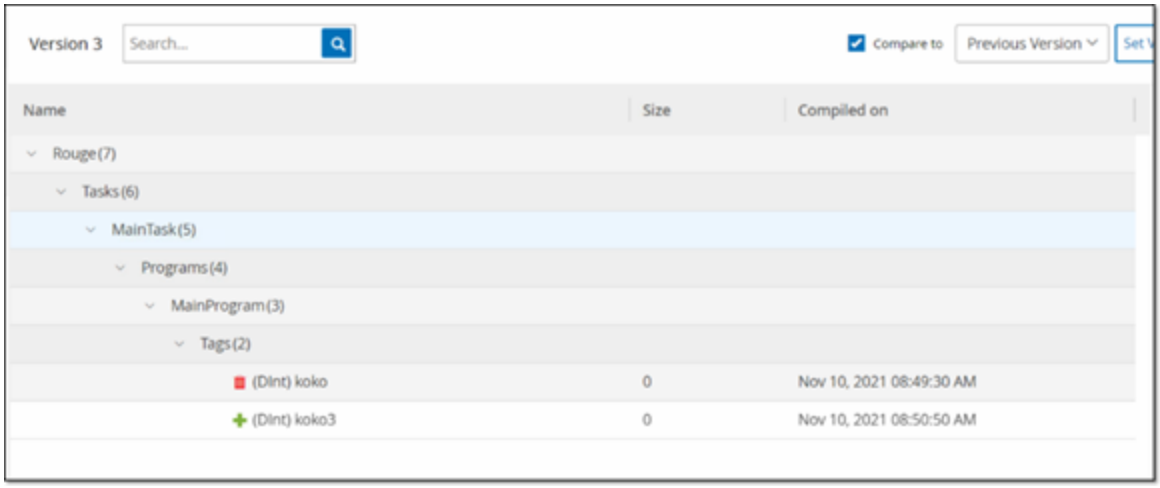
🗑 Gelöscht – Code, der aus der ausgewählten Version gelöscht wurde.

Bearbeitet – Code, der in der ausgewählten Version bearbeitet wurde.

So vergleichen Sie eine Snapshot-Version mit der vorherigen Version:

1. Wählen Sie im Bildschirm Inventar > Controller den gewünschten Controller aus.
2. Klicken Sie auf die Registerkarte Coderevision.
3. Wählen Sie im Bereich Versionsauswahl die Version aus, die Sie analysieren möchten.
4. Wählen Sie oben im Bereich Snapshot-Details im Vergleichsfeld Vorherige Version aus dem Dropdown-Menü aus.
5. Klicken Sie auf das Kontrollkästchen Vergleichen mit.

   Der Bereich „Snapshot-Details“ zeigt alle Unterschiede zwischen den beiden Versionen. Für jede Änderung gibt ein Symbol die Art der aufgetretenen Änderung an.




So vergleichen Sie eine Snapshot-Version mit einer früheren Version (nicht der vorherigen Version):

1. Wählen Sie im Bildschirm Inventar > Controller den gewünschten Controller aus.
2. Klicken Sie auf die Registerkarte Coderevision.

3. Wählen Sie im Bereich Versionsauswahl die Version aus, die Sie als Baseline für den Vergleich verwenden möchten.
4. Klicken Sie oben im Bereich Snapshot-Details auf Version als Baseline festlegen.

   Das Baseline-Tag wird für die ausgewählte Version angezeigt, was darauf hinweist, dass sie als Baseline-Version festgelegt ist.

   > Hinweis: Die Festlegung einer Version als Baseline wirkt sich nur auf Vergleiche aus, die mithilfe dieses Bildschirms durchgeführt werden. Sie wirkt sich nicht auf Richtlinien aus, die auf Snapshot-Konflikt prüfen.

5. Wählen Sie im Bereich Versionsauswahl die Version aus, die Sie mit der Baseline vergleichen möchten.
6. Klicken Sie auf das Kontrollkästchen Vergleichen mit.
7. Wählen Sie im Feld neben dem Kontrollkästchen Vergleichen mit die Option Baseline-Version aus dem Dropdown-Menü aus.

   Der Bereich Snapshot-Details zeigt alle Unterschiede zwischen den beiden Versionen. Für jede Änderung gibt ein Symbol die Art der aufgetretenen Änderung an.

## Snapshot erstellen

Sie können einen Snapshot manuell initiieren. Tenable empfiehlt, vor und nach der Wartung eines Controllers durch einen Techniker einen Snapshot zu erstellen.

### So erstellen Sie einen Snapshot eines Controllers:

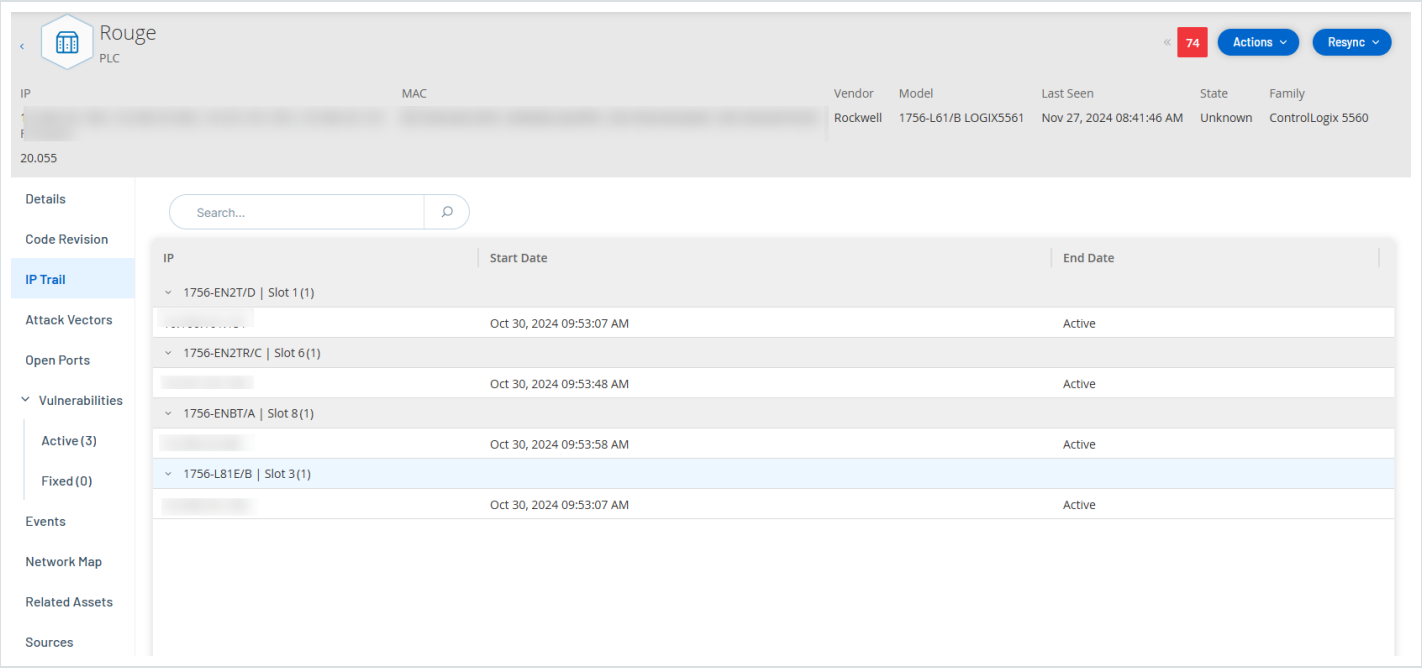
1. Wählen Sie im Bildschirm Inventar > Controller den gewünschten Controller aus.
2. Klicken Sie auf die Registerkarte Coderevision.
3. Klicken Sie in der oberen rechten Ecke des Bereichs Snapshot-Details auf Snapshot erstellen.

   Der vom Benutzer initiierte Snapshot wird erstellt.

Wenn keine Änderungen festgestellt werden, wird ein neuer vom Benutzer identifizierter Snapshot für die neueste Version zum Bereich „Revisionsverlauf“ hinzugefügt. Wenn Änderungen festgestellt werden, wird eine neue Version erstellt, die die Änderungen der Coderevision zeigt.

## IP-Trail

Die Registerkarte IP-Trail zeigt alle IPs, die für dieses Asset relevant sind. Die Spalte „Netzwerkkarte“ zeigt eine Liste der Netzwerkkarten, die von diesem Asset verwendet werden. Klicken Sie auf den Pfeil neben einer Netzwerkkarte, um die Liste zu erweitern und die IPs aller Assets anzuzeigen, die mit der gemeinsam genutzten Backplane verbunden sind.




Die Listen enthalten das Start- und Enddatum der Nutzung der IP-Adresse. Die Optionen für das Enddatum sind:

- Aktiv – Die IP-Adresse wird derzeit für dieses Asset verwendet.
- {Datum/Uhrzeit} – Das letzte Datum und die letzte Uhrzeit, an dem bzw. zu der die IP-Adresse für dieses Asset aktiv war (wenn sie innerhalb der letzten 30 Tage aktiv war).

- {Datum/Uhrzeit} (Inaktiv) – Das letzte Datum und die letzte Uhrzeit, an dem bzw. zu der die IP-Adresse für dieses Asset aktiv war (wenn sie mindestens 30 Tage lang inaktiv war).
- Inaktiv – Die IP-Adresse wird von einem anderen Asset verwendet.

## Angriffsvektoren

Ein Angreifer kann ein kritisches Asset kompromittieren, indem er einen verwundbaren „Schwachpunkt“ im Netzwerk ausnutzt, um Zugang zu dem kritischen Asset zu erhalten. Das kritische Asset ist das Ziel des Angriffs und der Angriffsvektor ist die Route, die der Angreifer nutzt, um sich Zugriff auf das Asset zu verschaffen.

### Wie wird ein Angriffsvektor bestimmt?

Sobald das Ziel-Asset festgelegt ist, berechnet das System alle potenziellen Angriffsvektoren, die den Zugriff auf dieses Asset ermöglichen könnten, und identifiziert den Pfad, der das höchste Risikopotenzial für die Kompromittierung dieses Assets aufweist. Bei der Berechnung werden mehrere Parameter berücksichtigt und ein risikobasierter Ansatz verwendet, um den kritischsten Angriffsvektor zu bestimmen. Zu den Parametern gehören:

- Asset-Risikostufe
- Länge des Angriffspfads
- Methode der Kommunikation zwischen Assets
- Externe Kommunikation (Internet/Unternehmensnetz) vs. interne Kommunikation

### Empfohlene Schritte zur Risikominderung

Um das Risiko eines potenziellen Angriffs über den ausgewählten Vektor zu minimieren, werden u. a. folgende Schritte zur Risikominderung empfohlen:

- Verringerung der verbundenen und individuellen Risikowerte der Assets, die in dem Angriffsvektor enthalten sind.
- Minimierung oder Entfernung des Zugangs zu externen Netzwerken (Internet oder Unternehmensnetzwerke).
- Untersuchung der Kommunikationswege entlang der Kette und Prüfung ihrer Relevanz für den Prozess. Wenn sie nicht unbedingt notwendig sind, sollten sie entfernt werden (z. B. Schließen von Ports oder Entfernen von Diensten), um den potenziellen Angriffspfad zu beseitigen.

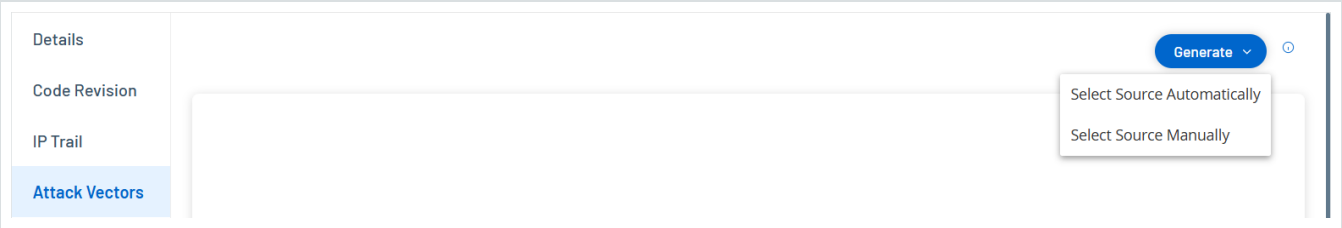
### Angriffsvektoren generieren

Angriffsvektoren müssen für jedes relevante Ziel-Asset manuell generiert werden. Dies erfolgt auf der Registerkarte „Angriffsvektoren“ für das gewünschte Ziel-Asset. Es gibt zwei Methoden zum Generieren von Angriffsvektoren:

- Automatisch – OT Security bewertet alle potenziellen Angriffsvektoren und identifiziert den anfälligsten Pfad.
- Manuell – Sie geben ein bestimmtes Quell-Asset an, und OT Security zeigt Ihnen den potenziellen Pfad (sofern vorhanden), der für den Zugriff auf Ihr Ziel-Asset verwendet werden kann.

### So generieren Sie einen automatischen Angriffsvektor:

1. Navigieren Sie zur Seite Asset-Details für das gewünschte Ziel-Asset und klicken Sie auf die Registerkarte Angriffsvektor.
2. Klicken Sie auf Generieren und dann in der Dropdown-Liste auf Quelle automatisch auswählen.

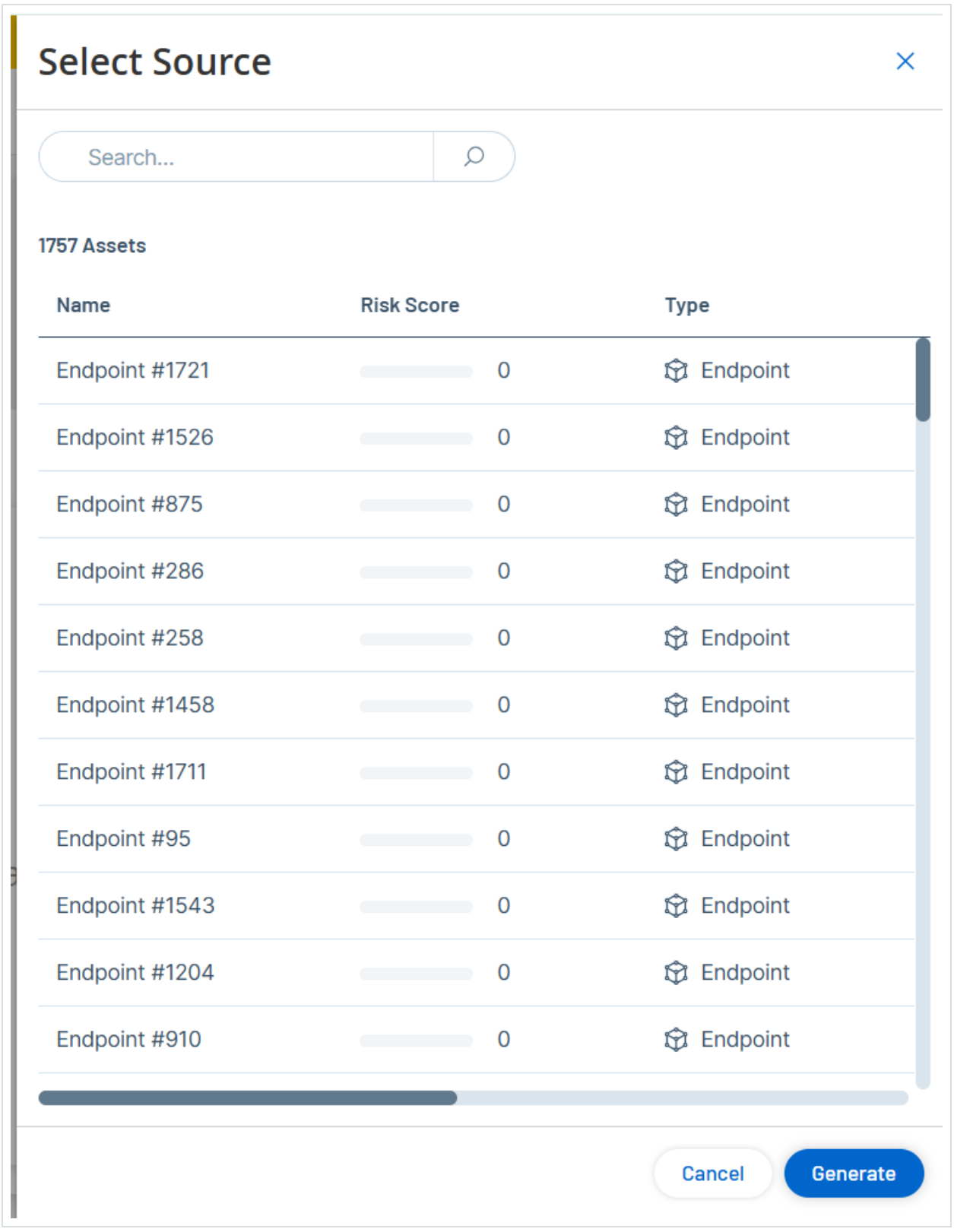



Der Angriffsvektor wird automatisch generiert und auf der Registerkarte Angriffsvektor angezeigt.

So generieren Sie einen manuellen Angriffsvektor:

1. Navigieren Sie zur Seite Asset-Details für das gewünschte Ziel-Asset und klicken Sie auf die Registerkarte Angriffsvektor.
2. Klicken Sie auf Generieren und dann in der Dropdown-Liste auf Quelle manuell auswählen.

   Das Fenster Quelle auswählen wird angezeigt.

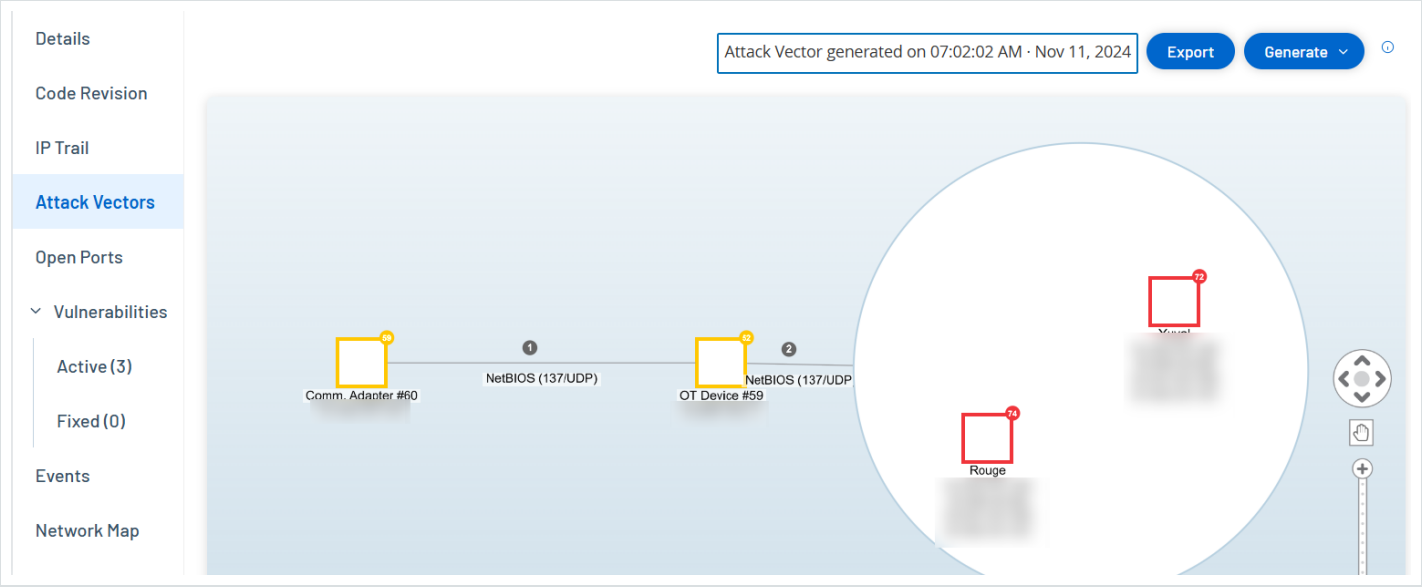

Select Source
Search...
1757 Assets
Name
Risk Score
Type
Endpoint #1721 0 Endpoint
Endpoint #1526 0 Endpoint
Endpoint #875 0 Endpoint
Endpoint #286 0 Endpoint
Endpoint #258 0 Endpoint
Endpoint #1458 0 Endpoint
Endpoint #1711 0 Endpoint
Endpoint #95 0 Endpoint
Endpoint #1543 0 Endpoint
Endpoint #1204 0 Endpoint
Endpoint #910 0 Endpoint
Cancel
Generate

> Hinweis: Standardmäßig werden die Quell-Assets nach Risikowert sortiert. Sie können die Anzeigeeinstellungen anpassen oder nach dem gewünschten Asset suchen.

3. Wählen Sie das gewünschte Quell-Asset aus.
4. Klicken Sie auf Generieren.

   Der Angriffsvektor wird generiert und auf der Registerkarte Angriffsvektor angezeigt.

## Anzeigen von Angriffsvektoren




Die Registerkarte „Angriffsvektoren“ zeigt ein Diagramm des zuletzt generierten Angriffsvektors für das angegebene Ziel-Asset. Das Feld neben der Schaltfläche „Generieren“ zeigt Datum und Uhrzeit der Generierung des angezeigten Angriffsvektors an. Das Angriffsvektor-Diagramm umfasst die folgenden Elemente:

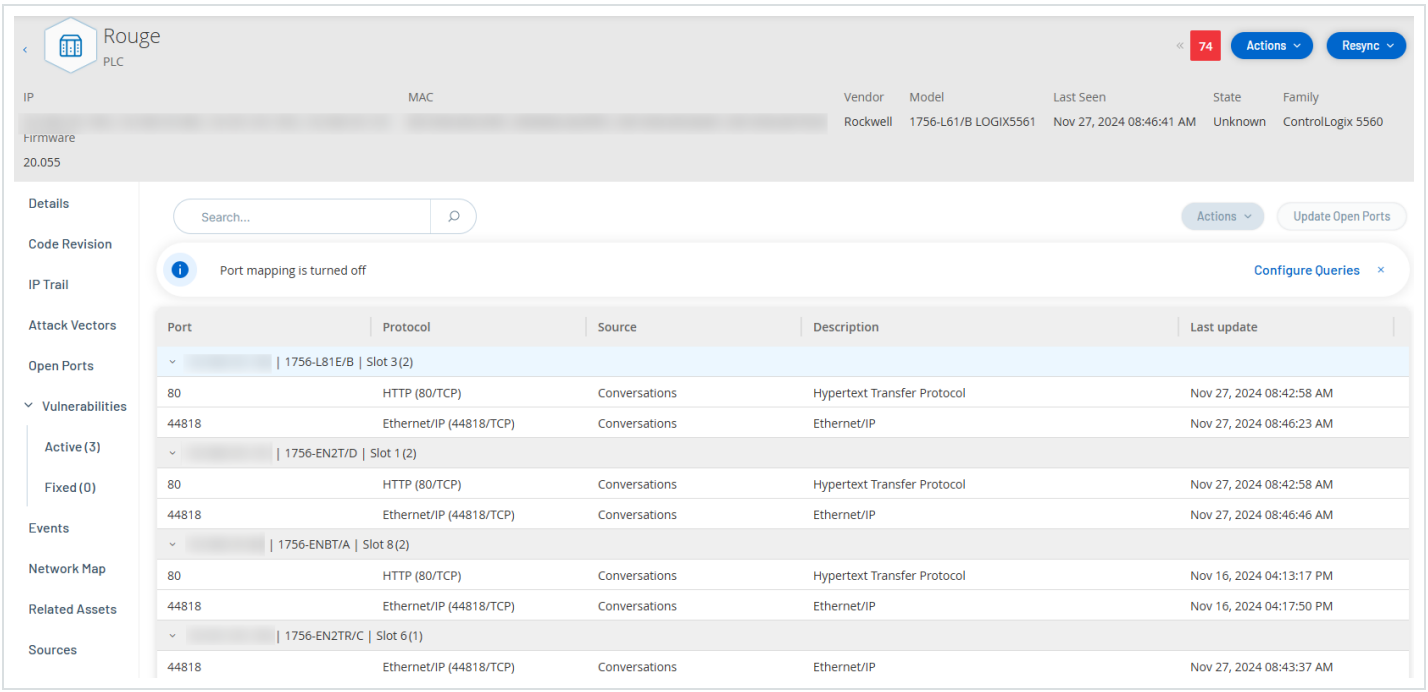
- Für jedes Asset, das im Angriffsvektor enthalten ist, werden die Risikostufe und die IP-Adressen angezeigt. Klicken Sie auf ein Asset-Symbol, um weitere Details zu seinen Risikofaktoren anzuzeigen.
- Für jede Netzwerkverbindung wird das Kommunikationsprotokoll angezeigt.

- Bei Assets, die eine Backplane gemeinsam nutzen, sind die Assets von einem Kreis umgeben.

> Hinweis: Klicken Sie auf die Hilfe-Schaltfläche in der oberen rechten Ecke der Registerkarte „Angriffsvektoren“, um eine Erklärung der Angriffsvektor-Funktion zu erhalten.

## Offene Ports

Die Registerkarte Offene Ports zeigt eine Liste der offenen Ports auf diesem Asset. Für jeden offenen Port werden Details zum verwendeten Protokoll, eine Beschreibung seiner Funktion, Datum und Uhrzeit der letzten Aktualisierung der Daten sowie die Informationsquelle (aktive Abfragen, Port-Zuordnung, Konversationen, Tenable Network Monitor- oder Tenable Nessus-Scans) angegeben, die angezeigt hat, dass der Port offen ist. Für jede IP-Adresse, die dem Asset zur Verfügung steht, wird eine separate Liste der offenen Ports angezeigt (einschließlich der Ports, auf die über eine gemeinsam genutzte Backplane zugegriffen wird). Klicken Sie auf den Pfeil neben einer IP-Adresse, um die Liste zu erweitern und ihre offenen Ports anzuzeigen.



Es gibt einen automatischen Zeitraum, nach dem offene Ports als veraltet gelten, nach dessen Ablauf ein Eintrag eines offenen Ports automatisch aus der Liste gelöscht wird, wenn kein weiterer Hinweis darauf eingegangen ist, dass der Port noch offen ist. Der Standardzeitraum beträgt zwei Wochen. Informationen zur Anpassung der Länge des Zeitraums, nach dem offene Ports als veraltet gelten, finden Sie unter Geräte.

Die Parameter für das Scannen offener Ports werden unter Aktive Abfragen konfiguriert. Sie können auch eine manuelle Abfrage des ausgewählten Assets ausführen, um die Liste der offenen Ports zu aktualisieren.

### Offene Ports aktualisieren

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager, Sicherheitsanalyst, Site-Operator

### So aktualisieren Sie die Liste der offenen Ports manuell:

1. Wählen Sie im Bildschirm Inventar > Controller/Netzwerk-Assets das gewünschte Asset aus.

   Der Bildschirm Asset-Details wird angezeigt.

2. Klicken Sie auf die Registerkarte Offene Ports.

3. Klicken Sie in der oberen rechten Ecke des Bereichs „Offene Ports“ auf Offene Ports aktualisieren.

   Es wird ein neuer Scan ausgeführt, der die für diesen Controller angezeigten offenen Ports aktualisiert.

### Zusätzliche Aktionen auf der Registerkarte „Offene Ports“

Auf der Registerkarte „Offene Ports“ für ein bestimmtes Asset können Sie die folgenden weiteren Aktionen für einen bestimmten offenen Port durchführen.

- Scannen – Führen Sie einen Scan des ausgewählten Ports durch.
- Anzeigen – Zeigt zusätzliche Gerätedetails und Diagnosen durch Zugriff auf die Webschnittstelle des Geräts.

Scan ausführen

### So führen Sie einen Scan auf einem bestimmten Port aus:

1. Wählen Sie im Bildschirm Inventar > Controller/Netzwerk-Assets das gewünschte Asset aus.

   Der Bildschirm Asset-Details wird angezeigt.
2. Klicken Sie auf die Registerkarte Offene Ports.
3. Wählen Sie einen bestimmten Port aus.
4. Klicken Sie auf das Menü Aktionen.
5. Wählen Sie im Dropdown-Menü Scannen aus.

   OT Security führt einen Scan auf dem ausgewählten Port durch.

Asset-Portal anzeigen

### So zeigen Sie das Portal für das Asset an:

> Hinweis: Diese Option ist nur verfügbar, wenn Port 80 (für den Webzugriff verwendet) einer der offenen Ports ist.

1. Wählen Sie im Bildschirm Inventar > Controller/Netzwerk-Assets das gewünschte Asset aus.

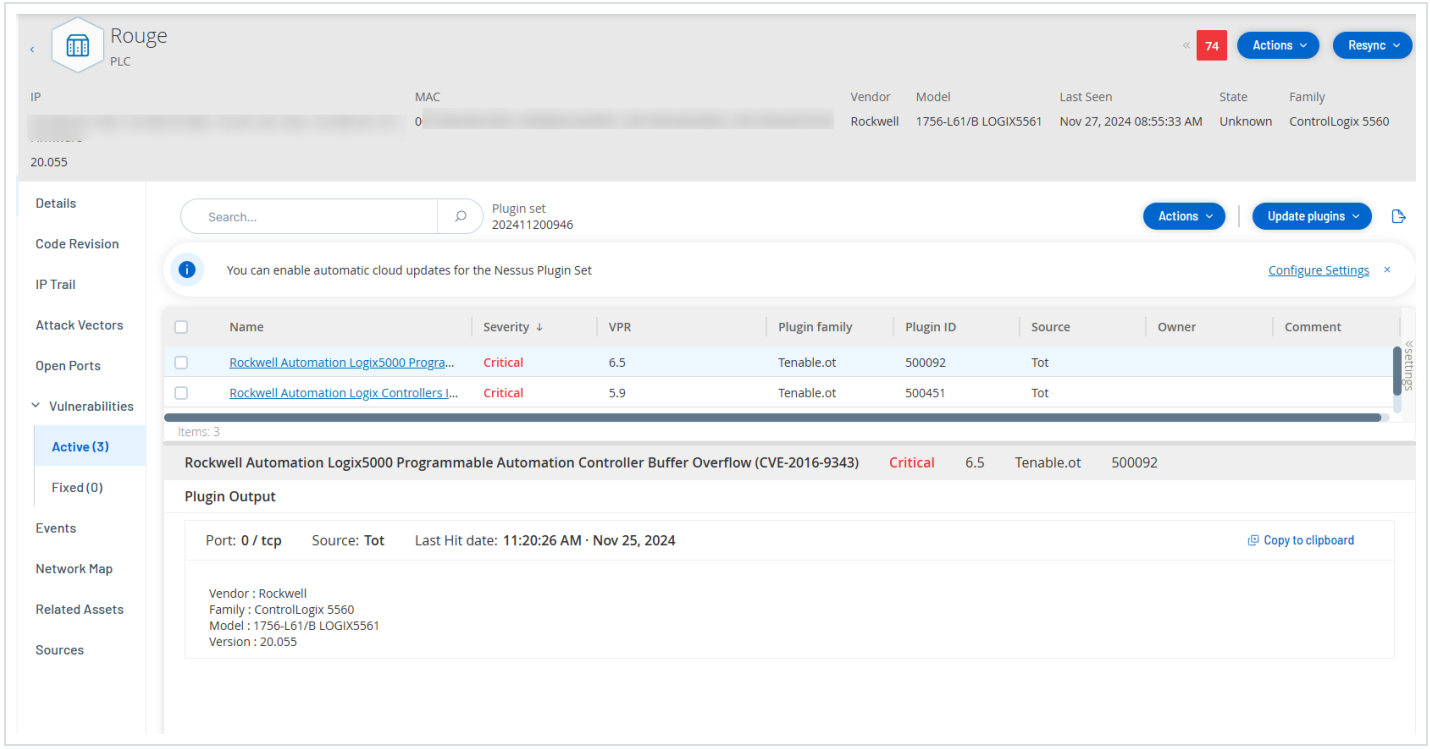
   Der Bildschirm Asset-Details wird angezeigt.
2. Klicken Sie auf die Registerkarte Offene Ports.
3. Wählen Sie einen bestimmten Port aus.
4. Klicken Sie auf das Menü Aktionen.

5. Wählen Sie im Dropdown-Menü Anzeigen aus.

   Eine neue Browser-Registerkarte wird geöffnet, die das Asset-Portal für dieses Asset anzeigt.

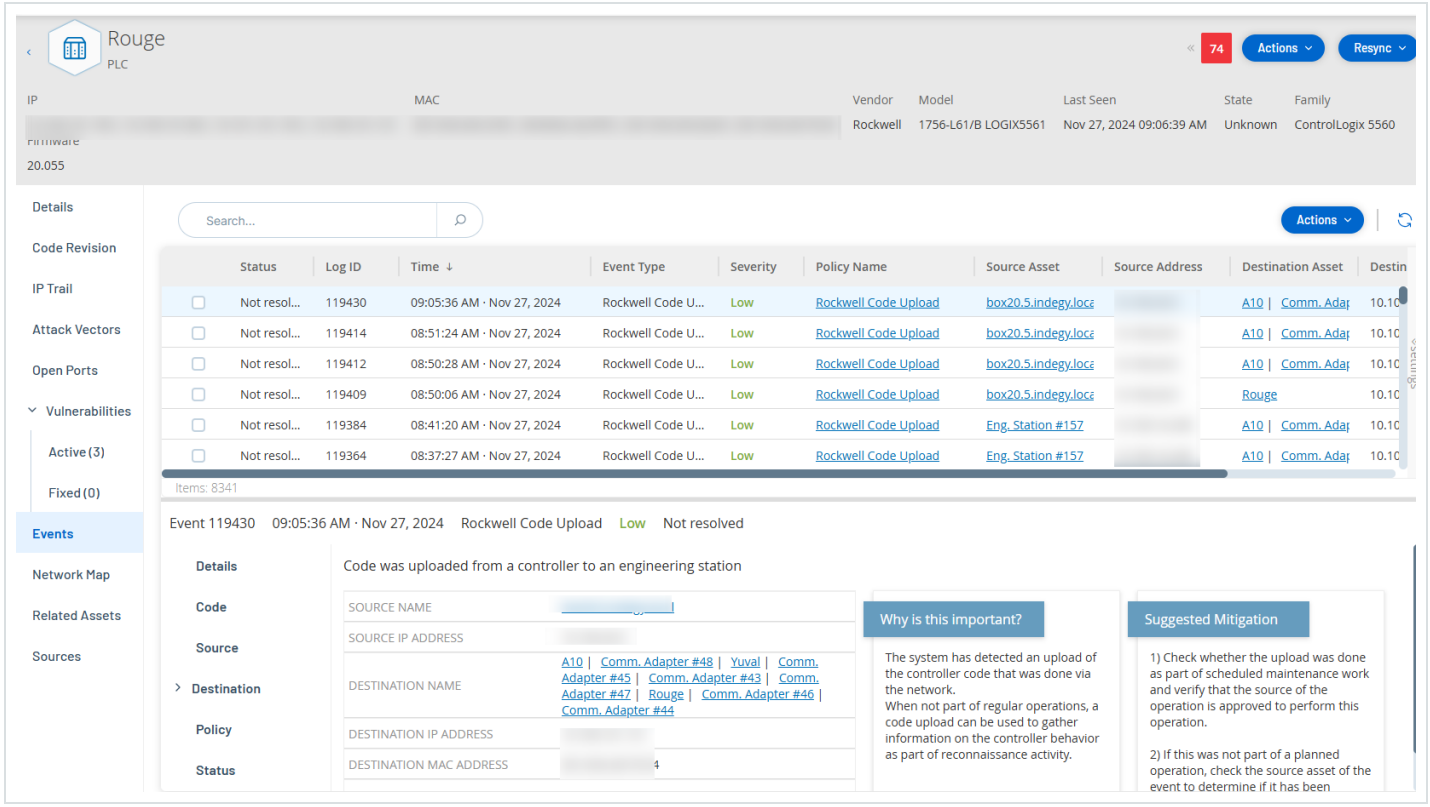
## Schwachstellen

Auf der Registerkarte Schwachstellen wird eine Liste aller Schwachstellen angezeigt, die das angegebene Asset betreffen und die von OT Security-Plugins erkannt wurden. Das System identifiziert Schwachstellen wie z. B. veraltete Windows-Betriebssysteme, die Verwendung anfälliger Protokolle und offene Kommunikationsports, die bekanntermaßen riskant oder für bestimmte Gerätetypen nicht unbedingt erforderlich sind. Die Schwachstellen werden in zwei Kategorien aufgeführt: Aktiv und Behoben. Jede Auflistung enthält Details über die Art der Bedrohung und ihren Schweregrad. Die auf dieser Registerkarte angezeigten Informationen sind identisch mit den Informationen auf der Seite Risiken > Schwachstellen, mit dem Unterschied, dass auf dieser Seite nur Schwachstellen angezeigt werden, die für das angegebene Asset relevant sind. Eine Erläuterung der Informationen zu Schwachstellen finden Sie unter Schwachstellen.




## Ereignisse

Auf der Registerkarte Ereignisse wird eine detaillierte Liste von Ereignissen im Netzwerk angezeigt, die das Asset betreffen und die von OT Security-Plugins erkannt wurden. Sie können die Anzeigeeinstellungen anpassen, indem Sie festlegen, welche Spalten angezeigt werden und wo die einzelnen Spalten positioniert sind. Die Ereignisse können nach verschiedenen Kategorien gruppiert werden (z. B. Ereignistyp, Schweregrad, Richtlinienname). Sie können die Ereignislisten auch sortieren und filtern sowie nach Text suchen. Eine Erläuterung der Anpassungsfunktionen finden Sie unter Elemente in der Benutzeroberfläche der Verwaltungskonsole.




Im unteren Teil der Seite werden auf verschiedenen Registerkarten detaillierte Informationen zum ausgewählten Ereignis angezeigt. Es werden nur Registerkarten angezeigt, die für den Ereignistyp des ausgewählten Ereignisses relevant sind. Weitere Informationen zu Ereignissen finden Sie unter Ereignisse.

Oben im Bereich befindet sich eine Schaltfläche Aktionen, mit der Sie die folgenden Aktionen für die ausgewählten Ereignisse ausführen können:

- Auflösen – Dieses Ereignis als „Aufgelöst“ markieren.
- Erfassungsdatei herunterladen – Die PCAP-Datei für dieses Ereignis herunterladen.
- Aus Richtlinie ausschließen – Einen Richtlinienausschluss für dieses Ereignis erstellen.

Detaillierte Informationen zu diesen Aktionen finden Sie im Kapitel Ereignisse.

Die für die einzelnen Ereignislisten angezeigten Informationen werden in der folgenden Tabelle beschrieben:

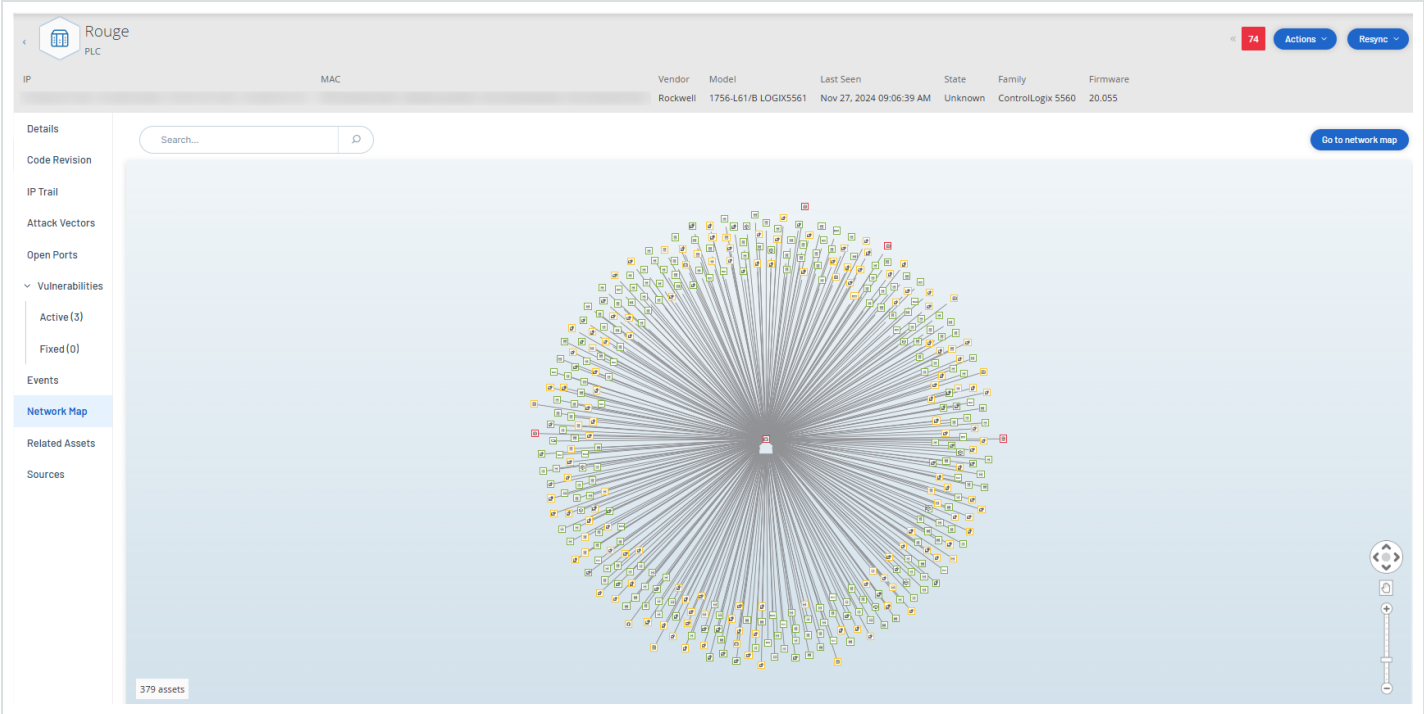
| Parameter | Beschreibung |
|---|---|
| Protokoll-ID | Die vom System generierte ID, um auf das Ereignis zu verweisen. |
| Uhrzeit | Das Datum und die Uhrzeit des Ereignisses. |
| Ereignistyp | Beschreibt die Art der Aktivität, die das Ereignis ausgelöst hat. Ereignisse werden von Richtlinien generiert, die im System eingerichtet sind. Eine Erläuterung der verschiedenen Arten von Richtlinien finden Sie unter Richtlinientypen. |
| Schweregrad | Zeigt den Schweregrad des Ereignisses an. Nachfolgend finden Sie eine Erläuterung zu den möglichen Werten:<br>• Kein – Kein Grund zur Besorgnis.<br>• Info – Kein unmittelbarer Grund zur Sorge. Sollte bei Gelegenheit geprüft werden.<br>• Warnung – Moderate Bedenken, dass potenziell schädliche Aktivitäten stattgefunden haben. Sollte behandelt werden, wenn es passt.<br>• Kritisch – Schwerwiegende Bedenken, dass potenziell schädliche Aktivitäten stattgefunden haben. Sollte sofort behandelt werden. |

| Parameter | Beschreibung |
| --- | --- |
| Richtlinienname | Der Name der Richtlinie, die das Ereignis generiert hat. Der Name ist ein Link zur Richtlinienliste. |
| Quell-Asset | Der Name des Assets, das das Ereignis initiiert hat. Dieses Feld ist ein Link zur Asset-Liste. |
| Quelladresse | Die IP- oder MAC-Adresse des Assets, das das Ereignis initiiert hat. |
| Quelladresse | Die IP- oder MAC-Adresse des Assets, das das Ereignis initiiert hat. |
| Ziel-Asset | Der Name des Assets, das von dem Ereignis betroffen war. Dieses Feld ist ein Link zur Asset-Liste. |
| Zieladresse | Die IP- oder MAC-Adresse des Assets, das von dem Ereignis betroffen war. |
| Protokoll | Sofern relevant, wird hier das Protokoll angezeigt, das für die Konversation verwendet wurde, die dieses Ereignis ausgelöst hat. |
| Ereigniskategorie | Zeigt die allgemeine Kategorie des Ereignisses an.<br><br>HINWEIS: Im Bildschirm „Alle Ereignisse“ werden Ereignisse aller Typen angezeigt. Auf jedem der spezifischen Ereignisbildschirme werden nur Ereignisse der angegebenen Kategorie angezeigt.<br><br>Im Folgenden finden Sie eine kurze Erläuterung der Ereigniskategorien (für eine ausführlichere Erläuterung siehe Richtlinienkategorien und Unterkategorien):<br><br>• Konfigurationsereignisse – Dies umfasst zwei Unterkategorien<br><br>• Controller-Validierungsereignisse – Diese Richtlinien erkennen Änderungen, die in den Controllern im Netzwerk stattfinden. |

| Parameter | Beschreibung |
| --- | --- |
| | • Controller-Aktivitätsereignisse – Aktivitätsrichtlinien beziehen sich auf die Aktivitäten, die im Netzwerk stattfinden (d. h. die „Befehle“, die zwischen Assets im Netzwerk implementiert werden).<br>• SCADA-Ereignisse – Richtlinien, die Änderungen identifizieren, die an der Datenebene von Controllern vorgenommen wurden.<br>• Netzwerkbedrohungsereignisse – Diese Richtlinien identifizieren Netzwerk-Traffic, der auf Bedrohungen durch Eindringlinge hinweist.<br>• Netzwerkereignisse – Richtlinien, die sich auf die Assets im Netzwerk und die Kommunikationsströme zwischen Assets beziehen. |
| Status | Zeigt an, ob das Ereignis als aufgelöst markiert wurde oder nicht. |
| Aufgelöst von | Zeigt für aufgelöste Ereignisse an, welcher Benutzer das Ereignis als aufgelöst markiert hat. |
| Aufgelöst am | Zeigt für aufgelöste Ereignisse an, wann das Ereignis als aufgelöst markiert wurde. |
| Kommentar | Zeigt alle Kommentare an, die hinzugefügt wurden, als das Ereignis aufgelöst wurde. |

## Netzwerkübersicht

Die Registerkarte Netzwerkübersicht zeigt eine grafische Visualisierung der Netzwerkverbindungen des Assets. Diese Ansicht zeigt alle Verbindungen, die das ausgewählte Asset in den letzten 30 Tagen hergestellt hat.




Die auf dieser Registerkarte angezeigten Informationen ähneln den im Bildschirm Netzwerkübersicht angezeigten Informationen, sind jedoch auf Verbindungen beschränkt, die dieses spezifische Asset betreffen. Außerdem zeigt dieser Bildschirm Verbindungen zu einzelnen Assets und nicht zu Asset-Gruppen, wie im Hauptbildschirm „Netzwerkübersicht“ dargestellt. Eine Erläuterung der auf dieser Registerkarte angezeigten Informationen finden Sie unter Netzwerkübersicht.

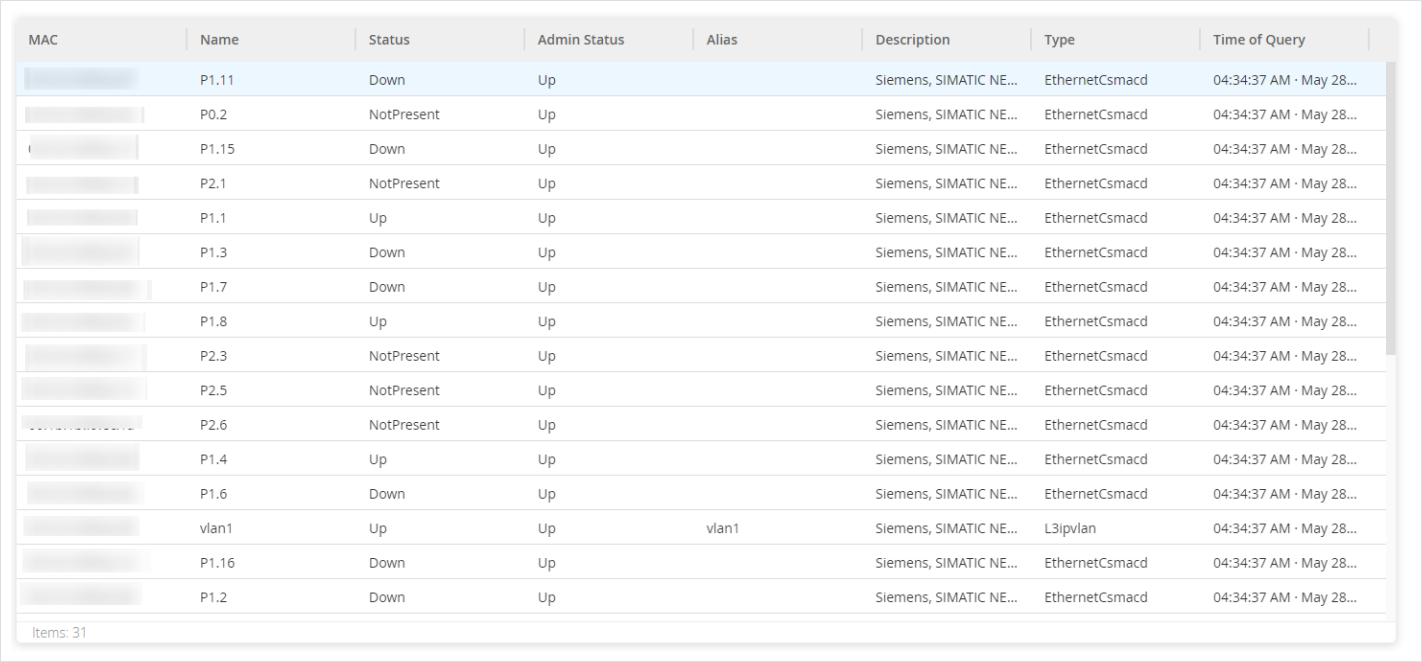
Um die Netzwerkübersicht für alle Assets anzuzeigen, klicken Sie auf die Schaltfläche Zur Netzwerkübersicht. Wenn Sie auf diese Schaltfläche klicken, wird die Netzwerkübersicht dynamisch vergrößert und zeigt dieses Asset und seine Verbindungen zu anderen Gruppen von Assets.

Wenn Sie auf eines der verbundenen Assets in der Übersicht klicken, werden Details zu diesem Asset angezeigt, und wenn Sie auf den Link im Namen des Assets klicken, gelangen Sie zum Detailbildschirm des ausgewählten Assets.

## Geräte-Ports

Die Registerkarte Geräte-Ports ist für Netzwerk-Switches verfügbar und enthält Details zu den Ports auf dem Netzwerk-Switch. OT Security sammelt diese Daten mithilfe von SNMP-Abfragen an den

Switch. Die angezeigten Details der jeweiligen Ports enthalten MAC-Adresse, Name, Verbindungsstatus (aktiv oder inaktiv), Alias und Beschreibung.



| MAC | Name | Status | Admin Status | Alias | Description | Type | Time of Query |
|---|---|---|---|---|---|---|---|
| | P1.11 | Down | Up | | Siemens, SIMATIC NE... | EthernetCsmacd | 04:34:37 AM · May 28... |
| | P0.2 | NotPresent | Up | | Siemens, SIMATIC NE... | EthernetCsmacd | 04:34:37 AM · May 28... |
| | P1.15 | Down | Up | | Siemens, SIMATIC NE... | EthernetCsmacd | 04:34:37 AM · May 28... |
| | P2.1 | NotPresent | Up | | Siemens, SIMATIC NE... | EthernetCsmacd | 04:34:37 AM · May 28... |
| | P1.1 | Up | Up | | Siemens, SIMATIC NE... | EthernetCsmacd | 04:34:37 AM · May 28... |
| | P1.3 | Down | Up | | Siemens, SIMATIC NE... | EthernetCsmacd | 04:34:37 AM · May 28... |
| | P1.7 | Down | Up | | Siemens, SIMATIC NE... | EthernetCsmacd | 04:34:37 AM · May 28... |
| | P1.8 | Up | Up | | Siemens, SIMATIC NE... | EthernetCsmacd | 04:34:37 AM · May 28... |
| | P2.3 | NotPresent | Up | | Siemens, SIMATIC NE... | EthernetCsmacd | 04:34:37 AM · May 28... |
| | P2.5 | NotPresent | Up | | Siemens, SIMATIC NE... | EthernetCsmacd | 04:34:37 AM · May 28... |
| | P2.6 | NotPresent | Up | | Siemens, SIMATIC NE... | EthernetCsmacd | 04:34:37 AM · May 28... |
| | P1.4 | Up | Up | | Siemens, SIMATIC NE... | EthernetCsmacd | 04:34:37 AM · May 28... |
| | P1.6 | Down | Up | | Siemens, SIMATIC NE... | EthernetCsmacd | 04:34:37 AM · May 28... |
| | vlan1 | Up | Up | vlan1 | Siemens, SIMATIC NE... | L3ipvlan | 04:34:37 AM · May 28... |
| | P1.16 | Down | Up | | Siemens, SIMATIC NE... | EthernetCsmacd | 04:34:37 AM · May 28... |
| | P1.2 | Down | Up | | Siemens, SIMATIC NE... | EthernetCsmacd | 04:34:37 AM · May 28... |

Items: 31

Hinweis: Aktivieren Sie diese Funktion in Ihrem Konto, damit die Registerkarte sichtbar ist. Um diese Funktion zu aktivieren, wenden Sie sich an den Tenable-Support.

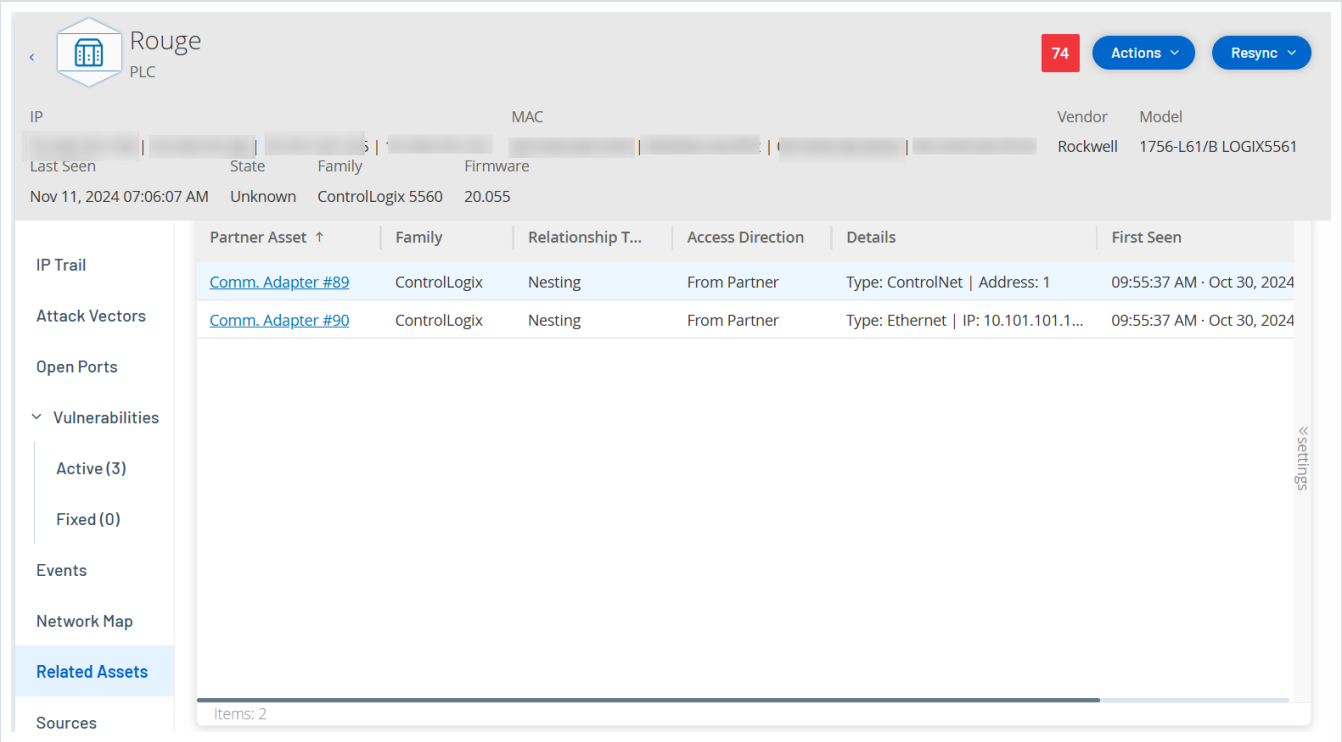
## Verwandte Assets

Auf der Seite Verwandte Assets eines Assets wird die Liste aller verschachtelten Assets angezeigt.

So greifen Sie auf die Seite Verwandte Assets zu:

1. Klicken Sie in der Tabelle Inventar > Alle Assets auf ein Asset, um die Seite mit Asset-Details zu öffnen.
2. Klicken Sie im linken Navigationsbereich auf Verwandte Assets.

Die Seite Verwandte Assets wird angezeigt.

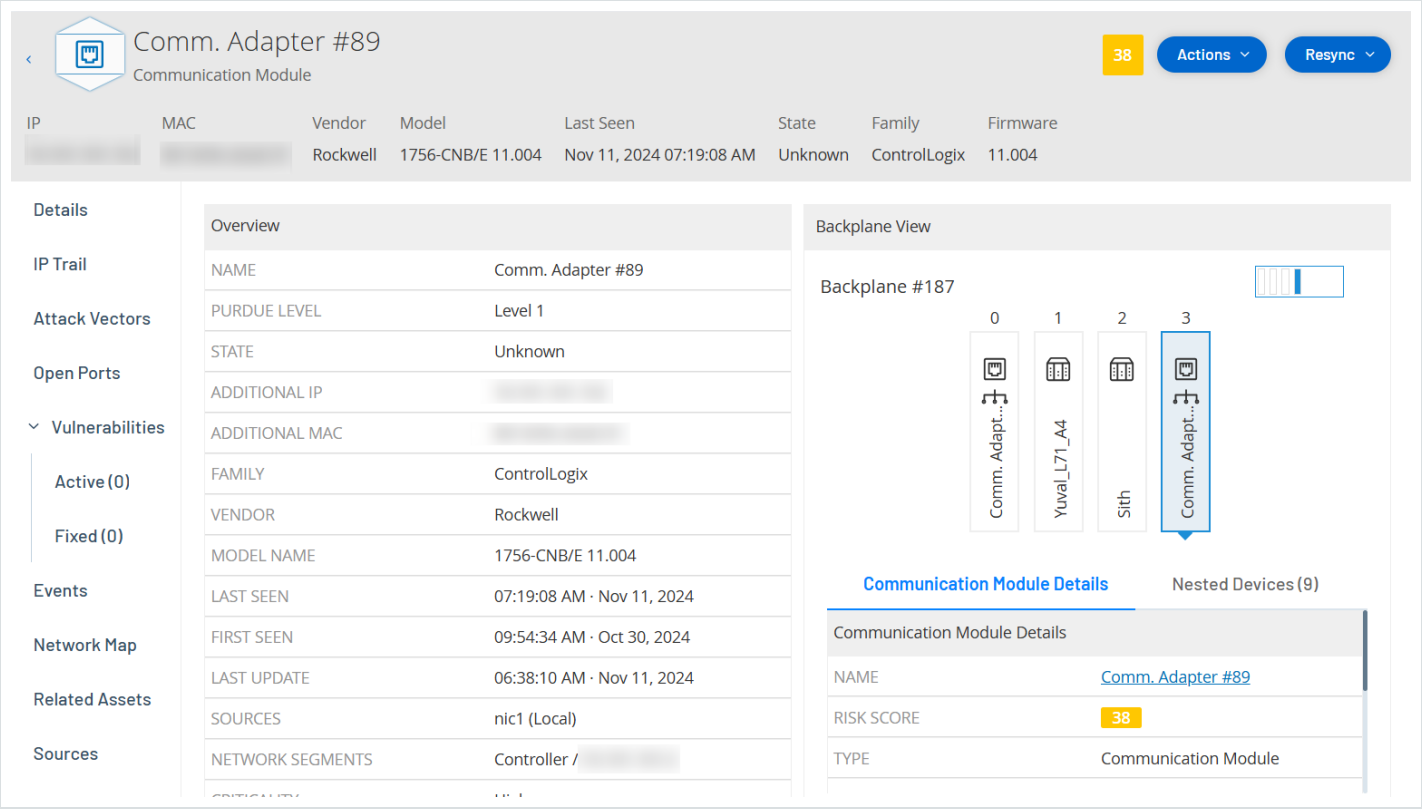



Die Seite Verwandte Assets enthält die folgenden Details:

| Spalte | Beschreibung |
|---|---|
| Partner-Asset | Der Name des verwandten Assets. |
| Beziehungstyp | Der Typ der Beziehung zum verwandten Asset: Verschachtelung. |
| Zugriffsrichtung | Die Richtung des Zugriffs zwischen dem Asset und seinem Partner. |
| Details | Die Details zum Asset-Typ. Beispiel: ControlNet oder IP. |
| Zum ersten Mal gesehen | Das Datum, an dem OT Security dieses Asset zum ersten Mal erfasst hat. |
| Zuletzt gesehen | Das Datum, an dem OT Security dieses Asset zuletzt erfasst hat. |

## Details zu verschachtelten Assets

Verschachtelte Geräte sind speicherprogrammierbare Steuerungen (SPS) oder andere ICS-Module (Industrial Control System, industrielles Steuerungssystem), die hinter einer SPS-Backplane oder einem Gerät angeschlossen sind. Dies ist vergleichbar mit einem Frequenzumrichter (Variable-Frequency Drive, VFD), der direkt an einen Kommunikationsadapter angeschlossen ist. Um die Details eines verschachtelten Assets anzuzeigen, klicken Sie auf der Seite Verwandte Assets auf den Link zum verschachtelten Asset. OT Security zeigt verschachtelte Geräte mit dem Symbol an.




Die Seite mit folgenden Details zum verschachtelten Asset wird angezeigt:

| Abschnitt | Beschreibung |
|---|---|
| Übersicht | Enthält Details zum Asset wie Name, Purdue-Level, Status und zusätzliche IP. |
| Allgemein | Enthält Details wie Seriennummer, Firmware-Version, Gerätetyp, Backplane- |

| | |
|---|---|
| | Nummer und Slot-Nummer. |
| Backplane-Ansicht | Enthält eine grafische Ansicht der Backplane. Klicken Sie in der Backplane-Ansicht auf den Gerätenamen, um die Registerkarten Details zum Kommunikationsmodul und Verschachtelte Geräte anzuzeigen. |

## IEC 61850

Basierend auf der von Ihnen hochgeladenen SCD-Datei (Station Configuration Description) generiert OT Security die Liste der MMS-Berichte (Manufacturing Message Specification), in denen die Kommunikation zwischen den Unterstations-Assets beschrieben wird. OT Security zeigt eine Fehlermeldung an, wenn ein nicht autorisierter Zugriff in der SCD-Dateikonfiguration erkannt wird. Weitere Informationen zum Hochladen von SCD-Dateien finden Sie unter SCD-Dateien.

### So greifen Sie auf die Seite „IEC 61850“ zu:

1. Gehen Sie zu Inventar > Alle Assets.

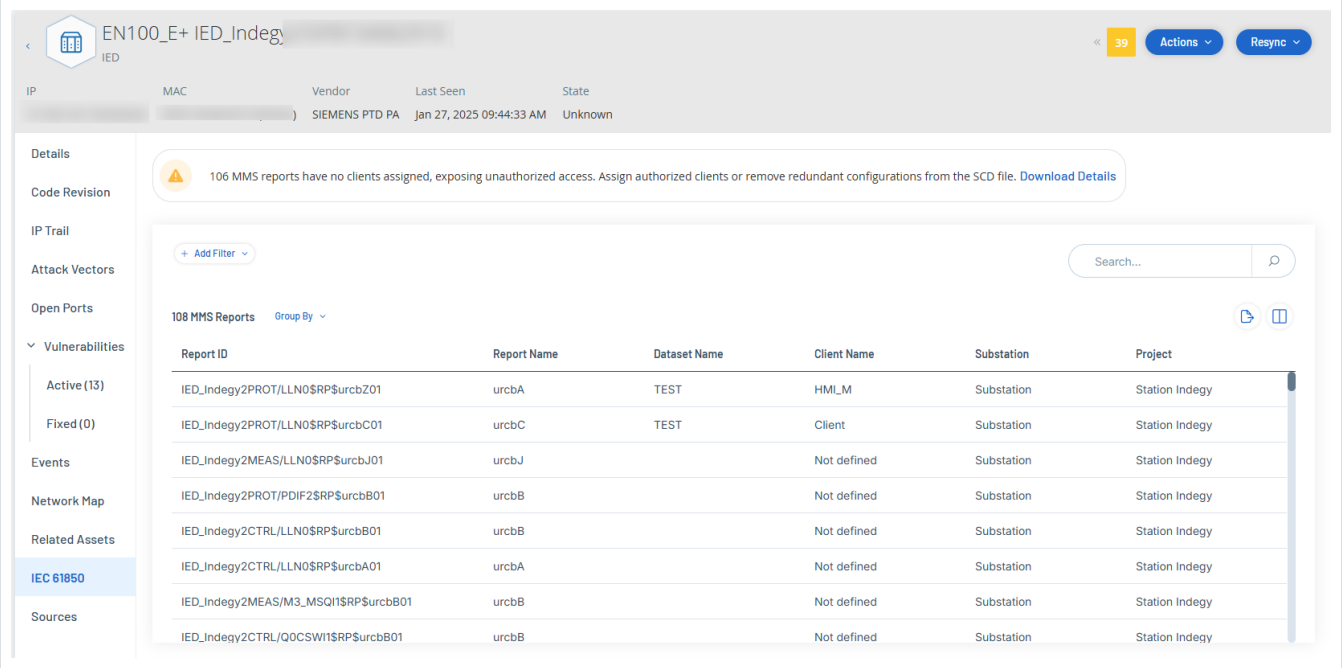
   Die Seite Alle Assets wird angezeigt.

2. Suchen Sie nach dem Asset oder der Unterstation, für das bzw. die Sie die IEC 61850-Konfiguration anzeigen möchten, und wählen Sie es bzw. sie aus.

   Die Seite mit Asset-Details wird geöffnet.

3. Wählen Sie in der linken Navigationsleiste die Option IEC 61850 aus.

   Die Seite IEC 61850 enthält die folgenden Details:



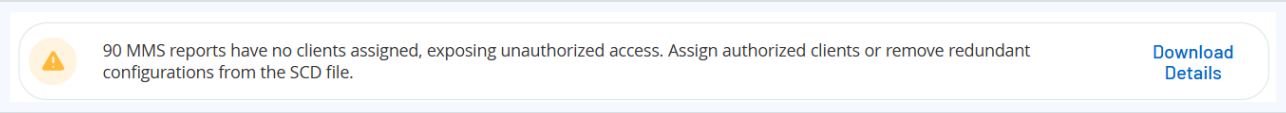

| Spalte | Beschreibung |
| --- | --- |
| Berichts-ID | Die MMS-Berichts-ID, die als eindeutiger Bezeichner für den Bericht dient. |
| Berichtsname | Die MMS-Berichts-ID, die als eindeutiger Bezeichner für den Bericht dient. |
| Dataset-Name | Der Name des Datasets, der mit dem MMS-Bericht verknüpft ist, der die im Bericht enthaltene Gruppe von Datenpunkten definiert. |
| Client-Name | Der Name der Client-Anwendung oder des Client-Systems, die bzw. das den Bericht abonniert und empfängt. |
| Unterstation | Die Unterstation, in der sich das IED (Intelligent Electronic Device, intelligentes elektronisches Gerät) befindet, das den MMS-Bericht generiert. |

| | |
|---|---|
| Projekt | Die übergeordnete IEC 61850-Projekt- oder -Systemkonfiguration, zu der der Bericht und die zugeordneten Komponenten gehören. |

4. So zeigen Sie Details der von OT Security erkannten Feststellungen an: Klicken Sie in der Fehlermeldung oben auf der Seite auf Details herunterladen.

   OT Security lädt die Details im CSV-Format herunter.

   Hinweis: Die Anzahl der MMS-Berichte in der Fehlermeldung bezieht sich auf das jeweilige Asset, während die heruntergeladene CSV-Datei Details zu allen Assets enthält.

## Quellen

Die Seite Quellen für ein Asset enthält alle Informationen im Zusammenhang mit der Quelle des Assets, wie z. B. Standort, Typ und Zeitpunkt der ersten und letzten Meldung. Die Quelle des Assets wird auch in der Spalte Quellen auf der Seite Inventar > Alle Assets angezeigt.

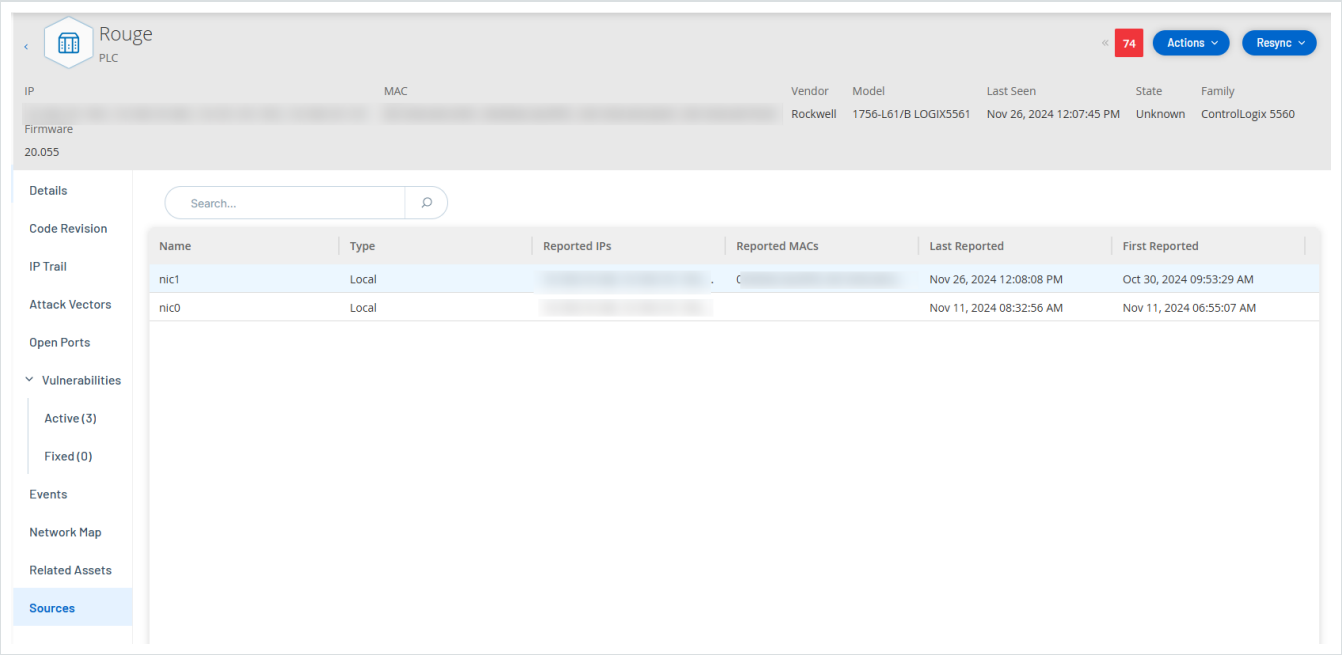
So greifen Sie auf die Seite Quellen zu:

1. Klicken Sie in der Tabelle Inventar > Alle Assets auf ein Asset, um die Seite mit Asset-Details zu öffnen.

   Die Seite mit Asset-Details wird geöffnet.

2. Klicken Sie im linken Navigationsbereich auf Quellen.

Die Seite Quellen wird angezeigt.




Die Seite Quellen enthält die folgenden Details:

| Spalte | Beschreibung |
|---|---|
| Name | Der Name der Quelle, zum Beispiel „nic1“ oder „nic2“ für eine lokale Quelle oder der Sensorname, wenn die Quelle ein Sensor ist. |
| Typ | Der Typ der Quelle: lokale(r) ICP oder Sensor. |
| Gemeldete IPs | Die IP-Adressen, die vom Quell-Asset stammen. |
| Gemeldete MACs | Die MAC-Adressen, die vom Quell-Asset stammen. OT Security meldet eine MAC-Adresse, wenn der Sensor nahe genug ist, um das Asset zu beobachten. Wenn der Sensor weit vom Asset entfernt ist, aber eine Konversation zwischen ihnen beobachtet, meldet OT Security nur die beobachteten IP-Adressen. |
| Zuletzt | Der Zeitpunkt, zu dem das Quell-Asset zum letzten Mal gemeldet wurde. |

| | |
|---|---|
| gemeldet | |
| Zuerst gemeldet | Der Zeitpunkt, zu dem das Quell-Asset zum ersten Mal gemeldet wurde. |

## Asset-Details bearbeiten

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Site-Operator

OT Security identifiziert Typ und Name des Assets automatisch anhand seiner internen Daten und seiner Aktivität im Netzwerk. Wenn das System diese Informationen nicht erfassen konnte oder Sie der Meinung sind, dass die automatische Identifizierung nicht korrekt ist, können Sie diese Parameter entweder direkt über die Benutzeroberfläche oder durch Hochladen einer CSV-Datei bearbeiten. Sie können auch eine allgemeine Beschreibung des Assets und eine Beschreibung des Standorts der Einheit hinzufügen.

### Asset-Details über die Benutzeroberfläche bearbeiten

So bearbeiten Sie Asset-Details für ein einzelnes Asset:

1. Klicken Sie unter Inventar auf Controller oder Netzwerk-Assets.
2. Wählen Sie das gewünschte Asset aus.
3. Klicken Sie in der Kopfleiste auf die Schaltfläche Aktionen.
4. Wählen Sie im Dropdown-Menü Bearbeiten aus.

   Das Fenster Asset-Details bearbeiten wird geöffnet.
5. Wählen Sie im Feld Typ den Asset-Typ aus der Dropdown-Liste aus.

6. Geben Sie im Feld Name einen Namen ein, mit dem das Asset in der Benutzeroberfläche von OT Security identifiziert wird.
7. Geben Sie im Feld Kritikalität die Kritikalität dieses Assets für das System ein.
8. Geben Sie im Feld Purdue-Level das Purdue Level basierend auf dem Asset-Typ ein.
9. Geben Sie im Feld Backplane (für Controller) den Namen der Backplane ein, auf der das Asset installiert ist.
10. Geben Sie im Feld Standort eine Beschreibung des Standorts des Assets ein. Dies ist ein optionales Feld. Die Daten werden in der Assets-Tabelle sowie im Bildschirm „Asset-Details“ für dieses Asset angezeigt.
11. Geben Sie im Feld Beschreibung eine Beschreibung des Assets ein. Dies ist ein optionales Feld. Die Daten werden auf der Seite „Asset-Details“ für dieses Asset angezeigt.
12. Klicken Sie auf Speichern.

    OT Security speichert die bearbeiteten Details.

So bearbeiten Sie mehrere Assets (Massenprozess):

1. Klicken Sie unter Inventar auf Controller oder Netzwerk-Assets.
2. Aktivieren Sie das Kontrollkästchen neben den gewünschten Assets.
3. Klicken Sie auf das Menü Massenaktionen und wählen Sie Bearbeiten in der Dropdown-Liste aus.

   Der Bildschirm Massenbearbeitung wird mit den für die Massenbearbeitung verfügbaren Parametern angezeigt.
4. Aktivieren Sie das Kontrollkästchen neben jedem Parameter, den Sie bearbeiten möchten (Typ, Kritikalität, Purdue-Level, Netzwerksegmente, Standort und Beschreibung).

> Hinweis: Filtern Sie bei der Massenbearbeitung von Netzwerksegmenten zuerst Ihre Assets nach Typ und wählen Sie dann die Assets aus, die Sie in einem Massenvorgang bearbeiten möchten. Assets mit mehreren IP-Adressen können nicht in eine Massenbearbeitung für Netzwerksegmente aufgenommen werden. Sie müssen jedes Asset manuell bearbeiten.

5. Stellen Sie jeden Parameter nach Bedarf ein.

> Hinweis: Die in die Felder für die Massenbearbeitung eingegebenen Informationen überschreiben alle aktuellen Inhalte für das ausgewählte Asset. Wenn Sie das Kontrollkästchen neben einem Parameter aktivieren, aber keine Auswahl treffen, werden die aktuellen Werte für diesen Parameter gelöscht.

6. Klicken Sie auf Speichern.

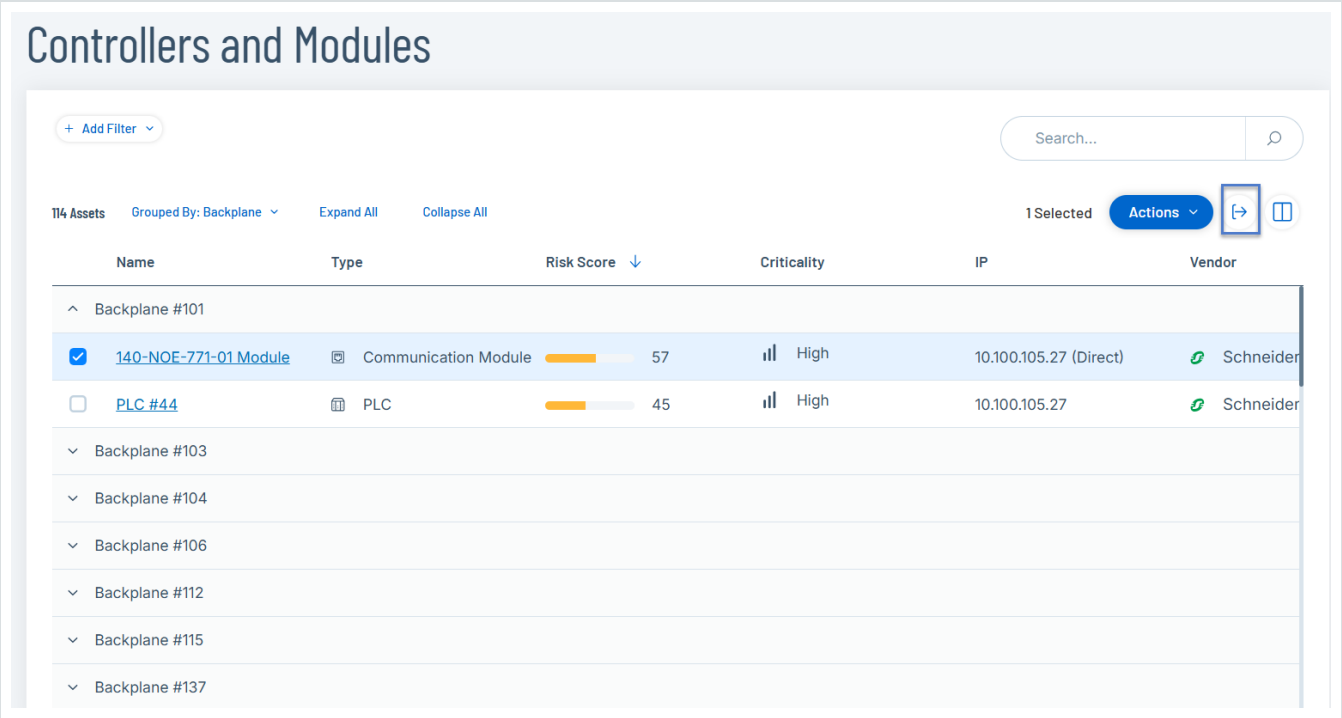
   OT Security speichert die Assets mit der neuen Konfiguration.

## Asset-Details durch Hochladen einer CSV-Datei bearbeiten

Mit dieser Methode zum Bearbeiten von Asset-Details können Sie eine große Anzahl von Assets über eine CSV-Datei bearbeiten, anstatt sie manuell in der Benutzeroberfläche zu bearbeiten. Die folgenden Details können mit dieser Methode bearbeitet werden: Typ, Name, Kritikalität, Purdue-Level, Standort, Beschreibung und benutzerdefinierte Felder.

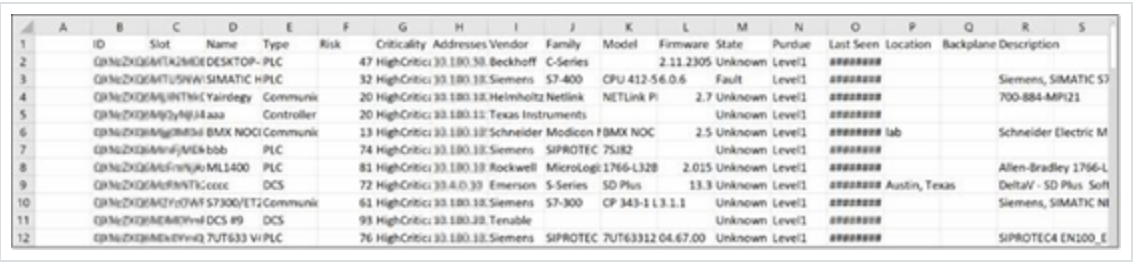
### So bearbeiten Sie Asset-Details über eine CSV-Datei:

1. Klicken Sie unter Inventar auf Alle Assets, Controller und Module oder Netzwerk-Assets.
2. Klicken Sie auf die Schaltfläche Exportieren.




Eine CSV-Datei des Inventars wird heruntergeladen.

3. Navigieren Sie zu der gerade heruntergeladenen Datei und öffnen Sie sie.



4. Bearbeiten Sie die zulässigen Parameter, indem Sie den Inhalt der Zellen ändern. Zulässige Parameter: Typ, Name, Kritikalität, Purdue-Level, Standort, Beschreibung und benutzerdefinierte Felder.

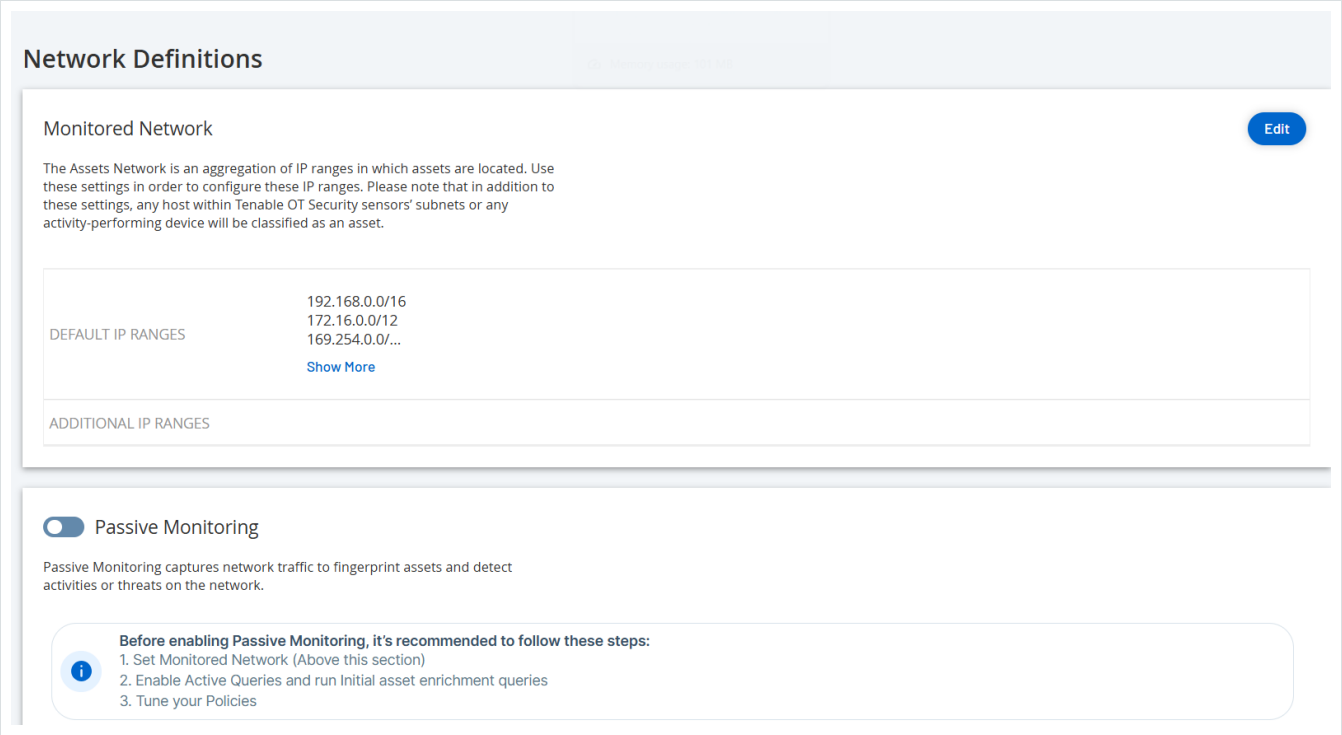
> Hinweis: Sie müssen gültige Daten für Parameter eingeben, die bestimmte Optionen erfordern (z. B. Typ, Kritikalität, Purdue-Level). Andernfalls kann das jeweilige Asset nicht aktualisiert werden.

5. Speichern Sie die Datei als CSV-Dateityp.

Hinweis: Nur die von Ihnen geänderten Assets werden im System aktualisiert. Assets, die nicht in der CSV-Datei enthalten sind, oder Zeilen, die Sie nicht geändert haben, bleiben im System unverändert. Es ist nicht möglich, Assets mit dieser Methode zu löschen.

6. Gehen Sie unter Einstellungen zu Umgebungseinstellungen >Netzwerkdefinitionen.

   Die Seite Netzwerkdefinitionen wird angezeigt.




7. Klicken Sie im Abschnitt Asset-Details per CSV aktualisieren auf Hochladen.

8. Folgen Sie den Navigationsanweisungen Ihres Geräts, um die soeben gespeicherte CSV-Datei hochzuladen.

   Es erscheint eine Bestätigung, die die Anzahl der aktualisierten Zeilen angibt.

   Das Feld Datum des letzten Uploads im Abschnitt „Asset-Details per CSV aktualisieren“ wird aktualisiert.

9. Um weitere Informationen zu den Ergebnissen des Uploads zu sehen, klicken Sie im Abschnitt Asset-Details per CSV aktualisieren auf Bericht herunterladen.

OT Security lädt eine CSV-Datei herunter, die die aktualisierten Asset-IDs auflistet und auch die fehlgeschlagenen Asset-IDs auflistet.

## Assets ausblenden

Sie können ein oder mehrere Assets aus der Asset-Inventarisierung ausblenden. Ein ausgeblendetes Asset wird nicht im Inventar angezeigt und aus Gruppen entfernt. Für das ausgeblendete Asset werden jedoch weiterhin Ereignisse und Netzwerkaktivitäten angezeigt.

Sie können ein ausgeblendetes Asset über die Seite Einstellungen > Umgebungs**einstellungen** > Ausgeblendete Assets wiederherstellen.

### So blenden Sie ein oder mehrere Assets aus:

1. Klicken Sie unter Inventar auf Controller oder Netzwerk-Assets.
2. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Assets, die Sie entfernen möchten.
3. Klicken Sie in der Kopfleiste auf Aktionen.

   Ein Menü wird angezeigt.
4. Wählen Sie Asset ausblenden aus.

   Die Seite Ausgeblendete Assets wird angezeigt.
5. (Optional) Fügen Sie im Feld Kommentare Textkommentare zu den Assets hinzu.

   > Hinweis: Die Kommentare werden in der Liste der entfernten Assets auf der Seite Einstellungen > Umgebungseinstellungen > Ausgeblendete Assets angezeigt.
6. Klicken Sie auf Ausblenden.

   OT Security blendet die Assets auf den Seiten Inventar und Gruppen aus.

# Diagnosedaten exportieren

Sie können den Diagnosebericht eines Assets oder einer Asset-Gruppe, das bzw. die falsch positive Ergebnisse anzeigt oder ein anderes Problem aufweist, exportieren und herunterladen. Sie können diesen Bericht zur detaillierten Analyse für Tenable-Support freigeben. Je nach Bedarf können Sie Diagnosedaten direkt aus der Asset-Inventarisierung oder über die Verwaltungsoberfläche von Tenable Core abrufen.

## Asset-Diagnosebericht exportieren

So exportieren Sie den Diagnosebericht:

1. Gehen Sie in der linken Navigationsleiste zu Inventar > Alle Assets.

   Die Seite Alle Assets wird angezeigt.

2. Wählen Sie in der Tabelle „Alle Assets“ ein oder mehrere Assets aus, die Sie im Diagnosebericht exportieren möchten.

3. Führen Sie einen der folgenden Schritte aus:

   - Für ein einzelnes Asset: Klicken Sie in der oberen rechten Ecke auf Aktionen > Diagnosedaten exportieren.
   - Für mehrere Assets: Klicken Sie in der oberen rechten Ecke auf Massenaktionen > Diagnosedaten exportieren.

   OT Security lädt den Diagnosebericht für das bzw. die ausgewählten Assets herunter. Der Diagnosebericht ist eine tar.gz-Datei, die die Asset-Details in einer JSON-Datei beinhaltet.

   Der Name des Diagnoseberichts enthält den Namen des Assets, den Zeitstempel und die OT Security-Version. Beispiele:

   Für ein einzelnes Asset: `TOTS_Rouge_3.19.15_2024-06-03T07_05_27.tar.gz`

Für mehrere Assets: `TOTS_AssetsReport_3.19.15_2024-06-03T07_17_54.tar.gz`

4. Extrahieren Sie den Diagnosebericht und teilen Sie ihn zur weiteren Analyse mit Tenable-Support.

## Tenable OT Security-Diagnosebericht exportieren (Tenable Core)

Sie können einen Tenable OT Security-spezifischen Diagnosebericht zur Fehlerbehebung generieren und aus Tenable Core exportieren.

### Bevor Sie beginnen

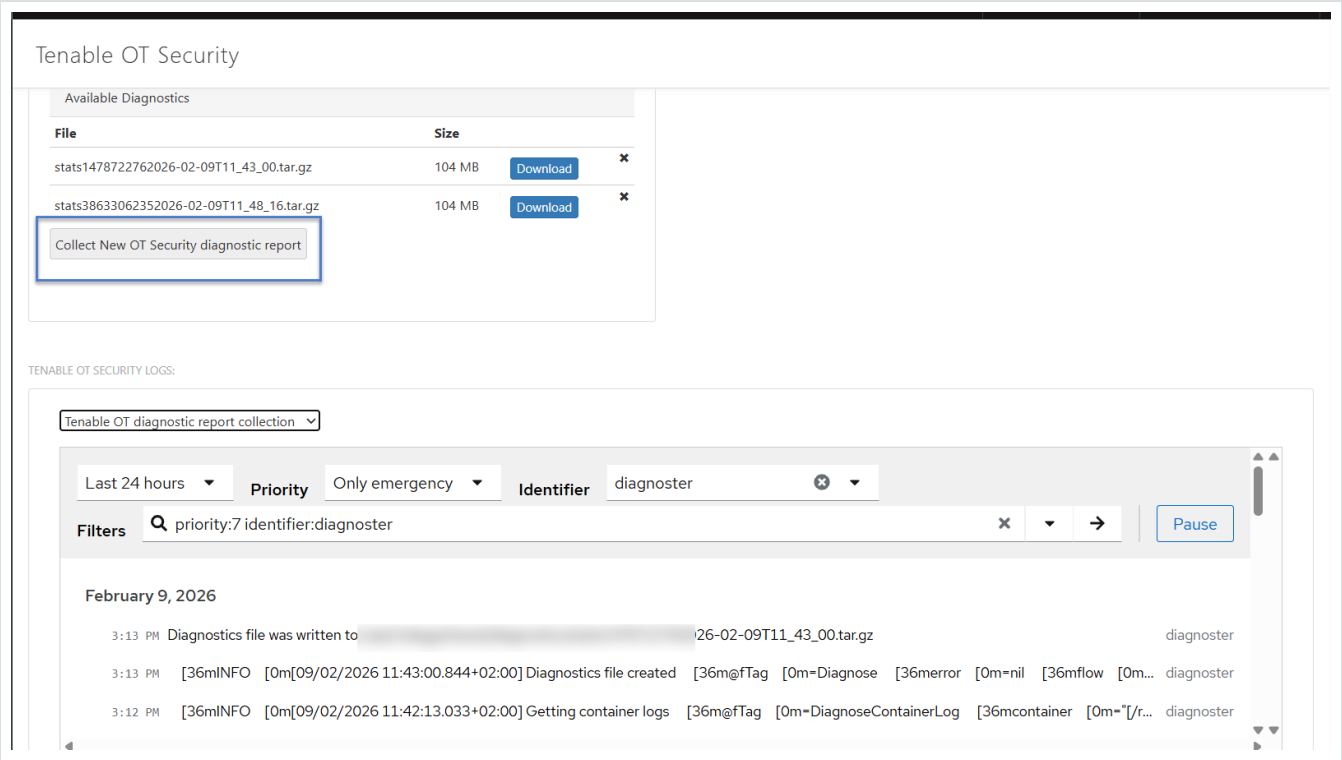
- Vergewissern Sie sich, dass Sie über Administratorzugriff verfügen.

### So generieren Sie den Diagnosebericht:

1. Loggen Sie sich bei Tenable Core ein.
2. Klicken Sie in der linken Navigationsleiste auf **Tenable OT Security**.

   Die Seite **Tenable OT Security** wird angezeigt.
3. Klicken Sie im Abschnitt OT Diagnostics auf Collect New OT Security Diagnostic Report.

   Der Diagnosebericht wird generiert.




4. Klicken Sie neben dem Bericht, den Sie herunterladen möchten, auf Download.

   Tenable Core lädt den Bericht auf Ihr System herunter. Nachdem Tenable Core die Protokolle generiert hat, kann es mehrere Minuten dauern, bis die Daten in den Debug-Protokollen angezeigt werden.

# Assets zusammenführen

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Site-Operator

Geräte in Ihrem Netzwerk können in OT Security aufgrund von passiver Traffic-Erkennung, bestimmter Routing-Konfigurationen oder unzureichenden Informationen zu Asset-Details als zwei oder mehr separate Assets angezeigt werden, was eine automatische interne Zusammenführung verhindert.

Beispielsweise verfügen Multihomed-Geräte wie Workstations, Server oder Controller in der Regel über mehrere IP-Adressen, die es ihnen ermöglichen, über verschiedene Netzwerke zu kommunizieren. Alternativ können Sie virtuelle Netzwerkschnittstellen auf einem Switch, Router oder einer Firewall in Betracht ziehen. Auch wenn es sich um virtuelle Erweiterungen eines einzelnen physischen Netzwerkgeräts handelt, kann jede dieser Erweiterungen als separates Asset im System erfasst werden.

In solchen Fällen können Sie die Option Assets zusammenführen verwenden, um zwei Assets zusammenzuführen und Duplikate zu entfernen. Sie können diese Option entweder über die Seite Inventar oder über die Detailseite eines einzelnen Assets aufrufen.

> Achtung: Diese Aktion kann nicht rückgängig gemacht werden.

### So führen Sie Assets zusammen:

1. Gehen Sie im linken Navigationsmenü zu Inventar > Alle Assets.

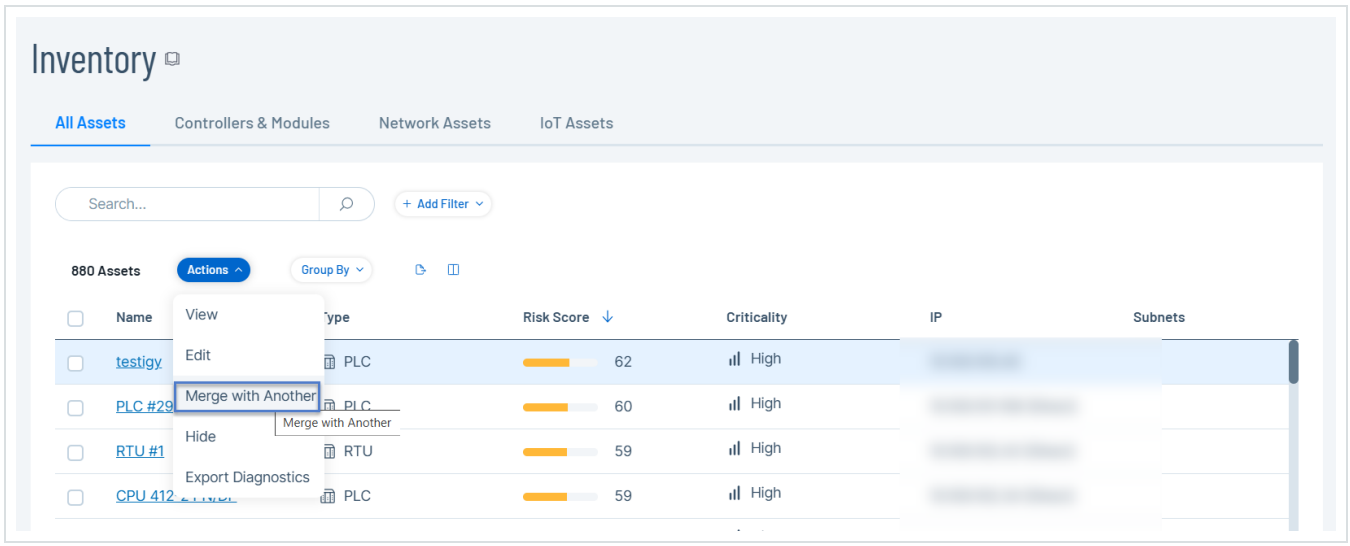
   Die Seite Alle Assets wird angezeigt.

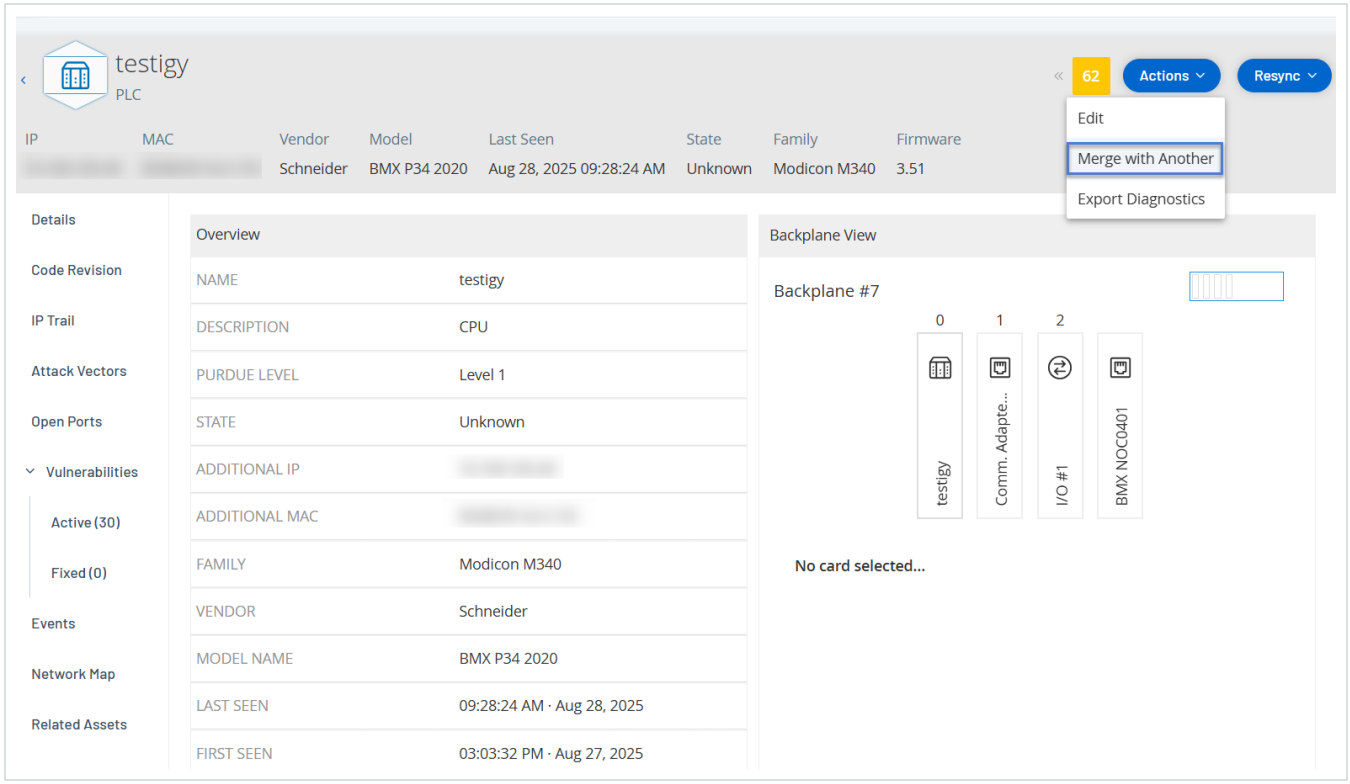
2. Führen Sie in der Tabelle „Alle Assets“ einen der folgenden Schritte aus:

   - Wählen Sie das Ziel-Asset aus, das zusammengeführt werden soll.
   - Klicken Sie auf den Asset-Link, um die Seite mit Asset-Details zu öffnen.

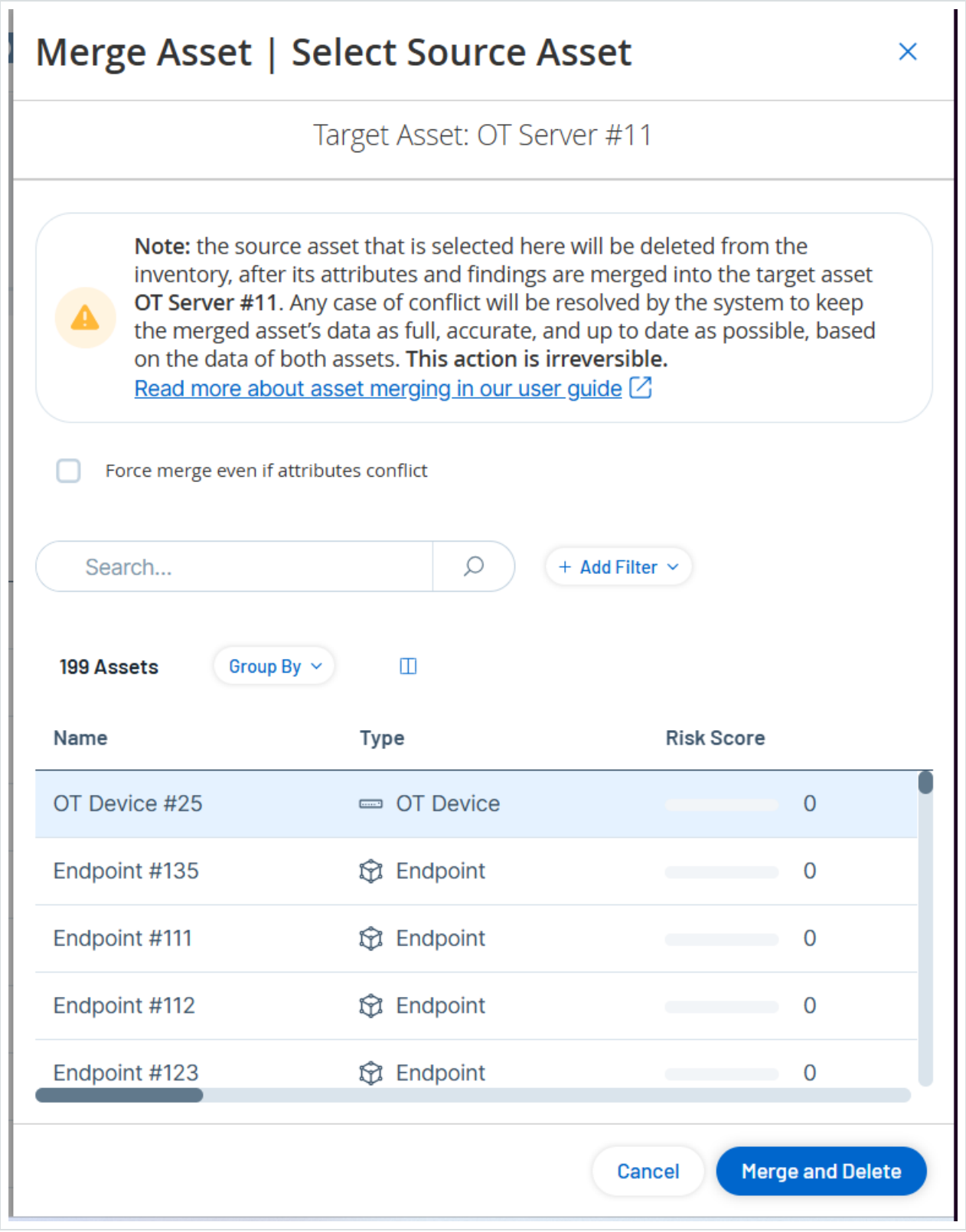
   In OT Security wird Aktionen aktiviert.

3. Klicken Sie auf Aktionen > Mit anderem Asset zusammenführen.




Der Bereich Asset zusammenführen | Quell-Asset auswählen wird angezeigt.




4. Filtern oder suchen Sie nach dem Quell-Asset.

5. Wählen Sie das Quell-Asset aus, das mit dem Ziel-Asset zusammengeführt werden soll.
6. (Optional) Aktivieren Sie das Kontrollkästchen Zusammenführung erzwingen, auch wenn Attribute in Konflikt stehen, um Konflikte zu umgehen.
7. Klicken Sie auf Zusammenführen und löschen.

   OT Security löscht das Quell-Asset und führt seine Attribute und Feststellungen im Ziel-Asset zusammen.

## Was geschieht, wenn Sie Assets zusammenführen

Der Prozess der Asset-Zusammenführung fasst zwei Assets zu einem einzigen Objekt zusammen und stellt sicher, dass die Datenintegrität systemweit gewahrt bleibt.

Dieser Vorgang umfasst die folgenden Schritte:

- Konsolidierung von Asset-Eigenschaften: Wenn Assets zusammengeführt werden, werden ihre Eigenschaften im Ziel-Asset zusammengeführt. Wenn beide Assets für dieselbe Eigenschaft unterschiedliche Werte aufweisen, verwendet das System einen Prioritätsmechanismus, um zu entscheiden, welcher Wert beibehalten wird. Dieser Prozess stellt sicher, dass das zusammengeführte Asset die genauesten oder neuesten Informationen enthält.
- Verbindungserhaltung: Netzwerkverbindungen, die zuvor auf eines der beiden Assets zeigten, verweisen jetzt auf das zusammengeführte Asset. Dazu gehören:
    - Direkte Verbindungen zu anderen Geräten.
    - Slot-basierte Verbindungen innerhalb von Backplanes.
    - Zuordnungen von Netzwerkschnittstellen, einschließlich IP- und MAC-Adressen. Das System stellt sicher, dass alle historischen Adressinformationen beibehalten und doppelte Einträge entfernt werden.

- Konsolidierung von Feststellungen: Das System konsolidiert alle Feststellungen, Schwachstellen und Sicherheitsereignisse unter dem neuen Asset und behält dadurch seinen vollständigen Sicherheitsverlauf bei.

### Zusammenführungskonflikte und erzwungene Zusammenführung

Die folgenden Assets können nicht zusammengeführt werden:

- Spezielle Assets wie ICP-, Sensor- oder Broadcast-Assets
- Assets aus verschiedenen Backplanes (nur eines von ihnen darf eine Backplane haben)
- Assets mit unterschiedlichen Steckplätzen (wenn beide Assets Slots haben, muss dieser identisch sein)
- Assets mit unterschiedlichen Seriennummern

Zusammenführung erzwingen: Wenn Sie das Kontrollkästchen Zusammenführung erzwingen aktivieren, werden die Systemprüfungen auf Konflikte in Bezug auf Backplane, Slot und Seriennummer umgangen. Auch wenn diese Option keine erfolgreiche Zusammenführung garantiert und die Merge-Engine ungültige Vorgänge möglicherweise trotzdem blockiert, fährt das System mit der Zusammenführung fort, bevor sie blockiert werden kann.

### So korrigieren Sie eine versehentliche Zusammenführung

Wenn eine Asset-Zusammenführung fälschlicherweise durchgeführt wurde oder Sie beide Assets in den Zustand vor der Zusammenführung zurückversetzen müssen, löschen Sie das Asset. Wenn Sie das Asset löschen, kann das System das einzelne Asset in seinem ursprünglichen Zustand wiederherstellen. Informationen zum Löschen eines einzelnen Assets oder einer Gruppe von Assets aus OT Security finden Sie in diesem Artikel in der Wissensdatenbank.

## Asset-spezifischen Tenable Nessus-Scan durchführen

Tenable Nessus ist ein Tool, mit dem IT-Geräte gescannt werden können, um Schwachstellen zu erkennen. Mit OT Security können Sie den Basic Network Scan von Tenable Nessus für spezifische IT-Assets in Ihrem OT-Netzwerk durchführen. Dies ist ein aktiver Scan des gesamten Systems, der zusätzliche Informationen über Schwachstellen auf den Servern und Netzwerkgeräten sammelt. Dieser Scan verwendet die WMI- und SNMP-Zugangsdaten, wenn diese verfügbar sind. Diese Aktion ist nur für relevante PC-basierte Maschinen verfügbar. Die Scan-Ergebnisse können Sie auf der Seite „Schwachstellen“ einsehen. Sie können auch benutzerdefinierte Scans erstellen, um einen bestimmten Satz von Tenable Nessus-Plugins für einen bestimmten Satz von Netzwerkressourcen auszuführen, siehe Tenable NessusPlugin-Scans.

Der Nessus-Scan in OT Security verwendet die gleichen Richtlinieneinstellungen wie ein Netzwerk-Basisscan in Tenable Nessus, Tenable Security Center und Tenable Vulnerability Management. Der einzige Unterschied sind die Leistungsoptionen in OT Security. Im Folgenden sind die Leistungsoptionen für den Nessus-Scan in OT Security aufgeführt. Diese Optionen gelten auch für den Nessus-Scan, den Sie über die Seite Verwaltung aktiver Abfragen starten.

- 5 Hosts gleichzeitig (max.)
- 2 gleichzeitige Prüfungen pro Host (max.)
- 15 Sekunden Zeitüberschreitung für Lesevorgänge im Netzwerk

> Hinweis: Tenable Nessus ist ein invasives Tool, das am besten in IT-Umgebungen funktioniert. Tenable empfiehlt, es nicht auf OT-Geräten zu verwenden, da es deren normalen Betrieb beeinträchtigen kann.

### So führen Sie einen Tenable Nessus-Scan für bestimmte Assets aus:

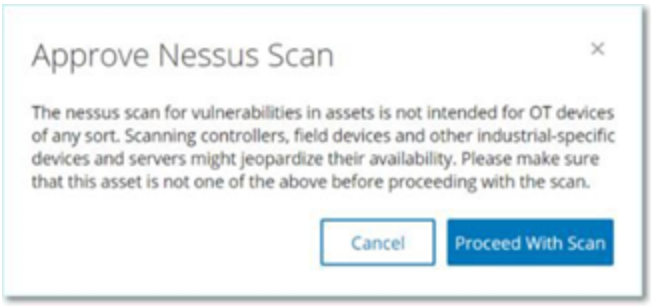
1. Gehen Sie zu Inventar > Netzwerk-Assets.

   Die Seite Netzwerk-Assets wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Assets, die Sie scannen möchten.

3. Klicken Sie in der oberen rechten Ecke auf Aktionen > Nessus-Scan.

Das Dialogfeld Nessus-Scan genehmigen wird angezeigt.




4. Klicken Sie auf Mit Scan fortfahren.

   OT Security führt den Nessus-Scan aus.

## Erneute Synchronisierung durchführen

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager, Sicherheitsanalyst, Site-Operator

Die Funktion „Erneut synchronisieren“ initiiert eine oder mehrere Abfragen an das Netzwerk und den Controller, um aktuelle Informationen für dieses Asset zu erfassen. Sie können alle verfügbaren Abfragen oder nur bestimmte Abfragen ausführen.

Die folgenden Abfragen sind für die Funktion „Erneut synchronisieren“ verfügbar:

- Backplane-Scan – Erfasst Module und ihre Spezifikationen innerhalb einer Backplane.
- DNS-Scanning – Sucht nach den DNS-Namen der Assets im Netzwerk.
- Detailabfrage – Ruft die Details zur Hardware und Firmware des Controllers ab. Das Ergebnis wird im Feld Firmware auf der Seite Assets > Controller und Module angezeigt.
- Identifizierungsabfrage – Verwendet mehrere Protokolle, um das Asset zu identifizieren.
- NetBIOS-Abfrage – Sendet ein NetBIOS-Unicast-Paket, mit dem Windows-Computer im Netzwerk klassifiziert und ermittelt werden.

- SNMP-Abfrage (für SNMP-fähige Assets) – Ruft Konfigurationsdetails für SNMP-fähige Assets ab.
- Status – Erkennt den aktuellen Status des Assets (d. h. Läuft, Angehalten, Fehler, Unbekannt und Test).
- ARP – Ruft die MAC-Adresse neuer IP-Adressen ab, die im Netzwerk erkannt wurden. Das Ergebnis wird im Abschnitt Details > Übersicht angezeigt.

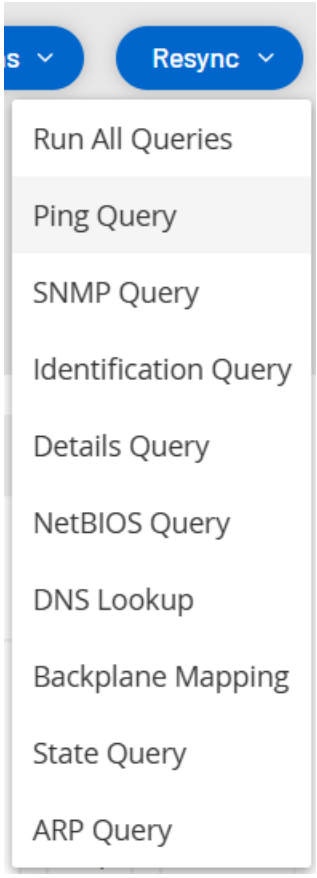
Die Schaltfläche Erneut synchronisieren kann unter bestimmten Bedingungen deaktiviert sein. Mögliche Gründe sind:

- Das Gerät ist nicht erreichbar oder es sind keine Abfragen verfügbar.
- Die auf der Seite Aktive Abfragen konfigurierte Berechtigung kann Konten ohne Administratorrechte daran hindern, bestimmte Abfragen zu initiieren.
- Abfragen sind für diese OT Security-Bereitstellung nicht aktiviert.
- Alle Abfragen im Abschnitt Aktive Abfragen > Manuell sind deaktiviert.
- Dem Asset fehlt eine bekannte IP-Adresse zum Abfragen.

### So führen Sie die erneute Synchronisierung von Asset-Daten aus:

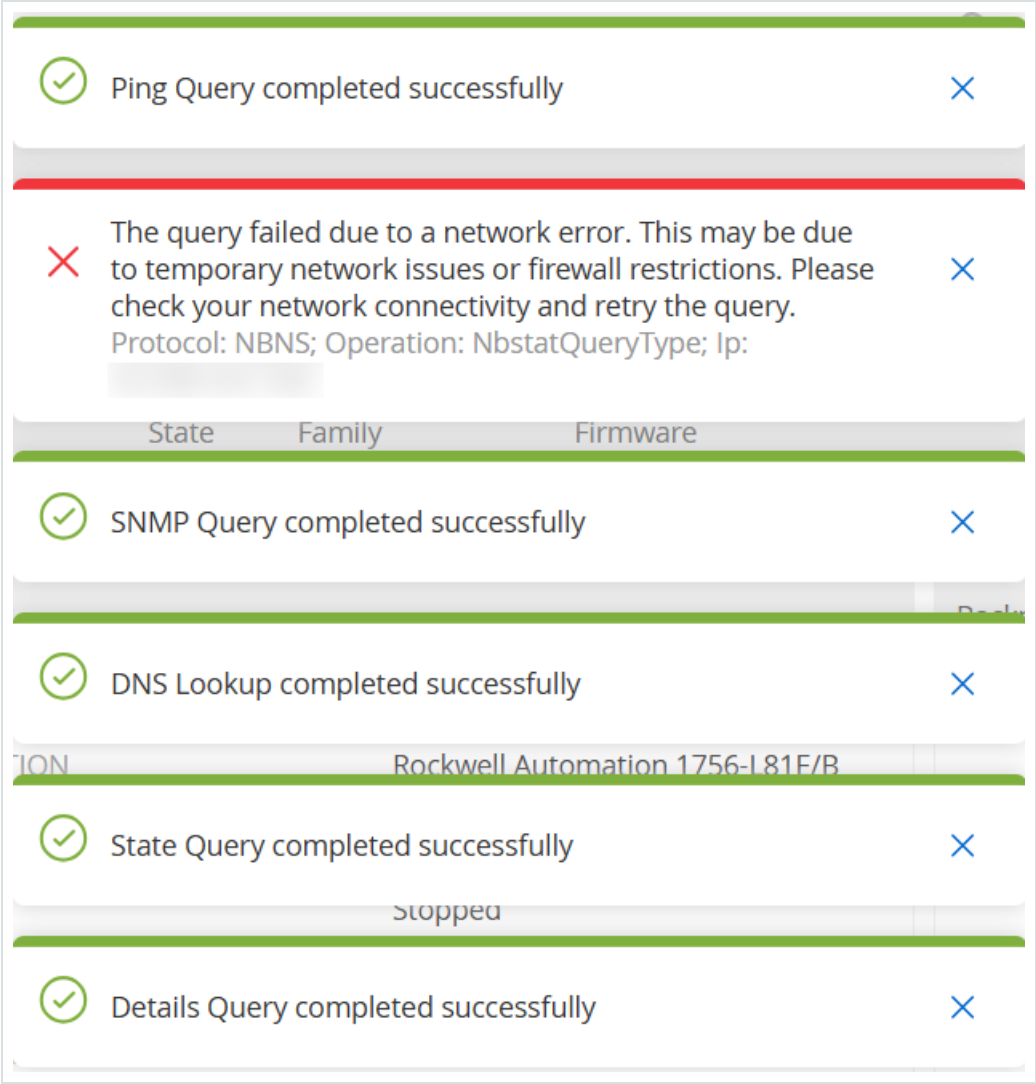
1. Klicken Sie auf der Seite Asset-Details für das gewünschte Asset in der oberen rechten Ecke auf Erneut synchronisieren.

   Eine Dropdown-Liste mit Abfragen wird angezeigt.




2. Klicken Sie auf die Abfrage, die Sie ausführen möchten, oder klicken Sie auf Alle Abfragen ausführen, um alle verfügbaren Abfragen auszuführen.

   Während die einzelnen Abfragen ausgeführt werden, wird eine Benachrichtigung mit dem Status der Abfrage angezeigt.




Für jede abgeschlossene Abfrage aktualisiert OT Security die Systemdaten für dieses Asset basierend auf den neuen Daten.

## Schwachstellen

OT Security identifiziert verschiedene Arten von Bedrohungen, von denen Assets in Ihrem Netzwerk betroffen sind. Sobald Informationen über neue Schwachstellen aufgedeckt und öffentlich

zugänglich gemacht werden, entwickeln Forschungsmitarbeiter von Tenable Programme, mit denen Tenable Nessus diese Schwachstellen erkennen kann.

Diese Programme werden als „Plugins“ bezeichnet und in der proprietären Tenable Nessus-Skriptsprache namens Tenable Nessus Attack Scripting Language (NASL) verfasst. Plugins erkennen CVEs sowie andere Bedrohungen, die Assets in Ihrem Netzwerk betreffen können (z. B. veraltete Betriebssysteme, Verwendung anfälliger Protokolle und anfällige offene Ports).

Plugins enthalten Schwachstelleninformationen, einen generischen Satz von Behebungsmaßnahmen sowie den Algorithmus, mit dem auf das Vorhandensein des Sicherheitsproblems getestet wird.

Informationen zum Aktualisieren Ihres Plugin-Satzes finden Sie unter Umgebungseinstellungen.

## Schwachstellen anzeigen

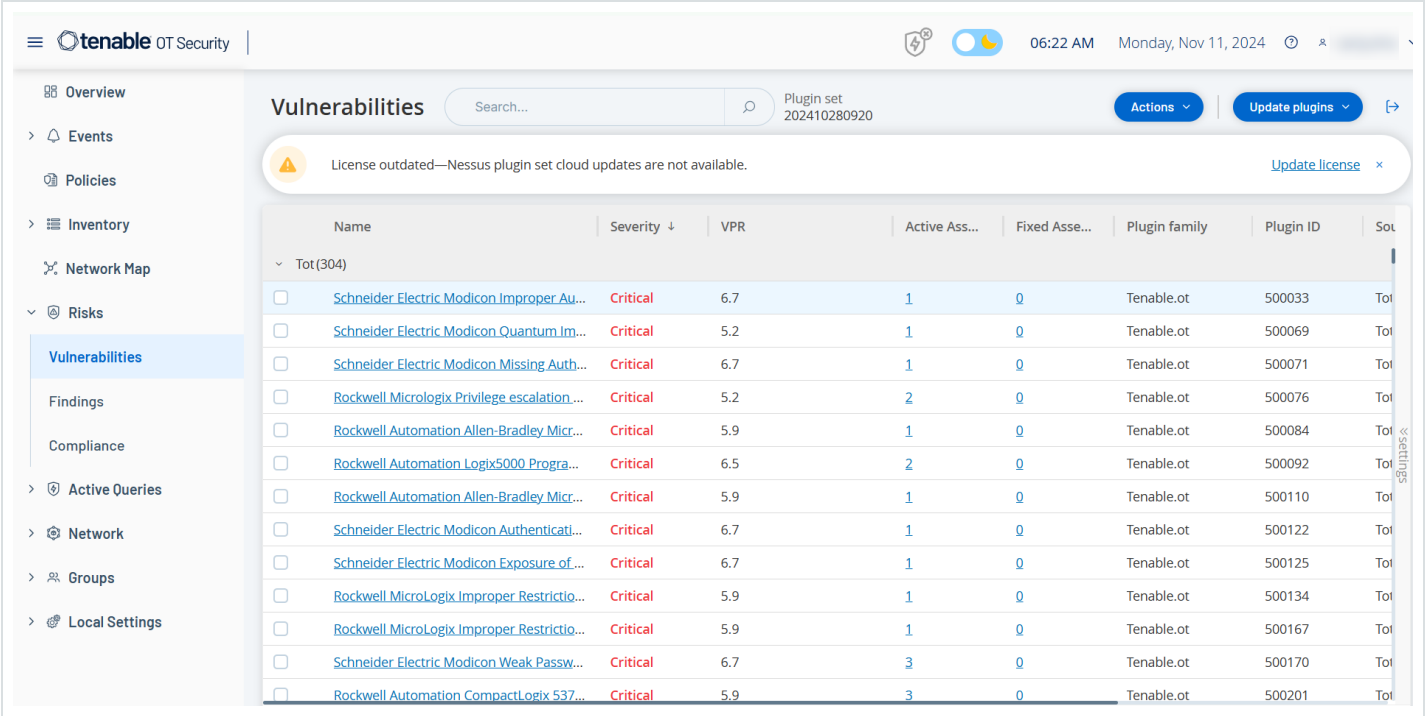
> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager, Sicherheitsanalyst, Site-Operator, Schreibgeschützt

Die Seite Schwachstellen enthält eine Liste aller von den Tenable-Plugins erkannten Schwachstellen, die Ihr Netzwerk und Ihre Assets betreffen.

Sie können die Anzeigeeinstellungen anpassen, indem Sie festlegen, welche Spalten angezeigt werden und wo die einzelnen Spalten positioniert sind. Eine Erläuterung der Anpassungsfunktionen finden Sie unter Elemente in der Benutzeroberfläche der Verwaltungskonsole.

(Nur für Version 3.19) Mit den Optionen Aktive Schwachstellen und Behobene Schwachstellen in der linken Navigationsleiste können Sie offene bzw. behobene Schwachstellen anzeigen.

> Hinweis: Behobene Schwachstellen werden in OT Security ein Jahr lang gespeichert, bevor sie als veraltet gelten.




Auf der Seite Schwachstellen werden die folgenden Details angezeigt:

| Parameter | Beschreibung |
|---|---|
| Name | Der Name der Schwachstelle. Der Name ist ein Link zur Anzeige der vollständigen Schwachstellenauflistung. |
| Schweregrad | Dieser Wert gibt den Schweregrad der von diesem Plugin erkannten Bedrohung an. Mögliche Werte: Info, Gering, Mittel, Hoch oder Kritisch. |
| VPR | Vulnerability Priority Rating (VPR) ist ein dynamischer Indikator des Schweregrads, der basierend auf der aktuellen Ausnutzbarkeit der Schwachstelle ständig aktualisiert wird. Dieser Wert wird von Tenable als Ausgabe von Predictive Prioritization generiert, eine Tenable-Funktion, die die technischen Auswirkungen und die Bedrohung durch die Schwachstelle bewertet. VPR-Werte reichen von 0,1 bis 10,0, wobei ein höherer Wert eine höhere Wahrscheinlichkeit einer Ausnutzung darstellt. |
| Plugin-ID | Der eindeutige Bezeichner des Plugins. |

| | |
|---|---|
| Aktive Assets | Die Anzahl der Assets in Ihrem Netzwerk, die aktuell von dieser Schwachstelle betroffen sind. |
| Behobene Assets | Die Anzahl der Assets in Ihrem Netzwerk, die von dieser Schwachstelle betroffen sind und für die die Schwachstelle kürzlich behoben wurde, über einen bestimmten Zeitraum (standardmäßig ein Jahr). Wenden Sie sich an Tenable-Support, um diesen Zeitraum anzupassen. |
| Plugin-Familie | Die Familie (Gruppe), der dieses Plugin zugeordnet ist. |
| Kommentar | Sie können Freitextkommentare zu diesem Plugin hinzufügen. |

## Plugin-Details

So zeigen Sie die Plugin-Details an:

1. Klicken Sie in der Zeile der Schwachstelle, für die Sie Details anzeigen möchten, auf den Namen der Schwachstelle.

   Das Fenster mit Schwachstellendetails wird angezeigt.

Hier finden Sie die folgenden Informationen:

- Kopfleiste – Enthält grundlegende Informationen zur angegebenen Schwachstelle. Um Schwachstellendetails zu bearbeiten, wählen Sie im Menü Aktionen die Option Details bearbeiten aus. Siehe Schwachstellendetails bearbeiten.
- Registerkarte „Details“ – Zeigt die vollständige Beschreibung der Schwachstelle und enthält Links zu relevanten Ressourcen.
- Registerkarte „Betroffene Assets“ – Zeigt eine Liste aller Assets, die von der angegebenen Schwachstelle betroffen sind. Jede Liste enthält detaillierte Informationen über das Asset sowie einen Link zum Aufrufen des Fensters „Asset-Details“ für das betreffende Asset.

## Schwachstellendetails bearbeiten

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager, Sicherheitsanalyst

So bearbeiten Sie Schwachstellendetails:

1. Klicken Sie auf der relevanten Seite mit Schwachstellendetails in der oberen rechten Ecke auf die Schaltfläche Aktionen.

   Das Menü Aktionen wird geöffnet.

2. Klicken Sie auf Details bearbeiten.

   Der Bereich Schwachstellendetails bearbeiten wird angezeigt.

3. Geben Sie im Feld Kommentare Kommentare zur Schwachstelle ein.

4. Geben Sie im Feld Besitzer den Namen der Person ein, die mit der Behebung der Schwachstelle beauftragt ist.

5. Klicken Sie auf Speichern.

## Plugin-Ausgabe anzeigen

Die Plugin-Ausgabe für ein Asset liefert Kontext oder eine Erklärung, warum ein bestimmtes Plugin für ein Asset aufgeführt wird.

### Plugin-Ausgabe unter „Schwachstellen“ anzeigen

So zeigen Sie die Plugin-Ausgabedetails über die Seite Schwachstellen an:

1. Gehen Sie zu Schwachstellen.

   Die Seite Schwachstellen wird angezeigt.

2. Wählen Sie in der Liste der Schwachstellen die Schwachstelle aus, für die Sie Details anzeigen möchten, und führen Sie einen der folgenden Schritte aus:

    - Klicken Sie auf den Schwachstellen-Link.
    - Klicken Sie mit der rechten Maustaste auf die Schwachstelle und wählen Sie Anzeigen aus.
    - Wählen Sie im Dropdown-Feld Aktionen die Option Anzeigen aus.

    Die Seite mit Schwachstellendetails wird angezeigt. Im Bereich Plugin-Ausgabe finden Sie die folgenden Informationen:

    - Trefferdatum
    - Quelle
    - Port
    - Plugin-Ausgabe

    > Hinweis: Die Plugin-Ausgabe ist nicht für alle Plugins verfügbar.

### Plugin-Ausgabe unter „Inventar“ anzeigen

So zeigen Sie die Plugin-Ausgabedetails über die Seite Inventar an:

1. Gehen Sie zu Inventar > Alle Assets.

    Die Seite Inventar wird angezeigt.

2. Wählen Sie in der Liste der Assets das Asset aus, für das Sie Details anzeigen möchten, und führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf den Asset-Link.
- Klicken Sie mit der rechten Maustaste auf das Asset und wählen Sie Anzeigen aus.
- Aktivieren Sie das Kontrollkästchen neben dem Asset und wählen Sie dann im Dropdown-Feld Aktionen die Option Anzeigen aus.

Die Seite mit Asset-Details wird geöffnet.

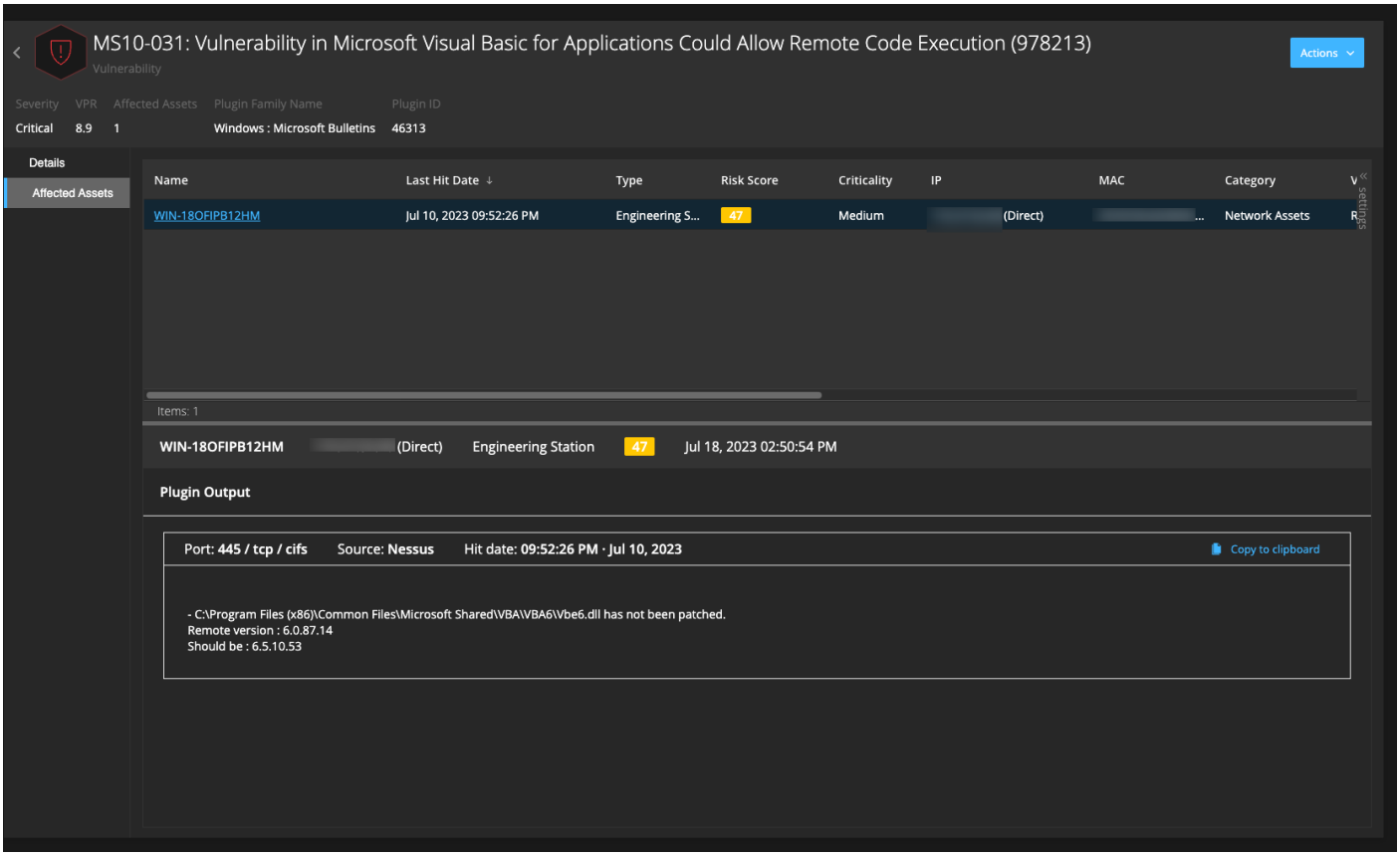
3. Klicken Sie auf die Registerkarte Schwachstellen.

   Die Liste der Schwachstellen wird angezeigt. Im Bereich Plugin-Ausgabe finden Sie die folgenden Informationen:

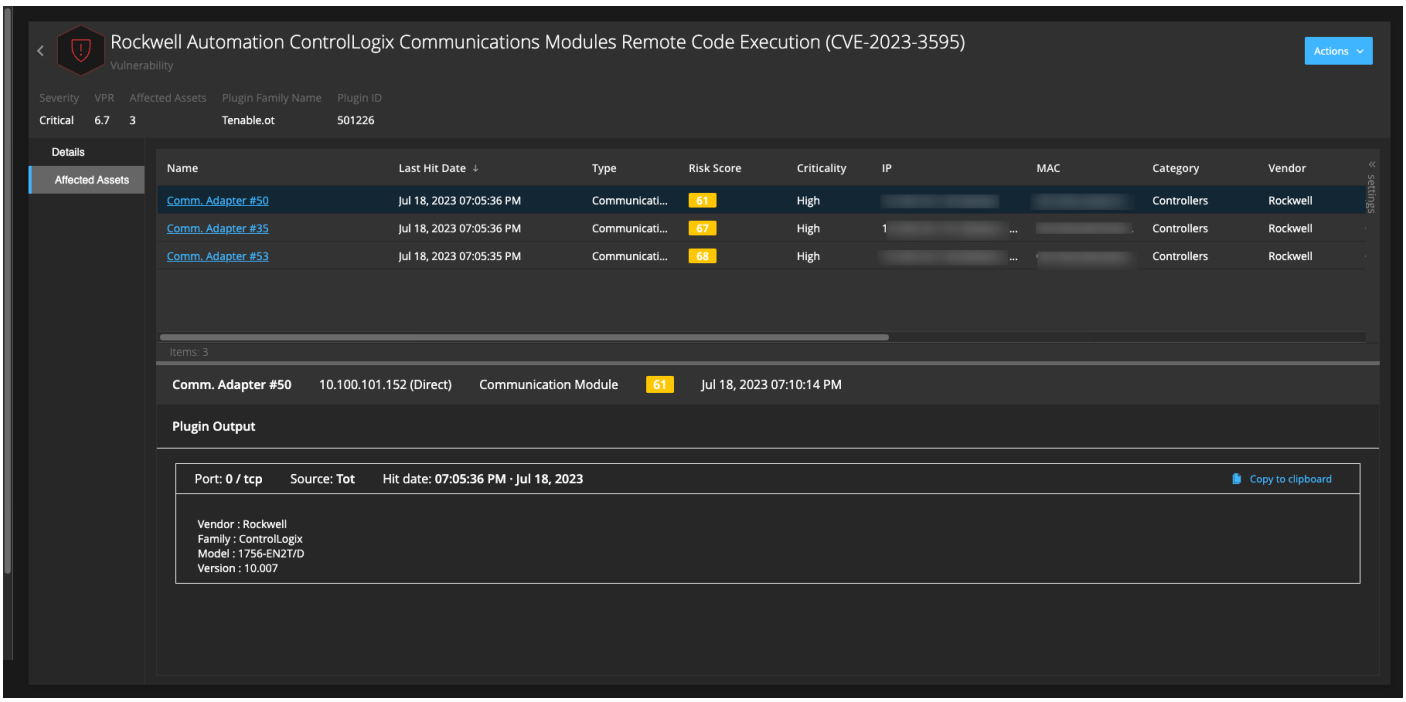
   - Trefferdatum
   - Quelle
   - Port
   - Plugin-Ausgabe

   > Hinweis: Die Plugin-Ausgabe ist nicht für alle Plugins verfügbar.

Beispiel einer Plugin-Ausgabe für ein Tenable Nessus-Plugin




Beispiel einer Plugin-Ausgabe für ein OT Security-Plugin



# Feststellungen

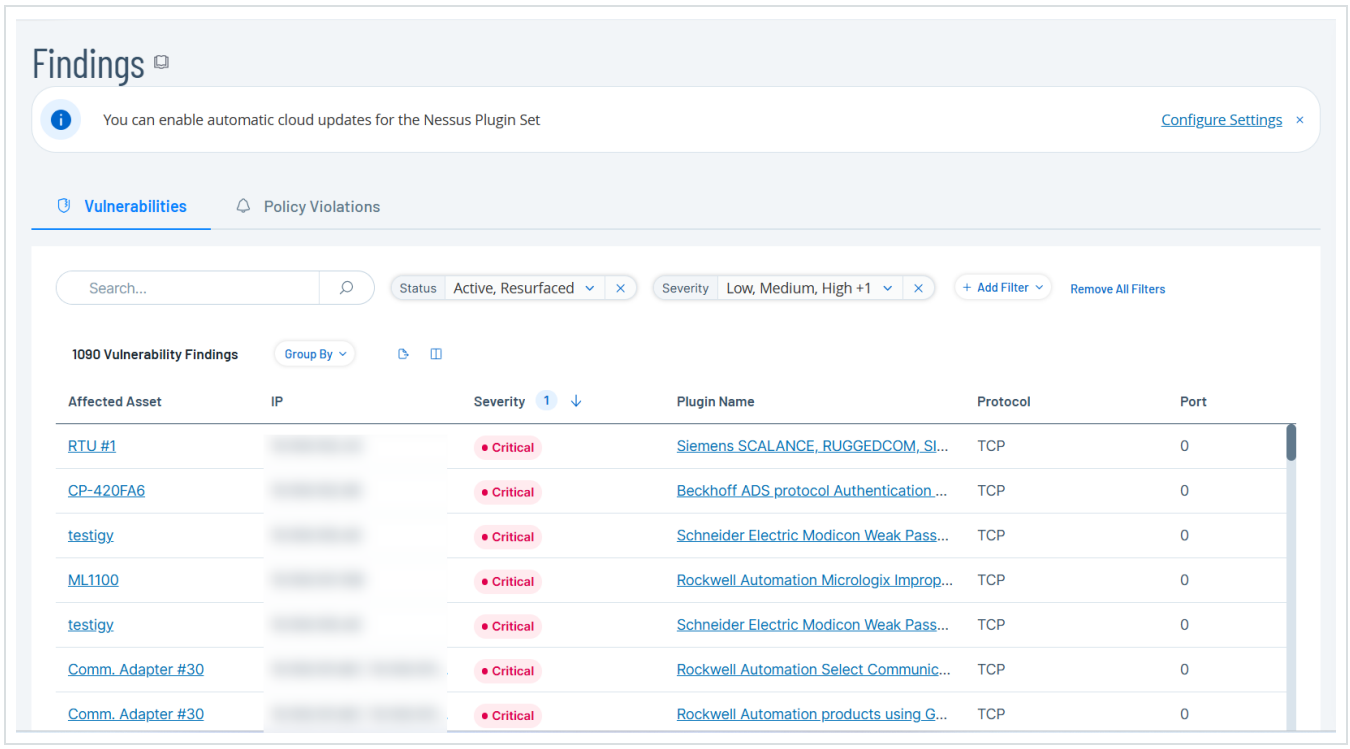
Auf der Seite Feststellungen können Sie die Liste der einzelnen Instanzen von Schwachstellen, die Ihre Umgebung betreffen, pro Asset überprüfen. Die Seite Feststellungen bietet Ihnen folgende Möglichkeiten:

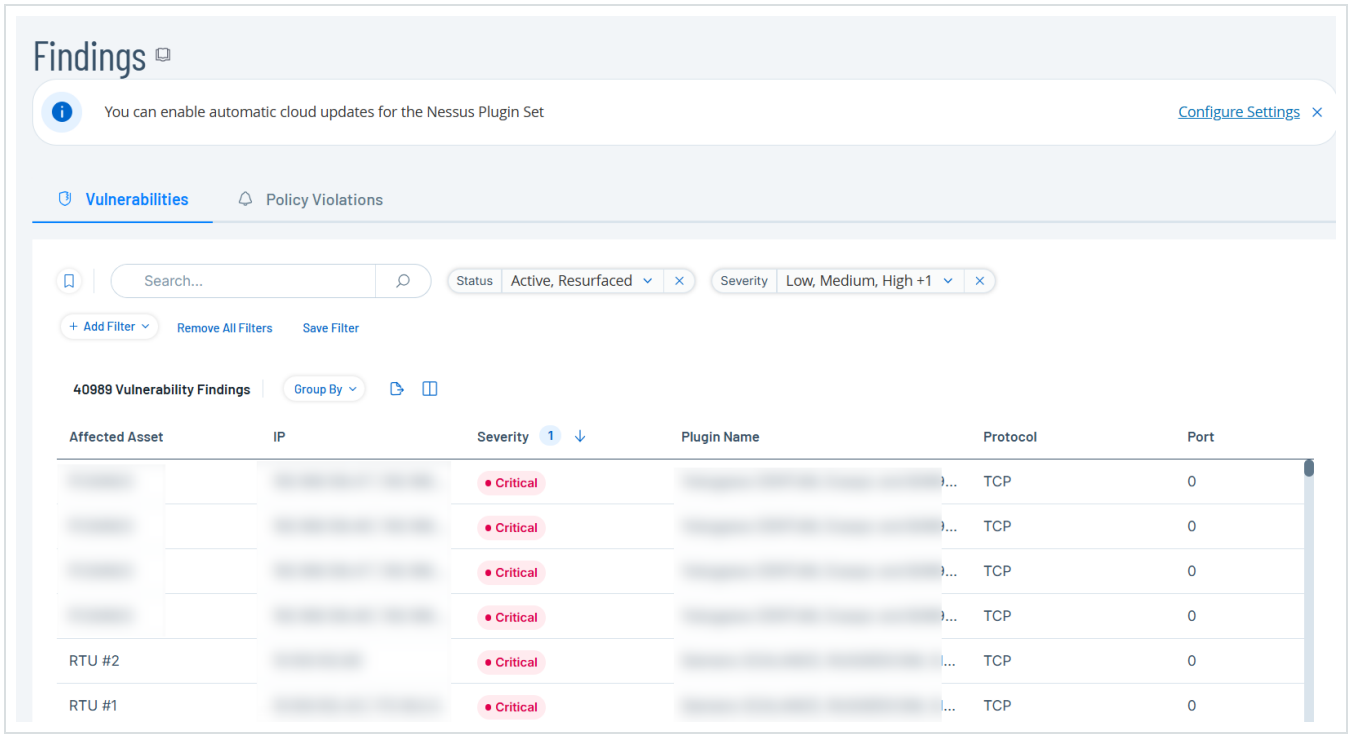
- Detaillierte Beweise für jeden spezifischen „Treffer“ einer Schwachstelle in Ihrer Umgebung anzeigen
- Die Liste der Schwachstellen entweder nach Eigenschaften des Plugins, des betroffenen Assets oder der spezifischen Instanz (z. B. Status, Letzter Treffer) oder nach einer beliebigen Kombination der Eigenschaften filtern
- Die gefilterte Liste der Feststellungen exportieren, um sie zur Behebung zuzuweisen

So greifen Sie auf die Seite Feststellungen zu:

1. Gehen Sie im linken Navigationsmenü zu Risiken > Feststellungen.

   Die Seite Feststellungen wird mit den Schwachstellen im Tabellenformat angezeigt.




Die Tabelle Feststellungen enthält die folgenden Details:

| Spalte | Beschreibung |
| --- | --- |
| Betroffenes Asset | Das Asset, bei dem die Schwachstelle erkannt wurde. |
| IP | Die IP-Adresse des Assets. |
| Schweregrad | Der Schweregrad der Schwachstelle: Kritisch, Mittel, Gering oder Information. |
| Plugin-Name | Das Plugin, das die Schwachstelle erkannt hat. |
| Plugin-ID | Die ID des Plugins. |
| Port | Der Port, an dem die Schwachstelle erkannt wurde. |
| Protokoll | Das Protokoll, das für die Kommunikation mit dem Asset verwendet wird. |
| VPR | Vulnerability Priority Rating (VPR) für die Schwachstelle. |
| Status | Der Status der Schwachstelle. Die möglichen Werte sind:<br><br>Aktiv – Gibt an, dass die Schwachstelle seit ihrer ersten Erkennung kontinuierlich aufgetreten ist.<br><br>Behoben – Gibt an, dass die Schwachstelle zunächst aufgetreten und verschwunden und danach nicht erneut aufgetreten ist.<br><br>Erneut aufgetreten – Gibt an, dass die Schwachstelle aufgetreten und verschwunden und anschließend erneut aufgetreten ist. |
| Plugin-Quelle | Die Plugin-Quelle. |
| Erster Treffer | Der Zeitpunkt, zu dem die Schwachstelle zum ersten Mal erkannt wurde. |

| Spalte | Beschreibung |
| --- | --- |
| Letzter Treffer | Der Zeitpunkt, zu dem die Schwachstelle zum letzten Mal erkannt wurde. |
| Asset-Tags | Die mit dem Asset verknüpften Tags. Siehe Asset-Tags und Gruppen. |
| Behoben am | Der Zeitpunkt, zu dem die Schwachstelle behoben wurde. |
| Plugin-Familie | Die Familie des Plugins. |
| Asset-Typ | Der Asset-Typ, z. B. SPS und OT-Gerät. |
| Asset-Risikowert | Der Risikowert des Assets. |
| Asset-Kategorie | Die Kategorie, zu der das Asset gehört, z. B. Controller, Netzwerk-Assets. |
| Asset-Anbieter | Der Name des Anbieters des Assets. |
| Asset-Kritikalität | Die Kritikalität des Assets, basierend auf dem Schweregrad der Schwachstelle: hohe Kritikalität, mittlere Kritikalität oder geringe Kritikalität. |
| Asset-Familie | Die Familie des Assets. |
| Asset-Modell | Das Modell des Assets. |
| Firmware | Die Firmware des Assets. |
| Betriebssystem | Das Betriebssystem, auf dem das Asset ausgeführt wird. |
| Asset-Status | Der aktuelle Status des Assets. |
| Purdue-Level | Der Purdue-Level des Assets. |

| Spalte | Beschreibung |
| --- | --- |
| Netzwerksegment | Das Netzwerksegment, zu dem das Asset gehört. |
| Standort | Der Standort des Assets. |
| Backplane-Name | Der Name der Backplane, auf der die Schwachstelle erkannt wurde. |

## Details zu Feststellungen anzeigen

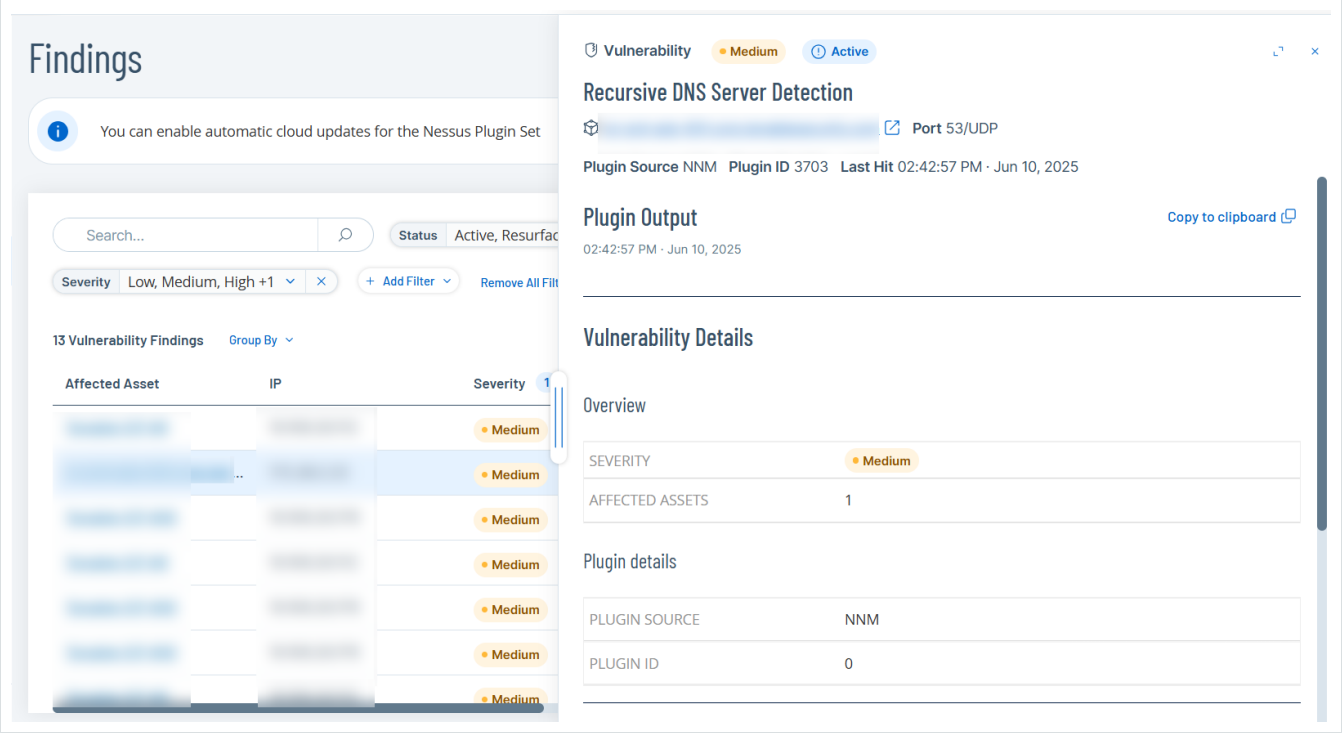
Die Details zu Feststellungen umfassen Folgendes:

- Plugin-Ausgabe
- Schwachstellendetails
- Betroffene Asset-Details

### So zeigen Sie Details zu Feststellungen an:

1. Klicken Sie auf der Seite Feststellungen auf den Link in der Spalte Betroffene Assets oder Plugin-Name.

   Der Bereich Schwachstellendetails wird angezeigt.




Sie sehen die folgenden Details:

- Schweregrad
- Betroffene Assets
- Plugin-Quelle
- Plugin-ID
- Details zu betroffenen Assets wie Name, Typ, Kritikalität, Risikowert, IP-Adresse, Purdue-Level.

- Um den Bereich mit Schwachstellendetails zu erweitern, klicken Sie oben rechts auf die Schaltfläche ⌞⌝.
- Um den Bereich zu schließen, klicken Sie oben rechts auf die Schaltfläche ×.
- Um die vollständigen Asset-Details anzuzeigen, klicken Sie im Abschnitt Betroffenes Asset auf Vollständige Asset-Details anzeigen ⧉.

- In OT Security wird eine separate Browser-Registerkarte mit der Seite Inventar geöffnet, auf der Details zu den einzelnen Assets angezeigt werden.

## Richtlinienverstöße

Auf der Seite Richtlinienverstöße werden alle Ereignisse angezeigt, die mit derselben Richtlinie, derselben Quelle und demselben Ziel verknüpft sind. Jede Feststellung auf der Seite ist eine Aggregation von mehreren Ereignissen, die durch dieselben Richtlinientreffer mit identischer Quelle und Zieladresse verursacht wurden.

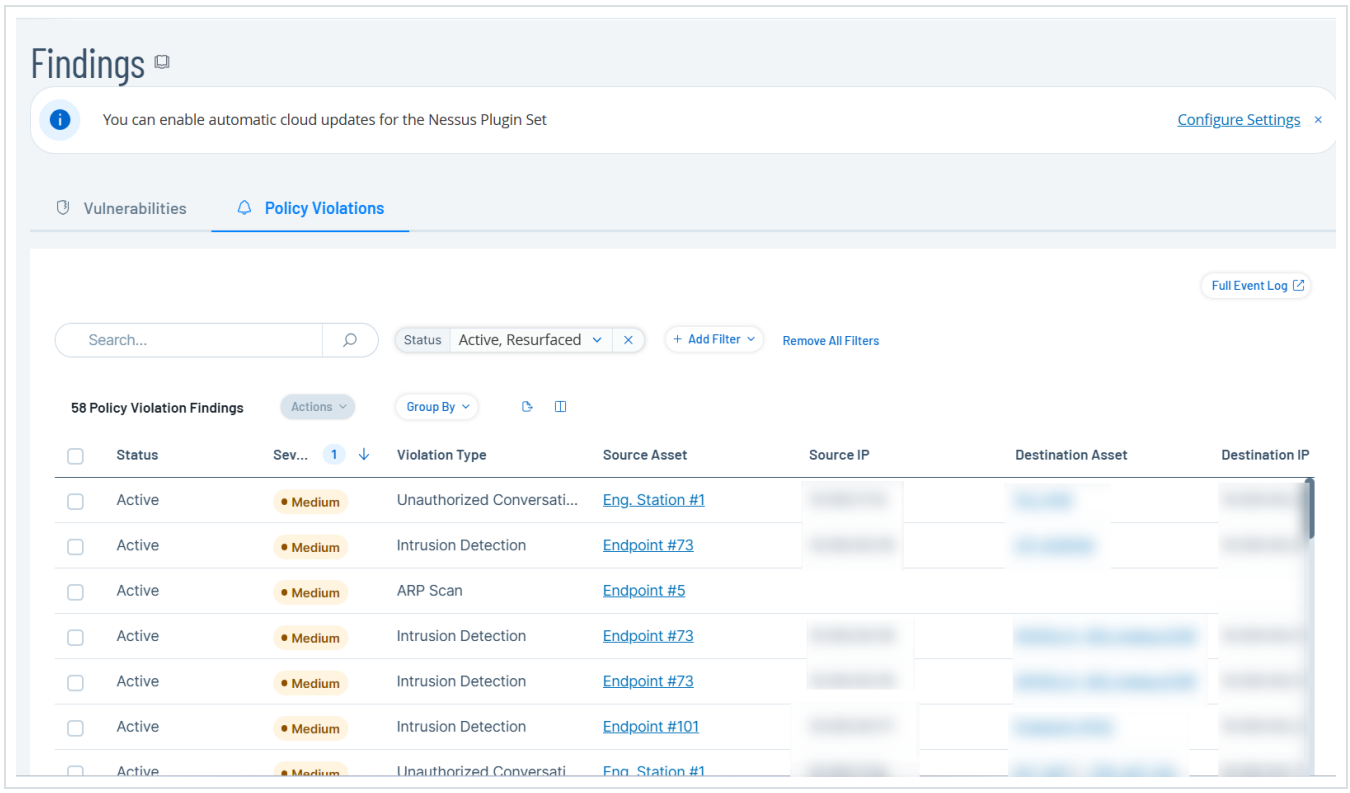
So greifen Sie auf die Seite Richtlinienverstöße zu:

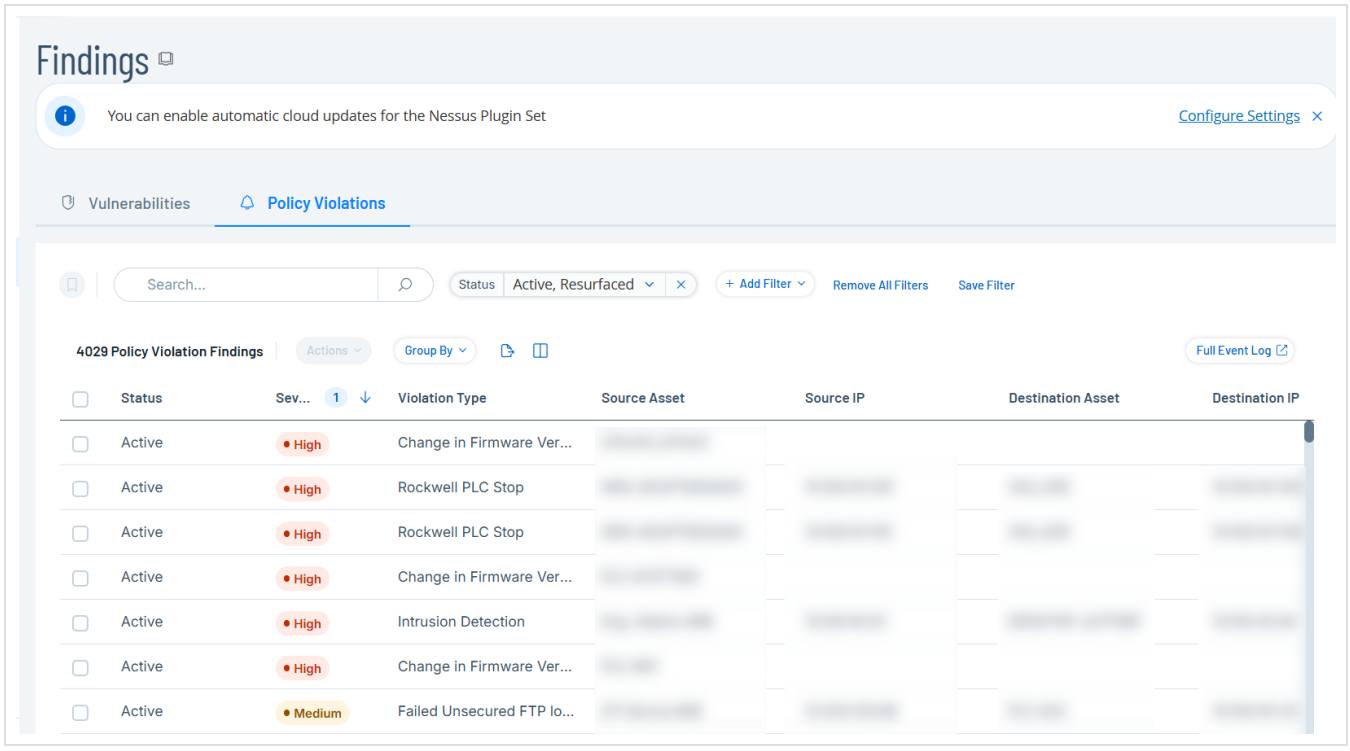
1. Klicken Sie im linken Navigationsmenü auf Risiken > Feststellungen.

   Die Seite Feststellungen wird angezeigt.

2. Klicken Sie auf die Registerkarte Richtlinienverstöße.

   Die Seite Richtlinienverstöße wird mit der Liste der Ereignisse angezeigt.




Die Registerkarte Richtlinienverstöße enthält die folgenden Angaben:

| Spalte | Beschreibung |
| --- | --- |
| ID | Die ID des Verstoßes. |
| Status | Der Status des Verstoßes: „Aktiv“, „Erneut aufgetreten“ oder „Aufgelöst“. |
| Schweregrad | Der Schweregrad des Verstoßes: „Hoch“, „Mittel“ oder „Gering“. |
| Verstoßtyp | Die Art des Verstoßes. Zum Beispiel „Nicht autorisierte Konversation“ und „Intrusion Detection“. |
| Verstoßkategorie | Die Kategorie, zu der der Verstoßtyp gehört. |
| Richtlinie | Die Richtlinie, die den Verstoß verursacht hat. |
| Plugin-Name | Die mit dem Verstoß verbundenen Plugins. |
| Mitre ICS-Taktiken | Der Grund hinter einer bestimmten Mitre Attack-Technik für industrielle Steuerungssysteme (ICS). |
| Mitre ICS-Techniken | Die Methode, mit der ein Gegner ein taktisches Ziel erreicht. |
| Quell-Asset | Das Asset, von dem der Verstoß ausgegangen ist. |
| Quell-IP | Die IP-Adresse des Quell-Assets. |
| Ziel-Asset | Das Asset, bei dem der Verstoß endete. |
| Ziel-IP | Die IP-Adresse des Ziel-Assets. |
| Protokoll | Das mit dem Verstoß verbundene Protokoll. |
| Erster Treffer | Der Zeitpunkt, zu dem der Verstoß zum ersten Mal erkannt wurde. |
| Letzter Treffer | Der Zeitpunkt, zu dem der Verstoß zum letzten Mal erkannt |

| Spalte | Beschreibung |
| --- | --- |
| | wurde. |
| Aktive Treffer | Die Anzahl der Ereignisse, die zu dem Verstoß geführt haben. |
| Asset-Typ | Die Art des Assets, bei dem der Verstoß erkannt wurde. |
| Asset-Kritikalität | Die Kritikalität des Assets. |
| Asset-Anbieter | Der mit dem Asset verbundene Anbieter. |
| Asset-Familie | Die Familie, zu der das Asset gehört. |
| Asset-Tags | Die mit dem Asset verknüpften Tags. |
| Purdue-Level | Der Purdue-Level des Assets. |
| Asset-Standort | Die Region, in der sich das Asset befindet. |
| Aufgelöst am | Das Datum, an dem der Verstoß aufgelöst wurde. |
| Aufgelöst von | Der Benutzer, der den Verstoß aufgelöst hat. |
| Kommentar | Die Kommentare, die der Benutzer bei der Auflösung des Verstoßes eingegeben hat. |

3. (Optional) Sie können auf der Seite Verstöße die folgenden Aktionen ausführen:
    - Passen Sie Spalten wie in Tabellen anpassen beschrieben an.
    - Filtern Sie die Tabelle „Feststellungen“. Siehe Tabellen filtern.
    - Exportieren Sie die Daten im CSV-Format.

## Menü Aktionen

Eine Feststellung auflösen

- So lösen Sie eine Feststellung auf:

    a. Wählen Sie die Zeile der Feststellung aus und klicken Sie auf Aktionen > Auflösen.

    Der Bereich Auflösen wird angezeigt.

    b. Geben Sie einen Kommentar zur Auflösung der Feststellung ein.

    c. Klicken Sie auf Speichern.

    OT Security löst die Feststellung auf und im Bereich Plugin-Details wird für den Status Aufgelöst angezeigt.

    > Hinweis: Wenn das Ereignis erneut auftritt, öffnet OT Security die Feststellung erneut und für den Status wird Erneut aufgetreten angezeigt.

Aus Richtlinie ausschließen

- So schließen Sie die Feststellung aus einer Richtlinie aus:

    a. Wählen Sie die Zeile der Feststellung aus und klicken Sie auf Aktionen > Aus Richtlinie ausschließen.

    Der Bereich Aus Richtlinie ausschließen wird angezeigt.

    b. Wählen Sie die Ausschlussbedingungen aus.

    > Hinweis: Die Ausschlussbedingungen basieren auf dem letzten und jüngsten Ereignis.

    c. Geben Sie eine Ausschlussbeschreibung ein.

    d. Klicken Sie auf Speichern.

    OT Security schließt das letzte Ereignis aus der Richtlinie aus.

Letzte Erfassungsdatei herunterladen

- So laden Sie die letzte Erfassungsdatei herunter:

    a. Wählen Sie die Zeile der Feststellung aus und klicken Sie auf Aktionen > Letzte Erfassungsdatei herunterladen.

    OT Security lädt die Erfassungsdatei für das letzte Ereignis herunter.

### Plugin-Details

So zeigen Sie die Details des Plugins für die Feststellung an:

1. Klicken Sie auf der Registerkarte Richtlinienverstöße auf die Zeile der Feststellung, um die zugehörigen Plugin-Details anzuzeigen.

    Der Bereich mit den Plugin-Details wird mit Angaben zu den Verstößen von der OT Security-Plugins-Seite angezeigt.

    Im Bereich werden die Details des Verstoßes auf vier separaten Registerkarten angezeigt: Details, Quelle, Ziele und Richtlinie.

### Nach Ereignissen suchen

So suchen Sie nach bestimmten Ereignissen, die den Verstoß verursacht haben:

a. Um die Ereignisse für eine bestimmte Feststellung zu suchen, klicken Sie auf Feststellungs-ID kopieren.

b. Klicken Sie auf den Link Vollständiges Ereignisprotokoll, um zur Seite Ereignisse zu wechseln.

    Die Seite Alle Ereignisse wird angezeigt.

c. Fügen Sie im Feld Suche die zuvor kopierte Feststellungs-ID ein.

    OT Security listet die Ereignisse für die jeweilige Feststellung auf.

# Compliance-Dashboard

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager, Sicherheitsanalyst, Site-Operator, Schreibgeschützt

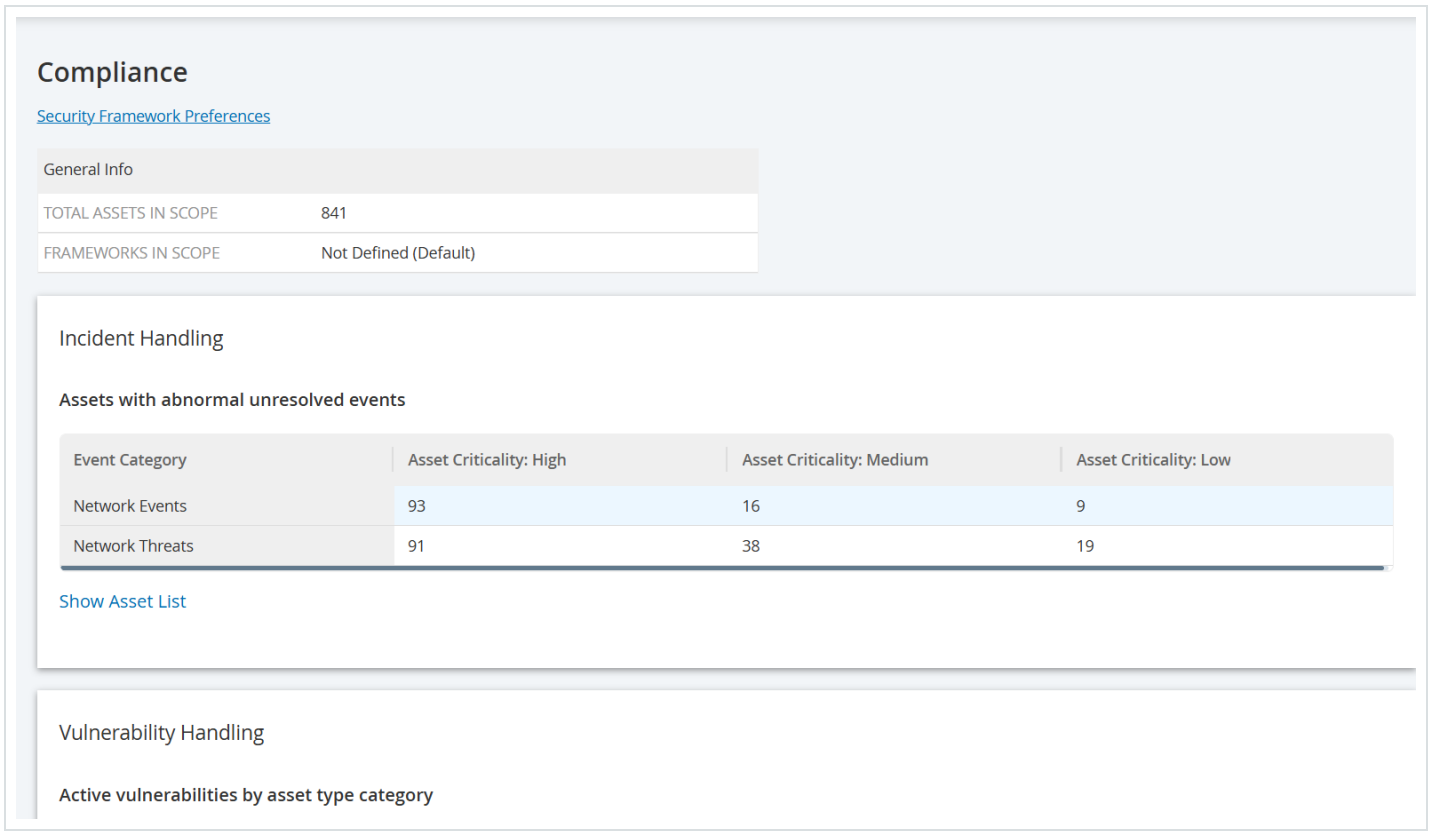
Die Einhaltung von Sicherheits-Frameworks wie der NIS 2-Richtlinie und der ISO 27001-Kontrollen ist jetzt für die meisten im Bereich kritischer Infrastrukturen tätigen Unternehmen obligatorisch, um Auditprüfungen zu bestehen.

Die Umsetzung von Compliance-Frameworks kann komplex sein und erfordert Fachwissen. Verwenden Sie das Compliance-Dashboard, um sich einen allgemeinen Überblick über alle Assets, Schwachstellen und Ereignisse zu verschaffen, die sich auf die kritischen Geschäftsabläufe Ihrer Organisation auswirken könnten, und um die folgenden kritischen Auditfragen zu beantworten:

- Über welche Sicherheitsrichtlinien verfügen Sie, um verdächtige Aktivitäten zu erkennen?
- Wie lange brauchen Sie, um einen Vorfall zu bearbeiten?
- Sind die Warnungen als Teil Ihres Vorfallsreaktionsplans (Incident Response, IR) in SOC/SIEM integriert?
- Wie viele Sicherheitsereignisse sind in der letzten Woche oder im letzten Monat bei Ihren kritischen Assets aufgetreten?

Über das Compliance-Dashboard können Sie wichtige Sicherheitsmaßnahmen an regulatorische Vorschriften anpassen, Ihre Fortschritte und Verbesserungen im Laufe der Zeit verfolgen und Ihre Sicherheitslage stärken.

Mithilfe der Dashboard-Daten können Sie Bereiche identifizieren, in denen das Unternehmen die Vorgaben einhält, und Bereiche verbessern, die ein Risiko für Ihr Unternehmen darstellen.




So zeigen Sie das Compliance-Dashboard an:

1. Klicken Sie in der linken Navigationsleiste auf Dashboards > Compliance.

   Das Compliance-Dashboard wird angezeigt.

2. Klicken Sie in der linken Navigationsleiste auf Risiken > Compliance.

   Das Compliance-Dashboard wird angezeigt.

Hinweis: Um die Einstellungen Ihres Sicherheits-Frameworks zu konfigurieren, gehen Sie zu Lokale Einstellungen > Systemkonfiguration > Compliance. Weitere Informationen finden Sie unter Einstellungen für das Compliance-Dashboard festlegen.

Das Dashboard enthält die folgenden Widgets.

Tipp: Fahren Sie mit dem Mauszeiger über das Symbol ⓘ neben den Widget-Abschnitten, um weitere Informationen zu den Framework-Maßnahmen zu erhalten, auf die sich die einzelnen Widgets beziehen.

| Widget | Beschreibung |
| --- | --- |
| Handhabung von Vorfällen | Dieses Widget bietet einen Überblick über die gefährdeten Assets nach ihrer Asset-Kritikalität: Hoch, Mittel oder Gering. Sie können diese Daten verwenden, um auf Sicherheitsvorfälle mit hohem Risiko zu reagieren.<br><br>Auf der Grundlage der Auflösung von Ereignissen mit hohem bis kritischen Schweregrad in den letzten 30 Tagen zeichnet OT Security die Mittlere Reaktionszeit für Ereignisse (MTTR) auf. Dieser Wert gibt Aufschluss über die mittlere Zeit, die für die Reaktion auf die einzelnen kritischen Ereignisse benötigt wird. MTTR ist ein wichtiger Leistungsindikator und ein niedrigerer MTTR-Wert weist auf einen effizienteren Prozess für die Vorfallbehebung hin.<br><br>Hinweis: Um alle Assets mit hohem Risiko und verdächtigen offenen Ereignissen anzuzeigen, klicken Sie auf den Link Asset-Liste einblenden. Um die Asset-Liste zu schließen, klicken Sie auf Asset-Liste ausblenden. |
| Handhabung von Schwachstellen | Dieses Widget bietet einen Überblick über alle Schwachstellen nach ihrem Schweregrad und den betroffenen Asset-Typen. Mit diesem Widget können Sie OT-, Netzwerk- und IoT-Schwachstellen kontinuierlich identifizieren, bewerten, melden und beheben.<br><br>Auf der Grundlage der in den letzten 90 Tagen behobenen Schwachstellen zeichnet OT Security die mittlere Reaktionszeit (MTTR) auf. MTTR- und SLA-Parameter (Service Level Agreement) geben Aufschluss über die durchschnittliche Reaktionszeit für die einzelnen kritischen Schwachstellen und |

| Widget | Beschreibung |
| --- | --- |
| | helfen dabei, die Fortschritte des Teams bei der Eindämmung von Schwachstellen auf der Grundlage der definierten SLAs zu verfolgen. Ein niedrigerer MTTR-Wert weist auf einen effizienteren Prozess für die Vorfallbehebung hin.<br><br>Hinweis: Um alle Assets mit hohem Risiko und aktiven kritischen Schwachstellen anzuzeigen, klicken Sie auf Asset-Liste einblenden. Um die Asset-Liste zu schließen, klicken Sie auf Asset-Liste ausblenden. |
| Konfiguration und Änderungsmanagement | Dieses Widget bietet einen Überblick über alle Assets mit nicht aufgelösten Konfigurationsereignissen, wie z. B. Änderungen, die nach dem Festlegen einer Baseline vorgenommen wurden, und kritische Controller-Statusaktivitäten wie dem Anhalten des Geräts. Die Daten in diesem Widget helfen Ihnen dabei, nicht autorisierte Änderungen und kritische Ereignisse zu erkennen und dadurch die Betriebskontinuität und eine schnelle Wiederherstellung bei Serviceunterbrechungen sicherzustellen.<br><br>Hinweis: Um Assets mit hohem Risiko und Konfigurationsänderungs-Ereignissen anzuzeigen, klicken Sie auf den Link Asset-Liste einblenden. Um die Asset-Liste zu schließen, klicken Sie auf Asset-Liste ausblenden. |
| Externes Exposure-Risiko | Dieses Widget bietet einen Überblick über externe Verbindungen zu ICS-Netzwerken (Industrial Control System, industrielles Steuerungssystem). Sie können die Daten in diesem Widget verwenden, um unerwartete externe Kommunikation in OT-, Netzwerk- und IoT-Assets zu identifizieren, zu bewerten und zu entschärfen. Diese Daten stellen außerdem die Einhaltung von Supply-Chain- |

| Widget | Beschreibung |
| --- | --- |
| | Sicherheitsmaßnahmen sicher, wenn Anbieter von ICS-Ausrüstung und -Maschinen Hybridmodelle verwenden und ihre Portale und Engineering-Stationen in die Cloud verlagern, wo die Möglichkeit einer externen Gefährdung besteht. |
| Unsichere Kryptographie | Dieses Widget bietet einen Überblick über unsichere kryptografische Ereignisse, wie z. B. nicht abgesicherte Logins und unverschlüsselte Zugangsdaten. Diese Daten können dabei helfen, unsichere kryptografische Ereignisse zu überwachen und zu erkennen und somit die Kompromittierung vertraulicher Daten und Serviceunterbrechungen zu verhindern.<br><br>Hinweis: Um alle Assets mit hohem Risiko und unsicheren Authentifizierungsereignissen anzuzeigen, klicken Sie auf den Link Asset-Liste einblenden. Um die Asset-Liste zu schließen, klicken Sie auf Asset-Liste ausblenden. |
| Überwachung unsicherer Kommunikation | Dieses Widget bietet einen Überblick über Assets mit hohem Risiko und nicht abgesicherten Kommunikationsereignissen sowie nicht autorisiertem Zugriff. Diese Daten können dabei helfen, unsichere Kommunikation und verdächtige, nicht authentifizierte Zugriffe zu vermeiden, die vertrauliche Daten oder kritische Assets für Angreifer offenlegen können.<br><br>Hinweis: Um alle Assets mit hohem Risiko und unsicheren Authentifizierungsereignissen anzuzeigen, klicken Sie auf den Link Asset-Liste einblenden. Um die Asset-Liste zu schließen, klicken Sie auf Asset-Liste ausblenden. |
| Risikobewertung | Dieses Widget bietet einen Überblick über gefährdete Assets nach ihrer Kritikalität. Diese Daten helfen Ihnen, die mit OT-, |

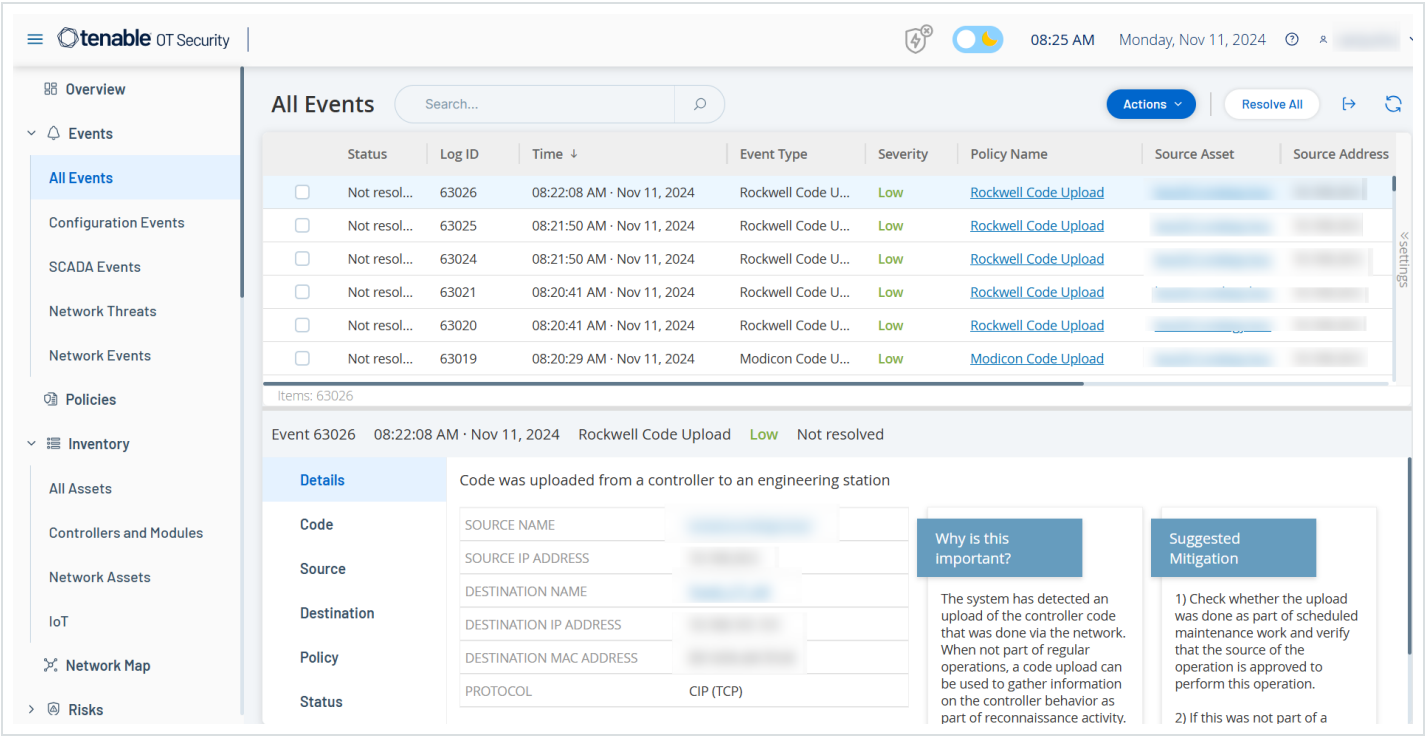
| Widget | Beschreibung |
| --- | --- |
| | Netzwerk- und IoT-Assets verbundenen Risiken zu bewerten und zu verwalten sowie potenzielle Bedrohungen proaktiv zu identifizieren und zu entschärfen.<br><br>Hinweis: Um alle Assets mit hohem Risiko anzuzeigen, klicken Sie auf den Link Asset-Liste einblenden. Um die Asset-Liste zu schließen, klicken Sie auf Asset-Liste ausblenden. |

# Ereignisse

Ereignisse sind vom System generierte Benachrichtigungen, um auf potenziell schädliche Aktivitäten im Netzwerk aufmerksam zu machen. Richtlinien, die Sie im OT Security-System einrichten, generieren Ereignisse in einer der folgenden Kategorien: Konfigurationsereignisse, SCADA-Ereignisse, Netzwerkbedrohungen oder Netzwerkereignisse. OT Security weist jeder Richtlinie einen Schweregrad zu, der den Schweregrad des Ereignisses angibt.

Sobald Sie eine Richtlinie aktivieren, löst jedes Ereignis im System, das den Richtlinienbedingungen entspricht, ein Ereignisprotokoll aus. Mehrere Ereignisse mit denselben Merkmalen werden in einem einzigen Cluster zusammengefasst.

## Anzeigen von Ereignissen




Alle Ereignisse, die im System aufgetreten sind, werden auf der Seite Alle Ereignisse angezeigt. Spezifische Untergruppen der Ereignisse werden in separaten Fenstern für jede dieser Ereigniskategorien angezeigt: Konfigurationsereignisse, SCADA-Ereignisse, Netzwerkbedrohungen und Netzwerkereignisse.

Für jede Ereignisseite (Konfigurationsereignisse, SCADA-Ereignisse, Netzwerkbedrohungen und Netzwerkereignisse) können Sie die Anzeigeeinstellungen anpassen, indem Sie auswählen, welche Spalten angezeigt und wo sie jeweils positioniert werden sollen. Sie können die Ereignisse nach Ereignistyp, Schweregrad und Richtlinienname gruppieren. Außerdem können Sie die Ereignislisten sortieren, filtern und durchsuchen. Weitere Informationen zu den Anpassungsfunktionen finden Sie unter Tabellen anpassen.

Verwenden Sie die Schaltfläche Aktionen in der Kopfleiste, um die folgenden Aktionen durchzuführen:

- Auflösen - Dieses Ereignis als „Aufgelöst“ markieren
- PCAP herunterladen - Die PCAP-Datei für dieses Ereignis herunterladen.
- Ausschließen - Einen Richtlinienausschluss für dieses Ereignis erstellen.

Im unteren Abschnitt der Seite werden auf verschiedenen Registerkarten Informationen zum ausgewählten Ereignis angezeigt. Es werden nur Registerkarten angezeigt, die für den Ereignistyp des ausgewählten Ereignisses relevant sind. Die folgenden Registerkarten werden für verschiedene Arten von Ereignissen angezeigt: Details, Code, Quelle, Ziel, Richtlinie, Gescannte Ports und Status.

> Hinweis: Sie können die Bereichstrennlinie nach oben oder unten ziehen, um die Anzeige des unteren Bereichs zu vergrößern/verkleinern.

Sie können die mit den einzelnen Ereignissen verknüpfte Paketerfassungsdatei herunterladen, siehe Netzwerk. Die für die einzelnen Ereignislisten angezeigten Informationen werden in der folgenden Tabelle beschrieben:

| Parameter | Beschreibung |
|---|---|
| Name | Der Name des Geräts im Netzwerk. Klicken Sie auf den Namen des Assets, um den Bildschirm „Asset-Details“ für dieses Asset anzuzeigen (siehe Inventar). |
| Adressen | Die IP- und/oder MAC-Adresse des Assets.<br>> Hinweis: Ein Asset kann mehrere IP-Adressen haben. |
| Typ | Der Asset-Typ. Eine Erläuterung der verschiedenen Asset-Typen finden Sie unter Asset-Typen. |
| Backplane | Die Backplane-Einheit, mit der der Controller verbunden ist. Weitere Details zur Backplane-Konfiguration werden im Bildschirm „Asset-Details“ angezeigt. |
| Slot | Bei Controllern, die sich auf Backplanes befinden, wird die Nummer des Steckplatzes angezeigt, an den der Controller angeschlossen ist. |
| Anbieter | Der Asset-Anbieter. |

| Parameter | Beschreibung |
|---|---|
| Familie | Der vom Controller-Anbieter definierte Name der Produktfamilie. |
| Firmware | Die aktuell auf dem Controller installierte Firmware-Version. |
| Standort | Der Standort des Assets, wie vom Benutzer in den Asset-Details von OT Security eingegeben. Siehe Inventar. |
| Zuletzt gesehen | Der Zeitpunkt, zu dem das Gerät zuletzt von OT Security gesehen wurde. Dies ist das letzte Mal, dass das Gerät mit dem Netzwerk verbunden war oder eine Aktivität durchgeführt hat. |
| Betriebssystem | Das Betriebssystem, das auf dem Asset ausgeführt wird. |
| Protokoll-ID | Die vom System generierte ID, um auf das Ereignis zu verweisen. |
| Uhrzeit | Das Datum und die Uhrzeit des Ereignisses. |
| Ereignistyp | Beschreibt die Art der Aktivität, die das Ereignis ausgelöst hat. Ereignisse werden von Richtlinien generiert, die im System eingerichtet sind. Eine Erläuterung der verschiedenen Arten von Richtlinien finden Sie unter Richtlinientypen. |
| Schweregrad | Zeigt den Schweregrad des Ereignisses an. Nachfolgend finden Sie eine Erläuterung zu den möglichen Werten:<br><br>Kein – Kein Grund zur Besorgnis.<br><br>Info – Kein unmittelbarer Grund zur Sorge. Sollte bei Gelegenheit geprüft werden.<br><br>Warnung – Moderate Bedenken, dass potenziell schädliche Aktivitäten stattgefunden haben. Sollte behandelt werden, wenn es passt.<br><br>Kritisch – Schwerwiegende Bedenken, dass potenziell schädliche |

| Parameter | Beschreibung |
| --- | --- |
| | Aktivitäten stattgefunden haben. Sollte sofort behandelt werden. |
| Richtlinienname | Der Name der Richtlinie, die das Ereignis generiert hat. Der Name ist ein Link zur Richtlinienliste. |
| Quell-Asset | Der Name des Assets, das das Ereignis initiiert hat. Dieses Feld ist ein Link zur Asset-Liste. |
| Quelladresse | Die IP- oder MAC-Adresse des Assets, das das Ereignis initiiert hat. |
| Ziel-Asset | Der Name des Assets, das von dem Ereignis betroffen war. Dieses Feld ist ein Link zur Asset-Liste. |
| Zieladresse | Die IP- oder MAC-Adresse des Assets, das von dem Ereignis betroffen war. |
| Protokoll | Sofern relevant, wird hier das Protokoll angezeigt, das für die Konversation verwendet wurde, die dieses Ereignis ausgelöst hat. |
| Ereigniskategorie | Zeigt die allgemeine Kategorie des Ereignisses an.<br><br>Hinweis: Im Bildschirm „Alle Ereignisse“ werden Ereignisse aller Typen angezeigt. Auf jedem der spezifischen Ereignisbildschirme werden nur Ereignisse der angegebenen Kategorie angezeigt.<br><br>Im Folgenden finden Sie eine kurze Erläuterung der Ereigniskategorien (für eine ausführlichere Erläuterung siehe Richtlinienkategorien und Unterkategorien):<br><br>• Konfigurationsereignisse – Dies umfasst zwei Unterkategorien<br><br>• Controller-Validierungsereignisse – Diese Richtlinien erkennen Änderungen, die in den Controllern im Netzwerk stattfinden. |

| Parameter | Beschreibung |
| --- | --- |
| | • Controller-Aktivitätsereignisse – Aktivitätsrichtlinien beziehen sich auf die Aktivitäten, die im Netzwerk stattfinden (d. h. die „Befehle“, die zwischen Assets im Netzwerk implementiert werden).<br>• SCADA-Ereignisse – Richtlinien, die Änderungen identifizieren, die an der Datenebene von Controllern vorgenommen wurden. • Netzwerkbedrohungsereignisse – Diese Richtlinien identifizieren Netzwerk-Traffic, der auf Bedrohungen durch Eindringlinge hinweist.<br>• Netzwerkereignisse – Richtlinien, die sich auf die Assets im Netzwerk und die Kommunikationsströme zwischen Assets beziehen. |
| Status | Zeigt an, ob das Ereignis als aufgelöst markiert wurde oder nicht. |
| Aufgelöst von | Zeigt für aufgelöste Ereignisse an, welcher Benutzer das Ereignis als aufgelöst markiert hat. |
| Aufgelöst am | Zeigt für aufgelöste Ereignisse an, wann das Ereignis als aufgelöst markiert wurde. |
| Kommentar | Zeigt alle Kommentare an, die hinzugefügt wurden, als das Ereignis aufgelöst wurde. |

## Anzeigen von Ereignisdetails

Unten auf der Seite Ereignisse werden zusätzliche Details zum ausgewählten Ereignis angezeigt. Die Informationen sind in Registerkarten unterteilt. Es werden nur Registerkarten angezeigt, die für das ausgewählte Ereignis relevant sind. Die detaillierten Informationen enthalten Links zu

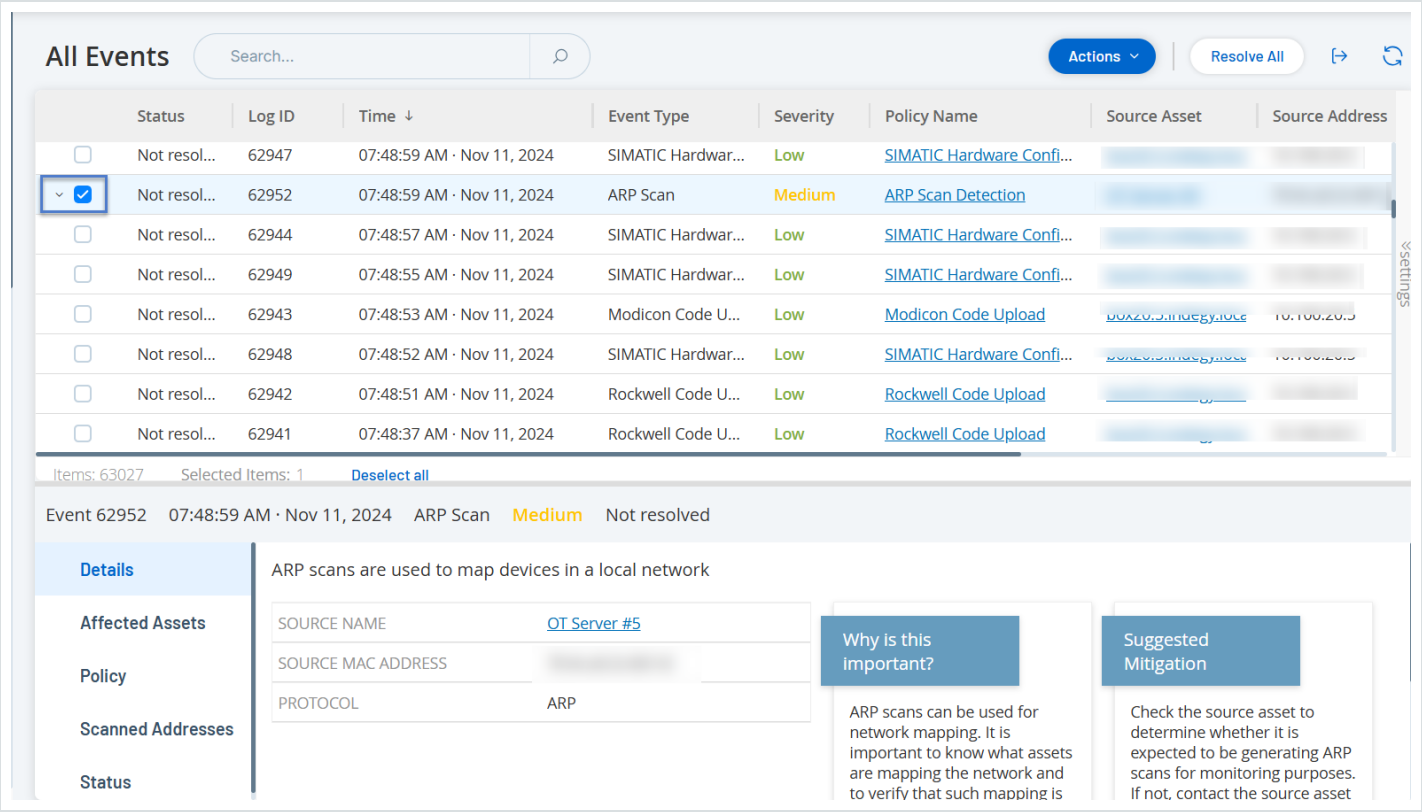
zusätzlichen Informationen über die relevanten Entitäten (Quell-Asset, Ziel-Asset, Richtlinie, Gruppe usw.).

- Kopfleiste – Zeigt einen Überblick über wichtige Informationen über das Ereignis.
- Details – Gibt eine kurze Beschreibung des Ereignisses sowie eine Erklärung, warum diese Informationen wichtig sind, und schlägt Schritte vor, die unternommen werden sollten, um den durch das Ereignis verursachten potenziellen Schaden zu mindern. Darüber hinaus werden die Quell- und Ziel-Assets angezeigt, die an dem Ereignis beteiligt waren.
- Regeldetails (für Intrusion Detection-Ereignisse) – Zeigt Informationen über die Suricata-Regel an, die für das Ereignis gilt.
- Code – Diese Registerkarte wird für Controller-Aktivitäten wie Code-Download und -Upload, HW-Konfiguration und Code-Löschung angezeigt. Sie enthält detaillierte Informationen über den relevanten Code, einschließlich spezifischer Codeblöcke, Zeilen und Tags. Die Codeelemente werden in einer Baumstruktur mit Pfeilen zum Erweitern/Minimieren der angezeigten Details angezeigt.
- Quelle – Zeigt detaillierte Informationen über das Quell-Asset für dieses Ereignis.
- Ziel – Zeigt detaillierte Informationen über das Ziel-Asset für dieses Ereignis.
- Betroffenes Asset – Zeigt detaillierte Informationen über das von diesem Ereignis betroffene Asset.
- Gescannte Ports (für Port-Scan-Ereignisse) – Zeigt die gescannten Ports an.
- Gescannte Adressen (für ARP-Scan-Ereignisse) – Zeigt die gescannten Adressen an.
- Richtlinie – Zeigt detaillierte Informationen über die Richtlinie, die das Ereignis ausgelöst hat.
- Status – Zeigt an, ob das Ereignis als aufgelöst markiert wurde oder nicht. Für aufgelöste Ereignisse werden Details dazu angezeigt, welcher Benutzer sie als aufgelöst markiert haben und wann sie aufgelöst wurden.

## Anzeigen von Ereignisclustern

Um die Überwachung von Ereignissen zu vereinfachen, werden mehrere Ereignisse mit denselben Merkmalen in einem einzigen Cluster zusammengefasst. Das Clustering basiert auf dem Ereignistyp (d. h. Nutzung derselben Richtlinie), Quell- und Ziel-Assets und dem Zeitraum, in dem die Ereignisse auftreten. Informationen zum Konfigurieren von Ereignisclustern finden Sie unter Ereigniscluster.

Geclusterte Ereignisse sind mit einem Pfeil neben der Protokoll-ID gekennzeichnet. Wenn Sie die einzelnen Ereignisse in einem Cluster anzeigen möchten, klicken Sie auf den Datensatz, um die Liste zu erweitern.




## Richtlinienausschlüsse erstellen

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager

Wenn eine Richtlinie Ereignisse für bestimmte Bedingungen generiert, die keine Sicherheitsbedrohung darstellen, können Sie diese Bedingungen von der Richtlinie ausschließen

(d. h. keine Ereignisse mehr für diese bestimmten Bedingungen generieren). Ein Beispiel: Wenn eine Richtlinie Änderungen des Controller-Status erkennt, die während der Arbeitszeit auftreten, Sie jedoch feststellen, dass Statusänderungen während dieser Zeiten für einen bestimmten Controller normal sind, können Sie diesen Controller aus der Richtlinie ausschließen.

Sie können Ausschlüsse auf der Seite Ereignisse erstellen, basierend auf Ereignissen, die von Ihren Richtlinien generiert wurden. Sie können angeben, welche Bedingungen eines bestimmten Ereignisses Sie aus der Richtlinie ausschließen möchten.

Um die Generierung von Ereignissen für die angegebenen Bedingungen zu einem späteren Zeitpunkt fortzusetzen, können Sie den Ausschluss löschen, wie unter Richtlinien beschrieben.

### So erstellen Sie einen Richtlinienausschluss:

1. Wählen Sie auf der entsprechenden Seite für Ereignisse (Konfigurationsereignisse, SCADA-Ereignisse, Netzwerkbedrohungen oder Netzwerkereignisse) das Ereignis aus, für das Sie einen Ausschluss erstellen möchten.
2. Klicken Sie in der Kopfleiste auf Aktionen oder klicken Sie mit der rechten Maustaste auf das Ereignis.

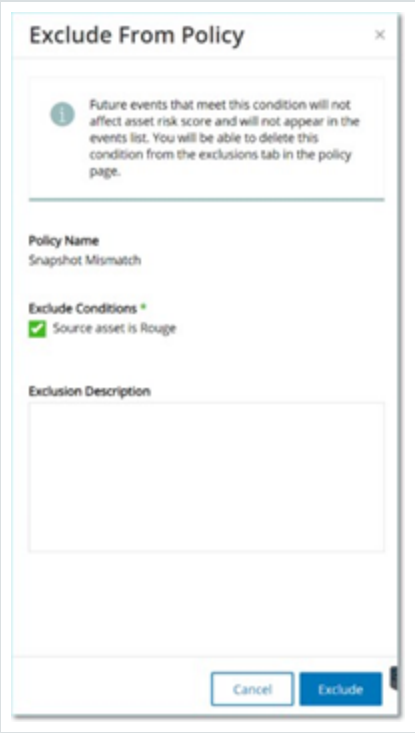
   Das Menü Aktionen wird geöffnet.
3. Klicken Sie auf Aus Richtlinie ausschließen.

   Das Fenster Aus Richtlinie ausschließen wird geöffnet.
4. Im Abschnitt Ausschlussbedingungen sind standardmäßig alle Bedingungen ausgewählt.

   Dies führt dazu, dass Ereignisse mit einer der angegebenen Bedingungen aus der Richtlinie ausgeschlossen werden. Sie können das Kontrollkästchen neben jeder Bedingung, für die weiterhin Ereignisse generiert werden sollen, deaktivieren.

   > Hinweis: Wenn Sie beispielsweise im folgenden Fenster die angegebenen Quell- und Ziel-Assets und -IP-Adressen aus dieser Richtlinie ausschließen möchten, diese Richtlinie jedoch

veiterhin auf UDP-Konversationen zwischen anderen Assets im Netzwerk angewendet werden oll, deaktivieren Sie die Bedingung „Protokoll ist UDP“.




Hinweis: Welche Bedingungen ausgeschlossen werden können, hängt vom Richtlinientyp ab, siehe folgende Tabelle.

5. (Optional) Im Feld Ausschlussbeschreibung können Sie einen Kommentar zum Ausschluss hinzufügen.
6. Klicken Sie auf Ausschließen.

   OT Security erstellt den Ausschluss.

   Die folgende Tabelle zeigt die Bedingungen, die für die einzelnen Ereignistypen ausgeschlossen werden können.

| Richtlinienkategorie | Ereignistyp | Ausschließbare Bedingungen |
|---|---|---|
| Controller-Aktivitäten | Konfigurationsereignisse (Aktivitäten) | • Quell-Asset<br>• Quell-IP<br>• Ziel-Asset<br>• Ziel-IP |
| Controller-Validierung | Änderung des Schlüsselstatus | Quell-Asset |
| | Änderung des Controller-Status | Quell-Asset |
| | Änderung der FW-Version | Quell-Asset |
| | Modul nicht gesehen | Quell-Asset |
| | Snapshot-Konflikt | Quell-Asset |
| Netzwerk | Asset nicht gesehen | Quell-Asset |
| | Änderung der USB-Konfiguration | • Quell-Asset<br>• USB-Geräte-ID |
| | IP-Konflikt | • MAC-Adressen<br>• IP-Adresse |
| | Netzwerk-Baseline-Abweichung | • Quell-Asset<br>• Quell-IP<br>• Ziel-Asset |

| Richtlinienkategorie | Ereignistyp | Ausschließbare Bedingungen |
|---|---|---|
| | | • Ziel-IP<br>• Protokoll |
| | Offener Port | • Quell-Asset<br>• Quell-IP<br>• Port |
| | RDP-Verbindung | • Quell-Asset<br>• Quell-IP<br>• Ziel-Asset<br>• Ziel-IP |
| | Nicht autorisierte Konversation | • Quell-Asset<br>• Quell-IP<br>• Ziel-Asset<br>• Ziel-IP<br>• Protokoll |
| | FTP-Login (fehlgeschlagen und erfolgreich) | • Quell-Asset<br>• Quell-IP<br>• Ziel-Asset<br>• Ziel-IP |

| Richtlinienkategorie | Ereignistyp | Ausschließbare Bedingungen |
|---|---|---|
| | Telnet-Login (Versuch, fehlgeschlagen und erfolgreich) | • Quell-Asset<br>• Quell-IP<br>• Ziel-Asset<br>• Ziel-IP |
| Netzwerkbedrohung | Intrusion Detection | • Quell-Asset<br>• Quell-IP<br>• Ziel-Asset<br>• Ziel-IP<br>• SID |
| | ARP-Scan | • Quell-Asset<br>• Quell-IP |
| | Port-Scan | • Quell-Asset<br>• Quell-IP |
| SCADA | Unzulässige Modbus-Datenadresse | • Quell-Asset<br>• Quell-IP<br>• Ziel-Asset<br>• Ziel-IP |
| | Unzulässiger Modbus-Datenwert | • Quell-Asset |

| Richtlinienkategorie | Ereignistyp | Ausschließbare Bedingungen |
|---|---|---|
| | | • Quell-IP<br>• Ziel-Asset<br>• Ziel-IP |
| | Unzulässige Modbus-Funktion | • Quell-Asset<br>• Quell-IP<br>• Ziel-Asset<br>• Ziel-IP |
| | Nicht autorisierter Schreibvorgang | • Quell-Asset<br>• Ziel-Asset<br>• Tag-Name |
| | IEC60870-5-104 StartDT<br>IEC60870-5-104 StopDT | • Quell-Asset<br>• Quell-IP<br>• Ziel-Asset<br>• Ziel-IP |
| | IEC60870-5-104 Funktionscode-basierte Ereignisse | • Quell-Asset<br>• Quell-IP<br>• Ziel-Asset<br>• Ziel-IP |

| Richtlinienkategorie | Ereignistyp | Ausschließbare Bedingungen |
|---|---|---|
| | | • COT |
| | DNP3-Ereignisse | • Quell-Asset<br>• Quell-IP<br>• Ziel-Asset<br>• Ziel-IP<br>• DNP3-Quelladresse<br>• DNP3-Zieladresse |

## Einzelne Erfassungsdateien herunterladen

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager, Sicherheitsanalyst

OT Security speichert die zugehörigen Paketerfassungsdaten jedes Ereignisses im Netzwerk. Die Daten werden als PCAP-Dateien gespeichert, die heruntergeladen und mit Tools zur Analyse von Netzwerkprotokollen (z. B. Wireshark) analysiert werden können. Sie können auch PCAP-Dateien für das gesamte Netzwerk herunterladen, siehe Netzwerk.

Hinweis: PCAP-Dateien sind nur verfügbar, wenn die Funktion „Paketerfassung“ aktiviert ist. Die Funktion „Paketerfassung“ kann über den Bildschirm Lokale Einstellungen > Systemkonfiguration > Paketerfassungen aktiviert werden, siehe Paketerfassungen. PCAP-Dateien sind nur für Ereignisse verfügbar, die sich auf Netzwerkaktivitäten beziehen, z. B. Controller-Aktivitäten, Netzwerkbedrohungen, SCADA-Ereignisse und einige Arten von Netzwerkereignissen.

### PCAP-Datei herunterladen

So laden Sie eine PCAP-Datei herunter:

1. Aktivieren Sie auf der Seite Ereignisse das Kontrollkästchen neben dem Ereignis, für das Sie die PCAP-Datei herunterladen möchten.
2. Klicken Sie in der Kopfleiste auf Aktionen.

   Das Menü Aktionen wird geöffnet.
3. Wählen Sie Erfassungsdatei herunterladen aus.

   Die gezippte PCAP-Datei wird auf Ihren lokalen Computer heruntergeladen.

## FortiGate-Richtlinien erstellen

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager

Die FortiGate-Integration ermöglicht es Ihnen, bestimmte OT Security-Ereignisse zu verwenden, um Firewall-Richtlinien/-Regeln in der FortiGate Next Generation Firewall (NGFW) zu erstellen. Die Ereignistypen, für die diese Funktion zur Verfügung steht (unterstützte Ereignisse), sind Baseline-Abweichung, Nicht autorisierte Konversation, Intrusion Detection und RDP-Verbindung (authentifiziert und nicht authentifiziert). Die FortiGate-Richtlinie ist so eingestellt, dass sie automatisch für die Quell- und Ziel-Assets gilt, die am OT Security-Ereignis beteiligt waren. Standardmäßig bewirkt die Richtlinie, dass FortiGate Traffic des angegebenen Typs ablehnt (d. h. blockiert). Ein FortiGate-Administrator kann die Richtlinieneinstellungen in der FortiGate-Anwendung anpassen.

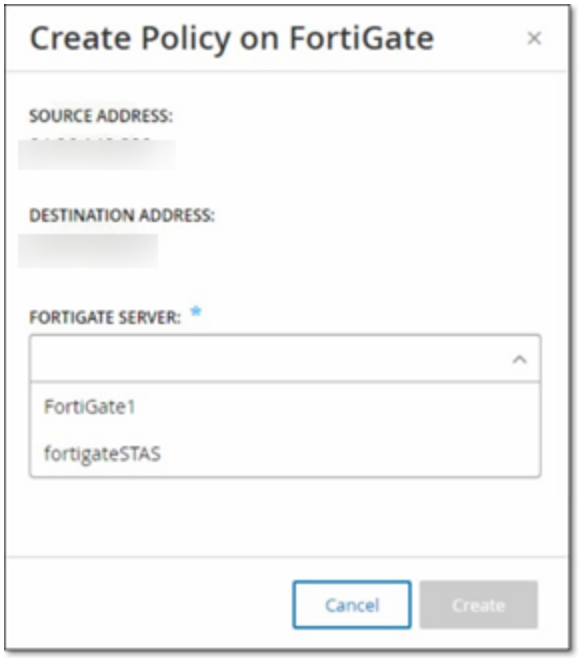
Bevor Sie FortiGate-Richtlinien vorschlagen, müssen Sie die Integration für den FortiGate-Firewall-Server mit OT Security einrichten. Siehe FortiGate-Firewalls.

So schlagen Sie eine FortiGate-Richtlinie vor:

1. Wählen Sie auf der entsprechenden Seite für Ereignisse(Konfigurationsereignisse, SCADA-Ereignisse, Netzwerkbedrohungen oder Netzwerkereignisse) das Ereignis aus, für das Sie eine FortiGate-Richtlinie erstellen möchten.
2. Klicken Sie in der Kopfleiste auf Aktionen oder klicken Sie mit der rechten Maustaste auf das Ereignis.

   Ein Dropdown-Menü wird geöffnet.
3. Wählen Sie FortiGate-Richtlinie erstellen aus.

   Das Fenster Richtlinie auf FortiGate erstellen wird geöffnet. Die Felder Quelladresse und Zieladresse der am OT Security-Ereignis beteiligten Assets sind bereits ausgefüllt.
4. Wählen Sie im Dropdown-Menü FortiGate-Server den erforderlichen Server aus.




5. Klicken Sie auf Erstellen.

   Die Richtlinie wird in FortiGate erstellt und das Fenster wird geschlossen. Sie können die neue Richtlinie in der FortiGate-Anwendung anzeigen. Ein FortiGate-Administrator kann die Einstellungen wie erforderlich anpassen.

# Netzwerk

OT Security überwacht alle Aktivitäten in Ihrem Netzwerk und zeigt die Daten auf den folgenden Seiten an:

- Netzwerk – Zusammenfassung – Zeigt eine Übersicht der Netzwerkaktivität.
- Paketerfassungen – Zeigt eine Liste der vom System erfassten PCAP-Dateien. Siehe Paketerfassungen.
- Konversationen – Zeigt eine Liste aller im Netzwerk erkannten Konversationen mit Details über den Zeitpunkt, an dem sie stattgefunden haben, und beteiligten Assets. Siehe Konversationen

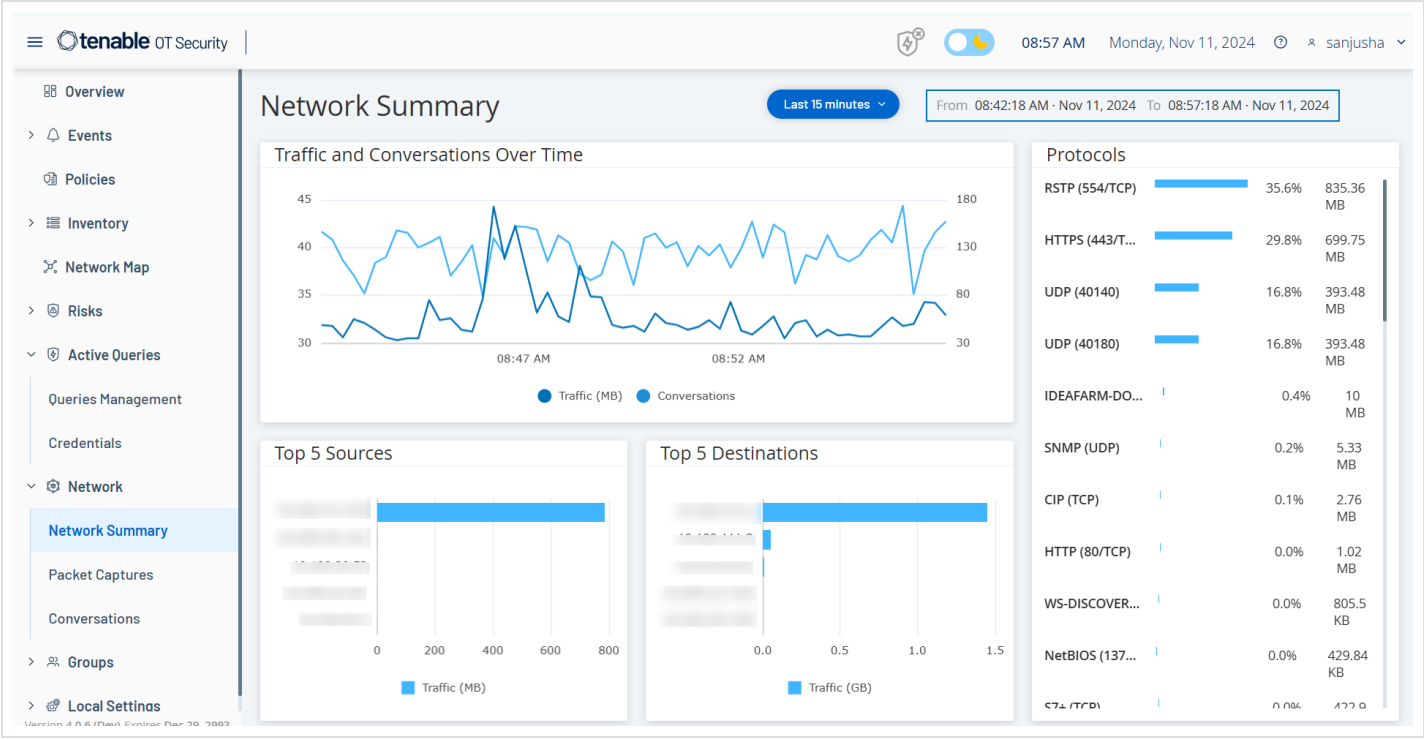
So greifen Sie auf die Seite Netzwerk zu:

1. Wählen Sie im linken Navigationsbereich Netzwerk aus.

   Die Seite Netzwerk – Zusammenfassung wird angezeigt.

## Netzwerk – Zusammenfassung

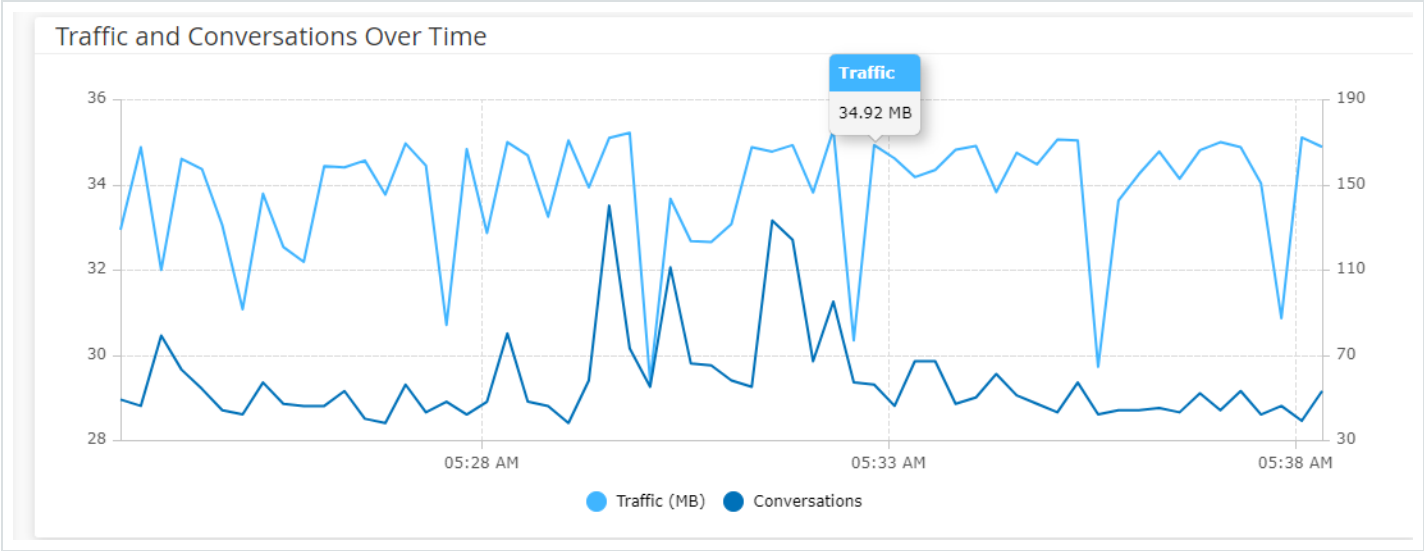
Die Seite Netzwerk – Zusammenfassung enthält visuelle Diagramme, die einen Überblick über die Netzwerkaktivitäten geben. Sie können die Daten für einen bestimmten Zeitraum anzeigen lassen.




Interagieren Sie mit den folgenden Widgets, um zusätzliche Details anzuzeigen.

## Traffic und Konversationen im zeitlichen Verlauf

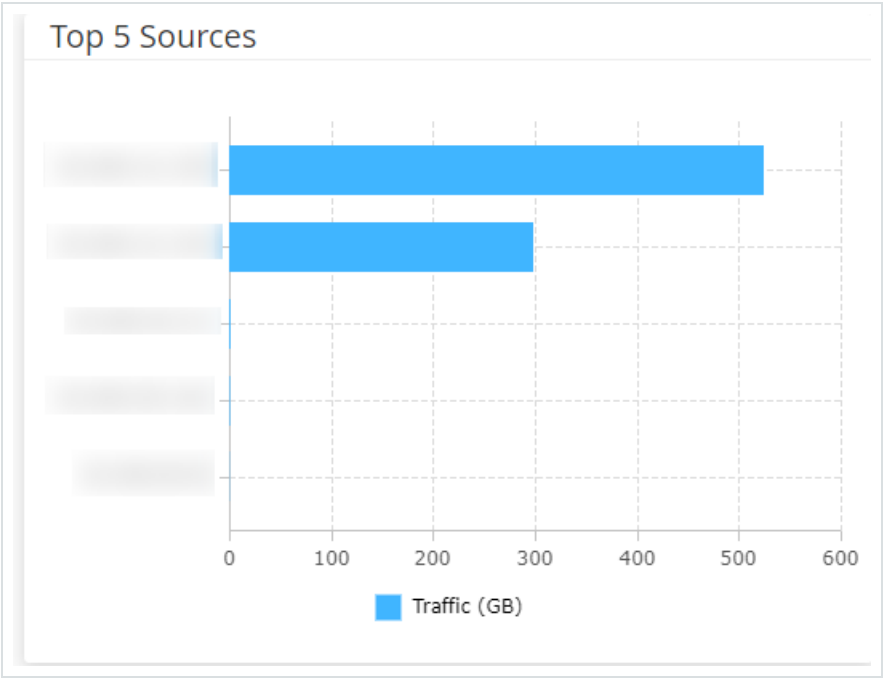
Ein Liniendiagramm zeigt das Traffic-Volumen (gemessen in KB/MB/GB) und die Anzahl der Konversationen im Netzwerk im Laufe der Zeit an. Die Legende wird oben im Diagramm angezeigt. Bewegen Sie den Mauszeiger über einen Punkt im Diagramm, um spezifische Daten über den Traffic und die Konversationen in diesem Zeitsegment anzuzeigen.




Hinweis: Die Länge des Zeitsegments wird entsprechend der im Diagramm angezeigten Zeitskala angepasst. Beispiel: Die Daten eines 15-Minuten-Zeitraums werden für jede Minute separat angezeigt, während die Daten eines 30-Tage-Zeitraums für Segmente von jeweils 6 Stunden angezeigt werden.

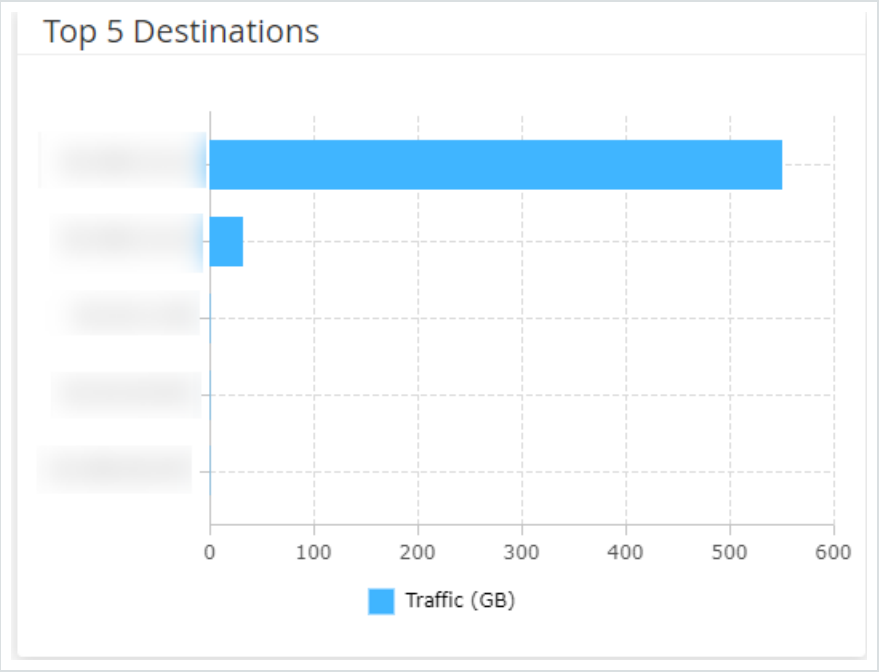
## Top 5 Quellen

Das Widget „Top 5 Quellen“ zeigt die Anzahl der Konversationen und das Traffic-Volumen für jedes der Top-5-Assets an, die während eines bestimmten Zeitraums Mitteilungen über das Netzwerk gesendet haben. Sie können die Quell-Assets anhand ihrer IP-Adressen identifizieren. Wenn Sie den Mauszeiger über ein Säulendiagramm bewegen, werden die Anzahl der Konversationen und das von diesem Asset gesendete Traffic-Volumen angezeigt.



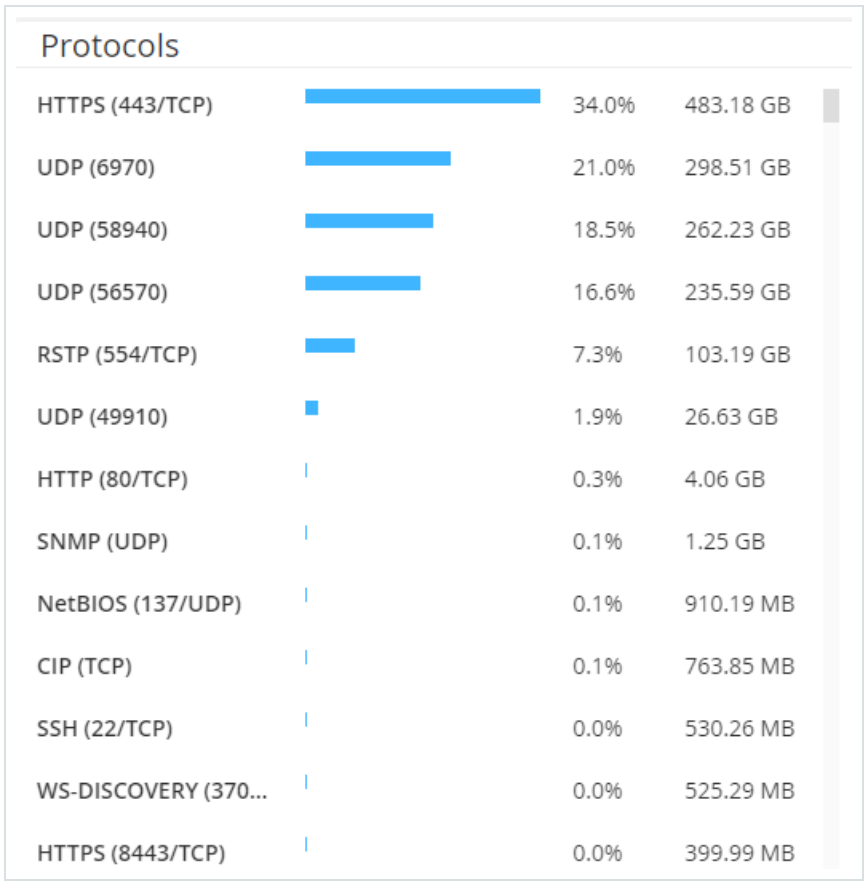

## Top 5 Ziele

Das Widget „Top 5 Ziele“ zeigt die Anzahl der Konversationen und das Traffic-Volumen für jedes der Top-5-Assets an, die während eines bestimmten Zeitraums Mitteilungen über das Netzwerk empfangen haben. Sie können die Ziel-Assets anhand ihrer IP-Adressen identifizieren. Wenn Sie den Mauszeiger über ein Säulendiagramm bewegen, werden die Anzahl der Konversationen und das von diesem Asset empfangene Traffic-Volumen angezeigt.




## Protokolle

Das Widget Protokolle enthält Daten über die Verwendung verschiedener Protokolle für die Kommunikation innerhalb des Netzwerks während eines bestimmten Zeitraums.




Die Protokolle sind von den am häufigsten verwendeten (oben) bis zu den am seltensten verwendeten (unten) angeordnet. Jedes Protokoll zeigt die folgenden Informationen:

- Ein Säulendiagramm mit der Nutzungsrate, wobei eine vollständige Säule die höchste Nutzung anzeigt und Teilsäulen das Ausmaß der Nutzung im Vergleich zum am häufigsten genutzten Protokoll angeben
- Prozentsatz der Nutzung
- Gesamtvolumen der Kommunikation

## Zeitraum festlegen

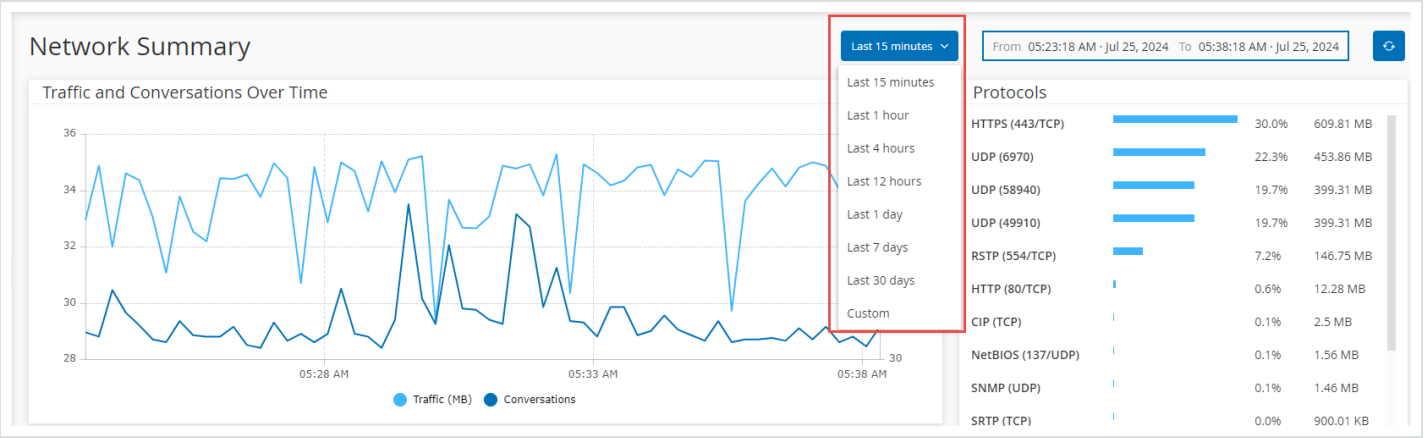
Auf der Seite Netzwerk – Zusammenfassung werden Daten angezeigt, die die Netzwerkaktivität während eines bestimmten Zeitraums darstellen. Die Kopfleiste zeigt den Zeitraum für die aktuell

angezeigten Daten. Der Standardzeitraum ist auf Letzte 15 Minuten festlegt. In der Kopfleiste werden außerdem die Start- und die Endzeit des Zeitraums angezeigt.

### So legen Sie den Zeitraum fest:

Klicken Sie in der Kopfleiste auf das Dropdown-Feld für den Zeitraum. Die Standardeinstellung lautet Letzte 15 Minuten.

Im Dropdown-Feld werden die verfügbaren Optionen aufgeführt.




Wählen Sie mit einer der folgenden Methoden einen Zeitraum aus:

- Wählen Sie einen voreingestellten Zeitraum aus, indem Sie auf den gewünschten Zeitraum klicken. Verfügbare Optionen: „Letzte 15 Minuten“, „Letzte Stunde“, „Letzte 4 Stunden“, „Letzte 12 Stunden“, „Letzter Tag“, „Letzte 7 Tage“ oder „Letzte 30 Tage“).
- Legen Sie einen benutzerdefinierten Zeitraum fest:
- Klicken Sie auf Benutzerdefiniert.

  Das Fenster Benutzerdefinierter Bereich wird angezeigt.
- Geben Sie das Startdatum, die Startzeit, das Enddatum und die Endzeit ein.
- Klicken Sie auf Anwenden.

Nachdem Sie den Zeitraum festgelegt haben, werden in der Kopfleiste das Start- und Enddatum sowie die Start- und Endzeit neben der Zeitraumauswahl angezeigt. OT Security aktualisiert die Seite, um Daten innerhalb des ausgewählten Zeitraums anzuzeigen.

## Paketerfassungen

OT Security speichert Dateien mit Netzwerk-Paketerfassungen von Aktivitäten im Netzwerk. Die Daten werden als PCAP-Dateien (Packet Capture, Paketerfassung) gespeichert, die mit Tools zur Analyse von Netzwerkprotokollen (z. B. Wireshark) analysiert werden können. Dies ermöglicht eine umfassende forensische Analyse kritischer Ereignisse. Wenn die Speicherkapazität des Systems 1,8 TB überschreitet, löscht das System ältere Dateien.

Die Seite Paketerfassungen zeigt alle PCAP-Dateien im System an. Der Bereich Abgeschlossen enthält Listen aller abgeschlossenen Dateien, die zum Herunterladen verfügbar sind. Der Bereich Laufend enthält Details zu der Paketerfassung, die derzeit ausgeführt wird.

Die Kopfleiste zeigt die älteste noch verfügbare erfasste Datei. Außerdem enthält sie eine Option zum Herunterladen von Dateien sowie zum manuellen Schließen der aktuellen Paketerfassung.

> Hinweis: Die Rollen Nur lesen und Site-Operator haben keine Berechtigung, laufende Erfassungen zu stoppen oder gespeicherte Paketerfassungen herunterzuladen.

In der Tabelle mit Paketerfassungen können Sie Spalten ein- und ausblenden und die Listen sortieren und filtern sowie nach Schlüsselwörtern suchen. Weitere Informationen zum Anpassen von Tabellen finden Sie unter Tabellen anpassen.

> Hinweis: Sie können die PCAP-Datei für ein einzelnes Ereignis auch über die Seite Ereignisse herunterladen, siehe Dateien herunterladen.

### Paketerfassungsparameter

Die Liste der Paketerfassungen enthält die folgenden Details:

| Parameter | Beschreibung |
|---|---|
| Startzeit | Das Datum und die Uhrzeit des Beginns der Paketerfassung. |
| Endzeit | Das Datum und die Uhrzeit des Endes der Paketerfassung. |
| Status | Der Status der Erfassung: Abgeschlossen oder Fortlaufend. |
| Sensor | Der OT Security Sensor, der das Paket erfasst hat. Für Pakete, die direkt von der OT Security Appliance erfasst wurden, wird der Wert `lokal` angezeigt. |
| Dateiname | Der Name der Datei. |
| Dateigröße | Die Größe der Datei, angegeben in KB/MB. |

### Anzeige der Paketerfassungen filtern

Sie können die Anzeige der Paketerfassungen filtern, um nach einer bestimmten PCAP-Datei zu suchen. Geben Sie hierzu die Parameter für Start- und/oder Endzeit an.

### So filtern Sie Paketerfassungen:

1. Gehen Sie zu Netzwerk > Paketerfassungen.
2. Um nach der Startzeit zu filtern, bewegen Sie den Mauszeiger über Startzeit und klicken Sie auf das Symbol ▽.

   Ein Dropdown-Menü wird geöffnet.

   1. So legen Sie den Filter fest:

      a. Wählen Sie im Dropdown-Menü den gewünschten Filter aus: Jederzeit (Standardeinstellung), Begonnen vor oder Begonnen nach.

b. Wenn Sie Begonnen vor oder Begonnen nach auswählen, wird ein Fenster mit den Feldern Datum und Uhrzeit angezeigt, in denen Sie das gewünschte Datum und die Uhrzeit wählen können.

c. Klicken Sie auf Anwenden.

3. Um nach der Endzeit zu filtern, bewegen Sie den Mauszeiger über Endzeit und klicken Sie auf das Symbol ▽.

   Ein Dropdown-Menü wird geöffnet.

   1. So legen Sie den Filter fest:

      a. Wählen Sie den gewünschten Filter aus: Jederzeit (Standardeinstellung), Beendet vor oder Beendet nach.

      b. Wenn Sie Beendet vor oder Beendet nach auswählen, wird ein Fenster mit den Feldern Datum und Uhrzeit angezeigt, in denen Sie das gewünschte Datum und die Uhrzeit wählen können.

      c. Klicken Sie auf Anwenden.

         OT Security wendet den Filter an, und nur die innerhalb des festgelegten Zeitraums generierten Dateien werden angezeigt.

## Paketerfassungen aktivieren oder deaktivieren

Sie können die Paketerfassungsfunktion unter Lokale Einstellungen > Systemkonfiguration > Gerät aktivieren oder deaktivieren.

Wenn die Funktion Paketerfassung deaktiviert ist, wird im Bildschirm Paketerfassungen eine entsprechende Informationsmeldung angezeigt.

> Wichtig: Sie können die Paketerfassungsfunktion unter Netzwerk > Paketerfassungen aktivieren, aber nicht deaktivieren.

### So aktivieren Sie die Paketerfassung:

1. Gehen Sie zu Netzwerk > Paketerfassungen.
2. Klicken Sie in der Kopfleiste auf Aktivieren.

   OT Security startet die Paketerfassung.

## Dateien herunterladen

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager, Sicherheitsanalyst

Sie können alle abgeschlossenen PCAP-Dateien auf Ihren lokalen Computer herunterladen. Anschließend können Sie die Dateien mit Tools zur Analyse von Netzwerkprotokollen wie Wireshark analysieren.

Noch laufende Dateierfassungen stehen noch nicht zum Herunterladen zur Verfügung. Sie können eine laufende Erfassung manuell schließen, um die aktuelle Datei zu schließen und mit der Erfassung von Informationen in einer neuen Datei zu beginnen.

### So laden Sie eine abgeschlossene Datei herunter:

1. Gehen Sie zu Netzwerk > Paketerfassungen.
2. Wählen Sie die gewünschte Datei in den Paketerfassungslisten aus.
3. Klicken Sie in der Kopfleiste auf Herunterladen.

   OT Security lädt die PCAP-Datei im ZIP-Format auf Ihren lokalen Computer herunter.

### So schließen Sie die aktuelle Paketerfassung manuell:

1. Gehen Sie zu Netzwerk > Paketerfassungen.
2. Klicken Sie in der Kopfleiste auf Laufende Erfassungen schließen.

   OT Security beendet die aktuelle Erfassung, und die Datei steht zum Herunterladen zur Verfügung. OT Security startet automatisch eine neue Paketerfassung.

# Konversationen

Konversationen sind Netzwerkkommunikationen zwischen zwei Assets – einer Quelle und einem Ziel. Beispielsweise eine Interaktion zwischen einer Engineering-Workstation und einer SPS oder zwischen zwei Servern. Die Seite Konversationen zeigt eine Liste der aktuellen und vergangenen Konversationen, einschließlich detaillierter Informationen zu den Konversationen.

Sie können auf der Seite Konversationen die folgenden Aktionen durchführen:

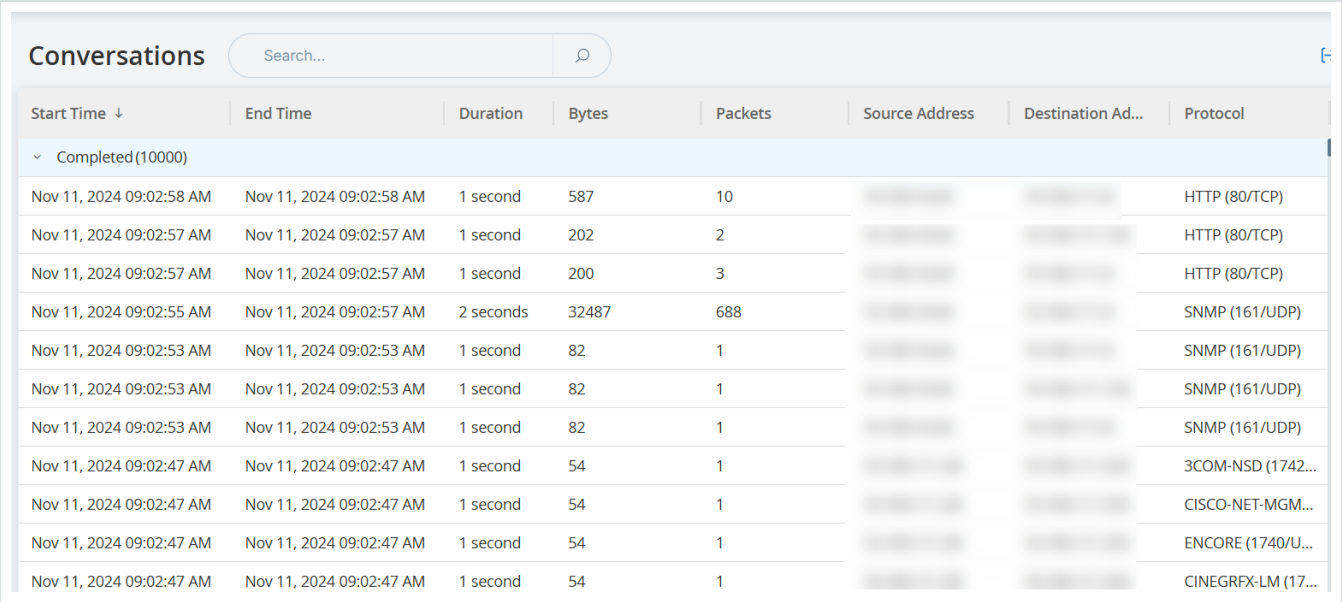
- Suchen – Suchen Sie nach bestimmten Konversationen, indem Sie Informationen zur Identifizierung in das Feld Suchen eingeben.
- Exportieren – Verwenden Sie die Schaltfläche  „Exportieren“, um alle Daten aus der Registerkarte Konversationen als CSV-Datei auf Ihren lokalen Computer zu exportieren.

  > Hinweis: Die Konversationstabelle enthält die letzten 10.000 Netzwerkkonversationen.

So greifen Sie auf die Seite Konversationen zu:

1. Gehen Sie zu Netzwerk > Konversationen.

   Die Seite Konversationen wird angezeigt.

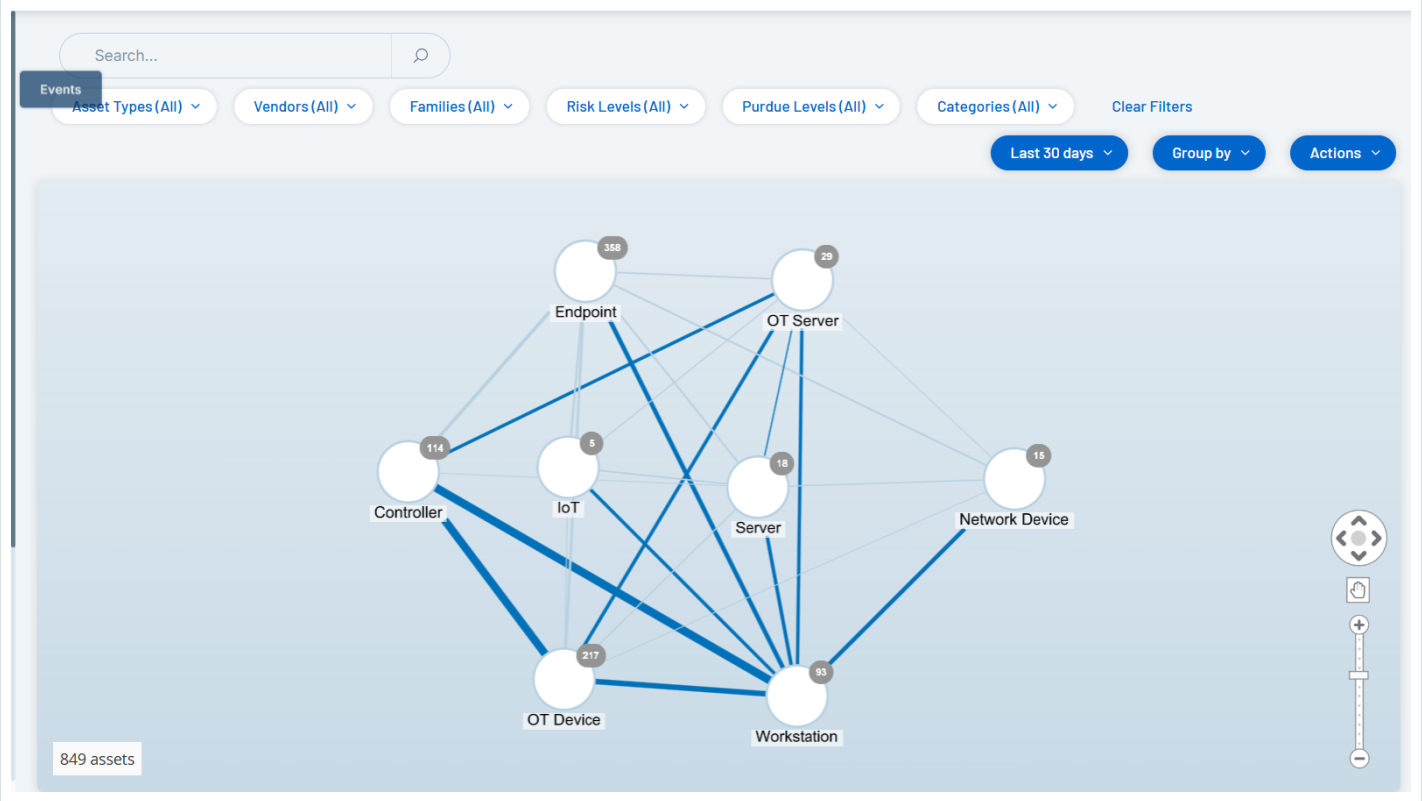



Die Seite „Konversationen“ enthält die folgenden Details:

| Parameter | Beschreibung |
|---|---|
| Startzeit | Die Uhrzeit, zu der die Konversation begonnen hat. |
| Endzeit | Die Uhrzeit, zu der die Konversation geendet hat. Zeigt Laufend für Konversationen an, die noch laufen. |
| Dauer | Die Dauer der Konversation. |
| Pakete | Die Anzahl der während der Konversation gesendeten Datenpakete. |
| Quelladresse | Die IP-Adresse des Assets, das die Daten gesendet hat. |
| Zieladresse | Die IP des Assets, das die Daten empfangen hat. |
| Protokoll | Das Protokoll, das für die Kommunikation verwendet wurde. |

## Netzwerkübersicht

Der Bildschirm Netzwerkübersicht bietet eine visuelle Darstellung der Netzwerk-Assets und ihrer Verbindungen im zeitlichen Verlauf, die von den Netzwerkerkennungsfunktionen von OT Security erfasst wurden. Die Netzwerkerkennung bietet detaillierte Echtzeit-Einblicke in alle Aktivitäten im Betriebsnetzwerk und konzentriert sich auf Engineering-Aktivitäten auf der Steuerungsebene wie z. B. Firmware-Downloads oder -Uploads, Code-Updates und Konfigurationsänderungen, die über proprietäre und anbieterspezifische Protokolle durchgeführt werden. Die Netzwerkübersicht zeigt die Assets nach Gruppen von verwandten Assets oder als einzelne Assets.




In der Netzwerkübersicht werden alle Assets und Verbindungen angezeigt, die während des angegebenen Zeitraums von Tenable erfasst wurden.

Die Seite Netzwerkübersicht enthält die folgenden Details:

- Suchfeld – Geben Sie einen Suchtext ein, um in der Anzeige nach Assets zu suchen. In der Netzwerkübersicht werden die Suchergebnisse durch Hervorheben aller Gruppen angezeigt, die mit dem Suchtext übereinstimmen. Sie können jede Gruppe aufschlüsseln, um die

relevanten Assets anzuzeigen.

- Filter – Filtern Sie die Übersicht nach einer oder mehreren der angegebenen Kategorien: Asset-Typ, Anbieter, Familien, Risikostufen, Purdue-Level. Eine Erläuterung der Asset-Typen finden Sie unter Asset-Typen.
- Zeitraum – Die Netzwerkübersicht zeigt Assets und Verbindungen an, die während des angegebenen Zeitraums erkannt wurden. Der Standardzeitraum ist auf Letzte 30 Tage festlegt. Wählen Sie im Dropdown-Feld „Zeitraum“ einen anderen Zeitraum aus.
- Gruppierung – Geben Sie die Kategorie an, nach der die Assets in der Anzeige gruppiert werden. Verfügbare Optionen: Asset-Typ, Purdue-Level, Risikostufe oder Keine Gruppierung. Die Option Alle Gruppen reduzieren behält die aktuelle Gruppierungsauswahl bei, reduziert jedoch alle geöffneten Gruppen.
- Aktionen – Sie können die folgenden Aktionen im Dropdown-Menü auswählen:
    - Als Baseline festlegen – Hiermit können Sie die Baseline festlegen, die zum Erkennen anomaler Netzwerkaktivitäten verwendet wird, siehe Netzwerk-Baseline festlegen.
    - Automatisch anordnen – Hiermit können Sie die Übersicht automatisch für die aktuell angezeigten Entitäten optimieren.
- Gruppen/Assets – Die Übersicht enthält ein Symbol für jede Gruppe von Assets, wobei jeder Asset-Typ durch ein eindeutiges Symbol darstellt wird, wie unter Asset-Typen beschrieben. Bei Gruppen gibt die Zahl oben im Symbol die Anzahl der Assets an, die in dieser Gruppe enthalten sind. Sie können die Anzeige aufschlüsseln, um separate Symbole für jede Untergruppe anzuzeigen, bis Sie zu den Symbolen für einzelne Assets gelangen. Bei einzelnen Assets zeigt die Farbe des Rahmens um das Asset dessen Risikostufe an (rot, gelb, grün).

> Hinweis: Sie können die Gruppen und Assets ziehen und neu positionieren, um einen besseren Überblick über die Assets und ihre Verbindungen zu erhalten.

- Verbindungen – Jede Kommunikation zwischen Asset-Gruppen und/oder einzelnen Assets, entsprechend dem Granularitätsgrad, der aktuell in der Übersicht angezeigt wird. Die Dicke der Linie zeigt das Kommunikationsvolumen über diese Verbindung an.

  In der Netzwerkübersicht werden IT- und OT-Protokolle durch Farbcodes unterschieden.

  - Eine graue Linie zeigt reine IT-Protokolle an (z. B. DNS, HTTP und FTP).
  - Eine blaue Linie zeigt das Vorhandensein von OT-Protokollen an (z. B. HTTP, Modbus, CIP und FTP).

- Gesamtzahl der angezeigten Assets – Zeigt die Anzahl der im Netzwerk erkannten (und in der Übersicht angezeigten) Assets basierend auf dem angegebenen Zeitraum und den Asset-Filtern. Diese Zahl wird relativ zur Gesamtzahl der in Ihrem Netzwerk erkannten Assets angezeigt.
- Navigationssteuerelemente – Sie können die Anzeige vergrößern und verkleinern und darin navigieren, um die gewünschten Elemente anzuzeigen. Hierzu können Sie die Steuerelemente auf dem Bildschirm oder die Standard-Maussteuerungen verwenden.

## Asset-Gruppierungen

Auf der Seite Netzwerkübersicht können Assets nach verschiedenen Kategorien gruppiert angezeigt werden. Es werden Verbindungen zwischen Gruppen von Assets angezeigt. Sie können auf ein Asset klicken, um die Gruppe aufzuschlüsseln und die darin enthaltenen Elemente anzuzeigen. Sie können auch mehrere Gruppen gleichzeitig aufschlüsseln. OT Security bietet mehrere Ebenen eingebetteter Gruppen, sodass Sie bei jeder Aufschlüsselung eine detailliertere Ansicht der enthaltenen Assets erhalten.

Im Folgenden sind die Gruppierungen aufgeführt, die Sie auf die Hauptanzeige anwenden können, sowie die Aufschlüsselungsoptionen für die jeweilige Auswahl.

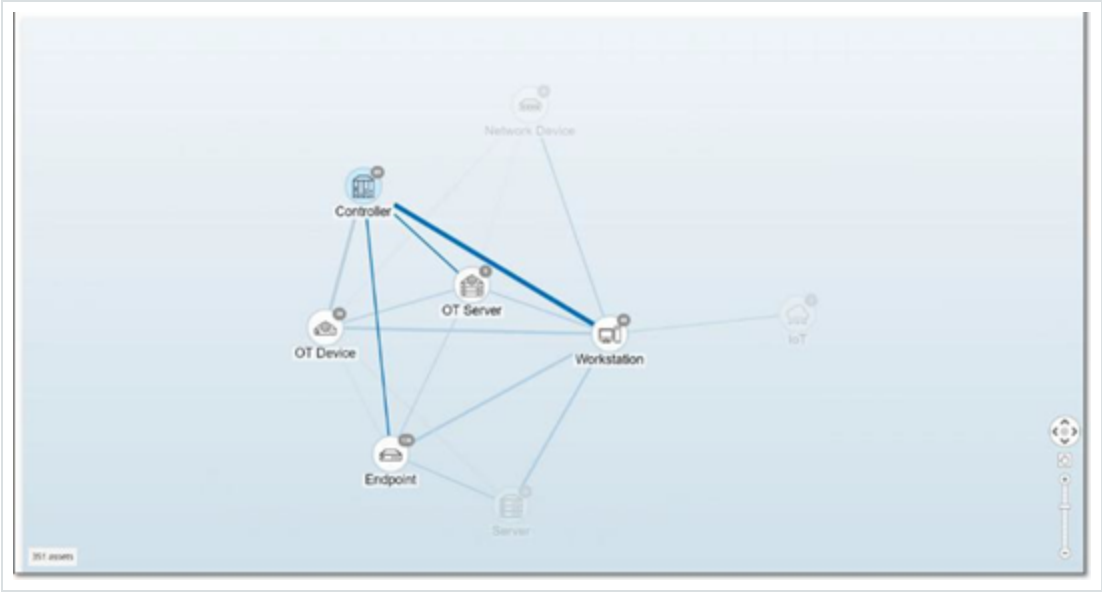
Wenn die Übersicht nach Asset-Typ (Standardeinstellung) gruppiert ist, sieht die Aufschlüsselungshierarchie wie folgt aus: Asset-Typ > Anbieter > Familie > Einzelnes Asset.

Wenn die Übersicht nach Risikostufe oder Purdue-Level gruppiert ist, wird eine zusätzliche Ebene über der Asset-Typ-Gruppierung hinzugefügt, sodass die Hierarchie wie folgt lautet: Purdue-Level/Risikostufe > Asset-Typ > Anbieter > Familie > Einzelnes Asset. Die enthaltenen Gruppen/Assets sind von einem Kreis umgeben, der jeweils eine einzelne Ebene darstellt.

Das folgende Beispiel zeigt, wie Sie die Anzeige aufschlüsseln können:

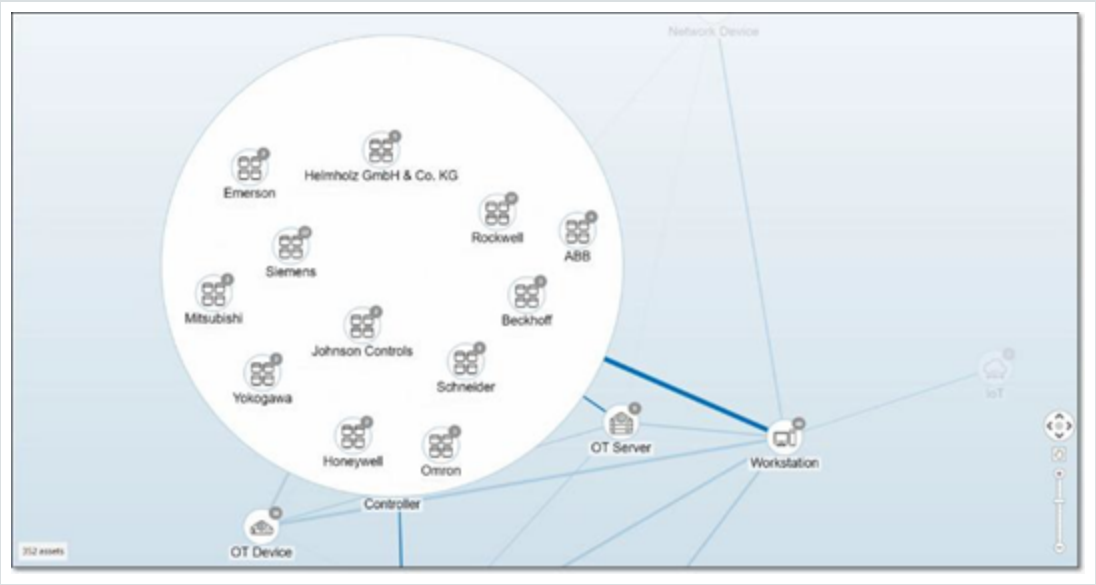
### So schlüsseln Sie eine Asset-Typ-Gruppe auf:

1. Standardmäßig wird der Bildschirm Netzwerkübersicht mit nach Asset-Typ gruppierten Assets geöffnet.

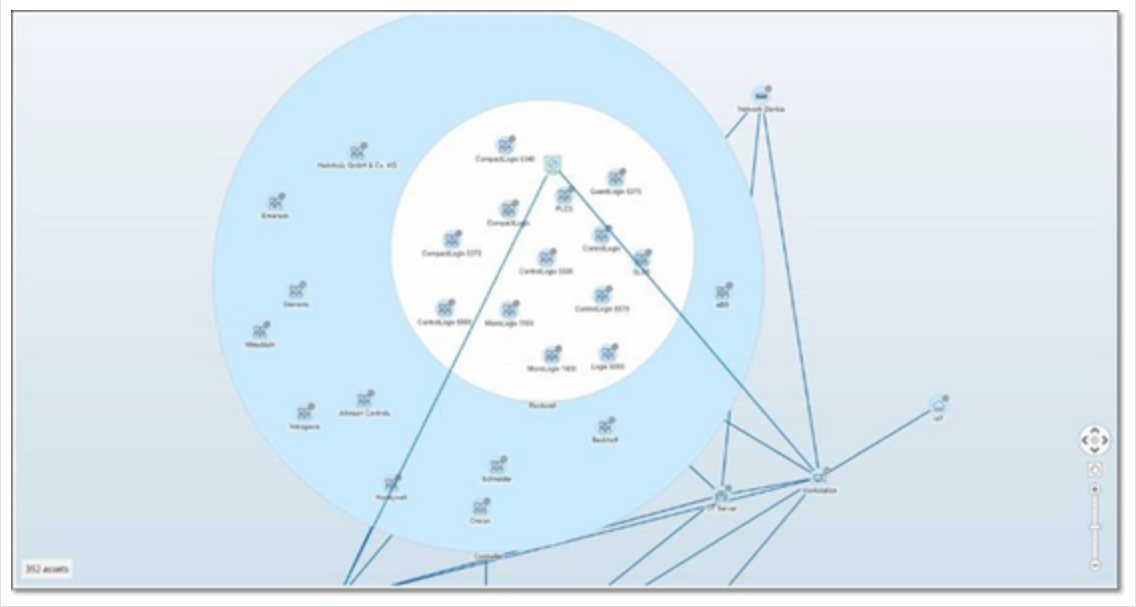



2. Doppelklicken Sie auf das Symbol der Gruppe, die Sie aufschlüsseln möchten (z. B. „Controller“).

   Die Gruppe wird erweitert und zeigt die Gruppen der Anbieter innerhalb dieser Gruppe an.

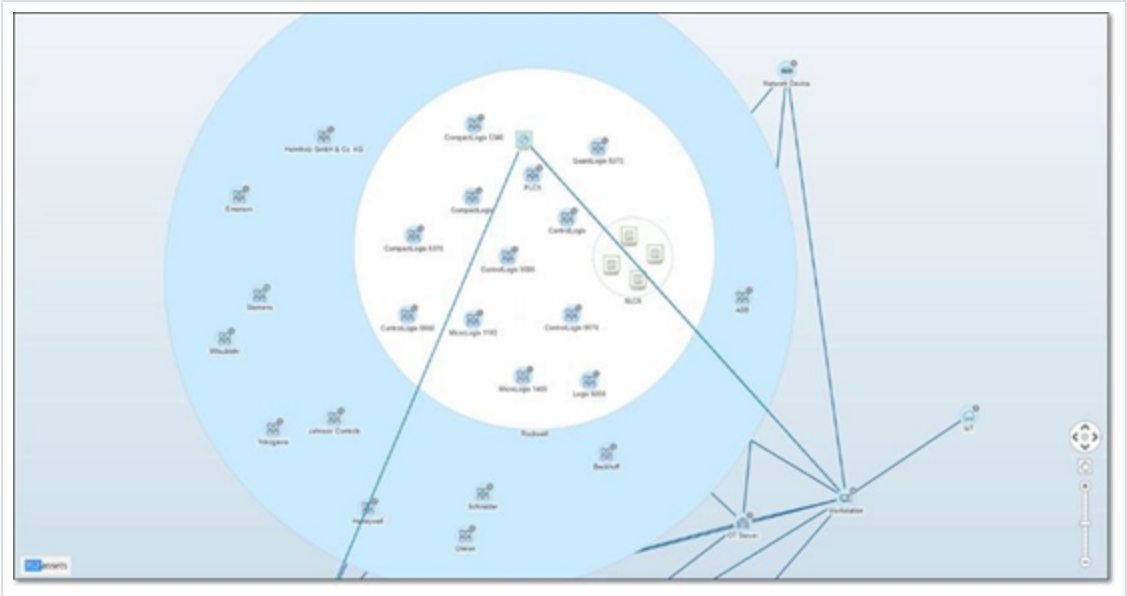



3. Zur weiteren Aufschlüsselung klicken Sie auf eine Anbietergruppe (z. B. Rockwell).



4. Um noch weiter aufzuschlüsseln, klicken Sie auf eine Familiengruppe (z. B. SLC5).

   Die einzelnen Assets innerhalb dieser Gruppe werden angezeigt.



5. Sie können jetzt auf ein bestimmtes Asset klicken, um Details für dieses Asset und seine Verbindungen anzuzeigen, siehe Inventar.

So reduzieren Sie die Anzeige:

1. Klicken Sie auf Gruppieren nach.
2. Klicken Sie auf Alle Gruppen reduzieren.

   Es werden wieder die Gruppen der obersten Ebene angezeigt.

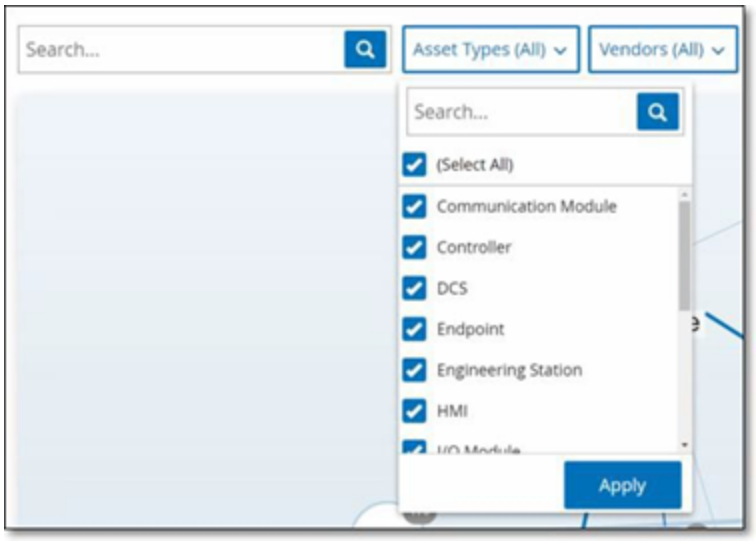
So entfernen Sie jegliche Gruppierung:

1. Klicken Sie auf die Schaltfläche Gruppieren nach.
2. Wählen Sie Keine Gruppierung aus.

   In der Übersicht werden alle einzelnen Assets ohne Gruppierung angezeigt.

## Filter auf die Übersicht anwenden

Sie können die Übersicht nach einer oder mehreren der angegebenen Kategorien filtern: Asset-Typ, Anbieter, Familien, Risikostufen, Purdue-Level.




So wenden Sie Filter auf die Übersicht an:

1. Klicken Sie auf die gewünschte Filterkategorie.
2. Aktivieren oder deaktivieren Sie die Kontrollkästchen für jedes Element, das Sie in die Anzeige einschließen bzw. aus der Anzeige ausschließen möchten.

   > Hinweis: Standardmäßig sind alle Elemente im Filter enthalten.

3. Sie können auf das Kontrollkästchen Alle auswählen klicken, um die Auswahl aller Werte aufzuheben, und dann die gewünschten Werte hinzufügen.
4. Sie können im Filtersuchfeld eine Suche durchführen, um einen bestimmten Wert im Filterfenster zu finden.
5. Wiederholen Sie den Vorgang nach Bedarf für jede Filterkategorie.
6. Klicken Sie auf Anwenden.

   In der Übersicht werden nur die ausgewählten Elemente angezeigt.

## Asset-Details anzeigen

Sie können auf ein bestimmtes Asset klicken, um grundlegende Informationen über das Asset und seine Netzwerkaktivitäten anzuzeigen, einschließlich Risikostufe, IP-Adresse, Asset-Typ, Anbieter und Familie. Die Übersicht zeigt Verbindungen vom ausgewählten Asset zu allen anderen Assets, die mit diesem kommunizieren. Sie können dann auf den als Link fungierenden Asset-Namen klicken, um zum Bildschirm Asset-Details mit detaillierteren Informationen über das Asset zu gelangen.


## Netzwerk-Baseline festlegen

Eine Netzwerk-Baseline ist eine Übersicht aller Konversationen, die während eines bestimmten Zeitraums zwischen Assets im Netzwerk stattgefunden haben. Die Netzwerk-Baseline wird in Richtlinien vom Typ „Netzwerk-Baseline-Abweichung“ verwendet, die vor anomalen Konversationen im Netzwerk warnen, siehe Netzwerkereignistypen.

Assets, die während der Baseline-Stichprobe nicht interagiert haben, lösen eine Richtlinienwarnung für jede Konversation aus (in der Annahme, dass sie im Geltungsbereich der angegebenen Richtlinienbedingungen liegt). Damit Richtlinien vom Typ „Netzwerk-Baseline-Abweichung“ erstellt werden können, müssen Sie zuerst eine anfängliche Netzwerk-Baseline im Bildschirm

Netzwerkübersicht erstellen. Sie können die Netzwerk-Baseline jederzeit durch Festlegen einer neuen Netzwerk-Baseline aktualisieren.

### So legen Sie eine Netzwerk-Baseline fest:

1. Wählen Sie im Bildschirm Netzwerkübersicht mithilfe der Zeitraumauswahl oben im Bildschirm den Zeitraum der Konversationen aus, die in die Netzwerk-Baseline aufgenommen werden sollen.

   Die Netzwerkübersicht für den ausgewählten Zeitraum wird angezeigt.

2. Wählen Sie in der oberen rechten Ecke Aktionen > Als Baseline festlegen aus.

   OT Security konfiguriert die neue Netzwerk-Baseline und wendet sie auf alle Richtlinien vom Typ „Netzwerk-Baseline-Abweichung“ an.

# Datenerfassung

Der Abschnitt Datenerfassung in OT Security enthält die folgenden Konfigurationsseiten:

- Richtlinien
- Aktive Abfragen verwalten
- Datenquellen

## Richtlinien

OT Security enthält Richtlinien, die bestimmte Arten von Ereignissen definieren, die verdächtig, nicht autorisiert, anormal oder anderweitig auffällig sind und im Netzwerk stattfinden. Wenn ein Ereignis eintritt, das alle Bedingungen der Richtliniendefinition für eine bestimmte Richtlinie erfüllt, generiert das System ein Ereignis. Das System protokolliert das Ereignis und sendet Benachrichtigungen gemäß den für die Richtlinien konfigurierten Richtlinienaktionen.

- Richtlinienbasierte Erkennung – Löst ein Ereignis aus, wenn die genauen Bedingungen der Richtlinie, wie durch eine Reihe von Ereignisdeskriptoren definiert, erfüllt sind.
- Anomalie-Erkennung – Löst Ereignisse aus, wenn OT Security anomale oder verdächtige Aktivitäten im Netzwerk erkennt.

OT Security verfügt über eine Reihe vordefinierter (sofort einsetzbarer) Richtlinien. Darüber hinaus können Sie die vordefinierten Richtlinien bearbeiten oder neue benutzerdefinierte Richtlinien definieren.

> Hinweis: Standardmäßig sind die meisten Richtlinien aktiviert. Informationen zum Aktivieren/Deaktivieren von Richtlinien finden Sie unter Richtlinien aktivieren oder deaktivieren.

### Richtlinienkonfiguration

Jede Richtlinie besteht aus einer Reihe von Bedingungen, die einen bestimmten Verhaltenstyp im Netzwerk definieren. Dazu gehören Überlegungen wie die Aktivität, die beteiligten Assets und der Zeitpunkt des Ereignisses. Nur ein Ereignis, das allen in der Richtlinie festgelegten Parametern entspricht, löst ein Ereignis für diese Richtlinie aus. Jede Richtlinie hat eine bestimmte Konfiguration für Richtlinienaktionen, die den Schweregrad, die Benachrichtigungsmethoden und die Protokollierung des Ereignisses definiert.

## Gruppen

Eine wesentliche Komponente bei der Definition von Richtlinien in OT Security ist die Verwendung von Gruppen. Bei der Konfiguration einer Richtlinie gehört jeder Richtlinienparameter zu einer Gruppe, nicht zu einzelnen Entitäten. Dadurch wird der Prozess für die Richtlinienkonfiguration optimiert. Wenn beispielsweise die Aktivität „Firmware-Update“ als verdächtige Aktivität gilt, wenn sie zu bestimmten Tageszeiten (z. B. während der Arbeitszeit) auf einem Controller durchgeführt wird, können Sie statt einer separaten Richtlinie für jeden Controller in Ihrem Netzwerk eine einzige Richtlinie erstellen, die für die Asset-Gruppe „Controller“ gilt.

Für die Richtlinienkonfiguration werden die folgenden Arten von Gruppen verwendet:

- Asset-Gruppen – Das System verfügt über vordefinierte Asset-Gruppen basierend auf dem Asset-Typ. Sie können benutzerdefinierte Gruppen hinzufügen, die auf anderen Faktoren wie Standort, Abteilung und Kritikalität basieren.
- Netzwerksegmente – Das System erstellt automatisch generierte Netzwerksegmente basierend auf Asset-Typ und IP-Bereich. Sie können benutzerdefinierte Netzwerksegmente erstellen, die eine beliebige Gruppe von Assets mit ähnlichen Kommunikationsmustern definieren.
- E-Mail-Gruppen – Gruppieren Sie mehrere E-Mail-Konten, die E-Mail-Benachrichtigungen für bestimmte Ereignisse erhalten. Sie können z. B. nach Rolle und Abteilung gruppieren.
- Port-Gruppen – Gruppieren Sie Ports, die auf ähnliche Weise verwendet werden. Zum Beispiel Ports, die auf Rockwell-Controllern offen sind.

- Protokollgruppen – Gruppieren Sie Kommunikationsprotokolle nach Protokolltyp (z. B. Modbus) oder Hersteller (z. B. von Rockwell zugelassene Protokolle).
- Planungsgruppen – Gruppieren Sie mehrere Zeitbereiche als Planungsgruppe mit einem bestimmten gemeinsamen Merkmal. Zum Beispiel Arbeitszeiten und Wochenende.
- Tag-Gruppen – Gruppieren Sie Tags, die ähnliche Betriebsdaten in verschiedenen Controllern enthalten. Zum Beispiel Tags, die die Ofentemperatur steuern.
- Regelgruppen – Gruppieren Sie verwandte Regeln, die durch ihre Suricata-Signatur-IDs (SIDs) identifiziert werden. Diese Gruppen werden als Richtlinienbedingung zum Definieren von Intrusion Detection-Richtlinien verwendet.

Richtlinien können nur mit Gruppen definiert werden, die in Ihrem System konfiguriert sind. Das System wird mit einer Reihe vordefinierter Gruppen geliefert. Sie können diese Gruppen bearbeiten und eigene Gruppen hinzufügen, siehe Gruppen.

> Hinweis: Richtlinienparameter können nur mithilfe von Gruppen festgelegt werden. Selbst wenn eine Richtlinie für eine einzelne Entität gelten soll, müssen Sie eine Gruppe konfigurieren, die nur diese Entität enthält.

## Schweregradstufen

Jeder Richtlinie ist ein bestimmter Schweregrad zugewiesen, der den Grad des Risikos angibt, das von der Situation ausgeht, die das Ereignis ausgelöst hat. In der folgenden Tabelle werden die verschiedenen Schweregrade beschrieben:

| Schweregrad | Beschreibung |
|---|---|
| Kein | Das Ereignis ist kein Grund zur Besorgnis. |
| Gering | Kein unmittelbarer Grund zur Sorge. Sollte bei Gelegenheit geprüft werden. |
| Mittel | Moderate Bedenken, dass potenziell schädliche Aktivitäten stattgefunden |

| | |
|---|---|
| | haben. Sollte behandelt werden, wenn es passt. |
| Hoch | Schwerwiegende Bedenken, dass potenziell schädliche Aktivitäten stattgefunden haben. Sollte sofort behandelt werden. |

## Ereignisbenachrichtigungen

Wenn ein Ereignis eintritt, das die Bedingungen der Richtlinie erfüllt, wird ein Ereignis ausgelöst. Im Abschnitt Ereignisse wird Alle Ereignisse angezeigt. Auf der Seite Richtlinie wird das Ereignis unter der Richtlinie aufgeführt, die das Ereignis ausgelöst hat. Auf der Seite Inventar wird das Ereignis unter dem betroffenen Asset aufgeführt. Darüber hinaus können Sie Richtlinien so konfigurieren, dass Benachrichtigungen über Ereignisse mithilfe des Syslog-Protokolls an ein externes SIEM-System und/oder an bestimmte E-Mail-Empfänger gesendet werden.

- Syslog-Benachrichtigung – Syslog-Nachrichten verwenden das CEF-Protokoll sowohl mit Standardschlüsseln als auch mit benutzerdefinierten Schlüsseln (für die Verwendung mit OT Security konfiguriert). Eine Erläuterung zur Interpretation von Syslog-Benachrichtigungen finden Sie im OT Security Syslog Integration Guide.
- E-Mail-Benachrichtigungen – E-Mail-Nachrichten enthalten Details über das Ereignis, das die Benachrichtigung generiert hat, sowie Schritte zur Eindämmung der Bedrohung.

## Richtlinienkategorien und Unterkategorien

In OT Security werden die Richtlinien nach folgenden Kategorien geordnet:

- Konfigurationsereignisse – Diese Richtlinien beziehen sich auf die Aktivitäten, die im Netzwerk stattfinden. Es gibt zwei Unterkategorien:
    - Controller-Validierung – Diese Richtlinien beziehen sich auf Änderungen, die in den Controllern im Netzwerk stattfinden. Dabei kann es sich um Statusänderungen eines Controllers, aber auch um Änderungen an Firmware, Asset-Eigenschaften oder

Codeblöcken handeln. Die Richtlinien können auf bestimmte Zeitpläne (z. B. Firmware-Upgrade während eines Arbeitstages) und/oder bestimmte Controller beschränkt werden.

- Controller-Aktivitäten – Diese Richtlinien beziehen sich auf bestimmte Engineering-Befehle, die sich auf den Status und die Konfiguration von Controllern auswirken. Es ist möglich, bestimmte Aktivitäten zu definieren, die immer Ereignisse generieren, oder eine Reihe von Kriterien zum Generieren von Ereignissen festzulegen. Zum Beispiel, wenn bestimmte Aktivitäten zu bestimmten Zeiten und/oder auf bestimmten Controllern ausgeführt werden. Sperrlisten und Zulassungslisten für Assets, Aktivitäten und Zeitpläne werden unterstützt.

- Netzwerkereignisse – Diese Richtlinien beziehen sich auf die Assets im Netzwerk und die Kommunikationsströme zwischen Assets. Dies schließt Assets ein, die dem Netzwerk hinzugefügt oder daraus entfernt werden. Dazu gehören auch Traffic-Muster, die für das Netzwerk ungewöhnlich sind oder als besorgniserregend gekennzeichnet wurden. Wenn beispielsweise eine Engineering-Station mit einem Controller über ein Protokoll kommuniziert, das nicht Teil eines vorkonfigurierten Satzes von Protokollen ist (z. B. Protokolle, die von Controllern verwendet werden, die von einem bestimmten Anbieter hergestellt werden), löst die Richtlinie ein Ereignis aus. Sie können diese Richtlinien auf bestimmte Zeitpläne und/oder bestimmte Assets beschränken. Anbieterspezifische Protokolle werden der Einfachheit halber nach Anbieter organisiert, es kann jedoch jedes Protokoll in einer Richtliniendefinition verwendet werden.

- SCADA-Ereignisrichtlinien – Diese Richtlinien erkennen Änderungen der Sollwerte, die den industriellen Prozess beeinträchtigen können. Diese Änderungen können aus einem Cyberangriff oder menschlichem Fehlverhalten resultieren.

- Netzwerkbedrohungsrichtlinien – Diese Richtlinien verwenden signaturbasierte OT- und IT-Bedrohungserkennung, um Netzwerk-Traffic zu identifizieren, der auf Bedrohungen durch Eindringlinge hinweist. Die Erkennung basiert auf Regeln, die in der Threats-Engine von Suricata katalogisiert sind.

## Richtlinientypen

Innerhalb jeder Kategorie und Unterkategorie gibt es eine Reihe verschiedener Typen von Richtlinien. OT Security enthält die vordefinierten Richtlinien der einzelnen Typen. Sie können auch Ihre eigenen benutzerdefinierten Richtlinien der einzelnen Typen erstellen. In den folgenden Tabellen werden die verschiedenen Richtlinientypen nach Kategorie gruppiert erläutert.

### Konfigurationsereignis – Typen von Controller-Aktivitätsereignissen

Controller-Aktivitäten beziehen sich auf die Aktivitäten, die im Netzwerk stattfinden. Zum Beispiel die „Befehle“, die zwischen Assets im Netzwerk implementiert werden. Es gibt viele verschiedene Typen von Controller-Aktivitätsereignissen. Der Typ des Controllers, auf dem die Aktivität stattfindet, sowie die spezifische Aktivität definieren den Typ der Controller-Aktivität. Beispiele: Rockwell-SPS-Stopp, SIMATIC-Code-Download und Modicon-Online-Sitzung.

Die Parameter für die Richtliniendefinition bzw. Richtlinienbedingungen, die für Controller-Aktivitätsereignisse gelten, sind „Quell-Asset“, „Ziel-Asset“ und „Zeitplan“.

### Konfigurationsereignis – Typen von Controller-Validierungsereignissen

Die folgende Tabelle beschreibt die verschiedenen Typen von Controller-Validierungsereignissen.

> Hinweis: Richtlinienbedingungen in Bezug auf betroffene Assets, Quellen oder Ziele können festgelegt werden, indem entweder eine Asset-Gruppe oder ein Netzwerksegment ausgewählt wird .

| Ereignistyp | Richtlinienbedingungen | Beschreibung |
|---|---|---|
| Änderung des Schlüsselschalters | Betroffenes Asset, Zeitplan | Eine Änderung am Controller-Status durch Anpassen der Position des physischen Schlüssels. Unterstützt derzeit nur Rockwell-Controller. |
| Statusänderung | Betroffenes Asset, Zeitplan | Der Controller wechselte von einem Betriebsstatus in einen anderen. Zum |

| | | |
|---|---|---|
| | | Beispiel „Wird ausgeführt“, „Gestoppt“ und „Test“. |
| Änderung der Firmware-Version | Betroffenes Asset, Zeitplan | Eine Änderung an der auf dem Controller ausgeführten Firmware. |
| Modul nicht gesehen | Betroffenes Asset, Zeitplan | Erkennt ein zuvor identifiziertes Modul, das von einer Backplane entfernt wurde. |
| Neues Modul erfasst | Betroffenes Asset, Zeitplan | Erkennt ein neues Modul, das einer vorhandenen Backplane hinzugefügt wird. |
| Snapshot-Konflikt | Betroffenes Asset, Zeitplan | Der letzte Snapshot eines Controllers (der den aktuellen Status des auf einem Controller bereitgestellten Programms erfasst) war nicht identisch mit dem vorherigen Snapshot dieses Controllers. |

### Netzwerkereignistypen

Die folgende Tabelle beschreibt die verschiedenen Typen von Netzwerkereignissen.

> Hinweis: Richtlinienbedingungen in Bezug auf betroffene Assets, Quellen oder Ziele können festgelegt werden, indem entweder eine Asset-Gruppe oder ein Netzwerksegment ausgewählt wird .

| Ereignistyp | Richtlinienbedingungen | Beschreibung |
|---|---|---|
| Asset nicht gesehen | Nicht gesehen seit, Betroffenes Asset, Zeitplan | Erkennt zuvor identifizierte Assets in der Gruppe „Betroffene Assets“, die für die angegebene Zeitdauer innerhalb |

| | | |
|---|---|---|
| | | des angegebenen Zeitraums aus dem Netzwerk entfernt wurden. |
| Rediscovered Asset (Erneut erfasstes Asset) | Inaktiv seit, Betroffene Assets, Zeitplan | Erkennt ein Asset, das online geschaltet wird oder wieder zu kommunizieren beginnt, nachdem es für eine bestimmte Zeit offline war. |
| Änderung der USB-Konfiguration | Betroffene Assets, Zeitplan | Erkennt, wenn ein USB-Gerät mit einer Windows-basierte Workstation verbunden oder von dieser getrennt wird. Die Richtlinie gilt für Änderungen an einem Asset in der Gruppe „Betroffene Assets“ während des angegebenen Zeitraums. |
| IP-Konflikt | Zeitplan | Erkennt, wenn mehrere Assets im Netzwerk die gleiche IP-Adresse verwenden. Dies kann auf einen Cyberangriff hindeuten oder auf mangelhafte Netzwerkverwaltung zurückzuführen sein. Die Richtlinie gilt für IP-Konflikte, die OT Security während des angegebenen Zeitraums erkennt. |
| Netzwerk-Baseline-Abweichung | Quelle, Ziel, Protokoll, Zeitplan | Erkennt neue Verbindungen zwischen Assets, die während der Netzwerk-Baseline-Stichprobe nicht miteinander kommuniziert haben. Diese Option ist nur verfügbar, nachdem eine Netzwerk-Baseline im System eingerichtet wurde. |

| | | |
|---|---|---|
| | | Informationen zum Festlegen der anfänglichen Netzwerk-Baseline oder zum Aktualisieren der Netzwerk-Baseline finden Sie unter Festlegen einer Netzwerk-Baseline. Die Richtlinie gilt für die Kommunikation von einem Asset in der Quell-Asset-Gruppe zu einem Asset in der Ziel-Asset-Gruppe unter Verwendung eines Protokolls aus der Protokollgruppe während des angegebenen Zeitraums. |
| Neues Asset erfasst | Betroffenes Asset, Zeitplan | Erkennt neue Assets des in der Quell-Asset-Gruppe angegebenen Typs, die während des angegebenen Zeitraums in Ihrem Netzwerk angezeigt wird. |
| Offener Port | Betroffenes Asset, Port | Erkennt neue offene Ports in Ihrem Netzwerk. Ungenutzte offene Ports können ein Sicherheitsrisiko darstellen. Die Richtlinie gilt für Assets in der Gruppe „Betroffene Assets“ und für Ports, die sich in der Port-Gruppe befinden. |
| Spitze im Netzwerk-Traffic | Zeitfenster, Empfindlichkeitsstufe, Zeitplan | Erkennt anomale Spitzen im Netzwerk-Traffic-Volumen. Die Richtlinie gilt für Spitzen relativ zum angegebenen Zeitfenster und basierend auf der angegebenen Empfindlichkeitsstufe. Sie ist auch auf den angegebenen Zeitbereich begrenzt. |

| | | |
|---|---|---|
| Spike in Konversation | Zeitfenster, Empfindlichkeitsstufe, Zeitplan | Erkennt anomale Spitzen in der Anzahl der Konversationen im Netzwerk. Die Richtlinie gilt für Spitzen relativ zum angegebenen Zeitfenster und basierend auf der angegebenen Empfindlichkeitsstufe. Sie ist auch auf den angegebenen Zeitbereich begrenzt. |
| RDP-Verbindung (authentifiziert) | Quelle, Ziel, Zeitplan | Im Netzwerk wurde eine RDP-Verbindung (Remote Desktop Protocol) mit Authentifizierungsdaten hergestellt. Die Richtlinie gilt für ein Asset in der Quell-Asset-Gruppe, das eine Verbindung zu einem Asset in der Ziel-Asset-Gruppe während des angegebenen Zeitraums herstellt. |
| RDP-Verbindung (nicht authentifiziert) | Quelle, Ziel, Zeitplan | Im Netzwerk wurde eine RDP-Verbindung (Remote Desktop Protocol) ohne Authentifizierungsdaten hergestellt. Die Richtlinie gilt für ein Asset in der Quell-Asset-Gruppe, das während des angegebenen Zeitraums eine Verbindung zu einem Asset in der Ziel-Asset-Gruppe herstellt. |
| Nicht autorisierte Konversation | Quelle, Ziel, Protokoll, Zeitplan | Erkennt Kommunikation, die zwischen Assets im Netzwerk gesendet wird. Die Richtlinie gilt für die Kommunikation von einem Asset in der Quell-Asset-Gruppe zu einem Asset in der Ziel- |

| | | |
|---|---|---|
| | | Asset-Gruppe unter Verwendung eines Protokolls aus der Protokollgruppe während des angegebenen Zeitraums. |
| Erfolgreiches ungesichertes FTP-Login | Quelle, Ziel, Zeitplan | OT Security betrachtet FTP als unsicheres Protokoll. Diese Richtlinie erkennt erfolgreiche Logins über FTP. |
| Fehlgeschlagenes ungesichertes FTP-Login | Quelle, Ziel, Zeitplan | OT Security betrachtet FTP als unsicheres Protokoll. Diese Richtlinie erkennt fehlgeschlagene Login-Versuche über FTP. |
| Erfolgreiches ungesichertes Telnet-Login | Quelle, Ziel, Zeitplan | OT Security betrachtet Telnet als unsicheres Protokoll. Diese Richtlinie erkennt erfolgreiche Logins über Telnet. |
| Fehlgeschlagenes ungesichertes Telnet-Login | Quelle, Ziel, Zeitplan | OT Security betrachtet Telnet als unsicheres Protokoll. Diese Richtlinie erkennt fehlgeschlagene Login-Versuche über Telnet. |
| Ungesicherter Telnet-Login-Versuch | Quelle, Ziel, Zeitplan | OT Security betrachtet Telnet als unsicheres Protokoll. Diese Richtlinie erkennt Login-Versuche über Telnet (für die der Ergebnisstatus nicht erkannt wurde). |

### Netzwerkbedrohungs-Ereignistypen

Die folgende Tabelle beschreibt die verschiedenen Typen von Netzwerkbedrohungsereignissen.

Hinweis: Richtlinienbedingungen in Bezug auf betroffene Assets, Quellen oder Ziele können festgelegt werden, indem entweder eine Asset-Gruppe oder ein Netzwerksegment ausgewählt wird .

| Ereignistyp | Richtlinienbedingungen | Beschreibung |
|---|---|---|
| Intrusion Detection | Quelle, betroffenes Asset, Regelgruppe, Zeitplan | Intrusion Detection-Richtlinien verwenden signaturbasierte OT- und IT-Bedrohungserkennung, um Netzwerk-Traffic zu identifizieren, der auf Bedrohungen durch Eindringlinge hinweist. Die Erkennung basiert auf Regeln, die in der Threats-Engine von Suricata katalogisiert sind. Die Regeln sind in Kategorien (ICS-Angriffe, Denial of Service und Malware) und Unterkategorien (ICS-Angriffe – Stuxnet, ICS-Angriffe – Black Energy) gruppiert. Das System wird mit einer Reihe von vordefinierten Gruppen verwandter Regeln geliefert. Sie können auch Ihre eigenen benutzerdefinierten Gruppierungen verschiedener Regeln konfigurieren.<br><br>Hinweis: Für IDS-Ereignisse (Intrusion Detection System, Angriffserkennungssystem) können die Asset-Gruppen Quelle und Ziel nicht bearbeitet werden. |
| ARP-Scan | Betroffenes Asset, Zeitplan | Erkennt ARP-Scans (Netzwerkaufklärungsaktivität), die im Netzwerk ausgeführt werden. Die Richtlinie gilt für Scans, die während des angegebenen Zeitraums in der Gruppe „Betroffene Assets“ übertragen werden. |

| | | |
|---|---|---|
| Port-Scan | Quell-Asset, Ziel-Asset, Zeitplan | Erkennt SYN-Scans (Netzwerkaufklärungsaktivität), die im Netzwerk ausgeführt werden, um offene (anfällige) Ports zu erkennen. Die Richtlinie gilt für Kommunikation von einem Asset in der Quell-Asset-Gruppe zu einem Asset in der Ziel-Asset-Gruppe während des angegebenen Zeitraums. |

## SCADA-Ereignistypen

Die folgende Tabelle beschreibt die verschiedenen Typen von SCADA-Ereignistypen.

> Hinweis: Richtlinienbedingungen in Bezug auf betroffene Assets, Quellen oder Ziele können festgelegt werden, indem entweder eine Asset-Gruppe oder ein Netzwerksegment ausgewählt wird .

| Ereignistyp | Richtlinienbedingungen | Beschreibung |
|---|---|---|
| Unzulässige Modbus-Datenadresse | Quell-Asset, Ziel-Asset, Zeitplan | Erkennt den Fehlercode „Unzulässige Datenadresse“ im Modbus-Protokoll. Die Richtlinie gilt für Kommunikation von einem Asset in der Quell-Asset-Gruppe zu einem Asset in der Ziel-Asset-Gruppe während des angegebenen Zeitraums. |
| Unzulässiger Modbus-Datenwert | Quell-Asset, Ziel-Asset, Zeitplan | Erkennt den Fehlercode „Unzulässiger Datenwert“ |

| | | |
|---|---|---|
| | | im Modbus-Protokoll. Die Richtlinie gilt für Kommunikation von einem Asset in der Quell-Asset-Gruppe zu einem Asset in der Ziel-Asset-Gruppe während des angegebenen Zeitraums. |
| Unzulässige Modbus-Funktion | Quell-Asset, Ziel-Asset, Zeitplan | Erkennt den Fehlercode „Unzulässige Funktion“ im Modbus-Protokoll. Die Richtlinie gilt für Kommunikation von einem Asset in der Quell-Asset-Gruppe zu einem Asset in der Ziel-Asset-Gruppe während des angegebenen Zeitraums. |
| Nicht autorisierter Schreibvorgang | Quell-Asset, Tag-Gruppe, Tag-Wert, Zeitplan | Erkennt nicht autorisierte Tag-Schreibvorgänge für die angegebenen Tags auf einem Controller (derzeit unterstützt für Rockwell- und S7-Controller) in der angegebenen Quell-Asset-Gruppe. Sie können die Richtlinie so konfigurieren, dass sie jeden neuen Schreibvorgang, eine |

| | | |
|---|---|---|
| | | Änderung von einem angegebenen Wert oder einen Wert außerhalb eines angegebenen Bereichs erkennt. Die Richtlinie gilt nur während des angegebenen Zeitraums. |
| ABB – Nicht autorisierter Schreibvorgang | Quell-Asset, Ziel-Asset, Zeitplan | Erkennt über MMS an ABB 800xA-Controller gesendete Schreibbefehle, die außerhalb des zulässigen Bereichs liegen. |
| IEC 60870-5-104-Befehle (Start/Stopp der Datenübertragung, Abfragebefehl, Zählerabfragebefehl, Uhrensynchronisationsbefehl, Befehl zur Prozessrücksetzung, Testbefehl mit Zeitmarke) | Quell-Asset, Ziel-Asset, Zeitplan | Erkennt bestimmte Befehle, die an übergeordnete oder untergeordnete IEC-104-Einheiten gesendet werden und als riskant gelten. |
| DNP3-Befehle | Quell-Asset, Ziel-Asset, Zeitplan | Erkennt alle Hauptbefehle, die über das DNP3-Protokoll gesendet werden. Zum Beispiel „Select“, „Operate“ und „Warm/Cold Restart“. Erkennt auch Fehler, die auf interne Indikatoren wie nicht unterstützte |

| | | |
|---|---|---|
| | | Funktionscodes und Parameterfehler zurückzuführen sind. |

## Richtlinien aktivieren oder deaktivieren

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager

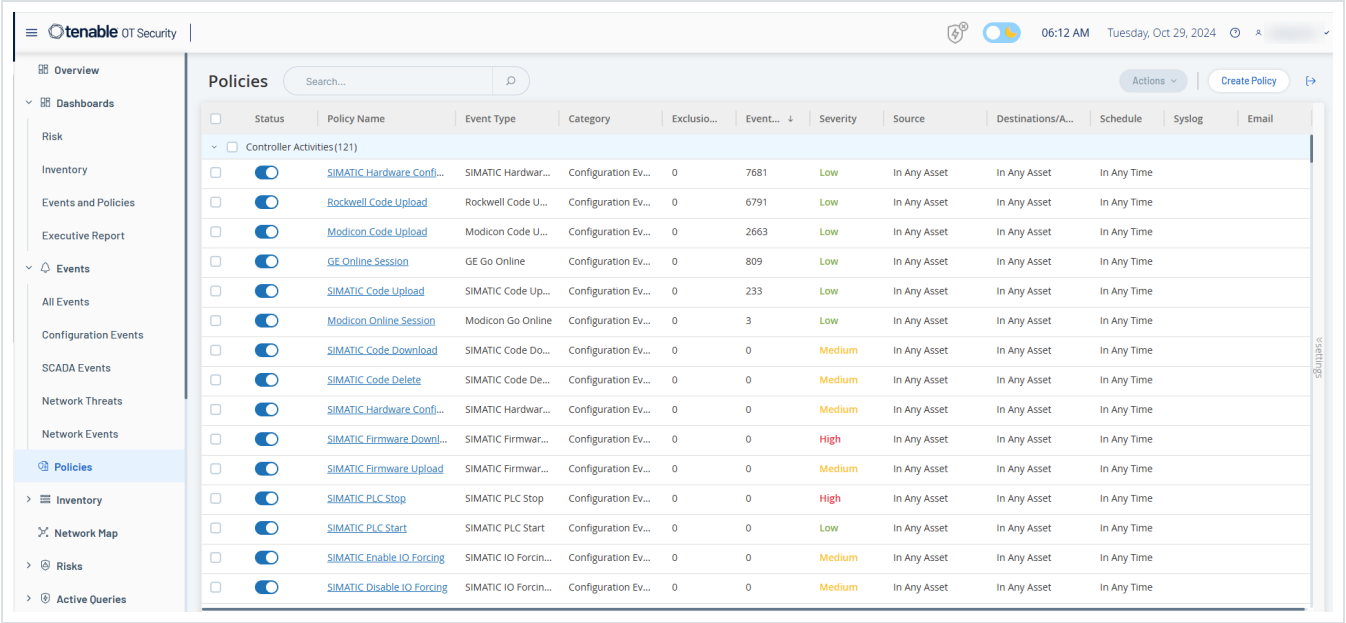
Sie können jede konfigurierte Richtlinie in Ihrem System (sowohl vorkonfiguriert als auch benutzerdefiniert) aktivieren oder deaktivieren. Sie können einzelne Richtlinien aktivieren/deaktivieren oder mehrere Richtlinien auswählen, um sie gesammelt zu aktivieren/deaktivieren.

> Hinweis: Viele Richtlinien sind bei der Erfassung von Daten auf Abfragen angewiesen. Wenn einige oder alle Abfragefunktionen deaktiviert sind, können die entsprechenden Richtlinien nicht angewendet werden. Sie können Abfragen über Aktive Abfragen aktivieren, siehe Aktive Abfragen.

### So aktivieren oder deaktivieren Sie eine Richtlinie:

1. Gehen Sie zu Richtlinien.

   Auf der Seite werden alle im System konfigurierten Richtlinien aufgelistet, gruppiert nach Richtlinienkategorie.

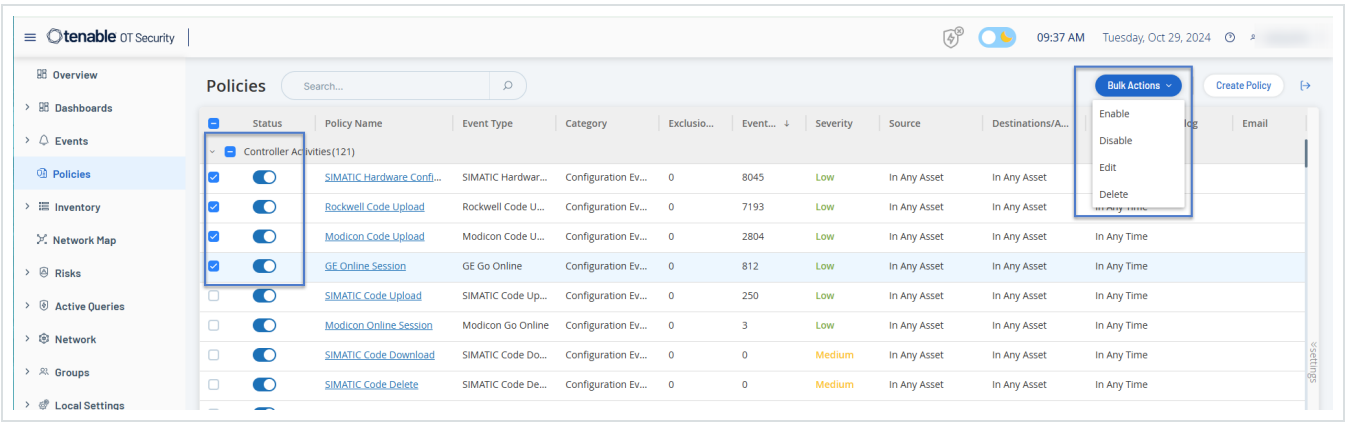



2. Um die Richtlinie zu aktivieren oder zu deaktivieren, klicken Sie auf den Umschalter Status neben der entsprechenden Richtlinie.

## So aktivieren oder deaktivieren Sie Richtlinien:

1. Gehen Sie zu Richtlinien.

   Auf der Seite werden alle im System konfigurierten Richtlinien aufgelistet, gruppiert nach Richtlinienkategorie.



2. Aktivieren Sie das Kontrollkästchen neben jeder Richtlinie, die Sie aktivieren zw. deaktivieren möchten. Verwenden Sie eine der folgenden Auswahlmethoden:

    - Einzelne Richtlinien auswählen – Klicken Sie auf das Kontrollkästchen neben bestimmten Richtlinien.
    - Richtlinientypen auswählen – Klicken Sie auf das Kontrollkästchen neben der Überschrift eines Richtlinientyps.
    - Alle Richtlinien auswählen – Klicken Sie auf das Kontrollkästchen in der Titelleiste oben in der Tabelle.

3. Wählen Sie im Dropdown-Feld Massenaktionen die gewünschte Aktion (Aktivieren oder Deaktivieren) aus.

    OT Security aktiviert oder deaktiviert die ausgewählten Richtlinien.

## Richtlinien anzeigen

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager, Sicherheitsanalyst, Site-Operator, Schreibgeschützt

Im Bildschirm Richtlinien werden alle konfigurierten Richtlinien in Ihrem System aufgeführt. Die Listen sind für jede Richtlinienkategorie auf separaten Registerkarten gruppiert. Auf dieser Seite werden sowohl vorkonfigurierte Richtlinien als auch benutzerdefinierte Richtlinien aufgelistet. Für jede Richtlinie gibt es einen Umschalter, der den aktuellen Status der Richtlinie anzeigt, sowie mehrere Parameter, die die Richtlinienkonfiguration angeben.

Sie können Spalten ein- und ausblenden und die Asset-Listen sortieren und filtern sowie nach Schlüsselwörtern suchen. Informationen zum Anpassen der Liste finden Sie unter Elemente in der Benutzeroberfläche der Verwaltungskonsole.

In der folgenden Tabelle werden die Richtlinienparameter beschrieben:

| Parameter | Beschreibung |
| --- | --- |
| Status | Zeigt an, ob die Richtlinie aktiviert oder deaktiviert ist. Wenn das System die Richtlinie automatisch deaktiviert hat, weil sie zu viele Ereignisse generiert hat, wird ein Warnsymbol neben dem Umschalter angezeigt. Schalten Sie den Status-Schalter um, um eine Richtlinie zu aktivieren/deaktivieren. |
| Richtlinien-ID | Ein eindeutiger Bezeichner für die Richtlinie im System. Richtlinien-IDs sind nach Kategorie gruppiert, mit einem anderen Präfix für jede Kategorie. Zum Beispiel P1 für Controller-Aktivitäten und P2 für Netzwerkereignisse. |
| Name | Der Name der Richtlinie. |
| Schweregrad | Der Schweregrad des Ereignisses. Mögliche Werte sind: Kein, Gering, Mittel oder Hoch. Eine Beschreibung der Schweregrade finden Sie im Abschnitt Schweregrade. |
| Ereignistyp | Der spezifische Ereignistyp, der diese Ereignisrichtlinie auslöst. |
| Kategorie | Die allgemeine Kategorie für den Ereignistyp, der diese Ereignisrichtlinie auslöst. Mögliche Werte sind: Konfiguration, SCADA, Netzwerkbedrohungen oder Netzwerkereignis. Weitere Informationen zu den verschiedenen Kategorien finden Sie unter Kategorien und Unterkategorien von Richtlinien. |
| Quelle | Eine Richtlinienbedingung. Die Quell-Asset-Gruppe/das Quell-Netzwerksegment (d. h. das Asset, das die Aktivität initiiert hat), für die bzw. das die Richtlinie gilt. |
| Ziel-Asset/Betroffenes Asset | Eine Richtlinienbedingung. Die Ziel-Asset-Gruppe/das Ziel-Netzwerksegment (d. h. das Asset, das die Aktivität erhält), für die bzw. das die Richtlinie gilt. Bei Richtlinien, die ein einzelnes Asset betreffen |

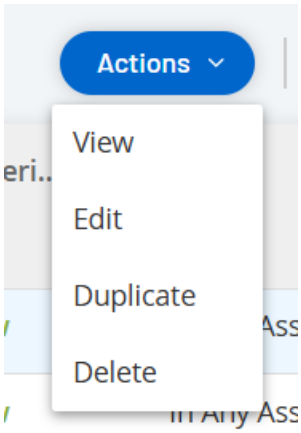
| | |
|---|---|
| | (ohne Quelle und Ziel), zeigt dieser Parameter das Asset an, das von dem Ereignis betroffen ist. |
| Zeitplan | Eine Richtlinienbedingung. Der Zeitraum, für den die Richtlinie gilt. |
| Syslog | Der Syslog-Server (SIEM), auf dem Ereignisse für diese Richtlinie protokolliert werden. |
| E-Mail | Die E-Mail-Gruppe, die die Ereignisbenachrichtigungen für diese Richtlinie sendet. |
| Unterkategorie | Die Unterkategorieklassifizierung des Ereignisses. Die Kategorie „Konfigurationsereignisse“ setzt sich aus den folgenden Unterkategorien zusammen: „Controller-Aktivitäten“ und „Controller-Validierung“. Informationen zu den verschiedenen Unterkategorien finden Sie unter Richtlinien anzeigen. |
| Anzahl der Ereignisse pro Richtlinie | Listet die Anzahl der Ereignisse auf, die von jeder Richtlinie generiert werden. Sie können auf die Spalte klicken, um die Liste zu sortieren, sodass Sie sich auf die Richtlinien mit den meisten Verstößen/Ereignissen konzentrieren können. |
| Ausschlüsse | Listet die Anzahl der Ausschlüsse auf, die jeder Richtlinie hinzugefügt wurden. Weitere Informationen finden Sie unter Ereignisse. |

## Richtliniendetails anzeigen

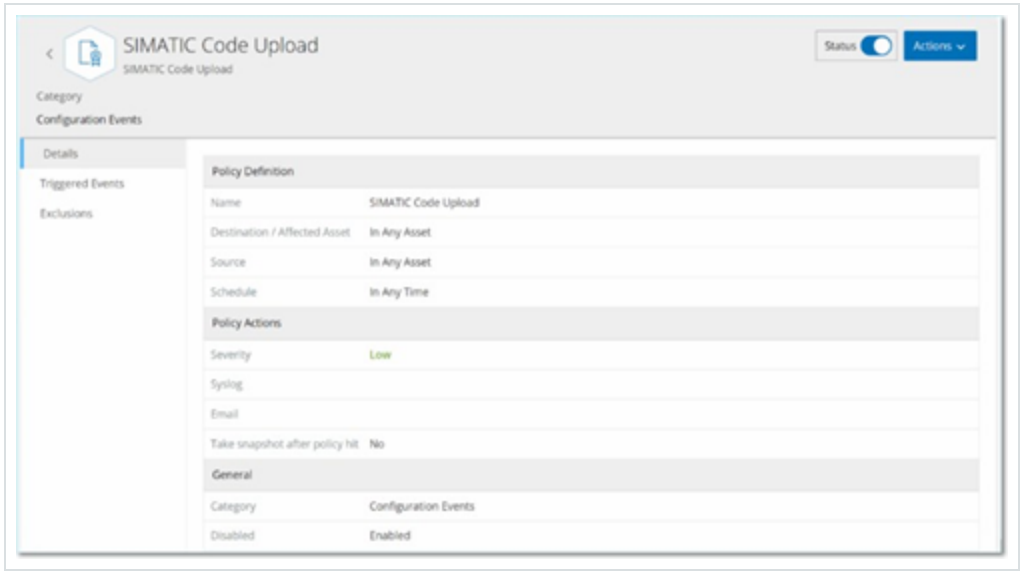
Sie können die Seite Richtliniendetails für eine Richtlinie öffnen, um weitere Details zur Richtlinie anzuzeigen. Auf dieser Seite werden alle Richtlinienbedingungen und -ereignisse aufgelistet, die durch die Richtlinie ausgelöst wurden.

### So öffnen Sie den Bildschirm Richtliniendetails für eine bestimmte Richtlinie:

1. Wählen Sie auf der Seite Richtlinien die gewünschte Richtlinie aus.
2. Wählen Sie im Dropdown-Feld Aktionen die Option Anzeigen aus.




Die Seite „Richtliniendetails“ für die ausgewählte Richtlinie wird angezeigt.




> Hinweis: Alternativ können Sie das Menü „Aktionen“ aufrufen, indem Sie mit der rechten Maustaste auf die entsprechende Richtlinie klicken.

Die Seite „Richtliniendetails“ enthält die folgenden Elemente:

- Kopfleiste – Zeigt Namen, Typ und Kategorie der Richtlinie an. Die Seite enthält außerdem einen Umschalter zum Aktivieren und Deaktivieren der Richtlinie und eine Dropdown-Liste der verfügbaren Aktionen (Bearbeiten, Duplizieren und Löschen).
- Registerkarte „Details“ – Zeigt Details zur Richtlinienkonfiguration in den folgenden Abschnitten an:
    - Richtliniendefinition – Zeigt alle Richtlinienbedingungen an. Dies umfasst alle relevanten Felder gemäß dem Richtlinientyp.
    - Richtlinienaktionen – Zeigt den Schweregrad sowie das Ziel (Syslog, E-Mail) von Ereignisbenachrichtigungen an. Zeigt auch an, ob die Funktion Snapshot nach Richtlinientreffer erstellen aktiviert ist.
    - Allgemein – Zeigt die Kategorie und den Status der Richtlinie an.
- Ausgelöste Ereignisse – Zeigt eine Liste von Ereignissen an, die von dieser Richtlinie ausgelöst wurden. Außerdem werden Details zu den an dem Ereignis beteiligten Assets und die Art des Ereignisses angezeigt. Die auf dieser Registerkarte angezeigten Informationen sind identisch mit den Informationen auf der Seite Ereignisse, außer dass auf dieser Registerkarte nur Ereignisse für die angegebene Richtlinie angezeigt werden. Eine Erläuterung der Ereignisinformationen finden Sie unter Anzeigen von Ereignissen.

  Registerkarte Ausschlüsse – Wenn eine Richtlinie Ereignisse für bestimmte Bedingungen generiert, die keine Sicherheitsbedrohung darstellen, können Sie diese Bedingungen von der Richtlinie ausschließen (d. h. keine Ereignisse mehr für diese bestimmten Bedingungen generieren). Ausschlüsse können auf der Seite Ereignisse hinzugefügt werden, siehe Ereignisse. Auf der Registerkarte Ausschlüsse werden alle Ausschlüsse angezeigt, die für diese Richtlinie gelten. Für jeden Ausschluss werden außerdem die spezifischen ausgeschlossenen Bedingungen angegeben. Auf dieser Registerkarte können Sie einen Ausschluss löschen, was es dem System ermöglicht, die Generierung von Ereignissen für die angegebenen Bedingungen fortzusetzen.

## Richtlinien erstellen

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager

Sie können benutzerdefinierte Richtlinien basierend auf den spezifischen Überlegungen für Ihr ICS-Netzwerk erstellen. Sie können genau bestimmen, auf welche Art von Ereignissen Ihre Mitarbeiter aufmerksam gemacht werden müssen und wie die Benachrichtigungen zugestellt werden. Bei der Bestimmung haben Sie völlige Flexibilität, wie spezifisch oder weit gefasst jede Richtlinie definieret werden soll.

Hinweis: Richtlinien werden mithilfe von Gruppen definiert, die in Ihrem System konfiguriert sind. Wenn die Dropdown-Liste für einen bestimmten Parameter nicht die spezifische Gruppierung enthält, auf die Sie die Richtlinie anwenden möchten, können Sie eine neue Gruppe entsprechend Ihren Anforderungen erstellen. Siehe Gruppen.

Wenn Sie eine neue Richtlinie erstellen, wählen Sie zunächst die Kategorie und den Typ der Richtlinie aus, die Sie erstellen möchten. Der Assistent zum Erstellen von Richtlinien führt Sie durch den Einrichtungsvorgang. Jeder Richtlinientyp hat seinen eigenen Satz relevanter Parameter für Richtlinienbedingungen. Der Assistent zum Erstellen von Richtlinien zeigt Ihnen die relevanten Parameter für Richtlinienbedingungen für den ausgewählten Richtlinientyp an.

Für die Parameter „Quelle“, „Ziel“ und „Zeitplan“ können Sie festlegen, ob die angegebene Gruppe auf die Zulassungsliste oder die Sperrliste gesetzt werden soll.

- Wählen Sie In aus, um die angegebene Gruppe auf die Zulassungsliste zu setzen (d. h. sie in die Richtlinie aufzunehmen), ODER
- Wählen Sie Nicht in aus, um die angegebene Gruppe auf die Sperrliste zu setzen (d. h. sie aus der Richtlinie herauszulassen).

Für Asset-Gruppen- und Netzwerksegment-Parameter (d. h. „Quelle“, „Ziel“ und „Betroffene Assets“) können Sie logische Operatoren (Und/Oder) verwenden, um die Richtlinie auf verschiedene Kombinationen oder Teilmengen Ihrer vordefinierten Gruppen anzuwenden. Wenn Sie beispielsweise möchten, dass eine Richtlinie auf jedes Gerät angewendet wird, das entweder ein ICS-Gerät oder ein ICS-Server ist, wählen Sie ICS-Geräte oder ICS-Server aus. Wenn eine

Richtlinie nur für Controller gelten soll, die sich in Werk A befinden, wählen Sie „Controller“ und „Geräte Werk A“ aus.

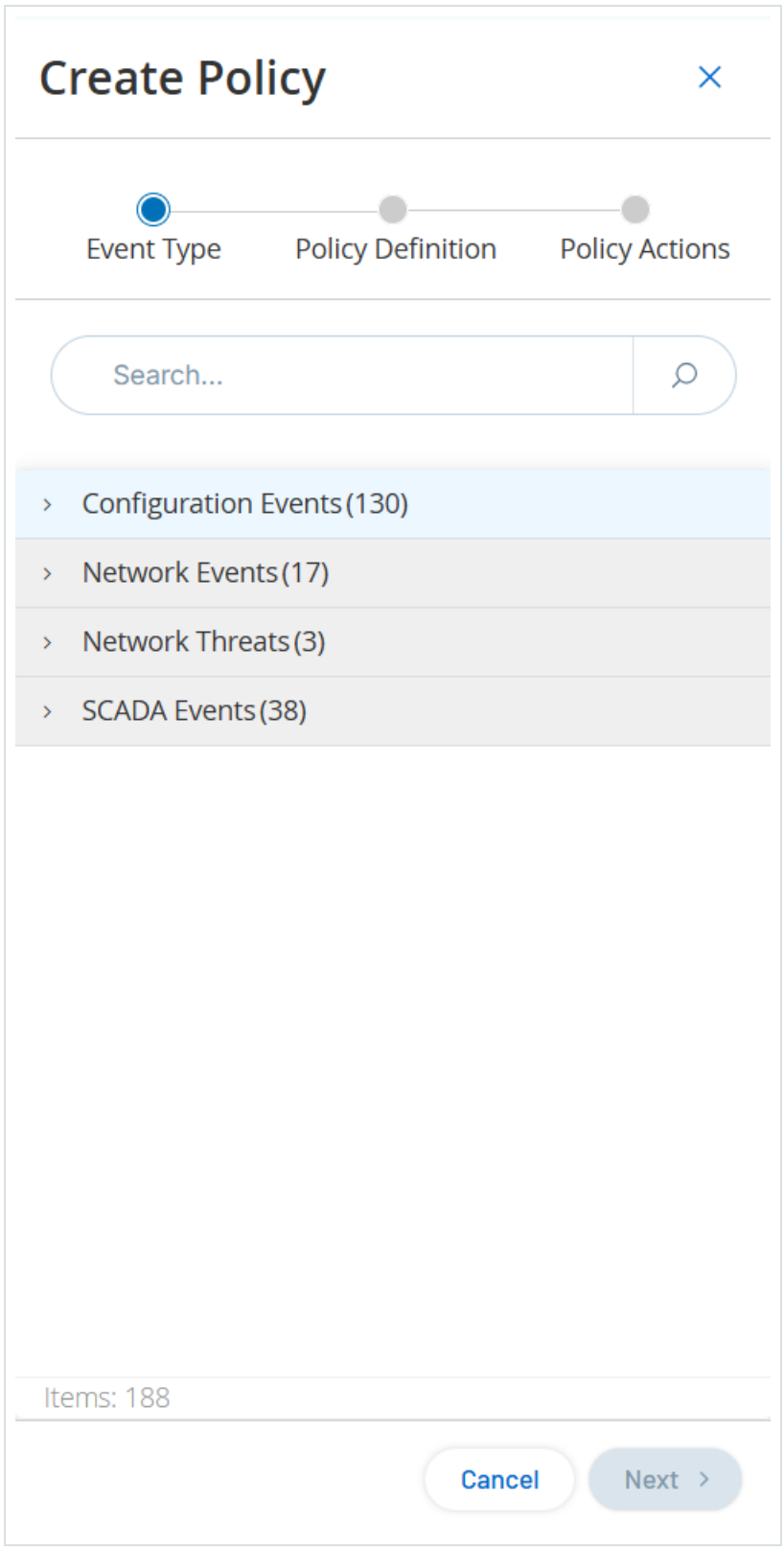
Wenn Sie eine neue Richtlinie mit ähnlichen Parametern wie eine vorhandene Richtlinie erstellen möchten, können Sie die ursprüngliche Richtlinie duplizieren und die erforderlichen Änderungen vornehmen, siehe Abschnitt Richtlinien erstellen.

> Hinweis: Wenn Sie nach dem Erstellen einer Richtlinie feststellen, dass die Richtlinie Ereignisse für Situationen generiert, die keine Aufmerksamkeit erfordern, können Sie bestimmte Bedingungen aus der Richtlinie ausschließen, siehe Ereignisse.

So erstellen Sie eine neue Richtlinie:

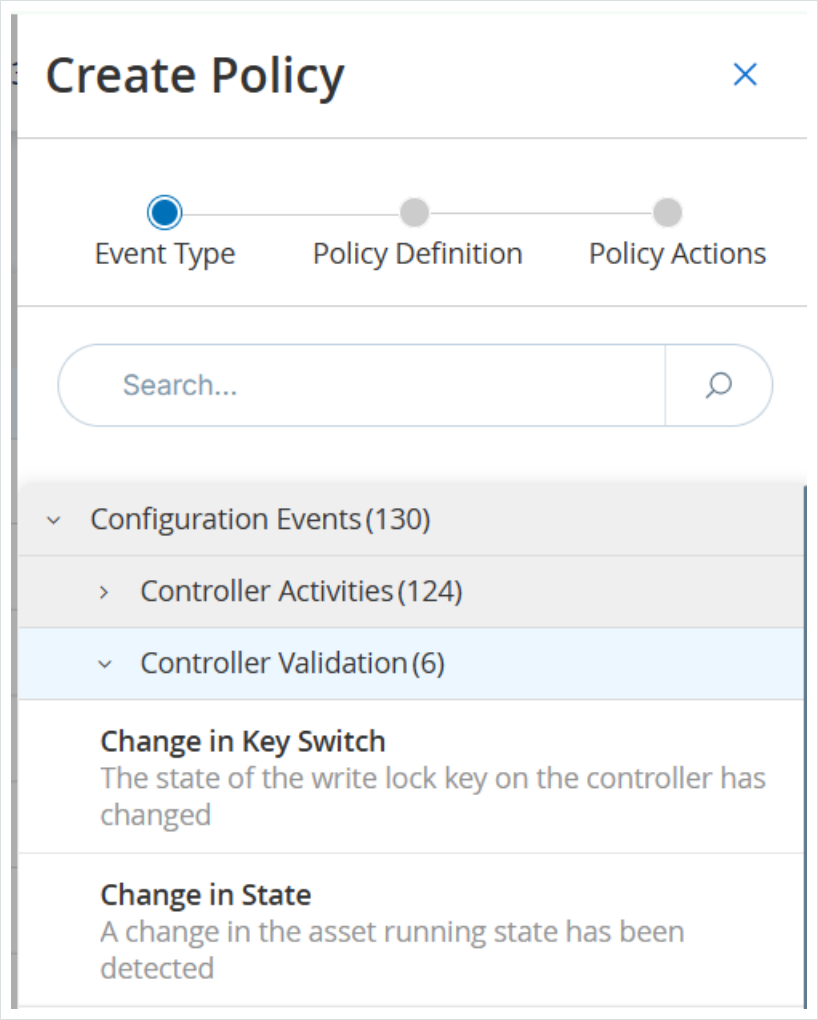
1. Klicken Sie im Bildschirm Richtlinien auf Richtlinie erstellen.

   Der Assistent Richtlinie erstellen wird geöffnet.

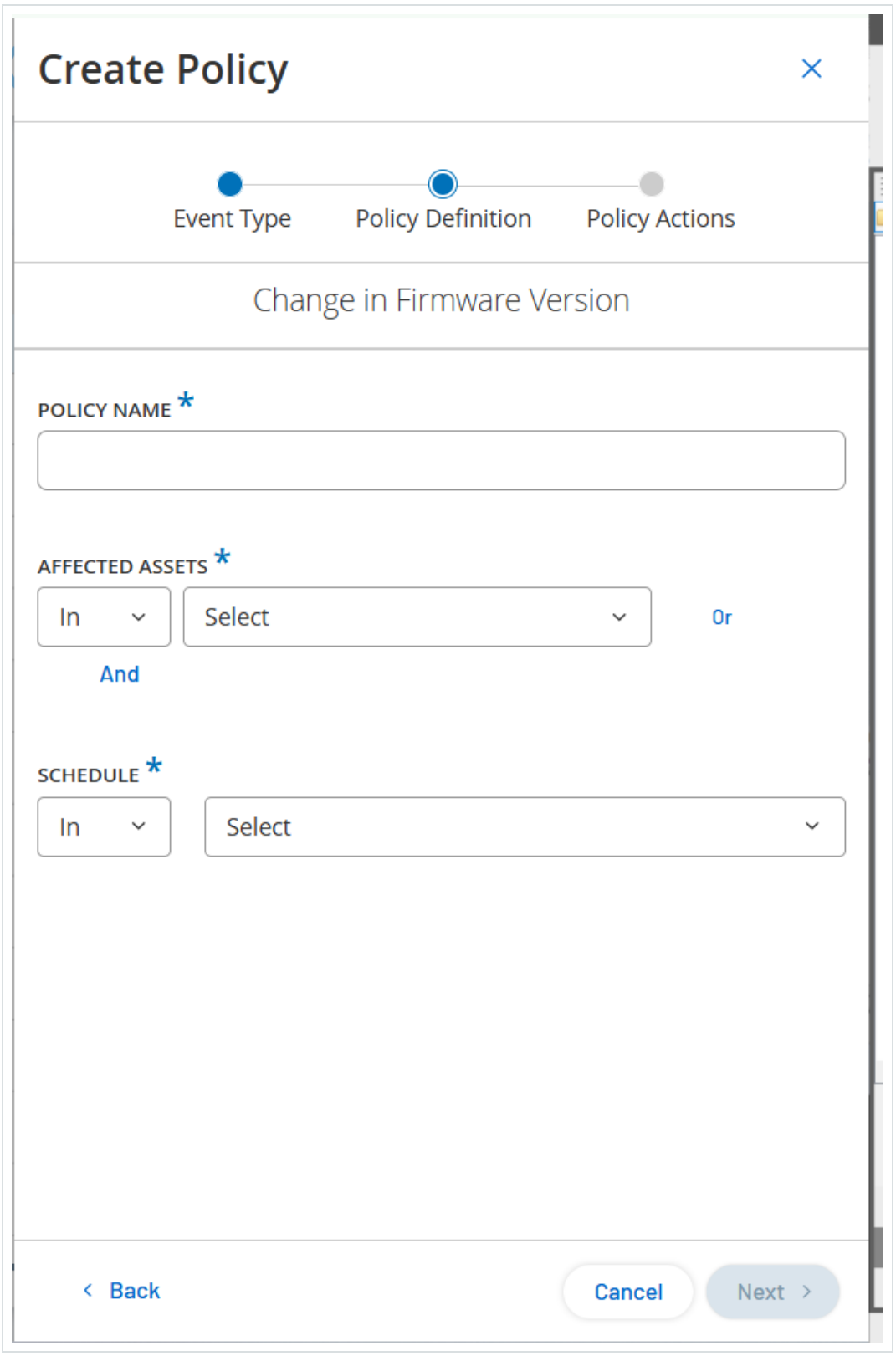

Create Policy
Event Type
Policy Definition
Policy Actions
Search...
Configuration Events (130)
Network Events (17)
Network Threats (3)
SCADA Events (38)
Items: 188
Cancel
Next

2. Klicken Sie auf eine Richtlinienkategorie, um die Unterkategorien und/oder Richtlinientypen anzuzeigen.

   Eine Liste aller Unterkategorien und/oder Typen, die in dieser Kategorie enthalten sind, wird angezeigt.




3. Wählen Sie einen Richtlinientyp aus.


Create Policy
Event Type
Policy Definition
Policy Actions
Change in Firmware Version
POLICY NAME *
AFFECTED ASSETS *
In
Select
Or
And
SCHEDULE *
In
Select
Back
Cancel
Next

4. Klicken Sie auf Weiter.

   Eine Reihe von Parametern zum Definieren der Richtlinie werden angezeigt. Alle relevanten Richtlinienbedingungen für den ausgewählten Richtlinientyp sind darin enthalten.

5. Geben Sie im Feld Richtlinienname einen Namen für diese Richtlinie ein.

   > Hinweis: Wählen Sie einen Namen aus, der die spezifische Art des Ereignistyps beschreibt, den die Richtlinie erkennen soll.

6. Führen Sie für jeden Parameter die folgenden Schritte aus:

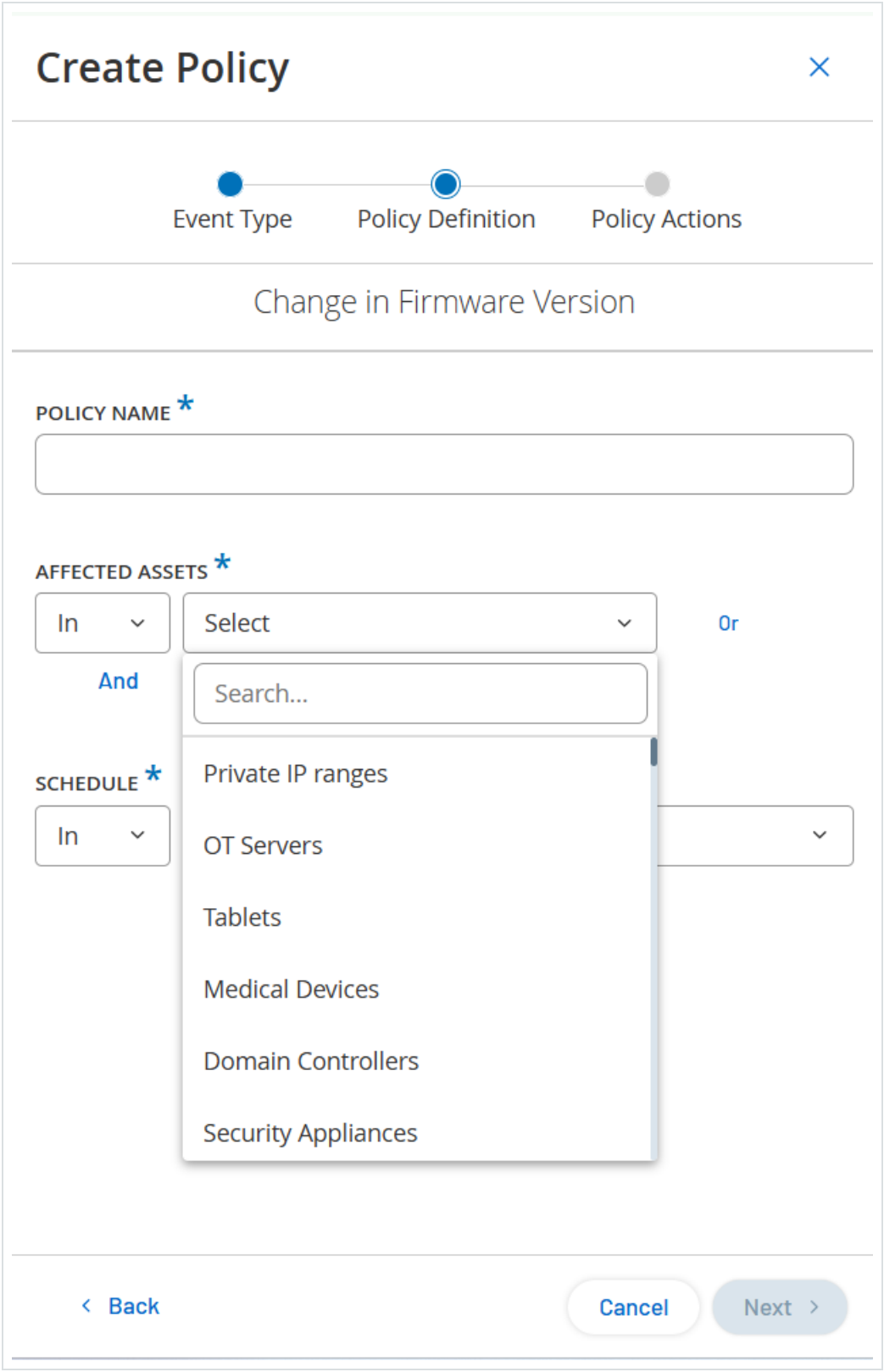
   > Achtung: Für IDS-Ereignisse (Intrusion Detection System, Angriffserkennungssystem) können die Asset-Gruppen Quelle und Ziel nicht bearbeitet werden.

   a. Wählen Sie gegebenenfalls In (Standard) aus, um das ausgewählte Element auf die Zulassungsliste zu setzen, oder Nicht in, um das ausgewählte Element auf die Sperrliste zu setzen.

   b. Klicken Sie auf Auswählen.

      Eine Dropdown-Liste relevanter Elemente (z. B. Asset-Gruppe, Netzwerksegment, Port-Gruppe, Planungsgruppe usw.) wird angezeigt.

      > Hinweis: Die verfügbare Auswahl umfasst alle Asset-Gruppen mit Ausnahme dynamischer Asset-Gruppen, deren Regelsatz eine der folgenden Asset-Eigenschaften enthält:
      > - Risikowert
      > - Backplane-Name
      > - Quellen
      > - Tags
      > - Hardware-Status
      > - Lebenszyklus-Status
      > - Nachfolgeprodukt


Create Policy
Event Type
Policy Definition
Policy Actions
Change in Firmware Version
POLICY NAME *
AFFECTED ASSETS *
In
Select
Or
And
Search...
Private IP ranges
OT Servers
Tablets
Medical Devices
Domain Controllers
Security Appliances
SCHEDULE *
In
Back
Cancel
Next

c. Wählen Sie das gewünschte Element aus.

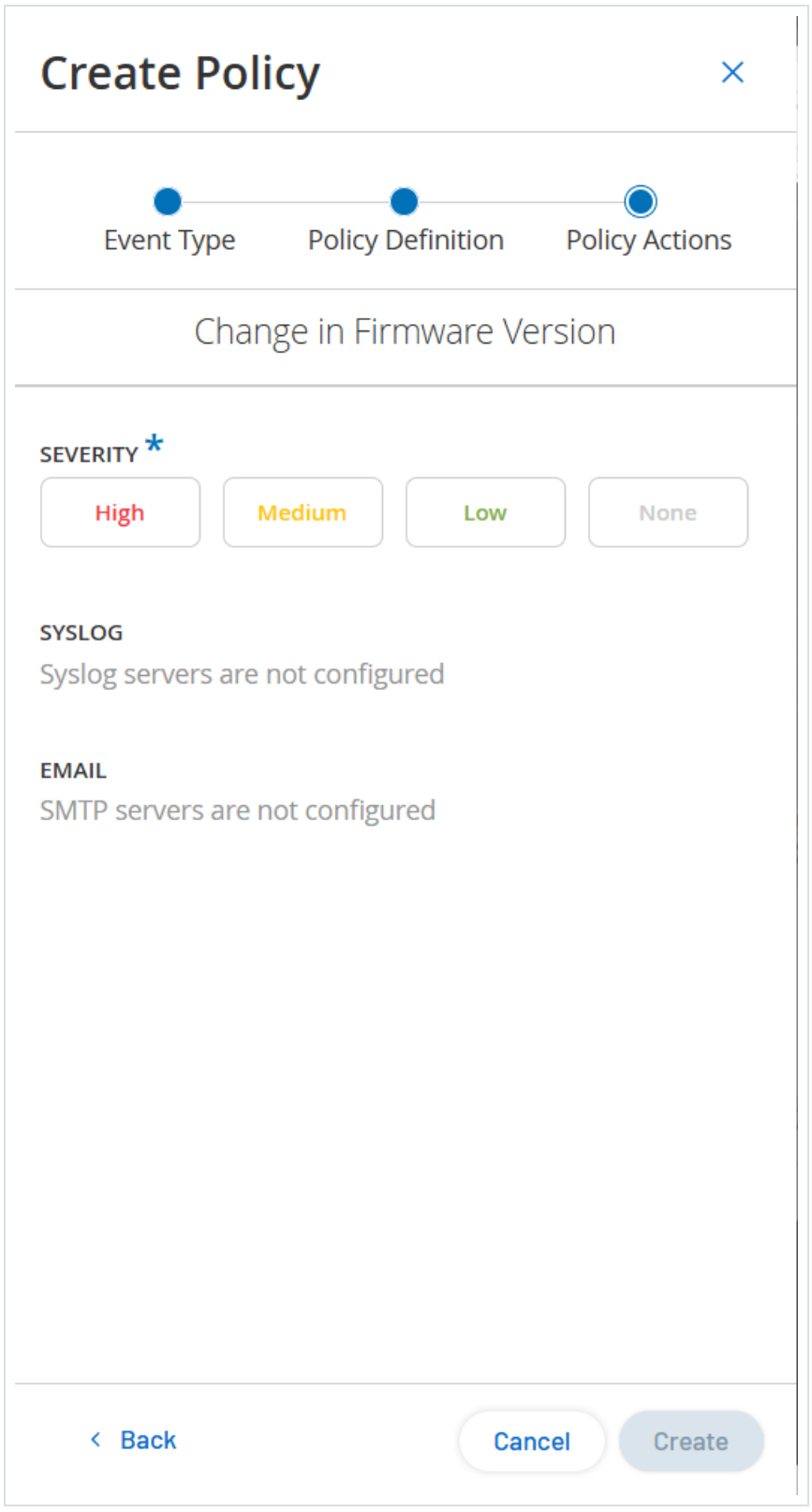
> Hinweis: Wenn die genaue Gruppierung, auf die Sie die Richtlinie anwenden möchten, nicht vorhanden ist, können Sie eine neue Gruppe entsprechend Ihren Anforderungen erstellen, siehe Gruppen.

d. Wenn Sie für Asset-Parameter (d. h. „Quelle“, „Ziel“ und „Betroffene Assets“) eine zusätzliche Asset-Gruppe/ein zusätzliches Netzwerksegment mit einer „Oder“-Bedingung hinzufügen möchten, klicken Sie auf die blaue Schaltfläche + Oder neben dem Feld und wählen Sie eine andere Asset-Gruppe/ein anderes Netzwerksegment aus.

e. Wenn Sie für Asset-Parameter (d. h. „Quelle“, „Ziel“ und „Betroffene Assets“) eine zusätzliche Asset-Gruppe/ein zusätzliches Netzwerksegment mit einer „Und“-Bedingung hinzufügen möchten, klicken Sie auf die blaue Schaltfläche + Und neben dem Feld und wählen Sie eine andere Asset-Gruppe/ein anderes Netzwerksegment aus.

7. Klicken Sie auf Weiter.

   Eine Reihe von Parametern für Richtlinienaktionen (d. h. die Aktionen, die vom System ausgeführt werden, wenn ein Richtlinientreffer auftritt) werden angezeigt.


Create Policy
Event Type
Policy Definition
Policy Actions
Change in Firmware Version
SEVERITY *
High
Medium
Low
None
SYSLOG
Syslog servers are not configured
EMAIL
SMTP servers are not configured
Back
Cancel
Create

8. Klicken Sie im Abschnitt Schweregrad auf den gewünschten Schweregrad für diese Richtlinie.
9. Wenn Sie Ereignisprotokolle an einen oder mehrere Syslog-Server senden möchten, aktivieren Sie im Abschnitt Syslog das Kontrollkästchen neben jedem Server, an den Sie die Ereignisprotokolle senden möchten.

   > Hinweis: Informationen zum Hinzufügen eines Syslog-Servers finden Sie unter Syslog-Server.

10. Wenn Sie E-Mail-Benachrichtigungen über Ereignisse senden möchten, wählen Sie im Feld „E-Mail-Gruppe“ in der Dropdown-Liste die zu benachrichtigende E-Mail-Gruppe aus.

    > Hinweis: Informationen zum Hinzufügen eines SMTP-Servers finden Sie unter SMTP-Server.

11. Im Abschnitt Zusätzliche Aktionen, wo die angegebene Aktion relevant ist:
    - Wenn Sie die Richtlinie nach dem ersten Richtlinientreffer deaktivieren möchten, aktivieren Sie das Kontrollkästchen Richtlinie nach erstem Treffer deaktivieren. (Diese Aktion ist für einige Typen von Netzwerkereignisrichtlinien und einige Typen von SCADA-Ereignisrichtlinien relevant.)
    - Wenn Sie jedes Mal einen automatischen Snapshot des betroffenen Assets initiieren möchten, wenn ein Richtlinientreffer erkannt wird, aktivieren Sie das Kontrollkästchen Snapshot nach Richtlinientreffer erstellen. (Diese Aktion ist für einige Typen von Richtlinien für Konfigurationsereignisse relevant.)
12. Klicken Sie auf Erstellen. Die neue Richtlinie wird erstellt und automatisch aktiviert. Die Richtlinie wird in der Liste im Bildschirm „Richtlinien“ angezeigt.

### Richtlinien für nicht autorisierte Schreibvorgänge erstellen

Dieser Richtlinientyp erkennt nicht autorisierte Schreibvorgänge für Controller-Tags. Die Richtliniendefinition umfasst die Angabe der relevanten Tag-Gruppen und des Schreibvorgangstyps, der einen Richtlinientreffer generiert.

So legen Sie die Richtliniendefinition für eine Richtlinie für nicht autorisierte Schreibvorgänge fest:

1. Erstellen Sie eine neue Richtlinie für nicht autorisierte Schreibvorgänge, wie unter Richtlinien erstellen beschrieben.
2. Wählen Sie im Abschnitt „Richtliniendefinition“ im Feld Tag-Gruppe die Tag-Gruppe aus, für die diese Richtlinie gilt.
3. Wählen Sie im Abschnitt Tag-Wert die gewünschte Option aus, indem Sie auf das Optionsfeld klicken und die erforderlichen Felder ausfüllen. Verfügbare Optionen:
    - Beliebiger Wert – Wählen Sie diese Option aus, um Änderungen am Tag-Wert zu erkennen.
    - Abweichend von Wert – Wählen Sie diese Option aus, um einen anderen als den angegebenen Wert zu erkennen. Geben Sie den angegebenen Wert in das Feld neben dieser Auswahl ein.
    - Außerhalb des zulässigen Bereichs – Wählen Sie diese Option aus, um Werte außerhalb des angegebenen Bereichs zu erkennen. Geben Sie die Unter- und Obergrenze des zulässigen Bereichs in die entsprechenden Felder neben dieser Auswahl ein.

      > Hinweis: Die Optionen „Abweichend von Wert“ und „Außerhalb des zulässigen Bereichs“ sind nur für Standard-Tag-Typen (z. B. Ganzzahl, Boolesch usw.) verfügbar, nicht jedoch für benutzerdefinierte Tags oder Zeichenfolgen.
4. Führen Sie die Verfahren zur Erstellung von Richtlinien wie unter Richtlinien erstellen beschrieben durch.

## Andere Aktionen zu Richtlinien

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager

### Richtlinien bearbeiten

Sie können die Konfiguration sowohl vordefinierter als auch benutzerdefinierter Richtlinien bearbeiten. Für die meisten Richtlinien können Sie sowohl die Parameter für die Richtliniendefinition (Richtlinienbedingungen) als auch die Parameter für Richtlinienaktionen anpassen. Für Intrusion Detection-Richtlinien können Sie nur die Parameter für die Richtlinienaktionen anpassen.

Außerdem können Sie die Parameter für Richtlinienaktionen für mehrere Richtlinien in einer Massenaktion bearbeiten.

### So bearbeiten Sie eine Richtlinie:

1. Aktivieren Sie im Fenster Richtlinien das Kontrollkästchen neben der erforderlichen Richtlinie.
2. Wählen Sie im Dropdown-Feld Aktionen die Option Bearbeiten aus.
3. Das Fenster Richtlinie bearbeiten wird mit der aktuellen Konfiguration angezeigt.
4. Passen Sie die Parameter der **Richtliniendefinition** wie erforderlich an.

   > Hinweis: Für IDS-Ereignisse (Intrusion Detection System, Angriffserkennungssystem) können die Asset-Gruppen Quelle und Ziel nicht bearbeitet werden.

5. Klicken Sie auf Weiter.
6. Passen Sie die Parameter der Richtlinienaktionen wie erforderlich an.
7. Klicken Sie auf Speichern.

   OT Security speichert die Richtlinie mit der neuen Konfiguration.

### So bearbeiten Sie mehrere Richtlinien (Massenprozess):

1. Aktivieren Sie im Fenster Richtlinien das Kontrollkästchen neben zwei oder mehr Richtlinien.
2. Wählen Sie im Dropdown-Feld Massenaktionen die Option Bearbeiten aus.
3. Das Fenster Massenbearbeitung wird mit den für die Massenbearbeitung verfügbaren Richtlinienaktionen angezeigt.

4. Aktivieren Sie das Kontrollkästchen neben jedem Parameter, den Sie bearbeiten möchten: Schweregrad, Syslog, E-Mail-Gruppe.
5. Stellen Sie jeden Parameter wie erforderlich ein.

   > Hinweis: Durch die im Fenster Massenbearbeitung eingegebenen Informationen werden alle aktuellen Inhalte für die ausgewählten Richtlinien überschrieben. Wenn Sie das Kontrollkästchen neben einem Parameter aktivieren, aber keine Auswahl treffen, werden die aktuellen Werte für diesen Parameter gelöscht.

6. Klicken Sie auf Speichern.

   OT Security speichert die Richtlinien mit der neuen Konfiguration.

### Duplizierte Richtlinien

Sie können eine neue Richtlinie erstellen, die einer bestehenden Richtlinie ähnlich ist, indem Sie die ursprüngliche Richtlinie duplizieren und die gewünschten Anpassungen vornehmen. Sie können sowohl vordefinierte als auch benutzerdefinierte Richtlinien duplizieren (mit Ausnahme von Intrusion Detection-Richtlinien).

### So duplizieren Sie eine Richtlinie:

1. Aktivieren Sie im Fenster Richtlinien das Kontrollkästchen neben der erforderlichen Richtlinie.
2. Wählen Sie im Dropdown-Feld Aktionen die Option Duplizieren aus.
3. Der Bildschirm Richtlinie duplizieren wird mit der aktuellen Konfiguration angezeigt und der Name ist standardmäßig auf „*Kopie von <Name der ursprünglichen Richtlinie>*“ festgelegt.
4. Passen Sie die Parameter der Richtliniendefinition wie erforderlich an.
5. Klicken Sie auf Weiter.
6. Passen Sie die Parameter der Richtlinienaktionen wie erforderlich an.

7. Klicken Sie auf Speichern.

   OT Security speichert die Richtlinie mit der neuen Konfiguration.

## Richtlinien löschen

Sie können eine Richtlinie aus dem System löschen. Sie können sowohl vordefinierte als auch benutzerdefinierte Richtlinien löschen (mit Ausnahme von Intrusion Detection-Richtlinien, die nicht gelöscht werden können).

Sie können auch mehrere Richtlinien in einer Massenaktion löschen.

> Hinweis: Nachdem Sie eine Richtlinie aus dem System gelöscht haben, können Sie sie nicht erneut aktivieren. Eine Alternative besteht darin, den Status auf AUS umzuschalten, um sie vorübergehend zu deaktivieren. Dann können Sie sie später wieder aktivieren.

### So löschen Sie eine Richtlinie:

1. Aktivieren Sie im Fenster Richtlinien das Kontrollkästchen neben der erforderlichen Richtlinie.
2. Wählen Sie im Dropdown-Feld Aktionen die Option Löschen aus.

   Daraufhin wird ein Bestätigungsfenster angezeigt.
3. Klicken Sie auf Löschen.

   OT Security löscht die Richtlinie aus dem System.

### So löschen Sie mehrere Richtlinien (Massenaktion):

1. Aktivieren Sie im Fenster Richtlinien das Kontrollkästchen neben jeder der erforderlichen Richtlinien.
2. Wählen Sie im Dropdown-Feld Massenaktionen die Option Löschen aus.

   Daraufhin wird ein Bestätigungsfenster angezeigt.

3. Klicken Sie auf Löschen.

   OT Security löscht die Richtlinien aus dem System.

### Richtlinienausschlüsse löschen

Wenn Sie einen Ausschluss löschen möchten, der auf eine bestimmte Richtlinie angewendet wurde, ist dies im Bildschirm Richtlinien möglich.

So löschen Sie einen Richtlinienausschluss:

1. Wählen Sie im Fenster Richtlinien die erforderliche Richtlinie aus.
2. Wählen Sie im Dropdown-Feld Aktionen die Option Anzeigen aus.

   > Hinweis: Alternativ können Sie das Menü „Aktionen“ aufrufen, indem Sie mit der rechten Maustaste auf die entsprechende Richtlinie klicken.

3. Klicken Sie auf die Registerkarte Ausschlüsse.

   Eine Liste der Ausschlüsse wird angezeigt.

4. Wählen Sie den Richtlinienausschluss aus, den Sie löschen möchten.
5. Klicken Sie auf Löschen.

   Daraufhin wird ein Bestätigungsfenster angezeigt.

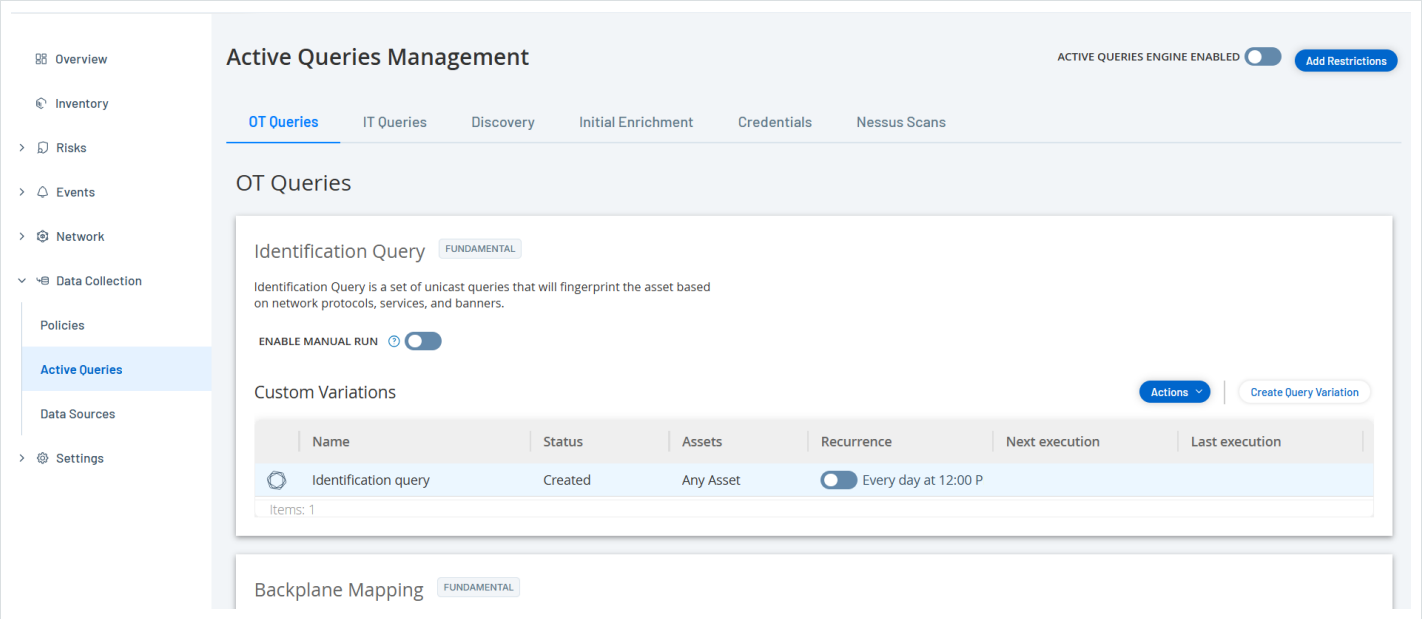
6. Klicken Sie im Bestätigungsfenster auf Löschen.

   OT Security löscht der Ausschluss aus dem System.

## Aktive Abfragen verwalten

Auf der Seite Verwaltung aktiver Abfragen können Sie aktive Abfragen konfigurieren und aktivieren. Tenable empfiehlt, die gesamte Abfragefunktionalität im Rahmen der Ersteinrichtung zu aktivieren.

Sie können die einzelnen Abfragefunktionen jederzeit aktivieren/deaktivieren. Außerdem können Sie die Einstellungen anpassen, die steuern, wann und wie die Abfragen ausgeführt werden.




Zusätzlich zu den regelmäßig ausgeführten automatischen Abfragen gibt es auch Abfragen, die bei Bedarf initiiert werden können. Aktivieren Sie hierzu den Umschalter Manuelle Ausführung aktivieren in der Abfragekarte. Wenn Sie die Option Manuelle Ausführung aktivieren deaktivieren, werden Sie von OT Security aufgefordert, die Option zu überschreiben, wenn Sie Erneute Synchronisierung durchführen auf der Seite Asset-Details auswählen (Inventar > Alle Assets).

Weitere Informationen zur Abfragetechnologie finden Sie unter OT Security-Technologien.

Hinweis: OT Security kann Assets möglicherweise nicht identifizieren, wenn Sie Abfragen deaktivieren. OT Security verfolgt Geräte durch passives Monitoring sowie aktive Abfragen.

Tipp: Damit aktive Abfragen funktionieren, klicken Sie auf den Umschalter Engine für aktive Abfragen ist aktiviert. Nachdem Sie die aktiven Abfragen aktiviert haben, zeigt OT Security das Symbol in der Kopfzeile an, um anzuzeigen, dass die Engine für aktive Abfragen ausgeführt wird. Um aktive Abfragen auszuführen, müssen Sie trotzdem jede einzelne Abfrage separat aktivieren.

Auf der Seite Verwaltung aktiver Abfragen werden Abfragen in die folgenden Typen eingeordnet. Für jeden Abfragetyp gibt es eine separate Abfrageregisterkarte mit einer entsprechenden Liste von Abfragen.

- OT-Abfragen – Diese Abfragen wurden entwickelt, um Controller und eingebettete Geräte auf sichere Weise unter Verwendung ihrer proprietären Protokolle nach weiteren Informationen abzufragen. OT Security führt schreibgeschützte Abfragen durch, um Geräteinformationen zu sammeln, wie z. B. den SPS-Ausführungsstatus und andere an die Backplane angeschlossene Module. Es fragt Geräte ab, die auf proprietäre Protokollen lauschen, die von OT Security unterstützt werden. Zu den Abfragetypen gehören Identifizierungsabfrage, Backplane-Zuordnung, Detailabfrage, Statusabfrage und Code-Snapshots.
- IT-Abfragen – Diese Abfragen rufen zusätzliche Datenpunkte von überwachten IT-Assets ab, die von OT Security beobachtet werden. Mit Ausnahme von NetBIOS erfordern diese IT-Abfragen Zugangsdaten.
    - Die NetBIOS-Abfrage versucht, alle Geräte zu erkennen, die im Broadcast-Bereich von OT Security Sensor oder OT Security selbst auf NetBIOS lauschen. Dieser Abfragetyp ist geeignet, um Windows-Geräte in der Nähe zu identifizieren.
    - Die SNMP-Abfrage verwendet SNMP V2- oder SNMP V3-Zugangsdaten, um Identifizierungsdetails von der Netzwerkinfrastruktur oder vernetzten Geräten anzufordern, die SNMP unterstützen. OT Security fragt die SNMP-Systembeschreibung und andere Parameter ab, um Asset-Kontext bereitzustellen und Fingerprinting zu unterstützen.

      Darüber hinaus bietet OT Security die folgenden Optionen zur Nutzung Ihrer SNMP-Abfrage:

        - SNMP-Port-Status – Aktivieren Sie den Umschalter SNMP-Port-Status, um den Netzwerk-Port-Status der Assets zu erhalten, und aktivieren Sie den Umschalter

Nachbargeräte abrufen.

- Nachbargeräte abrufen – Wenn Sie diese Option aktivieren, erfasst OT Security die MAC- und IP-Adressen der Geräte in der Nähe über SNMP. Um diese Assets zu Ihrem Inventar hinzuzufügen, aktivieren Sie Einstellungen > Umgebungseinstellungen > Netzwerkdefinitionen > Neue Assets über SNMP ermitteln.

- Die WMI-Detailabfrage ruft eine Vielzahl wichtiger Datenpunkte aus Windows-basierten Systemen ab. Dazu muss das System, das von OT Security abgefragt wird, über ein Windows-Konto (lokal oder Domäne) mit ausreichenden Berechtigungen verfügen, um den WMI-Dienst (Windows-Verwaltungsinstrumentation) abzufragen.

- WMI-USB-Statusabfragen ermitteln, ob Wechseldatenträger wie USB-Laufwerke oder tragbare Festplatten an das Windows-Gerät angeschlossen sind, z. B. eine Engineering-Workstation oder ein Engineering-Server. Diese Abfrage ist eng mit der Richtlinie Änderung der USB-Konfiguration auf Windows-Computern verbunden, da sie eine Voraussetzung für die ordnungsgemäße Funktion dieser Richtlinie ist.

- Der Nessus-Basisscan ruft Systemdetails wie IP-Adresse, FQDN, Betriebssysteme und offene Ports ab.

- Eine ARP-Abfrage (Abfrage über das Address Resolution Protocol) ruft die Hardwareadresse oder MAC-Adresse der Netzwerkschnittstelle für über IP verbundene Geräte in derselben Broadcast-Domäne ab.

- Erfassung – Dies sind Abfragen, die Live-Assets in dem von OT Security überwachten Netzwerk erkennen.

  - Asset-Erfassung – Verwendet das Internet Control Message Protocol (ICMP) oder Pings, um IP-Adressen zu erkennen, die live sind und antworten.

  - Automatische Erkennung von Subnetzen – Erkennt Subnetze durch Abfrage von Netzwerkgeräten über SNMP. Auf der Seite Inventar können Sie in der Spalte Subnetze

sehen, zu welchen Subnetzen die IP-Adressen der Assets gehören. Sie können Assets auch innerhalb eines bestimmten Subnetzes filtern.

- Aktive Asset-Verfolgung – Versucht in regelmäßigen Abständen, ein bekanntes, überwachtes Asset anzupingen, um sicherzustellen, dass es noch aktiv und verfügbar ist.
- Controller-Erfassung – Sendet eine Reihe von Multicast-Paketen an das Netzwerk, um Controller oder ICS-Geräte zu veranlassen, ihre Informationen direkt an OT Security zu senden.
- Ping-Abfrage – Sendet ICMP-Pings (Internet Control Message Protocol), um zu überprüfen, ob ein Asset erreichbar ist.
- DNS-Suche – Ruft die DNS-Serverdetails ab.
- Port-Zuordnung – Ruft Details zu offenen Ports überwachter Assets ab.

- Erste Anreicherung – Hierbei werden automatische OT Security-Abfragen auf der Grundlage bestimmter Kriterien oder Bedingungen durchgeführt. Auf Asset-Anreicherung basierende Abfragen finden immer dann statt, wenn Tenable ein Gerät erstmals passiv oder aktiv beobachtet. Bei aktivierter Asset-Anreicherung erstellt OT Security Fingerabdrücke und identifiziert das Gerät, sobald es im Netzwerk sichtbar wird.
- Nessus-Scans – Der Tenable Nessus-Plugin-Scan startet einen erweiterten Nessus-Scan, der eine benutzerdefinierte Liste von Plugins für die Assets ausführt, die in der Liste der CIDRs und IP-Adressen angegeben sind. Weitere Informationen finden Sie unter Nessus-Plugin-Scans erstellen.

## Benutzerdefinierte Abfragen erstellen

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

Für jeden Abfragetyp gibt es eine Systemstandard-Variation, die Sie regelmäßig oder bei Bedarf ausführen können. Sie können außerdem zusätzliche Variationen jeder Abfrage mit einer eigenen Konfiguration für verschiedene Projekte und Funktionen erstellen.

Sie können beispielsweise benutzerdefinierte Abfragen für die folgenden Szenarien konfigurieren:

- Unterschiedliche Wartungszeiten für verschiedene Teile der Anlage
- Unterschiedliche Projekte und Kritikalität für verschiedene Assets
- Unterschiedliche Abfragen für OT-Funktionen und IT-Funktionen

### So erstellen Sie eine Abfragevariation:

1. Gehen Sie zu Datenerfassung > Aktive Abfragen.

   Die Seite Verwaltung aktiver Abfragen wird angezeigt.

2. Klicken Sie auf die Registerkarte des gewünschten Abfragetyps.

   OT Security zeigt den Abfragetyp mit der Liste der verfügbaren Abfragen an.

3. Klicken Sie im Abschnitt des gewünschten Abfragetyps auf Abfragevariation erstellen.

   Der Bereich Abfragevariation erstellen wird angezeigt.

4. Geben Sie im Feld Name einen Namen für die Abfrage ein.

5. Wählen Sie im Dropdown-Feld Assets eine Asset-Gruppe aus.

   > Hinweis: Sie können auch das Suchfeld verwenden, um nach einer bestimmten Gruppe zu suchen.

6. Um die Abfrage zu wiederholen, klicken Sie auf den Umschalter Wiederkehrende Ausführung.

   OT Security aktiviert den Abschnitt Wiederholungen alle.

7. Geben Sie eine Zahl ein und wählen Sie Tage oder Wochen im Dropdown-Feld aus. Für bestimmte Abfragen können Sie auch Minuten und Stunden festlegen.

   Wenn Sie Wochen auswählen, geben Sie die Wochentage an, an denen die Abfragen ausgeführt werden sollen.

8. Legen Sie im Feld Um die Tageszeit fest, zu der die Abfragen ausgeführt werden sollen (im Format HH:MM:SS). Klicken Sie hierzu auf das Uhrsymbol und wählen Sie die Uhrzeit aus oder geben Sie die Uhrzeit manuell ein.

9. (Nur für Asset-Erfassung) Geben Sie im Feld IP-Bereiche die IP-Adressen der Assets ein.

10. (Nur für Erfassungsabfragen) Wählen Sie im Dropdown-Feld Anzahl an Assets, die gleichzeitig abgefragt werden die Anzahl der Assets aus (10, 20 oder 30).

11. (Nur für Erfassungsabfragen) Wählen Sie im Dropdown-Feld Zeit zwischen Erfassungsabfragen die Zeit zwischen den Erfassungsabfragen aus (1 bis 3 Sekunden).

12. (Nur für duplizierte Netzwerke) Wählen Sie im Feld Relevante Sensoren die zugehörigen Sensoren aus.

13. Klicken Sie auf Speichern.

    OT Security fügt die Abfrage zur Tabelle Benutzerdefinierte Variationen hinzu.

    Siehe Abfragevariation ausführen.

## Einschränkungen hinzufügen

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

Sie können die Ausführung von Abfragen für bestimmte Asset-Gruppen blockieren, wie z. B. IP-Bereiche, OT-Server, Tablets, medizinische Geräte und Domänencontroller. Sie können auch Einschränkungen auf bestimmte Protokolle (Clients) anwenden.

Hinweis: Einschränkungen gelten nicht für Abfragen vom Typ Erfassung (ICMP) und Prüfung offener Ports (in Asset-Anreicherung).

So fügen Sie Einschränkungen hinzu:

1. Gehen Sie zu Datenerfassung > Aktive Abfragen.

   Die Seite Verwaltung aktiver Abfragen wird angezeigt.

2. Klicken Sie in der oberen rechten Ecke auf Einschränkungen hinzufügen.

   Das Fenster Einschränkungen hinzufügen wird angezeigt.

3. Wählen Sie im Dropdown-Feld Blockierte Assets die Asset-Gruppen aus, die blockiert werden sollen.

   Hinweis: Sie können das Suchfeld verwenden, um nach bestimmten Asset-Gruppen zu suchen.

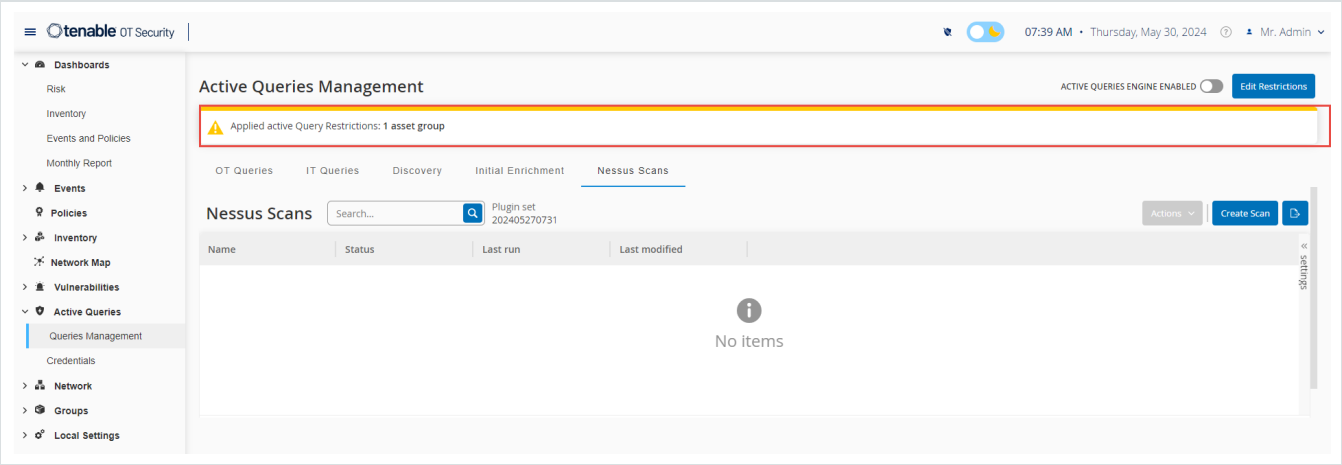
4. Wählen Sie im Dropdown-Feld Eingeschränkte Clients die gewünschten Clients aus.

5. Wählen Sie im Dropdown-Feld Ausfallzeitraum die Dauer aus, für die Sie die aktiven Abfragen sperren möchten. Die verfügbaren Optionen basieren auf Planungsgruppen. Standardoptionen: Keine, Arbeitszeiten (Working Hours).

6. Klicken Sie auf Speichern.

   OT Security wendet die Einschränkungen für die spezifischen Clients und Asset-Gruppen an. Oben auf jeder Registerkarte wird ein Banner angezeigt, das darauf hinweist, dass

Einschränkungen bestehen.




## Abfragevariation bearbeiten

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

So bearbeiten Sie die Details einer Abfrage:

1. Gehen Sie zu Datenerfassung > Aktive Abfragen.

   Das Fenster Verwaltung aktiver Abfragen wird angezeigt.

2. Wählen Sie in der Liste der Abfragen die zu bearbeitende Abfrage aus und führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die Abfrage und wählen Sie Bearbeiten aus.
   - Wählen Sie die Abfrage aus und klicken Sie auf Aktionen > Bearbeiten.

   Der Bereich Abfrage bearbeiten wird angezeigt.

3. Ändern Sie die Abfrage nach Bedarf.

4. Klicken Sie auf Speichern.

   OT Security speichert die Änderungen an der Abfragevariation.

## Abfragevariation duplizieren

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

1. Gehen Sie zu Datenerfassung > Aktive Abfragen.

   Die Seite Abfrageverwaltung wird angezeigt.

2. Wählen Sie in der Liste der Abfragen die zu kopierende Abfrage aus und führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die Abfrage und wählen Sie Duplizieren aus.
   - Wählen Sie die Abfrage aus und klicken Sie auf Aktionen > Duplizieren.

   Der Bereich Abfrage duplizieren mit Details der Abfrage wird angezeigt.

3. Benennen Sie die Abfrage um und ändern Sie die Details nach Bedarf.

4. Klicken Sie auf Speichern.

   OT Security speichert die Abfrage und zeigt sie in der Tabelle „Abfragen“ an.

## Abfragevariation ausführen

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

Sie können aktive Abfragen bei Bedarf ausführen.

So führen Sie eine Abfrage aus:

1. Gehen Sie zu Datenerfassung > Aktive Abfragen.

   Die Seite Abfrageverwaltung wird angezeigt.

2. Wählen Sie in der Liste der Abfragen die Abfrage aus, die Sie ausführen möchten, und führen Sie einen der folgenden Schritte aus:

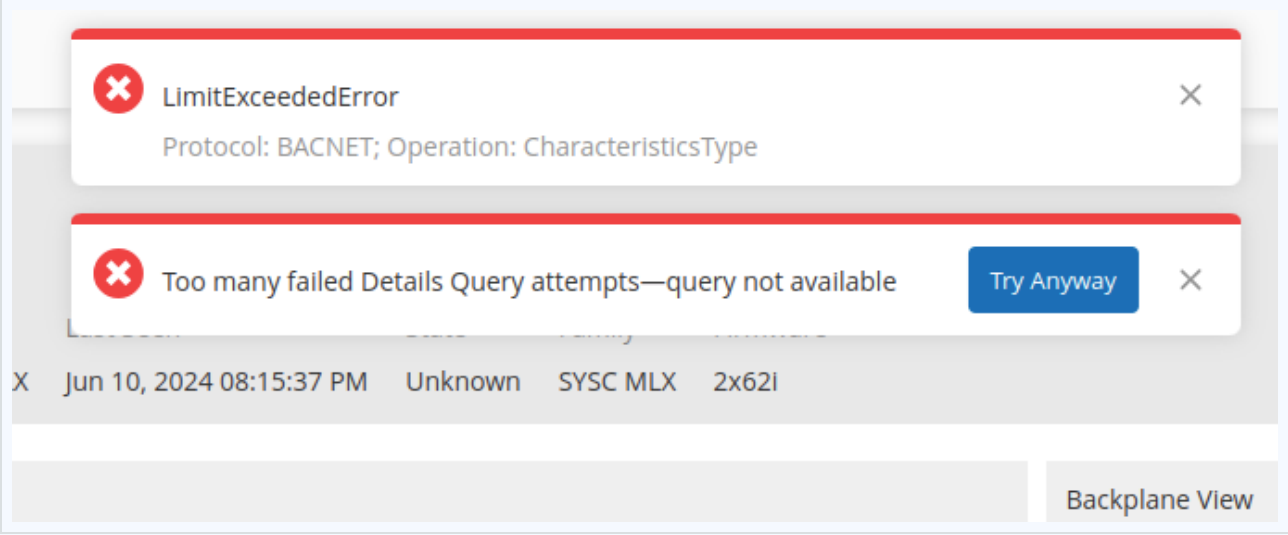
   - Klicken Sie mit der rechten Maustaste auf die Abfrage und wählen Sie Jetzt ausführen aus.
   - Klicken Sie im Menü Aktionen auf Jetzt ausführen.

   In einer Meldung werden Sie aufgefordert, die Ausführung der Abfrage zu bestätigen.

3. Klicken Sie auf OK.

   OT Security führt die ausgewählte Abfrage aus.

   Hinweis: Sie können die Option Trotzdem versuchen verwenden, um mit aktiven Abfragen für Geräten oder Netzwerke fortzufahren, und so das Limit für die Anzahl der aktiven Abfrageversuche überschreiben.




## Abfrageprotokoll herunterladen

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

Sie können das Protokoll der letzten Ausführung einer Abfragevariation herunterladen. Mithilfe des Protokolls können Sie Probleme mit Assets oder Protokollen, die in der aktiven Abfrage enthalten sind, beheben.

### So laden Sie das Protokoll der letzten Abfrage herunter:

1. Gehen Sie zu Datenerfassung > Aktive Abfragen.

   Das Fenster Verwaltung aktiver Abfragen wird angezeigt.

2. Wählen Sie in der Liste der Abfragen die Abfrage aus, deren Protokoll Sie herunterladen möchten, und führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die Abfrage und wählen Sie Protokoll der letzten Ausführung herunterladen aus.
   - Klicken Sie im Menü Aktionen auf Protokoll der letzten Ausführung herunterladen.

OT Security lädt das Protokoll der letzten aktiven Abfrage herunter.

## Typen von Erfassungsabfragen

OT Security verwendet die folgenden Abfragen zur Asset-Erfassung, um Daten über verschiedene Netzwerk- und Gerätetypen hinweg zu erfassen.

| Abfragetyp | Beschreibung |
|---|---|
| SnmpType (SNMP-Abfrage) | Standardisiert die Erfassung von Systemdaten aus verwalteten Netzwerkgeräten wie Switches und Routern. Diese Abfrage ruft Hardwaredetails, Schnittstellenstatus und grundlegende Systemkonfigurationen mithilfe von SNMP (Simple Network Management Protocol) ab. |

| | |
|---|---|
| ArpType (Layer 2 ARP-Broadcast) | Verwendet Layer 2 Address Resolution Protocol (ARP)-Broadcasts, um aktive Geräte im lokalen Netzwerksegment zu erkennen. Das ist wichtig, um Assets in der Nähe zu identifizieren, die möglicherweise nicht über Gateways kommunizieren. |
| IdentificationType (Identifizierungsabfrage) | Dient als primäres Fingerprinting-Tool, indem es die Core-Identität des Geräts abfragt. Mit dieser Abfrage werden Hersteller, Modell und Firmware-Version abgerufen, um das Baseline-Asset-Profil zu erstellen. |
| CharacteristicsType (Detailabfrage) | Verwendet proprietäre Industrieprotokolle, um Metadaten auf tiefer Ebene abzurufen. Diese Abfrage liefert detaillierte Informationen zu Hardware und Software, auf die standardmäßige Identifizierungsabfragen nicht zugreifen können. |
| BpScanType (Backplane-Scan) | Listet alle Module, Karten und Unterkomponenten auf, die sich auf einem physischen Chassis für modulare Hardware befinden. Mit dieser Abfrage wird die vollständige interne Architektur einer speicherprogrammierbaren Steuerung (SPS) oder eines Controllers bereitgestellt. |
| RunStatusType (Abfrage des Controller-Status) | Überwacht den Betriebsmodus von SPS, IEDs und Controllern. Modi sind beispielsweise RUN, STOP oder FAULT. Diese Abfrage ist wichtig, um festzustellen, ob ein Prozess aktiv ist oder ob ein Gerät in einen anfälligen Programmierstatus übergegangen ist. |
| NbstatQueryType (NetBIOS-Erfassung) | Fragt den NetBIOS-Namensdienst ab, um Windows-basierte Systeme und andere kompatible Geräte zu identifizieren. Verwenden Sie diese Abfrage, um Hostnamen und |

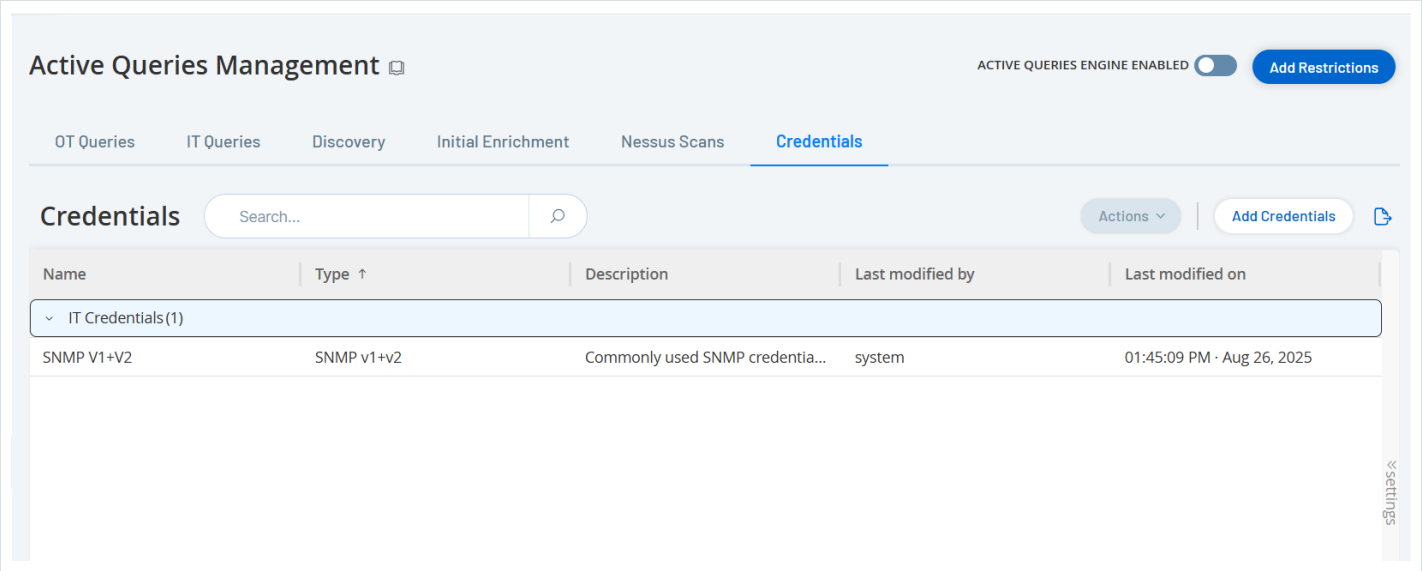
| | |
|---|---|
| | Arbeitsgruppeninformationen für Assets im lokalen Subnetz aufzulösen. |
| WmiType (erweiterte WMI-Abfrage) | Verwendet authentifizierte Windows-Verwaltungsinstrumentation (Windows Management Instrumentation, WMI), um umfassende Prüfungen von Windows-Endpunkten durchzuführen. Verwenden Sie diese Abfrage, um genaue Daten zu installierter Software, Betriebssystem-Patches, aktiven Benutzern und System-Hotfixes zu erfassen. |
| WmiUsbType (WMI-USB- oder HID-Abfrage) | Eine spezielle WMI-Anforderung zur Überwachung verbundener physischer Peripheriegeräte. Diese Abfrage erkennt und protokolliert Wechseldatenträger, z. B. USB-Speichersticks oder HID-Geräte (Human Interface Device). Diese Geräte sind gängige Vektoren für die Einschleusung von Malware in Air-Gapped-Umgebungen. |
| DnsType (DNS-Suche) | Verwendet konfigurierte DNS-Server, um eine IP-Adresse in ihren vollständig qualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) aufzulösen. Dadurch wird sichergestellt, dass Assets mit ihren lesbaren Netzwerknamen in der Verwaltungskonsole angezeigt werden. |

## Zugangsdaten

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

Verwenden Sie die Seite Zugangsdaten, um bei Bedarf die Zugangsdaten für das Gerät zu konfigurieren. Für die Kommunikation in ihren nativen Netzwerkprotokollen oder proprietären Protokollen benötigen Geräte keine Zugangsdaten. Für bestimmte Geräte, die von OT Security

unterstützt werden, sind jedoch möglicherweise Zugangsdaten erforderlich, um die Asset-Erfassung durchzuführen.




## Zugangsdaten hinzufügen

So fügen Sie Zugangsdaten hinzu:

1. Gehen Sie zu Datenerfassung > Aktive Abfragen.

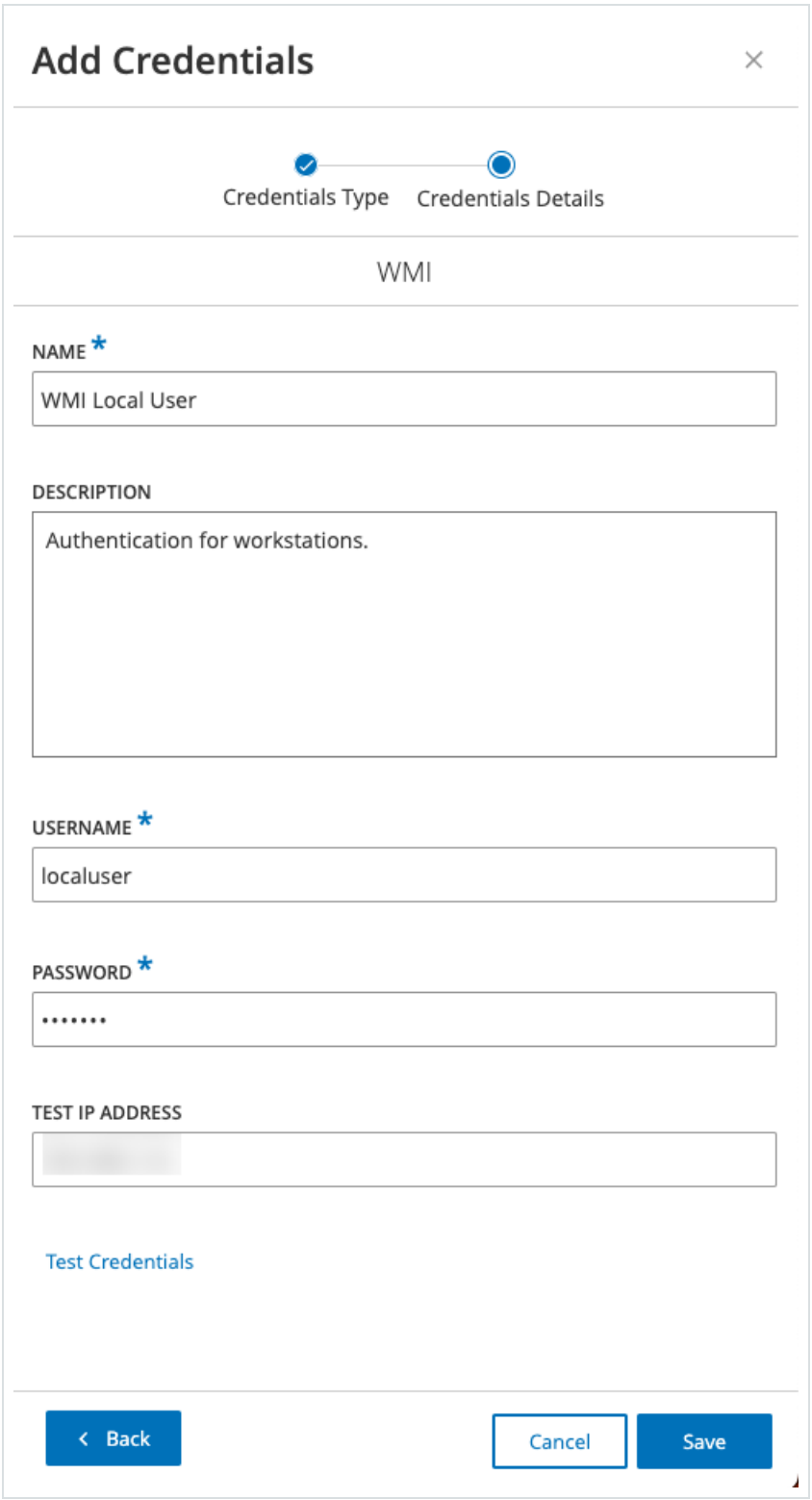
   Die Seite Verwaltung aktiver Abfragen wird angezeigt.

2. Klicken Sie auf die Registerkarte Zugangsdaten.

   Die Seite Zugangsdaten wird angezeigt.

3. Klicken Sie in der oberen rechten Ecke auf Zugangsdaten hinzufügen.

Der Bereich Zugangsdaten hinzufügen wird angezeigt.



4. Klicken Sie im Abschnitt Zugangsdatentyp auf den gewünschten Gerätetyp. Verfügbare Optionen sind:

    - ABB RTU 500
    - Bachmann
    - Concept
    - Sel
    - SicamA8000
    - SIPROTEC 5
    - SNMP v1+v2
    - SNMP v3
    - SSH
    - WMI

5. Klicken Sie auf Weiter.

    Der Bereich Zugangsdatendetails wird angezeigt.

6. Geben Sie die folgenden Details an:

    - Name – Ein Name für die Zugangsdaten
    - Beschreibung – Eine Beschreibung für die Zugangsdaten
    - Benutzername – Der Benutzername für das Gerät.
    - Passwort – Das Passwort für das Gerät.
    - Test-IP-Adresse – Die IP-Adresse des Geräts.

7. Klicken Sie auf Zugangsdaten testen, um zu überprüfen, ob OT Security das Gerät mit den Zugangsdaten erreichen kann.
8. (Für duplizierte Netzwerke) Wählen Sie im Feld Duplikat (Sensor) die zugehörigen Sensoren aus.
9. Klicken Sie auf Speichern.

   Die Zugangsdaten werden in OT Security gespeichert und auf der Seite Zugangsdaten angezeigt.

## Zugangsdaten bearbeiten

Sie können Ihre Zugangsdaten bearbeiten.

### So bearbeiten Sie Zugangsdaten:

1. Gehen Sie zu Datenerfassung > Aktive Abfragen.

   Die Seite Verwaltung aktiver Abfragen wird angezeigt.
2. Klicken Sie auf die Registerkarte Zugangsdaten.

   Die Seite Zugangsdaten wird angezeigt.
3. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die gewünschten Zugangsdaten und wählen Sie Bearbeiten aus.
   - Wählen Sie die gewünschten Zugangsdaten und dann im Menü Aktionen die Option Bearbeiten aus.

   Der Bereich Zugangsdaten bearbeiten wird angezeigt.
4. Ändern Sie die Details nach Bedarf.
5. Klicken Sie auf Speichern.

### Zugangsdaten löschen

Sie können die nicht mehr benötigten Zugangsdaten löschen.

#### So löschen Sie Zugangsdaten:

1. Gehen Sie zu Datenerfassung > Aktive Abfragen.

   Die Seite Verwaltung aktiver Abfragen wird angezeigt.

2. Klicken Sie auf die Registerkarte Zugangsdaten.

   Die Seite Zugangsdaten wird angezeigt.

3. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die gewünschten Zugangsdaten und wählen Sie Löschen aus.
   - Wählen Sie die gewünschten Zugangsdaten und dann im Menü Aktionen die Option Löschen aus.

   OT Security löscht die ausgewählten Zugangsdaten.

### WMI-Konten

Damit OT Security WMI-Abfragen (Windows-Verwaltungsinstrumentation) durchführen kann, können Sie ein WMI-Konto einrichten. OT Security stützt sich auf WMI-Abfragen, um weitere Informationen über Windows-Systeme zu erhalten.

OT Security verwendet bei der Durchführung von WMI-Abfragen dieselben WMI-Methoden wie Tenable Nessus. Informationen zum Einrichten eines WMI-Kontos für Scans finden Sie im Abschnitt Enable Windows Logins for Local and Remote Audits (Windows-Logins für lokale und Remote-Überwachungen aktivieren) im Benutzerhandbuch zu Tenable Nessus.

## Nessus-Plugin-Scans erstellen

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

Der Nessus-Plugin-Scan startet einen erweiterten Nessus-Scan, der eine benutzerdefinierte Liste von Plugins für die Assets ausführt, die in der Liste der CIDRs und IP-Adressen angegeben sind.

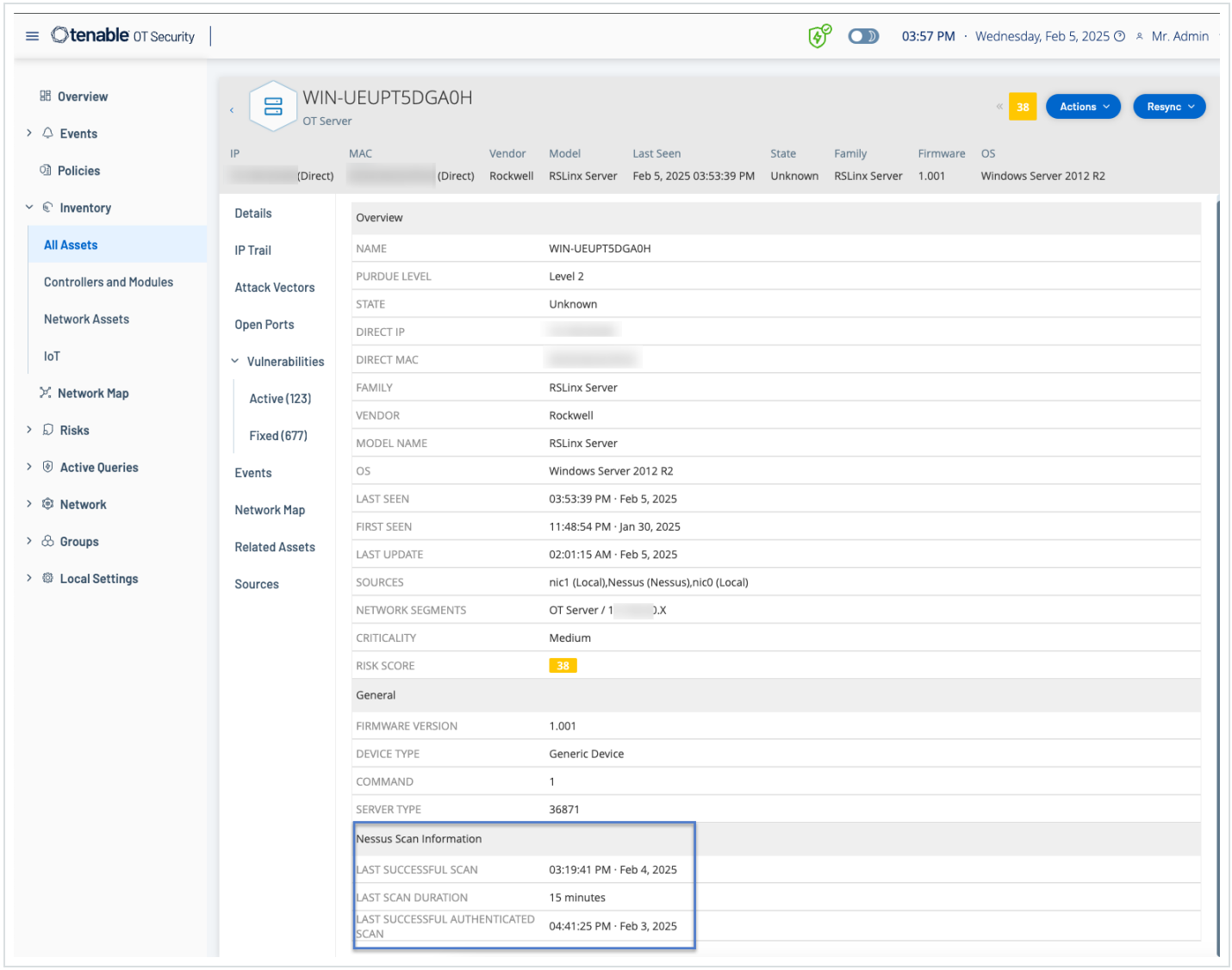
OT Security führt den Scan für reaktionsfähige Assets innerhalb der angegebenen CIDRs aus. Um Ihre OT-Geräte zu schützen, scannt OT Security jedoch nur bestätigte Netzwerk-Assets im angegebenen Bereich (Nicht-SPS). OT Security schließt Assets vom Typ Endgerät aus dem Scan aus.

Ab OT Security 4.1 können Sie mit den folgenden Optionen neue Scans erstellen:

- Gründliche Tests durchführen – Mit dieser Option kann Nessus einen detaillierten Scan durchführen, der Plugins umfasst, die zwar möglicherweise die Scandauer verlängern, aber dabei helfen, detaillierte Angaben wie JAR-Dateien oder installierte Python-Bibliotheken aufzudecken.
- Verarbeitung mit hoher Ausführlichkeit – Mit dieser Option kann der Scan zusätzliche Details über die Schwachstelle liefern, die Sie zur Behebung eines vom Scan festgestellten Problems verwenden können. Diese Option ermöglicht es Attack Path Analysis außerdem, die Daten der Nessus-Scan-Verbindungen zu nutzen.
- Netzwerk-Timeout (in Sekunden) – Dies ist die maximale Zeit, die Nessus auf eine Antwort vom Host warten muss. Wenn Sie über einen langsamen Host scannen, können Sie die Anzahl der Sekunden erhöhen. Der Standardwert ist 15 Sekunden.
- Max. gleichzeitige Prüfungen pro Host – Dies ist die maximale Anzahl von Prüfungen, die Nessus für den Host durchführen muss. Die Standardanzahl von Prüfungen ist 2.
- Max. gleichzeitige Hosts pro Scan – Dies ist die maximale Anzahl von Hosts, die Nessus gleichzeitig scannen kann. Die Standardanzahl von Hosts ist 10.

Die Nessus-Scan-Informationen für einen Credentialed-Scan enthalten die folgenden Details:

- Letzter erfolgreicher Scan
- Dauer des letzten Scans
- Letzter erfolgreicher authentifizierter Scan




Die Nessus-Scan-Informationen helfen Ihnen bei Folgendem:

- Bewertete und nicht bewertete Assets zu verstehen
- Nachzuvollziehen, ob auf Ihre Assets Credentialed-Scans oder Non-Credentialed-Scans angewendet werden
- Bei Scans und Schwachstellen-Management Best Practices anzuwenden. Beispielsweise können Sie Schwachstellenbewertungs-Scans für IT-Assets durchführen, auf denen Windows oder Linux ausgeführt wird. Scans, egal ob mit oder ohne Zugangsdaten, geben Aufschluss darüber, wie stark die Angriffsfläche Ihrer Organisation sowohl intern als auch extern gefährdet ist.

Der Nessus-Scan in OT Security verwendet die gleichen Richtlinieneinstellungen wie ein Netzwerk-Basisscan in Tenable Nessus, Tenable Security Center und Tenable Vulnerability Management. Der einzige Unterschied sind die Leistungsoptionen in OT Security. Im Folgenden sind die Leistungsoptionen für den Nessus-Scan in OT Security aufgeführt. Diese Optionen gelten auch für den Nessus-Basisscan, den Sie über die Seite Inventar > Alle Assets starten.

- 5 Hosts gleichzeitig (max.)
- 2 gleichzeitige Prüfungen pro Host (max.)
- 15 Sekunden Zeitüberschreitung für Lesevorgänge im Netzwerk

> Hinweis: Tenable Nessus ist ein invasives Tool, das am besten in IT-Umgebungen funktioniert. Tenable empfiehlt Tenable Nessus nicht für die Verwendung auf OT-Geräten, da es deren normalen Betrieb beeinträchtigen kann.

Informationen zum Durchführen eines Nessus-Basisscans für ein beliebiges einzelnes Asset finden Sie unter Asset-spezifischen Tenable Nessus-Scan durchführen.

## Einen Nessus-Plugin-Scan erstellen

### So erstellen Sie einen Nessus-Plugin-Scan:

1. Gehen Sie zu Aktive Abfragen > Abfrageverwaltung.

   Die Seite Verwaltung aktiver Abfragen wird angezeigt.

2. Gehen Sie zu Datenerfassung > Aktive Abfragen.

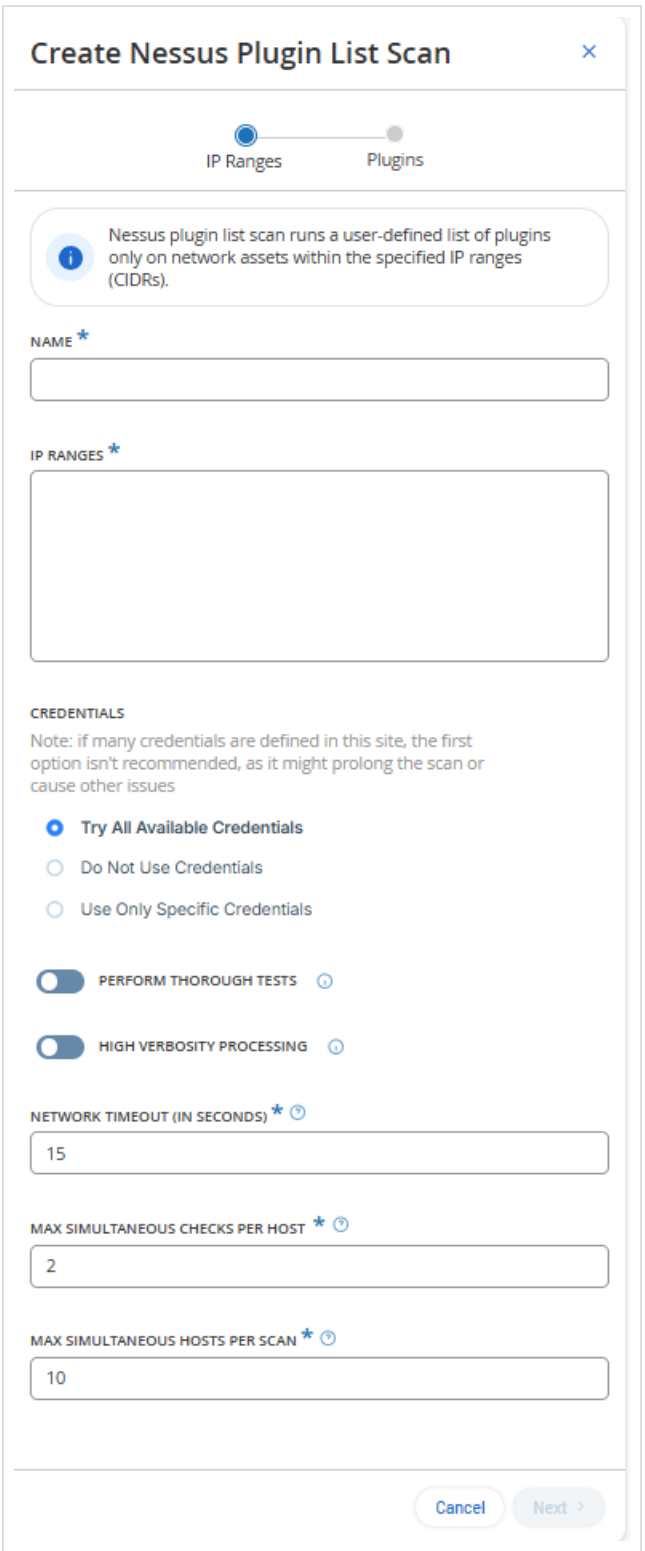
   Die Seite Verwaltung aktiver Abfragen wird angezeigt.

3. Klicken Sie auf die Registerkarte Nessus-Scans.

   Die Seite Nessus-Scans wird angezeigt.

4. Klicken Sie in der oberen rechten Ecke auf Scan erstellen.

   Der Bereich Nessus-Plugin-Listen-Scan erstellen wird angezeigt.


Create Nessus Plugin List Scan
IP Ranges
Plugins
Nessus plugin list scan runs a user-defined list of plugins only on network assets within the specified IP ranges (CIDRs).
NAME *
IP RANGES *
CREDENTIALS
Note: if many credentials are defined in this site, the first option isn't recommended, as it might prolong the scan or cause other issues
Try All Available Credentials
Do Not Use Credentials
Use Only Specific Credentials
PERFORM THOROUGH TESTS
HIGH VERBOSITY PROCESSING
NETWORK TIMEOUT (IN SECONDS) *
15
MAX SIMULTANEOUS CHECKS PER HOST *
2
MAX SIMULTANEOUS HOSTS PER SCAN *
10
Cancel
Next

> Hinweis: Die Abbildung zeigt die Standardwerte für die Erstellung eines neuen Nessus-Scans. Wenn Sie den Scan mit den Standardwerten ausführen, werden die Scans mit derselben Konfiguration wie die früheren Scans ausgeführt.

5. Geben Sie im Feld Name einen Namen für den Nessus-Scan ein.
6. Geben Sie im Feld IP-Bereiche einen Bereich von IP-Adressen oder CIDRs ein.
7. Wählen Sie eine der Optionen aus, um Zugangsdaten für den Nessus-Scan zuzuweisen:
    - Keine Zugangsdaten verwenden: Wählen Sie diese Option aus, wenn Sie einen nicht authentifizierten Scan ausführen möchten.

      > Tipp: Überspringen Sie diese Option, wenn mehrere Zugangsdaten konfiguriert sind, da die Auswahl dieser Option den Scan verlängern kann.

    - Alle verfügbaren Zugangsdaten testen: Wählen Sie diese Option aus, wenn der Scan alle verfügbaren Zugangsdaten testen soll.
    - Nur bestimmte Zugangsdaten verwenden
        a. Wählen Sie bei Auswahl von Nur bestimmte Zugangsdaten verwenden die erforderlichen Zugangsdaten aus einer Liste aller Zugangsdaten aus, die in der ICP definiert sind.
8. (Optional) Klicken Sie auf den Umschalter Gründliche Tests durchführen, um einen detaillierten Scan zu aktivieren.

> Hinweis: Zu den Optionen für Gründliche Tests durchführen gehören Plugins, die zwar möglicherweise die Scandauer verlängern, aber dem Nessus-Scan dabei helfen, detaillierte Angaben wie JAR-Dateien oder installierte Python-Bibliotheken aufzudecken.

9. (Optional) Klicken Sie auf den Umschalter Verarbeitung mit hoher Ausführlichkeit, damit der Scan zusätzliche Details zur Schwachstelle liefern kann.

Hinweis: Wenn Verarbeitung mit hoher Ausführlichkeit aktiviert wird, kann der Scan zusätzliche Details über die Schwachstelle liefern oder dabei helfen, ein vom Scan festgestelltes Problem zu beheben. Diese Option ermöglicht es Attack Path Analysis außerdem, die Daten der Nessus-Scan-Verbindungen zu nutzen.

10. Geben Sie im Feld Netzwerk-Timeout (in Sekunden) die maximale Zeit ein, die Nessus auf eine Antwort vom Host warten muss. Wenn Sie über einen langsamen Host scannen, können Sie die Anzahl der Sekunden erhöhen. Das Standard-Timeout beträgt 15 Sekunden.

11. Geben Sie im Feld Max. gleichzeitige Prüfungen pro Host die maximale Anzahl von Prüfungen ein, die Nessus für den Host durchführen muss. Die Standardanzahl von Prüfungen ist 2.

12. Geben Sie im Feld Max. gleichzeitige Hosts pro Scan die maximale Anzahl von Hosts ein, die Nessus gleichzeitig scannen kann. Die Standardanzahl von Hosts ist 10.

13. Klicken Sie auf Weiter.

    Der Bereich Plugins wird angezeigt.

    Hinweis: OT Security listet nur die Plugins auf, die für das Gerät spezifisch sind. Sie benötigen eine aktuelle Lizenz, um neue Plugins zu erhalten. Informationen zum Aktualisieren Ihrer Lizenz finden Sie unter Die Lizenz aktualisieren.

14. Wählen Sie in der Spalte Name der Plugin-Familie die erforderlichen Plugin-Familien aus, die in den Scan einbezogen werden sollen. Deaktivieren Sie in der rechten Spalte nach Bedarf die Kontrollkästchen für einzelne Plugins.

    Hinweis: Weitere Informationen zu Tenable Nessus-Plugin-Familien finden Sie unter https://de.tenable.com/plugins/nessus/families.

15. Klicken Sie auf Speichern.

    Der neue Nessus-Scan wird auf der Seite Nessus-Scans angezeigt.

    Hinweis: Um einen vorhandenen Tenable Nessus-Scan zu bearbeiten oder zu löschen, klicken Sie mit der rechten Maustaste auf den Scan und wählen Sie Bearbeiten oder Löschen aus.

### Einen Nessus-Plugin-Scan ausführen

So führen Sie einen Nessus-Plugin-Scan aus:

1. Führen Sie auf der Seite Nessus-Scans einen der folgenden Schritte aus:

    - Klicken Sie mit der rechten Maustaste auf den Scan und wählen Sie Jetzt ausführen aus.
    - Wählen Sie den Scan aus, den Sie ausführen möchten, und klicken Sie dann auf Aktionen > Jetzt ausführen.

    Das Dialogfeld Nessus-Scan genehmigen wird angezeigt.

2. Wenn Sie wissen, dass keine OT-Geräte in den Scan einbezogen sind, klicken Sie auf Trotzdem fortfahren.

    Das Dialogfeld wird geschlossen und OT Security speichert den Scan.

3. Um den Scan auszuführen, klicken Sie erneut mit der rechten Maustaste auf die Zeile des Scans und wählen Sie Jetzt ausführen aus.

    Das Dialogfeld Nessus-Scan genehmigen wird erneut angezeigt.

4. Klicken Sie auf Trotzdem fortfahren.

    OT Security führt jetzt den Scan aus. Sie können Scans je nach aktuellem Status anhalten/fortsetzen, stoppen oder abbrechen.

## Datenquellen

Der Abschnitt Datenquellen in OT Security enthält die folgenden Konfigurationsseiten:

- Sensoren – Sensoren anzeigen und verwalten, eingehende Sensor-Kopplungsanforderungen genehmigen oder löschen und aktive Abfragen konfigurieren, die von Sensoren durchgeführt werden. Siehe Sensoren.

- Agents – Erstellen Sie OT-Agents, um Windows-Remote-Computer zu scannen, wenn keine Sensoren installiert werden können. Siehe OT-Agents.
- IoT-Connectors – Ordnet alle verwalteten IoT-Geräte ihrem jeweiligen Anwendungsserver zu. Siehe IoT-Connectors verwalten.
- PCAP-Player – Eine PCAP-Datei mit aufgezeichneter Netzwerkaktivität hochladen und auf OT Security „abspielen“, wobei die Daten in Ihr System geladen werden. Siehe PCAP-Player.
- Manuelle Uploads:
    - Asset-Details per CSV aktualisieren – Die Details von Assets mithilfe einer CSV-Vorlage aktualisieren. Siehe Asset-Details per CSV aktualisieren.
    - Assets manuell hinzufügen – Der Asset-Liste mithilfe einer CSV-Vorlage neue Assets hinzufügen. Siehe Assets manuell hinzufügen.
    - SCD-Dateien – Laden Sie eine SCD-Datei in OT Security hoch und erhalten Sie Einblick in Ihre Assets, die IEC 61850-Konfiguration und Sicherheitserkenntnisse über Ihre Umgebung. Siehe SCD-Dateien.
    - Rockwell-Projektdateien – Laden Sie `Rockwell .L5X`-Dateien hoch, um Assets zu erstellen, Asset-Details anzureichern und Beziehungen zwischen Assets in Air-Gapped- oder Umgebungen mit eingeschränkter Sichtbarkeit aufzubauen. Siehe Rockwell-Projektdateien.

## Sensoren

Nachdem Sensoren über die Tenable Core-Benutzeroberfläche gekoppelt wurden, können Sie neue Kopplungen genehmigen und Sensoren anzeigen und mit den Funktionen Bearbeiten, Anhalten und Löschen im Menü Aktionen verwalten. Sie können auch die automatische Genehmigung von Sensorkopplungsanforderungen mit dem Umschalter Sensorkopplungsanforderungen automatisch genehmigen aktivieren.

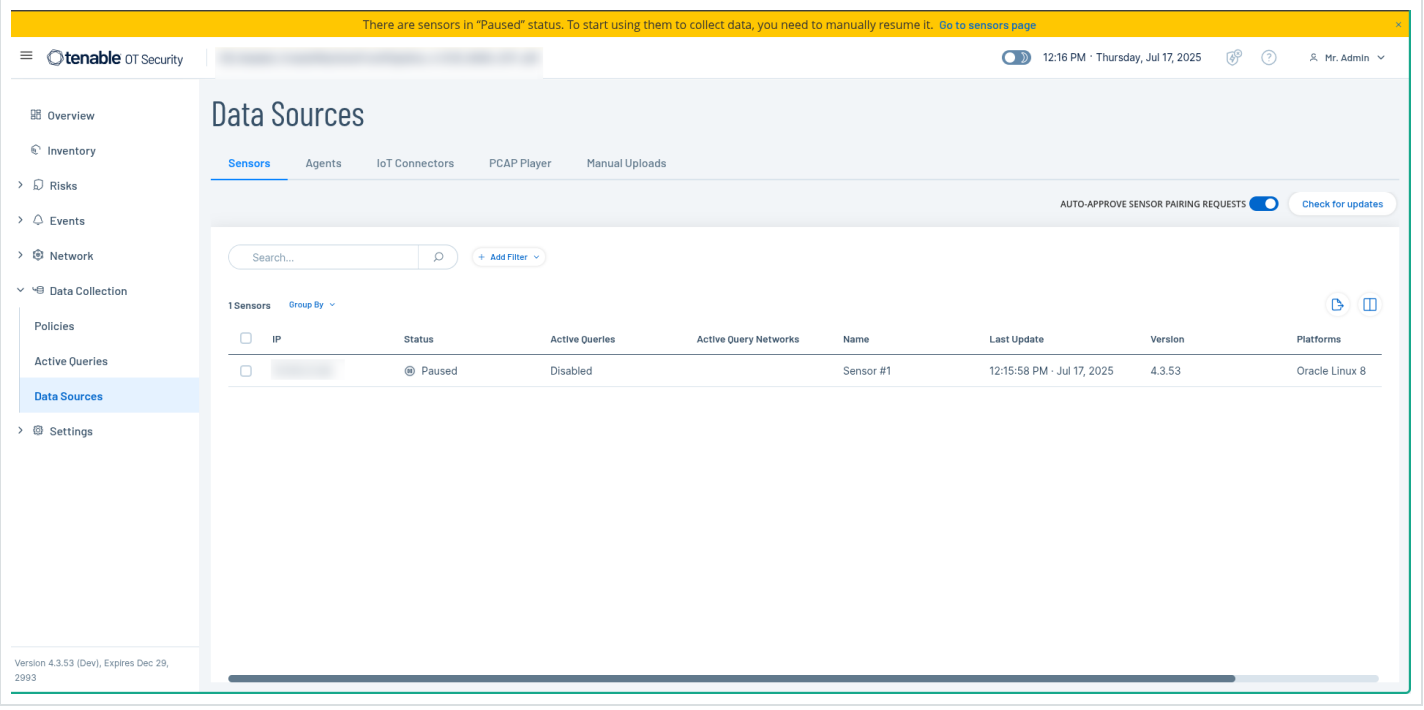
Hinweis: Sensormodelle vor Version 2.214 werden nicht auf der Seite „Sensoren“ für ICP angezeigt. Sie können jedoch weiterhin im nicht authentifizierten Modus verwendet werden.

Hinweis: Sie können eine unbegrenzte Anzahl von Sensoren mit ICP koppeln, aber das kombinierte SPAN-Traffic-Gesamtvolumen (Switched Port Analyzer) pro Appliance ist begrenzt. Sie können beispielsweise 10 Sensoren verwenden, von denen jeder zwischen 10 Mbit/s und 20 Mbit/s überträgt, aber der Gesamt-Traffic darf den ICP-Grenzwert nicht überschreiten. Weitere Informationen finden Sie im Abschnitt zu System- und Lizenzanforderungen im Benutzerhandbuch für Tenable Core und OT Security.

## Sensoren anzeigen

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager, Sicherheitsanalyst, Site-Operator, Schreibgeschützt

Die Sensortabelle enthält eine Liste aller Sensoren der Version 2.214 und höher im System. Informationen zum Anpassen von Tabellen finden Sie unter Elemente in der Benutzeroberfläche der Verwaltungskonsole.




Die Sensortabelle enthält die folgenden Details:

| Parameter | Beschreibung |
|---|---|
| IP | Die IPv4-Adresse des Sensors. |
| Status | Der Status des Sensors: Verbunden, Verbunden (nicht authentifiziert), Genehmigung ausstehend, Getrennt oder Angehalten.<br><br>Wichtig: Nach der Kopplung wird für alle Sensoren der Status Angehaltenangezeigt.<br><br>• So ändern Sie den Status für authentifizierte Sensoren: Klicken Sie in OT Security mit der rechten Maustaste auf die Sensoren und aktivieren Sie diese, indem Sie den Status von Angehalten in Verbunden ändern.<br><br>• So ändern Sie den Status für nicht authentifizierte Sensoren: Navigieren Sie in Tenable Core und OT Security Sensor zum Abschnitt OT Security Sensor > Kopplungsinfo und klicken Sie dann auf Resume Data Transfer (Datenübertragung wiederaufnehmen), um den Verbindungsstatus zu ändern. |
| Aktive Abfragen | Die Fähigkeit des Sensors, aktive Abfragen zu senden: Aktiviert, Deaktiviert oder N/A. |
| Aktive Abfragenetzwerke | Die Netzwerksegmente, denen der Sensor zugewiesen ist. |
| Name | Der Name des Sensors im System. |
| Letzte Aktualisierung | Datum und Uhrzeit der letzten Aktualisierung der Sensorinformationen. |
| Sensor-ID | Der universelle eindeutige Bezeichner (UUID) des Sensors, ein 128-Bit-Wert, der verwendet wird, um ein Objekt oder eine Entität im Internet eindeutig zu identifizieren. |
| Version | Die Version des Sensors. |

| | |
|---|---|
| Durchsatz | Ein Maß dafür, wie viele Daten den Sensor durchlaufen (in Kilobyte pro Sekunde). |

## Eingehende Sensorkopplungsanforderung manuell genehmigen

> Erforderliche OT Security-Benutzerrolle: Administrator

Wenn die Einstellung Sensorkopplungsanforderungen automatisch genehmigen auf AUS gestellt ist, müssen eingehende Sensorkopplungsanforderungen manuell genehmigt werden, bevor die Sensoren erfolgreich verbunden werden.

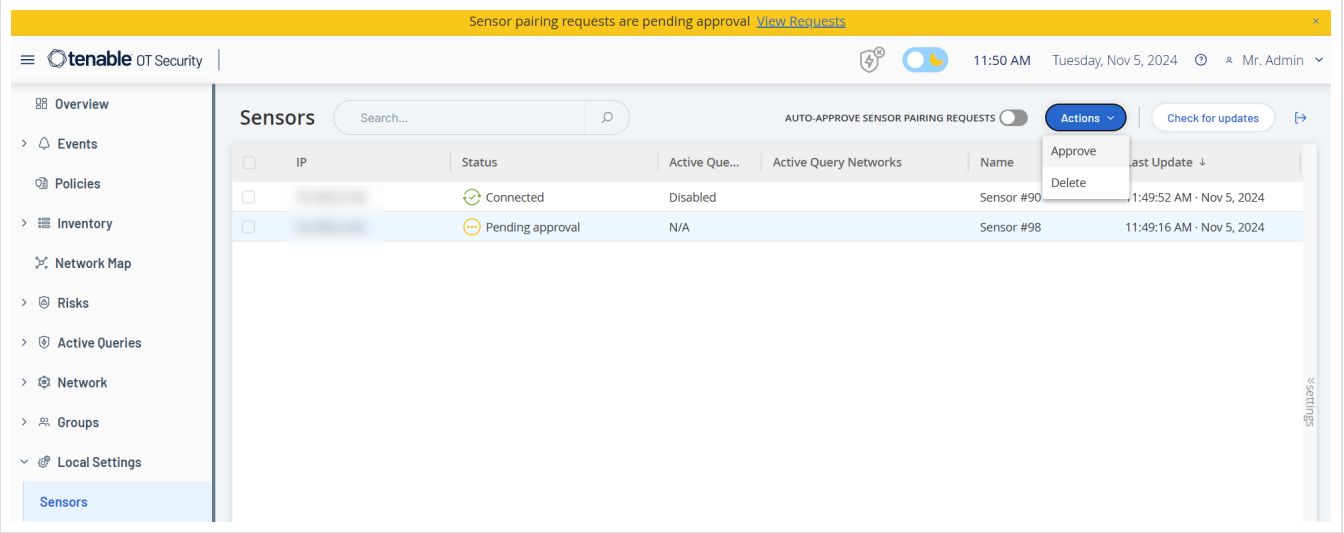
### So genehmigen Sie eine Sensorkopplungsanforderung manuell:

1. Klicken Sie auf der Seite Datenerfassung > Datenquellen auf die Registerkarte Sensoren.

   Die Seite Sensoren wird angezeigt.

2. Klicken Sie in der Tabelle auf eine Zeile mit dem Status Genehmigung ausstehend.

3. Klicken Sie auf Aktionen > Genehmigen oder klicken Sie mit der rechten Maustaste und wählen Sie Genehmigen aus.



> Hinweis: Um einen Sensor zu löschen, klicken Sie auf Aktionen > Löschen oder klicken Sie mit der rechten Maustaste und wählen Sie Löschen aus.

## Aktive Abfragen konfigurieren

> Erforderliche OT Security-Benutzerrolle: Administrator

Sobald ein Sensor im authentifizierten Modus verbunden ist, kann er so konfiguriert werden, dass er aktive Abfragen in den Netzwerksegmenten durchführt, denen er zugewiesen ist. Sie müssen angeben, welche Netzwerksegmente abgefragt werden.

> Hinweis: Sensoren führen unabhängig von dieser Konfiguration eine passive Netzwerkerkennung in allen verfügbaren Segmenten durch.

### So konfigurieren Sie aktive Abfragen:

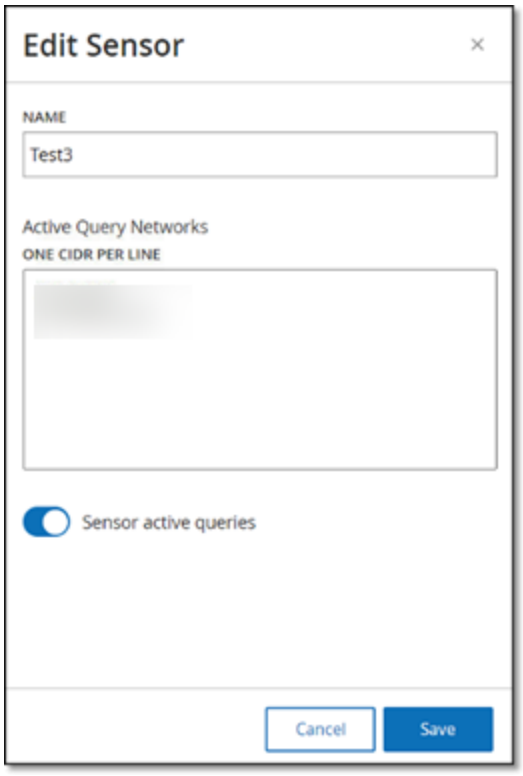
1. Klicken Sie auf der Seite Datenerfassung > Datenquellen auf die Registerkarte Sensoren.

   Die Seite Sensoren wird angezeigt.

2. Klicken Sie in der Tabelle auf eine Zeile mit dem Status Verbunden.

3. Klicken Sie auf Aktionen > Bearbeiten oder klicken Sie mit der rechten Maustaste und wählen Sie Bearbeiten aus.

   Das Fenster Sensor bearbeiten wird angezeigt.




4. Um den Sensor umzubenennen, bearbeiten Sie den Text im Feld Name.
5. Im Feld Aktive Abfragenetzwerke können Sie relevante Netzwerksegmente hinzufügen oder bearbeiten, an die der Sensor aktive Abfragen sendet. Verwenden Sie hierzu die CIDR-Notation und fügen Sie jedes Subnetzwerk in einer separaten Zeile hinzu.

   Hinweis: Abfragen können nur für CIDRs durchgeführt werden, die in den überwachten Netzwerkbereichen enthalten sind. Stellen Sie sicher, dass Sie nur CIDRs hinzufügen, auf die über diesen Sensor zugegriffen werden kann. Das Hinzufügen nicht zugänglicher CIDRs kann sich auf die Abfragemöglichkeiten der ICP über andere Mittel auswirken.

   Hinweis: Wenn der Sensor Teil eines duplizierten Netzwerks ist, wird der IP-Bereich des duplizierten Netzwerks im Feld Aktive Abfragenetzwerke angezeigt und kann nicht bearbeitet werden.

6. Klicken Sie auf den Umschalter Aktive Sensorabfragen, um aktive Abfragen zu aktivieren.
7. Klicken Sie auf Speichern.

Das Fenster wird geschlossen. In der Tabelle Sensoren wird in der Spalte Aktive Abfragen für die aktivierten Sensoren jetzt Aktiviert angezeigt.

## Sensoren aktualisieren

Erforderliche OT Security-Benutzerrolle: Administrator

Ab Version 3.16 erhält OT Security Sensor Software- und Sicherheitsupdates von der ICP, die für die Verwaltung zuständig ist. Sobald ein Sensor mit Authentifizierung gekoppelt ist, ist er darauf angewiesen, dass ihm alle erforderlichen Betriebssystem- und Softwareupdates von der Site bereitgestellt werden. Der Sensor muss nur OT Security erreichen, um Softwareupdates zu empfangen. In OT Security können Sie alle Ihre Sensoren über die zentrale Seite Sensoren aktualisieren.

Hinweis: OT Security verwendet die Offline-ISO für die zentralisierten Updates. Um alle authentifizierten Sensoren, die an eine ICP angeschlossen sind, zentral zu aktualisieren, platzieren Sie die Offline-ISO für die ICP/den Sensor unter `/srv/tenablecore/offlineiso/tenable-offline-updates.iso` auf der ICP.

Hinweis: (Nur für OT Security EM-Benutzer). OT Security verwendet die Offline-ISO für die zentralisierten Updates. Um alle authentifizierten Sensoren, die an eine ICP angeschlossen sind, zentral über EM zu aktualisieren, platzieren Sie die Offline-ISO für EM unter `/srv/tenablecore/offlineiso/tenable-offline-updates.iso` auf EM.

Wenn der Sensor aktualisiert werden muss, erhalten Sie in folgenden Situationen eine Warnung:

- Beim Start.
- Beim Abschluss der Kopplung zwischen Sensor und ICP.
- Bei einer periodischen Prüfung.
- Bei Verwendung der Option Nach Aktualisierungen suchen.

Hinweis: Die Kopplung des Sensors mit OT Security muss mit Authentifizierung erfolgen, um Remote-Sensoren aktualisieren zu können. Weitere Informationen zur Kopplung finden Sie unter Sensor koppeln.

So aktualisieren Sie einen authentifizierten Sensor der Version 3.16 oder höher mit der ICP:

1. Klicken Sie auf der Seite Datenerfassung > Datenquellen auf die Registerkarte Sensoren.

   Die Seite Sensoren wird angezeigt.

2. Überprüfen Sie die Spalte Version, um festzustellen, ob die Version auf dem neuesten Stand ist oder ob ein Update erforderlich ist.

3. Wenn die Version aktualisiert werden muss, gehen Sie wie folgt vor:

   ### So aktualisieren Sie einen einzelnen Sensor:

   - Klicken Sie mit der rechten Maustaste auf den gewünschten Sensor und wählen Sie Aktualisieren aus.
   - Aktivieren Sie das Kontrollkästchen neben dem gewünschten Sensor und wählen Sie dann im Menü Aktionen die Option Aktualisieren aus.

   ### So aktualisieren Sie mehrere Sensoren:

   - Wählen Sie einen oder mehrere Sensoren aus, für die ein Update erforderlich ist, und wählen Sie dann im Menü Aktionen die Option Aktualisieren aus.

OT Security aktualisiert die ausgewählten Sensoren.

Hinweis: Während des Updates ist der Sensor möglicherweise nicht verfügbar.

## OT-Agents

OT-Agents sind Softwarekomponenten, die Sie auf Remote-Windows-Computern installieren können, um OT Security-Assets in Umgebungen, in denen eine Sensorinstallation nicht möglich oder sinnvoll ist, aktiv abzufragen und zu erfassen. OT-Agenten nutzen aktive Abfragen, um duplizierte Netzwerke und Netzwerke mit aktiven Abfragen zu scannen, die unter Überwachte Netzwerke aufgeführt sind. Auf diese Weise kann der Agent, der auf einem Windows-basierten Gateway, einer Engineering-Workstation oder einer Mensch-Maschine-Schnittstelle (HMI) ausgeführt wird, kritische OT-/IoT- und eingebettete Geräte im Netzwerk identifizieren.

Jedes vom OT-Agent erfasste OT-Asset wird mit diesem spezifischen Agent als Erfassungsquelle verknüpft. So können Assets in Ihrem Netzwerk rückverfolgt und identifiziert werden.

Um Netzwerke scannen zu können, installieren und konfigurieren Sie zuerst den OT-Agent. In den folgenden Abschnitten wird beschrieben, wie Sie den OT-Agent installieren, konfigurieren und zum Ausführen von Scans verwenden.

1. OT-Agent herunterladen
2. OT-Agent installieren
3. OT-Agent konfigurieren
4. Scans ausführen

## OT-Agents anzeigen

Die Seite OT-Agents fungiert als zentraler Knotenpunkt für das Monitoring und die Konfiguration der Agents, die Sie zur Überwachung Ihres Netzwerks bereitstellen.

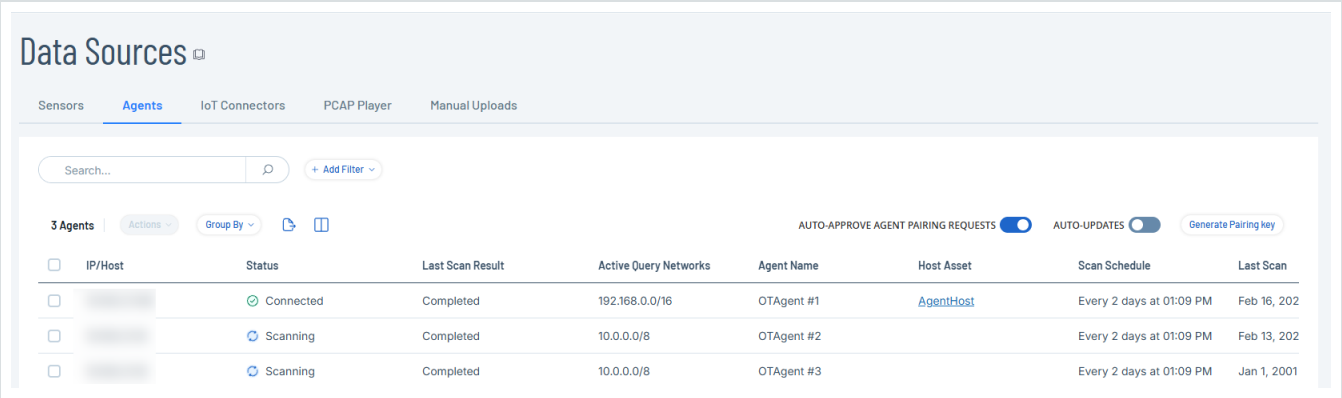
### So greifen Sie auf die Seite „OT-Agents“ zu:

1. Klicken Sie im linken Navigationsmenü auf Datenerfassung > Datenquellen.

   Die Seite Datenquellen wird angezeigt.

2. Klicken Sie auf die Registerkarte Agents.

Die Seite Agents wird mit einer Liste Ihrer bereitgestellten OT-Agents angezeigt.




Die Seite Agents enthält die folgenden Details:

| Parameter | Beschreibung |
|---|---|
| IP/Host | Die IPv4-Adresse des Computers, auf dem der OT-Agent installiert ist. |
| Status | Der Status des Agent:<br>• Verbunden<br>• Angehalten<br>• Getrennt<br>• Konfiguration ausstehend<br>• Genehmigung ausstehend<br>• Verbindung wird vorbereitet<br>• Warten auf Verbindung<br>• Aktualisierung läuft |

| | |
|---|---|
| | • Scan läuft |
| Ergebnis des letzten Scans | Der Status des letzten Scans: Abgeschlossen oder Fehlgeschlagen. |
| Aktive Abfragenetzwerke | Die spezifischen Netzwerksegmente, auf die OT-Agents im aktuellen Scan abzielen. |
| Agent-Name | Der eindeutige Name, der dem OT-Agent zugewiesen wurde. |
| Host-Asset | Ein direkter Link zur Seite mit Details des Host-Assets. |
| Scan-Zeitplan | Die für den Scan konfigurierte Frequenz. In der Spalte wird Deaktiviert angezeigt, wenn keine Zeitpläne vorhanden sind. |
| Letzter Scan | Das Datum und die Uhrzeit der Initiierung des letzten Scans. |
| Dauer des letzten Scans | Die Zeit, die bis zum Abschluss des letzten Scans vergangen ist. |
| Zugangsdaten | Die Zugangsdaten, die die Agents zum Scannen der Geräte verwenden. |
| **Gemeldete Assets** | Die Anzahl der im Scan erkannten Assets. |
| Agent-Version | Die Version des OT-Agent. |
| OTD-Version | Die Version der OT Discovery-Engine. |
| Host-Betriebssystem | Das Betriebssystem auf dem Hostcomputer. |

## OT-Agent installieren

> Erforderliche OT Security-Benutzerrolle: Administrator

Installieren Sie den OT-Agent auf einem Windows-Computer, um OT-Umgebungen zu scannen.

Bevor Sie beginnen

- Laden Sie den OT-Agent aus dem Tenable Download-Portal herunter.
- Dazu müssen Sie auf dem Windows-Computer über Administratorrechte verfügen.

Hinweis: Die Standardports für Kopplung und Verbindung sind 443 bzw. 28306. Informationen zu Ports finden Sie unter Überlegungen zur Firewall.

So installieren Sie den OT-Agent:

1. Übertragen Sie die Installationsdatei (`Tenable-OT-Agent-version.msi`) auf den Windows-Computer.
2. Klicken Sie auf die `.msi`-Installationsdatei, um den Installationsassistenten zu öffnen.
3. Klicken Sie im Fenster des OT-Agent-Setup-Assistenten auf Weiter.

   Das Fenster ICP-Details eingeben wird angezeigt.
4. Wählen Sie eine der folgenden Optionen aus:

   - Kopplungsschlüssel verwenden

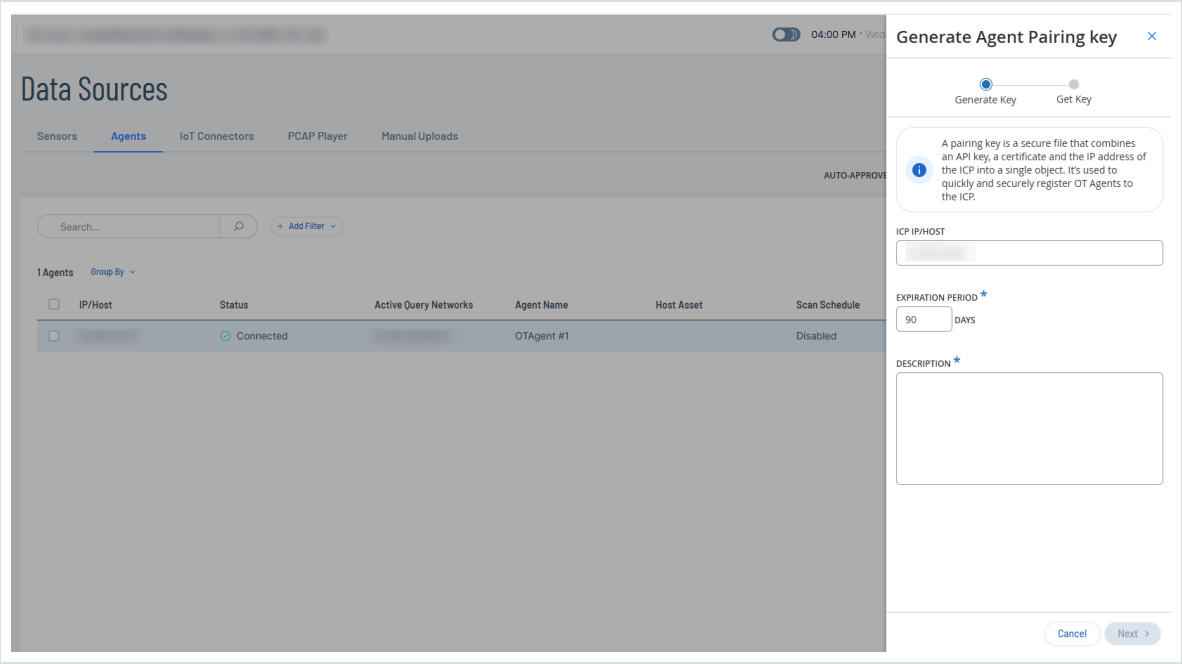
     Dies ist die Standardoption. Wenn Sie diese Option ausgewählt haben, führen Sie die folgenden Schritte aus:

     1. Gehen Sie in OT Security zu Datenerfassung > Datenquellen.

        Die Seite Datenquellen wird angezeigt.
     2. Klicken Sie auf die Registerkarte Agents.

        Die Seite Agents wird angezeigt.
     3. Klicken Sie in der oberen rechten Ecke auf Kopplungsschlüssel generieren.

Der Bereich Kopplungsschlüssel generieren wird angezeigt.

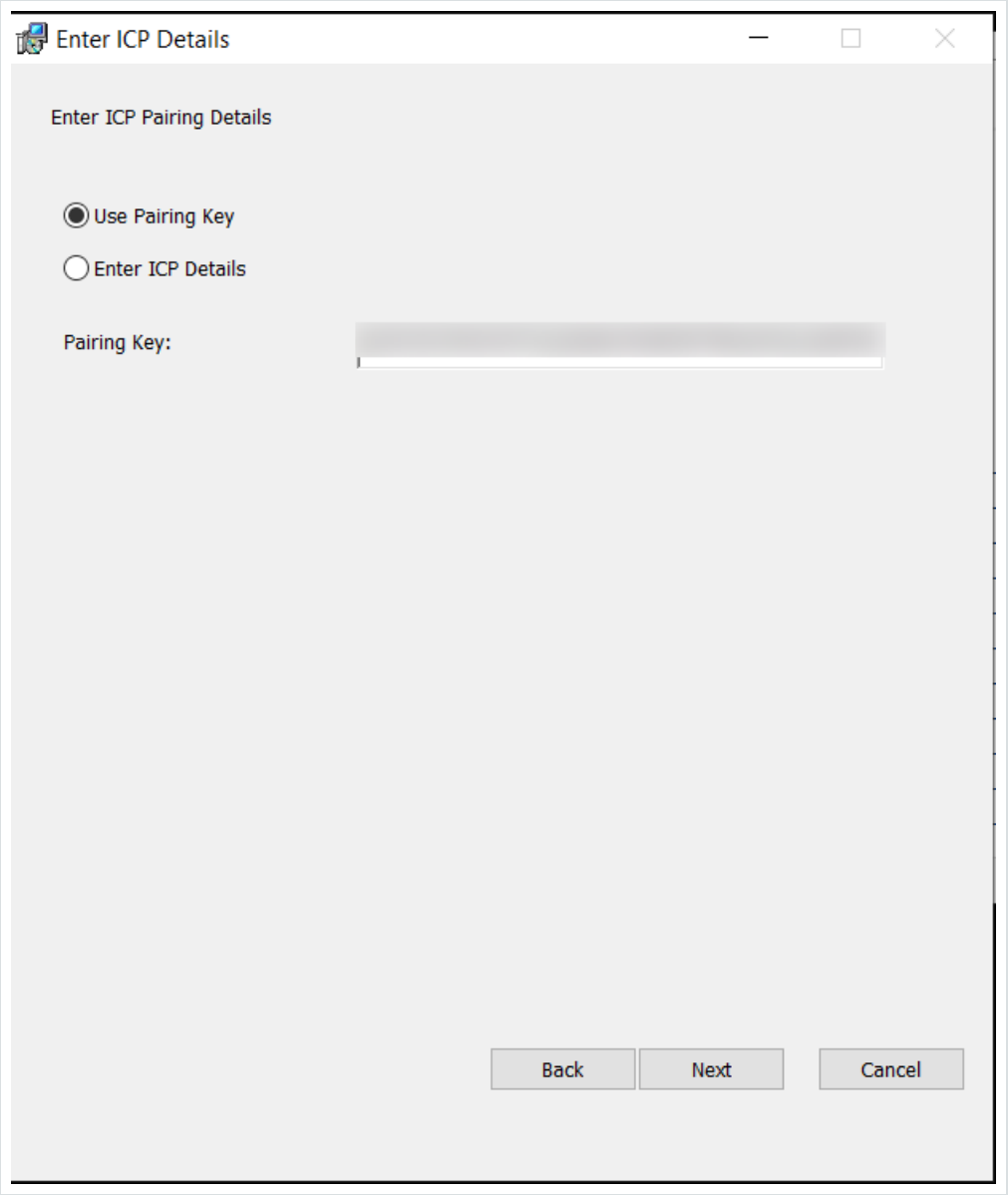



4. Geben Sie im Feld ICP-IP/-Host die IP-Adresse oder den Hostnamen der ICP ein.
5. Behalten Sie im Dropdown-Feld Ablauffrist den Standardwert von 90 Tagen bei oder legen Sie fest, nach wie vielen Tagen der Schlüssel abläuft.
6. Geben Sie im Feld Beschreibung eine Beschreibung für den Schlüssel ein.
7. Klicken Sie auf Weiter.

   OT Security generiert den Kopplungsschlüssel.
8. Klicken Sie auf die Schaltfläche , um den Kopplungsschlüssel zu kopieren.
9. Klicken Sie auf Fertig.

   OT Security schließt den Bereich.
10. Navigieren Sie zurück zum Windows-Hostcomputer.

11. Fügen Sie im Feld Kopplungsschlüssel den Kopplungsschlüssel ein, den Sie aus der ICP kopiert haben.




- ICP-Details eingeben

  Wenn Sie diese Option auswählen, werden die relevanten Felder angezeigt, in denen Sie die erforderlichen Details für die ICP angeben können.

1. Geben Sie im Feld ICP-Adresse die IP-Adresse der ICP ein.
2. Geben Sie im Feld ICP-Benutzername den Namen des ICP-Computers ein.
3. Geben Sie im Feld ICP-Passwort das Passwort des ICP-Computers ein.
4. Geben Sie im Feld API-Schlüssel den aus der ICP generierten API-Schlüssel an. Siehe API-Schlüssel generieren.
5. Geben Sie im Feld Zertifikat-Fingerabdruck den aus der ICP generierten Fingerabdruck an. Siehe Zertifikate.

> Hinweis: Der Kopplungsschlüssel und die Zertifikate sind nur für den Kopplungsvorgang erforderlich. Nach Abschluss der Kopplung können Sie den Kopplungsschlüssel und das Zertifikat löschen.

5. Klicken Sie auf Weiter.

   Das Fenster Zielordner wird angezeigt.

6. Behalten Sie im Feld Install OT-Agent to: (OT-Agent installieren unter:) das Standardziel bei oder geben Sie den Pfad zur Installation des OT-Agent an und klicken Sie auf Weiter.
7. Klicken Sie auf Installieren.

   Das Installationsprogramm installiert den OT-Agent und führt ihn auf der Registerkarte „Agents“ in OT Security mit dem Status Konfiguration ausstehend auf.

8. Klicken Sie auf Fertig stellen, um das Installationsprogramm zu schließen.

> Hinweis: Sollten bei der Kopplung Probleme auftreten, können Sie mit der Option Reparieren im Installationsassistenten des OT-Agent die Kopplungsdetails erneut angeben.

9. Um die Kopplungsanforderung automatisch zu genehmigen, aktivieren Sie den Umschalter Agent-Kopplungsanforderungen automatisch genehmigen.

   Wenn diese Option nicht aktiviert ist, gehen Sie wie folgt vor:

- Klicken Sie mit der rechten Maustaste auf den neu hinzugefügten OT-Agent.

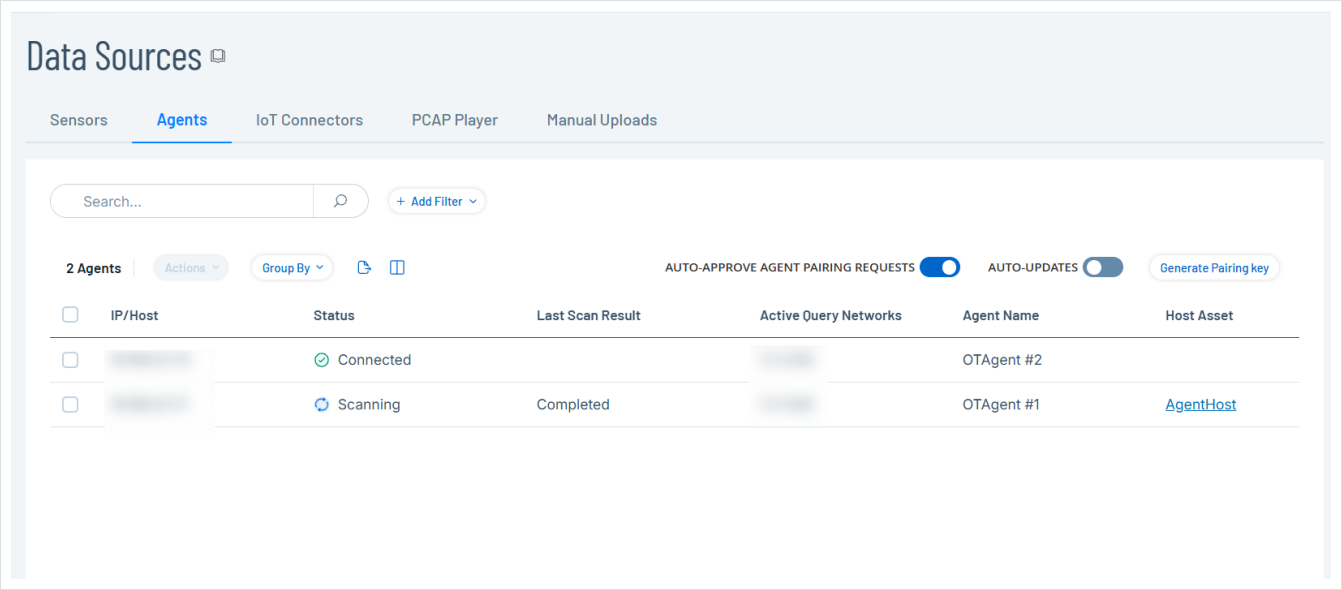
  Ein Menü wird angezeigt.

- Aktivieren Sie das Kontrollkästchen neben dem OT-Agent.

  In OT Security wird das Menü Aktionen > Genehmigen aktiviert.

10. Klicken Sie auf Genehmigen.

    OT Security genehmigt die Agent-Kopplung und ändert den Status in Konfiguration ausstehend.




> Hinweis: Prüfen Sie vor Ausführung des OT-Agent, dass seine Konfiguration abgeschlossen ist, auch wenn die Option Agent-Kopplungsanforderungen automatisch genehmigen aktiviert ist.

## Nächste Schritte

OT-Agent konfigurieren

## OT-Agent konfigurieren

> Erforderliche OT Security-Benutzerrolle: Administrator

Nachdem Sie den OT-Agent installiert haben, konfigurieren Sie ihn, um seinen Namen zu definieren, die gescannten Netzwerke anzugeben und einen Zeitplan für aktive Abfragen festzulegen.

Bevor Sie beginnen

- Installieren Sie den OT-Agent.

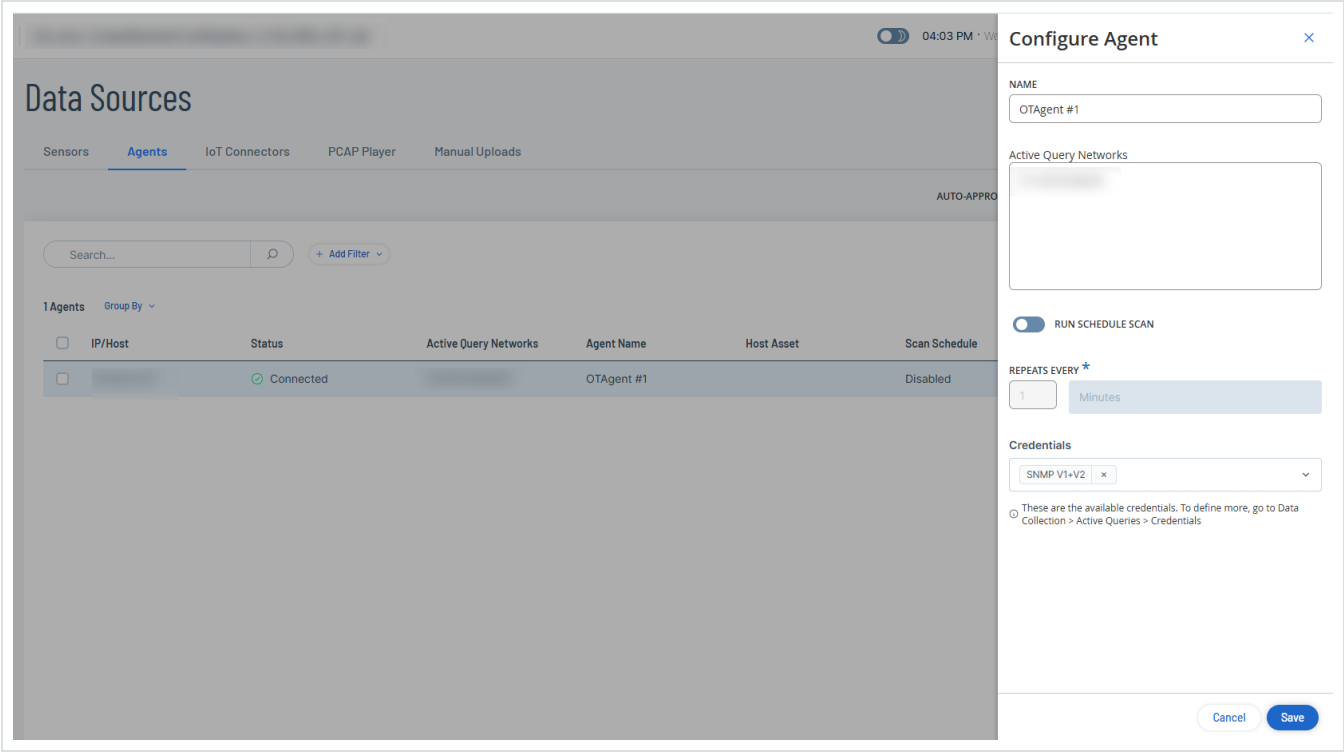
## So konfigurieren Sie den OT-Agent:

1. Führen Sie auf der Registerkarte Agents einen der folgenden Schritte aus:
    - Klicken Sie mit der rechten Maustaste auf den neu hinzugefügten OT-Agent.

      Ein Menü wird angezeigt.
    - Aktivieren Sie das Kontrollkästchen neben dem OT-Agent.

      In OT Security wird das Menü Aktionen > Konfigurieren aktiviert.
2. Klicken Sie auf Konfigurieren.

   Daraufhin wird der Bereich Agent konfigurieren angezeigt.




3. Geben Sie im Feld Name einen Namen für den Agent ein.
4. Geben Sie im Feld Aktive Abfrage die IP-Adressen der zu scannenden Netzwerke an.

   > Hinweis: Der OT-Agent scannt nur die IP-Adressen der aktiven Abfragenetzwerke, die zu den überwachten Netzwerken gehören (Umgebungseinstellungen > Netzwerkdefinitionen > Überwachte Netzwerke).

5. (Optional) Aktivieren Sie den Umschalter Geplanten Scan ausführen, damit geplante Scans ausgeführt werden.

   Daraufhin wird das Dropdown-Feld Wiederholungen alle in OT Security aktiviert.

6. (Optional) Geben Sie die erforderlichen Minuten, Stunden, Tage oder Wochen an.
7. Wählen Sie im Dropdown-Menü Zugangsdaten die erforderlichen Zugangsdaten aus.

   > Hinweis: In dieser Liste werden nur die Zugangsdaten angezeigt, die Sie unter Aktive Abfragen > Zugangsdaten erstellen. Weitere Informationen finden Sie unter Zugangsdaten.

8. Klicken Sie auf Speichern.

   OT Security aktualisiert den Status des OT-Agent auf Verbunden.

### Nächste Schritte

Scans ausführen

## Scans mit OT-Agent ausführen

> Erforderliche OT Security-Benutzerrolle: Administrator

Wenn Sie einen Agent-Scan initiieren, werden die folgenden aktiven Abfragen ausgelöst:

- Erfassung: Erkennt Live-Assets im überwachten Netzwerk.
- Prüfung offener Ports: Scannt die am häufigsten verwendeten Ports der Clients, die für aktive Abfragen verwendet werden.
- Erste Anreicherung: Identifiziert neu erfasste Assets mit Dynamic Fingerprinting Engine (DFE).
- OT-Abfragen: Sammelt Geräteinformationen, wie z. B. den SPS-Ausführungsstatus und andere an die Backplane angeschlossene Module.
- IT-Abfragen: Ruft Daten von IT-Geräten ab, die von OT Security überwacht werden.

Weitere Informationen finden Sie unter Aktive Abfragen verwalten.

### So scannen Sie einen Agent:

1. Führen Sie auf der Registerkarte Datenquellen > Agents einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf den neu hinzugefügten OT-Agent.

     Ein Menü wird angezeigt.

- Aktivieren Sie das Kontrollkästchen neben dem OT-Agent.

  In OT Security wird die Schaltfläche Aktionen in der Kopfleiste aktiviert.

> Hinweis: Um Scans für mehrere Agents zu initiieren, wählen Sie mehrere OT-Agents aus und klicken Sie dann auf Massenaktionen > Jetzt scannen.

2. Klicken Sie auf Aktionen > Jetzt scannen.

   Der Status des Agent ändert sich auf Scan läuft und das Scannen der angegebenen Netzwerke beginnt. Nachdem der Scan abgeschlossen wurde, klicken Sie in der Tabelle „Agents“ in der Spalte Gemeldete Assets auf den Link, um die gefilterten Ergebnisse auf der Seite Inventar anzuzeigen.

### Scan abbrechen

> Erforderliche OT Security-Benutzerrolle: Administrator

So stoppen Sie einen laufenden Scan:

1. Führen Sie auf der Registerkarte Datenquellen > Agents einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf den Agent und wählen Sie Scan abbrechen aus.
   - Aktivieren Sie das Kontrollkästchen neben dem Agent und klicken Sie dann auf Aktionen > Scan abbrechen.

   OT Security beendet den Scan und in der Spalte Ergebnis des letzten Scans wird Fehlgeschlagen angezeigt.

### OT-Agent aktualisieren

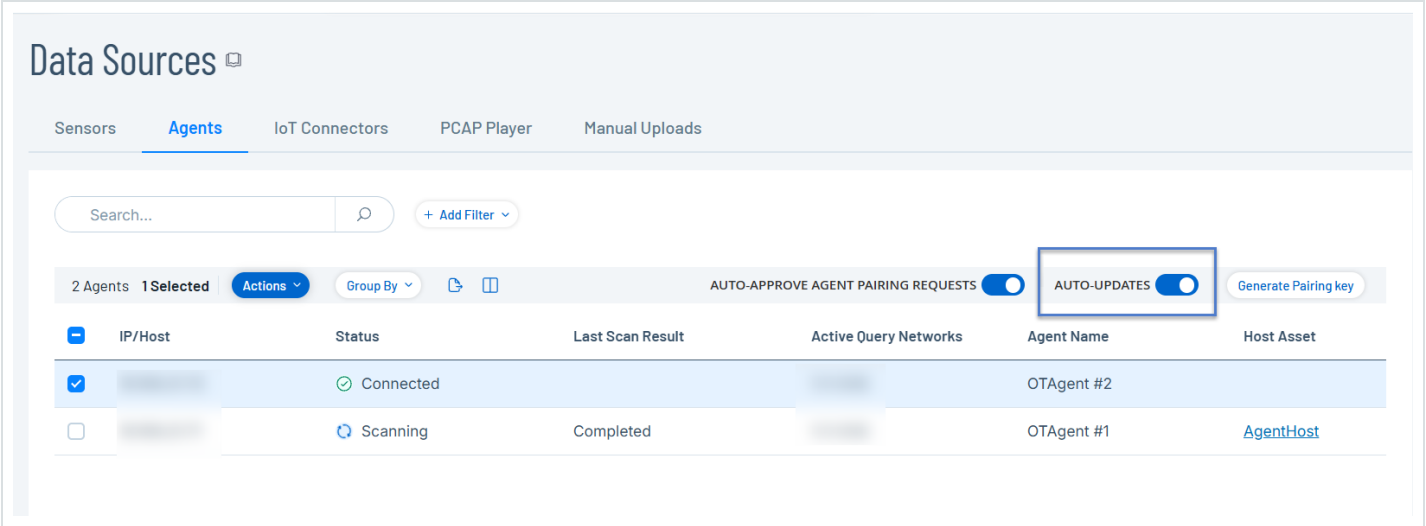
> Erforderliche OT Security-Benutzerrolle: Administrator

Zum Hochladen der Datei erforderliche **OT Security**-Benutzerrolle: Administrator, Supervisor und Sicherheitsanalyst.

OT-Agents verwenden die OT Discovery-Engine (OTD) zum aktiven Scannen Ihrer Umgebung. Sie können die Versionen der OT Discovery-Engine entweder manuell oder automatisch über die Seite Agents aktualisieren.

### Automatische Updates

Um die OTD-Versionen automatisch zu aktualisieren, wenn ein ICP-Update verfügbar ist, aktivieren Sie den Umschalter Automatische Updates. Der Umschalter ist standardmäßig deaktiviert. Wenn Sie Automatische Updates aktivieren, verschiebt OT Security automatisch die neueste OTD-Engine-Version zu verbundene Agents, sobald eine neue Version verfügbar ist.




### Manuelle Updates

Verwenden Sie manuelle Updates, wenn Sie die OTD-Engines zwischen den offiziellen Releases aktualisieren oder mehrere Agents gleichzeitig aktualisieren müssen.

### Bevor Sie beginnen

- Laden Sie die OTD-Datei im Abschnitt Systemkonfiguration > Updates > Update der OT Discovery-Engine (OTD) hoch, wie unter Updates der OT Discovery-Engine (OTD)

beschrieben.

- Stellen Sie sicher, dass der OT-Agent online ist und der Status Verbunden lautet.

### So aktualisieren Sie die OTD-Engine manuell:

1. Klicken Sie in der linken Navigationsleiste auf Datenquellen > Agents.

   Die Registerkarte Agents wird angezeigt.

2. Führen Sie eine der folgenden Aktionen aus, um Agents zu aktualisieren:

   - Klicken Sie mit der rechten Maustaste auf den Agent, den Sie aktualisieren möchten.

     Ein Menü wird angezeigt.

   - Aktivieren Sie das Kontrollkästchen neben dem Agent, den Sie aktualisieren möchten.

     In OT Security wird das Menü Aktionen aktiviert.

     > Hinweis: Um Massenaktualisierungen von OTD-Engines durchzuführen, wählen Sie mehrere Agents aus und klicken Sie dann auf Massenaktionen > Aktualisieren.

3. Klicken Sie auf Aktionen > Aktualisieren.

   Das Dialogfeld OTD-Version aktualisieren wird angezeigt.

4. Klicken Sie auf Aktualisieren, um zu bestätigen.

   OT Security aktualisiert die OT Discovery-Engines auf die neueste Version.

## OT-Agent löschen

> Erforderliche OT Security-Benutzerrolle: Administrator

Durch die Deinstallation des OT-Agent vom Windows-Computer ändert sich der Status des Agent in OT Security auf Getrennt.

### So löschen Sie einen OT-Agent:

1. Öffnen Sie auf dem Windows-Computer das Installationsprogramm und klicken Sie auf Entfernen.
2. Befolgen Sie die Schritte im Assistenten, um den Agent zu deinstallieren.

   Der OT-Agent wird vom Windows-Computer deinstalliert.
3. Navigieren Sie in OT Security zur Registerkarte Datenquellen > Agents.

   OT Security aktualisiert den Status des Agent auf Getrennt.
4. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf den neu hinzugefügten OT-Agent.

     Ein Menü wird angezeigt.
   - Aktivieren Sie das Kontrollkästchen neben dem OT-Agent.

     In OT Security wird das Menü Aktionen > Löschen aktiviert.

     > Hinweis: Um OT-Agents per Massenvorgang zu löschen, wählen Sie mehrere OT-Agents aus und klicken Sie dann auf Massenaktionen > Löschen.
5. Klicken Sie auf Löschen.

   OT Security löscht den OT-Agent.

   > Hinweis: Wenn duplizierte Netzwerke zugeordnet sind, müssen Sie diese zuerst löschen, bevor Sie den Agent löschen.

## OT-Agents mit CLI installieren

> Erforderliche OT Security-Benutzerrolle: Administrator

Verwenden Sie CLI-Befehle, um einen OT-Agent mit Kopplungsschlüssel, ICP-Zugangsdaten oder API-Schlüssel zu installieren. Sie können OT-Agents über die CLI auch deinstallieren.

Bevor Sie beginnen

- Laden Sie das Installationsprogramm für den OT-Agent aus dem Tenable-Download-Portal herunter.

Führen Sie den folgenden Befehl aus, um den OT-Agent mit einem Kopplungsschlüssel zu installieren:

```
msiexec.exe /i "<OtAgentInstaller.msi>" /qn PAIRING_KEY="<PairingKey>"
```

Dabei gilt:

- `OtAgentInstaller.msi` ist die Installationsdatei.
- `PairingKey` ist der Schlüssel, den Sie auf der Registerkarte Datenerfassung > Datenquellen > Agents in OT Security generieren.

Beispiel:

```
msiexec.exe /i "OtAgentInstaller.msi" /qn PAIRING_
KEY="xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxoxxxxxxxxxxxx"
```

Führen Sie den folgenden Befehl aus, um den OT-Agent mit Benutzernamen und Passwort zu installieren:

```
msiexec.exe /i "<OtAgentInstaller.msi>" /qn ICP_ADDRESS="<IpAddress>" ICP_USERNAME="<Username>" ICP_
PASSWORD="<Password>" ICP_FINGERPRINT="<CertFingerprint>"
```

Dabei gilt:

- `OtAgentInstaller.msi` ist die Installationsdatei.
- `IpAddress` ist die IP-Adresse der ICP.
- `Username` ist der Benutzername zum Einloggen bei der ICP.

- `Password` ist das ICP-Passwort.
- `CertFingerprint` ist das Zertifikat, das Sie in OT Security generieren.

Beispiel:

```
msiexec.exe /i "OtAgentInstaller.msi" /qn ICP_ADDRESS="XX.XXX.XX.XX" ICP_USERNAME="admin" ICP_
PASSWORD="xxxxxxx" ICP_FINGERPRINT="XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX"
```

Führen Sie den folgenden Befehl aus, um den OT-Agent mit einem API-Schlüssel zu installieren:

```
msiexec.exe /i "<OtAgentInstaller.msi>" /qn ICP_ADDRESS="<IpAddress>" ICP_APIKEY="<APIKey>" ICP_
FINGERPRINT="<CertFingerprint>"
```

(Optionaler Parameter) `INSTALLBASE='"<FullDirPath>"'`

Dabei gilt:

- `OtAgentInstaller.msi` ist die Installationsdatei.
- `IpAddress` ist die IP-Adresse der ICP.
- `APIKey` ist der aus der ICP generierte API-Schlüssel.
- `CertFingerprint` ist das aus der ICP generierte Zertifikat.
- `FullDirPath` ist der Pfad des Installationsverzeichnisses.

Beispiel 1:

```
msiexec.exe /i "OtAgentInstaller.msi" /qn ICP_ADDRESS="XX.XXX.XX.XX" ICP_APIKEY="kxxxxxxxxxxxxxxxxx_
xxxxxxxx=" ICP_FINGERPRINT="XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX"
```

Beispiel 2: Verwendung des `INSTALLBASE`-Parameters:

```
msiexec.exe /i "OtAgentInstaller.msi" /qn ICP_ADDRESS="xx.xxx.xx.xx" ICP_APIKEY="xxxxxxxxxxxxxxx_
xxxxxxxxxxx=" ICP_FINGERPRINT="XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX"
INSTALLBASE='"C:\Program Files\AAA"'
```

Führen Sie den folgenden Befehl aus, um den OT-Agent zu deinstallieren:

```
msiexec.exe /x "<OtAgentInstaller.msi>" /qn
```

Dabei gilt:

- `OtAgentInstaller.msi` ist die Installationsdatei.

## Geplante Scans für OT-Agents aktivieren, deaktivieren oder festlegen

Mit der Option Massenaktionen können Sie geplante Scans für mehrere OT-Agents gleichzeitig aktivieren oder deaktivieren.

### Bevor Sie beginnen

- Stellen Sie sicher, dass die OT-Agents online sind und in der Spalte Status Verbunden angezeigt wird.

### So führen Sie Massenaktionen für geplante Agent-Scans durch:

1. Wählen Sie in der Tabelle „Agents“ mehr als einen OT-Agent für den Scan aus.

   In OT Security wird Massenaktionen in der Kopfleiste aktiviert.

2. Wählen Sie eine der folgenden Optionen aus:

| Option für Massenaktionen | Beschreibung |
|---|---|
| Geplanten Scan aktivieren | Wählen Sie diese Option aus, um geplante Agent-Scans zu aktivieren. Der geplante Scan wird standardmäßig jede Minute ausgeführt. |

| | |
|---|---|
| Geplanten Scan deaktivieren | Wählen Sie diese Option aus, um geplante Agent-Scans zu deaktivieren. |
| Geplanten Scan festlegen | a. Um einen geplanten Scan zu konfigurieren, klicken Sie auf Massenaktionen > Geplanten Scan festlegen.<br><br>Der Bereich Zeitplan festlegen wird angezeigt.<br><br>b. Wählen Sie im Feld Wiederholung alle aus, wie oft der Scan wiederholt werden soll.<br><br>c. Geben Sie die erforderlichen Minuten, Stunden, Tage oder Wochen an.<br><br>Hinweis: Der hier angegebene Zeitplan setzt alle vorhandenen Zeitpläne für die Agents außer Kraft.<br><br>d. Klicken Sie auf Speichern. |

Vergleich von OT-Agent und Sensor

| Funktion | OT-Agent | Sensor |
|---|---|---|
| **Zielanwendungsfall** | Für Bewertungen, PoVs und flexible Windows-basierte OT-Umgebungen | Für vollständige Bereitstellungen, bei denen eine Untersuchung und Kontrolle des Traffics erforderlich ist |
| **Bereitstellungstyp** | Installation auf Windows-Computern (HMI, Workstation, Jump-Box) | Je nach Tenable Core-Betriebssystem Installation auf Hardware oder VM |
| **ICP-Abhängigkeit** | Erfordert Kopplung mit ICP, kann | Vollständig von ICP abhängig |

| | | |
|---|---|---|
| | aber unabhängig arbeiten, um Daten zu erfassen (Support + Skripts erforderlich) | |
| **Komplexität der Installation** | Leicht, flexibel; kann per Massenvorgang bereitgestellt werden | Erfordert physische oder virtuelle Bereitstellung + Konfiguration |
| **Datenfluss zu ICP** | Ergebnisse werden nach Abschluss des Scans übertragen | Kontinuierlicher Datenstrom (aktiv + passiv) |
| **Ausführungstyp** | Nur aktives Scannen | Aktives und passives Scannen |
| **Benutzeroberfläche für Scan-Verwaltung** | Wird nur über die Seite Agents verwaltet | Abfragen werden über die Seiten Aktive Abfrage und Inventar ausgelöst |
| **Nessus-Integration** | Nicht unterstützt | Nessus-Abfragen über Sensoren möglich |
| **Abgleich von Schwachstellen** | Verwendet eingebettetes Nessus in ICP für den Abgleich | Verwendet eingebettetes Nessus in ICP für den Abgleich und zum aktiven Scannen |
| **Scan-Planung** | Unterstützt (einmalig oder wiederkehrend) | Unterstützt (einmalig oder wiederkehrend) |
| **Asset-Sichtbarkeit** | Assets werden im Inventar angezeigt, können aber nicht über das Inventar abgefragt werden | Assets können vollständig über das Inventar abgefragt werden |
| **Umfang der Zugangsdaten** | Verwendet dedizierte Zugangsdaten, die pro Agent | Verwendet globale Zugangsdaten von ICP |

| | | |
|---|---|---|
| | konfiguriert werden | |
| **Unterstützung für duplizierte Netzwerke** | Unterstützt | Unterstützt |
| **Respektiert globale Einschränkungen** | In Version 4.3 nicht unterstützt | Unterstützt |
| **Kopplungsmethode** | Kopplungsschlüssel (API-Schlüssel + Zertifikat + ICP-IP in einem Blob) | Erfordert API-Schlüssel, Zertifikat oder IP (manuelle Konfiguration) |
| **Hardware** | Keine – wird auf vorhandenen Windows-Computern ausgeführt | Dedizierte Hardware oder VM erforderlich |
| **Passive Traffic-Erfassung** | Nicht unterstützt | Vollständig unterstützt |

## IoT-Connectors verwalten

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

Mit OT Security können Sie alle verwalteten IoT-Geräte (Internet of Things) ihrem jeweiligen Anwendungsserver zuordnen, indem Sie das IoT Connector-Modul konfigurieren und Assets vom betreffenden Anwendungsserver synchronisieren.

Für eine IP-Kamera sehen Sie beispielsweise den VMS-Server (Video Management System), der die Kamera verwaltet. Wenn Sie in OT Security auf der Seite Inventar zum VMS-Anwendungsserver navigieren, werden alle Kameras angezeigt, die auf der Seite Inventar > Verwandte Assets verwaltet werden.

Hinweis: Beim Importieren von Assets von einem IoT-Connector importiert OT Security standardmäßig die IP-Adresse zusammen mit der MAC-Adresse der Geräte. Um nur die MAC-Adresse zu importieren, navigieren Sie zu Einstellungen > Umgebungskonfiguration > Asset-Einstellungen und deaktivieren Sie die Option IP-Adresse für IoT-Assets abrufen.

### Anforderungen für den IoT-Connector-Agent

| Anforderungskategorie | Mindestanforderung |
|---|---|
| Betriebssystem | • Windows XP, 7, 10 oder 11; Windows Server 2003, 2008, 2012, 2016, 2019 oder 2022<br>• Ubuntu 20.x oder 22.x |
| Arbeitsspeicher | 1 GB |
| Festplattenspeicher | 1 GB |
| CPU | Jede Hardware mit mindestens 10 % dedizierter CPU-Kapazität. |

### IoT Connectors-Modul

OT Security enthält ein IoT Connector-Modul, das Sie in Ihre IoT/VMS-Server integrieren können.

Dieses Modul unterstützt zwei Verbindungsmethoden: die Authentifizierung mit einem Remote-API-Anwendungsdienst oder das Herstellen der Verbindung über einen Agent. Nach der Integration Ihrer Anwendungsserver mit dem Modul importiert OT Security alle verwalteten Geräte, wie z. B. Kameras, Badge-Zugangssysteme und Brandmeldezentralen.

Sie können für IoT-Connectors die folgenden Aufgaben durchführen:

### IoT-Connectors hinzufügen

1. Klicken Sie auf der Seite Datenerfassung > Datenquellen auf die Registerkarte IoT-Connectors.

   Die Seite IoT-Connectors wird angezeigt.

2. Klicken Sie in der oberen rechten Ecke auf IoT-Connector hinzufügen.

   Ein Dropdown-Menü wird geöffnet.

3. Wählen Sie eine der folgenden Optionen aus:

   - Über Agent

     1. Geben Sie im Feld Connector-Name einen Namen für den Connector ein.
     2. Geben Sie im Feld IP-Adresse des Servers die IP-Adresse des Connectors ein, der hinzugefügt werden soll.
     3. Um eine Verbindung zu dem in der Datenbank gehosteten VMS herzustellen, aktivieren Sie den Umschalter VMS-Zugangsdaten.

        OT Security aktiviert die relevanten Felder, die für VMS-Zugangsdaten erforderlich sind.

     4. Fügen Sie im Feld IP-Adresse der Datenbank die IP-Adresse der Datenbank hinzu, die das VMS hostet.
     5. Fügen Sie im Feld Datenbank-Port die Portnummer hinzu, über die eine Verbindung zum Server hergestellt werden soll.
     6. Geben Sie im Feld Benutzername den Benutzernamen für die Datenbank ein.
     7. Geben Sie im Feld Passwort das Passwort für die Datenbank ein.
     8. Klicken Sie auf Speichern.

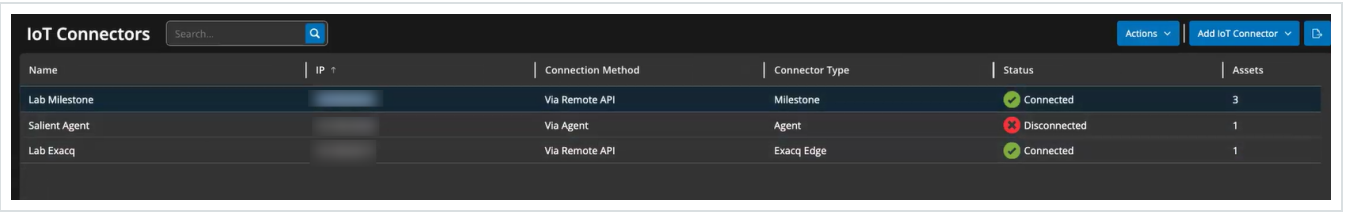
> Hinweis: Wenn der OT Security IoT Connector Agent auf Ihrem Anwendungsserver nicht installiert ist, schlägt die Verbindung fehl und OT Security zeigt eine Fehlermeldung an.

- Über Remote-API

1. Wählen Sie im Abschnitt Connector-Typ den hinzuzufügenden IoT-Connector aus.
2. Klicken Sie auf Weiter.

   Der Abschnitt Connector-Details wird angezeigt.
3. Geben Sie im Feld Connector-Name einen Namen für den Connector ein.
4. Geben Sie in das Feld IP die IP-Adresse des Connectors ein.
5. Geben Sie in das Feld Port die Portnummer ein, über die OT Security eine Verbindung herstellen kann. Die standardmäßige Portnummer lautet 22609.
6. Geben Sie im Feld Benutzername den Benutzernamen ein, der für das Einloggen beim Connector verwendet werden soll.
7. Geben Sie im Feld Passwort das Passwort für den Connector ein.
8. Klicken Sie auf Speichern.

OT Security speichert den Connector und er wird auf der Seite IoT-Connectors angezeigt.




## Mit dem IoT-Connector verknüpfte Assets anzeigen

Nachdem Sie eine Verbindung zum Anwendungsserver hergestellt haben, können Sie die zugehörigen Assets oder Dienste anzeigen, die vom Anwendungsserver verwaltet werden.

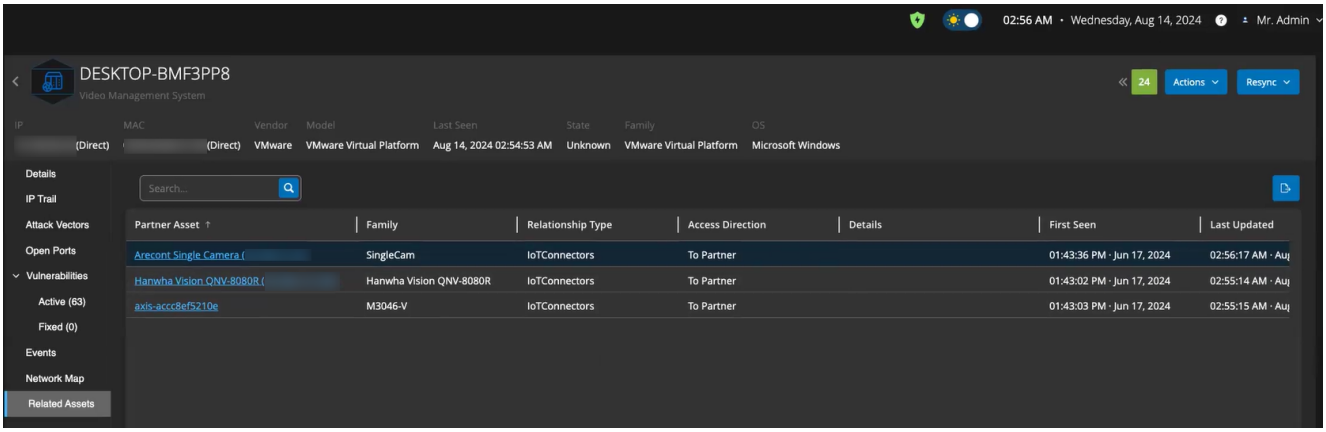
So zeigen Sie alle vom Server verwalteten Geräte an:

1. Gehen Sie zu Inventar > Alle Assets.

   Die Seite Alle Assets wird angezeigt.

2. Verwenden Sie das Suchfeld, um nach dem Anwendungsserver zu suchen.

   Die Seite des ausgewählten Anwendungsservers wird angezeigt. Dort finden Sie eine Liste der Geräte, die der Server verwaltet.




## IoT-Verbindung testen

Nachdem Sie einen IoT-Connector hinzugefügt haben, können Sie testen, ob OT Security sich mit ihm verbinden kann.

1. Führen Sie in der IoT-Connectors-Tabelle einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die Zeile des IoT-Connectors, den Sie testen möchten, und wählen Sie Verbindung testen aus.
   - Wählen Sie den IoT-Connector aus, den Sie testen möchten, und klicken Sie dann auf Aktionen > Verbindung testen.

   OT Security führt den Test aus, um zu verifizieren, dass es den Connector erreichen kann.

## IoT-Connector bearbeiten

1. Führen Sie in der IoT-Connectors-Tabelle einen der folgenden Schritte aus:

    - Klicken Sie mit der rechten Maustaste auf die Zeile des IoT-Connectors, den Sie bearbeiten möchten, und wählen Sie Bearbeiten aus.
    - Wählen Sie den IoT-Connector aus, den Sie bearbeiten möchten, und klicken Sie dann auf Aktionen > Bearbeiten.

    Der Bereich IoT-Connector über Agent/Remote-API bearbeiten wird angezeigt.

2. Ändern Sie die Details nach Bedarf.
3. Klicken Sie auf Speichern.

    OT Security speichert die am IoT-Connector vorgenommenen Änderungen.

### IoT-Connector löschen

1. Führen Sie in der IoT-Connectors-Tabelle einen der folgenden Schritte aus:

    - Klicken Sie mit der rechten Maustaste auf die Zeile des IoT-Connectors, den Sie löschen möchten, und wählen Sie Löschen aus.
    - Wählen Sie den IoT-Connector aus, den Sie löschen möchten, und klicken Sie dann auf Aktionen > Löschen.

    OT Security löscht den IoT-Connector.

    > Hinweis: Nachdem Sie einen IoT-Connector gelöscht haben, deinstalliert OT Security den IoT Connector-Agent auf dem Anwendungsserver. Wenn Sie eine Verbindung zum selben Anwendungsserver über den Agent herstellen möchten, müssen Sie den OT Security IoT Connector Agent installieren.

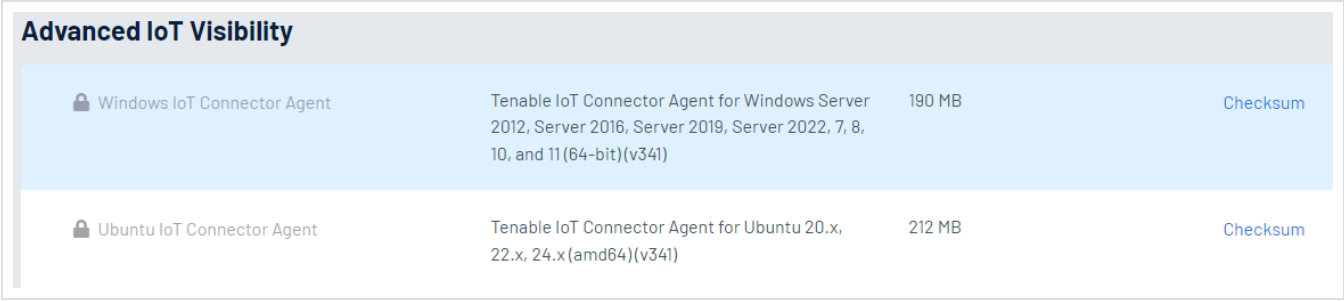
### IoT Connector Agent unter Windows installieren

> Erforderliche Rolle: Administrator

Mit OT Security können Sie alle verwalteten IoT-Geräte (Internet of Things) ihrem jeweiligen Anwendungsserver zuordnen, indem Sie das IoT Connector-Modul konfigurieren und Assets vom betreffenden Anwendungsserver synchronisieren. Um Ihren Anwendungsserver über den Agent zu verbinden, müssen Sie den OT Security IoT Connector Agent installieren.

So installieren Sie den OT Security IoT Connector Agent:

1. Melden Sie sich auf der Seite Tenable Downloads an.
2. Navigieren Sie zur Seite **OT Security**.
3. Laden Sie im Abschnitt Advanced IoT Visibility das Paket Windows IoT Connector Agent herunter.




4. Kopieren Sie das heruntergeladene Palet Windows IoT Connector Agent-Paket auf den Anwendungsserver, auf dem Sie es installieren möchten.
5. Führen Sie den Tenable IoT Connector Agent-Assistenten aus.

   Es wird eine Meldung angezeigt, dass der Connector-Agent-Assistent initialisiert wird, und das Fenster Welcome to the Tenable IoT Connector Agent Setup Wizard wird angezeigt.
6. Klicken Sie auf Weiter.

   Das Fenster License Agreement (Lizenzvereinbarung) wird angezeigt.
7. Wählen Sie I accept the agreement (Ich stimme der Vereinbarung zu) und klicken Sie auf Next.

Das Fenster Select Destination Directory (Zielverzeichnis auswählen) wird angezeigt.

8. Geben Sie das Verzeichnis an, in dem der IoT Connector Agent installiert werden soll (oder verwenden Sie das Standardverzeichnis) und klicken Sie auf Next

   Die Installation des Tenable IoT Connector Agent wird gestartet.

9. Überprüfen Sie nach Abschluss der Installation, ob der Tenable IoT Connector Agent-Dienst ausgeführt wird.

   a. Geben Sie im Fenster zum Ausführen von Befehlen `services.msc` ein.

      Das Fenster Dienste wird geöffnet.

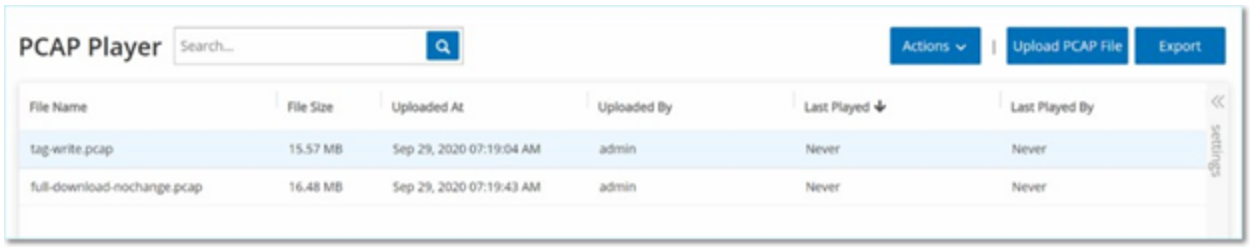
   b. Bestätigen Sie, dass der **OT Security** IoT Connector Agent in der Liste der derzeit ausgeführten Dienste angezeigt wird.

Sobald die Installation abgeschlossen ist, können Sie Ihren Anwendungsserver mit OT Security verbinden. Weitere Informationen zum Herstellen einer Verbindung zum Anwendungsserver über einen Remote-Agent finden Sie unter IoT-Connectors hinzufügen > Über Agent.

## PCAP-Player

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

OT Security ermöglicht es Ihnen, eine PCAP-Datei (Packet Capture, Paketerfassung) mit aufgezeichneter Netzwerkaktivität hochzuladen und auf OT Security „abzuspielen“. Wenn Sie eine PCAP-Datei „abspielen“, überwacht OT Security den Netzwerk-Traffic und zeichnet alle Informationen über erkannte Assets, Netzwerkaktivitäten und Schwachstellen so auf, als ob der Traffic in Ihrem Netzwerk stattgefunden hätte. Sie können diese Funktion zu Simulationszwecken oder zur Analyse von Traffic verwenden, der außerhalb des Netzwerks stattfindet, das von OT Security überwacht wird. Zum Beispiel Remote-Anlagen.




Hinweis: Der PCAP-Player unterstützt die folgenden Dateitypen: `.pcap`, `.pcapng`, `.pcap.gz` und `.pcapng.gz`. Sie können Dateien verwenden, die von einer Instanz von OT Security oder anderen Netzwerküberwachungstools aufgezeichnet wurden.

PCAP-Dateien hochladen

So laden Sie eine PCAP-Datei hoch:

1. Klicken Sie auf der Seite Datenerfassung > Datenquellen auf die Registerkarte PCAP-Player.

   Die Seite PCAP-Player wird angezeigt.

2. Klicken Sie auf PCAP-Datei hochladen.

   Der Datei-Explorer wird geöffnet.

3. Wählen Sie die gewünschte PCAP-Aufzeichnung aus.

4. Klicken Sie auf Öffnen.

   OT Security lädt die PCAP-Datei in das System hoch.

PCAP-Dateien abspielen

So spielen Sie eine PCAP-Datei ab:

1. Klicken Sie auf der Seite Datenerfassung > Datenquellen auf die Registerkarte PCAP-Player.

   Die Seite PCAP-Player wird angezeigt.

2. Wählen Sie die PCAP-Aufzeichnung aus, die Sie abspielen möchten.

3. Klicken Sie auf Aktionen > Abspielen.

   Der Assistent PCAP abspielen wird angezeigt.

4. Wählen Sie im Dropdown-Feld Abspielgeschwindigkeit die Geschwindigkeit aus, mit der das System die Datei abspielen soll.

   Verfügbare Optionen: 1X, 2X, 4X, 8X oder 16X.

   > Hinweis: Durch das Abspielen einer PCAP-Datei werden Daten in das System eingebracht. Sobald dieser Vorgang ausgeführt wird, können Sie ihn nicht mehr rückgängig machen oder anhalten.

5. Klicken Sie auf Abspielen.

   Das System spielt die PCAP-Datei ab. Alle Netzwerkaktivitäten in der PCAP-Datei werden im System registriert und vom System identifizierte Assets werden dem Asset-Inventar hinzugefügt.

   > Hinweis: Sie können keine andere PCAP-Datei abspielen, während bereits eine Datei abgespielt wird.

## Manuelle Uploads

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Site-Operator

Die Registerkarte Manuelle Uploads enthält die folgenden Informationen:

- Asset-Details per CSV aktualisieren
- Assets manuell hinzufügen
- SCD-Dateien
- Rockwell-Projektdateien

## Asset-Details per CSV aktualisieren

Sie können eine CSV-Datei der Tabelle „Alle Assets“ exportieren, Änderungen vornehmen und sie dann hochladen. Zu den bearbeitbaren Feldern gehören: Typ, Name, Kritikalität, Purdue-Level, Standort, Beschreibung und alle benutzerdefinierten Felder.

Sie können Asset-Details nur dann über eine CSV-Datei aktualisieren, wenn die Sprache auf Englisch eingestellt ist. Benutzer, die eine andere Sprache als Englisch verwenden, können beim Exportieren und Hochladen der CSV-Datei vorübergehend zu Englisch wechseln und anschließend wieder ihre bevorzugte Sprache einstellen.

So laden Sie die CSV-Datei mit Asset-Details hoch:

1. Klicken Sie auf der Seite Datenerfassung > Datenquellen auf die Registerkarte Manuelle Uploads.
2. Klicken Sie im Abschnitt Asset-Details per CSV aktualisieren auf Hochladen.
3. Navigieren Sie zum Speicherort der CSV-Datei und laden Sie sie hoch.

## Assets manuell hinzufügen

Um Ihr Inventar zu verfolgen, sollten Sie eventuell einige zusätzliche Assets anzeigen, die Sie besitzen, auch wenn diese Assets noch nicht von OT Security erkannt wurden. Sie können diese Assets manuell zu Ihrem Inventar hinzufügen, indem Sie eine CSV-Datei herunterladen und bearbeiten und die Datei dann in das System hochladen. Sie können nur Assets hochladen, deren IP-Adressen noch nicht von einem vorhandenen Asset im System verwendet werden. Falls das System ein Asset erkennt, das mit derselben IP über das Netzwerk kommuniziert, verwendet es die über das erkannte Asset abgerufenen Informationen und überschreibt die zuvor hochgeladenen Informationen. Das System behandelt das Asset als reguläres Asset, sobald es erkennt, dass das Asset im Netzwerk kommuniziert.

Die IP-Adressen hochgeladener Assets werden als Teil der Systemlizenzierung gezählt.

Für hochgeladene Assets wird der Risikowert 0 angezeigt, bis OT Security diese Assets erkennt.

Hinweis: Für manuell hinzugefügte Assets werden keine Ereignisse erkannt, bis OT Security erkennt, dass sie über das Netzwerk kommunizieren.

So fügen Sie Assets manuell hinzu:

1. Gehen Sie zu Datenerfassung > Datenquellen.

   Die Seite Datenquellen wird angezeigt.

2. Navigieren Sie auf der Registerkarte Manuelle Uploads zum Abschnitt Assets manuell hinzufügen.

3. Wählen Sie im Menü Aktionen die Option CSV-Vorlage herunterladen aus.

   OT Security lädt das Vorlagendokument „tot_Assets“ herunter.

4. Öffnen Sie das Vorlagendokument `tot_Assets`.

5. Bearbeiten Sie die Vorlage `tot_Assets` genau gemäß den Anweisungen in der Datei und behalten Sie nur die Spaltenüberschriften (etwa Name und Typ) und die von Ihnen angegebenen Werte bei.

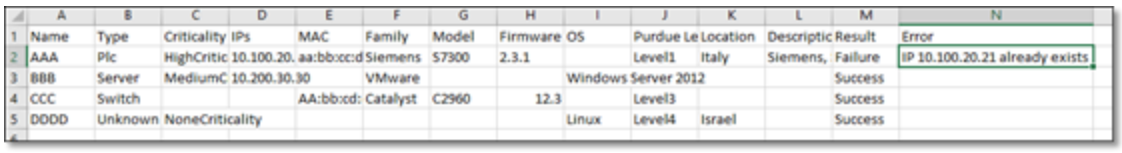
6. Speichern Sie die bearbeitete Datei.

7. Kehren Sie zur Seite Asset-Einstellungen zurück.

8. Wählen Sie im Menü Aktionen die Option CSV-Datei hochladen aus, navigieren Sie zu der gewünschten CSV-Datei und öffnen Sie sie, um sie hochzuladen.

9. Klicken Sie unter Assets manuell hinzufügen auf Bericht herunterladen.

   Daraufhin wird eine CSV-Datei mit dem Bericht angezeigt, die Erfolge und Fehler in der Spalte „Ergebnis“ angibt. Einzelheiten zu Fehlern befinden sich in der Spalte „Fehler“.



| | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Name | Type | Criticality | IPs | MAC | Family | Model | Firmware | OS | Purdue Le | Location | Descriptic | Result | Error |
| 2 | AAA | Plc | HighCritic | 10.100.20. | aa:bb:cc:d | Siemens | S7300 | 2.3.1 | | Level1 | Italy | Siemens, | Failure | IP 10.100.20.21 already exists |
| 3 | BBB | Server | MediumC | 10.200.30. | 30 | VMware | | | Windows Server 2012 | | | | Success | |
| 4 | CCC | Switch | | | AA:bb:cd: | Catalyst | C2960 | 12.3 | | Level3 | | | Success | |
| 5 | DDDD | Unknown | NoneCriticality | | | | | | Linux | Level4 | Israel | | Success | |

## SCD-Dateien

Die SCD-Datei (Substation Configuration Description) enthält die vollständigen kommunikationsbezogenen Details für eine Unterstation. Sie können jetzt eine SCD-Datei in OT Security hochladen und Einblick in Ihre Assets, die IEC 61850-Konfiguration und Sicherheitserkenntnisse über Ihre Umgebung erhalten.

Basierend auf den Informationen in der SCD-Datei meldet OT Security Feststellungen im Zusammenhang mit einer Fehlkonfiguration der Unterstation wie z. B. folgende:

- Zugriff auf MMS-Berichte (Manufacturing Message Specification) von nicht autorisierten Clients
- Nicht autorisierte Clients, die in der SCD-Datei nicht erwähnt werden und versuchen, MMS-Berichte zu abonnieren

> Hinweis: OT Security unterstützt für SCD-Dateien nur die folgenden Formate:
>
> - Substation Configuration Language(SCL)-Versionen 1.0 und 2.0
> - SCD-Dateien mit nur einer Unterstation

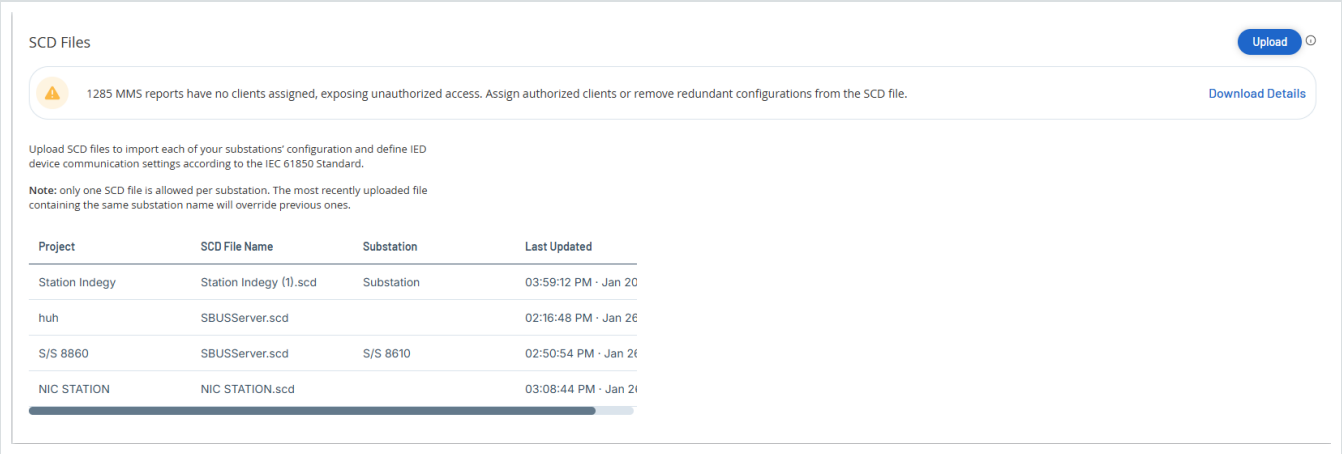
### So laden Sie eine SCD-Datei hoch:

1. Gehen Sie zu Datenerfassung > Datenquellen.

   Die Seite Datenquellen wird angezeigt.

2. Navigieren Sie auf der Registerkarte Manuelle Uploads zum Abschnitt SCD-Dateien.

3. Klicken Sie im Abschnitt SCD-Dateien auf Hochladen.




> Hinweis: Sie können nur eine SCD-Datei pro Unterstation hochladen. Die zuletzt hochgeladene Datei mit demselben Unterstationsnamen überschreibt die vorherige Datei.

4. Navigieren Sie zu der hochzuladenden Datei und wählen Sie sie aus.

   OT Security lädt die SCD-Datei hoch und zeigt die Asset-Details auf den Registerkarten Inventar > Details und IEC 61850 an. Jede Fehlkonfiguration in der SCD-Datei löst ein Ereignis aus und führt dazu, dass oben auf den Seiten Details und IEC 61850 eine Fehlermeldung zu nicht autorisiertem Zugriff angezeigt wird.

5. (Optional) Um die Feststellungsdetails herunterzuladen, klicken Sie in der Fehlermeldung auf Details herunterladen.

   OT Security lädt die Details im CSV-Format herunter.

## Rockwell-Projektdateien

Sie können Rockwell `.L5X`-Dateien hochladen, um Assets zu erstellen, Asset-Details anzureichern und Beziehungen zwischen Assets in Air-Gapped- oder Umgebungen mit eingeschränkter Sichtbarkeit aufzubauen. Die maximale Projektdateigröße beträgt 50 MiB.

> Wichtig: Standardmäßig ist `ProjectFilePopulatePrimaryLayerAssetIPs` auf `Wahr` und `ProjectFilePopulateNonPrimaryLayerAssetIPs` auf `Falsch` festgelegt. Beim Hochladen mehrerer Projektdateien, die Assets mit identischen IP-Adressen enthalten, werden duplizierte

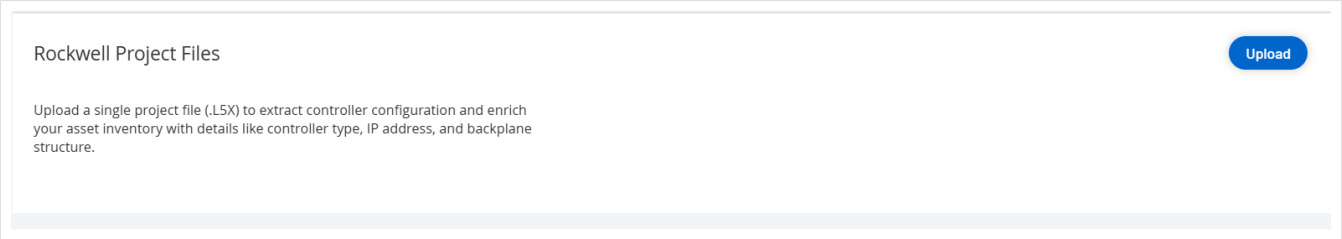
Assets aufgelöst, indem Sie den Konfigurationsparameter `ProjectFilePopulateNonPrimaryLayerAssetIPs` auf `Wahr` setzen. Dadurch kann das System die IP-Adressen von Assets in der nicht primären Ebene anzeigen, sodass Assets mit identischer IP-Adresse als ein einzelnes Asset aufgelöst und korrekt auf derselben Backplane positioniert werden können. Wenn Sie die Konfiguration ändern möchten, wenden Sie sich an Tenable Support.

So laden Sie eine Rockwell-Datei hoch:

1. Gehen Sie zu Datenerfassung > Datenquellen.

   Die Seite Datenquellen wird angezeigt.

2. Navigieren Sie auf der Registerkarte Manuelle Uploads zum Abschnitt Rockwell-Projektdateien.




3. Klicken Sie auf Hochladen.

4. Navigieren Sie zu der hochzuladenden Datei und wählen Sie sie aus.

   OT Security lädt die Rockwell-Projektdatei hoch und zeigt die Asset-Details auf den Registerkarten Inventar > Details an.

# Einstellungen

Der Abschnitt Einstellungen in OT Security enthält die meisten Konfigurationsseiten für OT Security:

Aktive Abfragen – Abfragefunktionen aktivieren/deaktivieren und ihre Frequenz und Einstellungen anpassen. Siehe Aktive Abfragen

Sensoren – Sensoren anzeigen und verwalten, eingehende Sensor-Kopplungsanforderungen genehmigen oder löschen und aktive Abfragen konfigurieren, die von Sensoren durchgeführt werden. Siehe Sensoren.

Systemkonfiguration

- Gerät – Gerätedetails und Netzwerkinformationen anzeigen und bearbeiten. Zum Beispiel Systemzeit, automatisches Ausloggen (d. h. Zeitüberschreitung bei Inaktivität).

  > Hinweis: Sie können DNS-Server in Tenable Core konfigurieren. Weitere Informationen finden Sie unter Manually Configure a Static IP Address im Tenable Core + Tenable OT Security Benutzerhandbuch.

- Portkonfiguration – Konfiguration der Ports auf dem Gerät anzeigen. Weitere Informationen zur Portkonfiguration finden Sie unter Gerät.

- Updates – Updates von Plugins durchführen, entweder automatisch oder manuell über die Cloud oder offline.

- Zertifikat – Informationen zu Ihrem HTTPS-Zertifikat anzeigen und eine sichere Verbindung sicherstellen, indem Sie entweder ein neues HTTPS-Zertifikat im System generieren oder Ihr eigenes hochladen. Siehe Systemkonfiguration.

- API-Schlüssel – API-Schlüssel generieren, um Apps von Drittanbietern den Zugriff auf OT Security über die API zu ermöglichen. Alle Benutzer können API-Schlüssel erstellen. Der API-Schlüssel verfügt über dieselben Berechtigungen wie der Benutzer, der ihn erstellt hat, abhängig von dessen Rolle. Ein API-Schlüssel wird nur einmal angezeigt, nämlich wenn er

generiert wird. Sie müssen ihn zur späteren Verwendung an einem sicheren Ort speichern. Siehe API-Schlüssel generieren.

- Lizenz – Ihre Lizenz anzeigen, aktualisieren und verlängern. Siehe Lizenz.

Umgebungs Einstellungen

- **Netzwerkdefinitionen**
  - Passives Monitoring – Passives Monitoring aktivieren, damit OT Security Assets erfassen kann. Siehe Passives Monitoring.
  - Asset-Details per CSV aktualisieren – Die Details von Assets mithilfe einer CSV-Vorlage aktualisieren. Siehe Asset-Details per CSV aktualisieren.
  - Assets manuell hinzufügen – Der Asset-Liste mithilfe einer CSV-Vorlage neue Assets hinzufügen. Siehe Assets manuell hinzufügen.

  > Hinweis: Maximal können 128 IP-Bereiche an den Tenable Network Monitor gesendet werden, daher empfiehlt Tenable, diese Grenze nicht zu überschreiten. Zusätzlich zu den angegebenen IP-Bereichen werden alle Hosts in den Subnetzen der OT Security-Plattform oder alle Geräte, die Aktivitäten ausführen, als Asset eingestuft.

- Überwachtes Netzwerk – Die Aggregation von IP-Bereichen, in denen das System Assets klassifiziert, anzeigen und bearbeiten. Siehe Überwachte Netzwerke.
- Ausgeblendete Assets – Eine Liste der ausgeblendeten Assets im System anzeigen. Dies sind Assets, die aus den Asset-Listen entfernt wurden, siehe Inventar. Sie können ausgeblendete Assets über diese Seite wiederherstellen.
- Benutzerdefinierte Felder – Benutzerdefinierte Felder erstellen, um Assets mit relevanten Informationen zu taggen. Ein benutzerdefiniertes Feld kann Klartext oder ein Link zu einer externen Ressource sein.
- Ereigniscluster – Mehrere ähnliche Ereignisse, die innerhalb eines bestimmten Zeitraums auftreten, zusammenfassen, um ihre Überwachung zu vereinfachen. Siehe Ereigniscluster.

- PCAP-Player – Eine PCAP-Datei mit aufgezeichneter Netzwerkaktivität hochladen und auf OT Security „abspielen“, wobei die Daten in Ihr System geladen werden. Siehe PCAP-Player.
- Benutzer und Rollen – Informationen zu allen Benutzerkonten anzeigen, bearbeiten und exportieren.
    - Benutzereinstellungen – Informationen zu dem derzeit beim System eingeloggten Benutzer anzeigen und bearbeiten (vollständiger Name, Benutzername und Passwort) und die Sprache der Benutzeroberfläche ändern (Englisch, Japanisch, Chinesisch, Französisch oder Deutsch).
    - Lokale Benutzer – Ein Administratorbenutzer kann lokale Benutzerkonten für bestimmte Benutzer erstellen und dem Konto eine Rolle zuweisen. Siehe Benutzerverwaltung.
    - Benutzergruppen – Ein Administratorbenutzer kann Benutzergruppen anzeigen, bearbeiten, hinzufügen und löschen. Siehe Benutzerverwaltung.
    - Authentifizierungsserver – Zugangsdaten von Benutzern können optional über einen LDAP-Server wie beispielsweise Active Directory zugewiesen werden. In diesem Fall werden die Benutzerrechte in Active Directory verwaltet. Siehe Benutzerverwaltung.
- Integrationen – Integration mit anderen Plattformen einrichten. OT Security unterstützt derzeit die Integration in Palo Alto Networks Next Generation Firewall (NGFW) und Aruba ClearPass sowie in andere Tenable-Produkte (Tenable Security Center und Tenable Vulnerability Management). Siehe Integrationen.
- Server – In Ihrem System konfigurierte Server anzeigen, erstellen und bearbeiten. Es sind separate Bildschirme für Folgendes verfügbar:
    - SMTP-Server – SMTP-Server ermöglichen das Versenden von Ereignisbenachrichtigungen per E-Mail.

- Syslog-Server – Syslog-Server ermöglichen das Protokollieren von Ereignisprotokollen auf einem externen SIEM-System.
- FortiGate-Firewalls – Mit der OT Security-FortiGate-Integration können Sie auf der Grundlage der OT Security-Netzwerkereignisse Vorschläge für Firewall-Richtlinien an eine FortiGate-Firewall senden.

- Systemaktionen – Zeigt ein Untermenü mit Systemaktivitäten an. Das Untermenü enthält die folgenden Optionen:
  - Auf Werkseinstellungen zurücksetzen – Setzt alle Einstellungen auf die standardmäßigen Werkseinstellungen zurück. Nur ein Administrator oder Sicherheitsmanager kann eine Zurücksetzung auf die Werkseinstellungen vornehmen.

    > Achtung: Dieser Vorgang kann nicht rückgängig gemacht werden und alle Daten im System gehen verloren.

    Die folgenden Optionen sind jetzt in Tenable Core verfügbar:
    - Systemsicherung – Ab Version 3.18 können Sie zum Sichern und Wiederherstellen von OT Security die Seite Backup/Restore (Sichern/Wiederherstellen) in Tenable Core verwenden. Weitere Informationen finden Sie unter Application Data Backup and Restore.Informationen zur Wiederherstellung über die CLI finden Sie unter Sicherung mithilfe der CLI wiederherstellen.
    - Einstellungen exportieren – Exportiert die Konfigurationseinstellungen der OT Security-Plattform als `NDG`-Datei auf den lokalen Computer. Dies dient als Backup im Falle einer Systemzurücksetzung oder ermöglicht das Importieren der Einstellungen in eine neue OT Security-Plattform.
    - Einstellungen importieren – Importiert die Konfigurationseinstellungen der OT Security-Plattform, die als `NDG`-Datei auf dem lokalen Computer gespeichert wurden.

- Diagnosedaten herunterladen – Erstellt eine Datei mit Diagnosedaten auf der OT Security-Plattform und speichert sie auf dem lokalen Computer.
- Neu starten – Startet die OT Security-Plattform neu. Dies ist für die Aktivierung bestimmter Konfigurationsänderungen erforderlich.
- Deaktivieren – Deaktiviert alle Überwachungsaktivitäten. Sie können die Überwachungsaktivitäten jederzeit wieder aktivieren.
- Herunterfahren – Fährt die OT Security-Plattform herunter. Drücken Sie zum Einschalten die Power-Taste auf der OT Security Appliance.

- Systemprotokoll – Zeigt ein Protokoll aller Systemereignisse an, die im System aufgetreten sind. Beispiele: Richtlinie aktiviert, Richtlinie bearbeitet und Ereignis aufgelöst. Sie können das Protokoll als CSV-Datei exportieren oder an einen Syslog-Server senden. Siehe Systemprotokoll.

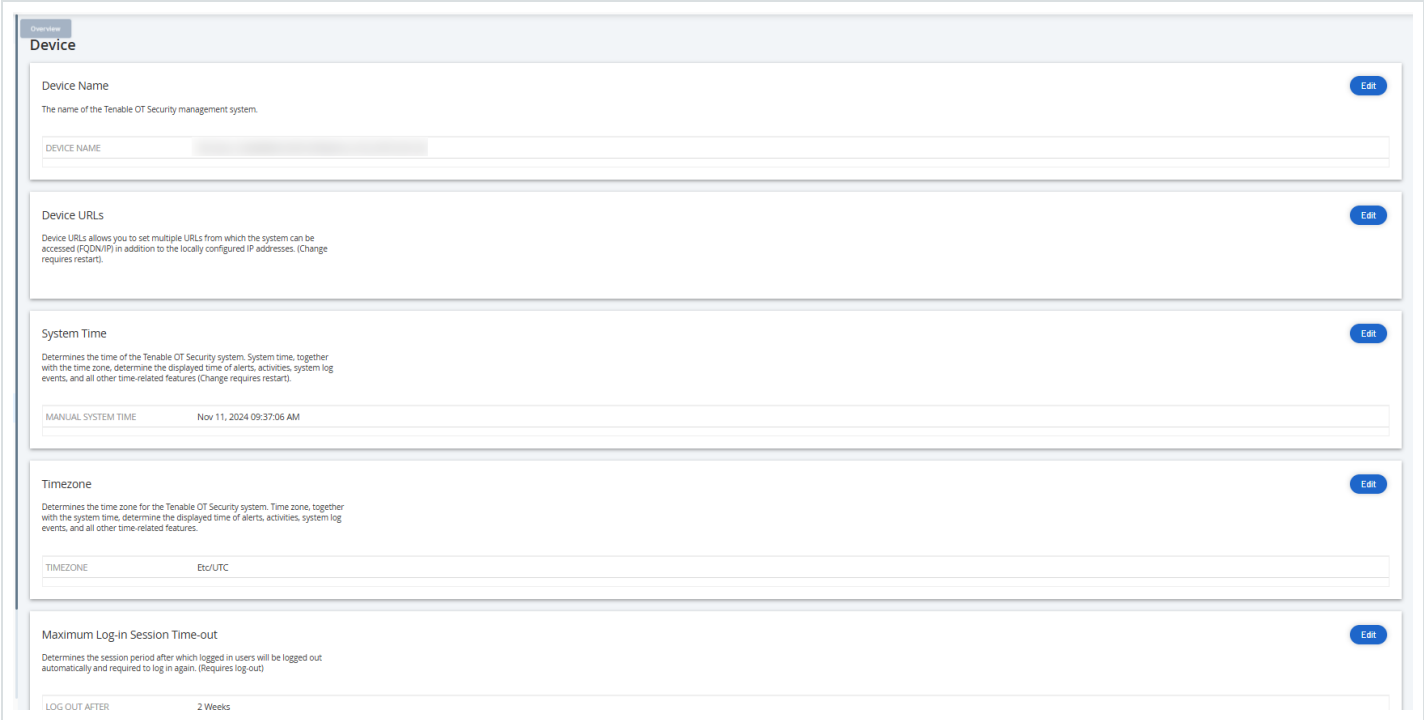
## Systemkonfiguration

Die Seiten zur Systemkonfiguration von OT Security ermöglichen es Ihnen, Plugin-Updates automatisch zu konfigurieren und manuell durchzuführen sowie Details zu Ihrem Gerät, HTTPS-Zertifikat, den API-Schlüsseln und der Lizenz anzuzeigen und zu aktualisieren.

### Gerät

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

Die Seite Gerät enthält detaillierte Informationen zu Ihrer OT Security-Konfiguration. Sie können auf dieser Seite die Konfiguration anzeigen und bearbeiten.




## Gerätename

Ein eindeutiger Bezeichner für die OT Security Appliance.

## Geräte-URLs

Hier können Sie die einzelne URL festlegen, über die auf das System zugegriffen werden kann (FQDN).

> Wichtig: Eine Bearbeitung der Geräte-URL ist eine kritische Änderung. Der neue FQDN wird nicht noch einmal angezeigt. Wenn Sie sich die exakte Zeichenfolge nicht notieren, wird die Benutzeroberfläche unzugänglich. Prüfen Sie unbedingt die Auflösung, bevor Sie fortfahren.

## Systemzeit

Die richtige Uhrzeit und das richtige Datum werden automatisch eingestellt, können jedoch bearbeitet werden.

> Hinweis: Die Einstellung des richtigen Datums und der richtigen Uhrzeit ist für die genaue Aufzeichnung von Protokollen und Warnungen unerlässlich.

### Maximales Timeout von Login-Sitzung

Der Sitzungszeitraum, nach dem Benutzer automatisch ausgeloggt werden und sich erneut einloggen müssen. Um den Timeout-Zeitraum für die Login-Sitzung zu ändern, klicken Sie auf Bearbeiten. Verfügbare Optionen für den Zeitraum: 2 Wochen, 30 Minuten, 1 Stunde, 4 Stunden, 12 Stunden, 1 Tag, 1 Woche und 2 Wochen.

### Maximales Timeout bei Inaktivität

Der Inaktivitätszeitraum, nach dem eingeloggte Benutzer automatisch ausgeloggt werden und sich erneut einloggen müssen. Um den Inaktivitätszeitraum zu ändern, klicken Sie auf Bearbeiten.

### Zeitraum, nach dem offene Ports als veraltet gelten

Legt den Zeitraum fest, nach dem Auflistungen offener Ports aus dem Bildschirm mit individuellen Asset-Details entfernt werden, wenn kein weiterer Hinweis darauf eingeht, dass der Port noch offen ist. Die Standardeinstellung ist zwei Wochen. Weitere Informationen finden Sie unter Inventar.

### Ping-Anfragen

Durch Aktivieren von Ping-Anfragen wird die automatische Antwort der OT Security-Plattform auf Ping-Anfragen aktiviert.

Klicken Sie auf den Umschalter Ping-Anfragen, um Ping-Anfragen zu aktivieren.

### Paketerfassung

Durch Einschalten der Funktion zur vollständigen Paketerfassung wird die kontinuierliche Aufzeichnung von vollständigen Paketerfassungen des gesamten Traffic im Netzwerk aktiviert. Dadurch sind umfangreiche Möglichkeiten zur Fehlersuche und forensischen Untersuchung gegeben. Wenn die Speicherkapazität 1,8 TB überschreitet, löscht das System ältere Dateien. Sie können verfügbare Dateien auf der Seite Netzwerk > Paketerfassungen anzeigen und herunterladen, siehe Abschnitt Netzwerk.

Klicken Sie auf den Umschalter Paketerfassung, um Paketerfassungen zu aktivieren.

Hinweis: Sie können die Paketerfassungsfunktion jederzeit beenden, indem Sie den Umschalter auf AUS stellen.

### Sensorkopplungsanforderungen automatisch genehmigen

Die Aktivierung der automatischen Genehmigung eingehender Sensorkopplungsanforderungen stellt sicher, dass alle Sensorkopplungsanforderungen genehmigt werden, ohne dass zusätzliche Schritte vom Administrator ausgeführt werden müssen. Wenn diese Option nicht aktiviert ist, ist eine abschließende manuelle Genehmigung erforderlich, damit sich neue Sensoren mit Ihrem Netzwerk verbinden können.

Klicken Sie auf den Umschalter Sensorkopplungsanforderungen automatisch genehmigen, um die automatische Genehmigung für eingehende Sensorkopplungsanforderungen zu aktivieren.

### Klassifizierungsbanner

Fügen Sie OT Security ein Banner hinzu, um die Daten anzugeben, auf die über die Software zugegriffen werden kann.

Um ein Banner hinzuzufügen, klicken Sie auf Bearbeiten. Klicken Sie nach dem Hinzufügen des Banners auf den Umschalter Klassifizierungsbanner, um ihn zu aktivieren.

### Nutzungsstatistiken aktivieren

Mit der Option Nutzungsstatistiken aktivieren wird festgelegt, ob Tenable anonyme Telemetriedaten über Ihre OT Security-Bereitstellung erfasst. Wenn diese Option aktiviert ist, erfasst Tenable Telemetriedaten, die keiner bestimmten Person zugeordnet werden können. Die Daten werden nur auf Unternehmensebene erhoben. Diese Informationen enthalten keine persönlichen Daten oder personenbezogenen Informationen (PII). Telemetriedaten umfassen unter anderem Angaben zu den von Ihnen besuchten Seiten, den von Ihnen verwendeten Berichten und Dashboards und den von Ihnen konfigurierten Funktionen. Tenable verwendet die Daten, um Ihre Benutzererfahrung in zukünftigen OT Security-Versionen zu verbessern sowie für andere angemessene Geschäftszwecke in Übereinstimmung mit dem Tenable-Rahmenvertrag. Diese Einstellung ist standardmäßig aktiviert.

Klicken Sie auf den Umschalter Nutzungsstatistiken aktivieren, um die Erfassung von Telemetriedaten zu aktivieren.

> Hinweis: Sie können das Teilen von Nutzungsstatistiken jederzeit deaktivieren, indem Sie auf den Umschalter klicken.

### GraphQL Playground

Eine browserinterne GraphQL-IDE. Mit diesem Umschalter können Sie die Verwendung des Playgrounds in der Produktion aktivieren oder deaktivieren, um Ihre API-Abfragen zu testen.

## Portkonfiguration

Ab Version 4.1 können Sie die Tenable Core-Schnittstelle für Split-Ports an Port 8000 überprüfen und konfigurieren.

## Einstellungen für das Compliance-Dashboard festlegen

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

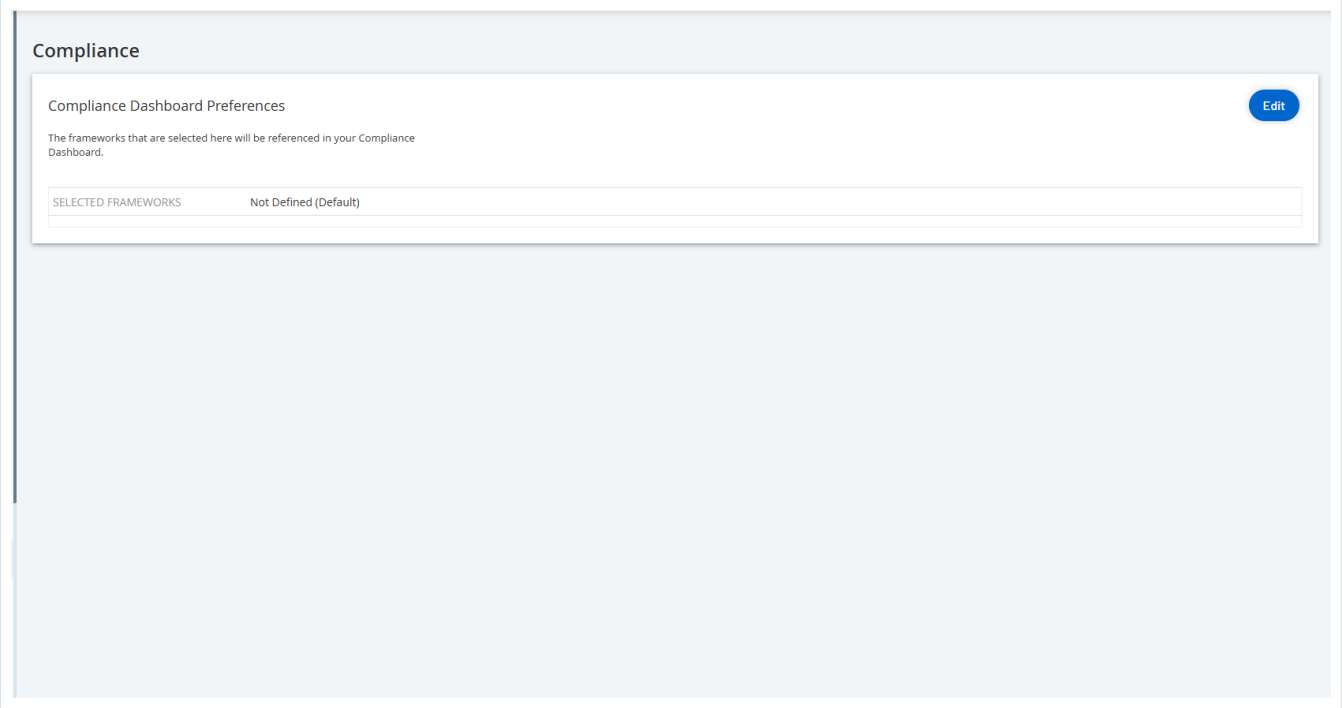
Sie können die Sicherheits-Frameworks angeben, auf die sich das Compliance-Dashboard beim Generieren der Daten stützen soll.

### So legen Sie die Einstellungen für das Compliance-Dashboard fest:

1. Führen Sie einen der folgenden Schritte aus:

    - Gehen Sie zu Einstellungen > Systemkonfiguration > Compliance.
    - Klicken Sie auf der Dashboard-Seite Compliance auf den Link Präferenzen für das Sicherheits-Framework.

    Daraufhin wird die Seite mit den Compliance-Einstellungen angezeigt.




2. Klicken Sie im Abschnitt Compliance-Dashboard-Einstellungen auf Bearbeiten.

   Der Fensterbereich Referenzierte Compliance-Frameworks bearbeiten wird angezeigt.

3. Wählen Sie die gewünschten Compliance-Frameworks aus. Sie können aus den folgenden Optionen wählen.

   - ISO 27001-Kontrollen
   - CAF-Prinzipien
   - OTCC-Subdomains:
   - NIS 2-Richtlinie (Artikel 21)
   - NERC-CIP-Anforderungen
   - IEC-62443-3-3-Anforderungen

4. Klicken Sie auf Speichern.

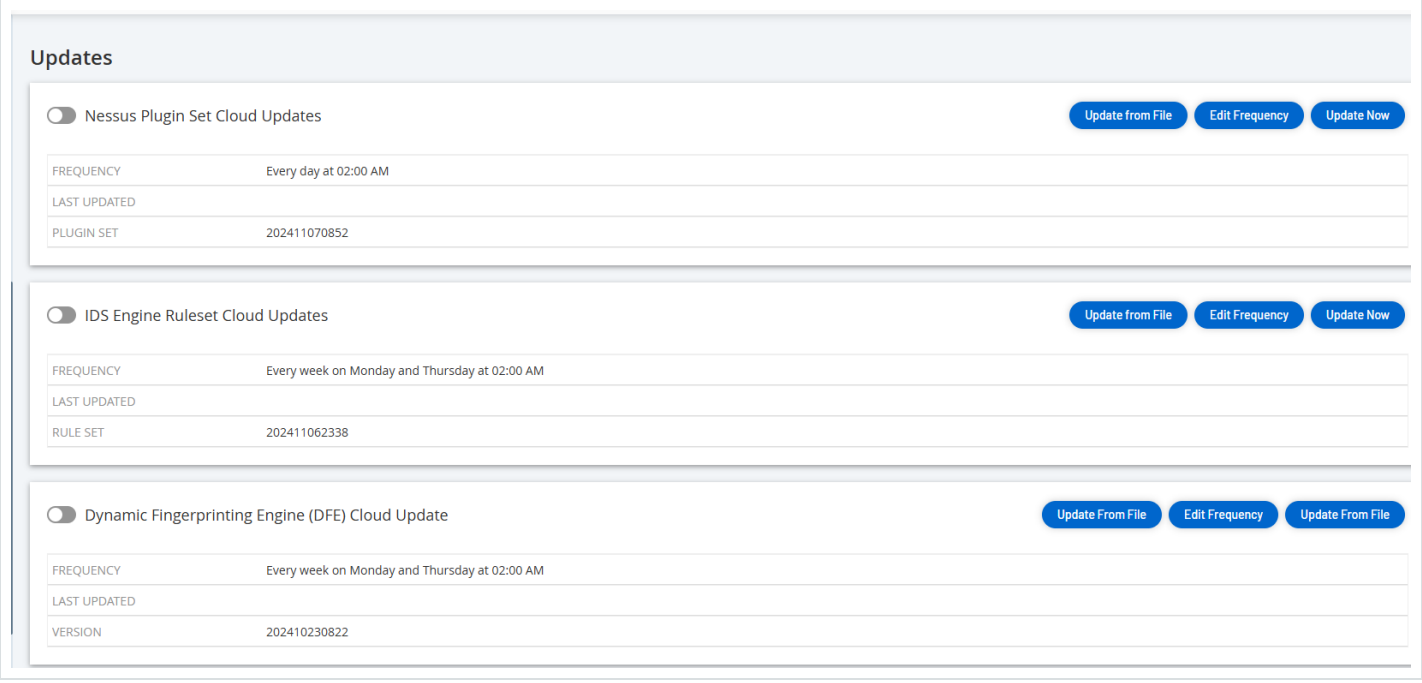
OT Security speichert die Einstellungen für das Compliance-Framework und überprüft die Compliance Ihrer Organisation anhand der festgelegten Einstellungen. OT Security zeigt die Ergebnisse der Compliance-Prüfungen im Compliance-Dashboard an.

## Updates

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager

Durch die Aktualisierung von Tenable Nessus-Plugins und des Regelsatzes der IDS-Engine (Intrusion Detection System) auf die neuesten Versionen wird sichergestellt, dass OT Security Ihre Assets auf die neuesten bekannten Schwachstellen überwacht. OT Security bietet eine Option zum Aktualisieren von Klassifizierung, Familie und Abdeckung über Dynamic Fingerprinting Engine (DFE)-Cloud-Updates. Sie können Updates über die Cloud – sowohl automatisch als auch manuell – und auch offline durchführen.

Hinweis: Informationen zum Aktualisieren von Tenable Core finden Sie unter Updates verwalten im Benutzerhandbuch für Tenable Core und OT Security.



Hinweis: Sie können Updates auch unter Schwachstellen > Plugins aktualisieren vornehmen.

Hinweis: Wenn die Benutzerlizenz abläuft, wird die Option zum Herunterladen neuer Updates blockiert und Plugins können nicht aktualisiert werden.

## Updates des Tenable Nessus-Plugin-Satzes

### Automatische Cloud-Updates von Plugins festlegen

### So aktivieren Sie automatische Updates von Plugins:

1. Gehen Sie zu Einstellungen > Systemkonfiguration > Updates.

   Das Fenster Updates wird angezeigt. Im Bereich Cloud-Updates für Nessus-Plugin-Satz werden die Nummer Ihres Plugin-Satzes, das Datum der letzten Aktualisierung und der Update-Zeitplan angezeigt.

2. Klicken Sie auf den Umschalter Cloud-Updates für Nessus-Plugin-Satz, um automatische Updates zu aktivieren.

### Frequenz von Plugin-Updates bearbeiten

1. Gehen Sie zu Einstellungen > Systemkonfiguration > Updates.

   Das Fenster Updates wird angezeigt. Im Bereich Cloud-Updates für Nessus-Plugin-Satz werden die Nummer Ihres Plugin-Satzes, das Datum der letzten Aktualisierung und der Update-Zeitplan angezeigt.

2. Klicken Sie auf Frequenz bearbeiten.

   Der Seitenbereich Frequenz bearbeiten wird angezeigt.


3. Legen Sie im Abschnitt Wiederholung alle das Zeitintervall fest, in dem Sie die Plugins aktualisieren möchten, indem Sie eine Zahl eingeben und eine Zeiteinheit (Tage oder Wochen) im Dropdown-Feld auswählen.

   Bei Auswahl von Wochen wählen Sie die Wochentage aus, an denen Sie ein wöchentliches Update der Plugins durchführen möchten.

4. Legen Sie im Abschnitt Um die Tageszeit fest, zu der Sie die Plugins aktualisieren möchten (im Format HH:MM:SS). Klicken Sie hierzu auf das Uhrsymbol und wählen Sie die Uhrzeit aus oder geben Sie die Uhrzeit manuell ein.

5. Klicken Sie auf Speichern.

   Es wird eine Meldung mit der Bestätigung angezeigt, dass die Frequenz erfolgreich aktualisiert wurde.

Manuelle Cloud-Updates von Plugins durchführen

So aktualisieren Sie Plugins manuell:

1. Gehen Sie zu Einstellungen > Systemkonfiguration > Updates.

   Die Seite Updates wird angezeigt. Im Bereich Cloud-Updates für Nessus-Plugin-Satz werden die Nummer Ihres Plugin-Satzes, das Datum der letzten Aktualisierung und der Update-Zeitplan angezeigt.

2. Klicken Sie auf Jetzt aktualisieren.

   In einer Meldung wird bestätigt, dass die Aktualisierung ausgeführt wird. Wenn das Update abgeschlossen ist, wird im Feld Plugin-Satz die Nummer des aktuellen Plugin-Satzes angezeigt.

   > Tipp: Lassen Sie das Browserfenster geöffnet und aktualisieren Sie die Seite nicht, während das Update des Plugin-Satzes durchgeführt wird.

Offline-Updates

Sollten Sie auf Ihrem OT Security-Gerät nicht über eine Internetverbindung verfügen, können Sie die Plugins manuell aktualisieren, indem Sie den neuesten Plugin-Satz aus dem Tenable Community-Portal herunterladen und die Datei hochladen.

### So aktualisieren Sie Plugins offline:

1. Gehen Sie zu Einstellungen > Systemkonfiguration > Updates.

   Die Seite Updates wird angezeigt. Im Bereich Cloud-Updates für Nessus-Plugin-Satz werden die Nummer Ihres Plugin-Satzes, das Datum der letzten Aktualisierung und der Update-Zeitplan angezeigt.

2. Klicken Sie auf Aus Datei aktualisieren.

Das Fenster Aus Datei aktualisieren wird angezeigt.

3. Sofern Sie dies noch nicht getan haben, klicken Sie auf den Link, um die neueste Plugin-Datei herunterzuladen, und kehren Sie dann zum Fenster Aus Datei aktualisieren zurück.

   > Hinweis: Das Herunterladen der neuesten Plugin-Datei über den Link ist nur über eine Internetverbindung möglich, z. B. mit einem mit dem Internet verbundenen PC.

4. Klicken Sie auf Durchsuchen und navigieren Sie zu der Datei mit dem Plugin-Satz, die Sie aus dem OT Security-Kundenportal heruntergeladen haben.

5. Klicken Sie auf Aktualisieren.

## Updates des IDS-Engine-Regelsatzes

### Automatische Cloud-Updates des IDS-Engine-Regelsatzes festlegen

### So aktivieren Sie automatische Updates des IDS-Engine-Regelsatzes:

1. Gehen Sie zu Einstellungen > Systemkonfiguration > Updates.

   Die Seite Updates wird angezeigt. Im Bereich Cloud-Updates für IDS-Engine-Regelsatz werden die Nummer Ihres Regelsatzes, das Datum der letzten Aktualisierung und der Update-Zeitplan angezeigt.

2. Klicken Sie auf den Umschalter Cloud-Updates für IDS-Engine-Regelsatz, um automatische Updates zu aktivieren.

### Frequenz von Updates des IDS-Engine-Regelsatzes bearbeiten

1. Gehen Sie zu Einstellungen > Systemkonfiguration > Updates.

   Die Seite Updates wird angezeigt. Im Bereich Cloud-Updates für IDS-Engine-Regelsatz werden die Nummer Ihres Regelsatzes, das Datum der letzten Aktualisierung und der Update-Zeitplan angezeigt.

2. Klicken Sie auf Frequenz bearbeiten.

   Der Seitenbereich Frequenz bearbeiten wird angezeigt.


3. Legen Sie im Abschnitt Wiederholung alle das Zeitintervall fest, in dem Sie den Regelsatz aktualisieren möchten, indem Sie eine Zahl eingeben und eine Zeiteinheit (Tage oder Wochen) im Dropdown-Feld auswählen.

   Bei Auswahl von Wochen wählen Sie die Wochentage aus, an denen Sie ein wöchentliches Update des Regelsatzes durchführen möchten.

4. Legen Sie im Abschnitt Um die Tageszeit fest, zu der Sie den IDS-Engine-Regelsatz aktualisieren möchten (im Format HH:MM:SS). Klicken Sie hierzu auf das Uhrsymbol und wählen Sie die Uhrzeit aus oder geben Sie die Uhrzeit manuell ein.

5. Klicken Sie auf Speichern.

   Es wird eine Meldung mit der Bestätigung angezeigt, dass die Frequenz erfolgreich aktualisiert wurde.

Manuelle Cloud-Updates des IDS-Engine-Regelsatzes durchführen

So aktualisieren Sie den IDS-Engine-Regelsatz manuell:

1. Gehen Sie zu Einstellungen > Systemkonfiguration > Updates.

   Die Seite Updates wird angezeigt. Im Bereich Cloud-Updates für IDS-Engine-Regelsatz werden die Nummer Ihres Regelsatzes, das Datum der letzten Aktualisierung und der Update-Zeitplan angezeigt.

2. Klicken Sie auf Jetzt aktualisieren.

   In einer Meldung wird bestätigt, dass die Aktualisierung ausgeführt wird. Wenn das Update abgeschlossen ist, wird im Feld Regelsatz die Nummer des aktuellen IDS-Engine-Regelsatzes angezeigt.

Offline-Updates

Sollten Sie auf Ihrem OT Security-Gerät nicht über eine Internetverbindung verfügen, können Sie Ihren IDS-Engine-Regelsatz manuell aktualisieren, indem Sie den neuesten Regelsatz aus dem Tenable-Kundenportal herunterladen und die Datei hochladen.

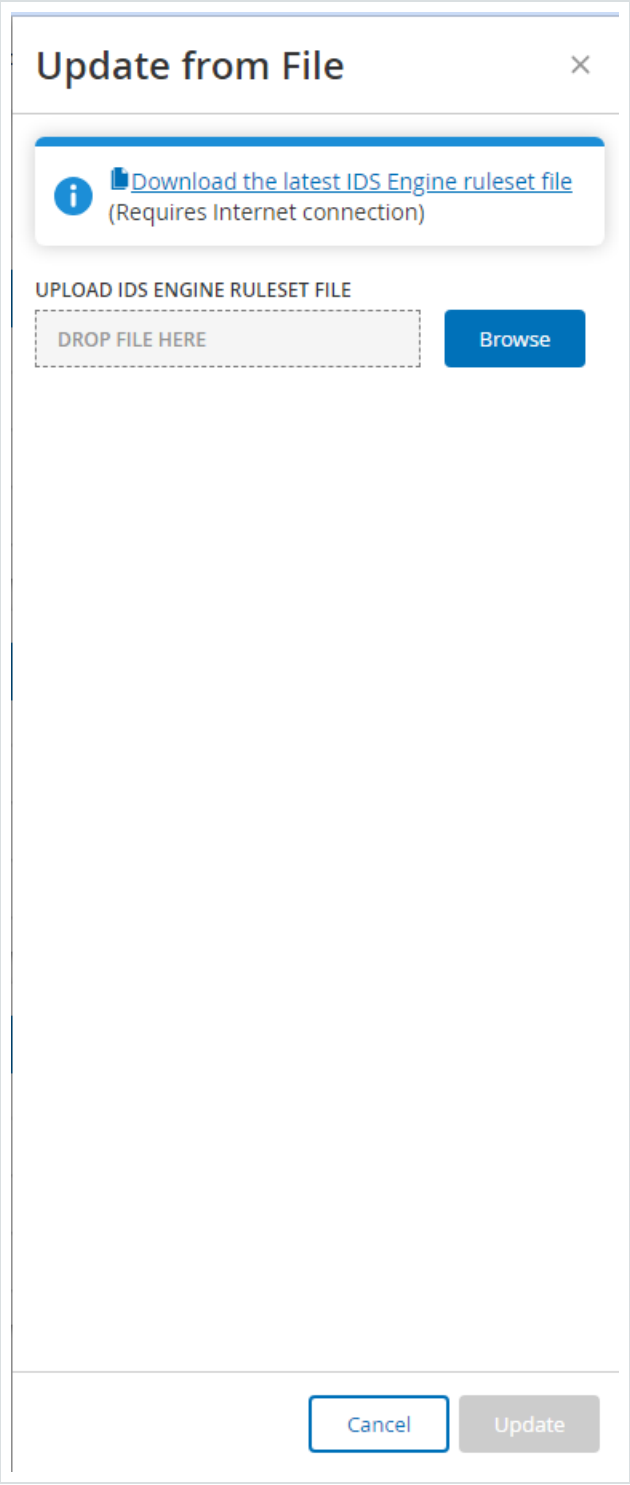
### So aktualisieren Sie den IDS-Engine-Regelsatz offline:

1. Gehen Sie zu Einstellungen > Systemkonfiguration > Updates.

   Das Fenster Updates wird angezeigt. Im Bereich Cloud-Updates für IDS-Engine-Regelsatz werden die Nummer Ihres Regelsatzes, das Datum der letzten Aktualisierung und der Update-Zeitplan angezeigt.

2. Klicken Sie auf Aus Datei aktualisieren.

   Das Fenster Aus Datei aktualisieren wird angezeigt.




3. Falls Sie dies noch nicht getan haben, klicken Sie auf den Link, um die neueste IDS-Engine-Regelsatzdatei herunterzuladen.

> Hinweis: Das Herunterladen der neuesten IDS-Engine-Regelsatzdatei über den Link ist nur über eine Internetverbindung möglich, z. B. über einen mit dem Internet verbundenen PC.

4. Klicken Sie auf Durchsuchen und navigieren Sie zu der IDS-Engine-Regelsatzdatei, die Sie aus dem OT Security-Kundenportal heruntergeladen haben.
5. Klicken Sie auf Aktualisieren.

## DFE-Cloud-Updates

Sie können den Abschnitt Dynamic Fingerprinting Engine (DFE)-Updates verwenden, um Änderungen zu aktualisieren oder eine neue Klassifizierung zu Ihrem OT Security-System hinzuzufügen.

### Automatische DFE-Cloud-Updates festlegen

### So aktivieren Sie automatische DFE-Updates:

1. Gehen Sie zu Einstellungen > Systemkonfiguration > Updates.

   Die Seite Updates wird angezeigt. Im Abschnitt DFE-Cloud-Updates werden die für automatische Updates festgelegte Frequenz, das Datum des letzten Updates und die aktuelle Version des Updates angezeigt.
2. Klicken Sie auf den Umschalter DFE-Cloud-Updates, um automatische Updates zu aktivieren.

### Frequenz von DFE-Updates bearbeiten

1. Gehen Sie zu Einstellungen > Systemkonfiguration > Updates.

   Die Seite Updates wird angezeigt. Im Abschnitt DFE-Cloud-Updates werden die für automatische Updates festgelegte Frequenz, das Datum des letzten Updates und die aktuelle Version des Updates angezeigt.
2. Klicken Sie auf Frequenz bearbeiten.

Der Seitenbereich Frequenz bearbeiten wird angezeigt.

3. Legen Sie im Abschnitt Wiederholung alle das Zeitintervall für das DFE-Update fest, indem Sie eine Zahl eingeben und eine Zeiteinheit (Tage oder Wochen) im Dropdown-Feld auswählen.

   Wenn Sie Wochen auswählen, wählen Sie die Wochentage für das wöchentliche DFE-Update aus.

4. Legen Sie im Abschnitt Um die Tageszeit für das DFE-Update fest (im Format HH:MM:SS). Klicken Sie hierzu auf das Uhrsymbol und wählen Sie die Uhrzeit aus oder geben Sie die Uhrzeit manuell ein.

5. Klicken Sie auf Speichern.

   Es wird eine Meldung mit der Bestätigung angezeigt, dass die Frequenz erfolgreich aktualisiert wurde.

Manuelle DFE-Cloud-Updates durchführen

## So aktualisieren Sie die DFE manuell:

1. Gehen Sie zu Einstellungen > Systemkonfiguration > Updates.

   Die Seite Updates wird angezeigt. Im Abschnitt DFE-Cloud-Updates werden die für automatische Updates festgelegte Frequenz, das Datum des letzten Updates und die aktuelle Version des Updates angezeigt.

2. Klicken Sie auf Jetzt aktualisieren.

   In einer Meldung wird bestätigt, dass die Aktualisierung ausgeführt wird. Wenn das Update abgeschlossen ist, wird im Feld Version die aktuelle DFE-Version angezeigt.

Offline-Updates

Sollten Sie auf Ihrem OT Security-Gerät nicht über eine Internetverbindung verfügen, können Sie die DFE manuell aktualisieren, indem Sie die neueste Version aus dem Tenable-Kundenportal herunterladen und die Datei hochladen.

### So führen Sie ein Offline-DFE-Update durch:

1. Gehen Sie zu Einstellungen > Systemkonfiguration > Updates.

   Das Fenster Updates wird angezeigt. Im Abschnitt DFE-Cloud-Updates werden die für automatische Updates festgelegte Frequenz, das Datum des letzten Updates und die aktuelle Version des Updates angezeigt.

2. Klicken Sie auf Aus Datei aktualisieren.

   Das Fenster Aus Datei aktualisieren wird angezeigt.


3. Falls Sie dies noch nicht getan haben, klicken Sie auf den Link, um die neueste Datei mit Gerätesignaturen herunterzuladen.

Hinweis: Das Herunterladen der neuesten Datei mit Gerätesignaturen über den Link ist nur über eine Internetverbindung möglich, z. B. mit einem mit dem Internet verbundenen PC.

4. Klicken Sie auf Durchsuchen und navigieren Sie zu der Datei mit den Gerätesignaturen, die Sie aus dem OT Security-Kundenportal heruntergeladen haben.
5. Klicken Sie auf Aktualisieren.

### Updates der OT Discovery-Engine (OTD)

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor und Sicherheitsanalyst

OT-Agents verwenden die OT Discovery-Engine (OTD) zum Scannen Ihrer Umgebung. Sie können die OTD-Engines entweder manuell oder automatisch über die Seite Datenquellen > Agents aktualisieren. Bevor Sie die OTD-Engine aktualisieren, müssen Sie zuerst die neueste OTD-Datei in OT Security hochladen.

Bevor Sie beginnen

- Laden Sie die OT Discovery-Engine-Datei aus dem Download-Portal herunter.

### So laden Sie die OTD-Engine-Datei hoch:

1. Gehen Sie zu Einstellungen > Systemkonfiguration > Updates.

   Die Seite Updates wird angezeigt.
2. Klicken Sie im Abschnitt Update der OT Discovery-Engine (OTD) auf Hochladen.

   Der Bereich Datei hochladen wird angezeigt.
3. Klicken Sie auf „Durchsuchen“ und navigieren Sie zu der OTD-Engine-Datei, die Sie aus dem Tenable-Download-Portal heruntergeladen haben.
4. Klicken Sie auf Hochladen.

5. Um die OTD-Engine zu aktualisieren, führen Sie die Schritte unter OT-Agent aktualisieren aus.

## Zertifikate

Erforderliche OT Security-Benutzerrolle: Administrator

### HTTPS-Zertifikat generieren

Das HTTPS-Zertifikat stellt sicher, dass das System eine sichere Verbindung zur OT Security Appliance und zum Server verwendet. Das Erstzertifikat läuft nach zwei Jahren ab. Sie können jederzeit ein neues selbstsigniertes Zertifikat generieren. Das neue Zertifikat ist ein Jahr gültig.

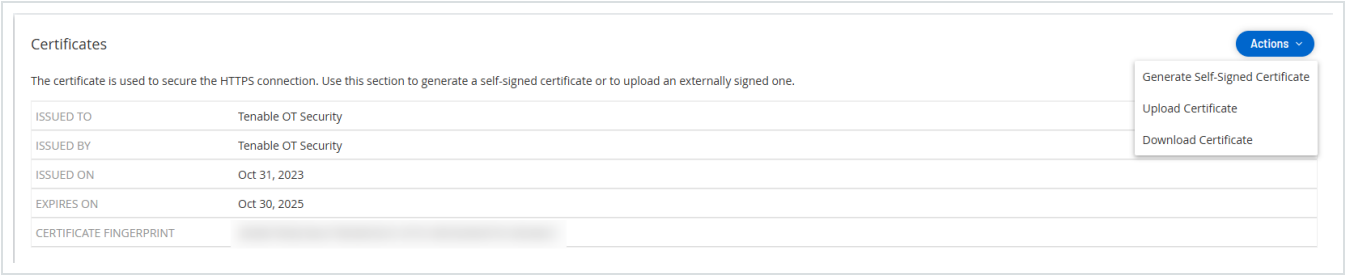
Hinweis: Wenn Sie ein neues Zertifikat generieren, wird das aktuelle Zertifikat überschrieben.

### So generieren Sie ein selbstsigniertes Zertifikat:

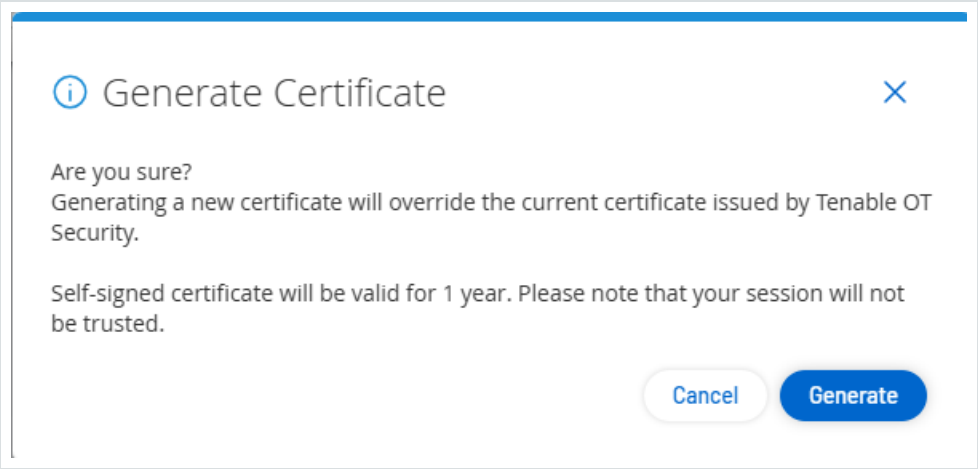
1. Gehen Sie zu Einstellungen > Systemkonfiguration > Zertifikate.

   Das Fenster Zertifikate wird angezeigt.

2. Wählen Sie im Menü Aktionen die Option Selbstsigniertes Zertifikat generieren aus.




   Das Bestätigungsfenster zum Generieren eines Zertifikats wird angezeigt.




3. Klicken Sie auf Generieren.

   OT Security generiert das selbstsignierte Zertifikat, das Sie auf der Seite Zertifikate einsehen können.

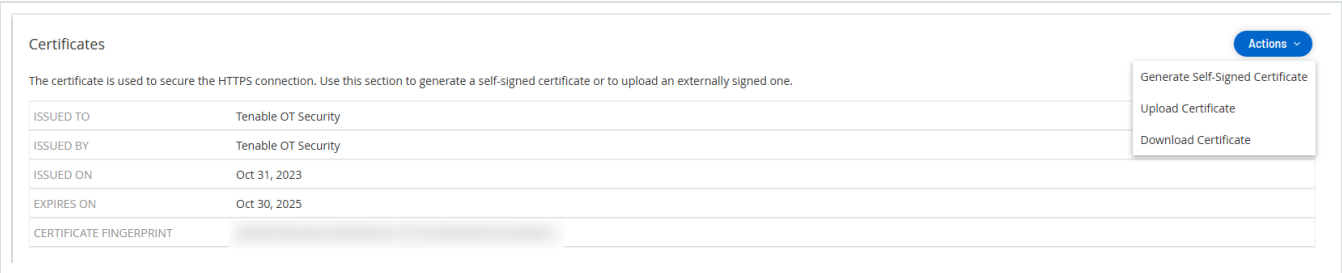
## HTTPS-Zertifikat hochladen

So laden Sie ein HTTPS-Zertifikat hoch:

1. Gehen Sie zu Einstellungen > Systemkonfiguration > Zertifikate.

   Das Fenster Zertifikate wird angezeigt.

2. Wählen Sie im Menü Aktionen die Option Zertifikat hochladen aus.




   Der Seitenbereich Zertifikat hochladen wird angezeigt.

3. Klicken Sie im Abschnitt Zertifikatdatei auf Durchsuchen und navigieren Sie zu der Zertifikatdatei, die Sie hochladen möchten.
4. Klicken Sie im Abschnitt Datei mit privatem Schlüssel auf Durchsuchen und navigieren Sie zu der Datei des privaten Schlüssels, die Sie hochladen möchten.
5. Geben Sie im Feld Passphrase für privaten Schlüssel die Passphrase des privaten Schlüssels ein.
6. Klicken Sie auf Hochladen, um die Dateien hochzuladen.

   Der Seitenbereich wird geschlossen.

   > Hinweis: Nachdem Sie das Zertifikat ersetzt haben, empfiehlt Tenable, die Registerkarte des Browsers neu zu laden, um sich zu vergewissern, dass die Aktualisierung des HTTP-Zertifikats erfolgreich war. Wenn der Upload nicht erfolgreich ist, zeigt OT Security eine Warnmeldung an.

## API-Schlüssel generieren

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager, Sicherheitsanalyst, Site-Operator, Schreibgeschützt

Die Generierung eines API-Schlüssels kann für die Integration von OT Security mit anderen Sicherheitstools und -systemen in Ihrer Organisation hilfreich sein.

### So generieren Sie API-Schlüssel in OT Security:

1. Gehen Sie zu Einstellungen > Systemkonfiguration > API-Schlüssel.

   Die Seite API-Schlüssel wird angezeigt.
2. Klicken Sie in der oberen rechten Ecke auf Schlüssel generieren.

   Der Bereich Schlüssel generieren wird angezeigt.

3. Wählen Sie im Feld Ablauffrist die Anzahl Tage aus, nach denen der API-Schlüssel als veraltet gelten soll.
4. Geben Sie im Feld Beschreibung eine Beschreibung für den API-Schlüssel ein.
5. Klicken Sie auf Generieren.

   Der Bereich Schlüssel generieren wird zusammen mit der ID und dem API-Schlüssel angezeigt.
6. Klicken Sie auf die Schaltfläche , um den API-Schlüssel zu kopieren.
7. Klicken Sie auf Fertig.

   Die Seite API-Schlüssel mit der ID des neu hinzugefügten API-Schlüssels wird angezeigt.

## ICP mit Enterprise Manager koppeln

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

Hinweis: Dieser Flow ist für OT Security 3.18 und höher verfügbar.

Sie können Ihre Industrial Core Platform (ICP) mit OT Security EM koppeln und alle Ihre Sites verwalten.

Hinweis: Nach der Kopplung mit EM müssen alle Updates auf EM-Ebene erfolgen, damit die Sites und ihre Sensoren die neuesten Versions-Updates erhalten.

### Bevor Sie beginnen

Stellen Sie Folgendes sicher:

- OT Security EM kann über die API eine Verbindung zur ICP herstellen.
- Stellen Sie sicher, dass TCP 443 und TCP 28305 für die Kommunikation von der ICP zu OT Security EM offen sind.

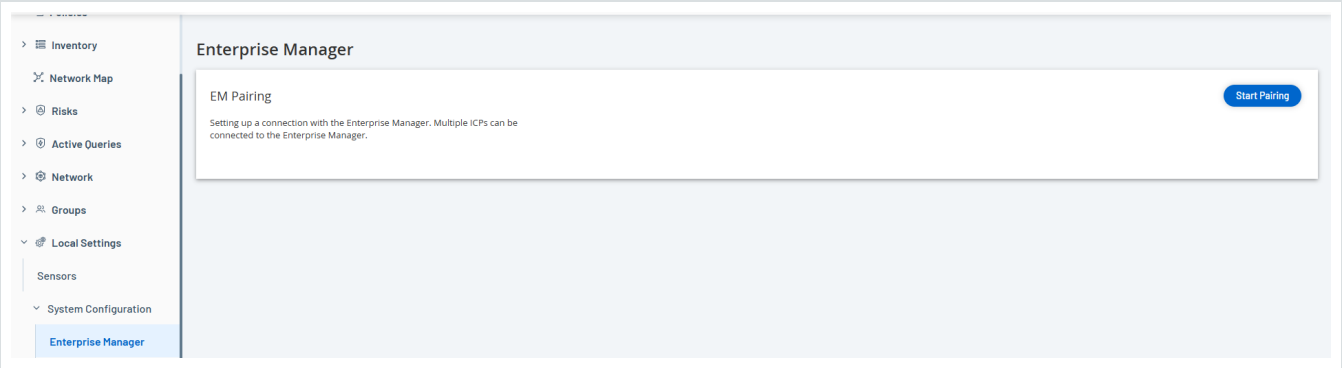
- Zwischen der ICP und OT Security EM bestehen HTTPS-Verbindungen.
- (Optional) Generieren Sie einen API-Schlüssel in OT Security EM.

> Hinweis: Dies ist nur bei einer Kopplung mit der API-Schlüssel-Option erforderlich.

So koppeln Sie die ICP mit OT Security EM:

1. Gehen Sie in OT Security zu Einstellungen > Systemkonfiguration > Enterprise Manager.

   Die Seite Enterprise Manager wird angezeigt.




2. Klicken Sie im Abschnitt EM-Kopplung auf Kopplung starten.

   Der Bereich EM-Kopplungskonfiguration wird angezeigt.

3. Wählen Sie eine der folgenden Optionen aus:
   - Mittels Benutzername und Passwort koppeln
   - Mittels API-Geheimnis koppeln

| Ausgewählte Option | Aktion |
|---|---|
| Mittels Benutzername und | 1. Geben Sie im Feld Hostname/IP den Hostnamen oder die IP-Adresse des EM ein. |

| | |
|---|---|
| Passwort koppeln | 2. Geben Sie im Feld Benutzername den Benutzernamen des EM-Administrators ein.<br>3. Geben Sie im Feld Passwort das Passwort des EM ein.<br>4. Fügen Sie im Feld EM-Zertifikat-Fingerabdruck das Zertifikat ein, das Sie auf der EM-Seite Zertifikate kopiert haben.<br>Tipp: Sie können diesen Schritt überspringen und das Zertifikat auf der Seite EM-Kopplung manuell genehmigen.<br>Hinweis: Sie können die Seite Zertifikate über Lokale Einstellungen > Systemkonfiguration in OT Security EM aufrufen. |
| Mittels API-Schlüssel koppeln | 1. Geben Sie im Feld Hostname/IP den Hostnamen oder die IP-Adresse des EM ein.<br>2. Fügen Sie im Feld API-Geheimnis den API-Schlüssel ein, den Sie in EM kopiert haben.<br>3. Fügen Sie im Feld EM-Zertifikat-Fingerabdruck das Zertifikat ein, das Sie auf der EM-Seite Zertifikate kopiert haben.<br>Tipp: Sie können diesen Schritt überspringen und das Zertifikat auf der Seite EM-Kopplung manuell genehmigen.<br>Hinweis: Sie können die Seite Zertifikate über |

| | |
|---|---|
| | Lokale Einstellungen > Systemkonfiguration in OT Security EM aufrufen. |

4. Klicken Sie auf Koppeln.

   In OT Security wird die Seite EM-Kopplung mit dem Kopplungsstatus angezeigt.

   > Hinweis: Der Status kann Warten auf Genehmigung des Zertifikats (wenn das Zertifikat nicht bereitgestellt wird) oder EM-Genehmigung ausstehend lauten (wenn die automatische Genehmigung von Kopplungsanforderungen deaktiviert ist).

5. (Optional) Wenn der Status Warten auf Genehmigung des Zertifikats lautet:

   a. Klicken Sie auf Zertifikat anzeigen.

      Der Bereich Zertifikat genehmigen wird angezeigt.

   b. Überprüfen Sie, ob der im Bereich angezeigte Fingerabdruck mit dem auf der EM-Seite Zertifikate identisch ist.

      Klicken Sie auf Genehmigen.

      OT Security genehmigt das Zertifikat und zeigt die EM-Kopplungsseite mit dem geänderten Status an, der jetzt EM-Genehmigung ausstehend lautet.

6. Die Statusanzeige EM-Genehmigung ausstehend bedeutet, dass die Option ICP-Kopplungsanforderungen automatisch genehmigen deaktiviert ist. Gehen Sie in diesem Fall wie folgt vor:

   > Tipp: Um Kopplungsanforderungen in OT Security EM automatisch zu genehmigen, aktivieren Sie die Option ICP-Kopplungsanforderungen automatisch genehmigen auf der Seite ICPs in OT Security EM.

   a. Wählen Sie in OT Security EM in der linken Navigationsleiste die Option ICPs aus.

      Die Seite ICPs wird angezeigt.

b. Bewegen Sie den Mauszeiger über die Zeile des Systems, das Sie koppeln möchten, und führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die Spalte Status und wählen Sie Genehmigen aus.
   - Klicken Sie in der oberen rechten Ecke auf Aktionen > Genehmigen.

OT Security EM genehmigt die Kopplung und zeigt den Status Verbunden an.

> Tipp: Nachdem die Kopplung abgeschlossen ist, wird in OT Security EM Folgendes angezeigt:
>
> - Die Daten aus der ICP werden in den EM-Dashboards angezeigt.
> - Die neu gekoppelte ICP wird auf der Seite ICPs angezeigt.
> - Um auf die ICP zuzugreifen, klicken Sie auf der Seite ICPs auf den ICP-Namen. Für die ICP-Instanz, auf die von EM aus zugegriffen wird, wird die Bezeichnung ICP in der Kopfzeile angezeigt. Weitere Informationen finden Sie unter ICPs im Tenable OT Security Enterprise Manager User Guide.

In OT Security wird auf der Seite Enterprise Manager der Status Verbunden angezeigt. Sie können auf Bearbeiten klicken, um die EM-Kopplungskonfiguration zu ändern.

## ICP-Kopplung mit Enterprise Manager trennen

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

Sie können die ICP-Kopplung von EM oder der ICP trennen, wenn die Kopplung nicht mehr benötigt wird.

Eine ICP-Kopplung von OT Security EM trennen

1. Wählen Sie in OT Security EM in der linken Navigationsleiste die Option ICPs aus.

   Die Seite ICPs wird angezeigt.

2. Bewegen Sie den Mauszeiger über die Zeile der ICP, die Sie löschen möchten, und führen Sie einen der folgenden Schritte aus:

    - Klicken Sie mit der rechten Maustaste auf die Spalte Status und wählen Sie Löschen aus.
    - Klicken Sie auf die ICP-Zeile. Dadurch wird die Zeile hervorgehoben und die Schaltfläche Aktionen wird aktiviert.

3. Klicken Sie auf Löschen.

OT Security EM trennt die Kopplung mit OT Security.

Eine ICP-Kopplung von OT Security trennen

1. Gehen Sie in OT Security zu Einstellungen > Systemkonfiguration > Enterprise Manager.

    Die Seite Enterprise Manager wird angezeigt.

2. Klicken Sie im Abschnitt „EM-Kopplung“ auf Bearbeiten.

    Der Bereich EM-Kopplung wird angezeigt.

3. Klicken Sie auf Keine Kopplung.
4. Klicken Sie auf Koppeln.

    OT Security trennt die Kopplung mit OT Security EM.

### Lizenz

Wenn Sie Ihre OT Security-Lizenz aktualisieren oder neu initialisieren müssen, wenden Sie sich an Ihren Tenable Account Manager. Sobald Ihr Tenable Account Manager Ihre Lizenz aktualisiert hat, können Sie Ihre Lizenz aktualisieren oder neu initialisieren. Weitere Informationen finden Sie im Lizenzaktivierung für OT Security.

## Umgebungseinstellungen

# Netzwerkdefinitionen

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Site-Operator

Die Seite „Netzwerkdefinitionen“ umfasst die folgenden Abschnitte:

- Passives Monitoring
- Duplizierte interne Netzwerke
- Neue Assets über SNMP ermitteln
- IP-Adresse für IoT-Assets abrufen

## Passives Monitoring

Passives Monitoring ist während der Erstkonfiguration von OT Security deaktiviert. Tenable empfiehlt, die Einrichtung Ihrer überwachten Netzwerke abzuschließen, bevor Sie passives Monitoring aktivieren. Dies hilft Ihnen, eine Überlastung durch eine große Anzahl anfänglicher Warnmeldungen und Sicherheitsereignisse zu vermeiden.

## Duplizierte interne Netzwerke

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

Wenn eine IP-Adresse mehreren Geräten zugewiesen wird, kommt es zu überlappenden IP-Bereichen. Überlappende IP-Bereiche kommen in Fertigungsumgebungen häufig vor, was die genaue Identifizierung und Verfolgung von Assets erschwert und dadurch zu Sichtbarkeitslücken und falschen Asset-Zuordnungen führen kann. Sie können Ihre überlappenden Netzwerke definieren, damit OT Security Assets auch dann genau verfolgen kann, wenn IP-Adressen in verschiedenen Segmenten wiederverwendet werden.

Hinweis: Wenn ein Asset in einem duplizierten Netzwerk sowohl von einem Sensor als auch von einer anderen Quelle (z. B. einem anderen Sensor oder dem lokalen ICP) erkannt wird, wird es von der OT Security-Oberfläche zu einem einzigen Asset zusammengeführt. Für Lizenzierungszwecke

wird es allerdings als zwei Assets gezählt. Um dies zu verhindern, empfiehlt Tenable, den duplizierten Netzwerkbereich so anzupassen, dass solche Assets ausgeschlossen werden.

Dupliziertes Netzwerk hinzufügen

## Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie authentifizierte Sensoren gekoppelt haben.

  Hinweis: OT Security unterstützt keine duplizierten Netzwerke auf nicht authentifizierten Sensoren.

## So definieren Sie die duplizierten Netzwerke in Ihrer Umgebung:

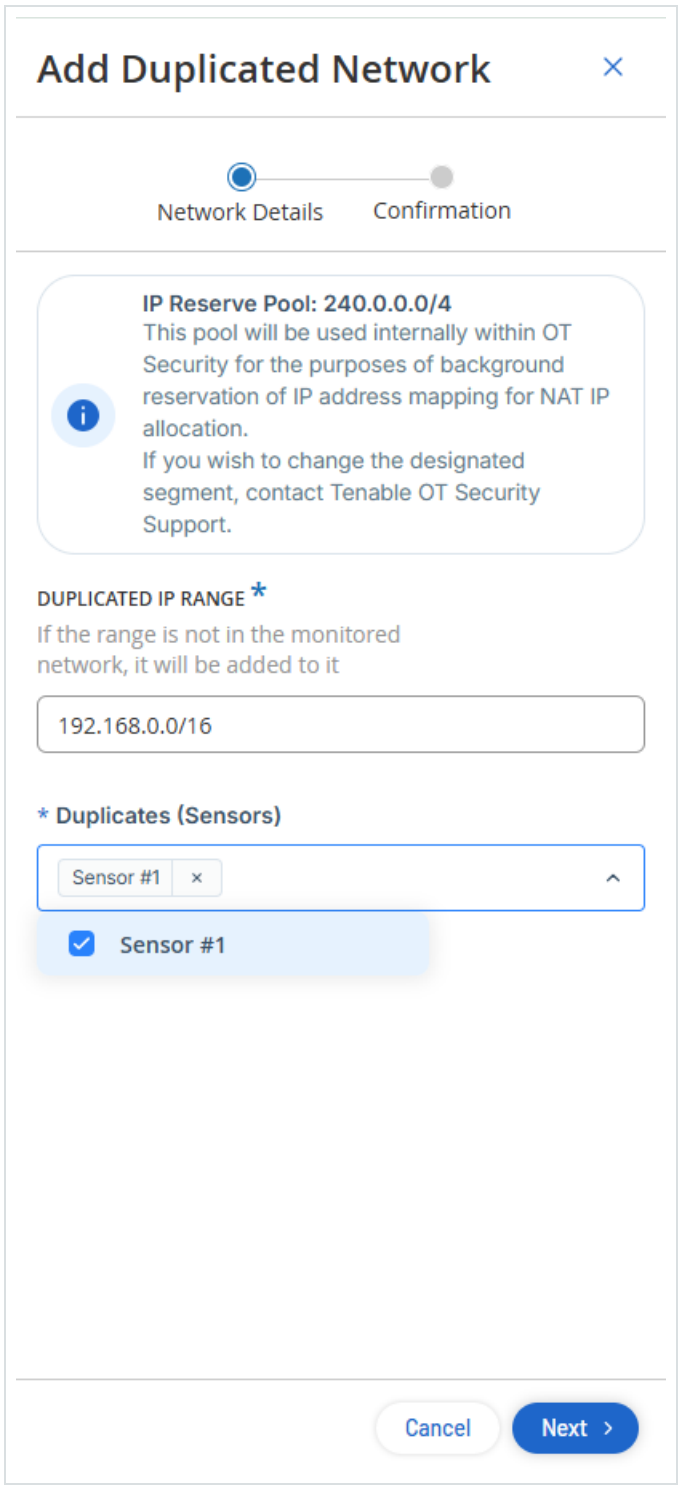
1. Gehen Sie zu Einstellungen > Umgebungseinstellungen > Netzwerkdefinitionen.

   Die Seite Netzwerkdefinitionen wird angezeigt.

2. Klicken Sie im Abschnitt Duplizierte interne Netzwerke auf Netzwerk hinzufügen.

   Das Fenster Dupliziertes Netzwerk hinzufügen mit den Netzwerkdetails wird angezeigt.

   Hinweis: OT Security verwendet den IP-Bereich 240.0.0.0/4 als internen Reservepool für die Zuordnung von IP-Adressen zur NAT-IP-Zuteilung. Um diesen Reservepoolbereich zu ändern, wenden Sie sich an Tenable Support.

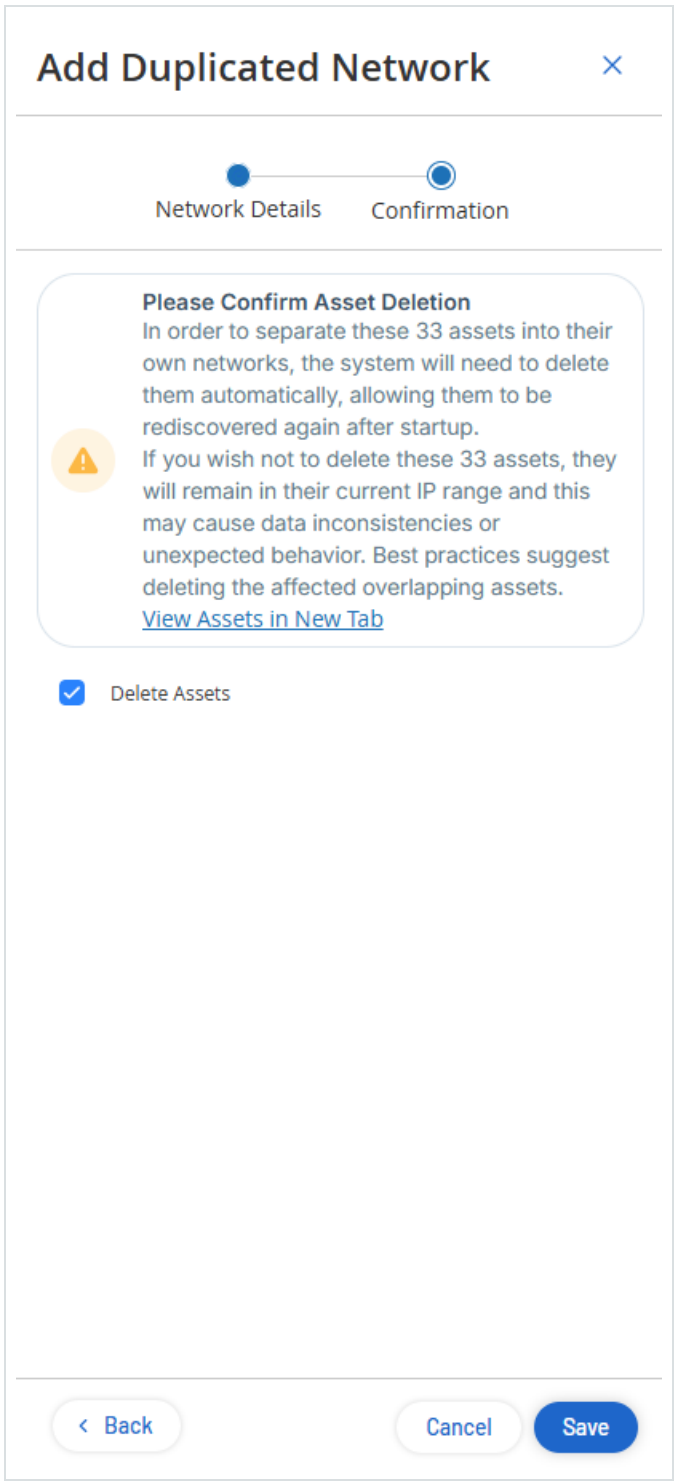



3. Geben Sie im Feld Duplizierter IP-Bereich den IP-Bereich im CIDR-Format ein, zum Beispiel 192.168.0.0/24.

4. Wählen Sie im Dropdown-Feld Duplikate (Sensoren) die Sensoren aus, die dem duplizierten IP-Bereich zugeordnet sind.

5. Klicken Sie auf Weiter.

   Das Fenster Bestätigung wird angezeigt.

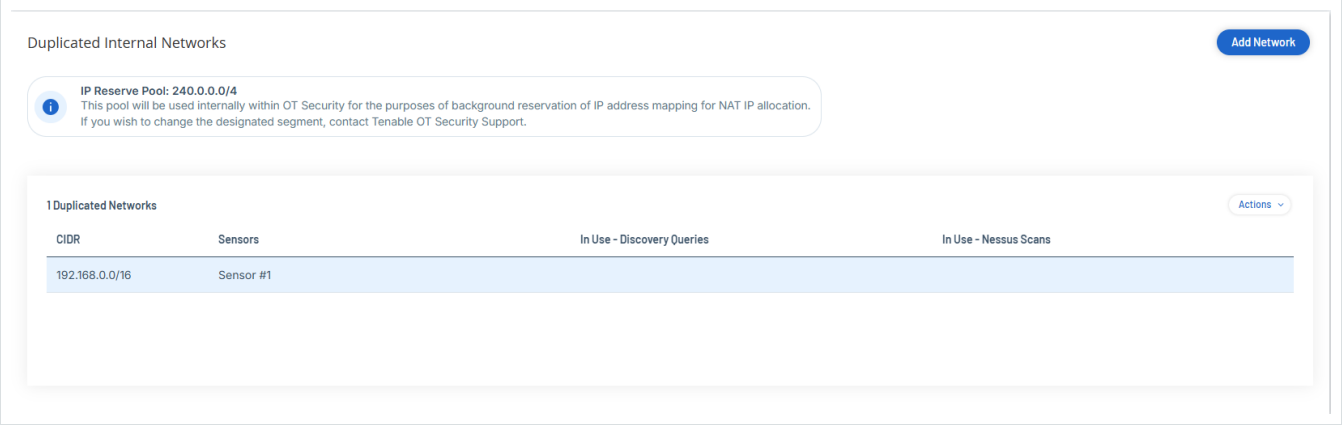



6. (Optional) Aktivieren Sie das Kontrollkästchen Assets löschen.

Tipp: Um alle ausgewählten Assets in ihre eigenen Netzwerke aufzuteilen, empfiehlt Tenable, dass Sie OT Security erlauben, die Assets zu löschen und nach dem Start erneut zu erfassen. Wenn Sie das Kontrollkästchen Assets löschen nicht aktivieren, verbleiben die Assets in ihrem aktuellen IP-Bereich, was zu Inkonsistenzen oder unerwartetem Verhalten führen kann.

7. Klicken Sie auf Speichern.

   OT Security speichert den duplizierten IP-Bereich und zeigt ihn in der Tabelle „Duplizierte interne Netzwerke“ an.




Wichtig: Nachdem Sie die Konfiguration der duplizierten Netzwerke abgeschlossen haben, empfiehlt Tenable einen Neustart von OT Security, bevor Sie die Sensoren aktivieren.

8. Starten Sie OT Security neu.

9. Zum Aktivieren der Sensoren gehen Sie zu Einstellungen > Sensoren:

   Hinweis: Die IP-Bereiche (CIDRs) für die aktive Abfrage sind diejenigen, die Sie in den Einstellungen unter Duplizierte interne Netzwerke konfiguriert haben.

   1. Führen Sie einen der folgenden Schritte aus:

      - Einzelner Sensor: Klicken Sie mit der rechten Maustaste auf den Sensor und klicken Sie auf Bearbeiten. Klicken Sie im Bereich Sensor bearbeiten auf den Umschalter Aktive Sensorabfragen, um aktive Abfragen zu aktivieren.

- Mehrere Sensoren: Wählen Sie alle benötigten Sensoren aus. Wählen Sie in der Kopfzeile Massenaktionen > Aktive Abfragen aktivieren aus.

2. Klicken Sie mit der rechten Maustaste auf die Sensoren und aktivieren Sie sie, indem Sie den Status von Angehalten in Verbunden ändern.

### Nächste Schritte

Nach der Konfiguration der duplizierten Netzwerke und dem Neustart von OT Security werden die Assets mit ihren tatsächlichen IP-Adressen in der Tabelle Alle Assets angezeigt. Wenn Sie eine IP-Adresse eingeben, die einem duplizierten Netzwerk zugewiesen ist, müssen Sie außerdem den entsprechenden Sensor auswählen. Beispiel: unter Aktive Abfrage > Erfassung/Nessus-Scan > Scan erstellen oder unter Zugangsdaten > Zugangsdaten testen:

- Zeigen Sie unter Inventar > Alle Assets die tatsächlichen IP-Adressen und die Quelle der Assets in der Tabelle „Alle Assets“ an. Beispielsweise zwei Assets, die dieselbe IP-Adresse haben, aber verschiedenen Sensoren zugeordnet sind.
- Wählen Sie bei der Konfiguration einer aktiven Abfrage mit duplizierten Netzwerken unter Aktive Abfragen > Abfrageverwaltung > Erfassung oder Nessus-Scans > Scan erstellen Relevante Sensoren für diesen IP-Bereich aus. Dadurch können Sie die Abfrage für Assets ausführen, die einem bestimmten Sensor zugeordnet sind, und die anderen Sensoren ausschließen.

  > Hinweis: OT Security aktiviert das Kontrollkästchen Relevante Sensoren nur für IP-Bereiche in duplizierten Netzwerken. Für alle anderen IP-Bereiche bleibt es deaktiviert.

- Wenn Sie beim Konfigurieren der Zugangsdaten unter Aktive Abfragen > Zugangsdaten > Zugangsdaten testen einen IP-Bereich in einem duplizierten Netzwerk eingeben, müssen Sie auch die zugehörigen Sensoren im Feld Duplikat (Sensor) auswählen.
- Um Asset-Gruppen für Assets zu erstellen, die Teil duplizierter Netzwerke sind, verwenden Sie die Option Asset-Auswahl und identifizieren Sie die spezifische IP anhand der Spalte Quelle in der Tabelle „Assets“.

### Tabelle „Duplizierte interne Netzwerke“

Die Tabelle „Duplizierte interne Netzwerke“ enthält die folgenden Details:

| Spalte | Beschreibung |
|---|---|
| CIDR | Der IP-Bereich des duplizierten Netzwerks. |
| Sensoren | Die Sensoren, die dem IP-Bereich des duplizierten Netzwerks zugeordnet sind. |
| In Verwendung – Erfassungsabfragen | Gibt an, ob die CIDRs in mindestens einer Asset-Erfassung (aktive Abfrage) verwendet werden. Wenn ja, entfernen Sie das CIDR aus der aktiven Erfassung, bevor Sie das duplizierte Netzwerk löschen, das dieses CIDR enthält. |
| In Verwendung – Nessus-Scans | Gibt an, ob die CIDRs in mindestens einem Nessus-Scan verwendet werden. Wenn ja, entfernen Sie das CIDR aus dem Nessus-Scan, bevor Sie das duplizierte Netzwerk löschen, das dieses CIDR enthält. |

Aktionen für duplizierte interne Netzwerke

### Dupliziertes Netzwerk bearbeiten

Sie können die Konfiguration des duplizierten Netzwerks nach Bedarf ändern.

So bearbeiten Sie ein dupliziertes Netzwerk:

1. Wählen Sie das duplizierte Netzwerk, das Sie bearbeiten möchten, im Abschnitt Duplizierte interne Netzwerke aus.
2. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie mit der rechten Maustaste auf das duplizierte Netzwerk und wählen Sie Bearbeiten aus.
- Wählen Sie in der oberen rechten Ecke des Abschnitts Aktionen > Bearbeiten aus.

  Der Bereich Dupliziertes Netzwerk bearbeiten mit den Details des ausgewählten duplizierten Netzwerks wird angezeigt.

3. Ändern Sie die Werte nach Bedarf.
4. Klicken Sie auf Weiter.
5. Klicken Sie im Bereich Bestätigung auf Speichern.

   OT Security speichert die Änderungen am duplizierten Netzwerk.

### Dupliziertes Netzwerk löschen

Sie können duplizierte Netzwerke, die Sie nicht mehr benötigen, löschen.

So löschen Sie ein dupliziertes Netzwerk:

1. Wählen Sie das duplizierte Netzwerk, das Sie löschen möchten, im Abschnitt Duplizierte interne Netzwerke aus.
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie mit der rechten Maustaste auf das duplizierte Netzwerk und wählen Sie Löschen aus.
   - Wählen Sie in der oberen rechten Ecke des Abschnitts Aktionen > Löschen aus.

OT Security löscht das duplizierte Netzwerk.

### In einem duplizierten Netzwerk verwendeten Sensor löschen

So löschen Sie einen Sensor, der in einem duplizierten Netzwerk verwendet wird:

1. Entfernen Sie die CIDRs aus dem Nessus-Scan/Active Discovery.
2. Löschen Sie den Sensor aus der Konfiguration des duplizierten Netzwerks.
3. Im Falle eines Austauschs legen Sie die neue Sensor-ID mithilfe der API fest und ersetzen Sie den alten Sensor.
4. Löschen Sie den alten Sensor auf der Seite Sensoren.

### Neue Assets über SNMP ermitteln

Wenn Sie die Option Neue Assets über SNMP ermitteln aktivieren, fügt OT Security die von SNMP-Abfragen erfassten Assets zur Asset-Inventarisierung hinzu.

### IP-Adresse für IoT-Assets abrufen

Beim Importieren von Assets von einem IoT-Connector importiert OT Security standardmäßig die IP-Adresse zusammen mit der MAC-Adresse der Geräte. Um nur die MAC-Adresse zu importieren, deaktivieren Sie die Option IP-Adresse für IoT-Assets abrufen. Weitere Informationen finden Sie unter IoT-Connectors verwalten.

### Ereigniscluster

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

Um die Überwachung von Ereignissen zu vereinfachen, werden mehrere Ereignisse mit denselben Merkmalen in einem einzigen Cluster zusammengefasst. Das Clustering basiert auf dem Ereignistyp (d. h. Ereignisse, die dieselbe Richtlinie nutzen), Quell- und Ziel-Assets.

Damit Ereignisse geclustert werden können, müssen sie innerhalb der folgenden konfigurierten Zeitintervalle generiert werden:

- Maximale Zeit zwischen aufeinanderfolgenden Ereignissen – Legt das maximale Zeitintervall zwischen Ereignissen fest. Wenn diese Zeit verstrichen ist, werden aufeinanderfolgende Ereignisse nicht geclustert.
- Maximale Zeit zwischen erstem und letztem Ereignis – Legt das maximale Zeitintervall für alle Ereignisse fest, die als Cluster angezeigt werden sollen. Ein Ereignis, das nach diesem Zeitintervall generiert wird, wird nicht in den Cluster aufgenommen.

So aktivieren Sie Clustering:

1. Gehen Sie zu Einstellungen > Umgebungseinstellungen > Ereigniscluster.

   Die Seite Ereigniscluster wird angezeigt.

2. Klicken Sie auf den Umschalter, um die gewünschten Kategorien für das Clustering zu aktivieren.
3. Um die Zeitintervalle für eine Kategorie zu konfigurieren, klicken Sie auf Bearbeiten.

   Das Fenster Konfiguration bearbeiten wird angezeigt.

4. Geben Sie den gewünschten Zahlenwert in das Zahlenfeld ein und wählen Sie die Zeiteinheit über das Dropdown-Feld aus.

   > Hinweis: Weitere Informationen zu Clustering und Zeitintervallen können Sie über das Symbol aufrufen.

5. Klicken Sie auf Speichern.

## Überwachte Netzwerke

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

Die Konfiguration des überwachten Netzwerks enthält eine Reihe von IP-Bereichen (CIDRs/Subnetze), die die Überwachungsgrenzen für OT Security definieren. OT Security ignoriert Assets außerhalb der konfigurierten Bereiche.

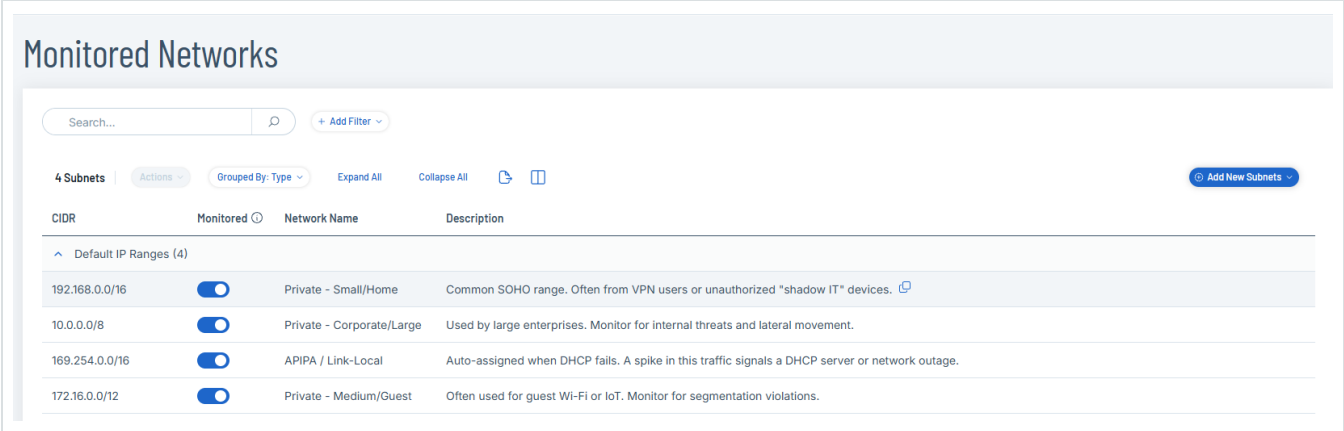
Standardmäßig konfiguriert OT Security drei öffentliche Standardbereiche: 10.0.0.0/8, 172.16.0.0/12 und 192.168.0.0/16 sowie den Link-Local-Bereich 169.254.0.0/16 (APIPA).

> Achtung: Wenn Sie mehr als 5.000 eindeutige überwachte Subnetze konfigurieren, kürzt OT Security die Liste auf die ersten 5.000 Einträge. Das System gibt im Falle einer Kürzung keine Benachrichtigung aus.
> Für NNM-Komponenten (Nessus Network Monitor) verarbeitet OT Security nur die ersten 128 Einträge.

So deaktivieren Sie einen der Standardbereiche oder fügen für Ihr Netzwerk geeignete Bereiche hinzu:

1. Gehen Sie zu Einstellungen > Umgebungseinstellungen > Überwachte Netzwerke.

   Die Seite Überwachte Netzwerke wird angezeigt.




2. Passen Sie Tabellen nach Bedarf an. Siehe Tabellen anpassen.

3. Die Tabelle „Überwachte Netzwerke“ enthält die folgenden Details:

| Spalte | Beschreibung |
| --- | --- |
| Standard-IP-Bereiche und Benutzerdefinierte IP-Bereiche | Der Abschnitt Standard-IP-Bereiche zeigt die in OT Security konfigurierten Standard-IP-Bereiche an.<br><br>Der Abschnitt Benutzerdefinierte IP-Bereiche zeigt von Ihnen erstellte IP-Bereiche an. |
| CIDR | In der Spalte CIDR werden die zu überwachenden IP-Adressen angezeigt. |
| Überwacht | Klicken Sie, um die Überwachung der konfigurierten IP-Adressen zu aktivieren oder zu deaktivieren. |
| Netzwerkname | Der Name des Netzwerks. |
| Beschreibung | Die Beschreibung zu den IP-Bereichen. |
|  | Verwenden Sie die Schaltfläche „Kopieren“ neben einem Parameter, um den Wert zu kopieren. |

### Subnetze hinzufügen

Sie können ein Subnetz oder eine Liste von Subnetzen zur Überwachung hinzufügen.

So fügen Sie ein neues Subnetz hinzu:

1. Klicken Sie im linken Navigationsmenü auf Einstellungen > Umgebungseinstellungen > Überwachte Netzwerke.

   Die Seite Überwachte Netzwerke wird angezeigt.

2. Klicken Sie in der oberen rechten Ecke auf Neue Subnetze hinzufügen.

   Ein Menü wird angezeigt.

3. Wählen Sie eine der folgenden Optionen aus:

    - Ein Subnetz hinzufügen: Wählen Sie diese Option aus, um ein einzelnes Subnetz hinzuzufügen.
    - Subnetzliste hinzufügen: Wählen Sie diese Option aus, um eine Liste mit Subnetzen hinzuzufügen.

    Der Bereich Subnetz hinzufügen wird angezeigt.

4. Wenn Sie Ein Subnetz hinzufügen ausgewählt haben:

    a. Geben Sie in das Feld CIDR den IP-Adressbereich ein. Beispiel: `192.168.1.0/24`.

    b. Klicken Sie auf den Umschalter Überwacht, damit OT Security Traffic erfassen und aktive Abfragen innerhalb des IP-Bereichs ausführen kann.

    > Hinweis: Der Umschalter Überwacht ist standardmäßig aktiviert. Um die Überwachung zu deaktivieren, klicken Sie auf den Umschalter Überwacht, um ihn zu deaktivieren.

    c. (Optional) Geben Sie im Feld Netzwerkname einen Namen für das Netzwerk ein.

    d. (Optional) Geben Sie im Feld Beschreibung eine Beschreibung für Subnetze ein.

    e. Klicken Sie auf Speichern.

5. Wenn Sie Subnetzliste hinzufügen ausgewählt haben, gehen Sie im Bereich Subnetze hinzufügen wie folgt vor:

    a. Geben Sie im Feld CIDR die Liste der CIDRs an, und zwar jeweils ein CIDR pro Zeile.

    b. Klicken Sie auf den Umschalter Überwacht (alle hinzugefügten Subnetze), damit OT Security Traffic erfassen und aktive Abfragen für alle aufgelisteten Subnetze ausführen kann.

> Hinweis: Der Umschalter Überwacht ist standardmäßig aktiviert. Um die Überwachung zu deaktivieren, klicken Sie auf den Umschalter Überwacht (alle hinzugefügten Subnetze), um ihn zu deaktivieren.

c. Klicken Sie auf Speichern.

OT Security speichert die Subnetze und sie werden auf der Seite Überwachte Netzwerke angezeigt.

### Subnetz bearbeiten

Sie können ein Subnetz bearbeiten, um Änderungen daran vorzunehmen.

1. Führen Sie einen der folgenden Schritte aus, um ein Subnetz zu bearbeiten:

   - Fahren Sie in der Tabelle „Überwachte Netzwerke“ mit dem Mauszeiger über die Zeile des IP-Bereichs, die Sie bearbeiten möchten.

     In OT Security wird das Menü Aktionen aktiviert.

   - Klicken Sie in der Tabelle „Überwachte Netzwerke“ mit der rechten Maustaste auf die Zeile des IP-Bereichs, die Sie bearbeiten möchten.

     Ein Menü wird angezeigt.

2. Wählen Sie Subnetz bearbeiten aus.

   Der Bereich Subnetz bearbeiten wird angezeigt.

3. Nehmen Sie die erforderlichen Änderungen vor.

4. Klicken Sie auf Speichern.

   OT Security speichert die Änderungen an den Subnetzen.

## Benutzerverwaltung

Der Zugriff auf die OT Security-Konsole wird über Benutzerkonten gesteuert, in denen die für den jeweiligen Benutzer verfügbaren Berechtigungen festgelegt sind. Die Berechtigungen des Benutzers werden durch die Benutzergruppen bestimmt, denen er zugewiesen ist. Jeder Benutzergruppe wird eine Rolle zugewiesen, die definiert, welche Berechtigungen ihren Mitgliedern zur Verfügung stehen. Wenn also beispielsweise die Benutzergruppe „Site-Operatoren“ die Rolle „Site-Operator“ hat, dann verfügen alle Benutzer, die dieser Gruppe zugewiesen sind, über die mit der Rolle „Site-Operator“ verknüpften Berechtigungen.

Das System wird mit einer Reihe vordefinierter Benutzergruppen geliefert, die den einzelnen verfügbaren Rollen entsprechen: Benutzergruppe „Administratoren“ > Rolle „Administrator“ und Benutzergruppe „Site-Operatoren“ > Rolle „Site-Operator“. Sie können außerdem benutzerdefinierte Benutzergruppen erstellen und ihre Rollen festlegen.

Es gibt drei Methoden, um Benutzer im System zu erstellen:

- Lokale Benutzer hinzufügen – Erstellen Sie Benutzerkonten, um den Zugriff einzelner Benutzer auf das System zu autorisieren. Weisen Sie Benutzer Benutzergruppen zu, die ihre Rollen definieren.
- Authentifizierungsserver – Verwenden Sie die Authentifizierungsserver Ihrer Organisation (z. B. Active Directory, LDAP), um den Zugriff von Benutzern auf das System zu autorisieren. Sie können OT Security-Rollen auf der Grundlage Ihrer vorhandenen Gruppen in Active Directory zuweisen.
- SAML – Richten Sie eine Integration mit Ihrem Identitätsanbieter (z. B. Microsoft Entra ID) ein und weisen Sie Ihrer OT Security-Anwendung Benutzer zu.

Lokale Benutzer

Benutzergruppen

Benutzerrollen

Zonen

Authentifizierungsserver

SAML

## Lokale Benutzer

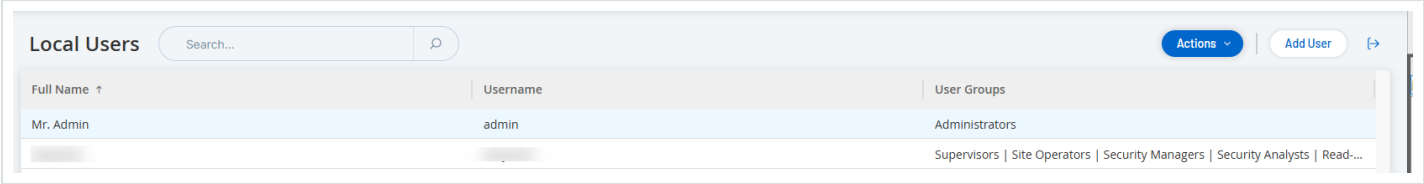
> Erforderliche OT Security-Benutzerrolle: Administrator

Ein Administratorbenutzer kann neue Benutzerkonten erstellen und vorhandene Konten bearbeiten. Jeder Benutzer wird einer oder mehreren Benutzergruppen zugewiesen, die die dem Benutzer zugewiesenen Rollen bestimmen.

> Hinweis: Benutzer können Benutzergruppen entweder während der Erstellung oder der Bearbeitung des Benutzerkontos oder der Benutzergruppe hinzugefügt werden.

### Lokale Benutzer anzeigen

Im Fenster Lokale Benutzer wird eine Liste aller lokalen Benutzer im System angezeigt.




Das Fenster Lokale Benutzer enthält die folgenden Details:

| Parameter | Beschreibung |
|---|---|
| Vollständiger Name | Der vollständige Name des Benutzers. |
| Benutzername | Der Benutzername des Benutzers, der zum Einloggen verwendet wird. |
| Benutzergruppen | Die Benutzergruppen, denen der Benutzer zugewiesen ist. |

### Lokale Benutzer hinzufügen

Sie können Benutzerkonten erstellen, um den Zugriff einzelner Benutzer auf das System zu autorisieren. Jeder Benutzer muss einer oder mehreren Benutzergruppen zugewiesen werden.

## So erstellen Sie ein Benutzerkonto:

1. Gehen Sie zu Einstellungen > Benutzerverwaltung > Lokale Benutzer.
2. Klicken Sie auf Benutzer hinzufügen.

   Daraufhin wird der Bereich Benutzer hinzufügen angezeigt.
3. Geben Sie im Feld Vollständiger Name den Vor- und Nachnamen ein.

   > Hinweis: Der eingegebene Name wird in der Kopfleiste angezeigt, wenn der Benutzer eingeloggt ist.
4. Geben Sie im Feld Benutzername einen Benutzernamen ein, der für das Einloggen beim System verwendet werden soll.
5. Geben Sie im Feld Passwort ein Passwort ein.
6. Geben Sie im Feld Passwort erneut eingeben das gleiche Passwort erneut ein.

   > Hinweis: Dies ist das Passwort, das der Benutzer beim ersten Login verwendet. Der Benutzer kann das Passwort im Fenster Einstellungen ändern, nachdem er sich beim System eingeloggt hat.
7. Aktivieren Sie im Dropdown-Feld Benutzergruppen das Kontrollkästchen für jede Benutzergruppe, der Sie diesen Benutzer zuweisen möchten.

   > Hinweis: Das System wird mit einer Reihe vordefinierter Benutzergruppen geliefert, die den einzelnen verfügbaren Rollen entsprechen, z. B. Benutzergruppe „Administratoren“ > Rolle „Administrator“, Benutzergruppe „Site-Operatoren“ > Rolle „Site-Operator“. Eine Erläuterung der verfügbaren Rollen finden Sie unter Lokale Benutzer.
8. Klicken Sie auf Erstellen.

OT Security erstellt das neue Benutzerkonto im System erstellt und fügt es der Liste der Benutzer unter Lokale Benutzer hinzu.

### Zusätzliche Aktionen für Benutzerkonten

## Benutzerkonto bearbeiten

Sie können einen Benutzer weiteren Benutzergruppen zuweisen oder den Benutzer aus einer Gruppe entfernen.

### So ändern Sie die Benutzergruppen eines Benutzers:

1. Gehen Sie zu Einstellungen > Benutzerverwaltung > Lokaler Benutzer.

   Die Seite Lokale Benutzer wird angezeigt.

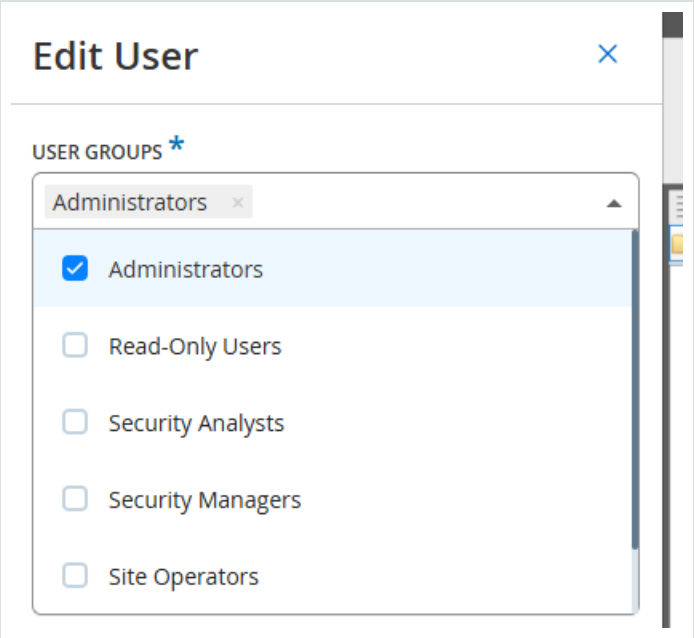
2. Klicken Sie mit der rechten Maustaste auf den gewünschten Benutzer, und wählen Sie Benutzer bearbeiten aus.

   > Hinweis: Alternativ können Sie einen Benutzer auswählen und dann im Menü Aktionen die Option Benutzer bearbeiten auswählen.

3. Der Bereich Benutzer bearbeiten wird angezeigt. Er zeigt die Benutzergruppen, denen der Benutzer zugewiesen ist.

4. Aktivieren bzw. deaktivieren Sie im Dropdown-Feld Benutzergruppen die gewünschten Benutzergruppen.




5. Klicken Sie auf Speichern.

## Benutzerpasswort ändern

> Hinweis: Mit diesem Verfahren kann ein Administratorbenutzer das Passwort für ein beliebiges Konto im System ändern. Alle Benutzer können ihr eigenes Passwort ändern, indem sie zu Lokale Einstellungen > Benutzer gehen.

### So ändern Sie ein Benutzerpasswort:

1. Gehen Sie zu Einstellungen > Benutzerverwaltung > Lokaler Benutzer.

   Die Seite Lokale Benutzer wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf den gewünschten Benutzer, und wählen Sie Passwort zurücksetzen aus.

   > Hinweis: Alternativ können Sie einen Benutzer auswählen und dann im Menü Aktionen die Option Passwort zurücksetzen auswählen.

   Das Fenster Passwort zurücksetzen wird angezeigt.

3. Geben Sie im Feld Neues Passwort ein neues Passwort ein.

4. Geben Sie im Feld Passwort erneut eingeben das neue Passwort erneut ein.
5. Klicken Sie auf Zurücksetzen.

   OT Security wendet das neue Passwort auf das angegebene Benutzerkonto an.

## Lokale Benutzer löschen

So löschen Sie ein Benutzerkonto:

1. Gehen Sie zu Einstellungen > Benutzerverwaltung > Lokaler Benutzer.

   Die Seite Lokale Benutzer wird angezeigt.
2. Klicken Sie mit der rechten Maustaste auf den gewünschten Benutzer, und wählen Sie Benutzer löschen aus.

   > Hinweis: Alternativ können Sie einen Benutzer auswählen und dann im Menü Aktionen die Option Benutzer löschen auswählen.

   Daraufhin wird ein Bestätigungsfenster angezeigt.
3. Klicken Sie auf Löschen.

   OT Security löscht das Benutzerkonto aus dem System.

## Benutzergruppen

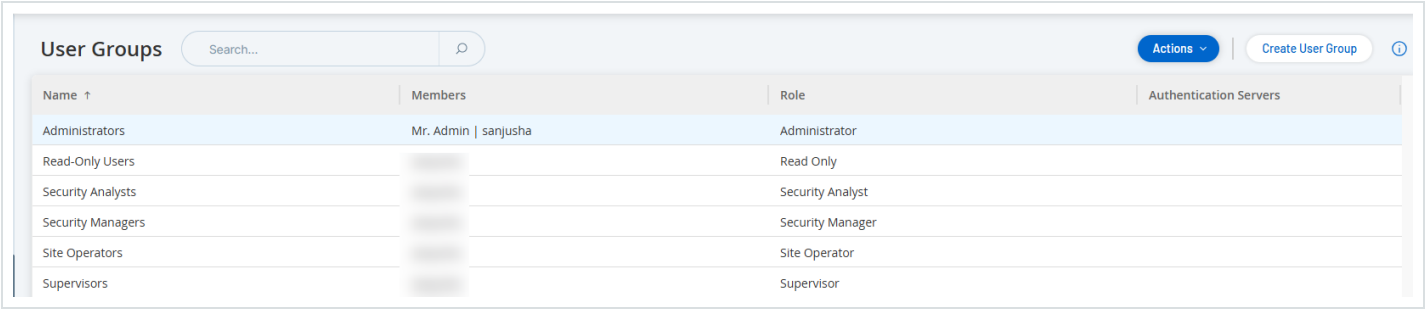
> Erforderliche OT Security-Benutzerrolle: Administrator

Ein Administratorbenutzer kann neue Benutzergruppen erstellen und vorhandene Gruppen bearbeiten. Jeder Benutzer wird einer oder mehreren Benutzergruppen zugewiesen, die die dem Benutzer zugewiesenen Rollen bestimmen.

Das System wird mit einer Reihe vordefinierter Benutzergruppen geliefert, die den einzelnen verfügbaren Rollen entsprechen: Benutzergruppe „Administratoren“ > Rolle „Administrator“ und Benutzergruppe „Site-Operatoren“ > Rolle „Site-Operator“. Eine Erläuterung der verfügbaren Rollen finden Sie unter Benutzerrollen.

## Anzeigen von Benutzergruppen

Auf der Seite „Benutzergruppen“ wird eine Liste aller Benutzergruppen im System angezeigt.




Die folgenden Details sind auf der Seite „Benutzergruppen“ verfügbar:

| Parameter | Beschreibung |
|---|---|
| Name | Der Name der Benutzergruppe. |
| Mitglieder | Eine Liste aller Mitglieder, die der Gruppe zugewiesen sind. |
| Rolle | Die dieser Gruppe zugewiesene Rolle. Eine Erläuterung der den einzelnen Rollen zugeordneten Berechtigungen finden Sie unter Tabelle der Benutzerrollen. |

## Benutzergruppen hinzufügen

Sie können neue Benutzergruppen erstellen und dieser Gruppe Benutzer zuweisen.

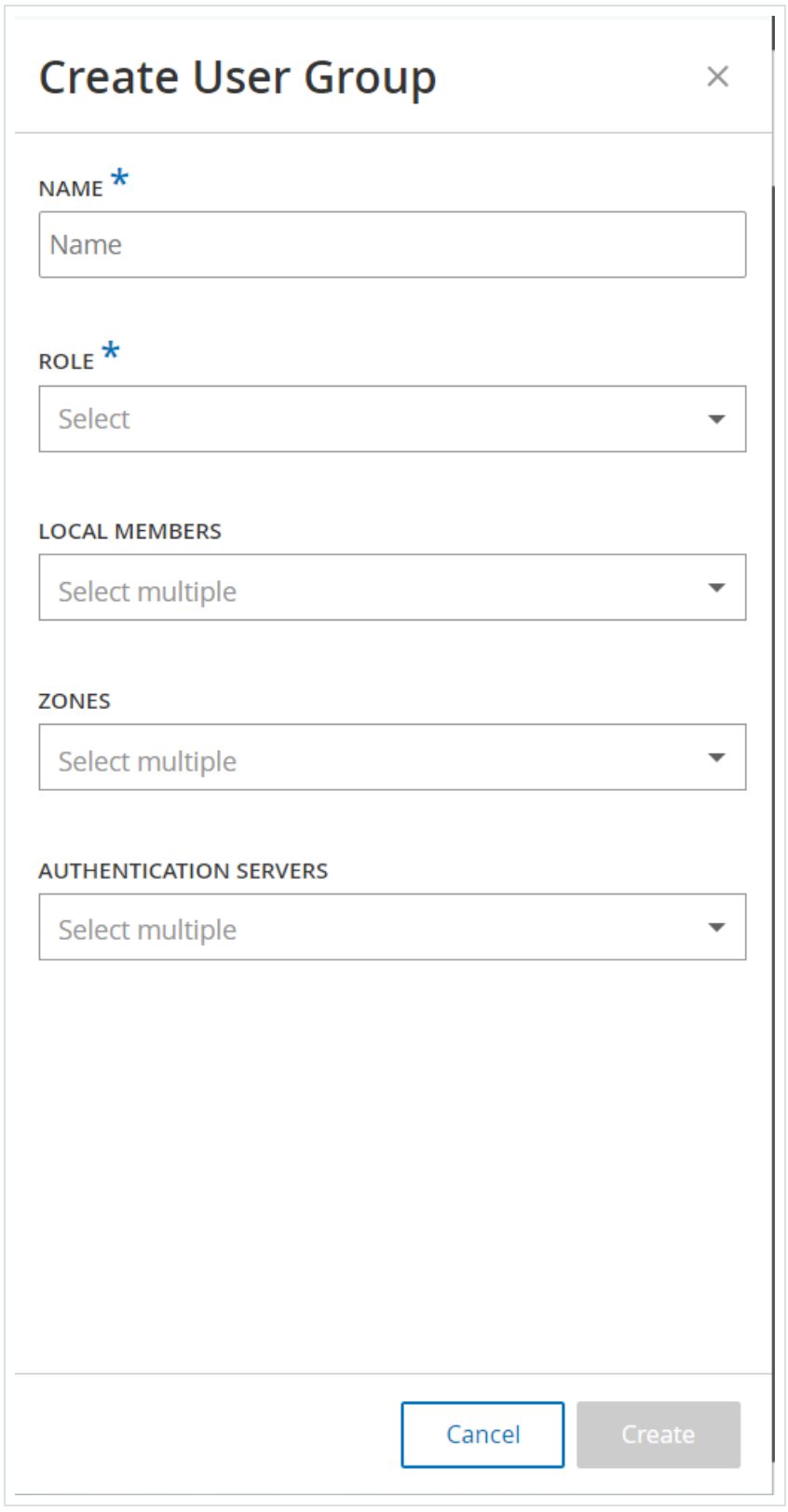
So erstellen Sie eine Benutzergruppe:

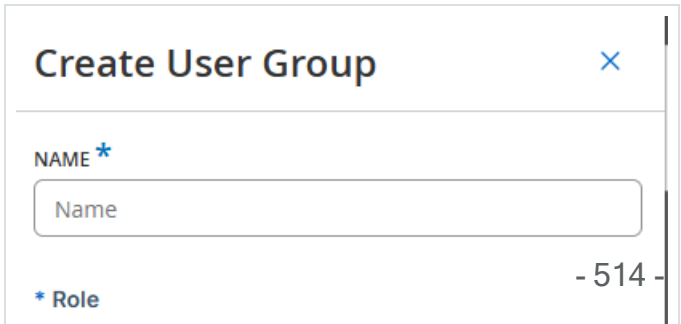
1. Gehen Sie zu Einstellungen > Benutzerverwaltung > Benutzergruppen.

   Der Bildschirm Benutzergruppen wird angezeigt.

2. Klicken Sie auf Benutzergruppe erstellen.

   Der Bereich Benutzergruppe erstellen wird angezeigt.


Create User Group
NAME *
Name
ROLE *
Select
LOCAL MEMBERS
Select multiple
ZONES
Select multiple
AUTHENTICATION SERVERS
Select multiple
Cancel
Create


Create User Group
NAME *
Name
* Role

3. Geben Sie im Feld Name einen Namen für die Gruppe ein.
4. Wählen Sie im Dropdown-Feld Rolle in der Dropdown-Liste die Rolle aus, die Sie dieser Gruppe zuweisen möchten. Verfügbare Rollen sind:
    - Schreibgeschützt
    - Sicherheitsanalyst
    - Sicherheitsmanager
    - Site-Operator
    - Supervisor
5. Wählen Sie im Dropdown-Feld Lokale Mitglieder die Benutzerkonten aus, die Sie der Gruppe zuweisen möchten.
6. Wählen Sie im Dropdown-Feld Zonen die Zonen aus, die Sie der Benutzergruppe zuweisen möchten.
7. Wählen Sie im Dropdown-Feld Authentifizierungsserver die Server aus, die Sie der Benutzergruppe zuweisen möchten.
8. Klicken Sie auf Erstellen.

    OT Security erstellt die neue Benutzergruppe und fügt sie der Liste der Gruppen hinzu, die im Bildschirm Benutzergruppen angezeigt werden.

## Zusätzliche Aktionen für Benutzergruppen

### Benutzergruppen bearbeiten

Sie können die Einstellungen bearbeiten und Mitglieder zu einer vorhandenen Benutzergruppe hinzufügen oder daraus entfernen, indem Sie die Gruppe bearbeiten.

Hinweis: Alternativ können Sie einen Benutzer auswählen und dann im Menü Aktionen die Option Benutzer löschen auswählen.

So bearbeiten Sie eine Benutzergruppe:

1. Gehen Sie zu Einstellungen > Benutzerverwaltung > Benutzergruppen.

   Der Bildschirm Benutzergruppen wird angezeigt.

2. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die gewünschte Benutzergruppe, und wählen Sie Bearbeiten aus.
   - Wählen Sie die Benutzergruppe aus, die Sie bearbeiten möchten. Das Menü Aktionen wird angezeigt. Wählen Sie Aktionen > Bearbeiten aus.

   Der Fensterbereich Benutzergruppe bearbeiten mit den Einstellungen der Gruppe wird angezeigt.

3. Ändern Sie den Namen und die Rolle. Sie können auch Benutzer aktivieren oder deaktivieren, um Benutzer zur Gruppe hinzuzufügen oder daraus zu entfernen.


4. Ändern Sie die Parameter nach Bedarf.
5. Klicken Sie auf Speichern.

## Benutzergruppen löschen

Hinweis: Sie können nur Benutzergruppen löschen, denen derzeit keine Benutzer zugewiesen sind. Wenn einer Gruppe Benutzer zugewiesen sind, müssen Sie zuerst die Benutzer aus der Gruppe entfernen, bevor Sie die Gruppe löschen können.

So löschen Sie eine Benutzergruppe:

1. Gehen Sie zu Einstellungen > Benutzerverwaltung > Benutzergruppen.

   Der Bildschirm Benutzergruppen wird angezeigt.

2. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die gewünschte Benutzergruppe, und wählen Sie Löschen aus.
   - Wählen Sie die Benutzergruppe aus, die Sie löschen möchten. Das Menü Aktionen wird angezeigt. Wählen Sie Aktionen > Löschen aus.

   Daraufhin wird ein Bestätigungsfenster angezeigt.

3. Klicken Sie auf Löschen.

   OT Security löscht die Benutzergruppe

## Benutzerrollen

Die folgenden Rollen sind verfügbar:

- Administrator – Verfügt über maximale Berechtigungen, um alle operativen und administrativen Aufgaben im System durchzuführen, wie zum Beispiel das Erstellen neuer Benutzerkonten.
- Schreibgeschützt – Kann Daten (Asset-Inventar, Ereignisse, Netzwerk-Traffic) anzeigen, aber keine Aktionen im System durchführen.
- Sicherheitsanalyst – Kann Daten im System anzeigen und Sicherheitsereignisse auflösen.

- Sicherheitsmanager – Kann alle sicherheitsbezogenen Funktionen verwalten, einschließlich Konfigurieren von Richtlinien, Anzeigen von Daten im System und Auflösen von Ereignissen.
- Site-Operator – Kann Daten im System anzeigen und das Asset-Inventar verwalten.
- Supervisor – Verfügt über vollständige Berechtigungen, um alle operativen Aufgaben im System und einige eingeschränkte administrative Aufgaben durchzuführen (die Erstellung neuer Benutzer oder andere sensible Aktivitäten gehören nicht dazu).

## Tabelle der Benutzerrollen

Die folgende Tabelle enthält eine detaillierte Aufschlüsselung der genauen Berechtigungen, die für die einzelnen Rollen aktiviert sind.

| Berechtigung | Administrator (lokal) | Administrator (extern/AD) | Supervisor | Sicherheitsmanager | Sicherheitsanalyst | Site-Operator | Schreibgeschützt |
|---|---|---|---|---|---|---|---|
| Ereignisse | | | | | | | |
| Ereignisse anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Auflösen | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| Erfassungsdatei herunterladen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Aus Richtlinie ausschließen | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |

| Berechtigung | Administrator (lokal) | Administrator (extern/AD) | Supervisor | Sicherheitsmanager | Sicherheitsanalyst | Site-Operator | Schreibgeschützt |
|---|---|---|---|---|---|---|---|
| Alle auflösen | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| Exportieren | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Richtlinie auf FortiGate erstellen | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Aktualisieren | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Richtlinien | | | | | | | |
| Richtlinien anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Aktivieren/Deaktivieren | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Aktion anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Bearbeiten | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Duplizieren | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Löschen | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Richtlinie erstellen | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |

| Berechtigung | Administrator (lokal) | Administrator (extern/AD) | Supervisor | Sicherheitsmanager | Sicherheitsanalyst | Site-Operator | Schreibgeschützt |
|---|---|---|---|---|---|---|---|
| Exportieren | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Assets | | | | | | | |
| Assets anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Aktion anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Bearbeiten | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ |
| Löschen | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ |
| Importieren (neue Assets über CSV-Datei hochladen) | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ |
| Ausblenden | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ |
| Exportieren | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Erneut synchronisieren | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |

| Berechtigung | Administrator (lokal) | Administrator (extern/AD) | Supervisor | Sicherheitsmanager | Sicherheitsanalyst | Site-Operator | Schreibgeschützt |
|---|---|---|---|---|---|---|---|
| Nessus-Scan | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| Snapshot erstellen (einzelnes Asset) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| Offene Ports aktualisieren (einzelnes Asset) | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| Port-Status aktualisieren (einzelnes Asset) | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| Im Browser anzeigen (einzelnes Asset) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| In der Haupt-Asset-Übersicht anzeigen (einzelnes | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Berechtigung | Administrator (lokal) | Administrator (extern/AD) | Supervisor | Sicherheitsmanager | Sicherheitsanalyst | Site-Operator | Schreibgeschützt |
|---|---|---|---|---|---|---|---|
| Asset) | | | | | | | |
| Angriffsvektor generieren (einzelnes Asset) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Schwachstellen (Plugins) | | | | | | | |
| Plugin-Treffer anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Aktion anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Kommentar bearbeiten | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| Plugin-Satz aktualisieren | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Exportieren | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Netzwerk | | | | | | | |
| Paketerfassung aktivieren | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |

| Berechtigung | Administrator (lokal) | Administrator (extern/AD) | Supervisor | Sicherheitsmanager | Sicherheitsanalyst | Site-Operator | Schreibgeschützt |
|---|---|---|---|---|---|---|---|
| Fortlaufende Erfassungen schließen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| PCAP-Datei herunterladen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Konversationstabelle exportieren | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Als Baseline festlegen | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Übersicht generieren | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Übersicht aktualisieren | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Gruppen | | | | | | | |
| Gruppen anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Aktion anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Berechtigung | Administrator (lokal) | Administrator (extern/AD) | Supervisor | Sicherheitsmanager | Sicherheitsanalyst | Site-Operator | Schreibgeschützt |
|---|---|---|---|---|---|---|---|
| Bearbeiten | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Duplizieren | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Löschen | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Gruppe erstellen | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Exportieren | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Bericht | | | | | | | |
| Berichte anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Generieren | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Herunterladen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Exportieren | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Netzwerksegmente | | | | | | | |
| Netzwerksegmente anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Berechtigung | Administrator (lokal) | Administrator (extern/AD) | Supervisor | Sicherheitsmanager | Sicherheitsanalyst | Site-Operator | Schreibgeschützt |
|---|---|---|---|---|---|---|---|
| Bearbeiten | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Löschen | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Erstellen | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Exportieren | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mehr erfahren | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Lokale Einstellungen | | | | | | | |
| Abfragen | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Systemkonfiguration – Gerätedetails | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Systemkonfiguration – Sensoren | ✓ | ✓ | ✓ | ✓ (Keine Aktionen) | ✓ (Keine Aktionen) | ✓ (Keine Aktionen) | ✓ (Keine Aktionen) |
| Systemkonfiguration – | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |

| Berechtigung | Administrator (lokal) | Administrator (extern/AD) | Supervisor | Sicherheitsmanager | Sicherheitsanalyst | Site-Operator | Schreibgeschützt |
|---|---|---|---|---|---|---|---|
| Portkonfiguration | | | | | | | |
| Systemkonfiguration – Updates | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Systemkonfiguration – Zertifikat (HTTPS) | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Systemkonfiguration – API-Schlüssel | ✓ | ✗ | ✓ (Nur lokale Benutzer) | ✓ (Nur lokale Benutzer) | ✓ (Nur lokale Benutzer) | ✓ (Nur lokale Benutzer) | ✓ (Nur lokale Benutzer) |
| Systemkonfiguration – Lizenz | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Umgebungskonfiguration – Asset- | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |

| Berechtigung | Administrator (lokal) | Administrator (extern/AD) | Supervisor | Sicherheitsmanager | Sicherheitsanalyst | Site-Operator | Schreibgeschützt |
|---|---|---|---|---|---|---|---|
| Einstellungen | | | | | | | |
| Umgebungskonfiguration – Ausgeblendete Assets | ✓ | ✓ | ✓ | ✓ – keine Wiederherstellung | ✓ – keine Wiederherstellung | ✓ | ✓ – keine Wiederherstellung |
| Umgebungskonfiguration – Benutzerdefinierte Felder | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Umgebungskonfiguration – Ereignisclusterer | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Umgebungskonfiguration – PCAP-Player | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Benutzer und Rollen – Benutzereinstellungen | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |

| Berechtigung | Administrator (lokal) | Administrator (extern/AD) | Supervisor | Sicherheitsmanager | Sicherheitsanalyst | Site-Operator | Schreibgeschützt |
|---|---|---|---|---|---|---|---|
| Benutzer und Rollen – Lokale Benutzer | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Benutzer und Rollen – Benutzergruppen | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Benutzer und Rollen – Active Directory | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Integrationen | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Server | ✓ | ✓ | ✓ | ✓ (Keine Aktionen) | ✓ (Keine Aktionen) | ✓ (Keine Aktionen) | ✓ (Keine Aktionen) |
| Systemaktionen | ✓ | ✓ ohne Zurücksetzung auf | ✓ nur Sich | ✓ nur Diagnose | ✗ | ✗ | ✗ |

| Berechtigung | Administrator (lokal) | Administrator (extern/AD) | Supervisor | Sicherheitsmanager | Sicherheitsanalyst | Site-Operator | Schreibgeschützt |
|---|---|---|---|---|---|---|---|
| | | Werkseinstellungen | erung und Diagnose | | | | |
| Systemprotokoll | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ kein Syslog |
| Aktivieren (beim Setup und nach Deaktivierung) | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Assets löschen | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |

| Berechtigung | Administrator (lokal) | Administrator (extern/AD) |
|---|---|---|
| Ereignisse | | |
| Ereignisse anzeigen | ✓ | ✓ |
| Auflösen | ✓ | ✓ |
| Erfassungsdatei herunterladen | ✓ | ✓ |

| | | |
|---|---|---|
| Aus Richtlinie ausschließen | ✓ | ✓ |
| Alle auflösen | ✓ | ✓ |
| Exportieren | ✓ | ✓ |
| Richtlinie auf FortiGate erstellen | ✓ | ✓ |
| Aktualisieren | ✓ | ✓ |
| Richtlinien | | |
| Richtlinien anzeigen | ✓ | ✓ |
| Aktivieren/Deaktivieren | ✓ | ✓ |
| Aktion anzeigen | ✓ | ✓ |
| Bearbeiten | ✓ | ✓ |
| Duplizieren | ✓ | ✓ |
| Löschen | ✓ | ✓ |
| Richtlinie erstellen | ✓ | ✓ |
| Exportieren | ✓ | ✓ |
| Assets | | |
| Assets anzeigen | ✓ | ✓ |
| Aktion anzeigen | ✓ | ✓ |

| | | |
|---|---|---|
| Bearbeiten | ✓ | ✓ |
| Löschen | ✓ | ✓ |
| Importieren (neue Assets über CSV-Datei hochladen) | ✓ | ✓ |
| Ausblenden | ✓ | ✓ |
| Exportieren | ✓ | ✓ |
| Erneut synchronisieren | ✓ | ✓ |
| Nessus-Scan | ✓ | ✓ |
| Snapshot erstellen (einzelnes Asset) | ✓ | ✓ |
| Offene Ports aktualisieren (einzelnes Asset) | ✓ | ✓ |
| Port-Status aktualisieren (einzelnes Asset) | ✓ | ✓ |
| Im Browser anzeigen (einzelnes Asset) | ✓ | ✓ |
| In der Haupt-Asset-Übersicht anzeigen (einzelnes Asset) | ✓ | ✓ |
| Angriffsvektor generieren (einzelnes Asset) | ✓ | ✓ |
| Schwachstellen (Plugins) | | |
| Plugin-Treffer anzeigen | ✓ | ✓ |

| | | |
|---|---|---|
| Aktion anzeigen | ✓ | ✓ |
| Kommentar bearbeiten | ✓ | ✓ |
| Plugin-Satz aktualisieren | ✓ | ✓ |
| Exportieren | ✓ | ✓ |
| Netzwerk | | |
| Paketerfassung aktivieren | ✓ | ✓ |
| Fortlaufende Erfassungen schließen | ✓ | ✓ |
| PCAP-Datei herunterladen | ✓ | ✓ |
| Konversationstabelle exportieren | ✓ | ✓ |
| Als Baseline festlegen | ✓ | ✓ |
| Übersicht generieren | ✓ | ✓ |
| Übersicht aktualisieren | ✓ | ✓ |
| Gruppen | | |
| Gruppen anzeigen | ✓ | ✓ |
| Aktion anzeigen | ✓ | ✓ |
| Bearbeiten | ✓ | ✓ |
| Duplizieren | ✓ | ✓ |

| | | |
|---|---|---|
| Löschen | ✓ | ✓ |
| Gruppe erstellen | ✓ | ✓ |
| Exportieren | ✓ | ✓ |
| Bericht | | |
| Berichte anzeigen | ✓ | ✓ |
| Generieren | ✓ | ✓ |
| Herunterladen | ✓ | ✓ |
| Exportieren | ✓ | ✓ |
| Netzwerksegmente | | |
| Netzwerksegmente anzeigen | ✓ | ✓ |
| Bearbeiten | ✓ | ✓ |
| Löschen | ✓ | ✓ |
| Erstellen | ✓ | ✓ |
| Exportieren | ✓ | ✓ |
| Mehr erfahren | ✓ | ✓ |
| Lokale Einstellungen | | |
| Abfragen | ✓ | ✓ |
| Systemkonfiguration – Gerätedetails | ✓ | ✓ |

| | | |
|---|---|---|
| Systemkonfiguration – Sensoren | ✓ | ✓ |
| Systemkonfiguration – Portkonfiguration | ✓ | ✓ |
| Systemkonfiguration – Updates | ✓ | ✓ |
| Systemkonfiguration – Zertifikat (HTTPS) | ✓ | ✓ |
| Systemkonfiguration – API-Schlüssel | ✓ | ✗ |
| Systemkonfiguration – Lizenz | ✓ | ✓ |
| Umgebungskonfiguration – Asset-Einstellungen | ✓ | ✓ |
| Umgebungskonfiguration – Ausgeblendete Assets | ✓ | ✓ |
| Umgebungskonfiguration – Benutzerdefinierte Felder | ✓ | ✓ |
| Umgebungskonfiguration – Ereigniscluster | ✓ | ✓ |
| Umgebungskonfiguration – PCAP-Player | ✓ | ✓ |
| Benutzer und Rollen – Benutzereinstellungen | ✓ | ✓ |
| Benutzer und Rollen – Lokale Benutzer | ✓ | ✗ |

| | | |
|---|---|---|
| Benutzer und Rollen – Benutzergruppen | ✓ | ✗ |
| Benutzer und Rollen – Active Directory | ✓ | ✗ |
| Integrationen | ✓ | ✓ |
| Server | ✓ | ✓ |
| Systemaktionen | ✓ | ✓ ohne Zurücksetzung auf Werkseinstellungen |
| Systemprotokoll | ✓ | ✓ |
| Aktivieren (beim Setup und nach Deaktivierung) | ✓ | ✓ |
| Assets löschen | ✓ | ✓ |

| Berechtigung | Supervisor | Sicherheitsmanager | Sicherheitsanalyst | Site-Operator | Schreibgeschützt |
|---|---|---|---|---|---|
| Ereignisse | | | | | |
| Ereignisse anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ |
| Auflösen | ✓ | ✓ | ✓ | ✗ | ✗ |
| Erfassungsdatei herunterladen | ✓ | ✓ | ✓ | ✓ | ✓ |
| Aus Richtlinie | ✓ | ✓ | ✗ | ✗ | ✗ |

| | | | | | |
|---|---|---|---|---|---|
| ausschließen | | | | | |
| Alle auflösen | ✓ | ✓ | ✓ | ✗ | ✗ |
| Exportieren | ✓ | ✓ | ✓ | ✓ | ✓ |
| Richtlinie auf FortiGate erstellen | ✓ | ✓ | ✗ | ✗ | ✗ |
| Aktualisieren | ✓ | ✓ | ✓ | ✓ | ✓ |
| Richtlinien | | | | | |
| Richtlinien anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ |
| Aktivieren/Deaktivieren | ✓ | ✓ | ✗ | ✗ | ✗ |
| Aktion anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ |
| Bearbeiten | ✓ | ✓ | ✗ | ✗ | ✗ |
| Duplizieren | ✓ | ✓ | ✗ | ✗ | ✗ |
| Löschen | ✓ | ✓ | ✗ | ✗ | ✗ |
| Richtlinie erstellen | ✓ | ✓ | ✗ | ✗ | ✗ |
| Exportieren | ✓ | ✓ | ✓ | ✓ | ✓ |
| Assets | | | | | |
| Assets anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ |

| | | | | | |
|---|---|---|---|---|---|
| Aktion anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ |
| Bearbeiten | ✓ | ✗ | ✗ | ✓ | ✗ |
| Löschen | ✓ | ✗ | ✗ | ✓ | ✗ |
| Importieren (neue Assets über CSV-Datei hochladen) | ✓ | ✗ | ✗ | ✓ | ✗ |
| Ausblenden | ✓ | ✗ | ✗ | ✓ | ✗ |
| Exportieren | ✓ | ✓ | ✓ | ✓ | ✓ |
| Erneut synchronisieren | ✓ | ✓ | ✓ | ✓ | ✗ |
| Nessus-Scan | ✓ | ✓ | ✓ | ✓ | ✗ |
| Snapshot erstellen (einzelnes Asset) | ✓ | ✓ | ✓ | ✓ | ✗ |
| Offene Ports aktualisieren (einzelnes Asset) | ✓ | ✓ | ✓ | ✗ | ✗ |
| Port-Status aktualisieren (einzelnes Asset) | ✓ | ✓ | ✓ | ✗ | ✗ |
| Im Browser anzeigen (einzelnes Asset) | ✓ | ✓ | ✓ | ✓ | ✓ |

| | | | | | |
|---|---|---|---|---|---|
| In der Haupt-Asset-Übersicht anzeigen (einzelnes Asset) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Angriffsvektor generieren (einzelnes Asset) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Schwachstellen (Plugins) | | | | | |
| Plugin-Treffer anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ |
| Aktion anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ |
| Kommentar bearbeiten | ✓ | ✓ | ✓ | ✗ | ✗ |
| Plugin-Satz aktualisieren | ✓ | ✓ | ✗ | ✗ | ✗ |
| Exportieren | ✓ | ✓ | ✓ | ✓ | ✓ |
| Netzwerk | | | | | |
| Paketerfassung aktivieren | ✓ | ✗ | ✗ | ✗ | ✗ |
| Fortlaufende Erfassungen schließen | ✓ | ✓ | ✓ | ✓ | ✗ |
| PCAP-Datei | ✓ | ✓ | ✓ | ✓ | ✓ |

| | | | | | |
|---|---|---|---|---|---|
| herunterladen | | | | | |
| Konversationstabelle exportieren | ✓ | ✓ | ✓ | ✓ | ✓ |
| Als Baseline festlegen | ✓ | ✓ | ✗ | ✗ | ✗ |
| Übersicht generieren | ✓ | ✓ | ✓ | ✓ | ✓ |
| Übersicht aktualisieren | ✓ | ✓ | ✓ | ✓ | ✓ |
| Gruppen | | | | | |
| Gruppen anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ |
| Aktion anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ |
| Bearbeiten | ✓ | ✓ | ✗ | ✗ | ✗ |
| Duplizieren | ✓ | ✓ | ✗ | ✗ | ✗ |
| Löschen | ✓ | ✓ | ✗ | ✗ | ✗ |
| Gruppe erstellen | ✓ | ✓ | ✗ | ✗ | ✗ |
| Exportieren | ✓ | ✓ | ✓ | ✓ | ✓ |
| Bericht | | | | | |
| Berichte anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ |
| Generieren | ✓ | ✓ | ✓ | ✓ | ✓ |

| | | | | | |
|---|---|---|---|---|---|
| Herunterladen | ✓ | ✓ | ✓ | ✓ | ✓ |
| Exportieren | ✓ | ✓ | ✓ | ✓ | ✓ |
| Netzwerksegmente | | | | | |
| Netzwerksegmente anzeigen | ✓ | ✓ | ✓ | ✓ | ✓ |
| Bearbeiten | ✓ | ✓ | ✗ | ✗ | ✗ |
| Löschen | ✓ | ✓ | ✗ | ✗ | ✗ |
| Erstellen | ✓ | ✓ | ✗ | ✗ | ✗ |
| Exportieren | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mehr erfahren | ✓ | ✓ | ✓ | ✓ | ✓ |
| Lokale Einstellungen | | | | | |
| Abfragen | ✓ | ✗ | ✗ | ✗ | ✗ |
| Systemkonfiguration – Gerätedetails | ✓ | ✗ | ✗ | ✗ | ✗ |
| Systemkonfiguration – Sensoren | ✓ | ✓(Keine Aktionen) | ✓ (Keine Aktionen) | ✓ (Keine Aktionen) | ✓ (Keine Aktionen) |
| Systemkonfiguration – Portkonfiguration | ✓ | ✗ | ✗ | ✗ | ✗ |

| | | | | | |
|---|---|---|---|---|---|
| Systemkonfiguration – Updates | ✓ | ✗ | ✗ | ✗ | ✗ |
| Systemkonfiguration – Zertifikat (HTTPS) | ✗ | ✗ | ✗ | ✗ | ✗ |
| Systemkonfiguration – API-Schlüssel | ✓ (Nur lokale Benutzer) | ✓ (Nur lokale Benutzer) | ✓ (Nur lokale Benutzer) | ✓ (Nur lokale Benutzer) | ✓ (Nur lokale Benutzer) |
| Systemkonfiguration – Lizenz | ✗ | ✗ | ✗ | ✗ | ✗ |
| Umgebungskonfiguration – Asset-Einstellungen | ✓ | ✗ | ✗ | ✗ | ✗ |
| Umgebungskonfiguration – Ausgeblendete Assets | ✓ | ✓ – keine Wiederherstellung | ✓ – keine Wiederherstellung | ✓ | ✓ – keine Wiederherstellung |
| Umgebungskonfiguration – Benutzerdefinierte Felder | ✓ | ✗ | ✗ | ✗ | ✗ |
| Umgebungskonfiguration – Ereigniscluster | ✓ | ✗ | ✗ | ✗ | ✗ |

| | | | | | |
|---|---|---|---|---|---|
| Umgebungskonfiguration – PCAP-Player | ✓ | ✗ | ✗ | ✗ | ✗ |
| Benutzer und Rollen – Benutzereinstellungen | ✓ | ✗ | ✗ | ✗ | ✗ |
| Benutzer und Rollen – Lokale Benutzer | ✗ | ✗ | ✗ | ✗ | ✗ |
| Benutzer und Rollen – Benutzergruppen | ✗ | ✗ | ✗ | ✗ | ✗ |
| Benutzer und Rollen – Active Directory | ✗ | ✗ | ✗ | ✗ | ✗ |
| Integrationen | ✗ | ✗ | ✗ | ✗ | ✗ |
| Server | ✓ | ✓ (Keine Aktionen) | ✓ (Keine Aktionen) | ✓ (Keine Aktionen) | ✓ (Keine Aktionen) |
| Systemaktionen | ✓ nur Sicherung und Diagnos | ✓ nur Diagnose | ✗ | ✗ | ✗ |

| | | | | | |
|---|---|---|---|---|---|
| | e | | | | |
| Systemprotokoll | ✓ | ✓ | ✓ | ✓ | ✓ kein Syslog |
| Aktivieren (beim Setup und nach Deaktivierung) | ✗ | ✗ | ✗ | ✗ | ✗ |
| Assets löschen | ✓ | ✗ | ✗ | ✗ | ✗ |

## Zonen

Erforderliche OT Security-Benutzerrolle: Administrator

Zonen steuern, welche Assets, Ereignisse und Schwachstellen eine bestimmte Benutzergruppe sehen kann. Eine bestimmte Benutzergruppe kann nur Assets und zugehörige Schwachstellen, Ereignisse und Verbindungen anzeigen, die in ihrer Zone liegen. Sie können Konten ohne Administratorrechte einer bestimmten Gruppe und Zone zuweisen, damit sie nur relevante Assets sehen können.

### Zonen erstellen

### So erstellen Sie Zonen:

1. Gehen Sie zu Einstellungen > Benutzerverwaltung > Zonen.

   Die Seite Zonen wird angezeigt.

2. Klicken Sie in der oberen rechten Ecke auf Erstellen.

   Der Bereich Zone erstellen wird angezeigt.

3. Geben Sie im Feld Name einen Namen für die Zone ein.
4. Wählen Sie im Feld Asset-Gruppen die Gruppen aus, die Sie der Zone zuweisen möchten. Sie können das Suchfeld verwenden, um nach einer bestimmten Asset-Gruppe zu suchen.
5. Wählen Sie im Feld Benutzergruppen die Benutzergruppen aus, die Sie der Zone zuweisen möchten.
6. (Optional) Geben Sie im Feld Beschreibung eine Beschreibung für die Zone ein.
7. Klicken Sie auf Erstellen.

   Die Zone wird von OT Security erstellt und auf der Seite Zonen angezeigt.

## Zonen anzeigen

1. Gehen Sie zu Einstellungen > Benutzerverwaltung > Zonen.

   Die Seite Zonen wird angezeigt. Auf der Seite Zonen werden die Zonen in einer Tabelle mit den folgenden Details angezeigt.

| Spalte | Beschreibung |
|---|---|
| Name | Der Name der Zone. |
| Asset-Gruppen | Die Asset-Gruppen, die der Zone zugewiesen sind. |
| Benutzergruppen | Die Benutzergruppen, die der Zone zugewiesen sind. |
| Beschreibung | Eine Beschreibung für die Zone. |
| Zuletzt geändert von | Der Benutzer, der die Zone zuletzt geändert hat. |
| Zuletzt geändert am | Das Datum, an dem die Zone zuletzt geändert wurde. |

## Zone bearbeiten

1. Gehen Sie zu Einstellungen > Benutzerverwaltung > Zonen.

   Die Seite Zonen wird angezeigt.

2. Klicken Sie auf die Zeile der Zone, die Sie bearbeiten möchten, und führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die Zone und wählen Sie Bearbeiten aus.
   - Klicken Sie in der Kopfleiste auf Aktionen > Bearbeiten.

   Der Bereich Zone bearbeiten wird angezeigt.

3. Ändern Sie die Konfiguration nach Bedarf.

4. Klicken Sie auf Speichern.

   OT Security aktualisiert die Zone.

### Zone duplizieren

1. Gehen Sie zu Einstellungen > Benutzerverwaltung > Zonen.

   Die Seite Zonen wird angezeigt.

2. Klicken Sie auf die Zeile der Zone, die Sie duplizieren möchten, und führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die Zone und wählen Sie Duplizieren aus.
   - Klicken Sie in der Kopfleiste auf Aktionen > Duplizieren.

   Der Bereich Zone duplizieren wird angezeigt.

3. Geben Sie im Feld Name einen Namen für die Zone ein.

   Der Standardwert ist der ursprüngliche Zonenname mit dem Präfix „Kopie von“.

4. Ändern Sie die Konfiguration nach Bedarf.

5. Klicken Sie auf Duplizieren.

   OT Security erstellt ein Duplikat der Zone.

### Zone löschen

Sie können Zonen löschen, die Sie nicht mehr benötigen.

> Hinweis: Sie können eine Zone nicht löschen, wenn ihr Benutzergruppen zugeordnet sind.

1. Gehen Sie zu Einstellungen > Benutzerverwaltung > Zonen.

   Die Seite Zonen wird angezeigt.

2. Klicken Sie auf die Zeile der Zone, die Sie löschen möchten, und führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die Zone und wählen Sie Löschen aus.
   - Klicken Sie in der Kopfleiste auf Aktionen > Löschen.

   OT Security löscht die Zone.

## Authentifizierungsserver

> Erforderliche OT Security-Benutzerrolle: Administrator

Auf der Seite Authentifizierungsserver werden Ihre vorhandenen Integrationen mit Authentifizierungsservern angezeigt. Sie können einen Server hinzufügen, indem Sie auf die Schaltfläche Server hinzufügen klicken.

### Active Directory

Sie können OT Security mit dem Active Directory (AD) Ihrer Organisation integrieren. Dies ermöglicht es Benutzern, sich mit ihren Active Directory-Zugangsdaten bei OT Security einzuloggen. Im Rahmen der Konfiguration richten Sie die Integration ein und ordnen dann Gruppen in Ihrem AD zu Benutzergruppen in OT Security zu.

> Hinweis: Das System wird mit einer Reihe vordefinierter Benutzergruppen geliefert, die den einzelnen verfügbaren Rollen entsprechen, z. B. Benutzergruppe „Administratoren“ > Rolle „Administrator“ und Benutzergruppe „Site-Operatoren“ > Rolle „Site-Operator“. Eine Erläuterung der verfügbaren Rollen finden Sie unter Authentifizierungsserver.

## So konfigurieren Sie Active Directory:

1. Optional können Sie ein CA-Zertifikat von der Zertifizierungsstelle Ihrer Organisation oder vom Netzwerkadministrator beziehen und es auf Ihren lokalen Rechner laden.
2. Gehen Sie zu Einstellungen > Benutzerverwaltung > Authentifizierungsserver.

   Das Fenster Authentifizierungsserver wird angezeigt.
3. Klicken Sie auf Server hinzufügen.

   Der Bereich Authentifizierungsserver erstellen mit dem Servertyp wird geöffnet.
4. Klicken Sie auf Active Directory und dann auf Weiter.

   Der Konfigurationsbereich Active Directory wird angezeigt.
5. Geben Sie im Feld Name den Namen ein, der im Login-Bildschirm verwendet werden soll.
6. Geben Sie im Feld Domäne den FQDN der Organisationsdomäne ein (z. B. firma.com).

   > Hinweis: Wenn Sie Ihren Domänennamen nicht kennen, können Sie nach ihm suchen, indem Sie den Befehl „set“ in die Windows-Eingabeaufforderung oder -Befehlszeile eingeben. Der für das Attribut „USERDNSDOMAIN“ angegebene Wert ist der Domänenname.
7. Geben Sie im Feld Basis-DN den Distinguished Name der Domäne ein. Das Format für diesen Wert ist „DC={Domäne der zweiten Ebene},DC={Domäne der obersten Ebene}“ (z. B.

DC=firma,DC=com).

8. Geben Sie für jede der Gruppen, die Sie aus einer AD-Gruppe einer OT Security-Benutzergruppe zuordnen möchten, den DN der AD-Gruppe in das entsprechende Feld ein.

   Um beispielsweise eine Gruppe von Benutzern der Benutzergruppe „Administratoren“ zuzuweisen, geben Sie den DN der Active Directory-Gruppe, der Sie Administratorrechte zuweisen möchten, in das Feld Administratorgruppen-DN ein.

   > Hinweis: Wenn Sie den DN der Gruppe, der Sie OT Security-Berechtigungen zuweisen möchten, nicht kennen, können Sie eine Liste aller in Ihrem Active Directory konfigurierten Gruppen anzeigen, die Benutzer enthalten, indem Sie den Befehl `dsquery group -name Users*` in die Windows-Eingabeaufforderung oder -Befehlszeile eingeben. Geben Sie den Namen der Gruppe, die Sie zuweisen möchten, im gleichen Format ein, in dem er angezeigt wird (z. B. „CN=IT_Admins,OU=Gruppen,DC=Firma,DC=Com“). Der Basis-DN muss ebenfalls am Ende jedes DN enthalten sein.

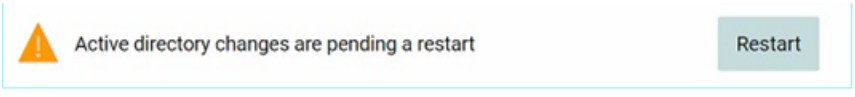
   > Hinweis: Diese Felder sind optional. Wenn ein Feld leer ist, werden dieser Benutzergruppe keine AD-Benutzer zugewiesen. Sie können eine Integration ohne zugeordnete Gruppen einrichten, aber in diesem Fall können erst dann Benutzer auf das System zugreifen, nachdem Sie mindestens eine Gruppenzuordnung hinzugefügt haben.

9. (Optional) Klicken Sie im Abschnitt Vertrauenswürdige Zertifizierungsstelle auf Durchsuchen und navigieren Sie zu der Datei, die das CA-Zertifikat Ihrer Organisation enthält (das Sie von Ihrer Zertifizierungsstelle oder Ihrem Netzwerkadministrator erhalten haben).

10. Aktivieren Sie das Kontrollkästchen Active Directory aktivieren.

11. Klicken Sie auf Speichern.

    In einer Meldung werden Sie zum Neustart des Geräts aufgefordert, um Active Directory zu aktivieren.

12. Klicken Sie auf Neu starten.

Das Gerät startet neu. Beim Neustart aktiviert OT Security die Active Directory-Einstellungen. Jeder Benutzer, der den festgelegten Gruppen zugewiesen ist, kann mit den Zugangsdaten der Organisation auf die OT Security-Plattform zugreifen.

> Hinweis: Um sich über Active Directory einzuloggen, muss der Benutzerprinzipalname (User Principal Name, UPN) auf der Login-Seite verwendet werden. In einigen Fällen muss hierfür einfach nur „@<Domäne>.com“ zum Benutzernamen hinzugefügt werden.

### LDAP

Sie können OT Security mit dem LDAP Ihrer Organisation integrieren. Dies ermöglicht es Benutzern, sich mit ihren LDAP-Zugangsdaten bei OT Security einzuloggen. Im Rahmen der Konfiguration richten Sie die Integration ein und ordnen dann Gruppen in Ihrem AD zu Benutzergruppen in OT Security zu.

#### So konfigurieren Sie LDAP:

1. Gehen Sie zu Einstellungen > Benutzerverwaltung > Authentifizierungsserver.
2. Klicken Sie auf Server hinzufügen.

   Der Bereich Authentifizierungsserver hinzufügen mit dem Servertyp wird geöffnet.
3. Wählen Sie LDAP aus und klicken Sie dann auf Weiter.

   Der Bereich LDAP-Konfiguration wird angezeigt.
4. Geben Sie im Feld Name den Namen ein, der im Login-Bildschirm verwendet werden soll.

   > Hinweis: Der Login-Name muss eindeutig sein und darauf hinweisen, dass er für LDAP verwendet wird. Falls sowohl LDAP als auch Active Directory konfiguriert sind, unterscheiden sich die verschiedenen Konfigurationen im Login-Bildschirm nur durch den Login-Namen.
5. Geben Sie im Feld Server den FQDN oder die Login-Adresse ein.

> Hinweis: Wenn Sie eine sichere Verbindung nutzen, empfiehlt Tenable, den FQDN anstelle einer IP-Adresse zu verwenden, um sicherzustellen, dass das bereitgestellte sichere Zertifikat verifiziert wird.

> Hinweis: Wenn ein Hostname verwendet wird, muss er in der Liste der DNS-Server im OT Security-System enthalten sein. Siehe Systemkonfiguration > Gerät.

6. Geben Sie im Feld Port den Wert 389 ein, um eine nicht sichere Verbindung zu verwenden, oder 636, um eine sichere SSL-Verbindung zu nutzen.

   > Hinweis: Wenn Port 636 gewählt wird, ist ein Zertifikat erforderlich, um die Integration abzuschließen.

7. Geben Sie im Feld Benutzer-DN den DN mit Parametern im DN-Format ein. Beispiel: Für den Servernamen „adsrv1.tenable.com“ kann der Benutzer-DN `CN=Administrator,CN=Benutzer,DC=adsrv1,DC=tenable,DC=com` lauten.

8. Geben Sie im Feld Passwort das Passwort des Benutzer-DN ein.

   > Hinweis: Die OT Security-Konfiguration mit LDAP funktioniert nur so lange, wie das Passwort des Benutzer-DN gültig ist. Falls sich das Passwort des Benutzer-DN ändert oder abläuft, muss daher auch die OT Security-Konfiguration aktualisiert werden.

9. Geben Sie im Feld Basis-DN des Benutzers den Basis-Domänennamen im DN-Format ein. Beispiel: Für den Servernamen „adsrv1.tenable.com“ kann der Basis-DN des Benutzers `OU=Benutzer,DC=adsrv1,DC=tenable,DC=com` lauten.

10. Geben Sie im Feld Basis-DN der Gruppe den Basis-Domänennamen der Gruppe im DN-Format ein. Beispiel: Für den Servernamen „adsrv1.tenable.com“ kann der Basis-DN der Gruppe `OU=Gruppe,DC=adsrv1,DC=tenable,DC=com` lauten.

11. Geben Sie im Feld Domänenanhang die Standarddomäne ein, die an die Authentifizierungsanforderung angehängt wird, falls der Benutzer keine Domäne angewendet hat, in der er Mitglied ist.

12. Geben Sie in die relevanten Gruppennamenfelder die Tenable-Gruppennamen ein, die der Benutzer mit der LDAP-Konfiguration verwenden soll.
13. Wenn Sie Port 636 für die Konfiguration verwenden, klicken Sie unter Vertrauenswürdige Zertifizierungsstelle auf Durchsuchen und navigieren Sie zu einer gültigen PEM-Zertifikatdatei.
14. Klicken Sie auf Speichern.

    OT Security startet den Server im Modus Deaktiviert.
15. Um die Konfiguration zu übernehmen, stellen Sie den Umschalter auf EIN.

    Das Dialogfeld Systemneustart wird angezeigt.
16. Klicken Sie auf Jetzt neu starten, um das System sofort neu zu starten und die Konfiguration anzuwenden, oder auf Später neu starten, um das System vorübergehend ohne die neue Konfiguration weiterzuverwenden.

    > Hinweis: Die Aktivierung/Deaktivierung der LDAP-Konfiguration wird erst abgeschlossen, wenn das System neu gestartet wird. Wenn Sie das System nicht sofort neu starten, klicken Sie im Banner am oberen Bildschirmrand auf die Schaltfläche Neu starten, wenn Sie zum Neustart bereit sind.

## SAML

> Erforderliche OT Security-Benutzerrolle: Administrator

Sie können OT Security mit dem Identitätsanbieter Ihrer Organisation (z. B. Microsoft Azure) integrieren. Dies ermöglicht es Benutzern, sich über ihren Identitätsanbieter zu authentifizieren. Die Konfiguration beinhaltet die Einrichtung der Integration, indem Sie eine OT Security-Anwendung innerhalb Ihres Identitätsanbieters erstellen, Informationen über Ihre erstellte OT Security-Anwendung eingeben, das Zertifikat Ihres Identitätsanbieters auf die OT Security-Seite SAML hochladen und dann Gruppen von Ihrem Identitätsanbieter zu Benutzergruppen in OT Security

zuordnen. Eine ausführliche Anleitung zur Integration von OT Security mit Microsoft Azure finden Sie unter Anhang – SAML-Integration für Microsoft Azure.

So konfigurieren Sie SAML:

1. Gehen Sie zu Einstellungen > Benutzerverwaltung > SAML.
2. Klicken Sie auf Konfigurieren.

   Daraufhin wird der Bereich SAML konfigurieren angezeigt.
3. Geben Sie im Feld IDP-ID die ID des Identitätsanbieters für die OT Security-Anwendung ein.
4. Geben Sie im Feld IDP-URL die URL des Identitätsanbieters für die OT Security-Anwendung ein.
5. Klicken Sie unter Zertifikatdaten auf Datei hier ablegen, navigieren Sie zur Zertifikatdatei des Identitätsanbieters, die Sie zur Verwendung mit der OT Security-Anwendung heruntergeladen haben, und öffnen Sie sie.
6. Geben Sie im Feld Username-Attribut das Username-Attribut vom Identitätsanbieter für die OT Security-Anwendung ein.
7. Geben Sie im Feld Groups-Attribut das Groups-Attribut vom Identitätsanbieter für die OT Security-Anwendung ein.
8. (Optional) Geben Sie im Feld Beschreibung eine Beschreibung ein.
9. Rufen Sie für jede Gruppenzuordnung, die Sie konfigurieren möchten, die Gruppenobjekt-ID des Identitätsanbieters für eine Gruppe von Benutzern auf und geben Sie sie im Feld der gewünschten Gruppenobjekt-ID ein, um sie der gewünschten OT Security-Benutzergruppe zuzuordnen.
10. Klicken Sie auf Speichern, um die Informationen im Seitenbereich zu speichern und diesen zu schließen.

11. Klicken Sie im Fenster SAML auf den Umschalter SAML Single Sign-On-Login, um das Single Sign-On-Login zu aktivieren.

    Das Benachrichtigungsfenster Systemneustart wird angezeigt.

12. Klicken Sie auf Jetzt neu starten, um das System sofort neu zu starten und die SAML-Konfiguration anzuwenden, oder klicken Sie auf Später neu starten, um die Anwendung der SAML-Konfiguration auf den nächsten Neustart des Systems zu verschieben. Wenn Sie sich für einen späteren Neustart entscheiden, wird das folgende Banner in OT Security angezeigt, bis der Neustart abgeschlossen ist:

    Beim Neustart werden die Einstellungen aktiviert und alle Benutzer, die den festgelegten Gruppen zugewiesen sind, können mit den Zugangsdaten ihres Identitätsanbieters auf die OT Security-Plattform zugreifen.

## Gruppen

Gruppen sind die grundlegenden Bausteine zum Erstellen von Richtlinien. Wenn Sie eine Richtlinie konfigurieren, legen Sie jede Richtlinienbedingung mit Gruppen anstatt mit einzelnen Entitäten fest. OT Security wird mit einigen vordefinierten Gruppen geliefert. Sie können außerdem Ihre eigenen benutzerdefinierten Gruppen erstellen. Um den Prozess der Bearbeitung und Erstellung von Richtlinien zu optimieren, empfiehlt Tenable, die benötigten Gruppen im Voraus zu konfigurieren.

> Hinweis: Richtlinienparameter können nur mithilfe von Gruppen festgelegt werden. Wenn Sie möchten, dass eine Richtlinie für eine einzelne Entität gilt, müssen Sie eine Gruppe konfigurieren, die nur diese Entität umfasst.

### Gruppen anzeigen

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager, Sicherheitsanalyst, Site-Operator, Schreibgeschützt

So zeigen Sie Gruppen an:

1. Gehen Sie zu Einstellungen > Gruppen.

   Der Abschnitt Gruppen wird erweitert und zeigt die Gruppentypen an.

Unter Gruppen können Sie alle Gruppen anzeigen, die in Ihrem System konfiguriert wurden. Gruppen sind in zwei Kategorien unterteilt:

- Vordefinierte Gruppen – Diese Gruppen sind vorkonfiguriert. Sie können diese Gruppen nicht bearbeiten.
- Benutzerdefinierte Gruppen – Diese Gruppen können Sie erstellen und bearbeiten.

Es gibt mehrere verschiedene Arten von Gruppen, von denen jede für die Konfiguration verschiedener Richtlinientypen verwendet wird. Jeder Gruppentyp wird auf einem separaten Bildschirm unter „Gruppen“ angezeigt. Die Gruppentypen sind:

- Asset-Gruppen und Tags – Assets sind Hardware-Einheiten im Netzwerk. Asset-Gruppen werden als Richtlinienbedingung für eine Vielzahl von Richtlinientypen verwendet.
- E-Mail-Gruppen – Gruppen von E-Mail-Adressen, die benachrichtigt werden, wenn ein Richtlinienereignis eintritt. Wird für alle Richtlinientypen verwendet.
- Port-Gruppen – Gruppen von Ports, die von Assets im Netzwerk verwendet werden. Wird für Richtlinien verwendet, die offene Ports identifizieren.
- Protokollgruppen – Gruppen von Protokollen, mit denen Konversationen zwischen Assets im Netzwerk geführt werden. Wird als Richtlinienbedingung für Netzwerkereignisse verwendet.
- Planungsgruppen – Planungsgruppen sind Zeitbereiche, mit denen die Zeit konfiguriert wird, zu der das angegebene Ereignis eintreten muss, um die Richtlinienbedingungen zu erfüllen.

- Controller-Tag-Gruppen – Tags sind Parameter in Controllern, die spezifische Betriebsdaten enthalten. Tag-Gruppen werden als Richtlinienbedingung für SCADA-Ereignisse verwendet.
- Regelgruppen – Regelgruppen bestehen aus einer Gruppe verwandter Regeln, die durch ihre Suricata-Signatur-IDs (SIDs) identifiziert werden. Diese Gruppen werden als Richtlinienbedingung zum Definieren von Intrusion Detection-Richtlinien verwendet.

Das Verfahren zum Erstellen der einzelnen Gruppentypen wird in den folgenden Abschnitten beschrieben. Darüber hinaus können Sie eine vorhandene Gruppe anzeigen, bearbeiten, duplizieren oder löschen, siehe Aktionen für Gruppen.

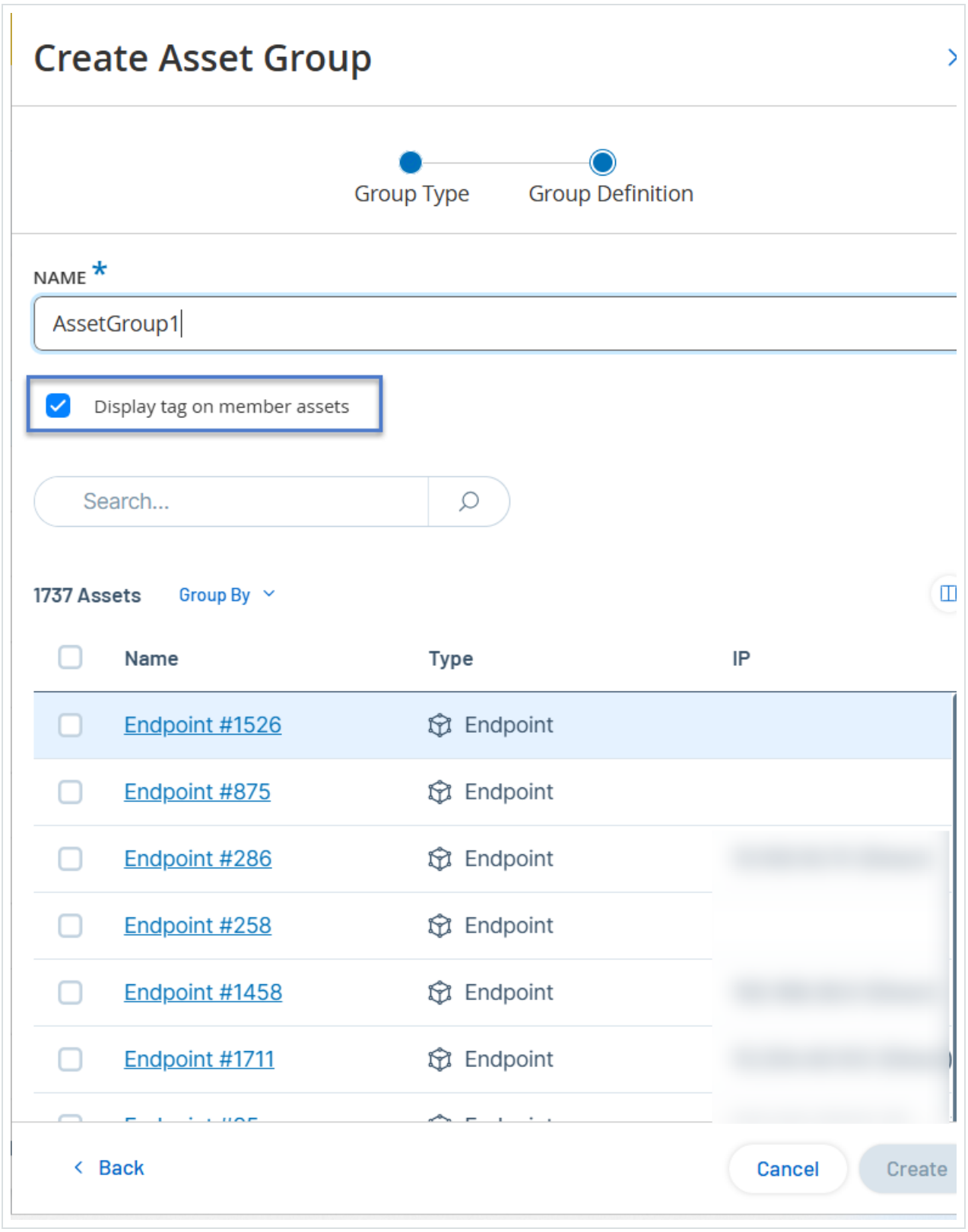
## Asset-Gruppen und Tags

Assets sind Hardwareentitäten im Netzwerk. Durch Gruppieren ähnlicher Assets können Sie Richtlinien erstellen, die für alle Assets in der Gruppe gelten. Beispielsweise könnten Sie eine Asset-Gruppe „Controller“ verwenden, um eine Richtlinie zu erstellen, die bei Firmware-Änderungen an einem Controller warnt. Asset-Gruppen werden als Richtlinienbedingung für eine Vielzahl von Richtlinientypen verwendet. Asset-Gruppen können verwendet werden, um das Quell-Asset, das Ziel-Asset oder das betroffene Asset für verschiedene Richtlinientypen anzugeben.

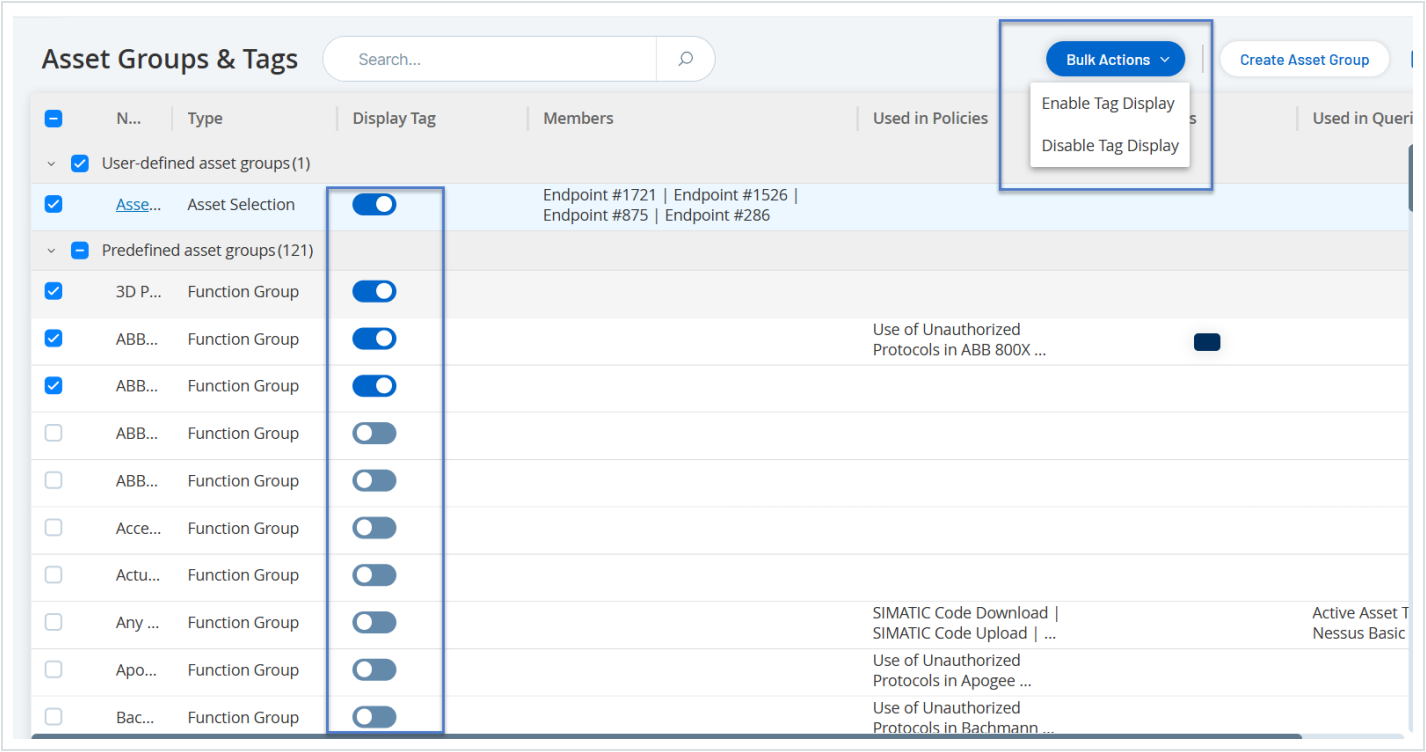
### Tags

Tags helfen dabei, Assets basierend auf einem bestimmten Kriterium zu gruppieren, sodass Sie verschiedene Workflows optimieren und priorisieren können. Wenn Sie Gruppen erstellen, konvertiert OT Security diese in Tags für Ihre Assets.

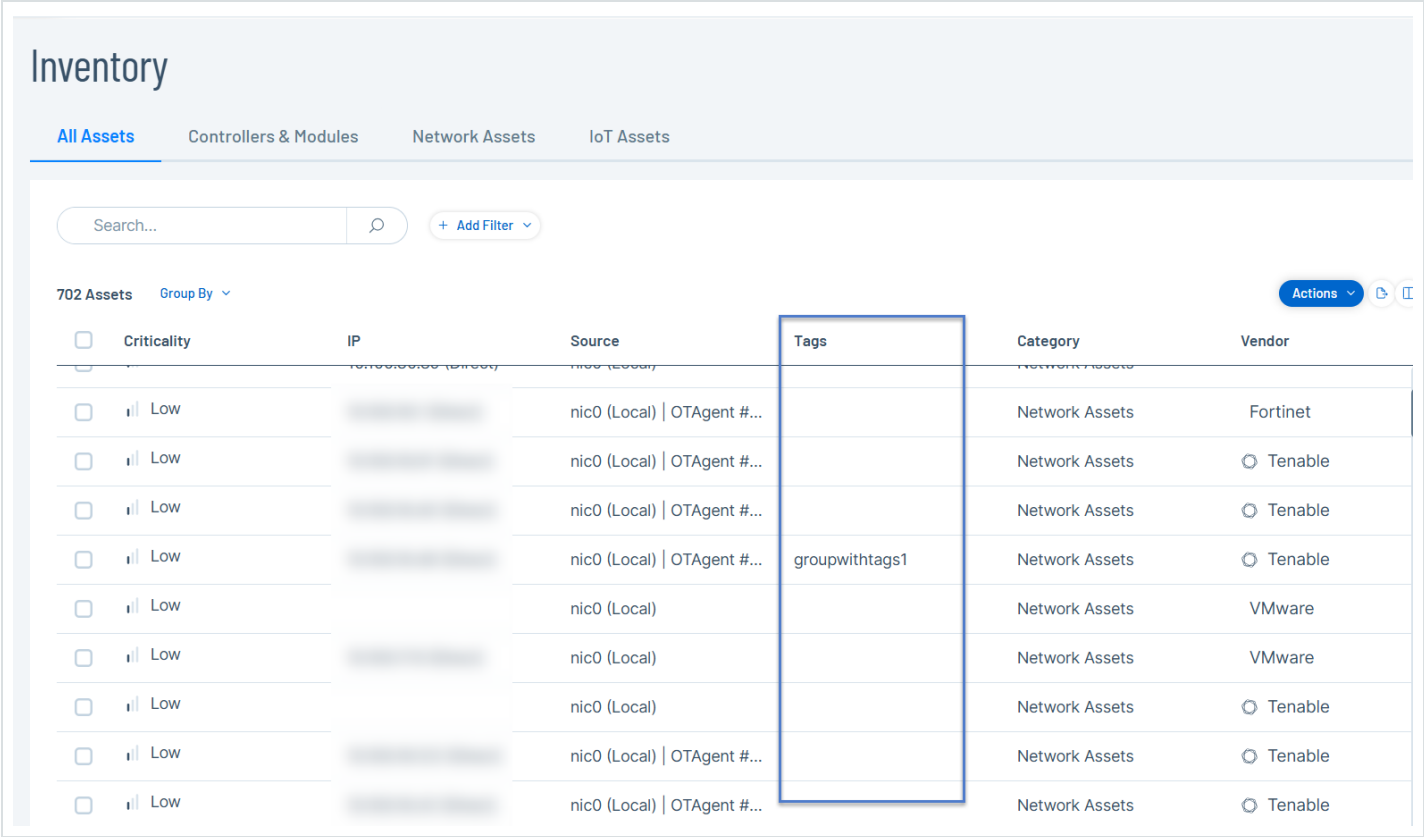
Um die Tags für Assets anzuzeigen, aktivieren Sie beim Erstellen von Asset-Gruppen das Kontrollkästchen Tag für Mitglieds-Assets anzeigen.


Create Asset Group
Group Type
Group Definition
NAME *
AssetGroup1
Display tag on member assets
Search...
1737 Assets
Group By
Name
Type
IP
Endpoint #1526
Endpoint
Endpoint #875
Endpoint
Endpoint #286
Endpoint
Endpoint #258
Endpoint
Endpoint #1458
Endpoint
Endpoint #1711
Endpoint
Back
Cancel
Create

Um die Anzeige von Tags für mehrere Assets zu aktivieren oder zu deaktivieren, wählen Sie mehrere Assets aus und wählen Sie im Menü Massenaktionen nach Bedarf die Option Tag-Anzeige aktivieren oder Tag-Anzeige deaktivieren aus. Außerdem können Sie den Umschalter in der Spalte Tag anzeigen für die einzelnen Assets aktivieren oder deaktivieren.




Diese Asset-Gruppen werden in der Spalte Tags auf der Seite Inventar > Alle Assets angezeigt.




## Asset-Gruppen und Tags anzeigen

Der Bildschirm Asset-Gruppen zeigt alle Asset-Gruppen, die derzeit im System konfiguriert sind. Die Registerkarte Vordefinierte Asset-Gruppen enthält Gruppen, die in das System integriert sind und die Sie nicht bearbeiten, duplizieren oder löschen können. Die Registerkarte Benutzerdefinierte Asset-Gruppen enthält benutzerdefinierte Gruppen, die vom Benutzer erstellt wurden. Sie können diese Gruppen bearbeiten, duplizieren oder löschen.

Die Tabelle „Asset-Gruppen“ enthält die folgenden Informationen:

| Parameter | Beschreibung |
|---|---|
| Status | Zeigt an, ob die Richtlinie aktiviert oder deaktiviert ist. Wenn das System die Richtlinie automatisch deaktiviert, weil sie zu viele Ereignisse generiert hat, wird ein Warnsymbol angezeigt. Schalten Sie den Status-Schalter um, um eine Richtlinie zu aktivieren/deaktivieren. |

| | |
|---|---|
| ID | Die ID, die der Asset-Gruppe zugewiesen ist. |
| Name | Der Name der Richtlinie. |
| Tag anzeigen | Der Umschalter, um die Anzeige der Tags auf der Seite Inventar > Alle Assets zu aktivieren. |
| Schweregrad | Der Schweregrad des Ereignisses. Mögliche Werte sind: Kein, Gering, Mittel oder Hoch. Weitere Informationen finden Sie in Abschnitt Schweregradstufen. |
| Ursprung | Der Ursprung der Asset-Gruppe: Benutzerdefiniert oder Systemdefiniert. |
| Ereignistyp | Der Ereignistyp, der diese Ereignisrichtlinie auslöst. |
| Kategorie | Die allgemeine Kategorie des Ereignisses, das diese Ereignisrichtlinie auslöst. Mögliche Werte sind: Konfiguration, SCADA, Netzwerkbedrohungen oder Netzwerkereignis. Eine Erläuterung der verschiedenen Kategorien finden Sie unter Richtlinienkategorien und Unterkategorien. |
| Quelle | Eine Richtlinienbedingung. Die Quell-Asset-Gruppe, für die die Richtlinie gilt. Eine Asset-Gruppe ist das Asset, das die Aktivität initiiert hat. |
| Name | Der Name zur Identifizierung der Gruppe. |
| Typ | Der Gruppentyp. Optionen sind:<br>• Funktion – Eine vordefinierte Asset-Gruppe, die erstellt wurde, um eine bestimmte Funktion zu erfüllen.<br>• Asset-Liste – Angegebene Assets sind in der Gruppe enthalten.<br>• IP-Liste – Assets mit der angegebenen IP-Adresse.<br>• IP-Bereich – Assets innerhalb des angegebenen Bereichs von IP- |

| | |
|---|---|
| | Adressen. |
| Typ | Der Gruppentyp. Verfügbare Optionen sind Statisch oder Dynamisch. |
| Mitglieder | Zeigt die Liste der Assets an, die in dieser Gruppe enthalten sind. Für Funktionsgruppen wird kein Wert angezeigt.<br><br>Hinweis: Wenn in dieser Zeile nicht genug Platz ist, um alle Assets anzuzeigen, klicken Sie auf Tabellenaktionen > Anzeigen > Registerkarte Mitglieder. |
| In Richtlinien verwendet | Zeigt den Namen jeder Richtlinie an, die diese Asset-Gruppe in ihrer Konfiguration verwendet.<br><br>Hinweis: Um weitere Details zu den Richtlinien anzuzeigen, in denen die Gruppe verwendet wird, klicken Sie auf Tabellenaktionen > Anzeigen > Registerkarte In Richtlinien verwendet. |
| In Abfragen verwendet | Zeigt den Namen der Abfrage an, die diese Asset-Gruppe verwendet. |
| In Zonen verwendet | Zeigt den Namen der Zone an, die diese Asset-Gruppe verwendet. |

Die Verfahren zum Erstellen verschiedener Typen von Asset-Gruppen werden im folgenden Abschnitt beschrieben. Darüber hinaus können Sie eine vorhandene Gruppe anzeigen, bearbeiten, duplizieren oder löschen, siehe Aktionen für Gruppen.

## Asset-Gruppen erstellen

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager

Sie können benutzerdefinierte Asset-Gruppen erstellen, um sie bei der Konfiguration von Richtlinien zu verwenden. Indem Sie ähnliche Assets in Gruppen zusammenfassen, können Sie Richtlinien erstellen, die für alle Assets in der Gruppe gelten.

Es gibt drei Arten von benutzerdefinierten Asset-Gruppen:

- Asset-Auswahl – Angabe der Assets, die in der Gruppe enthalten sind.
- IP-Liste – Angabe der IP-Adressen der Assets, die in der Gruppe enthalten sind.
- IP-Bereich – Angabe des Bereichs der IP-Adressen der Assets, die in der Gruppe enthalten sind.

Hinweis: Verwenden Sie für duplizierte Netzwerke die Option Asset-Auswahl, um eine Asset-Gruppe zu erstellen.

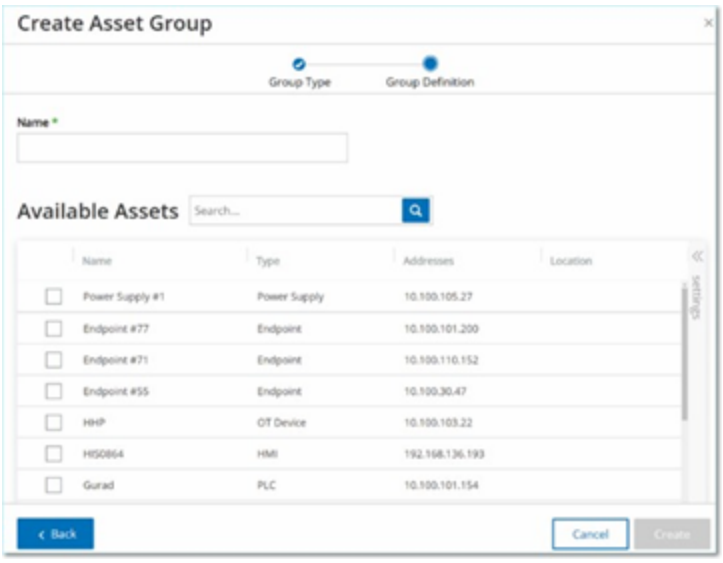
Es gibt verschiedene Verfahren zum Erstellen der einzelnen Arten von Asset-Gruppen.

So erstellen Sie eine Asset-Gruppe vom Typ „Asset-Auswahl“:

1. Gehen Sie zu Einstellungen > Gruppen > Asset-Gruppen.
2. Klicken Sie auf Asset-Gruppe erstellen.

   Der Bereich Asset-Gruppe erstellen wird angezeigt.
3. Klicken Sie auf Asset-Auswahl.
4. Klicken Sie auf Weiter.

   Die Liste der verfügbaren Assets wird angezeigt.




5. Um die Tags für die Assets anzuzeigen, aktivieren Sie das Kontrollkästchen Tag für Mitglieds-Assets anzeigen.

   > Hinweis: Wenn diese Option ausgewählt ist, zeigt OT Security die Tags in der Spalte Tags auf der Seite Inventar > Alle Assets an.

6. Geben Sie im Feld Name einen Namen für die Gruppe ein.

   Wählen Sie einen Namen, der ein gemeinsames Element beschreibt, das die in der Gruppe enthaltenen Assets kategorisiert.

7. Aktivieren Sie das Kontrollkästchen neben jedem Asset, das Sie in die Gruppe aufnehmen möchten.

8. Klicken Sie auf Erstellen.

   OT Security erstellt die neue Asset-Gruppe und zeigt sie im Bildschirm Asset-Gruppen an. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

So erstellen Sie eine Asset-Gruppe vom Typ „IP-Bereich“:

1. Gehen Sie zu Einstellungen > Gruppen > Asset-Gruppen.
2. Klicken Sie auf Asset-Gruppe erstellen.

Der Bereich Asset-Gruppe erstellen wird angezeigt.

3. Klicken Sie auf IP-Bereich.
4. Klicken Sie auf Weiter.

   Der Fensterbereich zur Auswahl des IP-Bereichs wird angezeigt.

5. Geben Sie im Feld Name einen Namen für die Gruppe ein.

   Wählen Sie einen Namen, der ein gemeinsames Element beschreibt, das die in der Gruppe enthaltenen Assets kategorisiert.

6. Geben Sie im Feld Start-IP die IP-Adresse am Anfang des Bereichs ein, den Sie einschließen möchten.
7. Geben Sie im Feld End-IP die IP-Adresse am Ende des Bereichs ein, den Sie einschließen möchten.
8. Klicken Sie auf Erstellen.

   OT Security erstellt die neue Asset-Gruppe und zeigt sie im Bildschirm Asset-Gruppen an. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

So erstellen Sie eine Asset-Gruppe vom Typ „IP-Liste“:

1. Gehen Sie zu Einstellungen > Gruppen > Asset-Gruppen.
2. Klicken Sie auf Asset-Gruppe erstellen.

   Der Bereich Asset-Gruppe erstellen wird angezeigt.

3. Klicken Sie auf IP-Liste.
4. Klicken Sie auf Weiter.

   Der Bereich IP-Liste wird angezeigt.

5. Geben Sie im Feld Name einen Namen für die Gruppe ein.

Wählen Sie einen Namen, der ein gemeinsames Element beschreibt, das die in der Gruppe enthaltenen Assets kategorisiert.

6. Geben Sie im Feld IP-Liste eine IP-Adresse oder ein Subnetz ein, die bzw. das in die Gruppe aufgenommen werden soll.
7. Um der Gruppe weitere Assets hinzuzufügen, geben Sie jede zusätzliche IP-Adresse oder jedes zusätzliche Subnetz in einer separaten Zeile ein.
8. Klicken Sie auf Erstellen.

   OT Security erstellt die neue Asset-Gruppe und zeigt sie im Bildschirm Asset-Gruppen an. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

## Asset-Gruppen und Tags erstellen

Sie können benutzerdefinierte Asset-Gruppen erstellen, um sie bei der Konfiguration von Richtlinien zu verwenden. Durch Gruppieren ähnlicher Assets können Sie Richtlinien erstellen, die für alle Assets in der Gruppe gelten. Sie können Gruppen erstellen, indem Sie entweder die gewünschten Assets auswählen oder eine Filterregel festlegen, um Assets in einer bestimmten Kategorie zu gruppieren. Die dynamische Gruppierung von Assets basierend auf ausgewählten Kriterien hilft Ihnen, Prozesse wie Priorisierung und Reporting zu optimieren und zu skalieren.

## So erstellen Sie eine Asset-Gruppe:

1. Gehen Sie zu Gruppen > Asset-Gruppen und Tags.

   Die Seite Asset-Gruppen und Tags wird angezeigt.
2. Um eine Asset-Gruppe zu erstellen, klicken Sie auf Asset-Gruppe erstellen.

   Das Fenster Asset-Gruppe erstellen wird angezeigt.
3. Wählen Sie im Abschnitt Gruppentyp eine der folgenden Optionen aus:

- Statisch (Manuelle Auswahl) – Statische Asset-Gruppen werden definiert, indem Assets manuell ausgewählt und zur Gruppe hinzugefügt werden. Nachdem Sie die Gruppe festgelegt haben, ändern sich ihre Mitglieder nicht, es sei denn, Sie bearbeiten sie.
- Dynamisch (Regelbasiert) – Dynamische Asset-Gruppen verwenden Regeln, um Ihr Asset Inventory zu filtern. Da die Asset-Erfassung und -Anreicherung fortlaufend ist, werden Mitglieder automatisch zur Gruppe hinzugefügt oder daraus entfernt, sodass sie stets auf dem neuesten Stand ist.

4. Klicken Sie auf Weiter.

   Der Bereich Gruppendefinition wird angezeigt.

5. Geben Sie im Feld Name einen Namen für die Asset-Gruppe ein. Wählen Sie einen Namen, der ein gemeinsames Element beschreibt, das die in der Gruppe enthaltenen Assets kategorisiert.

6. Wenn Sie Statisch ausgewählt haben, gehen Sie wie folgt vor:

   a. Aktivieren Sie die Kontrollkästchen neben den Assets, die Sie der Gruppe hinzufügen möchten.

7. Wenn Sie Dynamisch ausgewählt haben, klicken Sie auf Filter hinzufügen, um eine Regel für die Gruppenerstellung zu aktivieren. Siehe Assets filtern.

   > Hinweis: Sie müssen mindestens einen Filter hinzufügen, um die Gruppenerstellung zu ermöglichen.

8. Um die Tags für die einzelnen Assets anzuzeigen, aktivieren Sie das Kontrollkästchen Tag für Mitglieds-Assets anzeigen. Diese Option ist standardmäßig aktiviert.

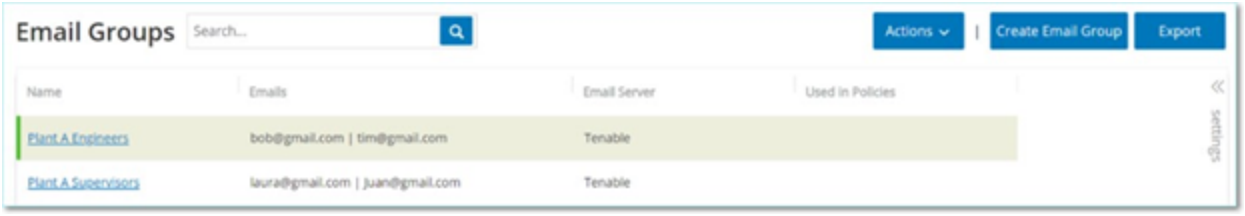
9. Klicken Sie auf Erstellen.

   OT Security erstellt die Asset-Gruppe und zeigt sie auf der Seite Asset-Gruppen und Tags an. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

## E-Mail-Gruppen

E-Mail-Gruppen sind Gruppen von E-Mail-Adressen relevanter Parteien. E-Mail-Gruppen werden verwendet, um Empfänger für Ereignisbenachrichtigungen anzugeben, die durch bestimmte Richtlinien ausgelöst werden. Eine Gruppierung nach Rolle und Abteilung ermöglicht es Ihnen beispielsweise, die Benachrichtigungen für bestimmte Richtlinienereignisse an die relevanten Parteien zu senden.

## E-Mail-Gruppen anzeigen




Der Bildschirm E-Mail-Gruppen zeigt alle E-Mail-Gruppen, die derzeit im System konfiguriert sind.

Die Tabelle „E-Mail-Gruppen“ enthält die folgenden Informationen:

> Hinweis: Sie können zusätzliche Details zu einer bestimmten Gruppe anzeigen, indem Sie die Gruppe auswählen und auf Aktionen > Anzeigen klicken.

| Parameter | Beschreibung |
|---|---|
| Name | Der Name zur Identifizierung der Gruppe. |
| E-Mails | Die Liste der in der Gruppe enthaltenen E-Mails.<br><br>> Hinweis: Wenn nicht genügend Platz vorhanden ist, um alle Mitglieder der Gruppe anzuzeigen, klicken Sie auf Aktionen > Anzeigen > Registerkarte Mitglieder. |
| E-Mail-Server | Der Name des SMTP-Servers, der zum Senden von E-Mails an die Gruppe verwendet wird. |
| In Richtlinien verwendet | Zeigt die Namen der Richtlinien an, für die Benachrichtigungen an diese Gruppe gesendet werden. |

| | |
|---|---|
| | Hinweis: Um weitere Details zu den Richtlinien anzuzeigen, in denen die Gruppe verwendet wird, klicken Sie auf Aktionen > Anzeigen > Registerkarte In Richtlinien verwendet. |

Darüber hinaus können Sie eine vorhandene Gruppe anzeigen, bearbeiten, duplizieren oder löschen. Weitere Informationen finden Sie unter Aktionen für Gruppen.

## E-Mail-Gruppen erstellen

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager

Sie können E-Mail-Gruppen erstellen, die bei der Konfiguration von Richtlinien verwendet werden. Indem Sie zusammengehörige E-Mail-Adressen gruppieren, legen Sie fest, dass Benachrichtigungen zu Richtlinienereignissen an alle relevanten Mitarbeiter gesendet werden.

Hinweis: Sie können jeder Richtlinie nur eine E-Mail-Gruppe zuweisen. Daher ist es sinnvoll, sowohl weit gefasste, allgemeine Gruppen als auch spezifische, begrenzte Gruppen zu erstellen, damit Sie jeder Richtlinie die entsprechende Gruppe zuweisen können.

### So erstellen Sie eine E-Mail-Gruppe:

1. Gehen Sie zu Einstellungen > Gruppen > E-Mail-Gruppen.
2. Klicken Sie auf E-Mail-Gruppe erstellen.

   Der Bereich E-Mail-Gruppe erstellen wird angezeigt.
3. Geben Sie im Feld Name einen Namen für die Gruppe ein.
4. Wählen Sie im Dropdown-Feld SMTP-Server den Server aus, der zum Versenden der E-Mail-Benachrichtigungen verwendet wird.

   Hinweis: Wenn im System kein SMTP-Server konfiguriert ist, müssen Sie zuerst einen Server konfigurieren, bevor Sie eine E-Mail-Gruppe erstellen können, siehe SMTP-Server.

5. Geben Sie im Feld E-Mails die E-Mail-Adresse jedes Mitglieds der Gruppe in einer separaten Zeile ein.
6. Klicken Sie auf Erstellen.

   OT Security erstellt die neue E-Mail-Gruppe und zeigt sie auf der Seite E-Mail-Gruppen an. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

## Port-Gruppen

Port-Gruppen sind Gruppen von Ports, die von Assets im Netzwerk verwendet werden. Port-Gruppen werden als Richtlinienbedingung zum Definieren von Netzwerkereignis-Richtlinien für offene Ports verwendet, die offene Ports im Netzwerk erkennen.

Die Registerkarte Vordefiniert zeigt die im System vordefinierten Portgruppen. Diese Gruppen umfassen Ports, von denen erwartet wird, dass sie auf Controllern eines bestimmten Anbieters offen sind. Beispielsweise umfasst die Gruppe „Siemens-SPS – Offene Ports“: 20, 21, 80, 102, 443 und 502. Dies ermöglicht die Konfiguration von Richtlinien, die offene Ports erkennen, von denen nicht erwartet wird, dass sie für Controller von diesem Anbieter geöffnet sind. Diese Gruppen können nicht bearbeitet oder gelöscht werden, sie können aber dupliziert werden.

Die Registerkarte Benutzerdefiniert enthält benutzerdefinierte Gruppen, die vom Benutzer erstellt wurden. Sie können diese Gruppen bearbeiten, duplizieren oder löschen.

### Port-Gruppen anzeigen

Die Tabelle „Port-Gruppen“ enthält die folgenden Details:

| Parameter | Beschreibung |
|---|---|
| Name | Der Name zur Identifizierung der Gruppe. |
| TCP-Port | Die Liste der Ports und/oder Port-Bereiche, die in der Gruppe enthalten sind. |

| | |
|---|---|
| | Hinweis: Wenn in der Tabelle nicht alle Mitglieder der Gruppe angezeigt werden, klicken Sie auf Aktionen > Anzeigen > Registerkarte Mitglieder, um die Mitglieder anzuzeigen. |
| In Richtlinien verwendet | Zeigt den Namen jeder Richtlinie an, die diese Port-Gruppe in ihrer Konfiguration verwendet.<br><br>Hinweis: Um weitere Informationen zu den Richtlinien anzuzeigen, in denen diese Gruppe verwendet wird, klicken Sie auf Aktionen > Anzeigen > Registerkarte In Richtlinien verwendet. |

## Port-Gruppen erstellen

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager

Sie können benutzerdefinierte Port-Gruppen erstellen, die Sie bei der Konfiguration von Richtlinien verwenden können. Durch Gruppieren ähnlicher Ports ermöglichen Sie die Erstellung von Richtlinien, die vor offenen Ports warnen, die ein besonderes Sicherheitsrisiko darstellen.

### So erstellen Sie eine Port-Gruppe:

1. Gehen Sie zu Einstellungen > Gruppen > Port-Gruppen.
2. Klicken Sie auf Port-Gruppe erstellen.

   Der Bereich Port-Gruppe erstellen wird angezeigt.
3. Geben Sie im Feld Name einen Namen für die Gruppe ein.
4. Geben Sie im Feld TCP-Port einen einzelnen Port oder einen Bereich von Ports ein, die in die Gruppe aufgenommen werden sollen.
5. So fügen Sie der Gruppe weitere Ports hinzu:

a. Klicken Sie auf + Port hinzufügen.

   Ein Feld zur Auswahl eines neuen Ports wird angezeigt.

b. Geben Sie im neuen Feld Port-Nummer einen einzelnen Port oder einen Bereich von Ports ein, die in die Gruppe aufgenommen werden sollen.

6. Klicken Sie auf Erstellen.

   OT Security erstellt die neue Port-Gruppe und zeigt sie in der Liste der Port-Gruppen an. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

## Protokollgruppen

Protokollgruppen sind Gruppen von Protokollen, die für Konversationen zwischen Assets im Netzwerk verwendet werden. Protokollgruppen sind eine Richtlinienbedingung für Netzwerkrichtlinien. Außerdem definieren sie, welche Protokolle, die zwischen bestimmten Assets verwendet werden, eine Richtlinie auslösen.

OT Security enthält eine Reihe vordefinierter Protokollgruppen, die verwandte Protokolle umfassen. Diese Gruppen stehen zur Verwendung in Richtlinien zur Verfügung. Sie können diese Gruppen nicht bearbeiten oder löschen. Protokolle können danach gruppiert werden, welche Protokolle von einem bestimmten Anbieter zugelassen werden.

Zu den von Schneider zugelassenen Protokollen gehören beispielsweise: TCP:80 (HTTP), TCP:21 (FTP), Modbus, Modbus_UMAS, Modbus_MODICON, TCP:44818 (CIP), UDP:69 (TFTP), UDP:161 (SNMP), UDP :162 (SNMP), UDP:44818, UDP:67-68 (DHCP). Sie können auch nach Protokolltyp, z. B. Modbus, PROFINET und CIP, gruppiert werden. Sie können außerdem Ihre eigenen benutzerdefinierten Protokollgruppen erstellen.

### Protokollgruppen anzeigen

Der Bildschirm Protokollgruppen zeigt alle Protokollgruppen an, die derzeit im System konfiguriert sind. Die Registerkarte Vordefiniert zeigt die in das System integrierten Gruppen an. Sie können

diese Gruppen nicht bearbeiten oder löschen, aber Sie können sie duplizieren. Die Registerkarte Benutzerdefiniert zeigt die benutzerdefinierten Gruppen, die Sie erstellt haben. Sie können diese Gruppen bearbeiten, duplizieren oder löschen.

Die Tabelle „Protokollgruppen“ enthält diese Details:

| Parameter | Beschreibung |
|---|---|
| Name | Der Name zur Identifizierung der Gruppe. |
| Protokolle | Die Liste der Protokolle, die in der Gruppe enthalten sind.<br><br>Hinweis: Wenn Sie nicht alle Mitglieder der Gruppe anzeigen können, klicken Sie auf die Registerkarte Aktionen > Anzeigen > Mitglieder. |
| In Richtlinien verwendet | Zeigt den Namen jeder Richtlinie an, die diese Protokollgruppe in ihrer Konfiguration verwendet.<br><br>Hinweis: Um weitere Details zu den Richtlinien anzuzeigen, in denen diese Gruppe verwendet wird, klicken Sie auf Aktionen > Anzeigen > Registerkarte In Richtlinien verwendet. |

## Protokollgruppen erstellen

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager

Sie können benutzerdefinierte Protokollgruppen erstellen, die bei der Konfiguration von Richtlinien verwendet werden. Durch die Gruppierung ähnlicher Protokolle ermöglichen Sie die Erstellung von Richtlinien, die festlegen, welche Protokolle verdächtig sind.

### So erstellen Sie eine Protokollgruppe:

1. Gehen Sie zu Einstellungen > Gruppen > Protokollgruppen.
2. Klicken Sie auf Protokollgruppe erstellen.

Der Bereich Protokollgruppe erstellen wird angezeigt.

3. Geben Sie im Feld Name einen Namen für die Gruppe ein.
4. Wählen Sie im Dropdown-Feld Protokolle einen Protokolltyp aus.
5. Wenn das ausgewählte Protokoll TCP oder UDP ist, geben Sie im Feld Port eine Port-Nummer oder einen Bereich von Ports ein.

   Bei anderen Protokolltypen müssen Sie keinen Wert in das Feld Port eingeben.
6. So fügen Sie der Gruppe weitere Protokolle hinzu:

   a. Klicken Sie auf + Protokoll hinzufügen.

      Ein neues Protokollauswahl-Feld wird angezeigt.

   b. Füllen Sie die neue Protokollauswahl wie in den Schritten 4 bis 5 beschrieben aus.
7. Klicken Sie auf Erstellen.

   OT Security erstellt die neue Protokollgruppe und zeigt sie in der Liste der Protokollgruppen an. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

## Planungsgruppe

Eine Planungsgruppe definiert einen Zeitbereich oder eine Gruppe von Zeitbereichen, die bestimmte Merkmale aufweisen, die in diesem Zeitraum stattfindende Aktivitäten erwähnenswert machen. Beispielsweise wird erwartet, dass bestimmte Aktivitäten während der Arbeitszeit stattfinden, während andere Aktivitäten voraussichtlich während der Ruhezeiten stattfinden.

### Planungsgruppen anzeigen

Der Bildschirm Planungsgruppen zeigt alle Planungsgruppen, die derzeit im System konfiguriert sind. Die Registerkarte Vordefinierte Planungsgruppen enthält die in das System integrierten Gruppen. Sie können diese Gruppen nicht bearbeiten, duplizieren oder löschen. Die Registerkarte

Benutzerdefinierte Planungsgruppen zeigt die benutzerdefinierten Gruppen, die Sie erstellt haben. Sie können diese Gruppen bearbeiten, duplizieren oder löschen.

Die Tabelle „Planungsgruppen“ enthält die folgenden Details:

| Parameter | Beschreibung |
|---|---|
| Name | Der Name zur Identifizierung der Gruppe. |
| Typ | Der Gruppentyp. Optionen sind:<br>• Funktion – Eine vordefinierte Planungsgruppe, die erstellt wurde, um eine bestimmte Funktion zu erfüllen.<br>• Wiederkehrend – Ein Zeitplan, der sich täglich oder wöchentlich wiederholt. Beispielsweise kann ein Arbeitszeitplan als Zeitraum von Montag bis Freitag von 9:00 bis 17:00 Uhr definiert werden.<br>• Intervall – Ein Zeitplan, der an einem bestimmten Datum oder in einem bestimmten Datumsbereich liegt. Ein Zeitplan für die Renovierung einer Anlage könnte zum Beispiel durch den Zeitraum vom 1. Juni bis zum 15. August definiert werden. |
| Zeitplan | Eine Zusammenfassung der Planungseinstellungen.<br>Hinweis: Wenn Sie nicht alle Mitglieder der Gruppe anzeigen können, klicken Sie auf die Registerkarte Aktionen > Anzeigen > Mitglieder. |
| In Richtlinien verwendet | Zeigt die Richtlinien-ID jeder Richtlinie an, die diese Planungsgruppe in ihrer Konfiguration verwendet.<br>Hinweis: Um weitere Details zu den Richtlinien anzuzeigen, in denen diese Gruppe verwendet wird, klicken Sie auf Aktionen > Anzeigen > Registerkarte In Richtlinien verwendet. |

## Planungsgruppen erstellen

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager

Sie können benutzerdefinierte Planungsgruppen erstellen, die bei der Konfiguration von Richtlinien verwendet werden. Geben Sie einen Zeitbereich oder eine Gruppe von Zeitbereichen mit gemeinsamen Merkmale an, um Ereignisse hervorzugeben, die in diesem Zeitraum stattfinden.

Es gibt zwei Arten von Planungsgruppen:

- Wiederkehrend – Zeitpläne, die sich wöchentlich wiederholen. Beispielsweise kann ein Arbeitszeitplan als Zeitraum von Montag bis Freitag von 9:00 bis 17:00 Uhr definiert werden.
- Einmalig – Zeitpläne, die an einem bestimmten Datum oder in einem bestimmten Datumsbereich liegen. Ein Zeitplan für die Renovierung einer Anlage könnte zum Beispiel durch den Zeitraum vom 1. Juni bis zum 15. August definiert werden. Es gibt verschiedene Verfahren zum Erstellen der einzelnen Arten von Planungsgruppen.

Es gibt verschiedene Verfahren zum Erstellen der einzelnen Arten von Planungsgruppen.

## So erstellen Sie eine Planungsgruppe vom Typ „Wiederkehrend“:

1. Gehen Sie zu Einstellungen > Gruppen > Planungsgruppen.

   Die Seite **Planungsgruppen** wird angezeigt.

2. Klicken Sie auf Planungsgruppe erstellen.

   Der Bereich Planungsgruppen erstellen wird angezeigt.

3. Klicken Sie auf Wiederkehrend.

4. Klicken Sie auf Weiter.

   Die Parameter zum Definieren einer wiederkehrenden Planungsgruppe werden angezeigt.

5. Geben Sie im Feld Name einen Namen für die Gruppe ein.

6. Wählen Sie im Feld Wird wiederholt aus, welche Wochentage in die Planungsgruppe aufgenommen werden.

   Optionen sind: Täglich, Montag bis Freitag oder ein bestimmter Wochentag.

   > Hinweis: Wenn Sie bestimmte Wochentage einbeziehen möchten, z. B. Montag und Mittwoch, müssen Sie für jeden Tag eine eigene Bedingung hinzufügen.

7. Geben Sie im Feld Startzeit die Tageszeit (HH:MM:SS AM/PM) für den Beginn des Zeitbereichs ein, der in der Planungsgruppe enthalten ist.
8. Geben Sie im Feld Endzeit die Tageszeit (HH:MM:SS AM/PM) für das Ende des Zeitbereichs ein, der in der Planungsgruppe enthalten ist.
9. So fügen Sie der Planungsgruppe weitere Bedingungen (d. h. zusätzliche Zeitbereiche) hinzu:
   a. Klicken Sie auf + Bedingung hinzufügen.

      Eine neue Zeile mit Planungsauswahlparametern wird angezeigt.

   b. Füllen Sie die Zeitplanfelder wie oben in Schritt 5 bis 7 beschrieben aus.
10. Klicken Sie auf Erstellen.

    OT Security erstellt die neue Planungsgruppe und zeigt sie in der Liste der Planungsgruppen an. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

### So erstellen Sie eine einmalige Planungsgruppe:

1. Gehen Sie zu Einstellungen > Gruppen > Planungsgruppen.
2. Klicken Sie auf Planungsgruppe erstellen.

   Der Assistent Planungsgruppe erstellen wird angezeigt.

3. Wählen Sie Zeitraum aus.
4. Klicken Sie auf Weiter.

Die Parameter zum Definieren einer Zeitraum-Planungsgruppe werden angezeigt.

5. Geben Sie im Feld Name einen Namen für die Gruppe ein.
6. Klicken Sie im Feld Startdatum auf das Kalendersymbol.

   Ein Kalenderfenster wird geöffnet.

7. Wählen Sie das Datum aus, an dem die Planungsgruppe beginnt. Standard: das aktuelle Datum.
8. Geben Sie im Feld Startzeit die Tageszeit (HH:MM:SS AM/PM) für den Beginn des Zeitbereichs ein, der in der Planungsgruppe enthalten ist.
9. Klicken Sie im Feld Enddatum auf das Kalendersymbol.

   Ein Kalenderfenster wird geöffnet.

10. Wählen Sie das Datum aus, an dem die Planungsgruppe endet. (Standard: das aktuelle Datum)
11. Geben Sie im Feld Endzeit die Tageszeit (HH:MM:SS AM/PM) für das Ende des Zeitbereichs ein, der in der Planungsgruppe enthalten ist.
12. Klicken Sie auf Erstellen.

    OT Security erstellt die neue Planungsgruppe und zeigt sie in der Liste der Planungsgruppen an. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

## Controller-Tag-Gruppen

Tags sind Parameter in Controllern, die spezifische Betriebsdaten enthalten. Controller-Tag-Gruppen werden als Richtlinienbedingung für Richtlinien für SCADA-Ereignisse verwendet. Durch Gruppieren von Tags, die ähnliche Rollen spielen, können Sie Richtlinien erstellen, die verdächtige Änderungen an den angegebenen Parametern erkennen. Indem Sie beispielsweise Tags

gruppieren, die die Ofentemperatur steuern, können Sie eine Richtlinie erstellen, die Temperaturänderungen erkennt, die für die Öfen schädlich sein könnten.

## Controller-Tag-Gruppen anzeigen

Auf der Seite Controller-Tag-Gruppen werden alle Tag-Gruppen angezeigt, die derzeit im System konfiguriert sind.

Die Tabelle „Controller-Tag-Gruppen“ enthält die folgenden Details:

| Parameter | Beschreibung |
|---|---|
| Name | Der Name zur Identifizierung der Gruppe. |
| Typ | Der Datentyp des Tags. Mögliche Werte sind: „Bool“, „Dint“, „Float“, „Int“, „Long“, „Short“, „Unknown (für Tags eines Typs, den OT Security nicht identifizieren konnte) oder „Any Type“ (was Tags verschiedener Typen umfassen kann). |
| Controller | Der Controller, auf dem das Tag überwacht wird. |
| Tags | Zeigt jedes in der Gruppe enthaltene Tag sowie den Namen des Controllers an, in dem es sich befindet.<br><br>Hinweis: Wenn Sie nicht alle Tags in dieser Zeile sehen können, klicken Sie auf Aktionen > Anzeigen > Registerkarte Mitglieder. |
| In Richtlinien verwendet | Zeigt die Richtlinien-ID jeder Richtlinie an, die diese Planungsgruppe in ihrer Konfiguration verwendet.<br><br>Hinweis: Um weitere Details zu den Richtlinien anzuzeigen, in denen diese Gruppe verwendet wird, klicken Sie auf Aktionen > Anzeigen > Registerkarte In Richtlinien verwendet. |

Sie können eine vorhandene Gruppe anzeigen, bearbeiten, duplizieren oder löschen, siehe Aktionen für Gruppen.

## Controller-Tag-Gruppen erstellen

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager

Sie können benutzerdefinierte Controller-Tag-Gruppen zur Verwendung in der Richtlinienkonfiguration erstellen. Durch Gruppieren ähnlicher Tags können Sie Richtlinien erstellen, die für alle Tags in der Gruppe gelten. Wählen Sie die Tags ähnlichen Typs aus und geben Sie ihnen einen Namen, der das gemeinsame Element der Tags darstellt.

Sie können auch Gruppen erstellen, die Tags unterschiedlicher Typen enthalten, indem Sie die Option Any Type (Beliebiger Typ) auswählen. In diesem Fall können Richtlinien, die auf diese Gruppe angewendet werden, nur Änderungen an Beliebiger Wert für die angegebenen Tags erkennen. Sie können jedoch nicht so festgelegt werden, dass sie bestimmte Werte erkennen.

Sie können Controller-Tag-Gruppen bearbeiten, duplizieren oder löschen.

### So erstellen Sie eine neue Tag-Gruppe:

1. Gehen Sie zu Einstellungen > Gruppen > Controller-Tag-Gruppen.
2. Klicken Sie auf Controller-Tag-Gruppe erstellen.

   Der Bereich Controller-Tag-Gruppe erstellen wird angezeigt.
3. Wählen Sie einen Tag-Typ aus.

   Optionen sind: „Bool“, „Dint“, „Float“, „Int“, „Long“, „Short“ oder „Any Type“ (was Tags verschiedener Typen umfassen kann).
4. Klicken Sie auf Weiter.

   Eine Liste der Controller in Ihrem Netzwerk wird angezeigt.
5. Wählen Sie einen Controller aus, für den Sie Tags in die Gruppe aufnehmen möchten.

6. Klicken Sie auf Weiter.

   Eine Liste von Tags des angegebenen Typs auf dem angegebenen Controller wird angezeigt.

7. Geben Sie im Feld Name einen Namen für die Gruppe ein.

8. Aktivieren Sie das Kontrollkästchen neben jedem Tag, das Sie in die Gruppe aufnehmen möchten.

9. Klicken Sie auf Erstellen.

   OT Security erstellt die neue Tag-Gruppe und zeigt sie in der Liste der Controller-Tag-Gruppen an. Sie können diese Gruppe jetzt beim Konfigurieren von SCADA-Ereignisrichtlinien verwenden.

## Regelgruppen

Regelgruppen bestehen aus einer Gruppe verwandter Regeln, die durch ihre Suricata-Signatur-IDs (SIDs) identifiziert werden. Diese Gruppen werden als Richtlinienbedingung zum Definieren von Intrusion Detection-Richtlinien verwendet.

OT Security bietet eine Reihe vordefinierter Gruppen verwandter Schwachstellen. Darüber hinaus können Sie einzelne Regeln aus unserem Schwachstellen-Repository auswählen und Ihre eigenen benutzerdefinierten Regelgruppen erstellen.

### Regelgruppen anzeigen

Der Bildschirm Regelgruppen zeigt alle Regelgruppen, die derzeit im System konfiguriert sind. Die Registerkarte „Vordefiniert“ umfasst die in das System integrierten Gruppen. Sie können diese Gruppen nicht bearbeiten, duplizieren oder löschen. Die Registerkarte Benutzerdefiniert zeigt die benutzerdefinierten Gruppen, die vom Benutzer erstellt wurden. Sie können diese Gruppen bearbeiten, duplizieren oder löschen.

Die Tabelle „Regelgruppen“ enthält die folgenden Details:

| Parameter | Beschreibung |
|---|---|
| Name | Der Name zur Identifizierung der Gruppe. |
| Anzahl an Regeln | Die Anzahl der Regeln (SIDs), aus denen diese Regelgruppe besteht. |
| In Richtlinien verwendet | Zeigt die Richtlinien-ID jeder Richtlinie an, die diese Regelgruppe in ihrer Konfiguration verwendet.<br><br>Hinweis: Um weitere Details zu den Richtlinien anzuzeigen, in denen diese Gruppe verwendet wird, klicken Sie auf Aktionen > Anzeigen > Registerkarte In Richtlinien verwendet. |

## Regelgruppen erstellen

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager

### So erstellen Sie eine neue Regelgruppe:

1. Gehen Sie zu Einstellungen > Gruppen > Regelgruppen.
2. Klicken Sie auf Regelgruppe erstellen.

   Der Bereich Regelgruppe erstellen wird angezeigt.
3. Geben Sie im Feld Name einen Namen für die Gruppe ein.
4. Aktivieren Sie im Abschnitt Verfügbare Regeln das Kontrollkästchen neben jeder Regel, die Sie in die Gruppe aufnehmen möchten.

   Hinweis: Verwenden Sie das Suchfeld, um die gewünschten Regeln zu finden.
5. Klicken Sie auf Erstellen.

OT Security erstellt die neue Regelgruppe und zeigt sie in der Liste der Regelgruppen an. Sie können diese Gruppe jetzt beim Konfigurieren von Intrusion Detection-Richtlinien verwenden.

## Aktionen für Gruppen

Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor, Sicherheitsmanager

Wenn Sie eine Gruppe in einem der Gruppen-Bildschirme auswählen, können Sie im Menü Aktionen oben im Bildschirm die folgenden Aktionen ausführen:

- Anzeigen – Zeigt Details zur ausgewählten Gruppe an, z. B. welche Entitäten in der Gruppe enthalten sind und welche Richtlinien die Gruppe als Richtlinienbedingung verwenden. Siehe Gruppendetails anzeigen
- Bearbeiten – Hier können Sie die Details der Gruppe bearbeiten. Siehe Gruppe bearbeiten
- Duplizieren – Ermöglicht das Erstellen einer neuen Gruppe mit einer ähnlichen Konfiguration wie die angegebene Gruppe. Siehe Gruppe duplizieren
- Löschen – Ermöglicht das Löschen der Gruppe aus dem System. Siehe Gruppe löschen

  Hinweis: Sie können vordefinierte Gruppen nicht bearbeiten oder löschen. Einige vordefinierte Gruppen können auch nicht dupliziert werden. Sie können das Menü Aktionen auch aufrufen, indem Sie mit der rechten Maustaste auf eine Gruppe klicken.

### Gruppendetails anzeigen

Wenn Sie eine Gruppe auswählen und auf Aktionen > Anzeigen klicken, wird der Bildschirm „Gruppendetails“ für die ausgewählte Gruppe geöffnet.

Der Bildschirm Gruppendetails enthält eine Kopfleiste, die den Namen und Typ der Gruppe zeigt. Er hat zwei Registerkarten:

- Mitglieder – Zeigt eine Liste aller Mitglieder der Gruppe.
- In Richtlinien verwendet – Zeigt eine Liste für jede Richtlinie, für die die angegebene Gruppe als Richtlinienbedingung verwendet wird. Die Richtlinienliste enthält einen Umschalter zum Aktivieren/Deaktivieren der Richtlinie. Weitere Informationen finden Sie unter Richtlinien anzeigen.

### So zeigen Sie Details einer Gruppe an:

1. Wählen Sie unter Gruppen den gewünschten Gruppentyp aus.

   Die Seite für den ausgewählten Gruppentyp wird angezeigt.

2. Wählen Sie die Gruppe aus, die Sie anzeigen möchten.

   In OT Security wird die Schaltfläche Aktionen aktiviert.

3. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf Aktionen und wählen Sie Anzeigen aus.
   - Klicken Sie mit der rechten Maustaste auf die gewünschte Gruppe und wählen Sie Anzeigen aus.

4. Wählen Sie Anzeigen aus.

   Die Seite mit Gruppendetails wird angezeigt.

## Gruppe bearbeiten

Sie können die Details einer bestehenden Gruppe bearbeiten.

### So bearbeiten Sie Details einer Gruppe:

1. Wählen Sie unter Gruppen den gewünschten Gruppentyp aus.

   Die Seite für den ausgewählten Gruppentyp wird angezeigt.

2. Wählen Sie auf der Seite Gruppen die Gruppe aus, die Sie bearbeiten möchten.

In OT Security wird die Schaltfläche Aktionen aktiviert.

3. Führen Sie einen der folgenden Schritte aus:

    - Klicken Sie auf Aktionen und wählen Sie Bearbeiten aus.
    - Klicken Sie mit der rechten Maustaste auf die gewünschte Gruppe und wählen Sie Bearbeiten aus.

4. Wählen Sie Bearbeiten aus.
5. Das Fenster Gruppe bearbeiten mit den relevanten Parametern für den angegebenen Gruppentyp wird angezeigt.
6. Ändern Sie die Parameter nach Bedarf.
7. Klicken Sie auf Speichern.

    OT Security speichert die Gruppe mit den neuen Einstellungen.

### Gruppe duplizieren

Um eine neue Gruppe mit ähnlichen Einstellungen wie eine bestehende Gruppe zu erstellen, können Sie die vorhandene Gruppe duplizieren. Wenn Sie eine Gruppe duplizieren, wird die neue Gruppe zusätzlich zur ursprünglichen Gruppe unter einem neuen Namen gespeichert.

### So duplizieren Sie eine Gruppe:

1. Wählen Sie unter Gruppen den gewünschten Gruppentyp aus.

    Die Seite für den ausgewählten Gruppentyp wird angezeigt.

2. Wählen Sie die Gruppe aus, die Sie duplizieren möchten.

    In OT Security wird die Schaltfläche Aktionen aktiviert.

3. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf Aktionen und wählen Sie Duplizieren aus.
- Klicken Sie mit der rechten Maustaste auf die gewünschte Gruppe und wählen Sie Duplizieren aus.

4. Wählen Sie Duplizieren aus.

   Das Fenster Gruppe duplizieren mit den relevanten Parametern für den angegebenen Gruppentyp wird angezeigt.

5. Geben Sie im Feld Name einen Namen für die neue Gruppe ein. Standardmäßig heißt die neue Gruppe „Kopie von <Name der ursprünglichen Gruppe>“.
6. Nehmen Sie die gewünschten Änderungen an den Gruppeneinstellungen vor.
7. Klicken Sie auf Duplizieren.

   OT Security speichert die neue Gruppe zusätzlich zur vorhandenen Gruppe mit den neuen Einstellungen.

### Gruppe löschen

Sie können benutzerdefinierte Gruppen löschen. Vordefinierte Gruppen können nicht gelöscht werden. Eine benutzerdefinierte Richtlinie, die als Richtlinienbedingung für eine oder mehrere Richtlinien verwendet wird, kann nicht gelöscht werden.

### So löschen Sie eine Gruppe:

1. Wählen Sie unter Gruppen den gewünschten Gruppentyp aus.

   Die Seite für den ausgewählten Gruppentyp wird angezeigt.

2. Wählen Sie die Gruppe aus, die Sie löschen möchten.

   In OT Security wird die Schaltfläche Aktionen aktiviert.

3. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf Aktionen und wählen Sie Löschen aus.
- Klicken Sie mit der rechten Maustaste auf die gewünschte Gruppe und wählen Sie Löschen aus.

4. Wählen Sie Löschen aus.

   Daraufhin wird ein Bestätigungsfenster angezeigt.

5. Klicken Sie auf Löschen.

   OT Security löscht die Gruppe dauerhaft aus dem System.

## Integrationen

Sie können Integrationen mit weiteren unterstützten Plattformen einrichten, damit OT Security mit Ihren anderen Cybersecurity-Plattformen synchronisiert werden kann.

### Tenable-Produkte

Sie können OT Security mit Tenable Security Center und Tenable Vulnerability Management integrieren. OT Security tauscht über diese Integrationen Daten mit den anderen Plattformen aus. Die synchronisierten Daten umfassen sowohl OT-Schwachstellen als auch Daten, die durch IT-bezogene Tenable Nessus-Scans erfasst wurden, die über OT Security initiiert wurden.

> Hinweis: OT Security sendet über die Integration keine Daten für ausgeblendete Assets an Tenable Security Center und Tenable Vulnerability Management.

> Hinweis: Um die Plattformen zu integrieren, muss OT Security Tenable Security Center und/oder Tenable Vulnerability Management über Port 443 erreichen können. Tenable empfiehlt, einen bestimmten Benutzer in Tenable Security Center und/oder Tenable Vulnerability Management zu erstellen, der als Integrationsbenutzer für OT Security verwendet werden soll.

#### Tenable Security Center

Erforderliche OT Security-Benutzerrolle: Administrator

Um Tenable Security Center zu integrieren, erstellen Sie in Tenable Security Center ein universelles Repository zur Speicherung von OT Security-Daten, und notieren Sie sich die Repository-ID. Weitere Informationen finden Sie unter Universal Repositories.

Hinweis: Tenable empfiehlt, in Tenable Security Center einen spezifischen Benutzer zu erstellen, der für die Integration mit OT Security verwendet wird. Der Benutzer sollte über die Rolle „Sicherheitsmanager/Sicherheitsanalyst“ oder „Schwachstellenanalyst“ verfügen und der Gruppe „Vollzugriff“ zugewiesen sein.

## So integrieren Sie Tenable Security Center:

1. Navigieren Sie in der Tenable OT Security-Benutzeroberfläche zu Einstellungen > Integrationen.

   Die Seite Integrationen wird angezeigt.

2. Klicken Sie in der oberen rechten Ecke auf Integrationsmodul hinzufügen.

   Der Bereich Integrationsmodul hinzufügen wird angezeigt.

3. Wählen Sie im Abschnitt Modultyp die Option Tenable Security Center aus.

4. Klicken Sie auf Weiter.

   Der Bereich Moduldefinition wird mit den relevanten Feldern angezeigt.

5. Geben Sie im Feld Hostname/IP den Hostnamen oder die IP-Adresse Ihres Tenable Security Center ein.

6. Geben Sie im Feld Benutzername die Benutzer-ID des Kontos ein.

7. Geben Sie im Feld Passwort das Passwort Ihres Kontos ein.

8. Geben Sie im Feld Repository-ID die ID des universellen Repository an.

9. Legen Sie im Dropdown-Feld Synchronisierungsfrequenz die Frequenz fest, mit der die Daten synchronisiert werden sollen.
10. Klicken Sie auf Speichern.

    OT Security erstellt die Integration und zeigt die neue Integration auf der Seite „Integrationen“ an.
11. Klicken Sie mit der rechten Maustaste auf die neue Integration und klicken Sie auf Synchronisieren.

### Tenable Vulnerability Management

Erforderliche OT Security-Benutzerrolle: Administrator

Hinweis: Sie müssen zuerst einen API-Schlüssel in der Tenable Vulnerability Management-Konsole generieren (Einstellungen (Settings) > Mein Konto (My Account) > API-Schlüssel (API Keys) > Generieren (Generate)). Sie erhalten einen Zugriffsschlüssel und einen geheimen Schlüssel, die Sie beim Konfigurieren der Integration in der OT Security-Konsole eingeben können.

#### So integrieren Sie Tenable Vulnerability Management:

1. Navigieren Sie in der Tenable OT Security-Benutzeroberfläche zu Einstellungen > Integrationen.

   Die Seite Integrationen wird angezeigt.
2. Klicken Sie in der oberen rechten Ecke auf Integrationsmodul hinzufügen.

   Der Bereich Integrationsmodul hinzufügen wird angezeigt.
3. Wählen Sie im Abschnitt Modultyp die Option Tenable Vulnerability Management aus.
4. Klicken Sie auf Weiter.

   Der Bereich Moduldefinition wird mit den relevanten Feldern angezeigt.
5. Geben Sie im Feld Zugriffsschlüssel den Zugriffsschlüssel an.

6. Geben Sie im Feld Geheimer Schlüssel den geheimen Schlüssel an.
7. Wählen Sie im Dropdown-Feld Synchronisierungsfrequenz die Frequenz aus, mit der die Daten synchronisiert werden sollen.

### Tenable One

> Erforderliche OT Security-Benutzerrolle: Administrator

Befolgen Sie zur Integration mit Tenable One die unter Mit Tenable One integrieren beschriebenen Schritte.

## Palo Alto Networks – Next Generation Firewall

> Erforderliche OT Security-Benutzerrolle: Administrator

Sie können von OT Security erfasste Asset-Inventarisierungsdaten an Ihr Palo Alto-System übertragen.

So integrieren Sie OT Security mit Ihren Palo Alto Networks Next Generation Firewalls (NGFW):

1. Navigieren Sie in der Tenable OT Security-Benutzeroberfläche zu Einstellungen > Integrationen.

   Die Seite Integrationen wird angezeigt.
2. Klicken Sie in der oberen rechten Ecke auf Integrationsmodul hinzufügen.

   Der Bereich Integrationsmodul hinzufügen wird angezeigt.
3. Wählen Sie im Abschnitt Modultyp die Option „Palo Alto Networks NGFW“ aus.
4. Klicken Sie auf Weiter.

5. Geben Sie im Feld Hostname/IP den Hostnamen oder die IP-Adresse Ihres Palo Alto Networks NGFW-Kontos ein.
6. Geben Sie im Feld Benutzername den Benutzernamen Ihres NGFW-Kontos ein.
7. Geben Sie im Feld Passwort das Passwort für Ihr NGFW-Konto ein.
8. Klicken Sie auf Speichern.

   OT Security speichert die Integration.

## Aruba – ClearPass-Richtlinienmanager

> Erforderliche OT Security-Benutzerrolle: Administrator

Sie können von OT Security erfasste Asset-Inventarisierungsdaten an Ihr Aruba-System übertragen.

So integrieren Sie OT Security mit Ihrem Aruba ClearPass-Konto:

1. Navigieren Sie in der Tenable OT Security-Benutzeroberfläche zu Einstellungen > Integrationen.

   Die Seite Integrationen wird angezeigt.
2. Klicken Sie in der oberen rechten Ecke auf Integrationsmodul hinzufügen.

   Der Bereich Integrationsmodul hinzufügen wird angezeigt.
3. Wählen Sie im Abschnitt Modultyp die Option „Aruba Networks ClearPass“ aus.
4. Klicken Sie auf Weiter.
5. Geben Sie im Feld Hostname/IP den Hostnamen oder die IP-Adresse Ihres Aruba Networks ClearPass-Kontos ein.

6. Geben Sie im Feld Benutzername den Benutzernamen Ihres Aruba Networks ClearPass-Kontos ein.
7. Geben Sie im Feld Passwort das Passwort für Ihr Aruba Networks ClearPass-Kontos ein.
8. Geben Sie im Feld Client-ID die Client-ID Ihres Aruba Networks ClearPass-Kontos ein.
9. Geben Sie im Feld API-Client-Geheimnis das API-Client-Geheimnis Ihres Aruba Networks ClearPass-Kontos ein.
10. Klicken Sie auf Speichern.

    OT Security speichert die Integration.

## Mit Tenable One integrieren

Sie können OT Security mit Tenable One integrieren und Daten zu Assets und Risikowerten in Tenable Exposure Management anzeigen.

Für die Integration mit Tenable One müssen Sie zuerst einen Linking Key in Tenable Vulnerability Management generieren und diesen in OT Security angeben. Tenable One wird regelmäßig mit allen Asset-Änderungen aktualisiert, die seit der letzten Synchronisierung erfolgt sind.

Nach der Integration sendet OT Security die folgenden Daten an Tenable One:

- OT Security synchronisiert alle Assets und Asset-Attribute mit der Seite Exposure Management > Inventar. Zu diesen Attributen gehören Anbieter, Marke, Modell, Status, Firmware und Seriennummer. Die Synchronisierung umfasst die folgenden Felder:
    - OT_BACKPLANE_ID
    - OT_BACKPLANE_NAME
    - OT_CATEGORY
    - OT_CRITICALITY

- OT_DESCRIPTION
- OT_FAMILY
- OT_FIRMWARE
- OT_ID
- OT_LOCATION
- OT_MODEL
- OT_SERIAL_NUMBER
- OT_SLOT
- OT_STATE
- OT_VENDOR
- OT_SENSOR_NAME
- OT_DIRECT_IP_ADDRESSES
- OT_RISK

- Alle mit Assets verbundenen Schwachstellenergebnisse, einschließlich Plugin-IDs, Plugin-Namen und Plugin-Ausgabe. Tenable One verwendet diese Daten, um für die einzelnen Assets zu verfolgen, ob der Schwachstellenstatus Aktiv oder Behoben lautet.
- (Version 4.4 und höher) Alle Feststellungen zu Richtlinienverstößen, die mit den einzelnen Assets verbunden sind. Zu diesen Daten gehören der Richtlinien-Ereignistyp, eine detaillierte Plugin-Ausgabe, die das Ereignis beschreibt, und die beteiligten Assets. Sie enthalten außerdem die relevanten TTPs (Tactics, Techniques, and Procedures) aus dem MITRE ATT&CK-Modell für die beobachtete Aktivität.
- (Version 4.5 und höher) Alle dynamischen Tags, die Assets zugeordnet sind. Diese werden in Tenable One als Externe Tags angezeigt.

> Hinweis: OT Security-Ergebnisse werden nicht in Tenable Vulnerability Management angezeigt, es sei denn, Sie integrieren Tenable Vulnerability Management mit OT Security oder verwenden die OT Discovery-Engine in Ihren Scans.

### Bevor Sie beginnen

- Stellen Sie sicher, dass Sie über den in Tenable Vulnerability Management generierten Linking Key verfügen. Weitere Informationen finden Sie unter OT Connectors im Benutzerhandbuch zu Tenable Vulnerability Management.

  > Hinweis: Ein in Tenable Vulnerability Management generierter Linking Key kann nur für eine einzelne OT Security-Site verwendet werden.

### So führen Sie die Integration mit Tenable One durch:

1. Navigieren Sie in der Tenable OT Security-Benutzeroberfläche zu Einstellungen > Integrationen.

   Die Seite Integrationen wird angezeigt.

2. Klicken Sie in der oberen rechten Ecke auf Integrationsmodul hinzufügen.

   Der Bereich Integrationsmodul hinzufügen wird angezeigt.

3. Klicken Sie im Abschnitt Modultyp auf **Tenable One**.

4. Klicken Sie auf Weiter.

   Der Abschnitt Moduldefinition wird angezeigt.

5. Geben Sie im Feld Cloud-Site den Namen der Cloud-Site ein.

   > Hinweis: Der Name der Cloud-Site wird im Fenster Add OT Connector von Tenable Vulnerability Management angezeigt, nachdem Sie den Linking Key generiert haben.

6. Geben Sie im Feld Linking Key den Linking Key ein, den Sie in Tenable Vulnerability Management generiert haben.

7. Klicken Sie auf Speichern.

   In OT Security wird die Meldung angezeigt, dass die Integration durchgeführt wurde. Sobald die Integration abgeschlossen ist, wird die verknüpfte Site auf der Seite Integrationen angezeigt. In Tenable One wird auf der Seite Sensors > OT Connectors der Gerätename angezeigt, der für diese Site in OT Security konfiguriert ist.

   Den Gerätenamen für eine Site finden Sie im Abschnitt Gerätename auf der Seite Systemkonfiguration > Gerät.

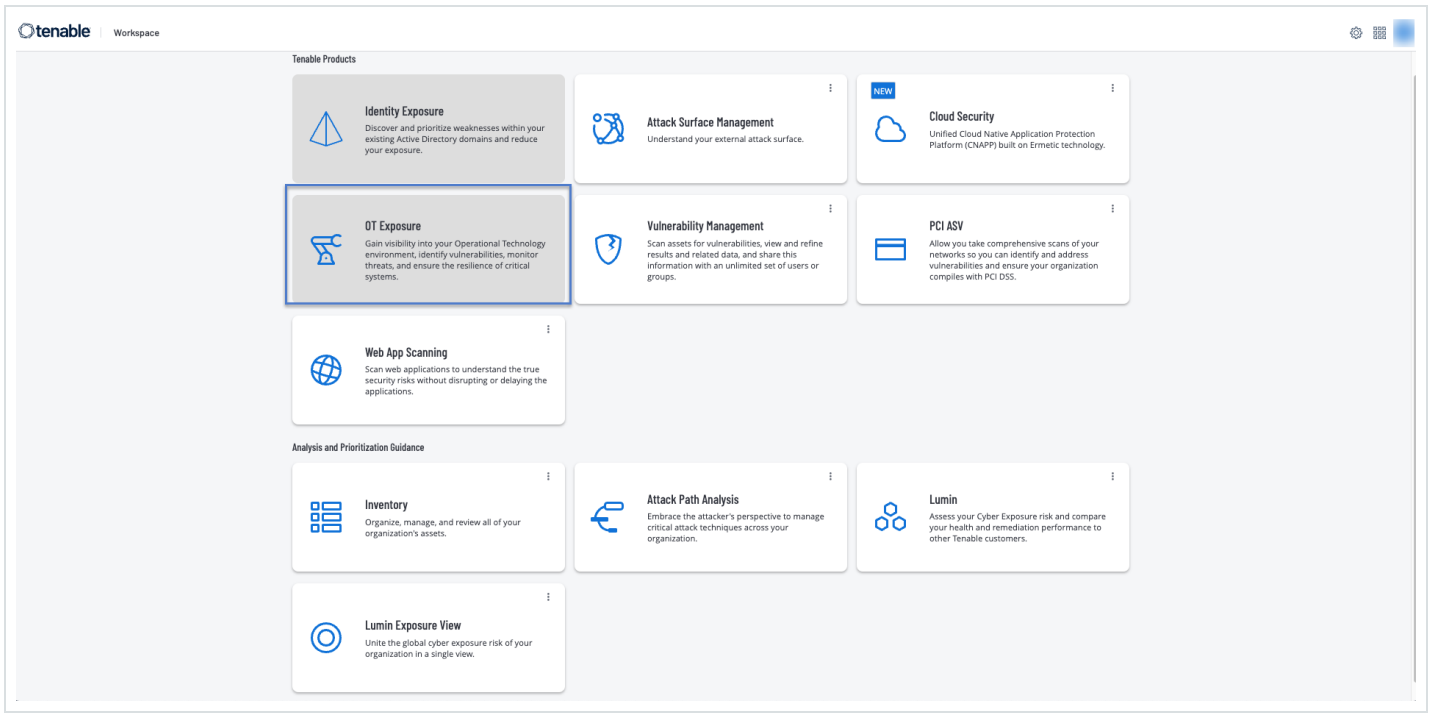
   > Hinweis: Wenn Sie den Namen Ihrer Site in OT Security ändern, nachdem die Kopplung bereits erfolgt hat, können Sie den Sensornamen in Tenable Vulnerability Management manuell so ändern, dass er dem neuen Site-Namen entspricht. Alternativ können Sie die Integration sowohl in OT Security als auch in Tenable Vulnerability Management löschen und die Kopplung erneut durchführen, um die Änderung des Site-Namens automatisch zu übernehmen.

Informationen zum vollständigen Verfahren für die Bereitstellung und Lizenzierung von Tenable OT Security für Tenable One finden Sie im Tenable One Deployment Guide.

## SAML-Integration für Tenable One konfigurieren

Konfigurieren Sie SAML auf Ihrer Tenable One-Instanz, um über SSO auf OT Security zugreifen zu können.

Die Kachel OT Exposure auf der Seite Workspace von Tenable One ist standardmäßig deaktiviert. Um die Kachel OT Exposure zu aktivieren, müssen Sie zuerst SAML für Tenable One konfigurieren.




## Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie über eine gültige Tenable One- und OT Security-Lizenz verfügen.

## So konfigurieren Sie SAML für Tenable OT Security:

1. Rufen Sie Details zum SAML-Identitätsanbieter (IDP) und Gruppenobjekt-IDs aus Tenable One ab:

    a. Loggen Sie sich in einem unterstützten Browser bei https://cloud.tenable.com ein, um auf die Seite Workspace zuzugreifen.

    b. Klicken Sie in der oberen rechten Ecke auf die Schaltfläche .

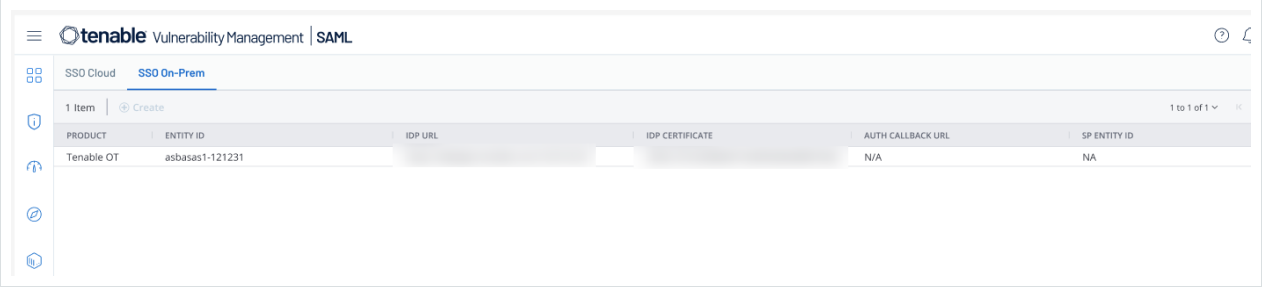
    Die Seite Settings wird angezeigt.

    c. Klicken Sie auf die Kachel SAML.

    Die Seite SAML wird angezeigt.

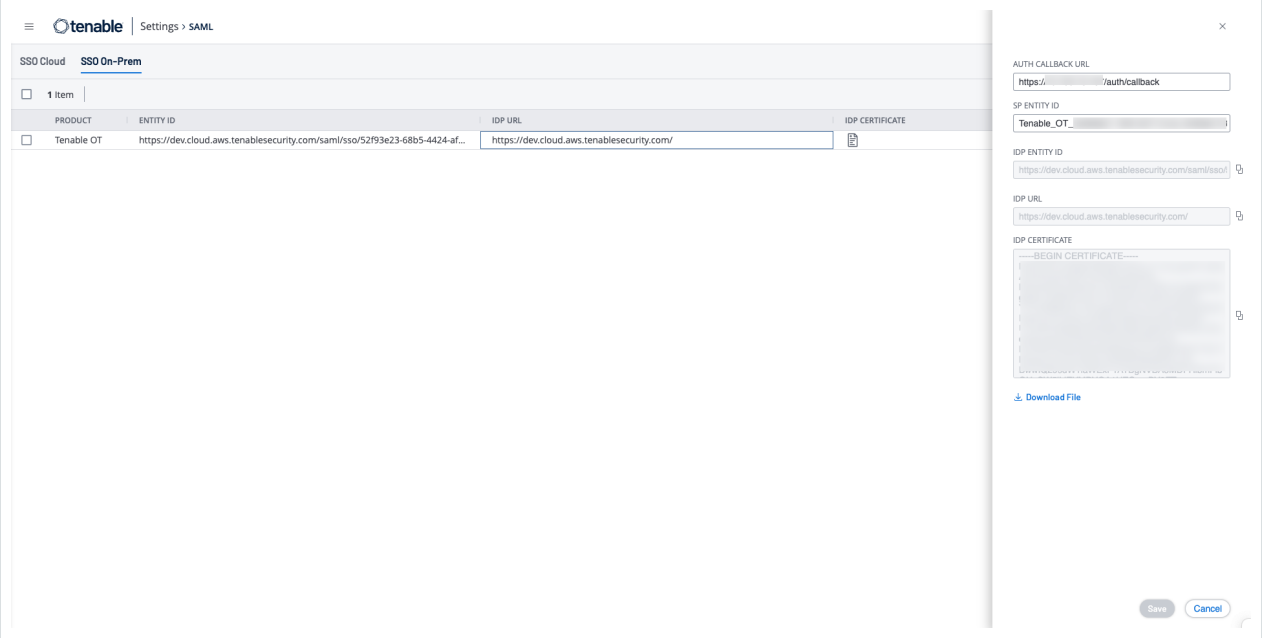
d. Klicken Sie auf die Registerkarte SSO On-Prem.

Die Seite SSO On-Prem mit der SSO-Konfiguration für Tenable OT Security wird angezeigt.




e. Bewegen Sie den Mauszeiger über die Zeile für Tenable OT Security und klicken Sie auf die Zeile.

Der Bereich mit den IDP-Details wird auf der rechten Seite angezeigt.



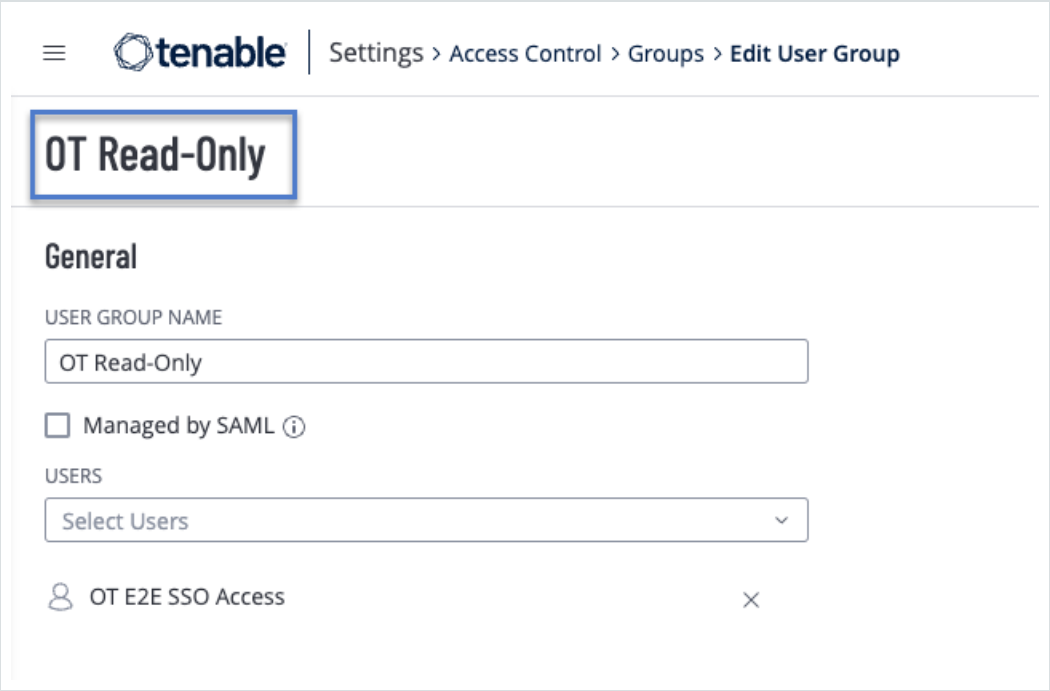

f. Kopieren Sie die folgenden Details mithilfe der Schaltfläche .

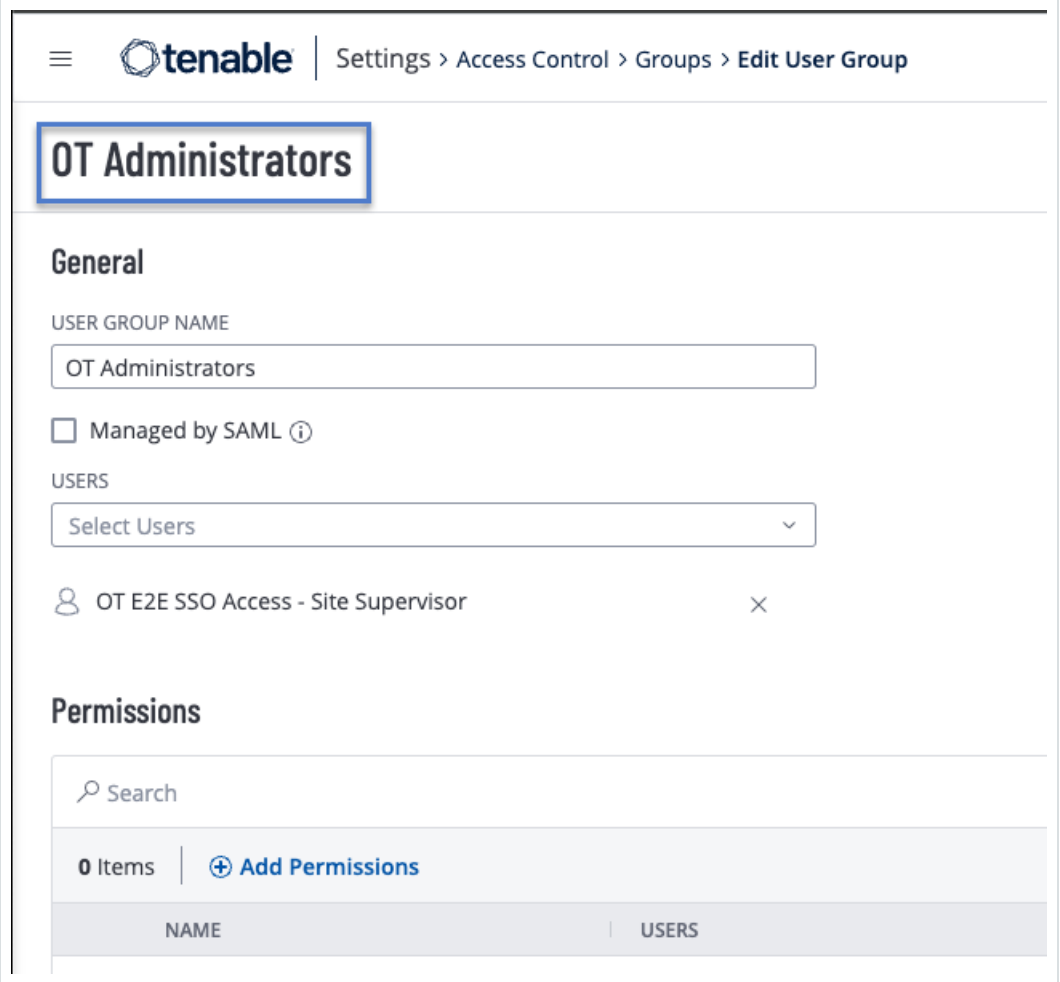
- IDP-Entitäts-ID
- IDP-URL
- IDP-Zertifikat

g. Klicken Sie auf Download File, um das Zertifikat auf Ihr lokales System herunterzuladen.

h. Rufen Sie die Zuordnungsdaten für Gruppen ab. Um die Gruppenobjekt-IDs zu ermitteln, gehen Sie zu Settings > Access Control > Groups und suchen Sie die relevanten Gruppen oder fügen Sie sie hinzu.

   Beispiel: Erstellen Sie in Tenable One zwei Gruppen: OT-Administratoren und OT Schreibgeschützt. Um sie den Benutzerrollen in OT Security zuzuordnen, fügen Sie die Gruppennamen zu den entsprechenden Feldern Gruppenobjekt-ID für Administratoren und Gruppenobjekt-ID für Schreibgeschützt auf der SAML-Seite in OT Security hinzu.


Settings > Access Control > Groups > Edit User Group
OT Read-Only
General
USER GROUP NAME
OT Read-Only
Managed by SAML
USERS
Select Users
OT E2E SSO Access


Settings > Access Control > Groups > Edit User Group
OT Administrators
General
USER GROUP NAME
OT Administrators
Managed by SAML
USERS
Select Users
OT E2E SSO Access - Site Supervisor
Permissions
Search
0 Items
Add Permissions
NAME
USERS

2. Konfigurieren Sie SAML in OT Security:

    a. Loggen Sie sich bei OT Security ein.

    b. Gehen Sie zu Einstellungen > Benutzerverwaltung > SAML.

    Die Seite SAML wird angezeigt.

    c. Klicken Sie auf Konfigurieren oder auf Bearbeiten, wenn Sie eine vorhandene Konfiguration bearbeiten.

    Die Seite SAML konfigurieren wird angezeigt.

    d. Geben Sie die folgenden Details an, die Sie auf der Seite SAML > SSO On-Prem in Tenable One kopiert haben:

        a. Fügen Sie im Feld IDP-ID die IDP-Entitäts-ID ein, die Sie auf der SAML-Seite in Tenable One kopiert haben.

        b. Geben Sie im Feld IDP-URL die IDP-URL ein, die Sie auf der SAML-Seite in Tenable One kopiert haben.

        c. Navigieren Sie im Feld Zertifikatdaten zu dem Speicherort, an den Sie die Zertifikatdatei heruntergeladen haben, und laden Sie sie hoch.

        d. Geben Sie im Feld Username-Attribut Folgendes ein:

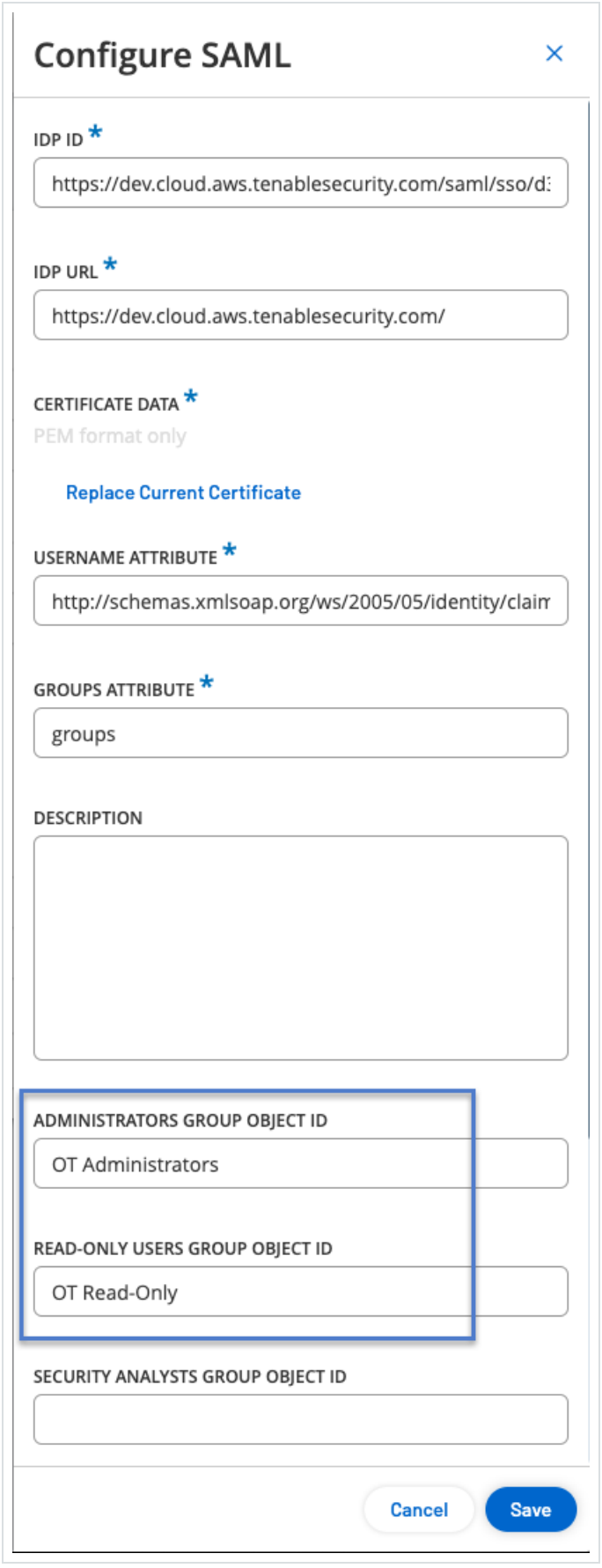
        ```
        http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
        ```

        e. Geben Sie im Feld Groups-Attribut **`groups`** ein (in Kleinbuchstaben, nicht Groups).

        f. Geben Sie die Gruppenobjekt-IDs an, die Sie aus Tenable One abgerufen haben.

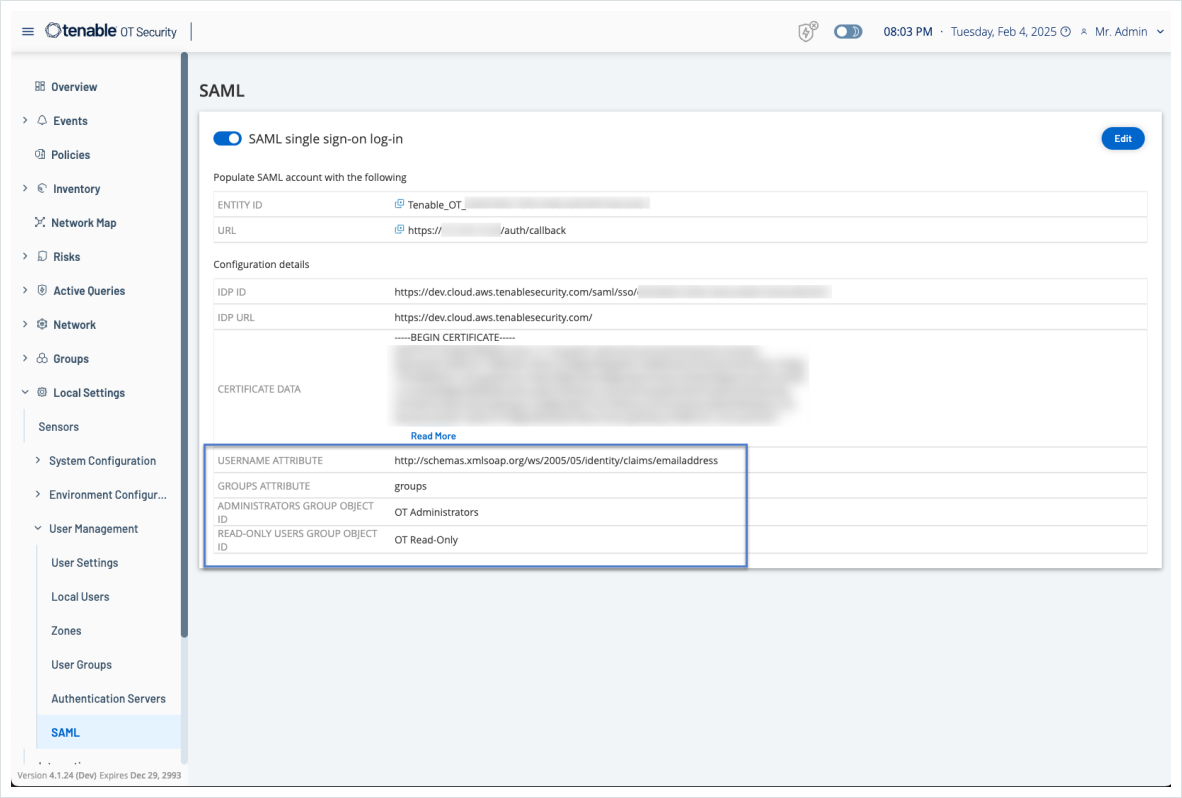
        Beispiel: Sie haben in Schritt h zwei Gruppen in Tenable One erstellt: OT-Administratoren und OT Schreibgeschützt. Fügen Sie diese Gruppennamen zu

den entsprechenden Feldern Gruppenobjekt-ID für Administratoren und Gruppenobjekt-ID für Schreibgeschützt auf der Seite SAML konfigurieren hinzu.


Configure SAML
IDP ID *
https://dev.cloud.aws.tenablesecurity.com/saml/sso/d
IDP URL *
https://dev.cloud.aws.tenablesecurity.com/
CERTIFICATE DATA *
PEM format only
Replace Current Certificate
USERNAME ATTRIBUTE *
http://schemas.xmlsoap.org/ws/2005/05/identity/claim
GROUPS ATTRIBUTE *
groups
DESCRIPTION
ADMINISTRATORS GROUP OBJECT ID
OT Administrators
READ-ONLY USERS GROUP OBJECT ID
OT Read-Only
SECURITY ANALYSTS GROUP OBJECT ID
Cancel
Save

g. Klicken Sie auf Speichern.

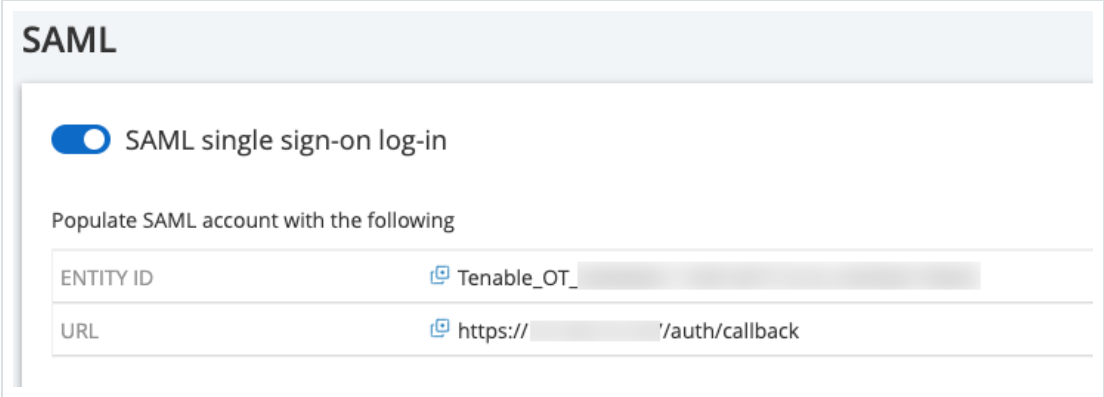
OT Security speichert die Konfiguration und zeigt die folgenden Informationen an:




> Wichtig: Führen Sie keinen Neustart durch, nachdem Sie die Konfiguration gespeichert haben. Starten Sie erst neu, nachdem Sie die Konfigurationsschritte in OT Security und in Tenable Oneabgeschlossen haben.

h. Kopieren Sie auf der Seite SAML die folgenden Werte. Sie benötigen diese Werte für die endgültige Konfiguration in Tenable One.

- Entitäts-ID
- URL




3. Schließen Sie die endgültige Konfiguration in Tenable One ab:

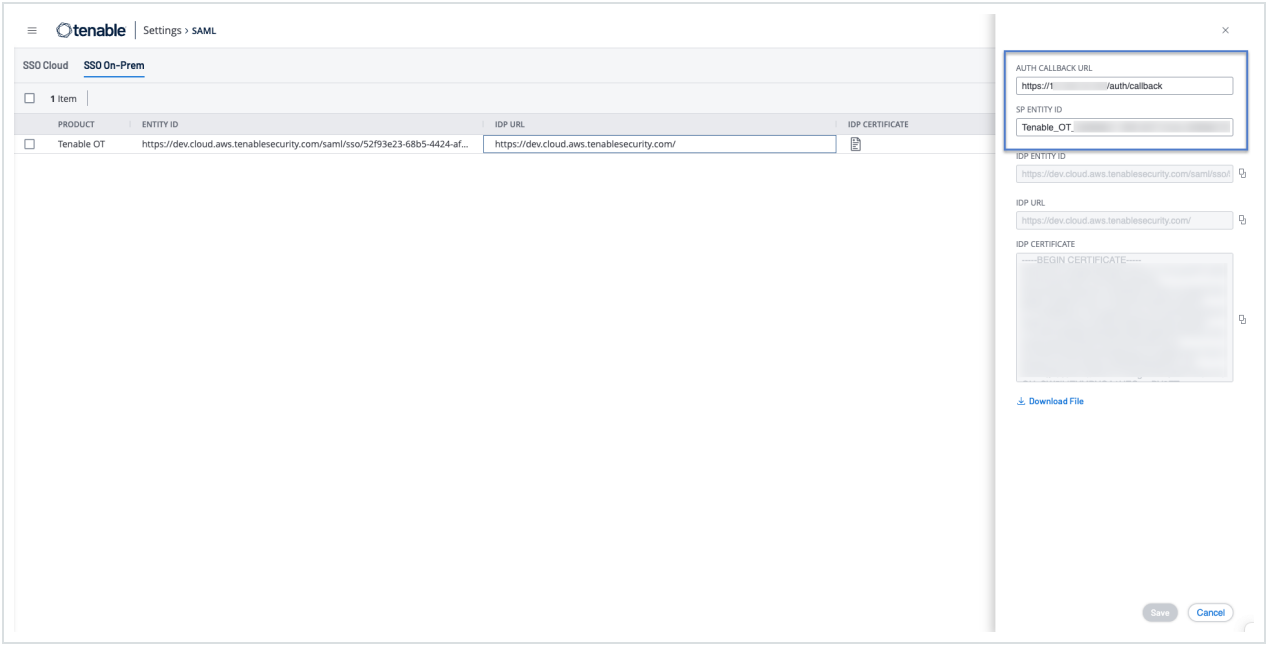
   a. Navigieren Sie in Tenable One zur Seite Settings > SAML > SSO On-Prem.

      Die Seite SSO On-Prem mit der SSO-Konfiguration für Tenable OT Security wird angezeigt.

   b. Klicken Sie auf die Zeile für OT Security.

      Der Bereich mit Konfigurationsdetails für OT Security wird angezeigt.

   c. Geben Sie die Details für Auth Callback URL und SP Entity ID an, die Sie auf der OT Security-Seite SAML kopiert haben.




d. Klicken Sie auf Speichern.

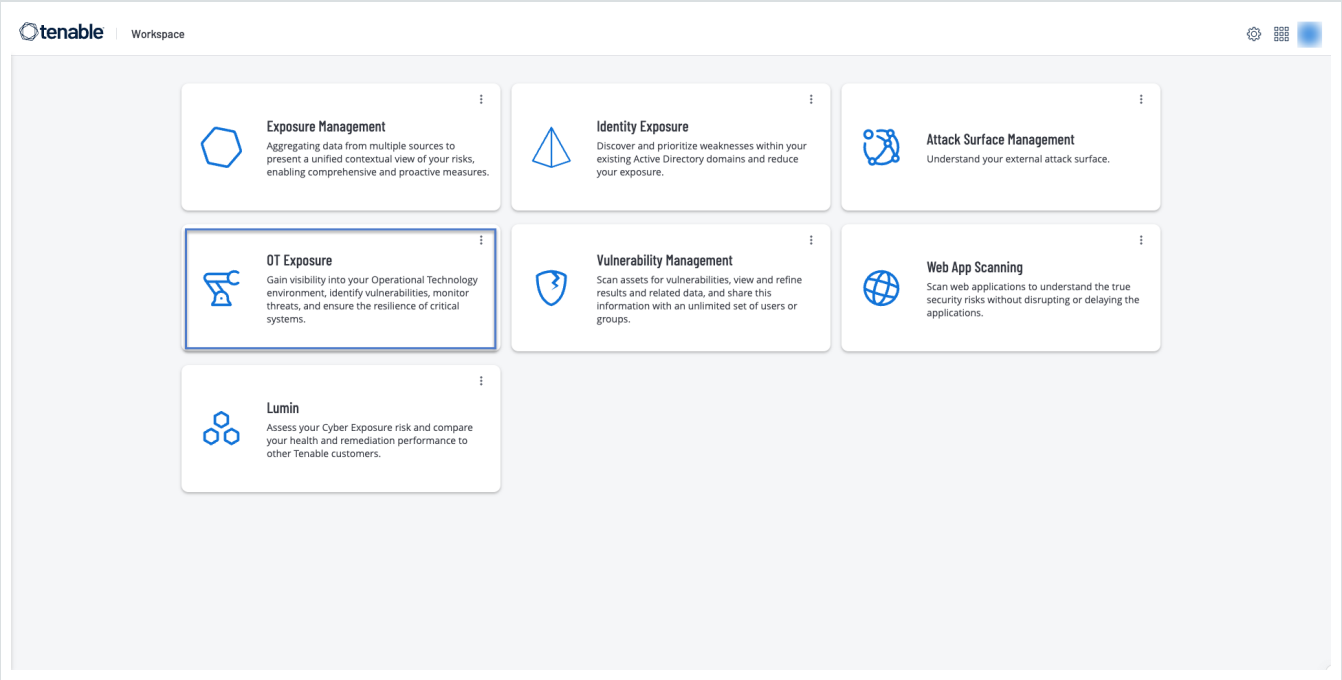
   OT Security speichert die SAML-Konfiguration.

4. Klicken Sie auf den Umschalter SAML Single Sign-On-Login, um SAML zu aktivieren.

   OT Security fordert Sie zum Neustart auf.

5. Starten Sie OT Security neu.

   In Tenable wird die Kachel OT Exposure auf der Seite Workspace aktiviert. Klicken Sie auf die Kachel OT Exposure und greifen Sie auf OT Security zu.




# Server

> Erforderliche OT Security-Benutzerrolle: Administrator, Supervisor

Sie können SMTP-Server und Syslog-Server im System einrichten, damit Ereignisbenachrichtigungen per E-Mail gesendet und/oder in einem SIEM-System protokolliert werden können. Sie können auch FortiGate-Firewalls einrichten, um FortiGate auf Grundlage von OT Security-Netzwerkereignissen Vorschläge zu Firewall-Richtlinien zu senden.

## SMTP-Server

Damit Ereignisbenachrichtigungen per E-Mail an die entsprechenden Parteien gesendet werden können, müssen Sie einen SMTP-Server im System einrichten. Wenn Sie keinen SMTP-Server einrichten, kann das System keine E-Mail-Benachrichtigungen senden, wenn Ereignisse generiert

werden. In jedem Fall können alle Ereignisse in der Verwaltungskonsole (Benutzeroberfläche) im Bildschirm Ereignisse eingesehen werden.

### So richten Sie einen SMTP-Server ein:

1. Gehen Sie zu Einstellungen > Server > SMTP-Server.
2. Klicken Sie auf SMTP-Server hinzufügen.

   Das Konfigurationsfenster SMTP-Server wird angezeigt.
3. Geben Sie im Feld Servername den Namen eines SMTP-Servers ein, der für E-Mail-Benachrichtigungen verwendet werden soll.
4. Geben Sie im Feld Hostname/IP einen Hostnamen oder eine IP-Adresse des SMTP-Servers ein.
5. Geben Sie im Feld Port die Portnummer ein, an der der SMTP-Server auf Ereignisse lauscht (Standard: 25).
6. Geben Sie im Feld E-Mail-Adresse des Absenders eine E-Mail-Adresse ein, die als Absender der Ereignisbenachrichtigungs-E-Mail angezeigt wird.
7. (Optional) Geben Sie in die Felder Benutzername und Passwort einen Benutzernamen und ein Passwort für den Zugriff auf den SMTP-Server ein.
8. Um eine Test-E-Mail zu senden und damit zu überprüfen, ob die Konfiguration erfolgreich war, klicken Sie auf Test-E-Mail senden, geben Sie die E-Mail-Adresse ein, an die gesendet werden soll, und überprüfen Sie den Posteingang, um festzustellen, ob die E-Mail angekommen ist. Wenn die E-Mail nicht angekommen ist, führen Sie eine Fehlerbehebung durch, um die Ursache des Problems zu ermitteln und es zu beheben.
9. Klicken Sie auf Speichern.

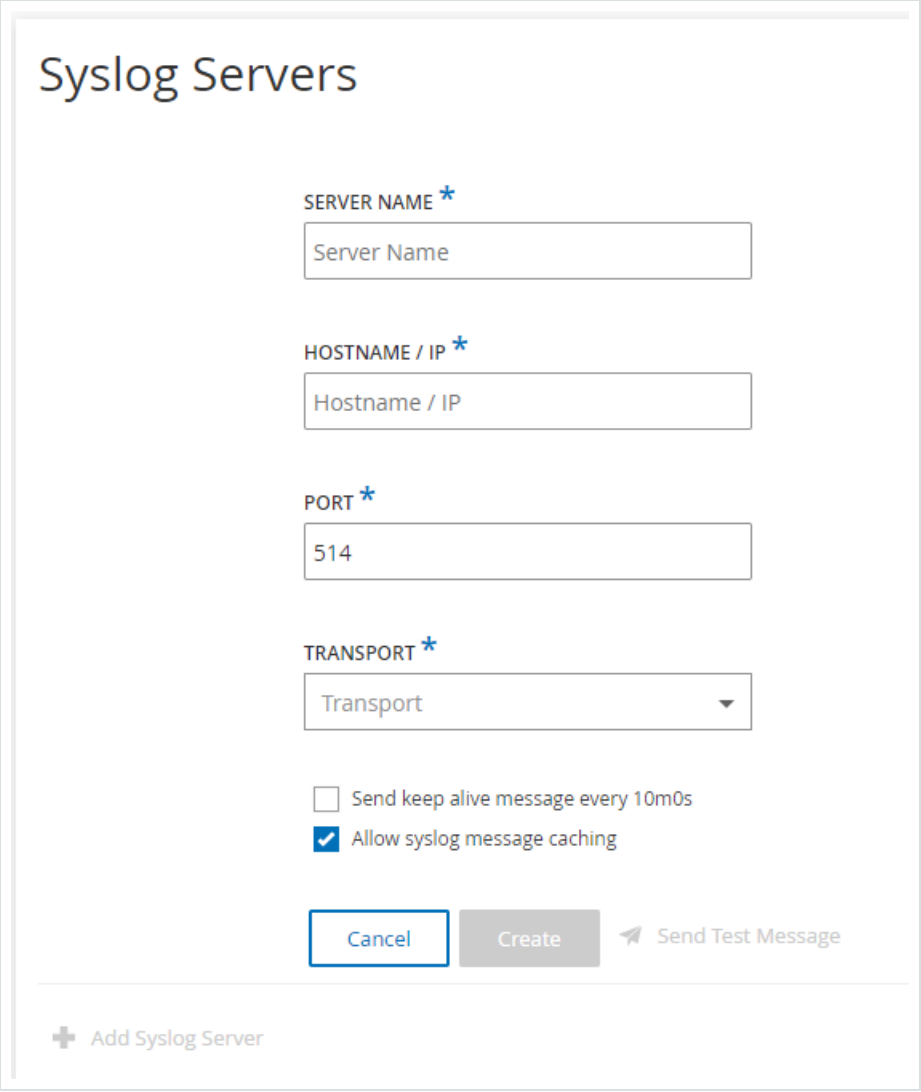
   Sie können weitere SMTP-Server einrichten, indem Sie den Vorgang wiederholen.

## Syslog-Server

Damit Ereignisprotokolle auf einem externen Server gesammelt werden können, müssen Sie einen Syslog-Server im System einrichten. Wenn Sie keinen Syslog-Server einrichten möchten, werden die Ereignisprotokolle nur auf der OT Security-Plattform gespeichert.

So richten Sie einen Syslog-Server ein:

1. Gehen Sie zu Einstellungen > Server > Syslog-Server.
2. Klicken Sie auf + Syslog-Server hinzufügen. Das Konfigurationsfenster Syslog-Server wird angezeigt.



3. Geben Sie im Feld Servername den Namen eines Syslog-Servers ein, der zum Protokollieren von Systemereignissen verwendet werden soll.
4. Geben Sie im Feld Hostname/IP einen Hostnamen oder eine IP-Adresse des Syslog-Servers ein.
5. Geben Sie im Feld Port die Portnummer auf dem Syslog-Server ein, an die Ereignisse gesendet werden. Standard: 514
6. Wählen Sie im Dropdown-Feld Transport das gewünschte Transportprotokoll aus. Verfügbare Optionen: TCP oder UDP.
7. Um eine Testnachricht zu senden und damit zu überprüfen, ob die Konfiguration erfolgreich war, klicken Sie auf Testnachricht senden und prüfen Sie, ob die Nachricht angekommen ist. Wenn die Nachricht nicht angekommen ist, führen Sie eine Fehlerbehebung durch, um die Ursache des Problems zu ermitteln und es zu beheben.
8. (Optional) Wählen Sie die Option Keep-Alive-Nachrichten senden alle 10 ms aus, um die Verbindung in kurzen Abständen zu überprüfen.
9. (Optional) Wählen Sie für TCP-Syslog-Verbindungen die Option Zwischenspeichern von Syslog-Meldungen zulassen aus, um Ereignisse zwischenzuspeichern, wenn die Verbindung unterbrochen wird, und sie zu senden, sobald die Verbindung wiederhergestellt wird.

   > Hinweis: UDP-Syslog-Meldungen verfügen nicht über Statusinformationen und können verloren gehen, wenn die Verbindung unterbrochen wird.

10. Klicken Sie auf Speichern.

    Sie können weitere Syslog-Server einrichten, indem Sie den Vorgang wiederholen.

## FortiGate-Firewalls

So richten Sie einen FortiGate-Server ein:

1. Gehen Sie zu Einstellungen > Server > FortiGate-Firewalls.
2. Klicken Sie auf Firewall hinzufügen.

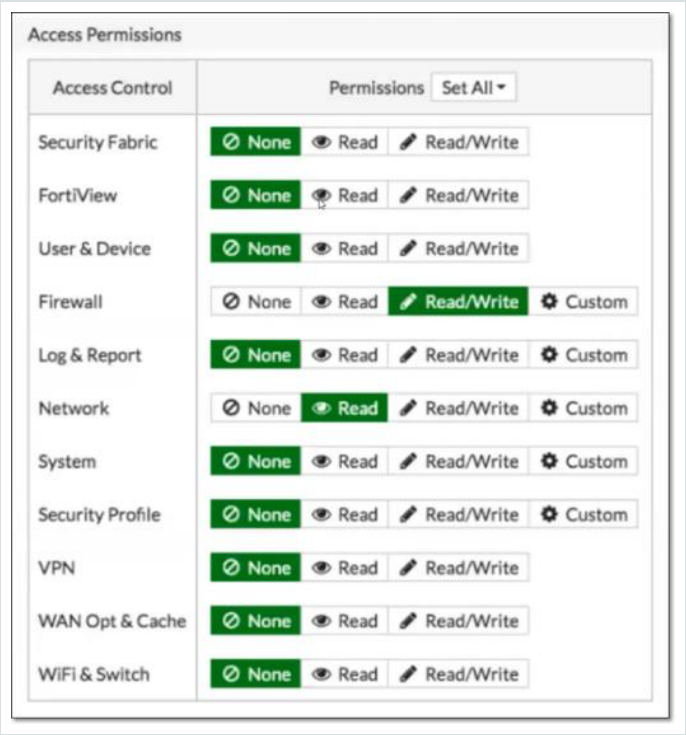
   Das Konfigurationsfenster FortiGate-Firewall hinzufügen wird angezeigt.
3. Geben Sie im Feld Servername den Namen eines FortiGate-Servers ein, den Sie verwenden möchten.
4. Geben Sie im Feld Host/IP einen Hostnamen oder eine IP-Adresse des FortiGate-Servers ein.
5. Geben Sie im Feld API-Schlüssel das API-Token ein, das Sie in FortiGate generiert haben.

   > Hinweis: Anweisungen zum Generieren eines FortiGate-API-Tokens finden Sie auf folgender Seite: https://registry.terraform.io/providers/fortinetdev/fortios/latest/docs/guides/fgt_token
6. Klicken Sie auf Hinzufügen.

   OT Security erstellt den FortiGate-Firewall-Server.

   > Hinweis: Verwenden Sie als Quelladresse (die erforderlich ist, um sicherzustellen, dass das API-Token nur von vertrauenswürdigen Hosts verwendet werden kann) die IP-Adresse Ihres OT Security-Geräts.

   Stellen Sie beim Erstellen eines Administratorprofils für OT Security sicher, dass Sie Zugriffsberechtigungen gemäß den folgenden Einstellungen anwenden:




## Systemprotokoll

Erforderliche OT Security-Benutzerrolle: Administrator

Die Seite Systemprotokoll enthält eine Liste aller Systemereignisse (z. B. Richtlinie aktiviert, Richtlinie bearbeitet und Ereignis aufgelöst), die im System aufgetreten sind. Dieses Protokoll umfasst sowohl vom Benutzer initiierte Ereignisse als auch automatisch auftretende Systemereignisse (z. B. Richtlinie aufgrund zu vieler Treffer automatisch deaktiviert). Dieses Protokoll enthält keine von einer Richtlinie generierten Ereignisse, die im Bildschirm Ereignisse angezeigt werden. Sie können die Protokolle als CSV-Datei exportieren. Sie können das System auch so konfigurieren, dass die Systemprotokollereignisse an einen Syslog-Server gesendet werden. Informationen zum Anpassen von Tabellen finden Sie unter Elemente in der Benutzeroberfläche der Verwaltungskonsole.

Jedes protokollierte Ereignis enthält die folgenden Details:

| Parameter | Beschreibung |
|---|---|
| Uhrzeit | Die Uhrzeit und das Datum des Ereignisses. |
| Ereignis | Eine kurze Beschreibung des aufgetretenen Ereignisses. |
| Benutzername | Der Name des Benutzers, der das Ereignis initiiert hat. Bei automatisch auftretenden Ereignissen wird kein Benutzername vergeben. |

### Systemprotokoll an einen Syslog-Server senden

So konfigurieren Sie das System zum Senden von Systemereignissen an einen Syslog-Server:

1. Gehen Sie zu Einstellungen > Systemprotokoll.
2. Klicken Sie in der oberen rechten Ecke auf das Dropdown-Feld, um die Liste der Server anzuzeigen.

   > Hinweis: Informationen zum Hinzufügen eines Syslog-Servers finden Sie unter Syslog-Server.

3. Wählen Sie den erforderlichen Server aus.

   OT Security sendet die Systemprotokollereignisse an den angegebenen Syslog-Server.

## Anhang – SAML-Integration für Microsoft Azure

OT Security unterstützt die Integration mit Azure über das SAML-Protokoll. Dies ermöglicht es Azure-Benutzern, die OT Security zugewiesen wurden, sich über Single Sign-On (SSO) bei OT Security einzuloggen. Mithilfe der Gruppenzuordnung können Sie Rollen in OT Security entsprechend den Gruppen zuzuweisen, denen Benutzer in Azure zugewiesen sind.

In diesem Abschnitt wird der vollständige Ablauf für die Einrichtung einer SSO-Integration für OT Security mit Azure erläutert. Im Rahmen der Konfiguration wird eine OT Security-Anwendung in Azure erstellt, um die Integration einzurichten. Anschließend können Sie Informationen zu dieser neu erstellten OT Security-Anwendung angeben und das Zertifikat Ihres Identitätsanbieters auf die SAML-Seite in OT Security hochladen. Die Konfiguration ist abgeschlossen, wenn Sie Gruppen von Ihrem Identitätsanbieter zu Benutzergruppen in OT Security zuordnen.

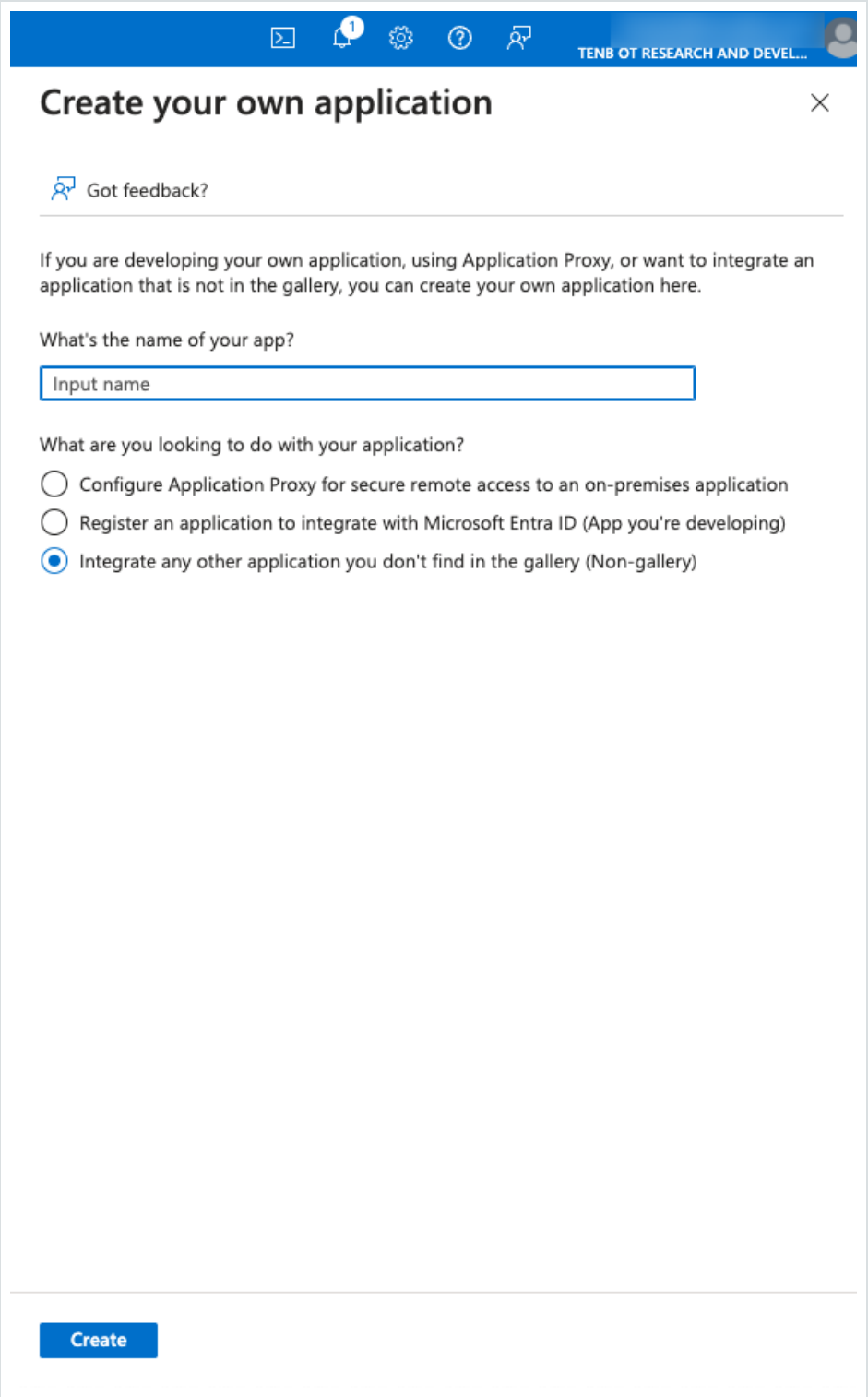
Um die Konfiguration einzurichten, müssen Sie sowohl bei Microsoft Azure als auch bei OT Security als Administrator eingeloggt sein.

## Schritt 1 – Erstellen der Tenable-Anwendung in Azure

So erstellen Sie die Tenable-Anwendung in Azure:

1. Gehen Sie in Azure zu Microsoft Entra ID > Unternehmensanwendungen und klicken Sie auf + Neue Anwendung.

   Die Seite Microsoft Entra ID-Katalog durchsuchen wird angezeigt.




2. Klicken Sie auf + Eigene Anwendung erstellen.

   Der Seitenbereich Eigene Anwendung erstellen wird angezeigt.

3. Geben Sie im Feld Wie lautet der Name der App? einen Namen für die Anwendung ein (z. B. Tenable_OT) und wählen Sie Beliebige andere, nicht im Katalog gefundene Anwendung integrieren aus (Standardeinstellung). Klicken Sie dann auf Erstellen, um die Anwendung hinzuzufügen.

## Schritt 2 – Erstkonfiguration

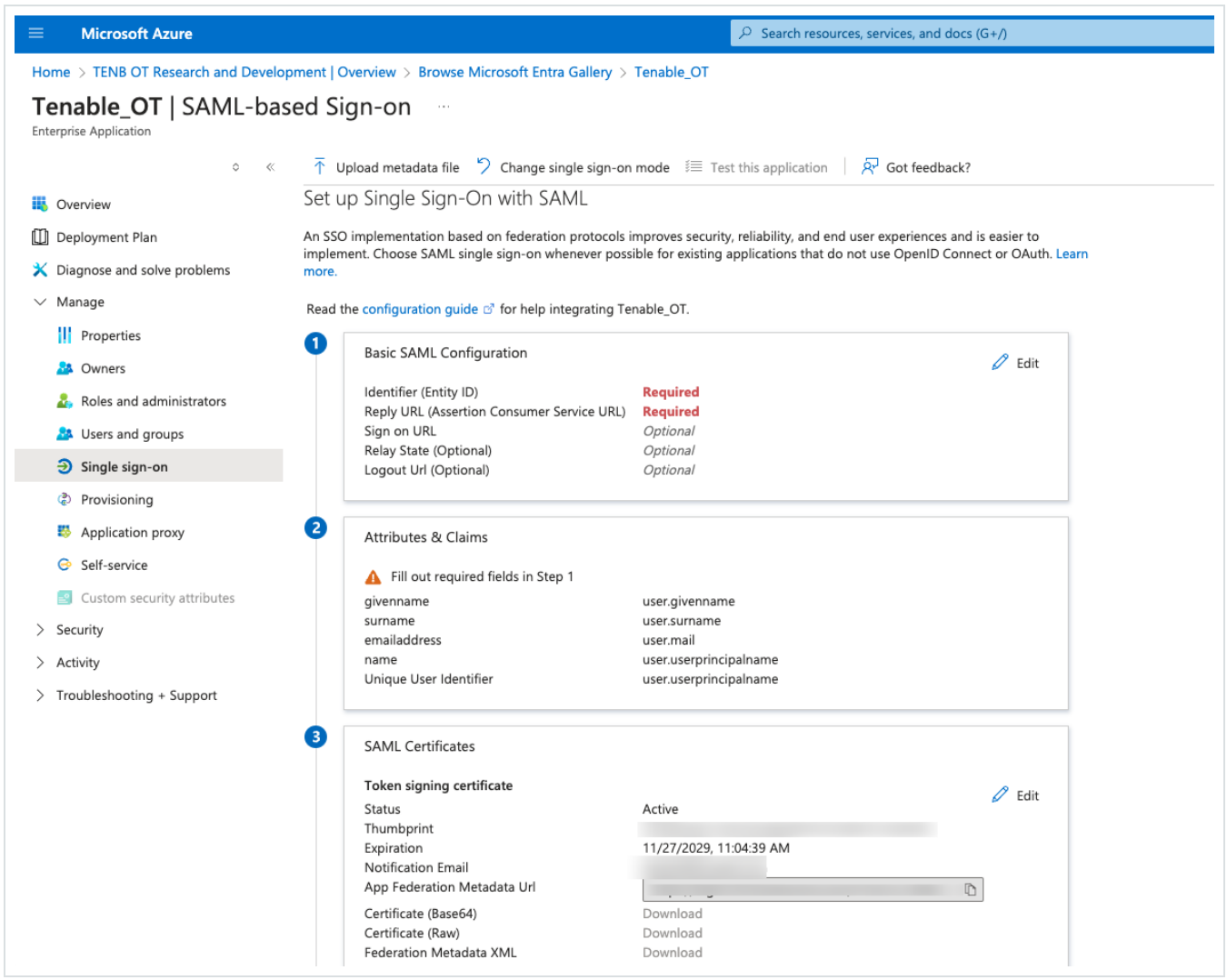
In diesem Schritt erfolgt die Erstkonfiguration der OT Security-Anwendung in Azure. Dies umfasst das Erstellen temporärer Werte für die grundlegenden SAML-Konfigurationswerte Bezeichner und Antwort-URL, um das erforderliche Zertifikat herunterzuladen.

> Hinweis: Konfigurieren Sie nur die in diesem Verfahren genannten Parameter. Behalten Sie für die anderen Parameter die Standardwerte bei.

So führen Sie die Erstkonfiguration durch:

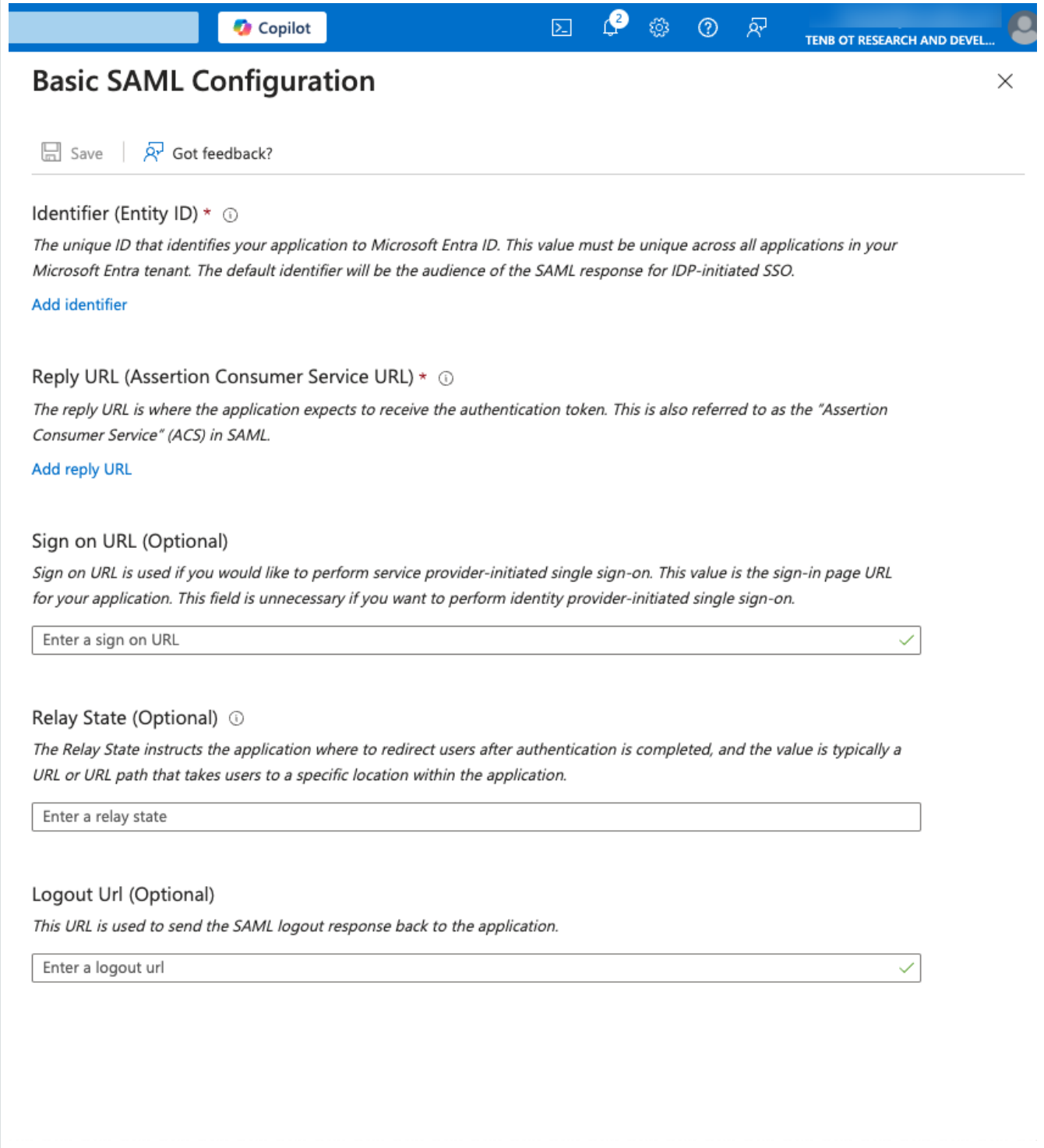
1. Klicken Sie im Navigationsmenü von Azure auf Einmaliges Anmelden und wählen Sie dann SAML als Methode für einmaliges Anmelden (Single Sign-On, SSO) aus.

   Die Seite SAML-basierte Anmeldung wird angezeigt.




2. Klicken Sie in Abschnitt 1, Grundlegende SAML-Konfiguration, auf  Bearbeiten.

Der Seitenbereich Grundlegende SAML-Konfiguration wird angezeigt.



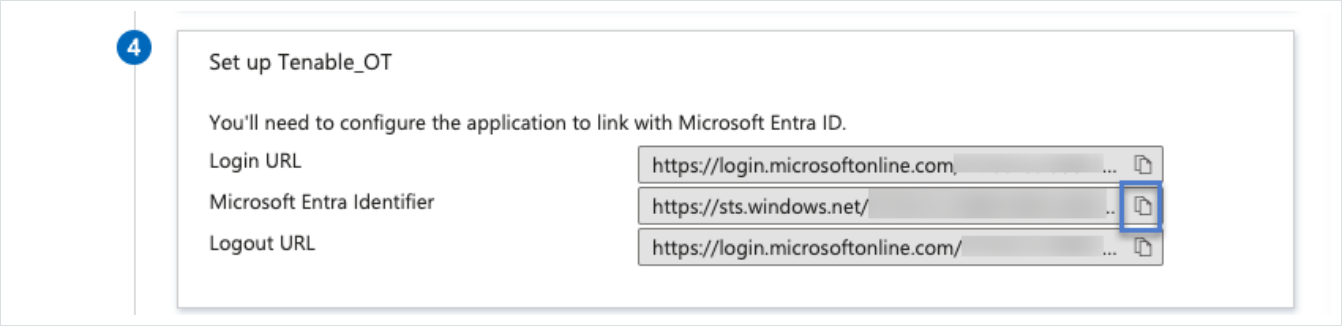

3. Geben Sie im Feld Bezeichner (Entitäts-ID) eine temporäre ID für die Tenable-Anwendung ein, z. B. `tenable_ot`.

4. Geben Sie im Feld Antwort-URL (Assertion Consumer Service-URL) eine gültige URL ein, z. B. `https://OT Security`.

   > Hinweis: Die Werte für Bezeichner und Antwort-URL sind temporäre Werte, die Sie später im Konfigurationsprozess ändern können.

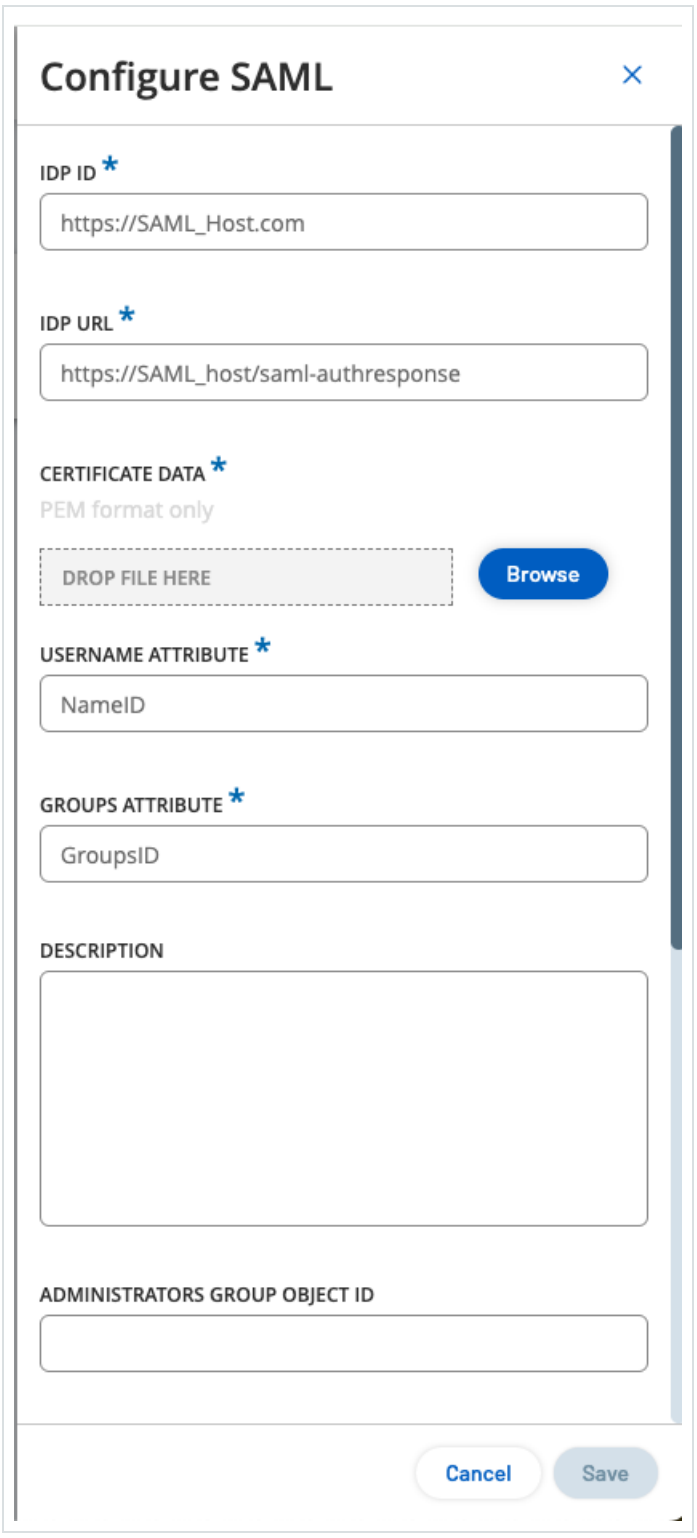
5. Klicken Sie auf Speichern, um die temporären Werte zu speichern und den Seitenbereich Grundlegende SAML-Konfiguration zu schließen.

6. Klicken Sie in Abschnitt 4, Einrichten, auf die Schaltfläche, um den Microsoft Entra ID-Bezeichner zu kopieren.

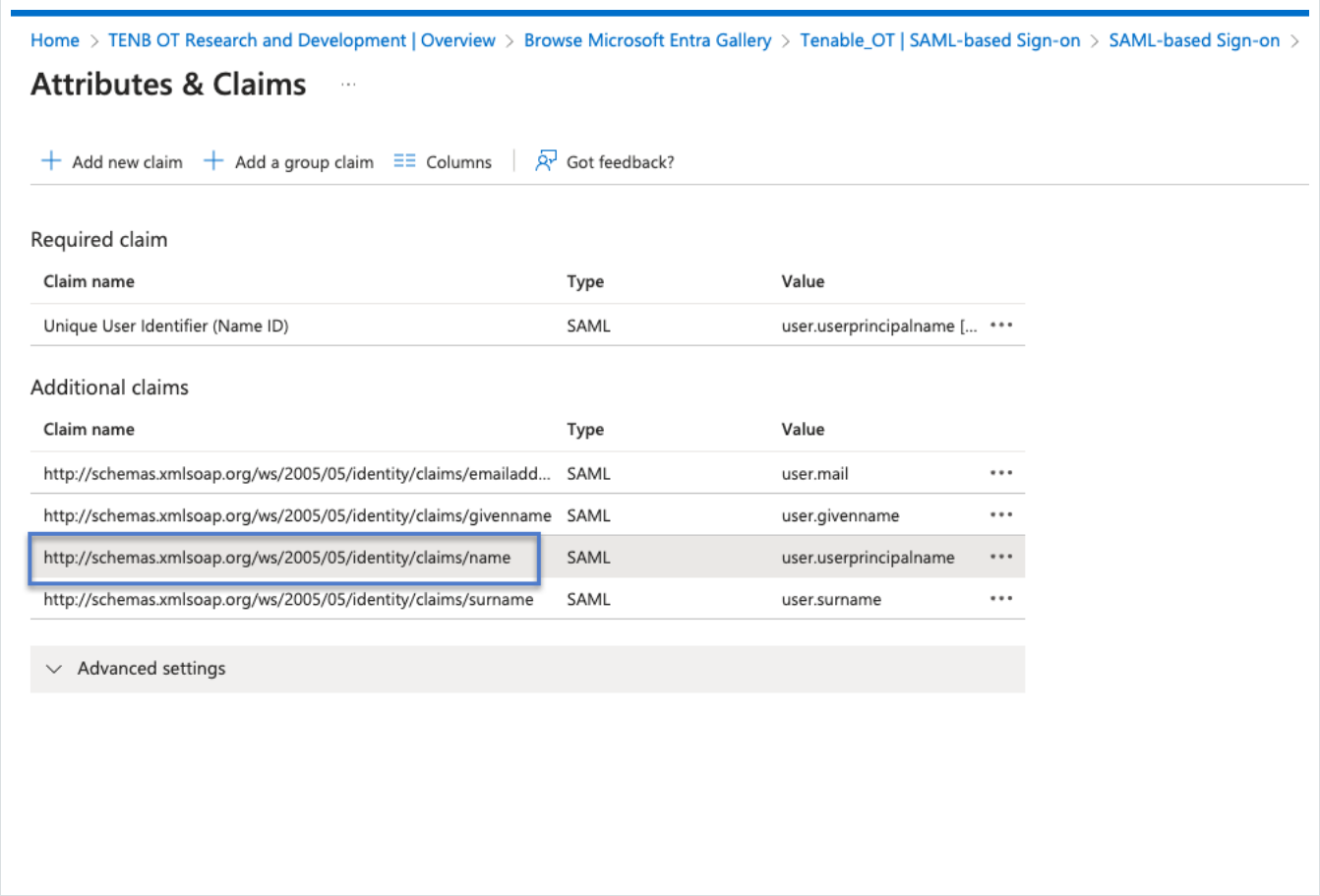



7. Wechseln Sie zur OT Security-Konsole und gehen Sie zu Benutzerverwaltung > SAML.

8. Klicken Sie auf Konfigurieren, um den Seitenbereich SAML konfigurieren anzuzeigen, und fügen Sie den kopierten Wert in das Feld IDP-ID ein.


Configure SAML
IDP ID *
https://SAML_Host.com
IDP URL *
https://SAML_host/saml-authresponse
CERTIFICATE DATA *
PEM format only
DROP FILE HERE
Browse
USERNAME ATTRIBUTE *
NameID
GROUPS ATTRIBUTE *
GroupsID
DESCRIPTION
ADMINISTRATORS GROUP OBJECT ID
Cancel
Save

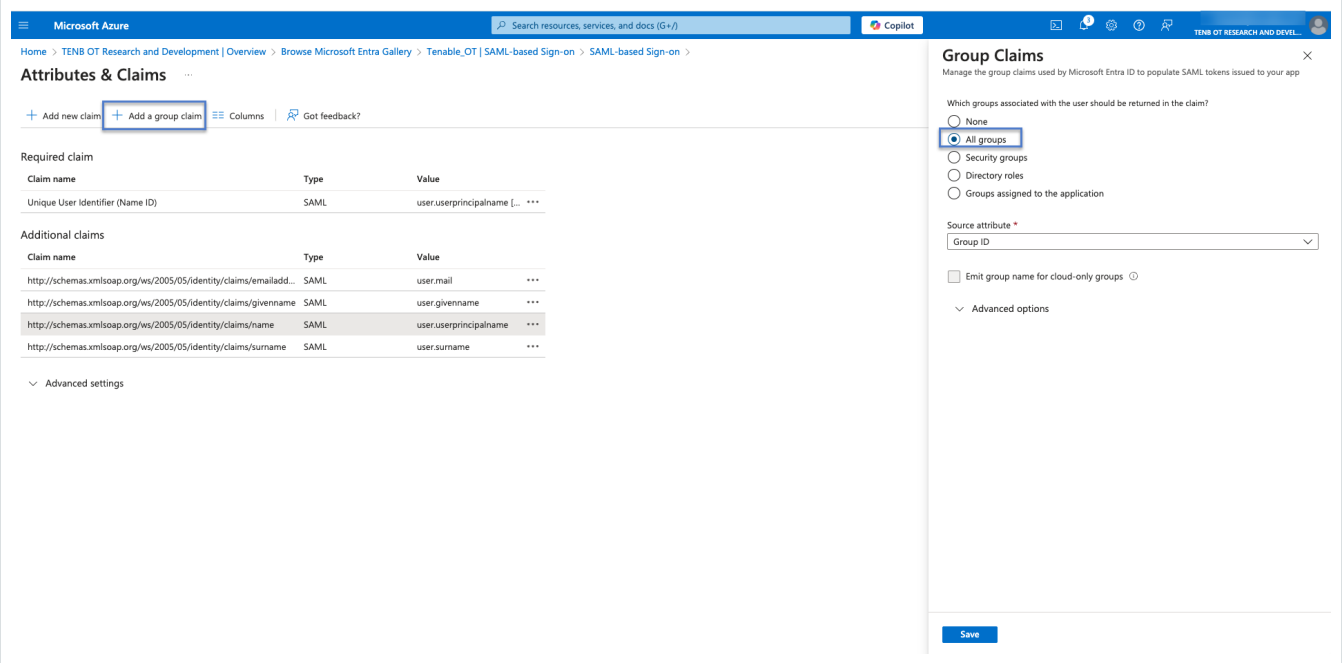
9. Klicken Sie in der Microsoft Azure-Konsole auf die Schaltfläche , um die Anmelde-URL zu kopieren.
10. Kehren Sie zur OT Security-Konsole zurück und fügen Sie den kopierten Wert in das Feld IDP-URL ein.
11. Klicken Sie in der Azure-Konsole in Abschnitt 3, SAML-Zertifikate, für Zertifikat (Base64) auf Herunterladen.
12. Kehren Sie zur OT Security-Konsole zurück und klicken Sie im Abschnitt Zertifikatdaten auf Durchsuchen. Navigieren Sie dann zur Sicherheitszertifikatdatei und wählen Sie sie aus.
13. Klicken Sie in der Azure-Konsole in Abschnitt 2, Attribute & Ansprüche, auf Bearbeiten.
14. Wählen Sie im Abschnitt Zusätzliche Ansprüche die URL unter Anspruchsname aus, die dem Wert user.userprincipalname entspricht, und kopieren Sie sie.




15. Kehren Sie zur OT Security-Konsole zurück und fügen Sie diese URL in das Feld Username-Attribut ein.

16. Klicken Sie in der Azure-Konsole auf + Gruppenanspruch hinzufügen.

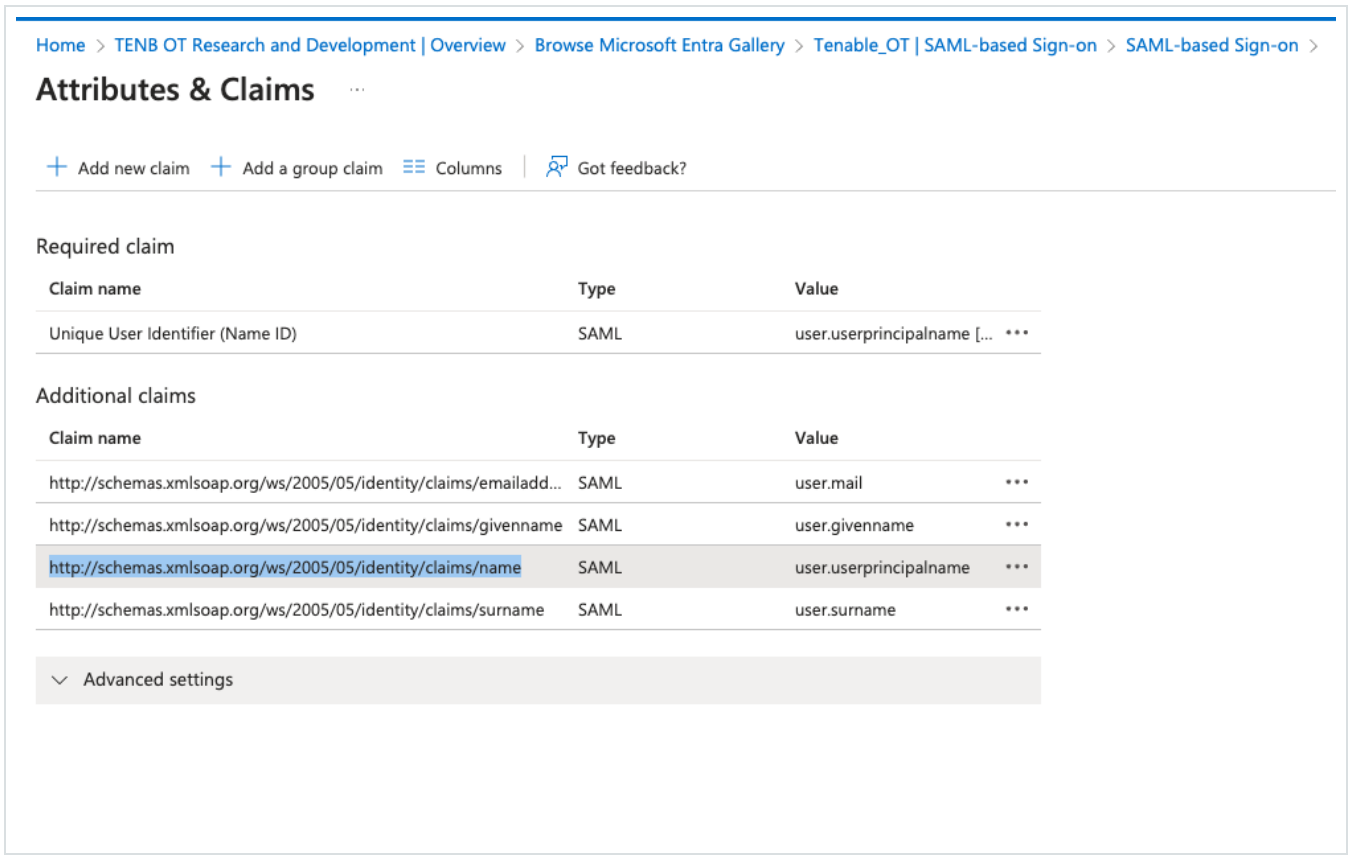
    Der Seitenbereich Gruppenansprüche wird angezeigt.




17. Wählen Sie im Abschnitt Welche dem Benutzer zugeordneten Gruppen sollen im Anspruch zurückgegeben werden? die Option Alle Gruppen aus und klicken Sie auf Speichern.

> Hinweis: Wenn Sie die Gruppeneinstellung in Azure aktivieren, können Sie Der Anwendung zugewiesene Gruppen anstelle von Alle Gruppen auswählen. Azure stellt dann nur die Benutzergruppen bereit, die der Anwendung zugewiesen sind.

18. Markieren und kopieren Sie im Abschnitt Zusätzliche Ansprüche die URL unter Anspruchsname, die dem Wert user.groups [All] zugeordnet ist.




19. Kehren Sie zur OT Security-Konsole zurück und fügen Sie die kopierte URL in das Feld Groups-Attribut ein.
20. (Optional) Geben Sie im Feld Beschreibung eine Beschreibung der SAML-Konfiguration ein.

## Schritt 3 – Zuordnen von Azure-Benutzern zu Tenable-Gruppen

In diesem Schritt weisen sie Azure-Benutzer der OT Security-Anwendung zu. Die jedem Benutzer gewährten Berechtigungen werden festgelegt, indem die Azure-Gruppen, denen die Benutzer zugewiesen sind, einer vordefinierten OT Security-Benutzergruppe zugeordnet werden, die eine zugeordnete Rolle und einen Satz von Berechtigungen hat. Die vordefinierten Benutzergruppen von OT Security sind folgende: „Administratoren“, „Schreibgeschützt“ (Benutzer mit reinen Leseberechtigungen), „Sicherheitsanalysten“, „Sicherheitsmanager“, „Site-Operatoren“ und „Supervisoren“. Weitere Informationen finden Sie unter Benutzerverwaltung. Jeder Azure-Benutzer

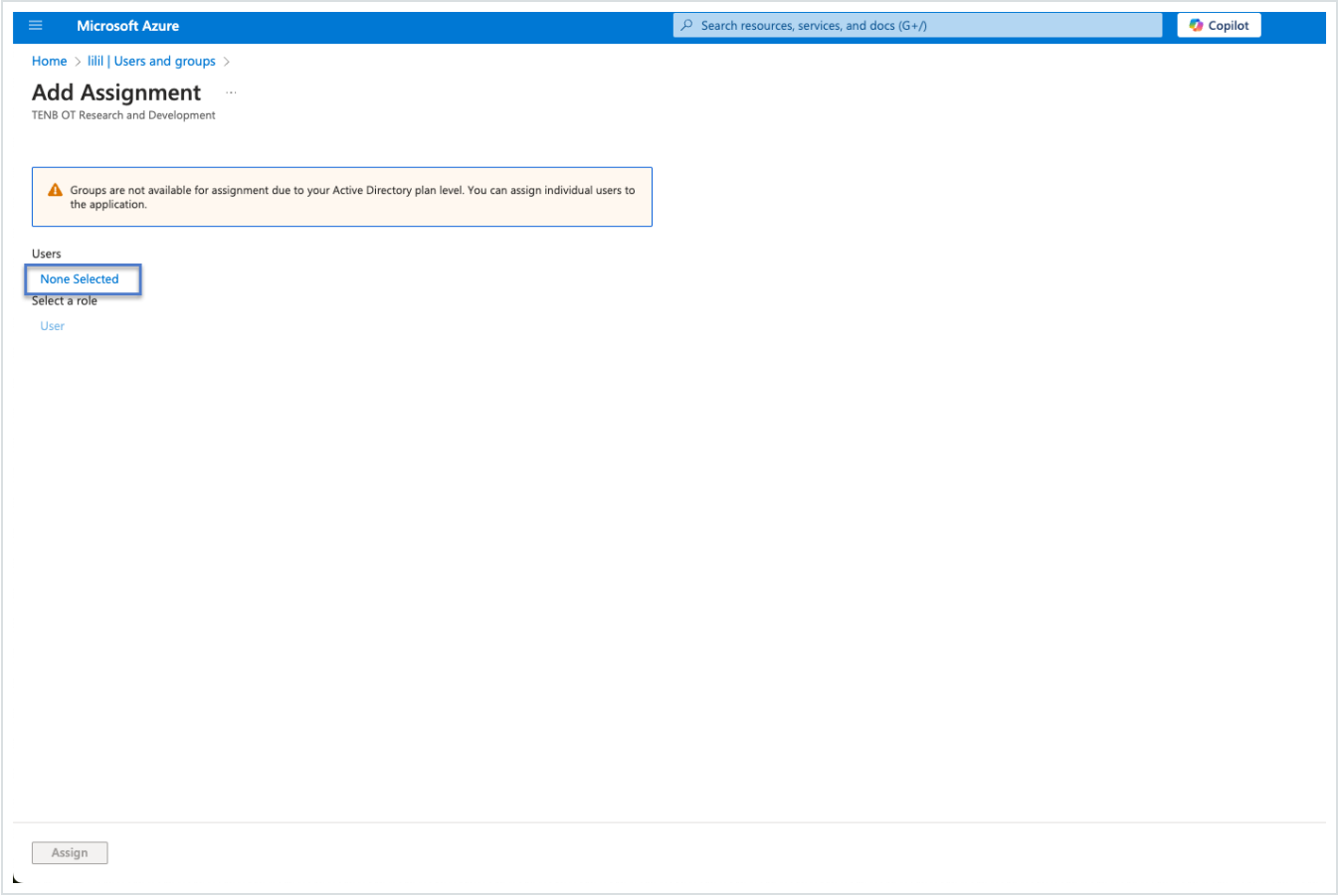
muss mindestens einer Gruppe zugewiesen werden, die einer OT Security-Benutzergruppe zugeordnet ist.

> Hinweis: Administratorbenutzer, die über SAML eingeloggt sind, werden als externe Administratoren betrachtet und erhalten nicht alle Berechtigungen lokaler Administratoren. Benutzern, die mehreren Benutzergruppen zugewiesen sind, werden die höchstmöglichen Berechtigungen aus ihren Gruppen gewährt.

So ordnen Sie Azure-Benutzer zu OT Security zu:

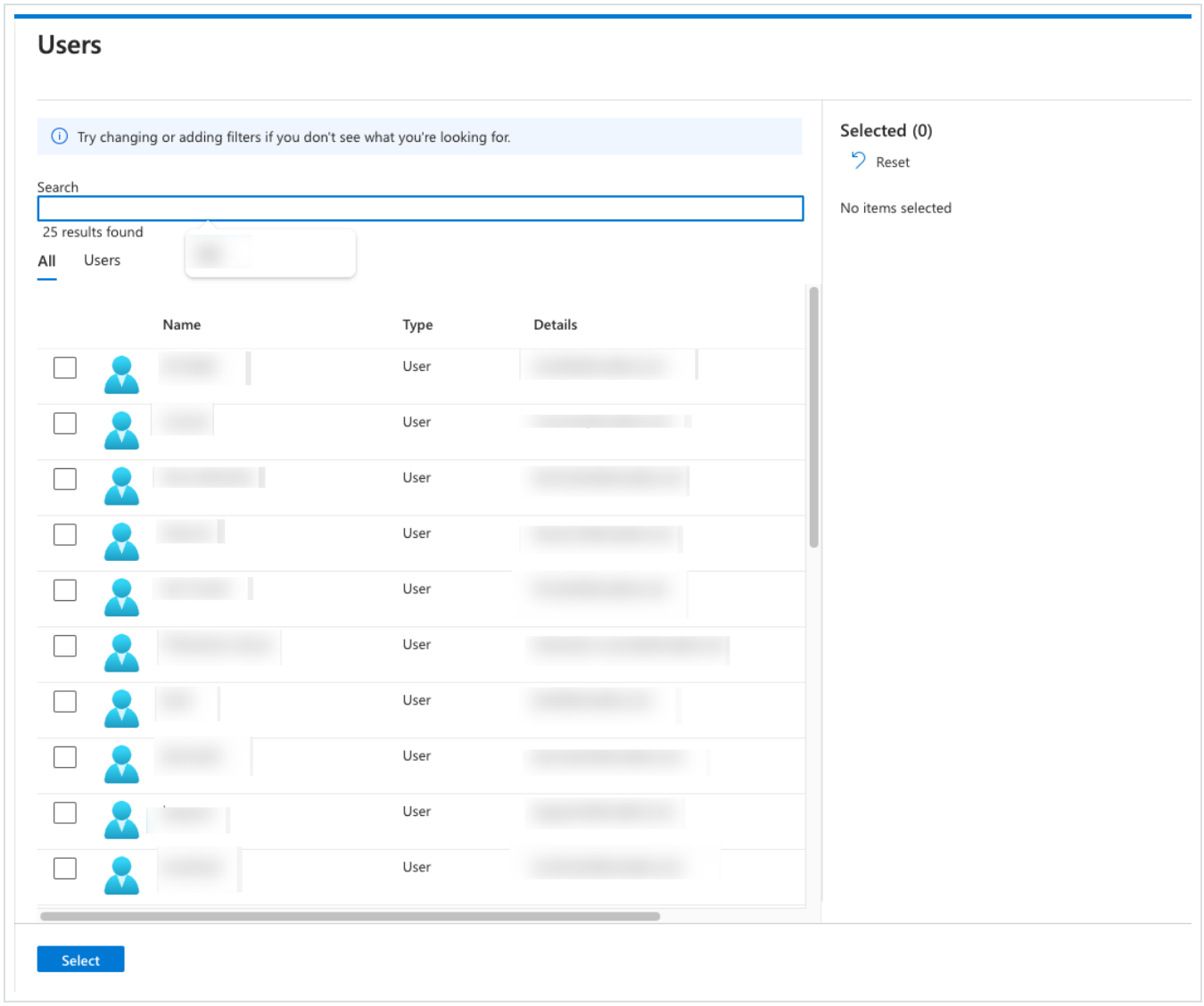
1. Navigieren Sie in Azure zur Seite Benutzer und Gruppen und klicken Sie auf + Benutzer/Gruppe hinzufügen.
2. Klicken Sie auf der Seite Zuweisung hinzufügen unter Benutzer auf Keine ausgewählt.

   Die Seite Benutzer wird angezeigt.



Hinweis: Wenn Sie die Gruppeneinstellung in Azure aktivieren und Der Anwendung zugewiesene Gruppen anstelle von Alle Gruppen auswählen, können Sie Gruppen anstelle von einzelnen Benutzern zuweisen.

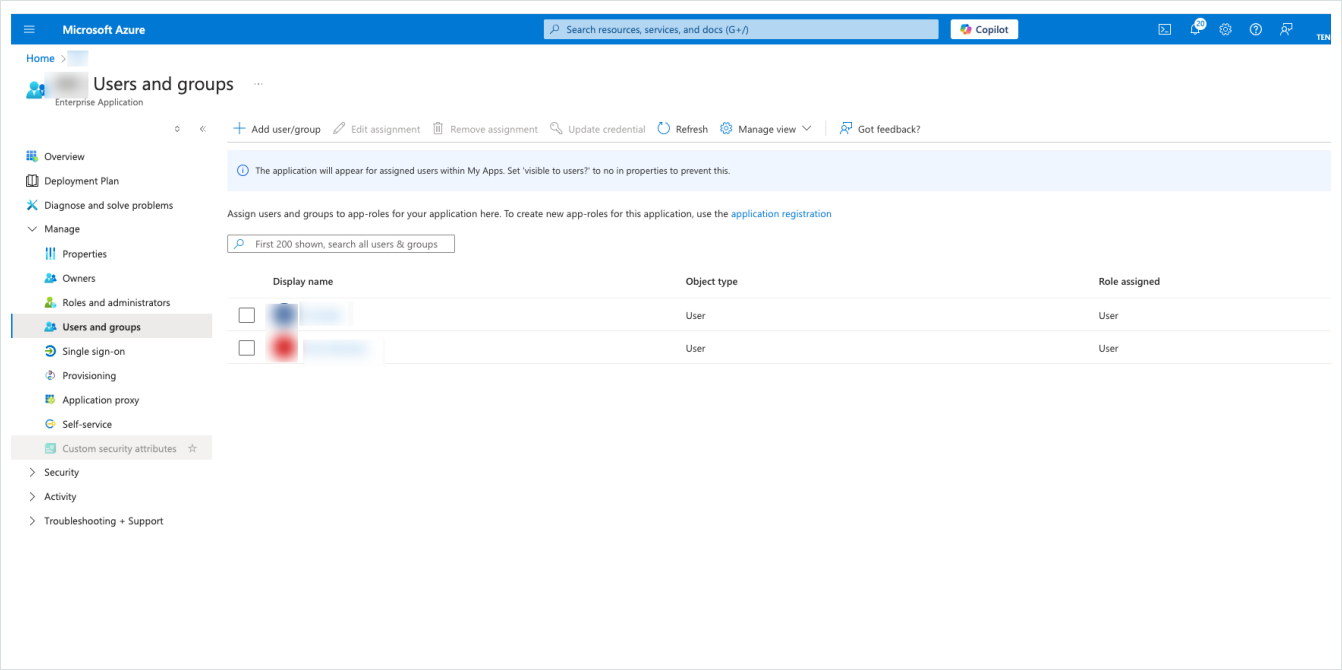
3. Suchen und markieren Sie alle erforderlichen Benutzer und klicken Sie dann auf Auswählen.




4. Klicken Sie auf Zuweisen, um sie der Anwendung zuzuweisen.

   Die Seite Benutzer und Gruppen wird angezeigt.

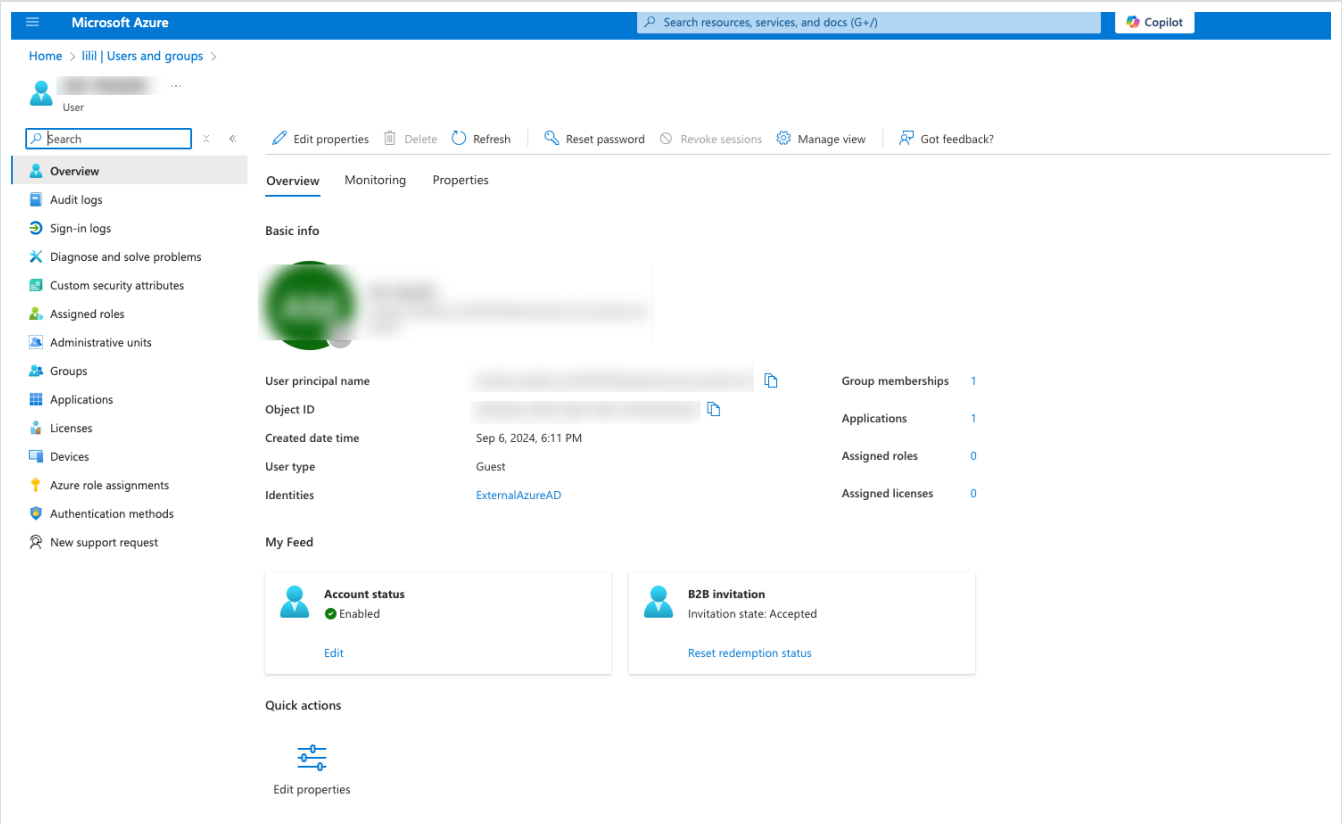
5. Klicken Sie auf den Anzeigenamen eines Benutzers (oder einer Gruppe), um das Profil dieses Benutzers (oder dieser Gruppe) anzuzeigen.



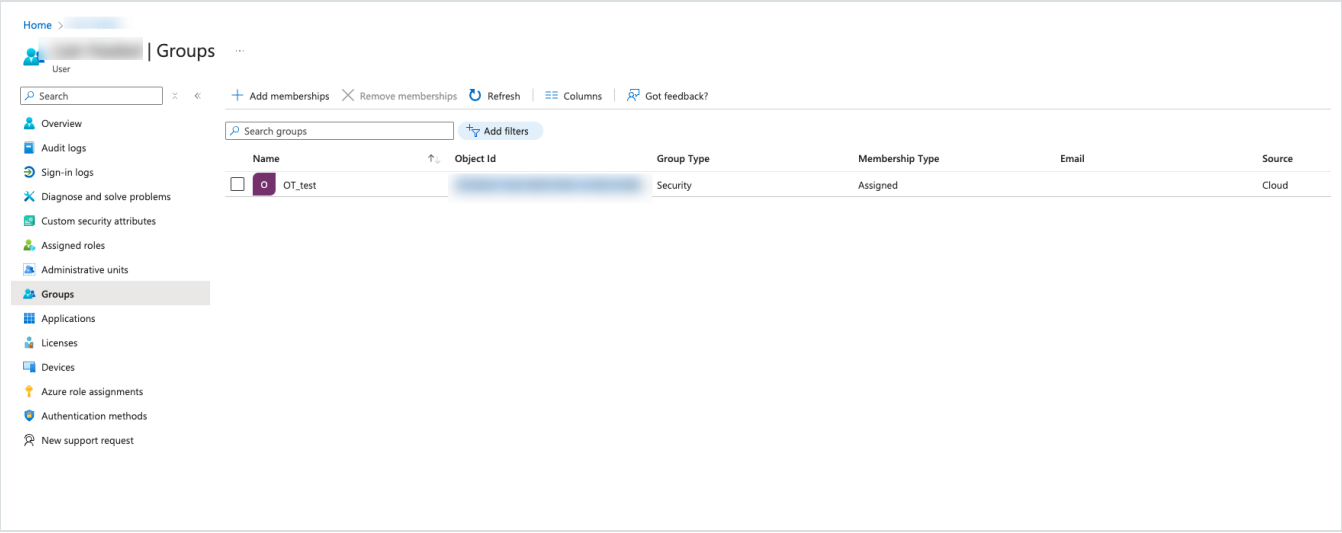

Die Seite Profil wird angezeigt.

6. Wählen Sie in der linken Navigationsleiste die Option Gruppen aus.

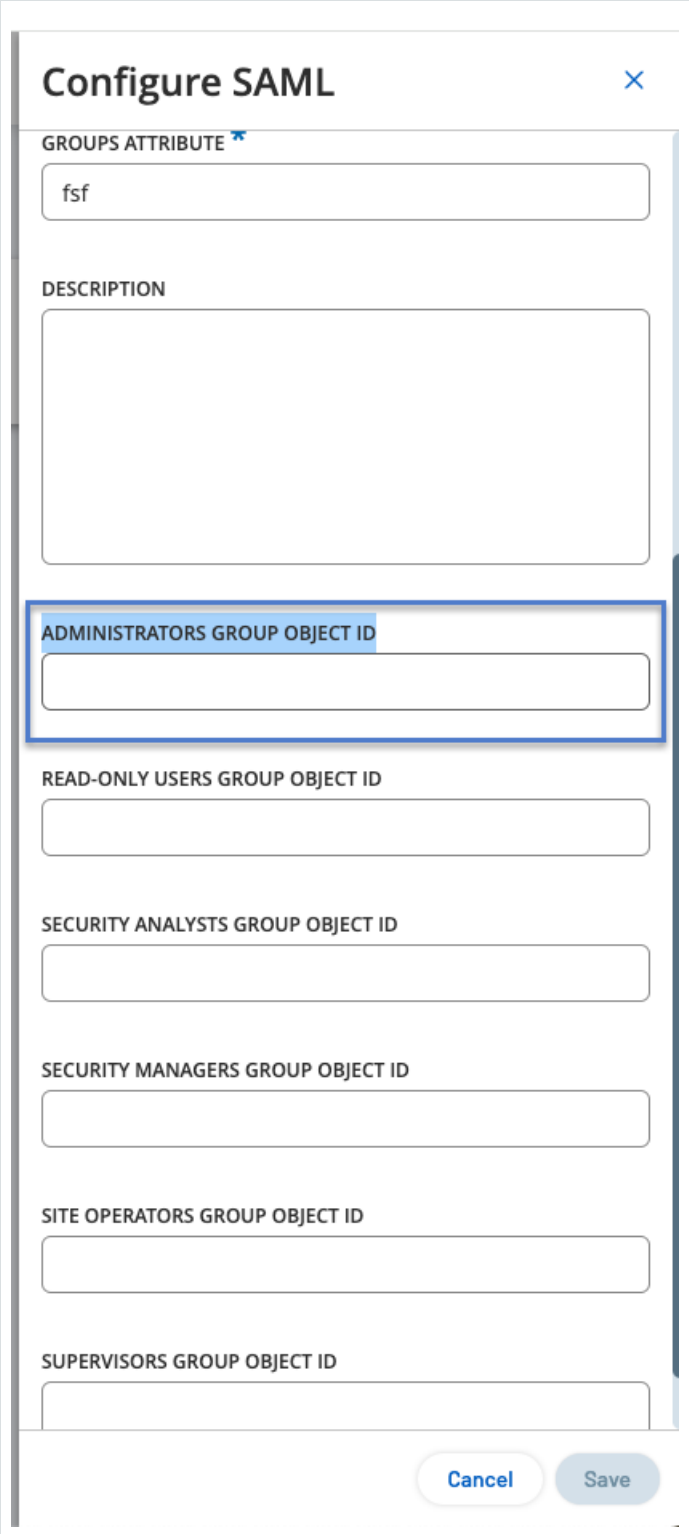
Die Seite Gruppen wird angezeigt.




7. Wählen Sie in der Spalte Objekt-ID den Wert für die Gruppe aus, die Tenable zugeordnet werden soll, und kopieren Sie ihn.



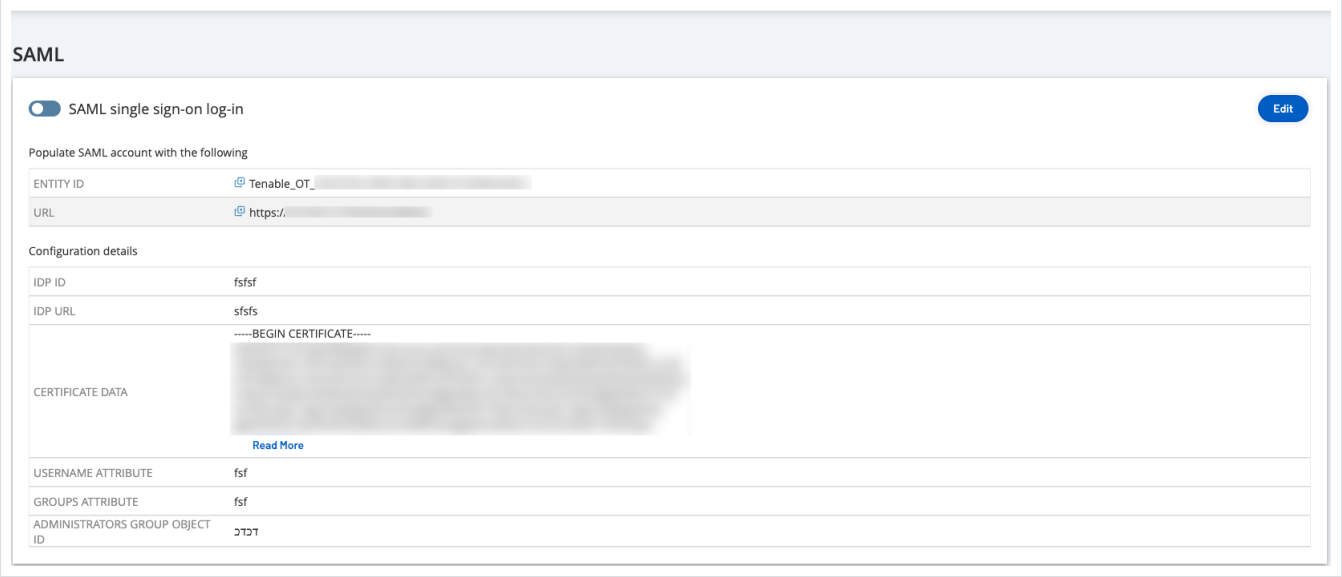
8. Kehren Sie zur OT Security-Konsole zurück und fügen Sie den kopierten Wert in das Feld der gewünschten Gruppenobjekt-ID ein. Zum Beispiel Gruppenobjekt-ID für Administratoren.



9. Wiederholen Sie die Schritte 1 bis 7 für jede Gruppe, die Sie einer bestimmten Benutzergruppe in OT Security zuordnen möchten.

10. Klicken Sie auf Speichern, um die Informationen im Seitenbereich zu speichern und diesen zu schließen.

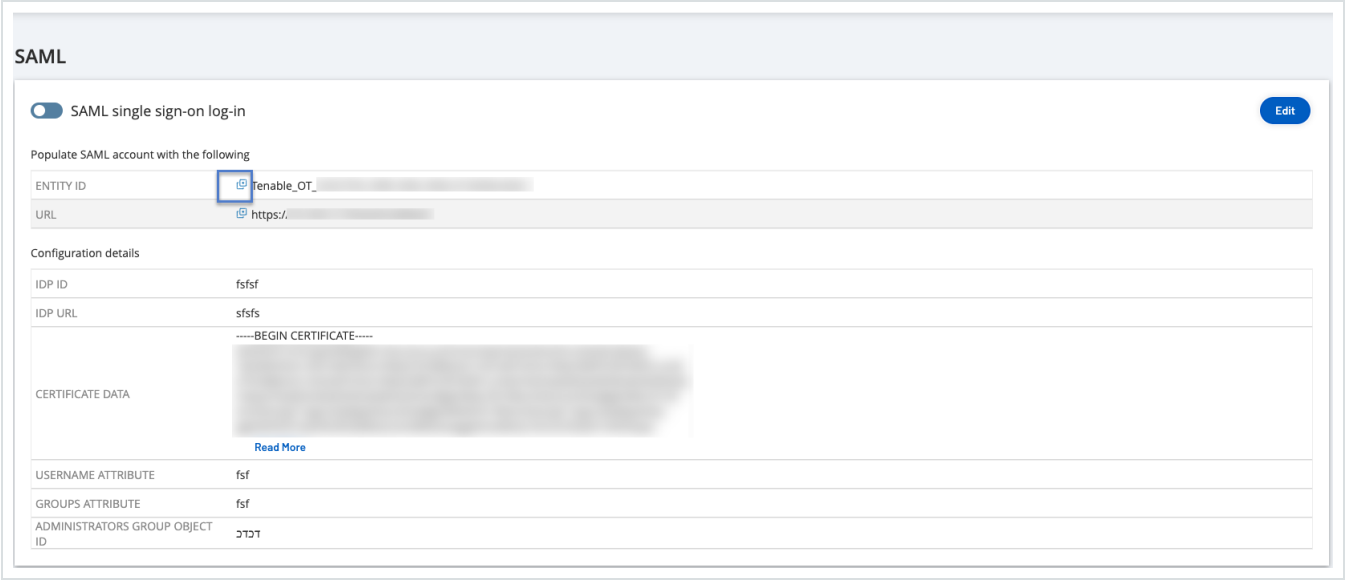
    Die SAML-Seite wird in der OT Security-Konsole mit den konfigurierten Informationen angezeigt.




## Schritt 4 – Abschließen der Konfiguration in Azure

So schließen Sie die Konfiguration in AzurAzure ab:

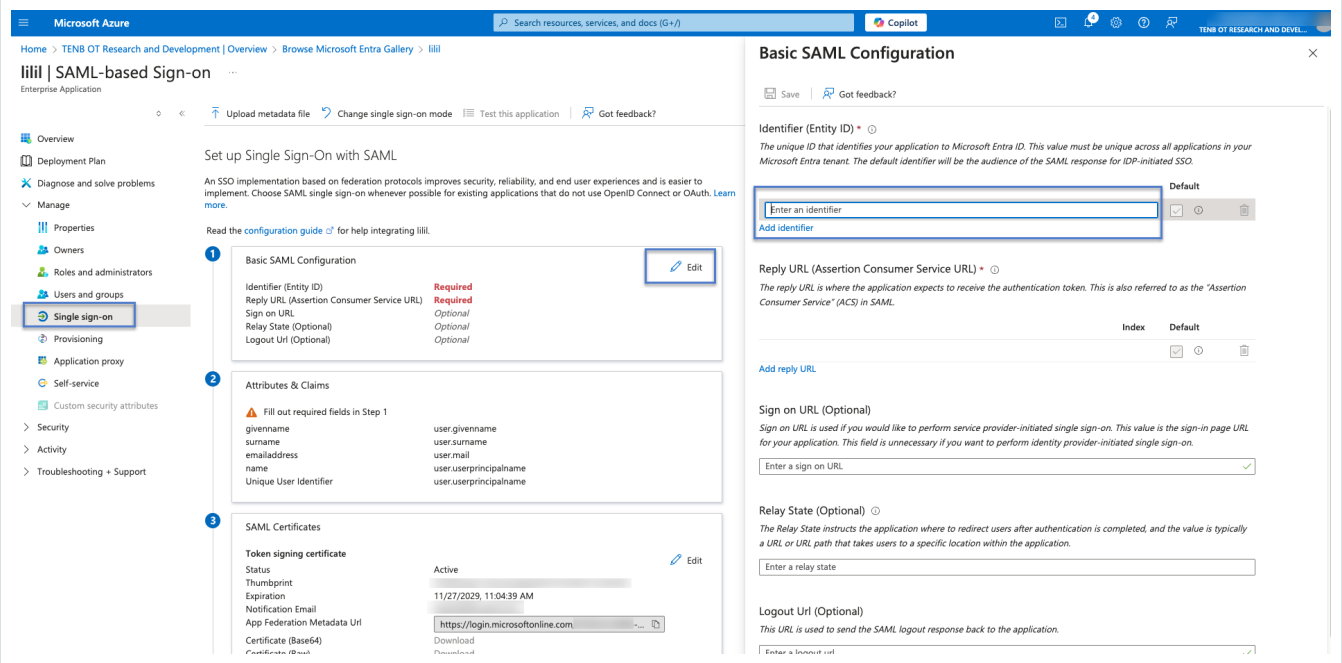
1. Klicken Sie auf der OT Security-Seite SAML auf die Schaltfläche , um die Entitäts-ID zu kopieren.




2. Klicken Sie in der Azure-Konsole im linken Navigationsmenü auf Single Sign-On.

   Die Seite SAML-basierte Anmeldung wird angezeigt.

3. Klicken Sie in Abschnitt 1, Grundlegende SAML-Konfiguration, auf Bearbeiten und fügen Sie den kopierten Wert in das Feld Bezeichner (Entitäts-ID) ein. Ersetzen Sie dabei den zuvor eingegebenen temporären Wert.




4. Wechseln Sie zu OT Security und klicken Sie auf der Seite SAML auf die Schaltfläche , um die URL zu kopieren.

5. Wechseln Sie zur Azure-Konsole und fügen Sie im Abschnitt Grundlegende SAML-Konfiguration die kopierte URL in das Feld Antwort-URL (Assertion Consumer Service-URL) ein. Ersetzen Sie dabei die zuvor eingegebene temporäre URL.

6. Klicken Sie auf Speichern, um die Konfiguration zu speichern, und schließen Sie den Seitenbereich.

   Die Konfiguration ist abgeschlossen und die Verbindung wird auf der Seite Azure-Unternehmensanwendungen angezeigt.

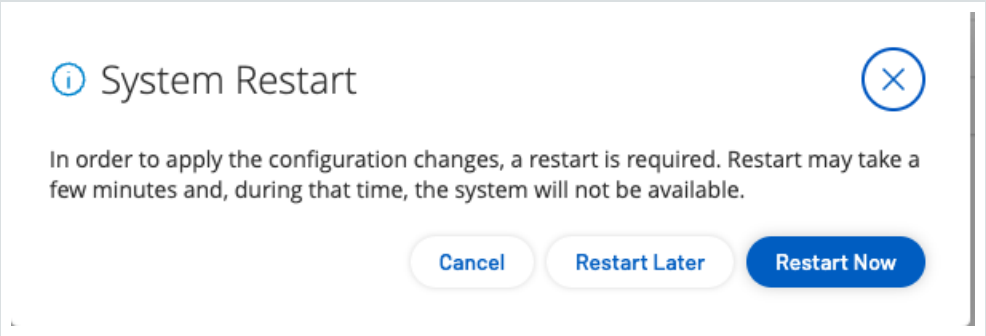
## Schritt 5 – Aktivieren der Integration

Um die SAML-Integration zu aktivieren, müssen Sie OT Security neu starten. Sie können das System sofort oder später neu starten.

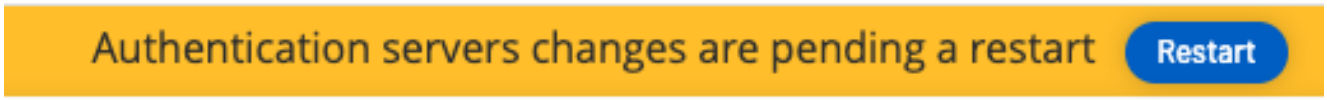
So aktivieren Sie die Integration:

1. Klicken Sie in der OT Security-Konsole auf der Seite SAML auf den Umschalter SAML Single Sign-On-Login, um SAML zu aktivieren.

   Das Benachrichtigungsfenster Systemneustart wird angezeigt.




2. Klicken Sie auf Jetzt neu starten, um das System sofort neu zu starten und die SAML-Konfiguration anzuwenden, oder klicken Sie auf Später neu starten, um die Anwendung der SAML-Konfiguration auf den nächsten Neustart des Systems zu verschieben. Wenn Sie sich für einen späteren Neustart entscheiden, wird das folgende Banner angezeigt, bis der Neustart abgeschlossen ist:

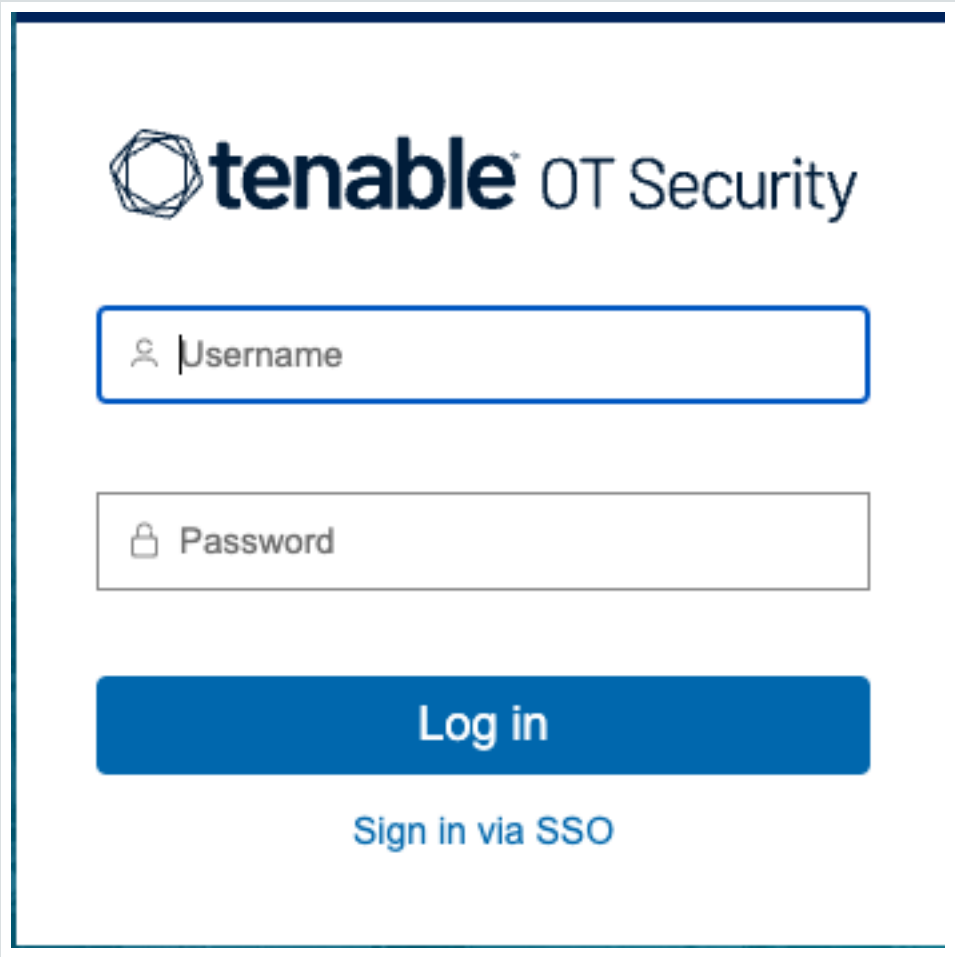



## Mit SSO einloggen

Nach dem Neustart enthält das OT Security-Login-Fenster unter der Schaltfläche Einloggen den neuen Link Über SSO einloggen. Azure-Benutzer, die OT Security zugewiesen sind, können sich mit ihrem Azure-Konto bei OT Security einloggen.

So loggen Sie sich mit SSO ein:

1. Klicken Sie im Login-Fenster von OT Security auf den Link Über SSO einloggen.




Wenn Sie bereits bei Azure eingeloggt sind, gelangen Sie direkt zur OT Security-Konsole, andernfalls werden Sie zur Login-Seite von Azure weitergeleitet.

Wenn Sie mehr als ein Konto haben, werden Sie von OT Security zur Microsoft-Seite Konto auswählen umgeleitet, auf der sie das gewünschte Konto für den Login auswählen können.