Guide de l'utilisateur Tenable OT Security 3.18

Dernière révision : 23 juin 2025

Copyright © 2025 Tenable, Inc. Tous droits réservés. Tenable, Tenable Nessus, Tenable Lumin, Assure et le logo Tenable sont des marques déposées de Tenable, Inc. ou de ses filiales. Tous les autres produits ou services sont des marques commerciales de leurs propriétaires respectifs.

Table des matières

Bienvenue dans Tenable OT Security **12**

Premiers pas avec OT Security 13

Technologies OT Security 13

Architecture de la solution 14

Composants de la plateforme OT Security 15

Composants réseau 15

Spécifications matérielles Tenable OT Security 16

Spécifications pour l'ICP 16

IEI ICP 16

Lanner ICP 17

Lenovo ICP 18

Dell ICP-XL 19

IEI ICP-Mini 21

Spécifications pour les capteurs 22

Capteur IEI 22

Capteur Lanner 23

Capteur Lenovo 24

Éléments système 25

Assets 25

Politiques et événements 26

Détection basée sur des politiques 26

Détection des anomalies 27

Catégories de politiques 28

Groupes 29
Événements 29
Composants de licence OT Security 29
Messages d'erreur 32
Premiers pas avec OT Security 44
Vérifier les conditions préalables 45
Installer l'ICP OT Security 45
Utiliser OT Security 46
Intégrer OT Security à Tenable One 46
Conditions préalables 49
Exigences système 50
Exigences d'accès 55
Considérations sur le réseau 57
Considérations sur le pare-feu 58
Plateforme OT Security Core 58
Capteurs OT Security 60
Requête active 60
Intégrations OT Security 61
Requête d'identification et de détails 62
Installer l'ICP OT Security 63
Installer une appliance matérielle ICP OT Security 63
Nouvelle installation Tenable Core + Tenable OT Security sur le matériel fourni par Tenable 65
Installer une appliance virtuelle ICP OT Security 72
Connecter OT Security au réseau 74

Configurer l'ICP OT Security 75
Configurer Tenable Core 75
Installer OT Security sur Tenable Core 81
Configurer les paramètres OT Security à l'aide de l'assistant de configuration 83
Se connecter à la console de gestion OT Security 84
Informations utilisateur 87
Appareil 89
Heure système 92
Connecter le port de gestion séparé (séparation des ports) 94
Activation de licence OT Security 95
Lancer OT Security 109
Activer le système OT Security 110
Commencer à utiliser OT Security 111
Installer le capteur OT Security 114
Configurer le capteur 120
Configurer un capteur pour montage en rack 121
Configurer un capteur configurable 123
Connecter le capteur au réseau 126
Accéder à l'assistant de configuration du capteur 127
Restaurer la sauvegarde à l'aide de la CLI 129
Éléments de l'interface utilisateur de la console de gestion 131
Principaux éléments de l'interface utilisateur 131
Naviguer dans OT Security 133
Personnaliser les tableaux 135

Exporter des données 140
Menu Actions 141
Dashboards 141
Dashboard Risques 142
Dashboard Inventaire 143
Dashboard Événements et politiques 144
Interagir avec les dashboards 145
Événements 149
Affichage des événements 149
Affichage des détails d'un événement 153
Affichage des clusters d'événements 154
Résoudre des événements 155
Créer des exclusions de politique 158
Télécharger des fichiers de capture individuels 164
Créer des politiques FortiGate 165
Politiques 166
Configuration des politiques 167
Groupes 167
Niveaux de sévérité 168
Notifications d'événement 169
Catégories et sous-catégories de politiques 169
Types de politiques 170
Activer ou désactiver des politiques 179
Afficher les politiques 181

Afficher les détails d'une politique 183
Créer des politiques 185
Création de politiques d'écriture non autorisée 191
Autres actions sur les politiques 193
Modifier des politiques 193
Dupliquer des politiques 196
Supprimer des politiques 198
Inventaire **201**
Affichage des assets 201
Types d'assets 204
Afficher les détails d'un asset 213
Volet d'en-tête 214
Détails 215
Révisions de code 217
Volet de sélection de version 218
Volet des détails d'un instantané 218
Volet d'historique des versions 219
Comparer les versions d'un instantané 219
Créer un instantané 221
Itinéraire IP 221
Vecteurs d'attaque 222
Générer des vecteurs d'attaque 223
Affichage des vecteurs d'attaque 226
Ports ouverts 227

Actions supplémentaires dans l'onglet Ports ouverts 227
Vulnérabilités 228
Événements 229
Cartographie du réseau 231
Ports du périphérique 232
Modifier les détails de l'asset 233
Modifier les détails d'un asset via l'interface utilisateur 233
Modifier les détails d'un asset en téléchargeant un fichier CSV 236
Masquer des assets 238
Effectuer un scan Tenable Nessus spécifique à un asset 239
Exécuter une resynchronisation 240
Cartographie du réseau **244**
Regroupements d'assets 246
Application de filtres à l'affichage de la cartographie 249
Affichage des détails d'un asset 250
Définir une base de référence réseau 250
Vulnérabilités **251**
Vulnérabilités 252
Détails du plug-in 253
Modifier les détails d'une vulnérabilité 254
Afficher la sortie d'un plug-in 255
Requêtes actives **258**
Créer une requête 260
Ajouter des restrictions 263

Afficher une requête 263
Modifier une requête 264
Dupliquer une requête 264
Exécuter une requête 265
Informations d'authentification 266
Ajouter des informations d'authentification 266
Modifier des informations d'authentification 269
Supprimer des informations d'authentification 269
Comptes WMI 269
Créer des scans des plug-ins Nessus 270
Réseau 274
Récapitulatif réseau 274
Définir la période 278
Captures de paquets 281
Paramètres de capture de paquets 281
Filtrer l'affichage de la capture de paquets 282
Activer ou désactiver les captures de paquets 283
Télécharger des fichiers 283
Communications 284
Groupes 285
Afficher les groupes 286
Groupes d'assets 287
Segments réseau 294
Groupes de messagerie 298

Groupes de ports 300
Groupes de protocoles 303
Groupe de planification 306
Groupes de tags 311
Groupes de règles 314
Actions sur les groupes 316
Paramètres locaux 324
Capteurs 327
Afficher les capteurs 328
Approuver manuellement les demandes entrantes d'appairage des capteurs 329
Configuration des requêtes actives 330
Mettre à jour les capteurs 331
Configuration système 333
Appareil 333
Configuration des ports 337
Mises à jour 337
Mises à jour de l'ensemble de plug-ins Tenable Nessus 338
Mises à jour de l'ensemble de règles du moteur IDS 343
Certificats 347
Générer des clés API 349
Appairer l'ICP avec Enterprise Manager 350
Déconnecter l'appairage ICP avec Enterprise Manager 354
Licence 355
Configuration de l'environnement 355

Paramètres des assets 355
Réseaux surveillés 355
Mettre à jour les détails des assets à l'aide d'un fichier CSV 358
Ajouter des assets manuellement 358
Groupes d'événements 359
Lecteur PCAP 362
Charger un fichier PCAP 362
Lire un fichier PCAP 362
Gestion des utilisateurs 363
Utilisateurs locaux 364
Afficher les utilisateurs locaux 364
Ajouter des utilisateurs locaux 365
Actions supplémentaires sur les comptes utilisateur 367
Groupes d'utilisateurs 369
Affichage des groupes d'utilisateurs 370
Ajouter des groupes d'utilisateurs 370
Actions supplémentaires sur les groupes d'utilisateurs 373
Rôles d'utilisateur 375
Zones 387
Serveurs d'authentification 390
Active Directory 391
LDAP 395
SAML 398
Intégrations 400

Produits Tenable 401
Tenable Security Center 401
Tenable Vulnerability Management 402
Tenable One 403
Palo Alto Networks – Pare-feu de nouvelle génération (NGFW) 403
Aruba – Gestionnaire de politiques ClearPass 403
Intégration à Tenable One 404
Serveurs 406
Serveurs SMTP 406
Serveurs Syslog 408
Pare-feux FortiGate 410
Journal système 412
Annexe – Intégration SAML pour Microsoft Azure 413
Étape 1 – Création de l'application Tenable dans Azure 414
Étape 2 – Configuration initiale 416
Étape 3 – Mappage des utilisateurs Azure aux groupes Tenable 423
Étape 4 – Finalisation de la configuration dans Azure 429
Étape 5 – Activation de l'intégration 430
Se connecter via SSO 431

Bienvenue dans Tenable OT Security

Tenable OT Security (OT Security, anciennement Tenable.ot) protège les réseaux industriels contre les cybermenaces, les malveillances internes et les erreurs humaines. Détection et atténuation des menaces, suivi des assets, gestion des vulnérabilités, contrôle de la configuration et vérification des requêtes actives : les fonctions de sécurité pour les systèmes de contrôles industriels (ICS) de OT Security permettent de maximiser la visibilité, la sécurité et le contrôle de vos environnements opérationnels.

OT Security fournit des outils et des rapports de sécurité complets pour le personnel chargé de la sécurité informatique et les ingénieurs OT. La solution offre une visibilité sur les segments IT et OT convergés et sur l'activité ICS, et elle vous informe des conditions de tous les sites et leurs assets OT respectifs, des serveurs Windows aux fonds de panier de contrôleur PLC, le tout dans une vue centralisée.

OT Security possède les fonctionnalités clés suivantes :

- **Visibilité à 360 degrés** – Dans une infrastructure IT/OT, les attaques peuvent facilement se propager. Grâce à une plateforme unique pour gérer et mesurer le cyber-risque sur vos systèmes OT et IT, vous obtenez une visibilité complète sur votre surface d'attaque convergée. OT Security s'intègre également de manière native aux outils de sécurité IT et opérationnels, tels que votre solution de gestion des informations et des événements de sécurité (SIEM), mais aussi les outils de gestion des journaux, les pare-feux de nouvelle génération et les systèmes de tickets. Tous ces éléments combinés forment un écosystème où tous vos produits de sécurité fonctionnent de façon coordonnée pour assurer la sécurité de votre environnement.
- **Détection et atténuation des menaces** – OT Security utilise un moteur de détection multiple pour détecter les événements et les comportements à haut risque susceptibles d'affecter les opérations OT. Ce type de moteurs permet une détection basée sur les politiques, le comportement et les signatures.
- **Inventaire et détection active des assets** – Tirant parti d'une technologie brevetée, OT Security offre une visibilité sur votre infrastructure, non seulement au niveau du réseau, mais jusqu'à l'appareil lui-même. Tenable OT Security utilise des protocoles de communication natifs pour interroger les appareils IT et OT dans votre environnement ICS, afin d'identifier

toutes les activités et actions se produisant sur votre réseau.

- **Gestion des vulnérabilités basée sur le risque** —En s'appuyant sur des capacités complètes et détaillées de suivi des assets IT et OT, OT Security génère des niveaux de vulnérabilité et de risque via la fonctionnalité Predictive Prioritization pour chaque asset de votre réseau de systèmes de contrôle industriels (ICS). Ces rapports incluent une évaluation des scores de risque, des informations exploitables détaillées, ainsi que des suggestions d'atténuation.
- **Contrôle des configurations** – OT Security fournit un historique granulaire complet des changements de configuration des appareils au fil du temps : segments spécifiques écrits en langage Ladder, tampons de diagnostic, tables d'inventaire, etc. Les administrateurs peuvent ainsi établir un instantané de sauvegarde du « dernier état opérationnel connu » pour accélérer le retour à la normale et garantir la conformité aux réglementations de l'industrie.

Conseils : le *guide de l'utilisateur Tenable OT Security* et l'interface utilisateur sont disponibles en anglais, japonais, allemand, français et chinois simplifié. Pour modifier la langue de l'interface utilisateur, voir Paramètres locaux.

Pour plus d'informations sur Tenable OT Security, consultez les supports de formation client suivants :

- Introduction à Tenable OT Security (Tenable University)

Premiers pas avec OT Security

Pour prendre en main OT Security, suivez les étapes décrites dans Premiers pas avec OT Security.

Technologies OT Security

La solution complète OT Security comprend deux technologies de collecte principales :

- **Détection réseau** – La technologie de détection réseau OT Security est un moteur passif d'inspection approfondie des paquets, spécialement conçu pour répondre aux caractéristiques et aux exigences uniques des systèmes de contrôle industriels. La détection réseau offre une visibilité approfondie et en temps réel de toutes les activités effectuées sur le réseau opérationnel, avec un accent particulier sur les activités d'ingénierie. Cela inclut les

chargements et téléchargements de firmwares, les mises à jour apportées au code et les modifications de configuration effectuées sur des protocoles de communication propriétaires spécifiques au fournisseur. La détection réseau signale en temps réel les activités suspectes/non autorisées et produit un journal complet des événements avec un relevé des preuves. La détection réseau génère trois types d'alertes :

- **Basées sur des politiques** – Pour déclencher des alertes, vous pouvez activer des politiques prédéfinies ou créer des politiques personnalisées qui mettent sur liste d'autorisation et/ou liste de blocage des activités spécifiques potentiellement révélatrices de cybermenaces ou d'erreurs opérationnelles. Des politiques peuvent également déclencher des vérifications par requêtes actives pour des situations prédéfinies.
- **Anomalies comportementales** – Le système détecte les déviations par rapport à une référence de trafic réseau, établie en fonction de modèles de trafic définis sur une plage de temps spécifiée. Il détecte également les scans suspects pouvant indiquer la présence de malware ou de comportements de reconnaissance.
- **Politiques de détection de signature** – Ces politiques détectent les menaces OT et IT basées sur les signatures, afin d'identifier le trafic réseau indiquant des menaces d'intrusion. La détection est basée sur des règles cataloguées dans le moteur de détection de menaces Suricata.

- **Requête active (Active Querying)** – La technologie d'active querying brevetée de OT Security permet de surveiller les appareils présents sur le réseau, en examinant périodiquement les métadonnées des appareils de contrôle du réseau ICS. Cette technologie améliore la capacité de OT Security à découvrir et à classer automatiquement tous les assets ICS. Cela inclut les appareils de niveau inférieur tels que contrôleurs logiques programmables (PLC) et les unités terminales à distance (RTU), même lorsqu'ils ne sont pas actifs sur le réseau. Elle identifie également les changements locaux dans les métadonnées de l'appareil (par exemple, la version du firmware, les détails de configuration et l'état) ainsi que les changements dans chaque code/bloc fonctionnel de la logique de l'appareil. En utilisant des requêtes en lecture seule dans les protocoles de communication natifs du contrôleur, elle est sûre et n'a aucun impact sur les appareils. Les requêtes peuvent être exécutées périodiquement selon un calendrier prédéfini ou à la demande de l'utilisateur.

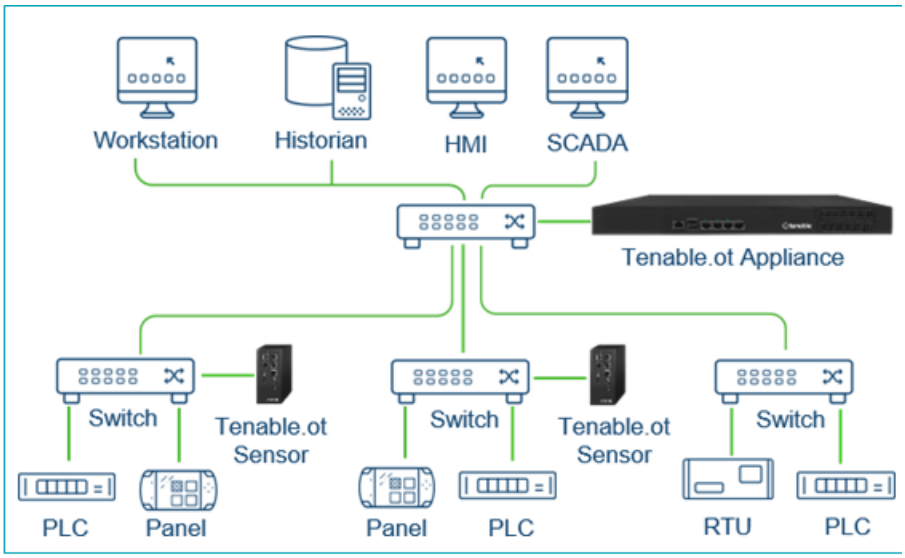
Architecture de la solution

Composants de la plateforme OT Security

Remarque : dans ce document, l'appliance OT Security est appelée ICP (plateforme Core industrielle).

La solution OT Security est constituée de ces composants :

- **ICP** (**appliance OT Security**) —Ce composant collecte et analyse le trafic réseau directement à partir du réseau (via un port SPAN ou un TAP réseau) et/ou à l'aide d'un flux de données provenant du capteur Capteur Tenable OT Security (Capteur OT Security). L'appliance ICP exécute à la fois les fonctions de détection réseau et de requête active.
- **Capteurs OT Security** – Il s'agit de petits appareils pouvant être déployés sur des segments de réseau dignes d'intérêt ; il est possible d'installer jusqu'à un capteur par commutateur géré. Les capteurs OT Security offrent une visibilité totale sur ces segments de réseau : ils capturent l'ensemble du trafic, compressent les données, puis communiquent les informations à l'appliance OT Security. Vous pouvez configurer les capteurs versions 3.14 et supérieures pour envoyer des requêtes actives aux segments de réseau sur lesquels ils sont déployés.



Composants réseau

OT Security prend en charge l'interaction avec les composants réseau suivants :

- **Utilisateur OT Security (gestion)** – Vous pouvez créer des comptes utilisateur pour contrôler l'accès à la console de gestion OT Security. Vous pouvez accéder à la console de gestion sur un navigateur (Google Chrome) via une authentification HTTPS en SSL (Secure Socket Layer).

Remarque : l'accès à l'interface utilisateur de OT Security nécessite la dernière version de Chrome.

- **Serveur Active Directory** – Les informations d'authentification de l'utilisateur peuvent éventuellement être attribuées à l'aide d'un serveur LDAP tel qu'Active Directory. Dans ce cas, les privilèges utilisateurs sont gérés dans Active Directory.
- **SIEM** – Les journaux d'événements OT Security peuvent être envoyés à un SIEM à l'aide du protocole Syslog.
- **Serveur SMTP** – Les notifications d'événements OT Security peuvent être envoyées par e-mail à des groupes spécifiques d'employés via un serveur SMTP.
- **Serveur DNS** – Les serveurs DNS peuvent être intégrés à OT Security pour aider à résoudre les noms d'assets.
- **Applications tierces** – Les applications externes peuvent interagir avec OT Security à l'aide de son API REST, ou accéder aux données à l'aide d'autres intégrations spécifiques[1].

[1]Par exemple, OT Security prend en charge l'intégration à Palo Alto Networks Next Generation Firewall (NGFW) et Aruba ClearPass, permettant ainsi à OT Security de partager les informations d'inventaire des assets avec ces systèmes. OT Security peut également s'intégrer à d'autres plateformes Tenable telles que Tenable Vulnerability Management et Tenable Security Center. Les intégrations sont configurées sous **Paramètres locaux** > **Intégrations**. Voir Intégrations.

Spécifications matérielles Tenable OT Security

Spécifications pour l'ICP

Voici les spécifications des appliances matérielles OT Security pour la plateforme Core industrielle (ICP) :

IEI ICP

Catégorie	IEI ICP

Processeur	Xeon®D-2177
Cœurs	14
RAM	64 Go
Stockage	SSD 256 Go NVMe 800 Go Disque dur 2 To
Réseau (cuivre Ethernet)	8 x 2,5 Gbit/s
Réseau (fibre Ethernet)	4 x 10 Go SFP+
Alimentation	Redondante 110-220 V
Format	1U demi-profondeur
Dimensions (L x H x P)	430 x 426 x 44,2 mm
Poids	7 kg
Température de fonctionnement	0~40 °C (32~104 °F)
Température de stockage	-10~50 °C (14~122 °F)
Humidité relative	5~90 % sans condensation
Certifications	CE/FCC/RoHS. Classe A CB, CCC, UL, RCM, NOM
Débit SPAN maximal	500 Mbit/s

Lanner ICP

Catégorie	Lanner ICP

Processeur	Intel®Xeon™D-1577, 1,3 GHz
Cœurs	16
RAM	64 Go
Stockage	SSD 1 To SSD 2 To
Réseau (cuivre Ethernet)	4 x 1 Gbit/s
Réseau (fibre Ethernet)	S/O
Alimentation	Unique 110-220 V
Format	1U demi-profondeur
Dimensions (L x H x P)	438 x 44 x 321 mm 17,2 x 1,73 x 12,64 po
Poids	7,5 kg
Température de fonctionnement	0~40 °C (32~104 °F)
Température de stockage	-20~70 °C (-4~158 °F)
Humidité relative	5~90 % sans condensation
Certifications	CE/FCC classe A, RoHS
Débit SPAN maximal	500 Mbit/s

Lenovo ICP

Catégorie	Lenovo ICP

Processeur	Intel®Xeon™D-2183dIT, 2,0 GHz
Cœurs	16
RAM	64 Go
Stockage	SATA M.2 1 To SATA M.2 2 To
Réseau (cuivre Ethernet)	6 x 1 Gbit/s
Réseau (fibre Ethernet)	2 x 10 Gbit/s SFP+
Alimentation	Adaptateur CA 2 x 240 W redondant
Format	1U demi-profondeur
Dimensions (L x H x P)	209 x 43 x 376 mm 8,2 x 1,7 x 14,8 po
Poids	3,6 kg
Température de fonctionnement	5~45 °C (41~113 °F)
Température de stockage	-20~60 °C (-4~140 °F)
Humidité relative	8~90 % sans condensation
Certifications	CE/FCC/RoHS. Classe A CB, CCC, UL, RCM, NOM
Débit SPAN maximal	500 Mbit/s

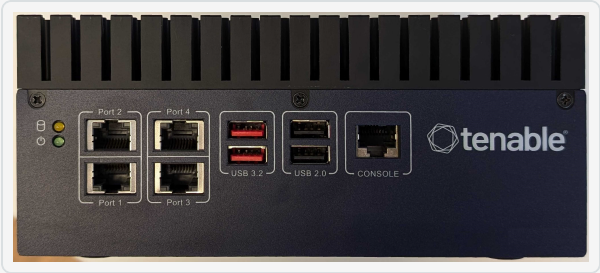
Dell ICP-XL

Catégorie	Dell ICP-XL

Processeur	2 x Xeon®Silver 4314
Cœurs	2 x 16
RAM	256 Go
Stockage	SSD 960 Go SAM FIPS-140 SED SSD 960 Go SAM FIPS-140 SED 2 x disques durs SAS 2,4 To FIPS-140 SED **Remarque :** le matériel est entièrement chiffré et conforme à la norme FIPS-140.
Réseau (cuivre)	6 x 1 Gbit/s
Réseau (fibre)	2 x 10 Go SFP+
Alimentation	Redondante 110-220 V, 165 W
Format	1U pleine profondeur
Dimensions (L x H x P)	Hauteur : 42,8 mm (1,69 po) x largeur* : 482,0 mm (18,98 po) x profondeur* : 698 mm (27,5 po) *Les dimensions incluent le cadre.
Poids	22 kg
Température de fonctionnement	0~40 °C (32~104 °F)
Température de stockage	-10~50 °C (14~122 °F)
Humidité relative	5~90 % sans condensation
Certifications	CE/FCC/RoHS CB, CCC, UL, RCM, NOM

Débit SPAN maximal	1 Gbit/s

IEI ICP-Mini

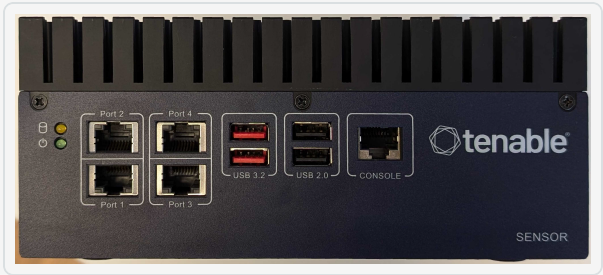
Catégorie	IEI ICP-Mini
	
Processeur	Intel® Core™ i7-1185G7E, 1,8 GHz
Cœurs	4
RAM	32 Go
Stockage	SSD 480 Go
Réseau (cuivre)	4 x 2,5 Gbit/s
Réseau (fibre)	S/O
Alimentation	Bornier 12~28 VCC
Format	Rail DIN
Dimensions (mm)	150 x 190 x 81 mm
Poids	1,9 kg
Température de fonctionnement	0~40 °C (32~104 °F)
Température de stockage	-10~50 °C (14~122 °F)
Humidité relative	10~95 % sans condensation
Certification	CE/FCC/RoHS Classe A CB, CCC, UL, ROM, NOM

Débit SPAN maximal	150 Mbit/s

Spécifications pour les capteurs

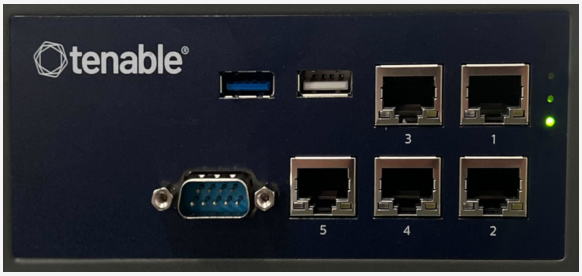
Capteur IEI

Voici les spécifications des appliances matérielles OT Security pour les capteurs :

Catégorie	Capteur IEI (4 ports)
	
Processeur	Celeron 630S5E (2 x 1,8 Ghz)
Cœurs	2
RAM	4 Go
Stockage	128 Go
Réseau (cuivre)	4 x 2,5 Gbit/s
Réseau (fibre)	S/O
Alimentation	Bornier 12~28 VCC
Format	Rail DIN
Dimensions (L x H x P) (mm)	150 x 190 x 81 mm
Poids	1,9 kg
Température de fonctionnement	0~40 °C (32~104 °F)
Température de stockage	-10 °C~50° C (14~122 °F)
Humidité relative	10~95 % sans condensation

Certification	CE Classe A, FCC Classe A, RoHS Classe A CB, CCC, UL, ROM, NOM
Débit SPAN maximal	S/O

Capteur Lanner

Catégorie	Capteur Lanner
	
Processeur	Intel®Atom™E3845, 1,91 GHz
Cœurs	4
RAM	4 Go
Stockage	SSD 64 Go
Réseau (cuivre)	5 x 1 Gbit/s
Réseau (fibre)	S/O
Alimentation	Bornier 12~28 VCC
Format	Rail DIN
Dimensions (L x H x P)	78 x 146 x 127 mm 3 x 5,75 x 5 po
Poids	1,25 kg
Température de fonctionnement	-40~70 °C (-40~158 °F)
Température de stockage	-40~85 °C (-40~185 °F)

Humidité relative	5~95 % sans condensation
Certifications	CE/FCC classe A, RoHS
Débit SPAN maximal	S/O

Capteur Lenovo

Catégorie	Capteur Lenovo
Processeur	Intel®Core™13-8145UE, 2,2 GHz
Cœurs	2
RAM	8 Go
Stockage	SATA M.2 128 Go
Réseau (cuivre)	2 x 1Gbit/s
Réseau (fibre)	S/O
Alimentation	36 W ; connecteur 2/6 broches Phoenix Contact avec verrouillage ou adaptateur d'alimentation externe 36 W, 100-240 V
Format	Très petit format
Dimensions (L x H x P)	179 x 88 x 34,5 mm 7,05 x 3,46 x 1,36 po
Poids	0,72 kg
Température de fonctionnement	0~50 °C (32~122 °F)
Température de stockage	-40~60 °C (-40~140 °F)

Humidité relative	20~80 % sans condensation
Certifications	RoHS, WEEE, REACH, ErP Lot 3, MIL-STD-810H
Débit SPAN maximal	S/O

Éléments système

Assets

Les assets représentent les composants matériels de votre réseau, tels que les contrôleurs, les stations d'ingénierie, les serveurs, etc. Les fonctions automatisées de découverte, de classification et de gestion des assets de OT Security fournissent un inventaire précis par le biais d'un suivi continu de toutes les modifications apportées aux appareils. Cela simplifie le maintien de la continuité, de la fiabilité et de la sécurité opérationnelles. Cela joue également un rôle clé dans la planification des projets de maintenance, la priorisation des mises à niveau, les déploiements de correctifs, la réponse aux incidents et les efforts d'atténuation.

Évaluation des risques

OT Security utilise des algorithmes sophistiqués pour évaluer le degré de risque posé à chaque asset du réseau. Un score de risque (de 0 à 100) est attribué à chaque asset du réseau. Le score de risque est basé sur les facteurs suivants :

- **Événements** – Événements qui se sont produits sur le réseau et qui ont affecté l'appareil (pondérés en fonction de la sévérité de l'événement et de la date à laquelle l'événement s'est produit).

  > **Remarque :** les événements sont pondérés en fonction de leur actualité, de sorte que les événements les plus récents ont un impact plus important sur le score de risque que les événements plus anciens.

- **Vulnérabilités** – Désigne les CVE qui affectent les assets de votre réseau, ainsi que d'autres menaces identifiées sur le réseau (par exemple, systèmes d'exploitation obsolètes, utilisation

de protocoles vulnérables, ports ouverts vulnérables, etc.). OT Security les détecte comme des correspondances de plug-in sur vos assets.

- **Criticité de l'asset** – Mesure de l'importance de l'appareil pour le bon fonctionnement du système.

  > **Remarque :** le score de risque des contrôleurs PLC connectés à un fond de panier est affecté par le score de risque des autres modules qui partagent ce fond de panier.

Politiques et événements

Les politiques définissent des types spécifiques d'événements suspects, non autorisés, anormaux ou autrement remarquables qui se produisent dans le réseau. Lorsqu'un événement se produit et répond à toutes les conditions de la définition d'une politique, OT Security génère un événement. OT Security consigne l'événement et envoie des notifications conformément aux Actions de politique configurées pour la politique.

Il existe deux types d'événements liés aux politiques :

- **Détection basée sur des politiques** – Déclenche des événements lorsque les conditions précises de la politique, telles que définies par une série de descripteurs d'événements, sont réunies.
- **Détection d'anomalies** – Déclenche des événements lorsqu'une activité anormale ou suspecte est identifiée sur le réseau.

Le système comporte un ensemble de politiques prédéfinies (prêtes à l'emploi). De plus, le système offre la possibilité de modifier les politiques prédéfinies ou d'établir de nouvelles politiques personnalisées.

Détection basée sur des politiques

Pour la détection basée sur des politiques, vous devez configurer les conditions spécifiques pour les événements du système qui déclencheront des notifications d'événement. Les événements basés sur des politiques ne sont déclenchés que lorsque les conditions précises de la politique sont réunies. Cela garantit l'absence de faux positifs, car le système signale les événements réels qui se produisent dans le réseau ICS, tout en fournissant des informations détaillées significatives sur

« qui », « quoi », « quand », « où » et « comment ». Les politiques peuvent être basées sur divers types d'événements et de descripteurs.

Voici quelques exemples de configurations de politique possibles :

- **Activité anormale ou non autorisée du plan de contrôle ICS (ingénierie)** – Une interface homme-machine (IHM) ne doit pas interroger la version du firmware d'un contrôleur (peut indiquer une reconnaissance). De même, un contrôleur ne doit pas être programmé pendant les heures de fonctionnement (peut indiquer une activité non autorisée et potentiellement malveillante).
- **Modification du code du contrôleur** – Une modification de la logique du contrôleur a été identifiée (Déviation par rapport à l'instantané).
- **Communications réseau anormales ou non autorisées** – Un protocole de communication non autorisé a été utilisé entre deux assets du réseau, ou une communication a eu lieu entre deux assets qui n'ont jamais communiqué auparavant.
- **Modifications anormales ou non autorisées de l'inventaire des assets** – Un nouvel asset a été découvert, ou un asset a cessé de communiquer sur le réseau.
- **Modifications anormales ou non autorisées des propriétés de l'asset** – Le firmware ou l'état de l'asset a changé.
- **Écritures de points de consigne anormales** – Des événements sont générés lorsque des modifications sont apportées à des paramètres spécifiques. Vous pouvez définir les plages autorisées pour un paramètre et générer des événements en cas de déviation par rapport à cette plage.

Détection des anomalies

Les politiques de détection des anomalies identifient les comportements suspects dans le réseau grâce aux fonctions intégrées au système qui détectent les écarts par rapport à une activité dite « normale ». Les politiques de détection d'anomalies suivantes sont disponibles :

- **Déviations par rapport au trafic réseau de référence** – L'utilisateur définit un trafic réseau « normal » de référence, basé sur la carte du trafic pendant une plage temporelle donnée. Tout écart génère alors une alerte. La référence peut être mise à jour à tout moment.

- **Pic de trafic réseau** – Une augmentation spectaculaire du volume du trafic réseau ou du nombre de communications est détectée.
- **Activité potentielle de reconnaissance du réseau/ cyber-attaque** – Des événements sont générés pour les activités au sein du réseau indiquant une reconnaissance ou une cyber-attaque, telles que les conflits IP, les scans de port TCP et les scans ARP.

Catégories de politiques

Les politiques sont organisées selon les catégories suivantes :

- **Politiques d'événements de configuration** – Ces politiques concernent des activités se déroulant sur le réseau. Il existe deux sous-catégories de politiques d'événements de configuration :
    - **Validation du contrôleur** – Ces politiques concernent les changements ayant lieu au sein des contrôleurs du réseau. Cela peut impliquer des modifications de l'état d'un contrôleur, ainsi que des modifications du firmware, des propriétés des assets ou des blocs de code. Les politiques peuvent être limitées à des planifications spécifiques (par exemple, la mise à niveau du firmware pendant une journée de travail) et/ou à un ou plusieurs contrôleurs spécifiques.
    - **Activités du contrôleur** – Ces politiques concernent des commandes d'ingénierie spécifiques qui ont un impact sur l'état et la configuration des contrôleurs. Il est possible de définir des activités spécifiques qui génèrent systématiquement des événements ou de désigner un ensemble de critères pour la génération d'événements. Par exemple, si certaines activités sont effectuées à certains moments et/ou sur certains contrôleurs. La création d'une liste de blocage (ou liste rouge) et d'une liste d'autorisations (liste verte) pour les assets, les activités et les calendriers est prise en charge.
- **Politiques d'événements réseau** – Ces politiques concernent les assets du réseau et les flux de communication entre les assets. Cela inclut les assets qui ont été ajoutés ou supprimés du réseau. Cela inclut également les modèles de trafic jugés anormaux pour le réseau, ou signalés comme particulièrement préoccupants. Par exemple, si une station d'ingénierie communique avec un contrôleur à l'aide d'un protocole non pré-configuré (par exemple, des

protocoles utilisés par des contrôleurs fabriqués par un fournisseur spécifique), un événement est déclenché. Ces politiques peuvent être limitées à des horaires et/ou à des assets spécifiques. Les protocoles spécifiques aux fournisseurs sont organisés par fournisseur pour plus de commodité, tandis que n'importe quel protocole peut être utilisé dans une définition de politique.

- **Politiques d'événement SCADA** – Ces politiques détectent les changements dans les valeurs de point de consigne qui peuvent nuire au processus industriel. Ces changements peuvent résulter d'une cyber-attaque ou d'une erreur humaine.
- **Politiques de détection des menaces réseau** – Ces politiques utilisent la détection des menaces OT et IT basée sur les signatures pour identifier le trafic réseau qui indique des menaces d'intrusion. La détection est basée sur des règles cataloguées dans le moteur de détection de menaces Suricata.

Groupes

Les groupes sont un aspect essentiel de la définition des politiques dans OT Security. Lors de la configuration d'une politique, chacun des paramètres s'applique à un groupe et non à des entités individuelles. Cela simplifie considérablement le processus de configuration de la politique.

Événements

Lorsqu'un événement qui répond à toutes les conditions d'une politique se produit, un événement est généré dans le système. Tous les événements sont affichés sur l'écran Événements et sont également accessibles via les écrans Inventaire et Politique pertinents. Chaque événement est associé à un niveau de sévérité indiquant son degré de risque. Des notifications peuvent être automatiquement envoyées aux destinataires des e-mails et aux SIEM, comme spécifié dans les Actions de politique de la politique qui a généré l'événement.

Un événement peut être marqué comme résolu par un utilisateur autorisé et un commentaire peut être ajouté.

Composants de licence OT Security

Cette rubrique décompose le processus de gestion des licences pour Tenable OT Security en tant que produit autonome. Elle explique également comment les assets sont comptabilisés, répertorie les composants supplémentaires que vous pouvez acheter, explique comment les licences sont récupérées et décrit ce qui se passe en cas de dépassement ou d'expiration de licence.

Conseil : pour mettre à jour ou réinitialiser votre licence, voir Workflow de licence OT Security.

Gestion des licences Tenable OT Security

Tenable OT Security est disponible sur abonnement ou en version perpétuelle/de maintenance.

Pour utiliser Tenable OT Security, vous achetez des licences en fonction de vos besoins organisationnels et des spécificités de votre environnement. Tenable OT Security attribue ensuite ces licences à vos *assets*, c'est-à-dire tous les appareils détectés avec des adresses IP. Une licence est affectée à chaque adresse IP.

Lorsque votre environnement s'agrandit, le nombre de vos assets augmente lui aussi ; vous allez donc acheter davantage de licences pour tenir compte de cette évolution. Les licences Tenable sont soumises à des tarifs dégressifs. Autrement dit, plus vous en achetez, plus le prix unitaire est bas. Pour connaître les prix, contactez votre représentant Tenable.

Comment les assets sont comptabilisés

Dans Tenable OT Security, le nombre de licences est basé sur le nombre d'adresses IP uniques dans votre environnement. Les assets sont sous licence à partir du moment où ils sont détectés.

Remarque : les assets qui résident sur les réseaux internes derrière des adresses IP actives ne sont pas pris en compte dans votre licence. Par exemple, dans un châssis de contrôleur logique programmable (PLC) connecté de manière redondante avec deux adresses IP actives derrière lesquelles se trouvent 10 modules, seules les deux adresses IP actives sont prises en compte dans votre licence.

Remarque : bien que vous puissiez connecter un achat autonome de OT Security à votre instance de Tenable One, la gestion des licences de ces assets n'est pas prise en charge. Les clients Tenable One disposent d'un grand nombre de solutions Tenable disponibles sous licence, y compris OT Security, mais les licences doivent d'abord faire partie de la licence Tenable One. Vous pouvez échanger avec vos Customer Success Managers (CSM) pour mettre à jour le compte en conséquence.

Composants Tenable OT Security

Vous pouvez personnaliser Tenable OT Security selon votre cas d'utilisation en ajoutant des composants. Certains composants sont des modules complémentaires que vous achetez.

Inclus à l'achat	Composant complémentaire
• Appliance Core virtuelle • Tenable Security Center.	• Tenable OT Security Enterprise Manager. • Capteur configurable Tenable OT Security • Capteur configurable certifié Tenable OT Security • Plateforme Core certifiée Tenable OT Security • Plateforme Core Tenable OT Security • Plateforme Core XL Tenable OT Security

Récupération de licences

Lorsque vous achetez des licences, le nombre total de vos licences reste le même pendant toute la durée de votre contrat, sauf si vous achetez des licences supplémentaires. Cependant, Tenable OT Security récupère des licences en temps réel à mesure que le nombre de vos assets change.

Tenable OT Security récupère les licences des assets suivants :

- Assets masqués
- Assets hors ligne depuis plus de 30 jours
- Assets supprimés ou masqués dans l'interface utilisateur

Dépassement de la limite de licences

Dans Tenable OT Security, vous ne pouvez utiliser que le nombre de licences qui vous a été attribué, à moins que vous n'achetiez d'autres licences.

Lorsque vous dépassez la limite de licences :

- Les non-administrateurs ne peuvent plus accéder à Tenable OT Security.
- Un message indiquant le dépassement de licences apparaît dans l'interface utilisateur.
- Vous ne pouvez plus restaurer d'assets à partir des paramètres de Tenable OT Security.

- Vous ne pouvez plus mettre à jour les plug-ins de vulnérabilité ni les signatures IDS (mises à jour de flux).

Remarque : lorsque vous dépassez votre limite de licences, Tenable OT Security peut toujours détecter et ajouter de nouveaux assets.

Licences expirées

Les licences Tenable OT Security que vous achetez sont valables pendant toute la durée de votre contrat. Trente jours avant l'expiration de votre licence, un avertissement apparaît dans l'interface utilisateur. Pendant cette période de renouvellement, échangez avec votre représentant Tenable pour ajouter ou supprimer des produits ou bien pour modifier le nombre de vos licences.

Une fois votre licence expirée, Tenable OT Security est désactivé et vous ne pouvez plus l'utiliser.

Messages d'erreur

Le tableau suivant décrit les messages d'erreur qui peuvent apparaître dans Tenable OT Security.

Catégorie	Nom de la catégorie d'erreurs	Description de l'erreur	Message de l'interface utilisateur	Action recommandée
Gestion des requêtes actives	**NoRoutesForClient**	Une requête a reçu une erreur de routage du réseau.	Vous rencontrez peut-être un problème de connectivité réseau. Veuillez vérifier la connectivité réseau, puis renvoyer la requête.	Vérifiez votre connectivité réseau, puis renvoyez la requête active.

Gestion des requêtes actives	**InternalError**	Une erreur interne s'est produite lors de la tentative d'envoi de la requête.	Une erreur inattendue s'est produite. Veuillez réessayer plus tard. Si le problème persiste, contactez l'assistance technique.	Renvoyez la requête après un certain temps. Si le problème persiste, contactez l'assistance Tenable.
Gestion des requêtes actives	**DnsError**	Nom d'hôte DNS introuvable pour l'adresse IP cible.	Aucun nom d'hôte DNS n'a été trouvé pour l'adresse IP cible. Veuillez vous assurer que le DNS inversé est activé et qu'un enregistrement PTR est défini pour l'adresse IP.	Vérifiez si la recherche DNS inversée est activée et si l'enregistrement de pointeur DNS (PTR) est défini pour l'adresse IP.
Gestion des requêtes actives	**HostUnreachableError**	Impossible d'atteindre une cible de requête. Vérifiez votre routage.	Impossible d'accéder à l'appareil. Cela peut être dû à un problème de connectivité réseau.	Vérifiez les paramètres de connectivité réseau et du pare-feu, puis renvoyez la requête

			Veuillez vérifier les paramètres de votre réseau ou de votre pare-feu, puis réessayez.	active.
Gestion des requêtes actives	**TimeoutError**	Une requête n'a reçu aucune réponse de la cible et le délai d'attente a expiré.	Expiration du délai d'attente du réseau. Cela peut être dû à des problèmes temporaires de réseau ou à une réponse lente de la part de l'appareil. Veuillez réessayer de lancer la requête plus tard.	Renvoyez la requête après un certain temps.
Gestion des requêtes actives	**NetworkError**	Une requête a reçu une réponse d'erreur du réseau.	Une erreur réseau s'est produite. Cela peut être dû à des problèmes temporaires de réseau ou à des restrictions de pare-feu.	Vérifiez votre connectivité réseau, puis renvoyez la requête.

			Veuillez vérifier votre connectivité réseau, puis renvoyer la requête.	
Gestion des requêtes actives	**ProtocolError**	Une requête a reçu une réponse inattendue de la cible.	Format de réponse de la cible non pris en charge. Cela peut être dû à une version de protocole incompatible sur l'appareil ou à un problème temporaire du réseau. Veuillez vérifier la compatibilité de l'appareil ou renvoyer la requête plus tard.	Vérifiez si l'appareil cible est compatible ou renvoyez la requête après un certain temps.
Gestion des requêtes actives	**AuthenticationError**	Des identifiants d'authentification non valides ont été utilisés dans la	Échec de l'authentification auprès de l'appareil. Les informations d'identification	Vérifiez vos informations d'authentification et renvoyez la requête.

		requête.	sont peut-être incorrectes ou manquantes. Veuillez vérifier vos informations d'identificatio n.	
Gestion des requêtes actives	**LimitExceededError**	OT Security a atteint la limite d'échecs pour les requêtes adressées à la cible.	Les requêtes actives adressées à cet appareil sont suspendues en raison d'un trop grand nombre d'échecs. Veuillez réessayer plus tard. Si le problème persiste, contactez l'assistance.	Plusieurs requêtes adressées à l'appareil ont échoué. Renvoyez la requête après un certain temps. Si le problème persiste, contactez l'assistance technique.
Gestion des requêtes actives	**NoPotentialClients**	Il n'existe aucun client valide dans la plage de requêtes cible (bloc CIDR, liste d'assets	La requête active n'a trouvé aucun appareil accessible dans la plage cible. Des restrictions	Il se peut que les appareils cibles ne soient pas accessibles en raison de restrictions appliquées

		ou plage d'adresses IP).	appliquées par les utilisateurs pourraient bloquer certains appareils (bloc CIDR, liste d'assets ou plage d'adresses IP). Veuillez vérifier votre sélection et vos contrôles d'accès.	par l'utilisateur. Revoyez vos paramètres de contrôle d'accès et renvoyez la requête.
Gestion des requêtes actives	**NoAllowedClients**	Il n'existe aucun client autorisé dans la plage de requêtes cible (bloc CIDR, liste d'assets ou plage d'adresses IP).	La requête active n'a trouvé aucun appareil compatible dans la plage cible (bloc CIDR, liste d'assets ou plage d'adresses IP). Veuillez vérifier votre sélection et vos contrôles d'accès.	Il se peut que les appareils cibles ne soient pas compatibles avec les paramètres OT Security. Revoyez vos paramètres de contrôle d'accès et renvoyez la requête.
Internet des objets (IoT)	**ServiceUnavailable**	Service indisponible.	Le service de connecteur IoT	Le service de connecteur I

		Un problème s'est peut-être produit lors du démarrage ou après la réinitialisation.	n'est pas disponible ou a rencontré un problème. Réessayez plus tard. Si le problème persiste, contactez l'assistance.	oT est peut-être temporairement indisponible. Renvoyez la requête après un certain temps. Si le problème persiste, contactez l'assistance technique.
IoT	**IotConnectorSecureModeError**	Le connecteur IoT ne peut pas se connecter à un agent IoT installé à distance.	Erreur du mode sécurisé du connecteur IoT. L'agent IoT présent sur le système distant doit être réinstallé pour permettre à nouveau des connexions.	Réinstallez l'agent IoT sur le système distant et relancez la connexion.
IoT	**IotConnectorIpAlreadyExists**	L'utilisateur essaie d'ajouter un connecteur avec une	Échec de la création du connecteur. L'adresse IP fournie est	Fournissez une adresse IP unique et essayez d'ajouter le

		adresse IP qui existe déjà.	déjà utilisée par un autre connecteur. Veuillez fournir une adresse IP unique, puis réessayer.	connecteur.
Appairage du serveur : (Enterprise Manager (EM), serveur externe, FW)	**WrongCertificate**	L'utilisateur essaie d'appairer l'ICP à EM avec un certificat non valide.	Le serveur d'appairage a présenté un certificat de sécurité non valide. Veuillez vérifier le certificat du serveur et réessayer. Si le problème persiste, consultez l'administrateur du serveur.	Générez un nouveau certificat de sécurité et essayez d'appairer l'ICP à EM. Si le problème persiste, contactez l'administrateur du serveur.
Appairage du serveur : (EM, serveur externe, FW)	**MissingEmAddress**	Uniquement via l'API	Aucune adresse de serveur n'a été fournie pour l'appairage. Veuillez fournir l'adresse IP ou le nom d'hôte du serveur auquel vous souhaitez vous connecter,	Fournissez l'adresse IP ou le nom d'hôte du serveur auquel vous souhaitez vous connecter, puis réessayez.

			puis réessayer.	
Appairage du serveur : (EM, serveur externe, FW)	**MissingPassword**	Uniquement via l'API	Les informations d'authentification fournies sont incomplètes. Veuillez saisir le mot de passe du serveur d'appairage et réessayer.	Fournissez un nom d'utilisateur et le mot de passe du serveur, puis réessayez.
Appairage du serveur : (EM, serveur externe, FW)	**MissingCredentials**	Uniquement via l'API	Informations d'identification de connexion manquantes pour le serveur d'appairage. Veuillez fournir les informations d'identification requises (par exemple, nom d'utilisateur et mot de passe) et réessayer.	Fournissez des informations d'identification valides pour le serveur et réessayez.
Appairage du serveur : (EM, serveur externe, FW)	**BothApiKeyAndUserCredentials**	Uniquement via l'API	Une seule méthode d'authentification est autorisée pour	Utilisez soit la clé API, soit les informations d'identificati

			l'appairage avec ce serveur. Veuillez supprimer la clé API ou les informations d'identification de l'utilisateur, puis réessayer.	on de l'utilisateur pour l'appairage.
Flux OT: PII/Suricata/Nessus	**NessusNotReady**	Service indisponible. Un problème s'est peut-être produit lors du démarrage ou après la réinitialisation.	Le service Nessus n'est pas encore disponible ou a rencontré un problème. Réessayez plus tard. Si le problème persiste, contactez l'assistance.	Le service Nessus est peut-être indisponible. Réessayez d'accéder au service après un certain temps ou, si le problème persiste, contactez Assistance Tenable.
Flux OT: PII/Suricata/Nessus	**MissingFile**	Uniquement via l'API	Aucun fichier de configuration joint. Veuillez charger un fichier de configuration valide au format pris en charge pour	Charger un fichier de configuration valide.

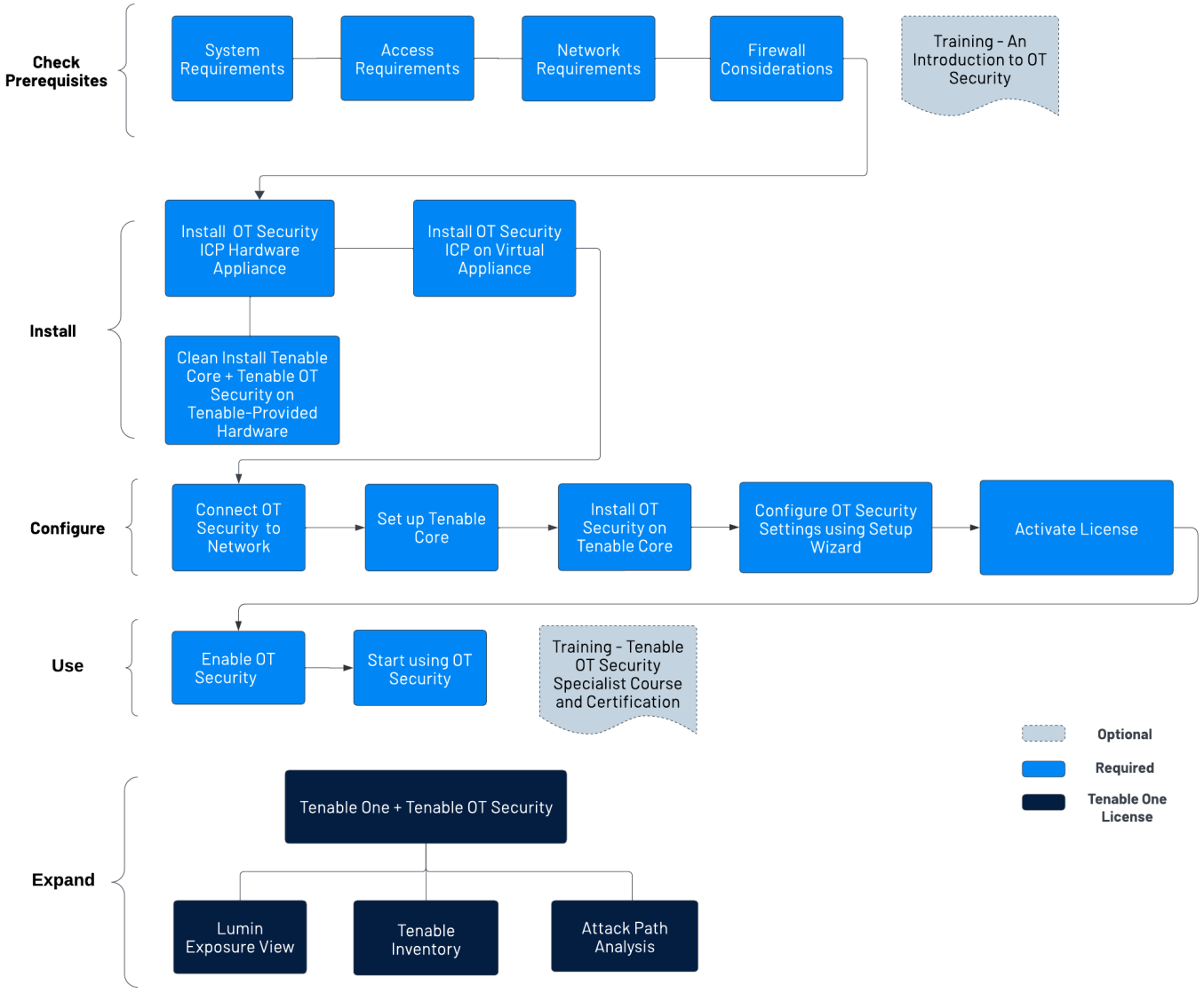
			continuer.	
Flux OT: PII/ Suricata/ Nessus	**InvalidFile**	Le fichier chargé n'est pas valide.	Le fichier chargé n'est pas valide. Il se peut que le format ne soit pas pris en charge ou que les informations de version soient absentes. Veuillez consulter la documentation sur les formats pris en charge et les champs obligatoires, puis réessayer.	Vérifiez si le format ou la version du fichier chargé est valide avant de charger le fichier.
Flux OT: PII/ Suricata/ Nessus	**NoSpaceLeftOnDevice**	Chargement d'un fichier en mode en ligne ou hors ligne alors qu'il n'y a plus d'espace disponible sur l'appareil pour le nouveau fichier.	L'appareil ne dispose pas de suffisamment d'espace de stockage pour accueillir le nouveau fichier de configuration. Veuillez libérer de l'espace sur l'appareil et réessayer.	Libérez de l'espace sur l'appareil et essayez de charger le fichier de configuration.

Flux OT: PII/Suricata/Nessus	**OldLicense**	L'utilisateur utilise une licence sans informations d'identification valides.	Action non autorisée en raison d'un format de version obsolète. Veuillez vous procurer une nouvelle licence au format pris en charge et réessayer.	Mettez à niveau votre licence OT Security dans le format pris en charge.
Flux OT: PII/Suricata/Nessus	**UpdateAlreadyInProgress**	L'utilisateur exécute actuellement une mise à jour alors qu'une tâche est déjà en cours. Une seule mise à jour peut être exécutée à la fois.	Une mise à jour est déjà en cours pour cet appareil. Veuillez attendre que la mise à jour en cours soit terminée avant d'en tenter une autre.	Attendez que la mise à jour en cours soit terminée avant de réessayer.
Flux OT: PII/Suricata/Nessus	**OlderVersionUpdateAttempt**	L'utilisateur tente de revenir à une version antérieure.	Échec du téléchargement du fichier en raison d'une version active plus récente. Assurez-vous	Assurez-vous que le fichier que vous essayez de charger est la dernière version.

			d'avoir le fichier le plus à jour et essayez de le télécharger à nouveau.	

Premiers pas avec OT Security

Suivez la séquence de démarrage ci-dessous pour installer OT Security et commencer à l'utiliser.



Vérifier les conditions préalables

- Conditions préalables —Passez en revue la configuration requise, ainsi que les exigences matérielles, virtuelles et de licence pour OT Security.
    - Exigences système —Passez en revue les exigences pour installer et exécuter Tenable Core + OT Security.
    - Exigences d'accès —Passez en revue la configuration Internet et la configuration des ports requises pour exécuter Tenable Core + OT Security.
    - Considérations sur le réseau —Passez en revue les interfaces réseau pour connecter OT Security.
    - Considérations sur le pare-feu —Passez en revue les ports qui doivent être ouverts pour que OT Security fonctionne correctement.
    - Introduction à Tenable OT Security —Parcourez le support de formation pour vous familiariser avec OT Security.

Installer l'ICP OT Security

OT Security est une application qui s'exécute au-dessus du système d'exploitation de Tenable Core et est soumise aux exigences de base de Tenable Core. Suivez les instructions ci-dessous pour installer et configurer Tenable Core + OT Security.

Pour installer OT Security :

1. Installer l'ICP OT Security
    - Installer une appliance matérielle ICP OT Security —Configurez OT Security en tant qu'appliance matérielle.

      > **Remarque** : le matériel Tenable Core fourni par Tenable est livré avec Tenable Core + OT Security pré-installé. Si vous installez une appliance antérieure ou ancienne, vous pouvez opter pour une nouvelle installation. Pour plus d'informations, voir Nouvelle installation Tenable Core + Tenable OT Security sur le matériel fourni par Tenable.

- Installer une appliance virtuelle ICP OT Security —Déployez Tenable Core + OT Security en tant que machine virtuelle à l'aide du fichier `.ova` pré-configuré contenant la configuration standard de la machine virtuelle, ou personnalisez votre appliance à l'aide du fichier d'installation `.iso`.

2. Connecter OT Security au réseau —Connectez l'appliance matérielle et virtuelle OT Security au réseau.
3. Configurer l'ICP OT Security
   a. Configurer Tenable Core —Configurez Tenable Core via la CLI ou l'interface utilisateur.
   b. Installer OT Security sur Tenable Core —Terminez manuellement l'installation de Tenable OT Security dans Tenable Core.
   c. Configurer les paramètres OT Security à l'aide de l'assistant de configuration —Utilisez l'assistant de configuration pour configurer les paramètres de base dans OT Security.
      - Connectez-vous à la console OT Security et configurez les paramètres Informations utilisateur, Appareil, Heure système et Séparation des ports.
4. Activer la licence OT Security —Activez votre licence après avoir terminé l'installation de OT Security.

Utiliser OT Security

Lancer OT Security

1. Activer OT Security —Activez OT Security après avoir activé votre licence.
2. Commencer à utiliser OT Security —Configurez vos réseaux surveillés, la séparation des ports, les utilisateurs, les groupes, les serveurs d'authentification, etc. pour commencer à utiliser OT Security.

> **Conseil** : pour acquérir une expérience pratique et pour obtenir la certification Specialist Tenable OT Security, suivez le Cours Specialist pour Tenable OT Security.

Intégrer OT Security à Tenable One

Remarque : cela nécessite une licence Tenable One. Pour plus d'informations sur l'essai de Tenable One, voir Tenable One.

Intégrez OT Security à Tenable One et exploitez les fonctionnalités suivantes :

- Dans Lumin Exposure View, révélez les niveaux de risque convergés et découvrez les faiblesses cachées au-delà de la frontière entre les domaines IT et OT. Vous pouvez contrôler et suivre en permanence les vulnérabilités potentielles grâce aux données OT améliorées :
    - Consultez la fiche d'exposition **Global Exposure Card** (Fiche d'exposition globale) pour comprendre votre score holistique. Cliquez sur **Per Exposure** (Par exposition) pour comprendre quels facteurs déterminent votre score et dans quelle mesure.
    - Consultez la fiche d'exposition **Operational Technologies Card** (Fiche des technologies opérationnelles).
    - Configurez les paramètres de la vue de l'exposition (Exposure View Settings) pour définir une cible de carte personnalisée et paramétrer les options **Remediation SLA** (SLA de remédiation) et **SLA Efficiency Target** (Efficacité du SLA) en fonction de la politique de votre entreprise.
    - Créez une carte d'exposition personnalisée (Custom Exposure Card) en fonction du contexte opérationnel et incluez le nouveau tag que vous avez créé dans Tenable Inventory.
- Dans Tenable Inventory, enrichissez la découverte des assets avec des informations spécifiques à l'OT, telles que les versions de firmware, les fournisseurs, les modèles et les états opérationnels. Accédez aux renseignements OT que les outils de sécurité informatiques standard ne peuvent pas fournir :
    - Examinez vos assets OT pour comprendre la nature stratégique de l'interface. Cela devrait vous aider à choisir les fonctionnalités à utiliser dans Tenable Inventory et dans quelles circonstances les utiliser.
    - Passez en revue les requêtes **Tenable** (Tenable Queries) que vous pouvez utiliser, modifier et ajouter aux favoris.

- Familiarisez-vous avec le générateur de requêtes de recherche globale, ainsi qu'avec ses objets et propriétés. Ajoutez des requêtes personnalisées aux favoris pour les réutiliser ultérieurement.

  > **Conseil :** pour obtenir un aperçu des propriétés disponibles :
  >
  > - Dans le générateur de requêtes, saisissez *has*. La liste des propriétés d'asset suggérées s'affiche.
  > - Personnalisez la liste en ajoutant une colonne. La liste des colonnes/propriétés disponibles s'affiche.

- Explorez la page des détails de l'asset pour consulter les propriétés de l'asset et toutes les vues contextuelles associées.

- Créez un tag dynamique pour vos assets OT, où :

  - Opérateur = **type de système hôte**
  - Valeur = **PLC**

- (Facultatif) Créez un tag qui combine différentes classes d'assets.

- Dans Attack Path Analysis, exposez les chemins réseau vulnérables qui pourraient perturber des opérations clés telles que les lignes de production ou les centres de données. Vous pouvez suivre les chemins de communication OT et les modifications non autorisées :

  - Affichez le **dashboard Attack Path Analysis** (Analyse du chemin d'attaque) pour obtenir une vue de haut niveau sur les assets vulnérables avec le nombre de chemins d'attaque menant à ces assets critiques, le nombre de détections ouvertes et leur sévérité, une matrice permettant d'afficher les chemins avec différents scores d'exposition de nœud source et des combinaisons de valeurs cibles ACR, ainsi qu'une liste de tendances concernant les chemins d'attaque.

    - Consultez la **Top Attack Path Matrix** (matrice des principaux chemins d'attaque) et cliquez sur la tuile **Top Attack Paths** (Chemins d'attaque principaux) pour afficher des informations supplémentaires sur vos assets les plus précieux, c'est-à-dire ceux avec un classement ACR de 7 ou plus.

  Vous pouvez les ajuster si nécessaire pour visualiser les données et les détections les plus critiques concernant les chemins d'attaque.

- Sur la page **Findings** (Détections), affichez toutes les techniques d'attaque présentes dans un ou plusieurs chemins d'attaque qui mènent à un ou plusieurs assets critiques en associant vos données à des analyses graphiques avancées et au cadre MITRE ATT&CK® Vous pourrez ainsi créer des détections qui vous aideront à comprendre et à traiter les inconnues qui favorisent et amplifient l'impact des menaces sur vos assets et vos informations.
- Sur la **carte thermique (Heatmap) Mitre Att&ck**, sélectionnez l'option de carte thermique **ICS** pour vous concentrer sur les tactiques et techniques ICS (systèmes de contrôle industriels).
- Sur la page **Discover** (Découvrir), générez des requêtes de chemin d'attaque pour afficher vos assets dans le cadre de chemins d'attaque potentiels :
  - Generate an Attack Path using a Built-in Query (Générer un chemin d'attaque à l'aide d'une requête intégrée)
  - Generate an Asset Query using the Asset Query Builder (Générer une requête d'asset à l'aide du générateur de requêtes d'asset)
  - Generate an Attack Path Query using the Attack Path Query Builder (Générer une requête de chemin d'attaque à l'aide du générateur de requêtes de chemin d'attaque)

  Vous pouvez ensuite afficher et les données des requêtes de chemin d'attaque (Attack Path Queries) et des requêtes d'asset (Asset Queries)et interagir avec elles via la liste des résultats des requêtes et le graphe interactif.

Conditions préalables

Objectif : vérifier que vous disposez de tout ce dont vous avez besoin pour réussir l'installation de l'ICP.

Tenable OT Security est une application qui s'exécute au-dessus du système d'exploitation de Tenable Core et est soumise aux exigences de base de Tenable Core.

La combinaison Tenable Core + Tenable OT Security peut être aussi bien déployée sur une appliance matérielle qu'une machine virtuelle. Le déploiement d'une machine virtuelle doit répondre aux exigences minimales mentionnées dans Configuration matérielle requise.

Configuration matérielle requise

Plusieurs tailles d'appliances matérielles Tenable Core + Tenable OT Security dédiées sont disponibles (vendues séparément). Pour les spécifications matérielles, voir la fiche du matériel physique Tenable OT Security.

Le système d'exploitation Tenable Core et l'application Tenable OT Security sont pré-installés sur toutes les appliances matérielles disponibles.

Vous pouvez également installer Tenable Core + Tenable OT Security sur du matériel personnalisé conforme à la configuration requise. Pour obtenir les instructions, contactez votre Customer Success Manager Tenable.

Pour plus d'informations sur les exigences pour Tenable Core + Tenable OT Security, consultez les rubriques suivantes :

- Exigences système
- Exigences d'accès

Configuration requise pour les appliances virtuelles

Tenable Core + Tenable OT Security peut être déployé des manières suivantes :

- À l'aide du fichier `.ova` —Ce fichier est prêt à être déployé et contient toute la configuration standard et prise en charge des machines virtuelles.
- À l'aide du fichier `.iso` —Il s'agit d'une image disque d'installation à usage général. Déployez-la sur une machine virtuelle correctement configurée, conforme à la configuration requise.

Exigences de licence

Pour des informations générales sur la gestion des licences de OT Security, voir Composants de licence OT Security.

Pour le workflow de gestion des licences, voir Activation de licence OT Security.

Exigences système

Pour installer et exécuter Tenable Core + OT Security ou le Capteur OT Security, votre application et votre système doivent répondre aux exigences suivantes.

Conseil : OT Security propose des appliances clés en main qui sont livrées directement pré-imagées. Cette option est beaucoup plus facile à utiliser et à déployer, ce qui accélère le délai de rentabilisation. Cependant, vous pouvez également vous procurer votre propre matériel et lui appliquer notre image ISO. Si vous fournissez votre matériel ou choisissez d'utiliser le nôtre, suivez les spécifications matérielles Tenable OT comme guide ou meilleure pratique. Tous les composants de OT Security, l'ICP EM et le capteur peuvent être exécutés sur n'importe quel matériel répondant aux spécifications.

Remarque : Tenable ne recommande pas de déployer plusieurs applications sur une même instance de Tenable Core. Pour déployer plusieurs applications sur Tenable Core, déployez une instance pour chaque application.

Remarque : l'Assistance Tenable ne vous aide pas à résoudre les problèmes liés à votre système d'exploitation hôte, même si vous les rencontrez lors de l'installation ou du déploiement.

Environnement		Format de fichier Tenable Core	Plus d'informations
Machine virtuelle	VMware	Fichier `.ova`	Déployer Tenable Core dans VMware
	Microsoft Hyper-V	fichier`.zip`	
Matériel Matériel fourni par Tenable		Image `.iso`	Installer Tenable Core sur du matériel

Remarque : bien que vous puissiez utiliser les paquets pour exécuter Tenable Core dans d'autres environnements, Tenable ne fournit pas de documentation pour ces procédures.

Configuration matérielle requise pour OT Security

Pour plus d'informations sur la configuration matérielle spécifique à OT Security ou Capteur OT Security, voir Spécifications matérielles Tenable OT Security dans le guide *General Requirements* (Exigences générales).

Configuration du matériel virtuel OT Security

Les réseaux d'entreprise peuvent varier en termes de performances, de capacité, de protocoles et d'activité globale. Les exigences en ressources à prendre en compte pour les déploiements incluent la vitesse brute du réseau, la taille du réseau à surveiller et la configuration de l'application.

Le tableau suivant décrit les directives de base pour le fonctionnement de Tenable Core + OT Security dans un environnement virtuel.

Tenable Core + OT Security nécessite des processeurs avec AVX et AVX2 (par exemple, Intel Haswell ou plus récent).

Scénario d'installation	Cœurs de processeur	Mémoire	Espace disque
Machine virtuelle	8 cœurs	16 Go de RAM	200 Go

Conditions de stockage requises

Tenable recommande d'installer OT Security sur des appareils de stockage en attachement direct (DAS), de préférence des lecteurs à l'état solide (SSD), pour de meilleures performances. Tenable encourage fortement l'utilisation d'un stockage à l'état solide (SSS) doté d'un taux élevé d'écritures sur disque par jour (DWPD) afin d'assurer la longévité.

Tenable ne prend pas en charge l'installation de OT Security sur des appareils de stockage attachés au réseau (NAS). Les réseaux de zones de stockage (SAN) avec une latence de stockage de 10 millisecondes ou moins, ou les appliances matérielles Tenable, sont une bonne alternative dans de tels cas.

Espace disque requis

Les réseaux d'entreprise peuvent varier en termes de performances, de capacité, de protocoles et d'activité globale. Les exigences en ressources à prendre en compte pour les déploiements incluent la vitesse brute du réseau, la taille du réseau à surveiller et la configuration de l'application. La sélection des processeurs, de la mémoire et de la carte réseau dépend fortement de ces configurations de déploiement. L'espace disque requis varie en fonction de l'utilisation, de la quantité de données et de la durée pendant laquelle vous stockez des données sur le système.

OT Security doit effectuer des captures de paquets complets du trafic surveillé, et le volume des données d'événements liés aux politiques stockées par OT Security dépend du nombre d'appareils et du type d'environnement.

Vous pouvez calculer les besoins de stockage par jour (Go/jour) en multipliant le taux de trafic (Mbit/s) par 2,7, en tenant compte d'un facteur de compression de 0,25.

Dans un exemple avec deux capteurs recevant du trafic SPAN à 23 Mbit/s chacun, les besoins de stockage par jour (Go/jour) sont calculés comme suit : (23*2)*2,7=124 Go d'espace par jour pour le stockage du trafic.

Remarque : si les exigences en matière de conformité ou de sécurité nécessitent que vous stockiez jusqu'à 30 jours de trafic, vous avez besoin d'un lecteur de stockage PCAP (capture de paquets) de 3,75 To pour répondre à cette exigence. Une fois que les données de trafic stockées ont atteint la taille maximale, OT Security écrase les données PCAP les plus anciennes et les remplace par le nouveau trafic.

Directives sur les exigences système de l'ICP

Débit SPAN/TAP maximal (Mbit/s)	Cœurs de processeur[1]	Mémoire (DDR4)	Conditions de stockage requises	Interfaces réseau
50 Mbit/s ou moins	4	16 Go de RAM	128 GB	Minimum 4 x 1 Gbit/s
50–150 Mbit/s	16	32 Go de RAM	512 GB	Minimum 4 x 1 Gbit/s
150–300 Mbit/s	32	64 Go de RAM	1 To	Minimum 4 x 1 Gbit/s
300 Mbit/s à 1 Go	32-64	128 Go de RAM ou plus	2 To ou plus	Minimum 4 x 1 Gbit/s

Configuration requise pour les partitions de disque

OT Security utilise les partitions montées suivantes :

Partition	Contenu
/	système d'exploitation
/opt	fichiers d'application et de base de données

/var/pcap	captures de paquets (capture de paquet complet, événement, requête)

Le processus d'installation standard place ces partitions sur le même disque. Tenable recommande de les déplacer vers des partitions sur des disques distincts pour augmenter le débit. OT Security est une application gourmande en espace disque et l'utilisation de disques à vitesses de lecture/d'écriture élevées, tels que les disques SSD, permet d'obtenir les meilleures performances. Tenable recommande d'utiliser un SSD avec des taux DWPD élevés sur les installations matérielles fournies par le client lors de l'utilisation de la fonction de capture de paquet dans OT Security.

Conseil : le déploiement de OT Security sur une plateforme matérielle configurée avec un tableau redondant de disques indépendants (RAID 0) peut considérablement améliorer les performances.

Conseil : Tenable ne reqiuert pas de disques RAID, même pour nos plus gros clients. Cependant, dans un cas, les temps de réponse aux requêtes avec un disque RAID plus rapide, chez un client ayant plus d'un million de vulnérabilités gérées, sont passés de quelques secondes à moins d'une seconde.

Configuration requise de l'interface réseau

Il doit y avoir au moins deux interfaces réseau présentes sur votre appareil avant d'installer OT Security. Tenable recommande l'utilisation d'interfaces en gigabits. L'OVA VMware crée ces interfaces automatiquement. Créez ces interfaces manuellement lorsque vous installez l'ISO (telle que Hyper-V).

Remarque : Tenable ne fournit pas de prise en charge SR-IOV pour l'utilisation de cartes réseau 10 G et ne garantit pas les vitesses 10 G avec des cartes réseau 10 G.

Configuration requise pour les NIC

- OT Security ne nécessite qu'un seul NIC pour EM.
- OT Security nécessite un minimum de deux NIC pour l'ICP et les capteurs.
- OT Security nécessite l'utilisation d'adresses IP statiques pour l'ICP/EM/les capteurs.
- Le capteur et l'ICP peuvent être configurés pour surveiller plusieurs interfaces SPAN.

Remarque : à partir de OT Security 4.1, les noms de profils pour les interfaces réseau sont les suivants :

- nic0 —Port système 1
- nic1—Port système 2
- nic2 —Port système 3
- nic3 —Port système 4

nic0 ou **Port système 1** (192.168.1.5) et **nic3** ou **Port système 4** (192.168.3.3) ont des adresses IP statiques lorsque vous installez Tenable Core + OT Security dans un environnement matériel ou virtuel. Les autres contrôleurs d'interface réseau (NIC) utilisent le protocole DHCP.

nic3 ou **Port système 4** (192.168.3.3) a une adresse IP statique lorsque vous déployez Tenable Core + OT Security sur VMware. Les autres NIC utilisent le protocole DHCP. Confirmez que l'adresse MAC de **nic1** ou **Port système 2** dans Tenable Core + OT Security correspond à l'adresse MAC NIC dans votre configuration de scan passif VMware. Modifiez votre configuration VMware pour qu'elle corresponde à votre adresse MAC Tenable Core si nécessaire.

Pour plus d'informations, voir Manually Configure a Static IP Address (Configurer manuellement une adresse IP statique), Manage System Networking (Gérer le trafic réseau du système) et la *documentation VMware*.

[1]Les cœurs de processeur font référence aux cœurs PHYSIQUES, ce qui suppose un processeur de classe serveur (Xeon, Opteron).

Exigences d'accès

Votre déploiement doit répondre aux exigences suivantes.

- Configuration Internet requise
- Configuration de ports requise

Configuration Internet requise

Vous devez avoir accès à Internet pour télécharger les fichiers Tenable Core et effectuer des installations en ligne.

Après avoir transféré un fichier sur votre ordinateur, les exigences d'accès à Internet pour déployer ou mettre à jour Tenable Core varient en fonction de votre environnement.

Remarque : vous devez accéder à `appliance.cloud.tenable.com` pour effectuer des installations à partir des ISO en ligne (et pour obtenir des mises à jour en ligne) et à `capteur.cloud.tenable.com` pour récupérer des tâches de scan.

Environnement		Format Tenable Core	Configuration Internet requise
Machine virtuelle	VMware	Fichier `.ova`	Aucun accès Internet n'est requis pour déployer ou mettre à jour Tenable Core.
Matériel		Image `.iso`	Nécessite un accès Internet pour installer ou mettre à jour Tenable Core.

Conseil : vous n'avez pas besoin d'accéder à Internet lorsque vous installez des mises à jour via un fichier `.iso` hors ligne. Pour plus d'informations, voir Update Tenable Core Offline (Mettre à jour Tenable Core hors ligne).

Configuration de ports requise

Votre déploiement Tenable Core nécessite l'accès à des ports spécifiques pour le trafic entrant et sortant. Tenable Security Center nécessite également un accès à certains ports spécifiques à l'application. Pour plus d'informations, voir Port Requirements (Configuration des ports requise) dans le (missing or bad snippet).OT Security nécessite également un accès à certains ports spécifiques à l'application. Pour plus d'informations, voir Considérations sur le pare-feu.

Trafic entrant

Autoriser le trafic entrant vers les ports suivants :

Remarque : le trafic entrant fait référence au trafic provenant des utilisateurs qui configurent Tenable Core.

Port	Trafic
TCP 22	Connexions SSH entrantes.

TCP 443	Communications entrantes vers l'interface OT Security.
TCP 8000	Communications HTTPS entrantes vers l'interface Tenable Core.

Trafic sortant

Autoriser le trafic sortant vers les ports suivants :

Port	Trafic
TCP 22	Connexions SSH sortantes, y compris les connexions de stockage à distance.
TCP 443	Communications sortantes vers les serveurs `appliance.cloud.tenable.com` et `sensor.cloud.tenable.com` pour les mises à jour système.
UDP 53	Communications DNS sortantes pour OT Security et Tenable Core.

Considérations sur le réseau

L'appliance OT Security (à la fois physique et virtuelle) doit atteindre les interfaces réseau suivantes :

Interface de gestion et des requêtes actives

- Une interface configurée avec une adresse IP qui autorise l'accès au réseau pour gérer et configurer l'appliance,
- Permet à l'appliance d'atteindre les assets du réseau pour les requêtes actives (recommandé, mais facultatif),
- Vous permet de partager deux interfaces réseau distinctes. Voir Connecter le port de gestion séparé (pour l'option Séparation des ports).

Interface de surveillance

- Surveille et collecte passivement le trafic à des fins d'analyse.
- Doit être connecté à l'interface cible de mise en miroir, d'analyseur de port commuté (SPAN) ou d'analyseur de port commuté à distance (RSPAN) d'un commutateur.

- (Facultatif) Utilise des capteurs et la configuration d'analyseur de ports encapsulé à distance (ERSPAN) pour surveiller le trafic qui ne peut pas être mis en miroir directement dans l'interface de l'appliance.

Considérations sur le pare-feu

Lors de la configuration de votre système OT Security, il est important de planifier les ports ouverts pour que le système Tenable puisse fonctionner correctement. Les tableaux suivants indiquent les ports à réserver à l'usage de l'ICP OT Security et des capteurs OT Security, ainsi que les ports requis pour exécuter des requêtes actives et pour l'intégration avec Tenable Vulnerability Management et Tenable Security Center.

Remarque : pour plus d'informations sur la liste des sites et domaines Tenable que vous devez autoriser à franchir le pare-feu, voir l'article de la base de connaissances.

Plateforme OT Security Core

Les ports suivants doivent rester ouverts pour assurer la communication avec la plateforme OT Security Core.

Sens du flux	Port	Communique avec	Usage
Entrant	TCP 443 et TCP 28304	Capteur OT	Authentification, appairage et réception des informations du capteur.
Sortant	TCP 443 et TCP 28305	OT Security EM	Appairage de l'ICP et d'EM
Entrant	TCP 8000	Interface web pour Tenable Core	Accès par navigateur à Tenable Core
Entrant	TCP 28304	ICP/OT Security	Communication du capteur
Entrant	TCP 22	Appliance pour l'accès SSH	Accès par ligne de commande au système d'exploitation ou à l'appliance

Sortant	TCP 443	Tenable Security Center	Envoie les données pour intégration
Sortant*	TCP 443	cloud.tenable.com	Envoie les données pour intégration
Sortant*	Divers protocoles industriels	PLC/contrôleurs	Requête active
Sortant*	TCP 25 ou 587	Serveur de messagerie pour les alertes	SMTP (e-mails d'alerte, rapports)
Sortant*	UDP 514	Serveur Syslog	Envoie des alertes d'événements de politique et des messages syslog
Sortant*	UDP 53	Serveur DNS	Résolution de nom
Sortant*	UDP 123	Serveur NTP	Service de temps
Sortant*	TCP 389 ou 636	Serveur AD	Authentification AD LDAP
Sortant*	TCP 443	Fournisseur SAML	Authentification unique
Sortant*	UDP 161	Serveur SNMP	Surveillance SNMP vers Tenable Core
Sortant*	TCP 443	*.tenable.com *.nessus.org	Mises à jour automatiques des plug-ins, des applications et du système d'exploitation**
Sortant	TCP 10146 (port sécurisé)	Connecteur IoT	Connecte l'ICP à l'IoT Connector Agent

*Services optionnels

**Procédure hors ligne disponible

Capteurs OT Security

Les ports suivants doivent rester ouverts pour la communication avec les capteurs OT Security.

Sens du flux	Port	Communique avec	Usage
Entrant	TCP 8000	Interface web	Accès du navigateur à l'IGU
Entrant	TCP 22	Appliance pour l'accès SSH	Accès par ligne de commande au système d'exploitation ou à l'appliance
Sortant*	TCP 25	Serveur de messagerie pour les alertes	SMTP (e-mails d'alerte, rapports)
Sortant*	UDP 53	Serveur DNS	Résolution de nom
Sortant*	UDP 123	Serveur NTP	Service de temps
Sortant*	UDP 161	Serveur SNMP	Surveillance SNMP vers Tenable Core
Sortant	TCP 28303	ICP/OT Security Envoie la communication du capteur, reçoit sur ICP/OT Security	Non authentifié / Connexion à un capteur passif uniquement
Sortant	TCP 443 et TCP 28304	ICP/OT Security Envoie la communication du capteur, reçoit sur ICP/OT Security	Authentifié / Tunnel sécurisé entre le capteur et l'ICP

*Services optionnels

Requête active

Les ports suivants doivent rester ouverts pour permettre l'utilisation des requêtes actives.

Sens du flux	Port	Communique avec	Usage
Sortant	TCP 80	Appareils OT	Empreinte digitale HTTP
Sortant	TCP 102	Appareils OT	Protocole S7/S7+
Sortant	TCP 443	Appareils OT	Empreinte digitale HTTPS
Sortant	TCP 445	Appareils OT	Requêtes WMI
Sortant	TCP 502	Appareils OT	Protocole Modbus
Sortant	TCP 5432	Appareils OT	Requêtes PostgreSQL
Sortant	UDP/TCP 44818	Appareils OT	Protocole CIP
Sortant	TCP/UDP 53	Appareils OT	DNS
Sortant	ICMP	Appareils OT	Découverte des assets
Sortant	UDP 161	Appareils OT	Requêtes SNMP
Sortant	UDP 137	Appareils OT	Requêtes NBNS
Sortant	UDP 138	Appareils OT	Requêtes NetBIOS

Remarque : les ports utilisés par les appareils varient selon le fournisseur et la ligne de produits. Pour obtenir une liste des ports et protocoles pertinents nécessaires pour garantir le succès des requêtes actives, voir Requête d'identification et de détails.

Intégrations OT Security

Les ports suivants doivent rester ouverts pour communiquer avec les intégrations Tenable Vulnerability Management et Tenable Security Center.

Sens du flux	Port	Communique avec	Usage
Sortant	TCP 443	cloud.tenable.com	Intégration Tenable Vulnerability Management
Sortant	TCP 443	Tenable Security Center	Intégration de Tenable Security Center

Requête d'identification et de détails

Vous pouvez utiliser les ports suivants pour les requêtes d'identification et de détails :

Remarque : vous devrez peut-être ouvrir les ports pour OT Security ou ses capteurs sur le pare-feu afin d'atteindre le port pertinent pour vos assets.

Port	Nom du port
21	FTP
80	HTTP
102	Step-7/S7+
111	Emerson OVATION
135	WMI
161	SNMP
443	HTTPS
502	MODBUS/MMS
1911	Niagara FOX
2001	Profibus
2222	PCCC_AB-ETH
2404	CEI 60870-5
3500	Bachmann
4000	Emerson ROC
4911	Niagara FOX TLS
5002	Mitsubishi MELSEC
5007	Mitsubishi MELSEC
5432	PSQL/SEL

18245	SRTP
20000	DNP3
20256	PCOM
44818	EthernetIP/CIP
47808	BACNET (udp)
48898	ADS
55553	Honeywell CEE
55565	Honeywell FTE

Installer l'ICP OT Security

Objectif : installer l'ICP OT Security et la préparer à l'utilisation.

Avant de commencer

- Voir Conditions préalables.

Suivez ces étapes selon les besoins pour installer et connecter l'ICP OT Security au réseau :

- Installer une appliance matérielle ICP OT Security

  Remarque : le matériel Tenable Core fourni par Tenable est livré avec Tenable Core + OT Security pré-installé. Si vous installez une appliance antérieure ou ancienne, vous pouvez opter pour une nouvelle installation. Pour plus d'informations, voir Nouvelle installation Tenable Core + Tenable OT Security sur le matériel fourni par Tenable.

- Installer une appliance virtuelle ICP OT Security

Étape suivante

- Connecter OT Security au réseau

Installer une appliance matérielle ICP OT Security

Vous pouvez monter l'appliance OT Security sur un rack, ou simplement la placer sur une surface plane, comme un bureau.

Conseil : Tenable vous recommande d'effectuer la configuration de base décrite dans Configurer Tenable Core et Assistant de configuration OT Security à votre bureau, avant de déplacer l'appliance vers un rack ou tout autre emplacement distant.

Montage en rack

Pour monter l'appliance OT Security sur un rack standard de 19 pouces :

1. Insérez l'unité serveur dans un emplacement 1U disponible du rack.

   Remarque :

   - Assurez-vous que le rack est électriquement relié à la terre.
   - Assurez-vous que l'entrée d'air du ventilateur de refroidissement (situé sur le panneau arrière) et les orifices de ventilation (sur le panneau supérieur) ne sont pas obstrués.

2. Installez l'unité en fixant les supports de montage en rack (fournis) au cadre du rack, à l'aide des vis adéquates (non fournies).
3. Branchez le câble d'alimentation CA fourni sur le port d'alimentation du panneau arrière, puis branchez le câble sur l'alimentation CA (secteur).

Surface plane

Pour installer l'appliance OT Security sur une surface plane :

1. Placez l'appliance sur une surface sèche et plane (un bureau, par exemple).

   Remarque :

   - Assurez-vous que le plan de travail est plat et sec.
   - Vérifiez que l'entrée d'air du ventilateur de refroidissement (situé sur le panneau arrière) et que les orifices de ventilation (sur le panneau supérieur) ne sont pas obstrués.
   - Si vous placez une unité dans la pile d'autres appliances électriques, assurez-vous qu'il y a suffisamment d'espace derrière le ventilateur de refroidissement (situé sur le panneau arrière) pour permettre une ventilation et un refroidissement appropriés.

2. Branchez le câble d'alimentation CA fourni sur le port d'alimentation du panneau arrière, puis branchez le câble sur l'alimentation CA (secteur).

Pour plus d'informations sur la connectivité, voir Considérations sur le réseau.

Que faire ensuite

Connecter OT Security au réseau

Nouvelle installation Tenable Core + Tenable OT Security sur le matériel fourni par Tenable

Tenable Core + OT Security sont pré-installés et prêts à l'emploi sur le matériel officiel fourni par Tenable. Dans certains cas, une nouvelle installation (également appelée ré-actualisation) est recommandée.

Remarque : si vous avez récemment reçu une nouvelle appliance, vous pouvez ignorer cette procédure.

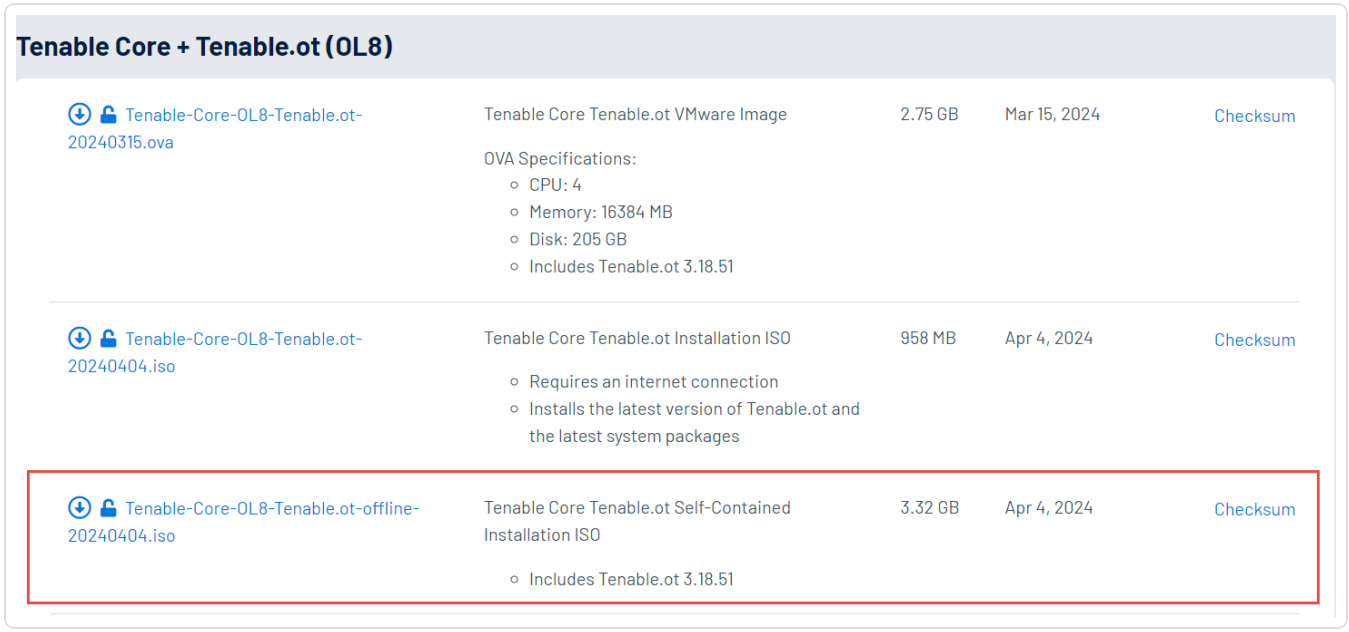
Avant de commencer

Vous devez disposer de ce qui suit :

- Une application pour formater et créer des clés USB démarrables, telle que Rufus.
- Un câble série.
- Une application de terminal série, telle que PuTTY.
- Un lecteur USB d'environ 8 Go ou plus.

Pour installer le fichier ISO Tenable Core + OT Security :

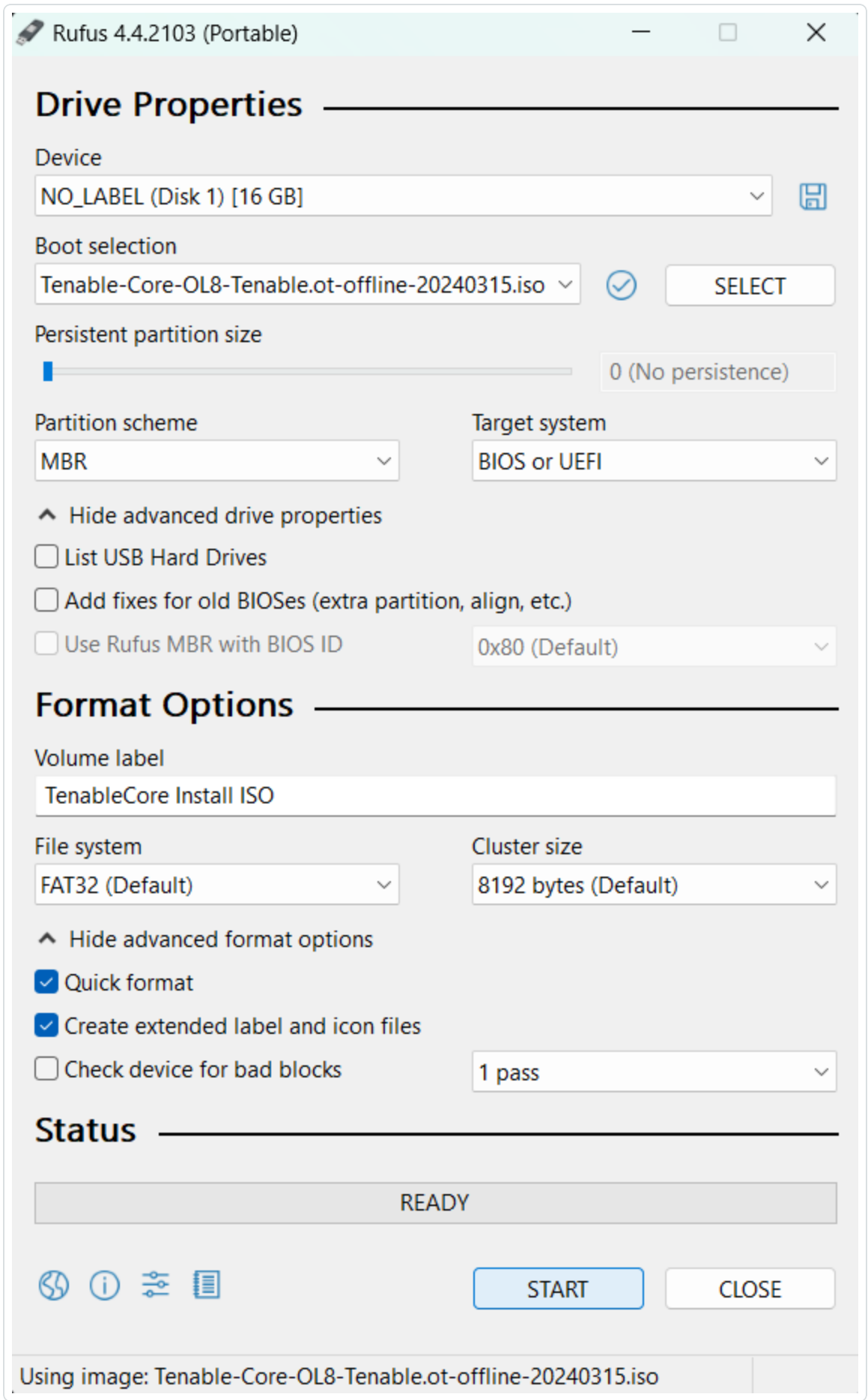
1. Téléchargez le dernier fichier ISO hors ligne à partir des [téléchargements Tenable](#).

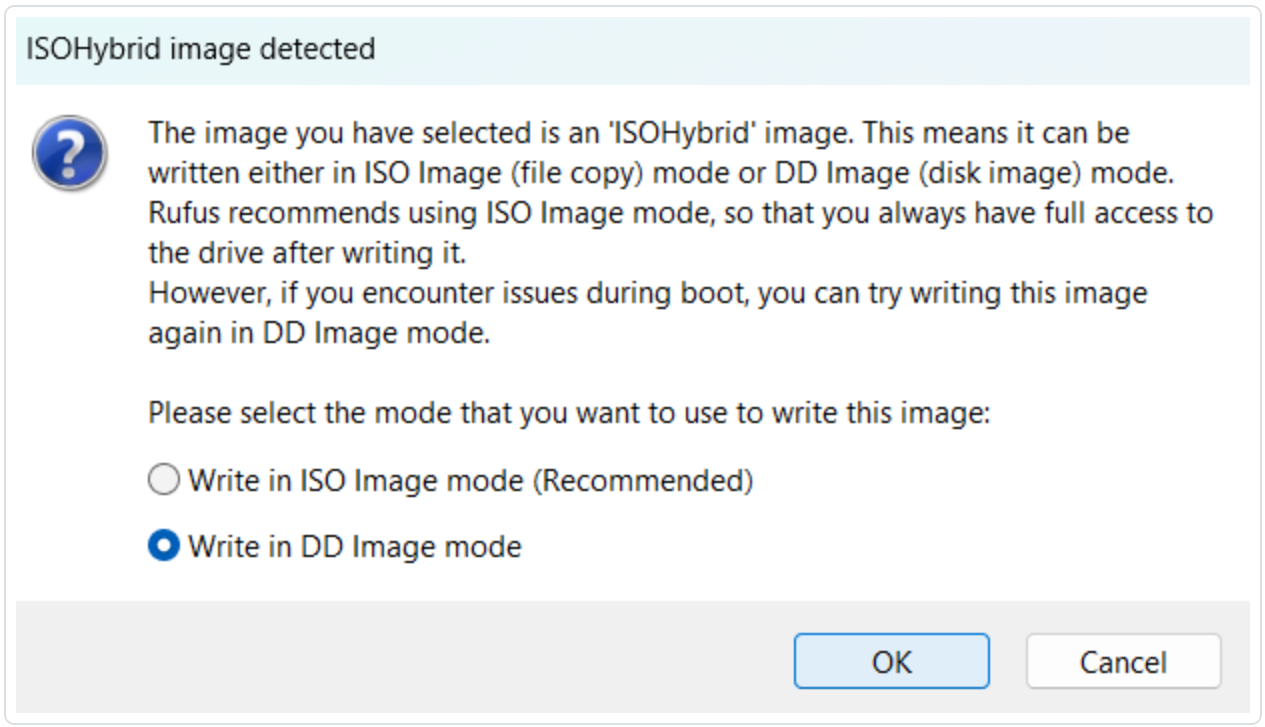


Tenable Core + Tenable.ot (OL8)

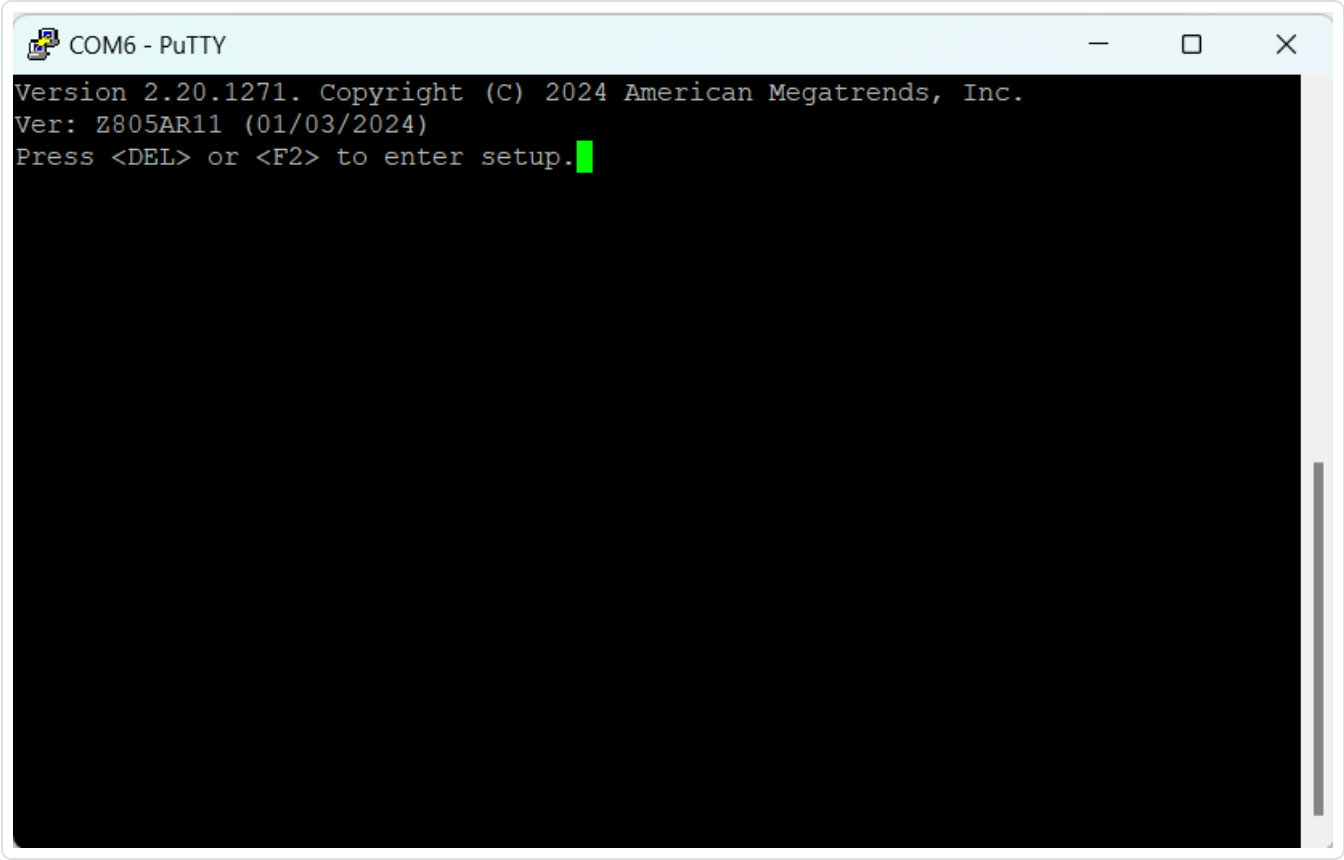
Tenable-Core-OL8-Tenable.ot-20240315.ova	Tenable Core Tenable.ot VMware Image OVA Specifications: ○ CPU: 4 ○ Memory: 16384 MB ○ Disk: 205 GB ○ Includes Tenable.ot 3.18.51	2.75 GB	Mar 15, 2024	Checksum
Tenable-Core-OL8-Tenable.ot-20240404.iso	Tenable Core Tenable.ot Installation ISO ○ Requires an internet connection ○ 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 ○ Includes Tenable.ot 3.18.51	3.32 GB	Apr 4, 2024	Checksum

2. Branchez le lecteur USB sur un PC et flashez l'ISO sur le lecteur flash en mode DD.

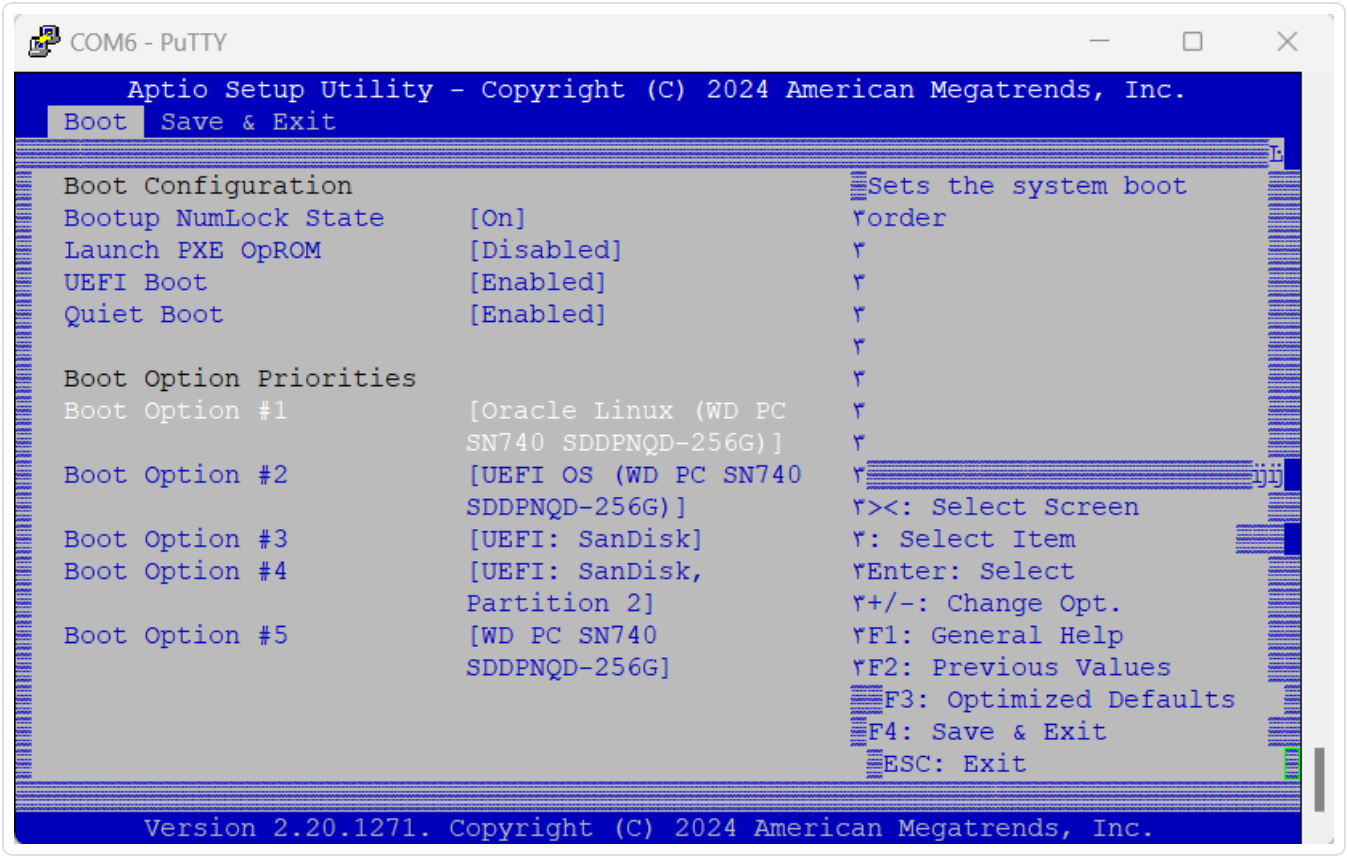

Rufus 4.4.2103 (Portable)
Drive Properties
Device
NO_LABEL (Disk 1) [16 GB]
Boot selection
Tenable-Core-OL8-Tenable.ot-offline-20240315.iso
SELECT
Persistent partition size
0 (No persistence)
Partition scheme
MBR
Target system
BIOS or UEFI
Hide advanced drive properties
List USB Hard Drives
Add fixes 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. Une fois terminé, connectez le lecteur USB à un port USB de l'appliance OT Security.
4. Connectez-vous à l'appliance via l'interface série de la console (débit en bauds de 115 200 bits/s avec une configuration 8N1) et mettez-la sous tension.

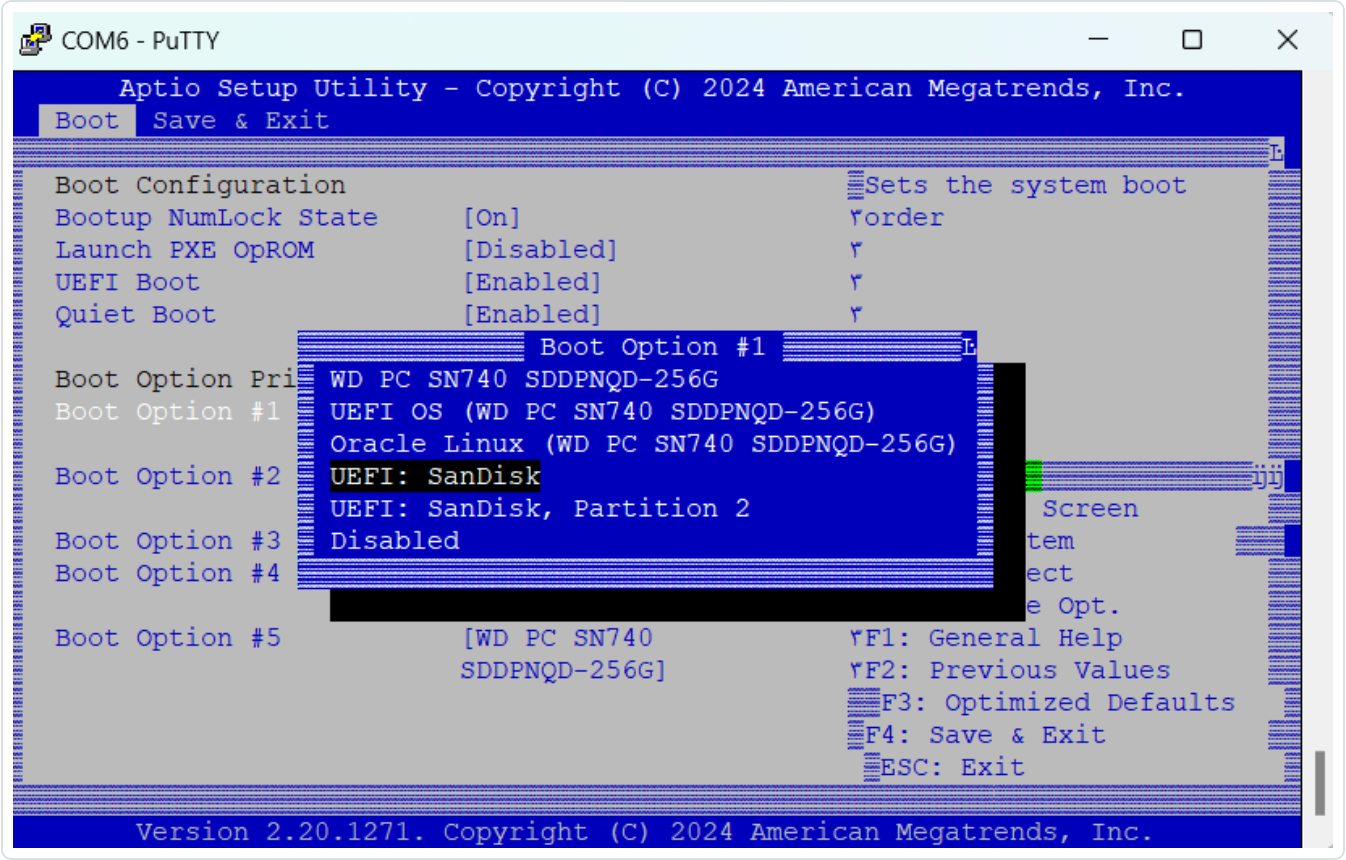


5. Lorsque vous y êtes invité, appuyez sur <DEL> pour accéder à la configuration.
6. Dans la configuration du système, utilisez les touches de direction pour accéder à la section **Boot** (Démarrage).



7. Sélectionnez **Boot Option #1** (Option de démarrage 1) et modifiez-la sur votre lecteur USB.

> **Remarque** : utilisez l'option Unified Extensible Firmware Interface (UEFI).

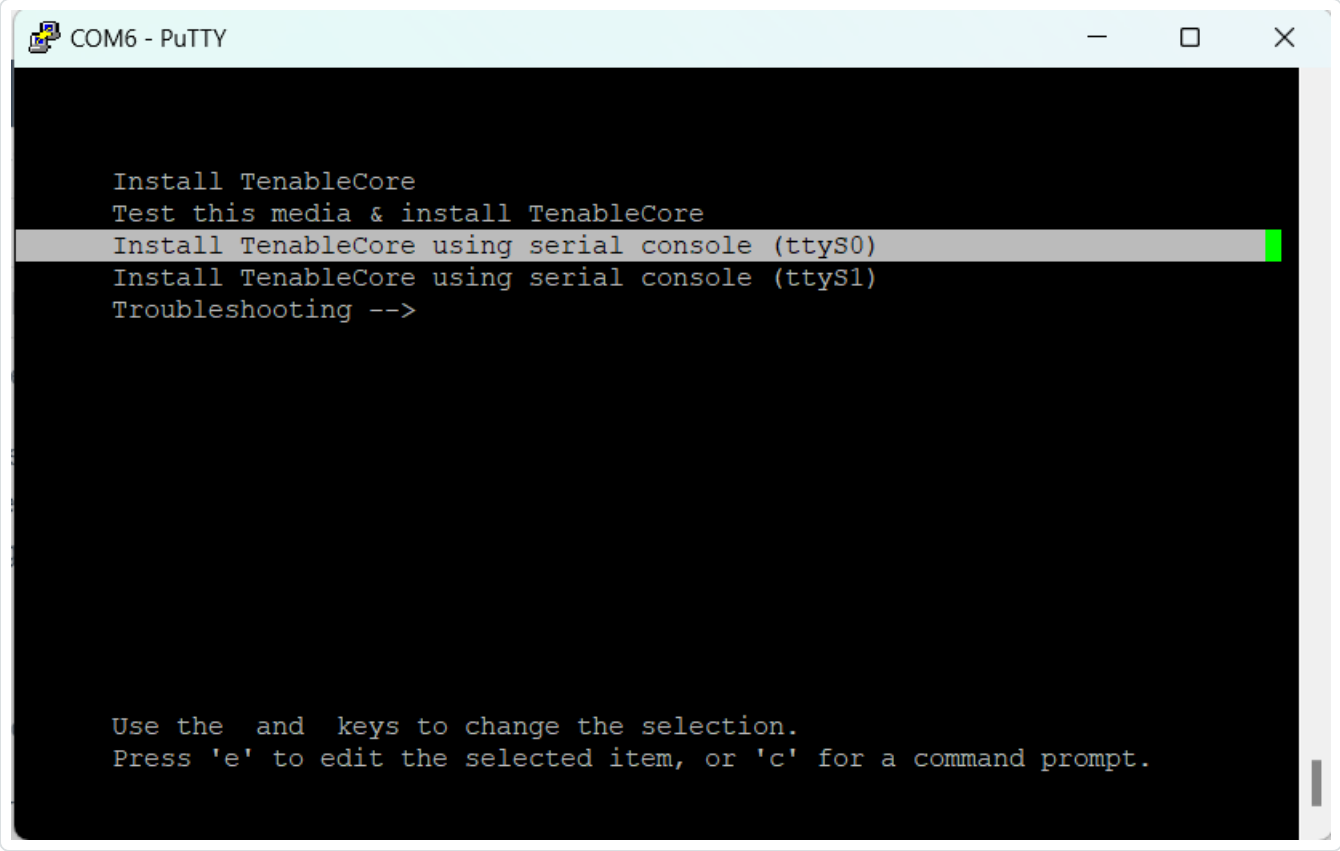


Remarque : vous pouvez utiliser l'option « One-shot boot » (Démarrage ponctuel) sur les appliances qui prennent en charge cette fonctionnalité.

8. Dans la section **Save & Exit** (Enregistrer et quitter), sélectionnez **Save Changes and Reset** (Enregistrer les modifications et réinitialiser).

9. Après le redémarrage de l'appliance et lorsque vous y êtes invité, sélectionnez **Install TenableCore using serial console (ttyS0)** (Installer TenableCore à l'aide de la console série [ttyS0]). De cette façon, le résultat de l'installation est envoyé à la connexion de console série de l'appliance.

   Remarque : si votre matériel prend en charge une sortie moniteur (VGA, HDMI, etc.), vous pouvez sélectionner l'option **Install TenableCore** (Installer TenableCore). Dans ce cas, la sortie de l'installation apparaît sur votre moniteur connecté.



Laissez l'appliance terminer l'installation. Le système peut redémarrer plusieurs fois. L'installation est terminée lorsqu'une invite de connexion apparaît. Le système peut s'arrêter une fois l'installation terminée, selon la conception sur certaines appliances.

> **Remarque** : le système peut effectuer quelques procédures d'installation même après l'apparition de l'invite de connexion. Tenable vous recommande d'attendre quelques minutes avant de démarrer l'assistant de configuration Tenable Core.

10. Déconnectez le lecteur USB uniquement une fois l'installation terminée.

Que faire ensuite

Connecter OT Security au réseau

Installer une appliance virtuelle ICP OT Security

Pour déployer Tenable Core + OT Security en tant que machine virtuelle VMware, vous devez télécharger le fichier `.ova` de Tenable Core + OT Security et le déployer sur un hyperviseur.

Remarque : si vous déployez le fichier `.iso` au lieu du fichier `.ova` pré-configuré :

- Suivez les exigences système pour Tenable Core + OT Security.
- Lorsque vous êtes invité à choisir une méthode de configuration, sélectionnez **Installer Tenable Core**. Voir Nouvelle installation de Tenable Core + Tenable OT Security.
- Suivez et surveillez le processus d'installation à l'aide de l'interface utilisateur d'installation, via la console de la machine virtuelle. Le processus d'installation est entièrement automatisé, donc n'interagissez pas avec le système tant que l'installation n'est pas terminée.

Avant de commencer :

- Confirmez que votre environnement prend en charge votre utilisation prévue de l'instance, comme décrit dans Exigences système.
- Confirmez que votre accès à Internet et aux ports prend en charge l'utilisation que vous prévoyez de faire de l'instance, comme décrit dans Exigences d'accès.

Pour déployer Tenable Core + OT Security en tant que machine virtuelle :

1. Téléchargez le fichier `.ova` de Tenable Core + OT Security depuis la page des téléchargements de Tenable.
2. Ouvrez votre machine virtuelle VMware dans l'hyperviseur.
3. Importez le fichier `.ova` VMware de Tenable Core + OT Security depuis votre ordinateur vers votre machine virtuelle.
   Pour plus d'informations sur la configuration de vos machines virtuelles VMware, voir la documentation VMware.
4. Dans l'invite de configuration, configurez la machine virtuelle pour répondre aux besoins et aux exigences de stockage de votre organisation, et à ceux décrits dans OT SecurityExigences système.
5. Lancez votre instance Tenable Core + OT Security.

   Le processus de démarrage de la machine virtuelle apparaît dans une fenêtre de terminal. Le processus de démarrage peut prendre plusieurs minutes.

> **Remarque** : le système peut effectuer quelques procédures d'installation finales même après l'apparition de l'invite de connexion.Tenable vous recommande d'attendre quelques minutes avant de démarrer l'assistant de configuration Tenable Core.

> **Conseil** : si vous souhaitez augmenter votre espace disque pour répondre aux besoins de stockage de données de votre organisation, consultez Gestion des disques.

Que faire ensuite

Connecter OT Security au réseau

Connecter OT Security au réseau

Vous pouvez utiliser OT Security à la fois pour les fonctions Requête active et Surveillance réseau. Pour plus d'informations, voir Considérations sur le réseau.

- **Surveillance réseau** —Connectez l'unité à un port de mise en miroir sur le commutateur réseau connecté aux contrôleurs/ PLC pertinents.
- **Requête active** —Connectez l'unité à un port standard possédant une adresse IP sur le commutateur réseau connecté aux contrôleurs/ PLC pertinents.

Dans la configuration par défaut, la requête active et la console de gestion utilisent le même port sur l'unité (port 1). Cependant, après la configuration initiale, vous pouvez séparer le port de gestion du port de requête active en configurant la gestion sur le port 3. Après cette configuration, vous pouvez connecter le port 3 de l'unité à un port standard du commutateur pour assurer la gestion comme décrit dans Connecter le port de gestion séparé (séparation des ports).

Pour la configuration initiale, connectez le port 1à un port standard du commutateur réseau et le port 2 à un port de mise en miroir.

Pour connecter l'appliance OT Security au réseau :

Sur une appliance matérielle :

1. Sur l'appliance OT Security, connectez le câble Ethernet (fourni) au port 1.
2. Connectez le câble à un port standard du commutateur réseau.
3. Sur l'unité, connectez un autre câble Ethernet (fourni) au port 2.

4. Connectez le câble à un port de mise en miroir du commutateur réseau.

Sur une appliance virtuelle :

Si vous avez déployé l'appliance à l'aide du fichier `.ova`, l'appliance est pré-configurée avec quatre interfaces réseau.

Si vous avez déployé une appliance virtuelle personnalisée à l'aide du fichier `.iso` ou `.zip` (Hyper-V), assurez-vous de configurer la machine virtuelle selon les exigences décrites dans Exigences système. Pour plus d'informations sur la configuration de la mise en réseau sur les machines virtuelles, voir la documentation VMware ou la documentation Hyper-V.

Configurer l'ICP OT Security

Objectif : préparer le logiciel pour l'activation.

Après avoir installé l'ICP OT Security, vous pouvez configurer votre OT Security. Procédez comme suit :

1. Configurer Tenable Core —Terminez la configuration initiale de Tenable Core via la CLI ou l'interface utilisateur.
2. Installer OT Security sur Tenable Core —Terminez votre installation de OT Security sur Tenable Core.
3. Configurer les paramètres OT Security à l'aide de l'assistant de configuration —Configurez les paramètres de base de votre ICP OT Security à l'aide de l'assistant de configuration.

Configurer Tenable Core

Vous pouvez effectuer la configuration initiale de Tenable Core à partir de la CLI et de l'interface utilisateur Tenable Core.

L'utilisation de l'interface utilisateur Tenable Core est obligatoire pour terminer la configuration des déploiements d'appliances virtuelles.

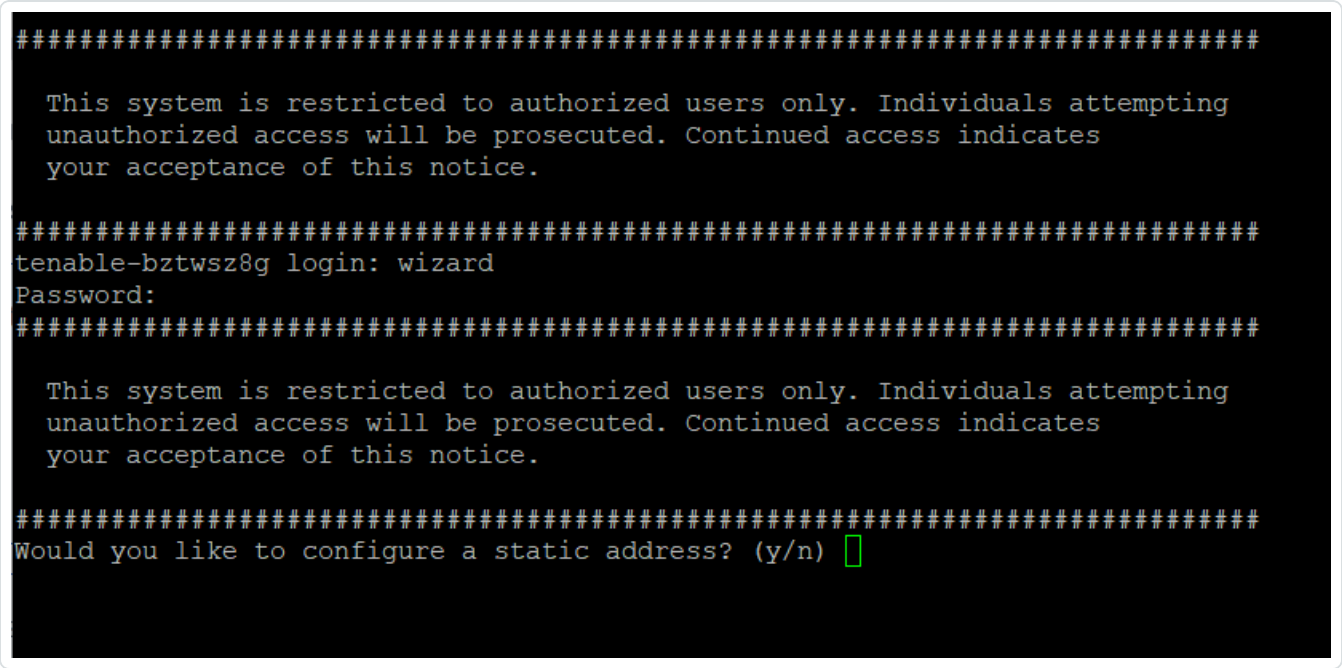
Remarque : si vous ne terminez pas l'assistant de configuration en 30 minutes environ, redémarrez l'appliance.

Configuration initiale via la CLI (facultatif)

Pour configurer Tenable Core à l'aide de la CLI :

1. Connectez-vous à l'appliance OT Security à l'aide de la console série comme décrit dans Nouvelle installation de Tenable Core + OT Security.
2. Connectez-vous avec le nom d'utilisateur `wizard` et le mot de passe `admin`.

   L'interface du terminal **Network Manager** (Gestionnaire réseau) apparaît.



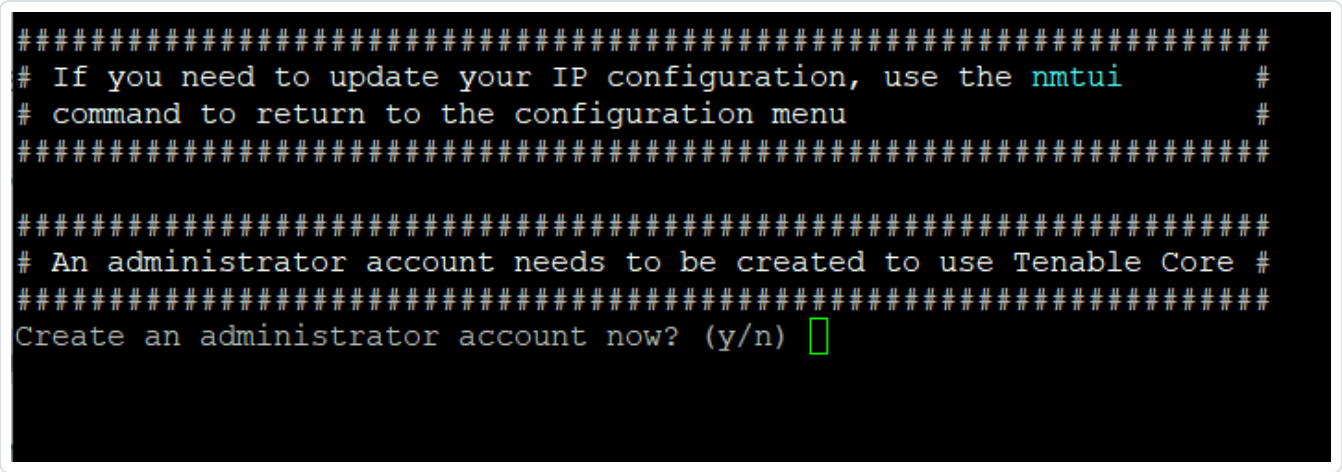
3. (Facultatif) Pour configurer l'adresse IP de gestion, saisissez **y** (oui).
4. Appuyez sur **Entrée**.flèche du

   La fenêtre **Edit Connection** (Modifier la connexion) apparaît.
5. Naviguez à l'aide des touches de direction et configurez votre adresse IP, votre passerelle par défaut, vos serveurs DNS, etc. Vous pourrez modifier cette configuration ultérieurement.
6. À l'aide de la flèche vers le bas, accédez au bas de l'écran et sélectionnez **<OK>**.

   La fenêtre **Network Manager** (Gestionnaire réseau) apparaît.
7. Sélectionnez **<Quit>** (Quitter).

> **Remarque** : par défaut, `nic0` ou le Port système 1est pré-configuré avec l'adresse IP 192.168.1.5/24. Vous pouvez utiliser cette adresse IP pour terminer la configuration du système à l'aide de l'interface Tenable Core (port 8000) à partir de n'importe quel PC accessible depuis le réseau IP.

8. Tapez **y** (oui) et suivez les invites pour créer un compte administrateur. Utilisez ce compte uniquement pour vous connecter à Tenable Core (console de terminal, SSH et interface utilisateur Tenable Core). Utilisez des comptes distincts pour l'application OT Security.



9. Après avoir créé le compte, utilisez-le pour vous connecter au terminal via la console ou à l'aide d'une connexion réseau : via SSH ou l'interface Tenable Core (https://<mgmt-IP>:8000).

Configuration initiale via l'interface utilisateur Tenable Core

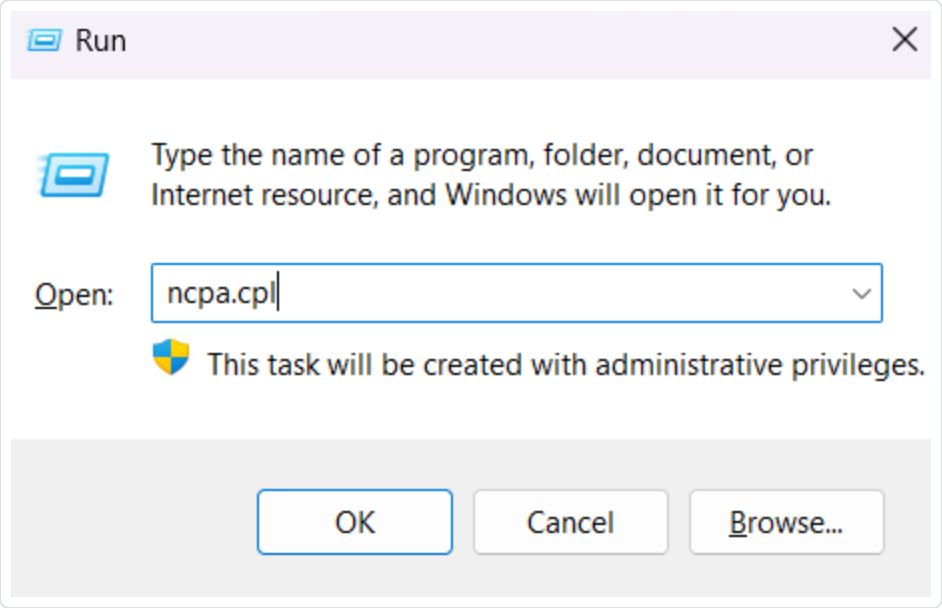
Pour terminer la configuration initiale via l'interface utilisateur Tenable Core (disponible sur https://<mgmt-IP>:8000), vous avez besoin d'une connexion réseau fonctionnelle à l'appliance.

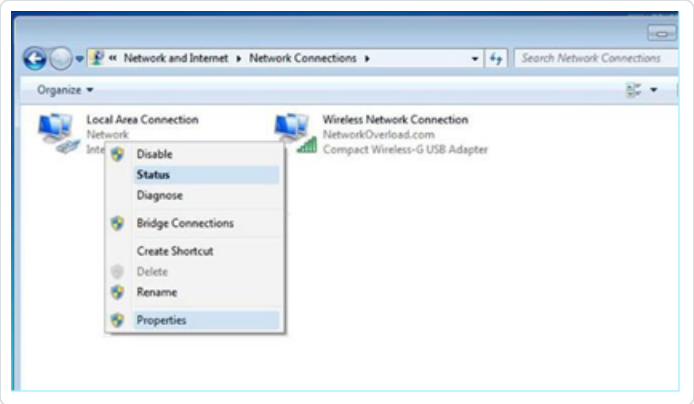
Si vous n'avez pas configuré l'adresse IP de gestion, vous pouvez utiliser soit un PC directement connecté, soit un réseau correctement configuré pour accéder à l'interface utilisateur Tenable Core sur l'une des options suivantes :

- **système 1** —Interface de gestion par défaut, pré-configurée avec l'adresse IP 192.168.1.5/24
- **système 4** —Interface d'ingénierie, pré-configurée avec l'adresse IP 192.168.3.3/24. Si elle n'est pas modifiée ultérieurement, elle pourra être utilisée pour les procédures de récupération.

Pour vous connecter à Tenable Core directement via votre PC ou votre ordinateur portable :

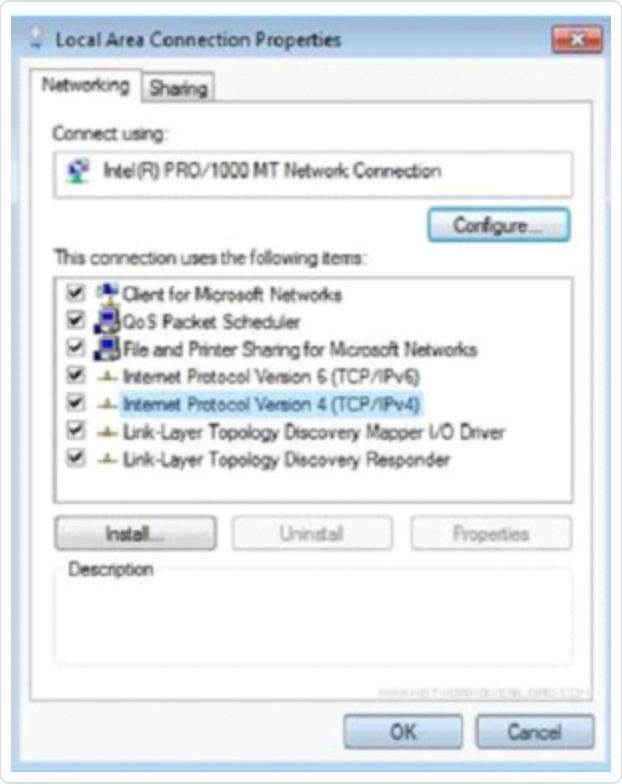
1. Connectez un câble Ethernet entre votre PC et l'un des ports pré-configurés sur l'appliance OT Security.
2. Sous Windows, utilisez **win+R** pour ouvrir **Exécuter** et tapez `ncpa.cpl` pour ouvrir **Connexions réseau**.





3. Effectuez un clic droit sur votre connexion réseau (appelée **Connexion au réseau local**) et sélectionnez **Propriétés**.

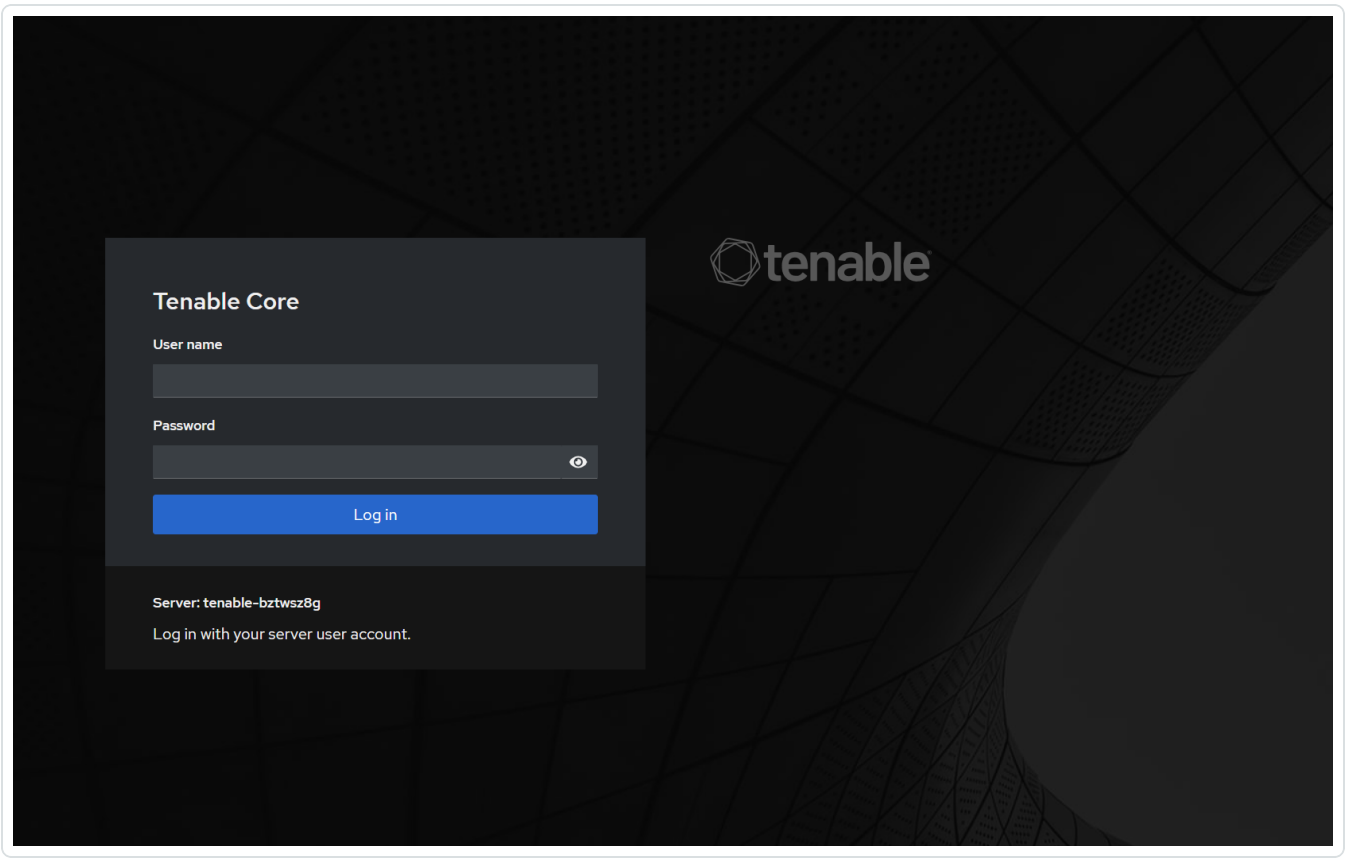
   La fenêtre **Propriétés de la connexion au réseau local** apparaît.



4. Sélectionnez **Protocole Internet version 4 (TCP/ IPv4)** et cliquez sur **Propriétés**.

   La fenêtre **Propriétés d'Internet Protocol Version 4 (TCP/ IPv4)** apparaît.

5. Sélectionnez **Utiliser l'adresse IP suivante**.
6. Dans la zone **Adresse IP**, saisissez l'adresse IP correspondant à l'interface à laquelle vous vous connectez. Par exemple, 192.168.1.10 pour l'adresse par défaut du Port 1/ nic0 ou 192.168.3.10 pour l'adresse par défaut du .
7. Dans la zone **Masque de sous-réseau**, saisissez 255.255.255.0.
8. Cliquez sur **OK**.
9. Depuis votre navigateur web Chrome, accédez à https://<mgmt-ip>:8000.



10. Si vous n'avez pas encore configuré le compte utilisateur administrateur, le système vous invite à le faire maintenant, puis à vous reconnecter avec votre utilisateur nouvellement créé. Pour plus d'informations, voir Create an initial Administrator Account (Créer et initialiser un compte administrateur).

    Après avoir créé le compte administrateur, Tenable vous recommande de configurer l'adresse IP de gestion. Si vous avez l'intention d'utiliser la configuration en **port fractionné**,

assurez-vous que les interfaces peuvent atteindre les réseaux appropriés. Pour plus d'informations, voir Considérations sur le réseau.

> **Remarque** : pour configurer ou modifier l'adresse IP de gestion, reconnectez-vous à Tenable Core, activez l'accès administratif et modifiez la configuration réseau.

Que faire ensuite

Installer OT Security sur Tenable Core

Installer OT Security sur Tenable Core

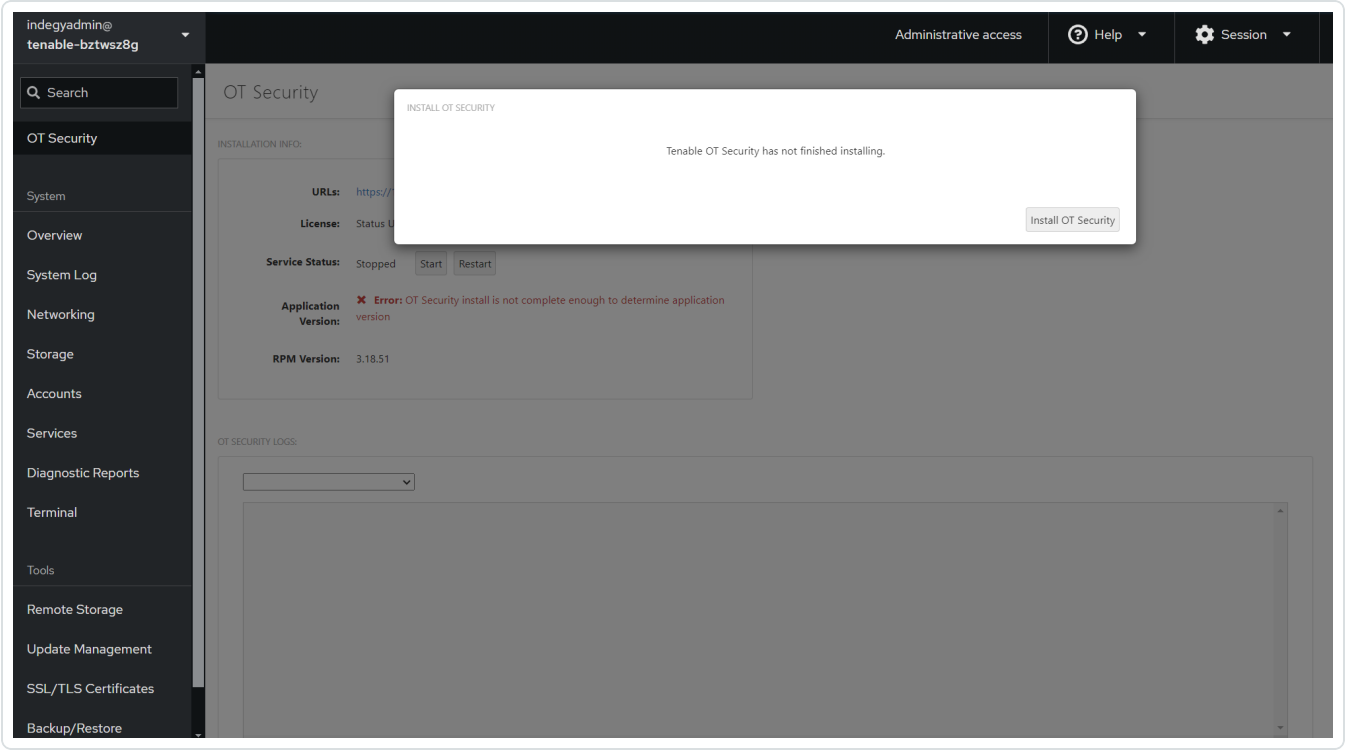
Sur le matériel ou les machines virtuelles non fournis par Tenable, vous devez terminer manuellement l'installation de l'application OT Security.

Pour installer OT Security sur Tenable Core :

1. Pour vous connecter à Tenable Core depuis votre navigateur web Chrome, accédez à `https://<mgmt-ip>:8000`.

   > **Remarque** : assurez-vous de disposer d'un accès administrateur.

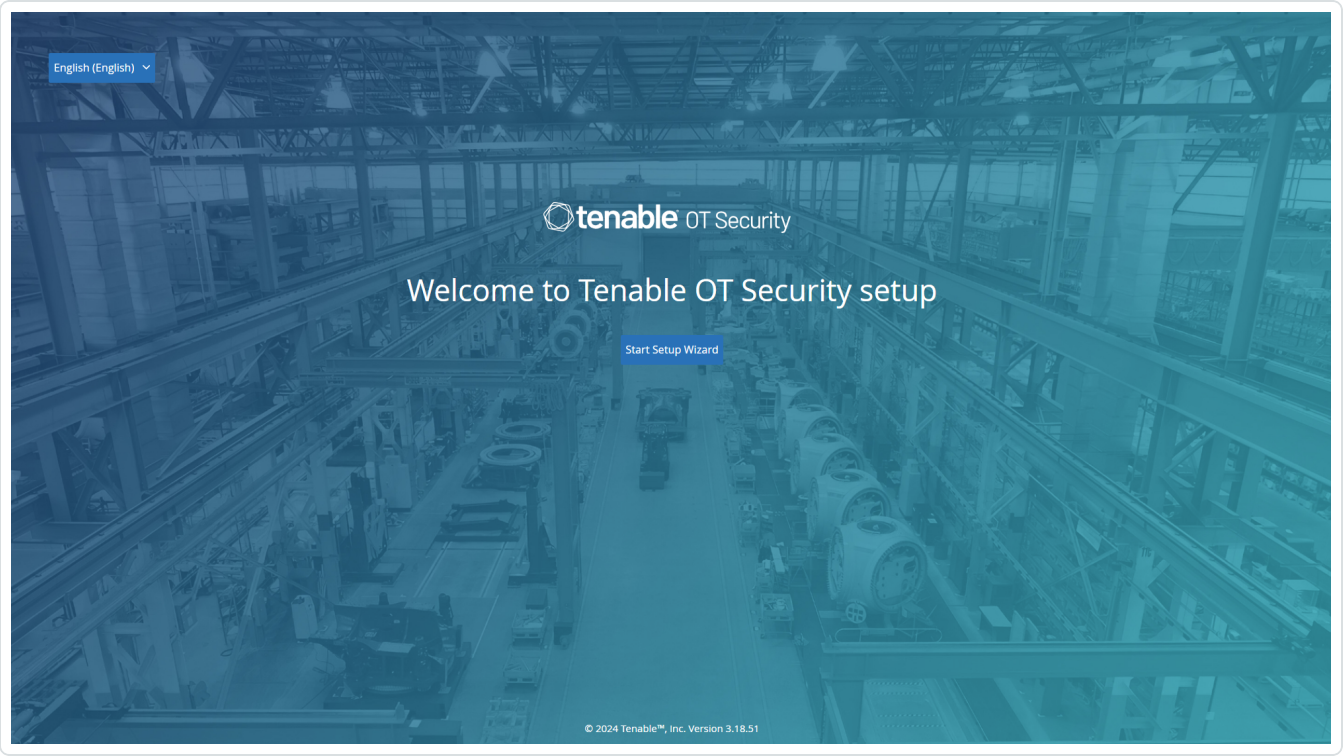
2. Accédez à OT Security.
3. À l'invite d'installation, cliquez sur **Installer Tenable OT Security**.



Remarque : le processus d'installation peut prendre un certain temps. N'interrompez pas le processus d'installation.

Une fois l'installation terminée, vous pouvez vous connecter à l'interface utilisateur OT Security à l'adresse `https://<mgmt-ip>`.

`mgmt-ip` est votre adresse IP qui apparaît dans le champ **URL** en haut de la fenêtre Tenable Core.



Que faire ensuite

Configurer les paramètres OT Security à l'aide de l'assistant de configuration

Configurer les paramètres OT Security à l'aide de l'assistant de configuration

L'assistant de configuration OT Security vous guide tout au long du processus de configuration des paramètres système de base.

> **Remarque :** vous pouvez modifier la configuration si nécessaire dans l'écran **Paramètres** de la console de gestion (interface utilisateur).

Pour accéder à l'assistant de configuration, vous devez d'abord vous connecter à la console de gestion OT Security. Pour plus d'informations sur la façon de vous connecter à la console de gestion, consultez Se connecter à la console de gestion OT Security.

Configurez les éléments suivants à l'aide de l'assistant de configuration :

1. Informations utilisateur
2. Appareil

3. Heure système
4. Connecter le port de gestion séparé (séparation des ports)

Remarque : après avoir terminé l'assistant de configuration, OT Security vous invite à redémarrer le système.

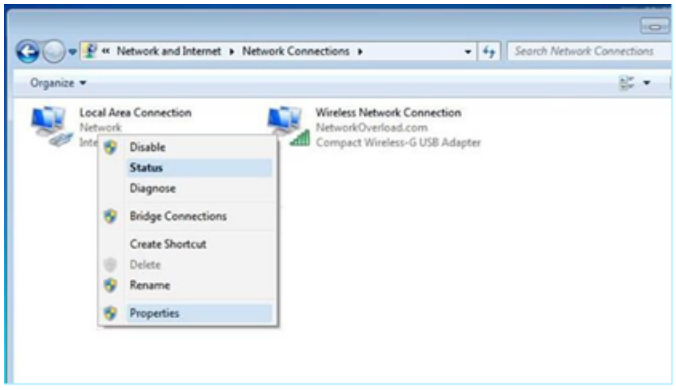
Se connecter à la console de gestion OT Security

Pour se connecter à la console de gestion OT Security :

1. Effectuez l'une des actions suivantes :
   - Connectez le poste de travail de la console de gestion (PC, ordinateur portable, etc.) directement au port 1de l'appliance OT Security à l'aide du câble Ethernet.
   - Connectez le poste de travail de la console de gestion au commutateur réseau.

   Remarque : vérifiez que le poste de travail de la console de gestion fait partie du même sous-réseau que l'appliance OT Security (192.168. 10/24) ou qu'elle est routable vers l'unité.
2. Configurez une adresse IP statique pour vous connecter à l'appliance OT Security comme suit :
   a. Accédez à **Réseau et Internet** > **Centre Réseau et partage** > **Modifier les paramètres de la carte**.

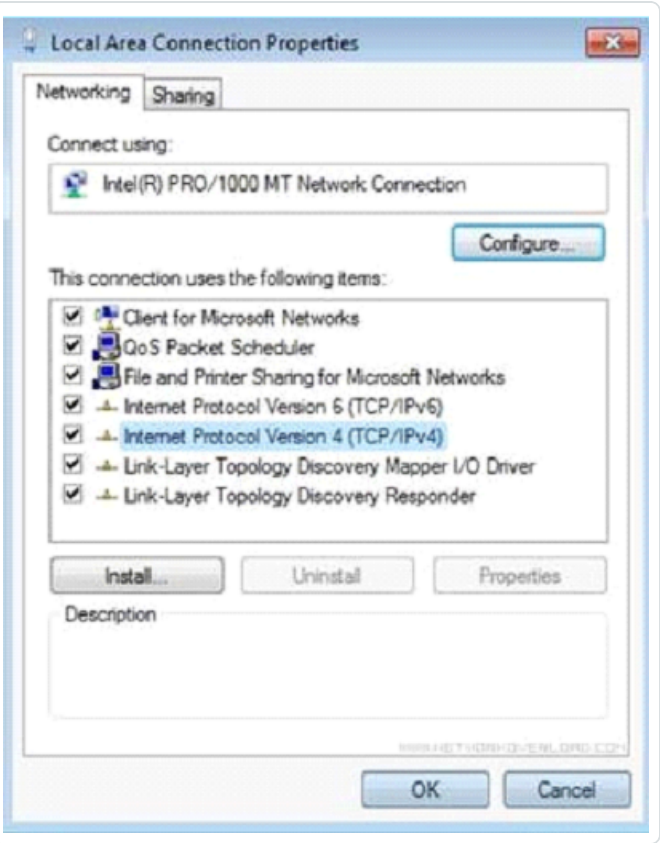
   L'écran **Connexions réseau** apparaît.

   Remarque : la navigation peut varier légèrement selon la version de Windows.

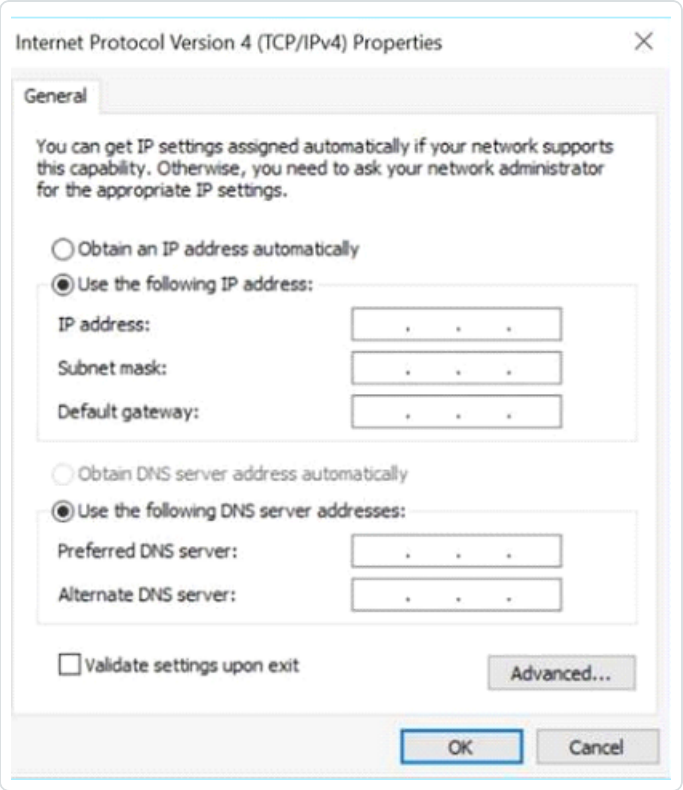
b. Effectuez un clic droit sur **Connexions au réseau local** et sélectionnez **Propriétés**.

La fenêtre **Connexions au réseau local** apparaît.



c. Sélectionnez **Protocole Internet version 4 (TCP/ IPv4)** et cliquez sur **Propriétés**.

La fenêtre **Propriétés d'Internet Protocol Version 4 (TCP/ IPv4)** apparaît.



d. Sélectionnez **Utiliser l'adresse IP suivante**.

e. Dans la zone **Adresse IP**, saisissez 192.168.1.10.

f. Dans la zone **Masque de sous-réseau**, saisissez 255.255.255.0.

g. Cliquez sur **OK**.

   OT Security applique les nouveaux paramètres.

h. Dans votre navigateur web Chrome, accédez à https://192.168.1.5.

   L'écran de **bienvenue** de l'assistant de configuration apparaît.

Remarque : l'accès à l'interface utilisateur nécessite la dernière version de Chrome.

i. Cliquez sur **Démarrer l'assistant de configuration**.

L'assistant de configuration apparaît et affiche la page **Informations utilisateur**.

Que faire ensuite

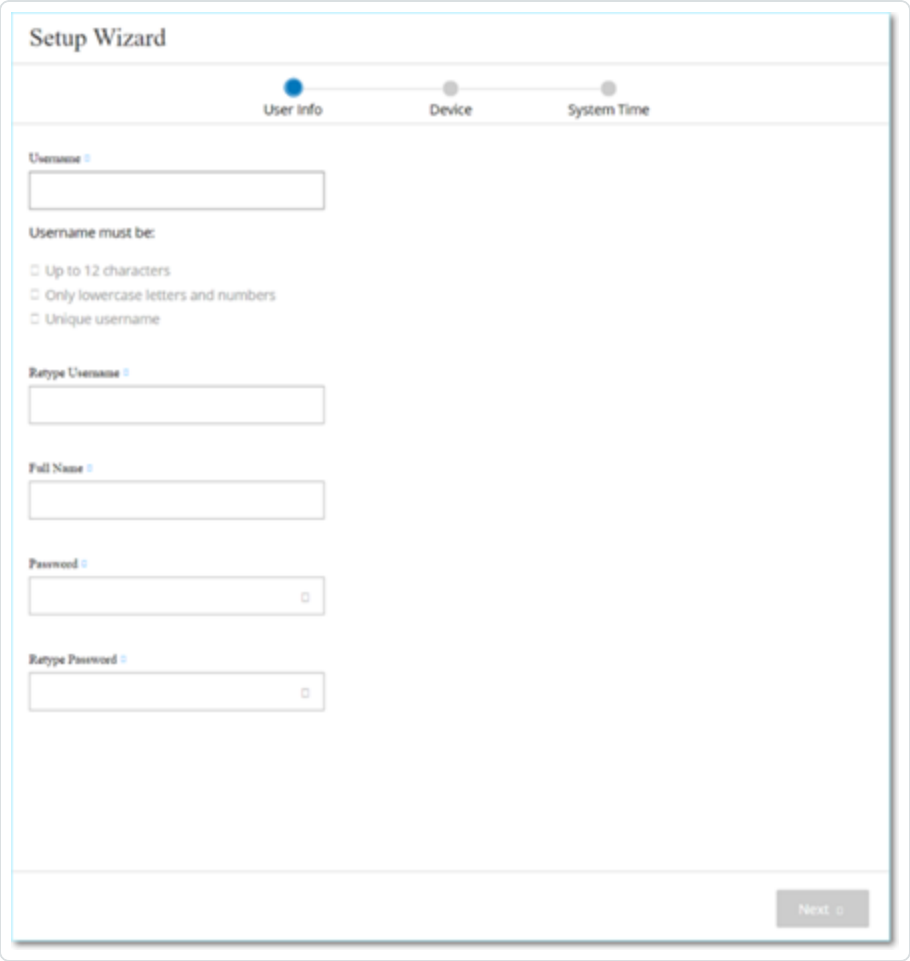
Informations utilisateur

Informations utilisateur

L'assistant de configuration OT Security vous guide tout au long du processus de configuration des paramètres système de base.

Remarque : vous pouvez modifier la configuration si nécessaire dans l'écran **Paramètres** de la console de gestion (interface utilisateur).

Informations utilisateur



Sur la page **Informations utilisateur**, remplissez les informations de votre compte utilisateur.

Remarque : dans l'assistant de configuration, vous pouvez configurer les informations d'authentification pour un compte administrateur. Après vous être connecté à l'interface utilisateur, vous pourrez créer des comptes utilisateur supplémentaires. Pour plus d'informations sur les comptes utilisateur, voir Utilisateurs et rôles.

1. Dans la zone **Nom d'utilisateur**, saisissez le nom d'utilisateur à utiliser pour la connexion au système.

   Le nom d'utilisateur peut comporter jusqu'à 12 caractères et ne doit inclure que des lettres minuscules et des chiffres.

2. Dans la zone **Confirmer le nom d'utilisateur**, saisissez à nouveau le nom d'utilisateur.

3. Dans la section **Nom complet**, saisissez vos **prénom et nom de famille**.

> **Remarque :** c'est le nom qui apparaît dans la barre d'en-tête et sur les journaux de votre activité dans le système.

4. Dans la zone **Mot de passe**, saisissez le mot de passe à utiliser pour vous connecter au système. Les mots de passe doivent contenir au moins :
    - 12 caractères
    - Une lettre majuscule
    - Une lettre minuscule
    - Un chiffre
    - Un caractère spécial
5. Dans la zone **Confirmer le mot de passe**, ressaisissez le même mot de passe.
6. Cliquez sur **Suivant**.

    La page **Appareil** de l'assistant de configuration apparaît.

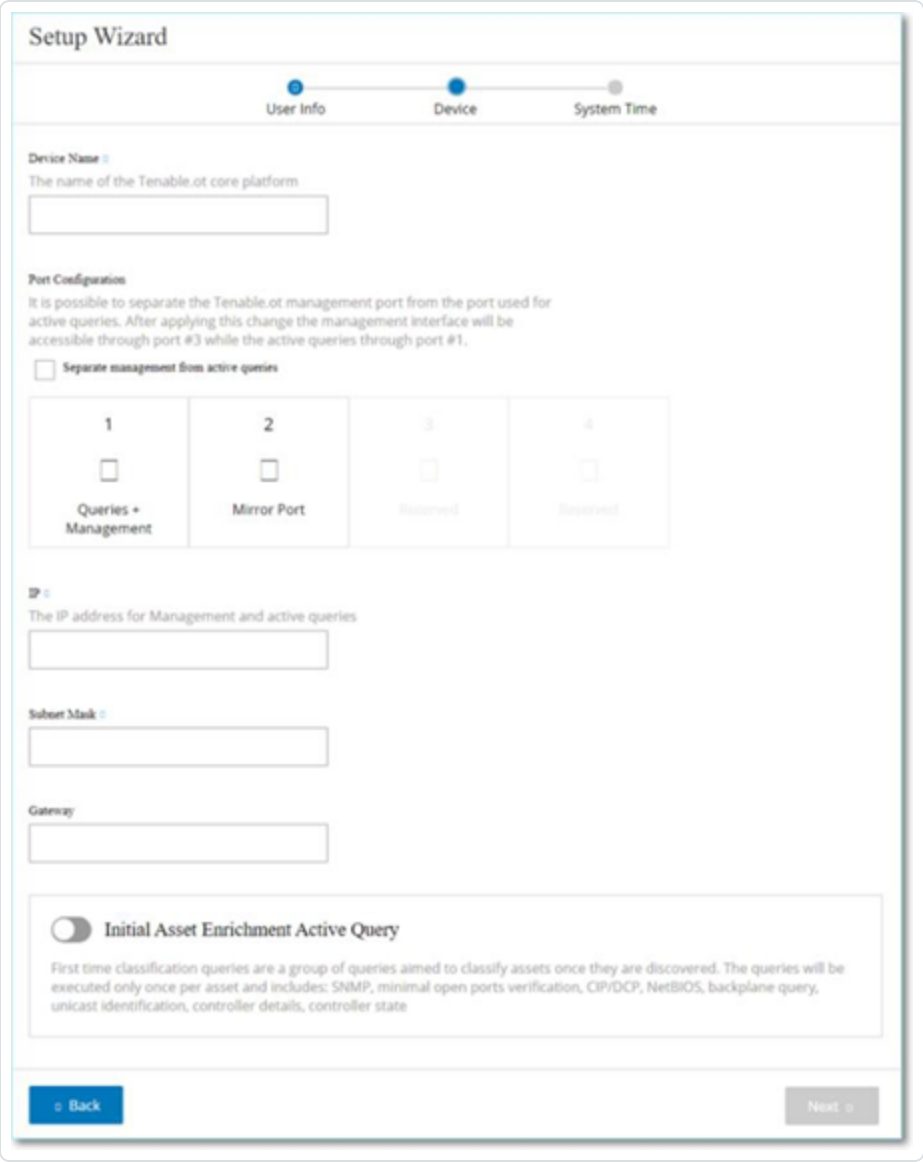
Que faire ensuite

Configurer l'Appareil.

Appareil

L'assistant de configuration OT Security vous guide tout au long du processus de configuration des paramètres système de base.

> **Remarque :** vous pouvez modifier la configuration si nécessaire dans l'écran **Paramètres** de la console de gestion (interface utilisateur).



Sur la page **Appareil**, fournissez des informations sur la plateforme OT Security :

1. Dans la zone **Nom de l'appareil**, saisissez l'identifiant unique de la plateforme OT Security.
2. Dans la section **Configuration des ports**, effectuez l'une des actions suivantes :
    - **Séparation des ports** —Si vous souhaitez utiliser des ports différents pour la gestion et pour les requêtes, cochez la case **Séparer la gestion des requêtes actives**. La sélection de cette option configure le port 1comme port de requêtes uniquement et le port 3 comme port de gestion uniquement.

> **Remarque :** sur certains systèmes, l'option de séparation des ports peut ne pas être disponible. Contactez votre agent d'assistance pour obtenir de l'aide.

- **Aucune séparation** —Pour maintenir les requêtes et la gestion sur le même port, ne sélectionnez pas **Séparer la gestion des requêtes actives**. Dans ce cas, vous pouvez ignorer l'étape 3 de cette procédure et passer à l'étape 4.

3. Si vous sélectionnez l'option de **séparation des ports** :

   a. Dans la zone **IP des requêtes actives**, saisissez l'adresse IP du port de requêtes de l'unité.

      Ce port se connecte à un port standard du commutateur réseau, qui peut contacter les contrôleurs ou router vers ces derniers. Étant donné que OT Security se connecte aux contrôleurs, il a besoin d'une adresse IP dans le sous-réseau du réseau.

   b. Dans la zone **Masque de sous-réseau des requêtes actives**, saisissez le masque de sous-réseau du port de requêtes.

   c. Dans la zone (facultative) **Passerelle des requêtes actives**, saisissez l'adresse IP de la passerelle dans le réseau opérationnel.

4. Dans la zone **IP de gestion**, saisissez l'adresse IP (dans le sous-réseau du réseau) à appliquer à la plateforme OT Security.

   Elle devient l'adresse IP de gestion OT Security. Cette adresse IP est également l'adresse des requêtes s'il n'y a pas de séparation entre les ports.

5. Dans la zone **Masque de sous-réseau de gestion**, saisissez le masque de sous-réseau du réseau.

6. (Facultatif) Si vous souhaitez configurer une passerelle, dans la zone **Passerelle de gestion**, saisissez l'adresse IP de la passerelle du réseau.

   > **Remarque :** si vous ne fournissez pas l'adresse IP de la passerelle de gestion, OT Security ne peut pas communiquer avec des composants externes en dehors du sous-réseau, tels que les serveurs de messagerie, les serveurs Syslog, etc.

7. La **requête active pour l'enrichissement initial des assets** comprend un ensemble de requêtes exécutées sur chaque asset détecté au sein du système.

Elle aide OT Security à classifier les assets. Pour exécuter ces requêtes sur chaque nouvel asset découvert par OT Security, activez **Requête active pour l'enrichissement initial des assets** en cliquant sur le curseur.

8. Cliquez sur **Suivant**.

   La page **Heure système** de l'assistant de configuration apparaît.

Que faire ensuite

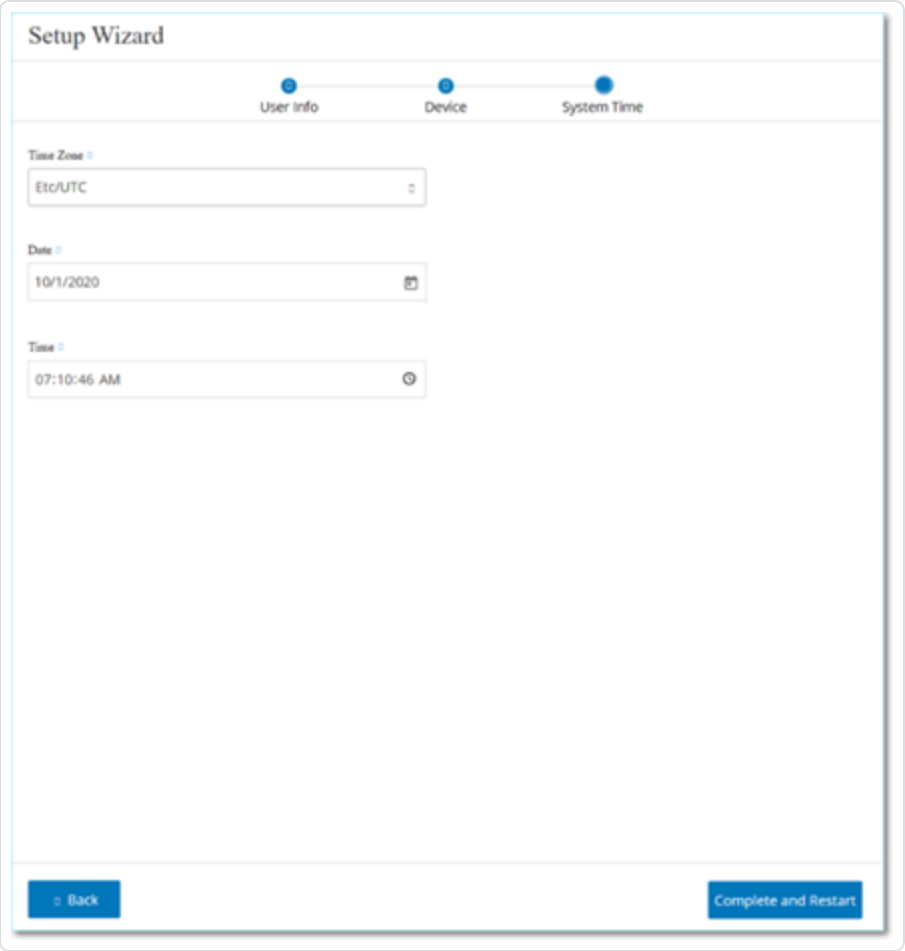
Configurer les paramètres Heure système.

Heure système

L'assistant de configuration OT Security vous guide tout au long du processus de configuration des paramètres système de base.

> **Remarque :** vous pouvez modifier la configuration si nécessaire dans l'écran **Paramètres** de la console de gestion (interface utilisateur).

Heure système

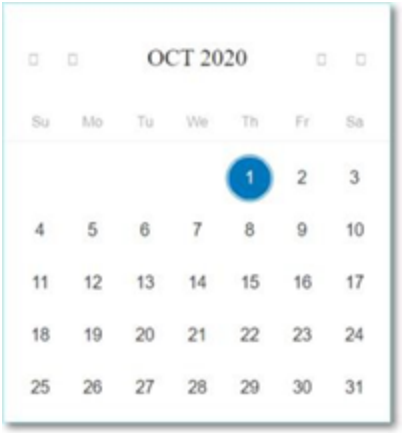


Remarque : la définition de la date et de l'heure est essentielle pour un enregistrement précis des journaux et des alertes.

Sur la page **Heure système**, l'heure et la date correctes apparaissent automatiquement. Si ce n'est pas le cas, procédez comme suit :

1. Dans la zone déroulante **Fuseau horaire**, sélectionnez le fuseau horaire local correspondant à l'emplacement du site.
2. Dans la zone **Date**, cliquez sur l'icône du calendrier .

   Un calendrier apparaît dans une fenêtre pop-up.



3. Sélectionnez la date actuelle.
4. Dans la zone **Heure**, sélectionnez respectivement les heures, les minutes et les secondes, puis saisissez le nombre approprié à l'aide du clavier ou des flèches haut et bas.

   > **Remarque :** pour modifier l'une des pages précédentes de l'assistant de configuration, cliquez sur **Précédent**. Après avoir cliqué sur **Terminer et redémarrer**, vous ne pourrez pas revenir dans l'assistant de configuration. Cependant, vous pouvez modifier les paramètres de configuration dans la page **Paramètres** de l'interface utilisateur.

5. Pour finaliser la configuration, cliquez sur **Terminer et redémarrer**.

   Une fois le redémarrage terminé, OT Security vous redirige vers la fenêtre de **gestion de la licence**.

   > **Remarque** : si vous avez sélectionné l'option de séparation des ports, modifiez vos connexions réseau comme décrit dans Connecter le port de gestion séparé (séparation des ports).

Que faire ensuite

Effectuez les actions suivantes :

- Connecter le port de gestion séparé (séparation des ports)
- Activation de licence OT Security

Connecter le port de gestion séparé (séparation des ports)

Si vous avez sélectionné l'option **Séparation des ports** (pour séparer les requêtes de la gestion), vous devez connecter le port 3 de l'appliance OT Security (devenu le port de gestion) à l'un des ports

d'un commutateur réseau. Il peut s'agir d'un commutateur réseau différent, tel qu'un commutateur réseau du réseau IT.

Pour connecter le port de gestion :

1. Sur l'appliance OT Security, connectez un câble Ethernet (fourni) au port 3.
2. Connectez le câble à l'un des ports d'un commutateur réseau.

Que faire ensuite

Activation de licence OT Security

Activation de licence OT Security

Objectif : déverrouiller les fonctionnalités système avec l'activation de la licence.

Tenable calcule les licences en fonction du nombre d'adresses IP uniques dans le système. Chaque adresse IP nécessite une licence distincte. Par exemple, Tenable base les licences sur le nombre d'adresses IP uniques, même si plusieurs appareils partagent la même adresse IP ou si plusieurs appareils connectés au même fond de panier partagent les trois mêmes adresses IP. Par conséquent, vous avez besoin de trois licences, quel que soit le nombre d'appareils.

Après avoir installé l'appliance OT Security, vous pouvez activer votre licence.

Remarque : pour mettre à jour ou réinitialiser votre licence OT Security, contactez votre responsable de compte Tenable. Une fois que votre responsable de compte Tenable a mis à jour votre licence, vous pouvez la mettre à jour ou la réinitialiser.

Pour plus d'informations sur le déploiement et la gestion des licences de Tenable OT Security pour Tenable One, voir le Guide de déploiement de Tenable One.

Avant de commencer

- Installez l'appliance OT Security.
- Veillez à vous munir du code de licence (20 caractères, lettres et chiffres) que vous avez reçu de Tenable lorsque vous avez commandé votre appareil.

- Assurez-vous d'avoir accès à Internet. Si votre appareil OT Security n'est pas connecté à Internet, vous pouvez enregistrer la licence depuis n'importe quel PC.
- Assurez-vous d'avoir accès au portail Tenable Account Management. Pour y accéder, contactez votre Customer Success Manager Tenable.

Activer votre licence OT Security

Vous pouvez activer votre licence OT Security et utiliser le portail Tenable Account Management pour créer de nouveaux sites et gérer vos assets.

Pour plus d'informations sur le portail Account Management, voir la documentation sur le portail Account Management.

Pour activer votre licence OT Security :

1. Connectez-vous au portail Tenable Account Management à l'aide de votre compte de communauté.

   La page **Account** (Compte) apparaît avec les options que vous êtes autorisé à afficher.

2. Dans la barre de navigation de gauche, sélectionnez **Products** (Produits).

   La page **My Products** (Mes produits) apparaît et répertorie tous vos produits Tenable.

3. Cliquez sur la licence Tenable OT Security.

   La page des **détails** de **Tenable OT Security** apparaît. Les licences OT Security apparaissent avec des détails tels que la date d'achat, la date d'expiration et le nombre d'adresses IP et de sites sous licence.

4. Dans la colonne **Activation Code** (Code d'activation), copiez le code de licence OT Security à 20 chiffres.

5. Générez le certificat d'activation dans OT Security :

   a. Accédez à la page **Activation de licence** OT Security.

   b. À l'étape 1, cliquez sur **Saisir le nouveau code de licence**.

      Le panneau **Saisir le nouveau code de licence** apparaît sur le côté droit.

c. Dans la zone **Code de licence**, collez le code (**code d'activation**) que vous avez copié à partir du portail Account Management.

d. Cliquez sur **Vérifier**.

OT Security active la section **Générer un certificat d'activation**.

e. Cliquez sur **Générer un certificat**.

Le panneau **Générer un certificat** apparaît sur la droite.

f. Cliquez sur **Copier le texte dans le presse-papiers**, puis sur **Terminé**.

OT Security génère le certificat que vous devez fournir dans le portail Tenable Account Management pour ajouter vos sites.

6. À l'étape 3, dans le champ **Enter activation code** (Saisir le code d'activation), cliquez sur le lien **Self-service** (Libre-service) pour ouvrir le portail Tenable Account Management.

Remarque : pour activer votre période d'évaluation, cliquez sur le lien **Click here** (Cliquez ici).

7. Sur la page du produit Tenable OT Security, dans le portail Account Management, cliquez sur l'onglet **Sites**.

L'onglet **Sites** apparaît.

8. Pour créer un site, cliquez sur **Manage Sites** (Gérer les sites) > **Create Site** (Créer un site).

La fenêtre **Create New Site** (Créer un site) apparaît.

a. (Facultatif) Dans la zone **Label** (Étiquette), saisissez le nom du site.

b. Dans la zone **Size** (Taille), saisissez le nombre d'adresses IP que vous souhaitez attribuer à ce site.

Conseil : pour ajuster le nombre d'adresses IP attribuées à la licence, utilisez le curseur situé sous la zone **Size** (Taille).

c. Dans la zone **Activation Certificate** (Certificat d'activation), collez le certificat que vous avez copié à partir de OT Security. Voir l'étape 5f.

d. Cliquez sur **Créer**.

Une boîte de dialogue apparaît avec un code d'activation. Il s'agit d'un code à usage unique que vous devez copier sur l'instance OT Security.

e. Cliquez sur le bouton .

f. Cliquez sur **Confirm** (Confirmer).

9. Revenez à l'instance OT Security et, dans la section **3 Saisir le code d'activation**, cliquez sur **Saisir le code d'activation**.

   Le panneau **Saisir le code d'activation** apparaît à droite.

10. Dans la zone **Code d'activation**, collez le code unique que vous avez copié depuis la page **Tenable OT Security Account Management** (Gestion des comptes Tenable). Voir l'étape 8e.

11. Cliquez sur **Activer**.

    OT Security affiche un message confirmant que le système a bien été activé et l'interface OT Security apparaît.

12. Cliquez sur **Activer**.

    OT Security est maintenant activé et prêt à être utilisé.

13. Revenez au portail Tenable Account Management. Dans la boîte de dialogue du code d'activation à usage unique, cochez la case **I confirm I have saved the activation licence** (Je confirme avoir enregistré la licence d'activation).

14. Cliquez sur **Confirm** (Confirmer).

    Le site nouvellement ajouté apparaît dans l'onglet **Sites** pour OT Security.

Mettre à jour votre licence

Lorsque vous augmentez votre limite d'assets, prolongez la période de votre licence ou modifiez le type de votre licence, vous pouvez mettre à jour votre licence.

Avant de commencer

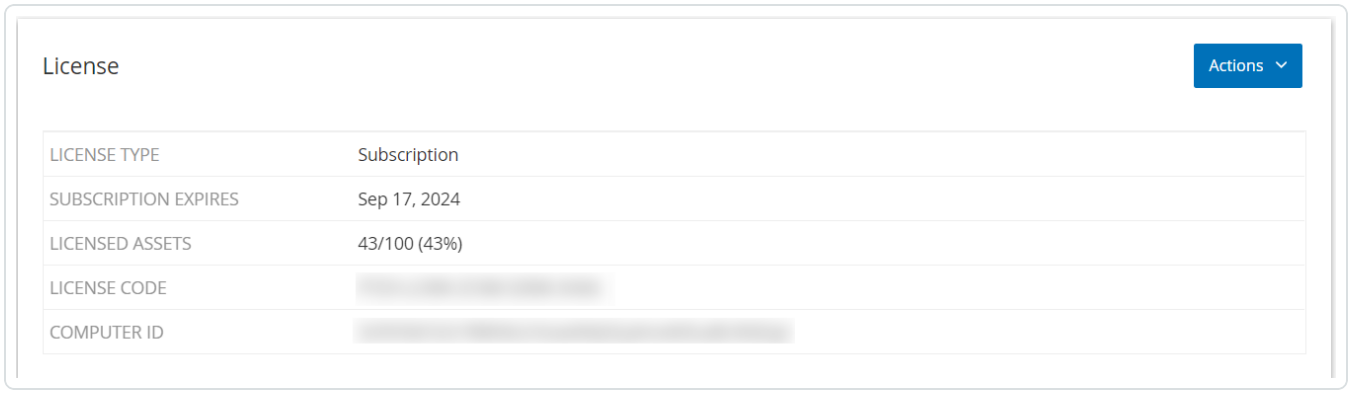
- Votre responsable de compte Tenable doit déjà avoir mis à jour vos informations de licence dans son système avant que vous puissiez mettre à jour la nouvelle licence.

- Vous devez avoir accès à Internet. Si votre appareil OT Security ne peut pas se connecter à Internet, vous pouvez enregistrer la licence depuis n'importe quel PC.

Pour mettre à jour votre licence :

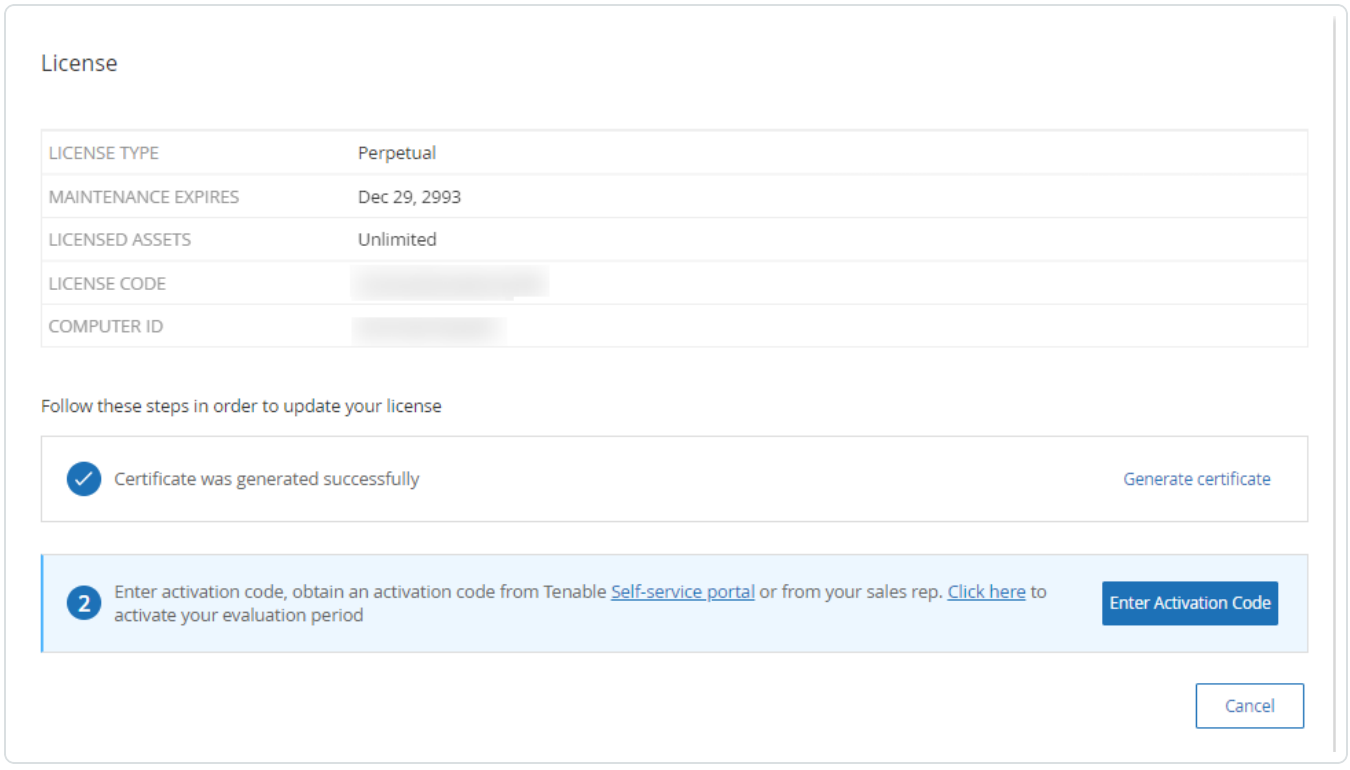
1. Accédez à **Paramètres locaux** > **Configuration système** > **Licence**.

   La fenêtre **Licence** apparaît.



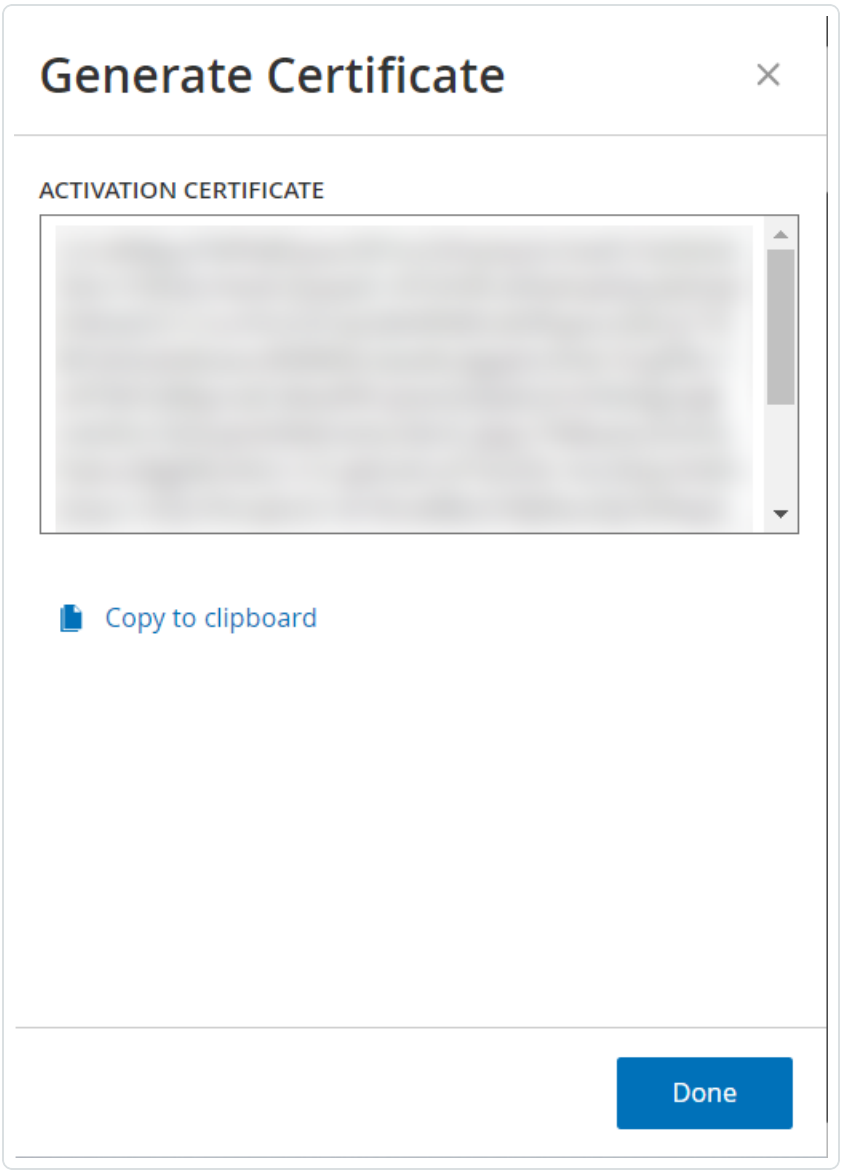
2. Dans le menu **Actions**, sélectionnez **Mettre à jour la licence**.

   Les étapes **Générer un certificat** et **Saisir le code d'activation** apparaissent.



3. Dans la zone **(1) Générer un certificat d'activation**, cliquez sur le bouton **Générer un certificat**.

   Le panneau **Générer un certificat** apparaît avec le **certificat d'activation**.



4. Cliquez sur **Copier le texte dans le presse-papiers**, puis sur **Terminé**.

   Le panneau latéral se referme.

5. Modifier les détails du site dans le portail Tenable Account Management :

a. Dans le portail Tenable Account Management, accédez à la page des détails de **Tenable OT Security** et cliquez sur le bouton sur la ligne du site que vous souhaitez mettre à jour.

   Un menu apparaît.

b. Cliquez sur **Edit Site** (Modifier le site).

   La fenêtre de modification du site apparaît.

c. Modifiez les détails selon les besoins.

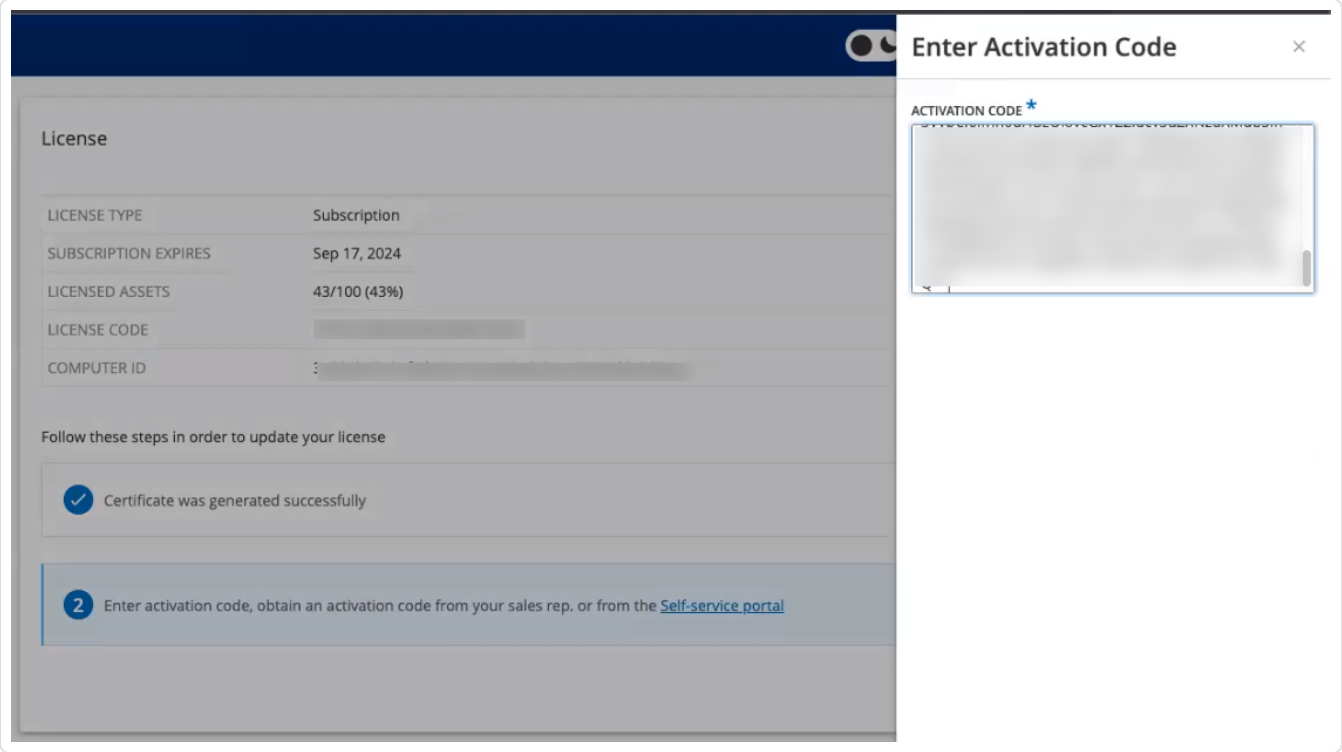
d. Dans la zone **Activation Certificate** (Certificat d'activation), collez le certificat que vous avez copié à partir de la fenêtre **Générer un certificat** dans OT Security.

e. Cliquez sur **Mettre à jour**.

   Le portail affiche une boîte de dialogue avec un code d'activation. Il s'agit d'un code à usage unique que vous devez copier sur l'instance OT Security.

f. Cliquez sur le bouton , puis cliquez sur **Confirm** (Confirmer).

6. Revenez à l'instance OT Security.
7. Dans la zone **(2) Saisir le code d'activation**, cliquez sur **Saisir le code d'activation**.
8. Dans la zone **Code d'activation**, collez le code unique que vous avez copié depuis la page **Tenable OT Security Account Management** (Gestion des comptes Tenable).

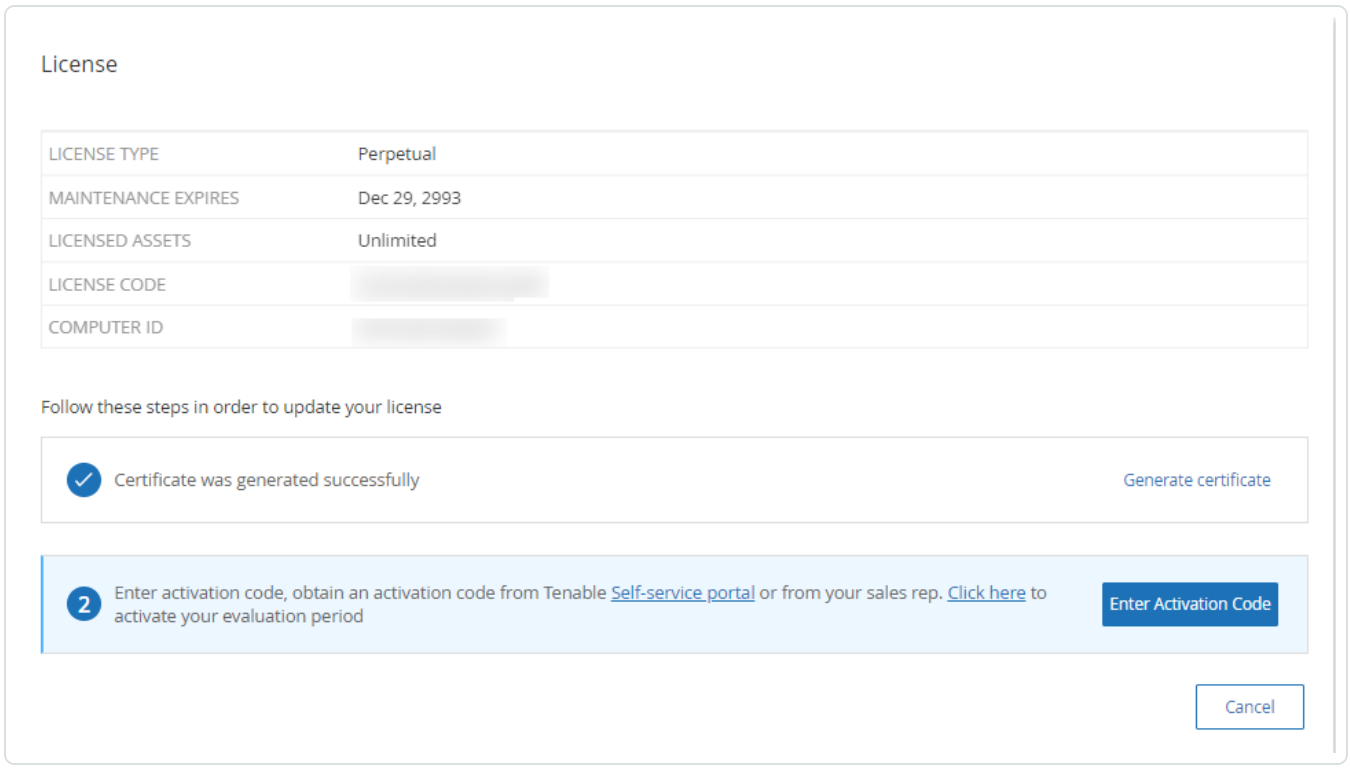


9. Cliquez sur **Activer**.

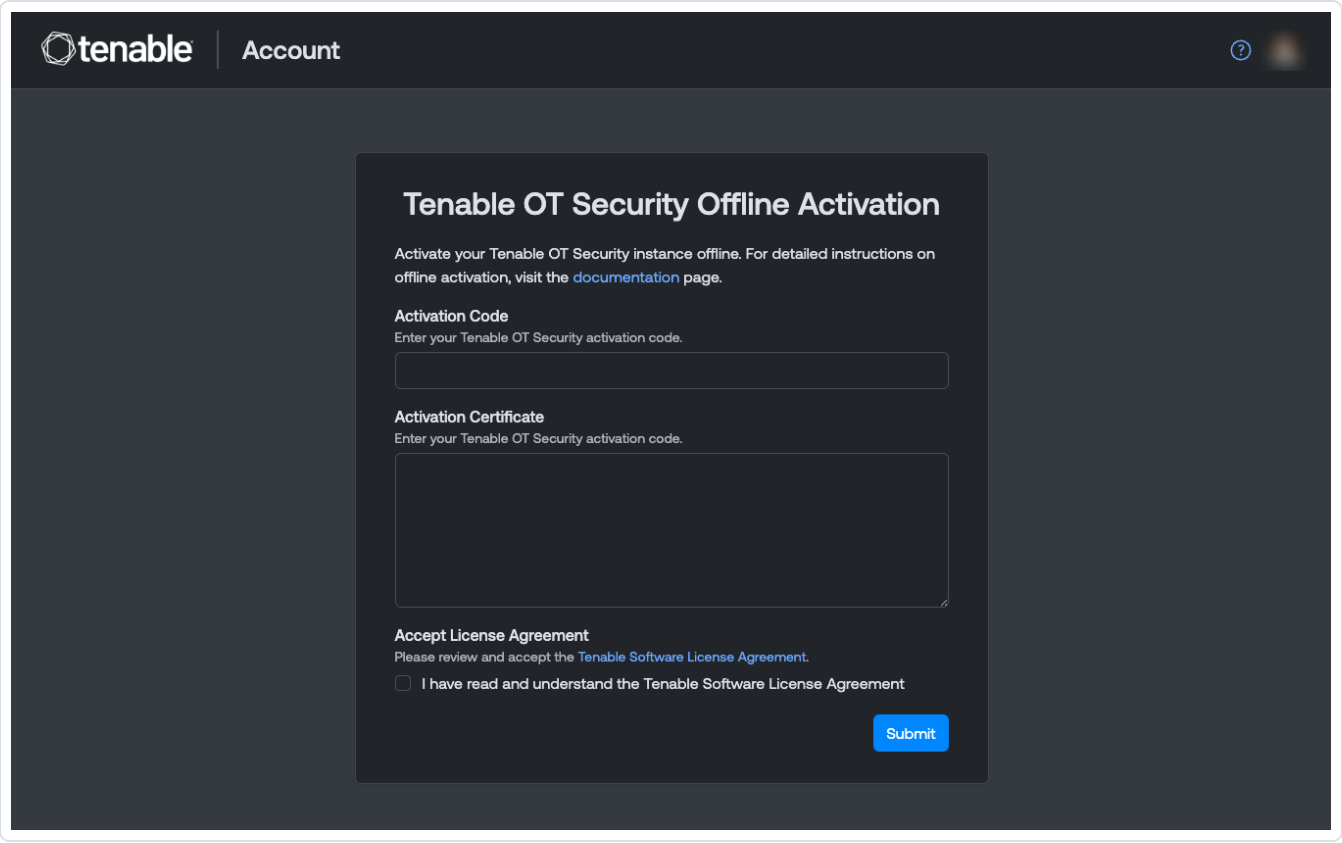
   OT Security affiche un message confirmant que le système est bien activé et la page **Licence** affiche les détails de la licence mise à jour.

Mettre à jour votre licence en mode hors ligne

1. Effectuez les étapes 1à 4 comme décrit dans la section Mettre à jour votre licence.
2. Dans la zone **(2) Saisir le code d'activation**, cliquez sur le lien vers le portail libre-service.



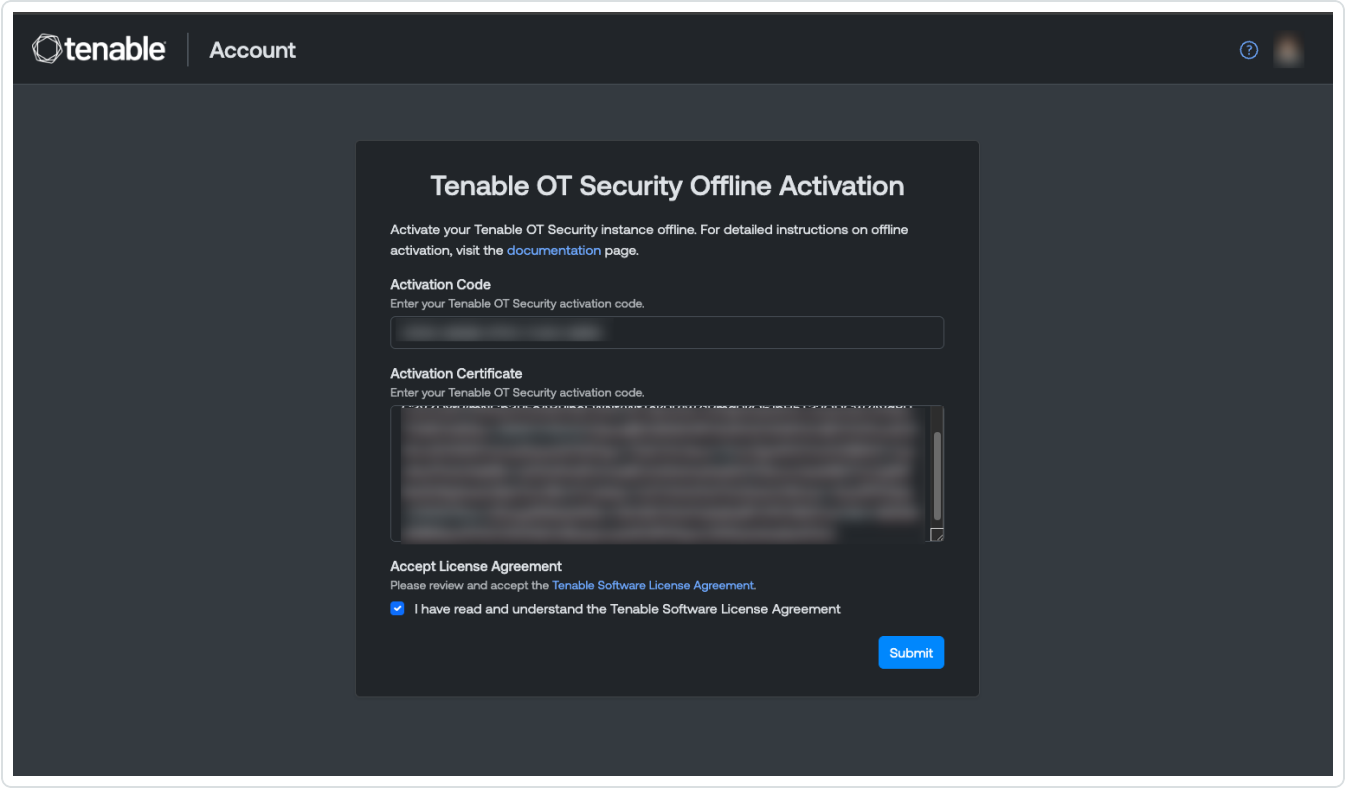
La fenêtre **Tenable OT Security Offline Activation** (Activaction hors ligne de Tenable OT Security) apparaît dans un nouvel onglet.



Remarque : vous pouvez accéder à l'écran Activate OT Security Offline (Activer OT Security hors ligne) à partir d'un appareil connecté à Internet via l'URL https://account.tenable.com/offline-activation/ot-security.

Remarque : si vous n'êtes pas connecté à tenable.com, vous pouvez vous connecter à l'aide de votre adresse e-mail et de votre mot de passe. Utilisez le compte de messagerie sur lequel vous avez reçu votre **code de licence**. Si vous n'avez pas les identifiants de connexion, vous pouvez soit cliquer sur **Don't remember your password** (Mot de passe oublié) et suivre les instructions, soit contacter votre responsable de compte Tenable.

3. Dans le champ **Activation Code** (Code d'activation), saisissez votre **code de licence** à 20 caractères (qui peut être copié et collé à partir de la fenêtre **Licence**).
4. Dans la zone **Activation Certificate** (Certificat d'activation), collez le **certificat d'activation**.
5. Cochez la case **I have read and understand the Tenable Software License Agreement** (J'ai lu et compris le contrat de licence du logiciel Tenable).



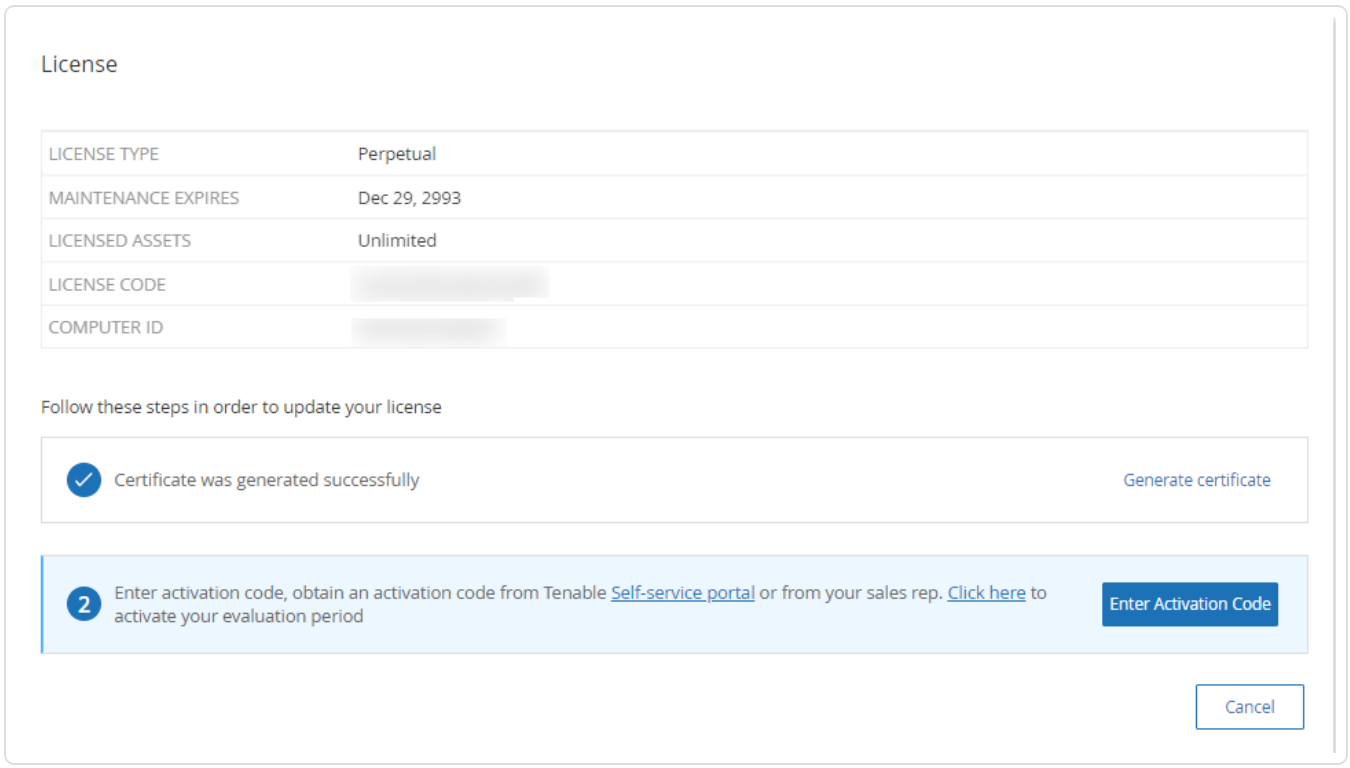
Remarque : pour afficher le contrat de licence, cliquez sur le lien **Tenable Software License Agreement** (Contrat de licence du logiciel Tenable).

6. Cliquez sur **Submit** (Soumettre).

   OT Security génère le code d'activation.

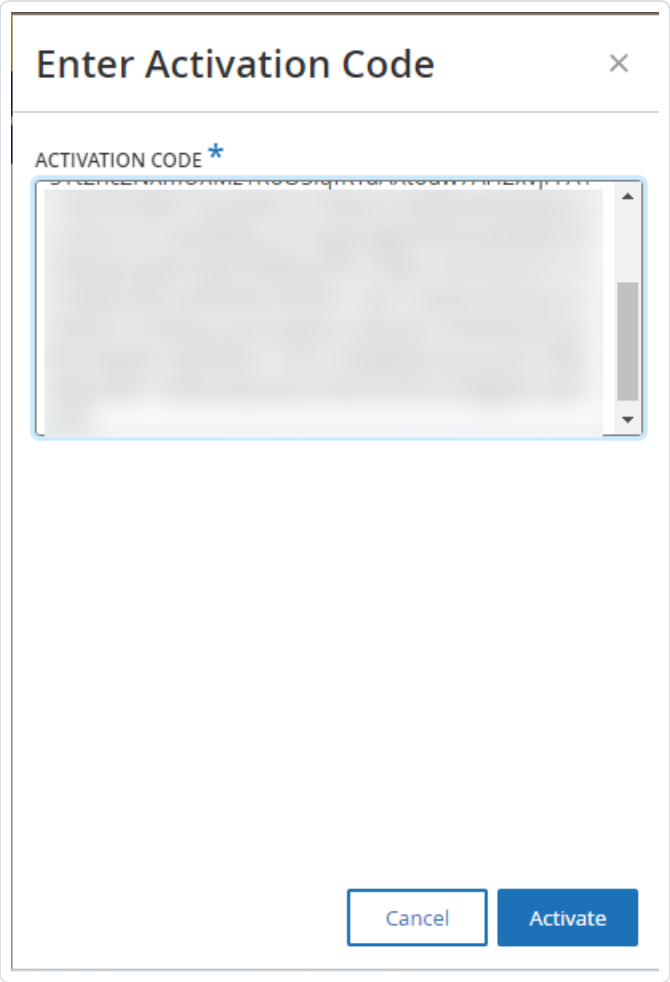
7. Pour copier le code d'activation, cliquez sur le bouton .

8. Revenez à l'onglet **Licence** dans OT Security et cliquez sur **Saisir le code d'activation**.



Le panneau latéral **Saisir le code d'activation** apparaît.

9. Dans la zone **Code d'activation**, collez votre code d'activation et cliquez sur **Activer**.



Le panneau latéral se referme et OT Security met à jour la licence.

Réinitialiser votre licence

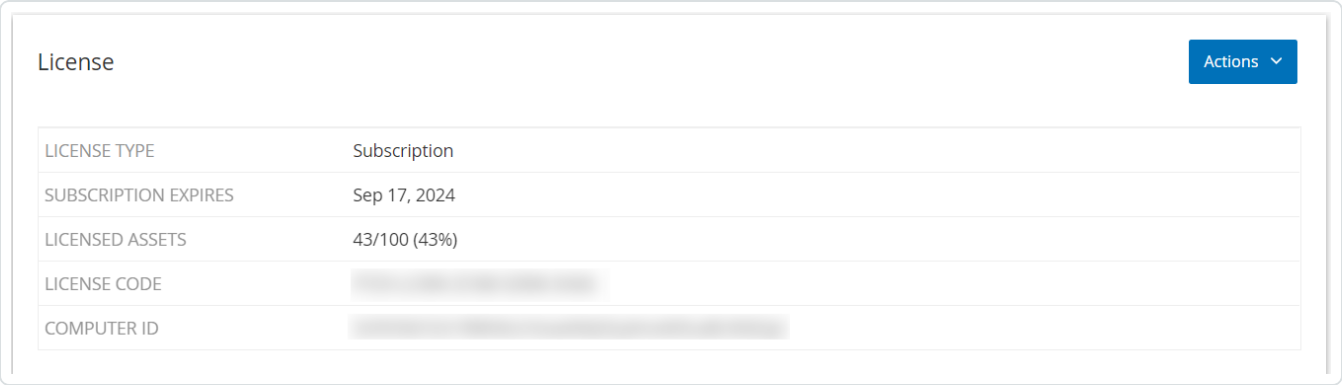
La réinitialisation de votre licence supprime votre licence actuelle du système et active une nouvelle licence, similaire à l'activation de la licence lors du premier démarrage de votre système. Si vous devez réinitialiser votre licence (c'est-à-dire si vous recevez une nouvelle licence), utilisez la procédure suivante.

Avant de commencer

- Votre responsable de compte Tenable doit déjà avoir émis votre nouvelle licence dans son système et vous avoir fourni un code de licence (20 lettres/chiffres).
- Vous devez avoir accès à Internet. Si vous ne pouvez pas connecter l'appareil OT Security à Internet, vous pouvez enregistrer la licence depuis n'importe quel PC.

Pour réinitialiser votre licence :

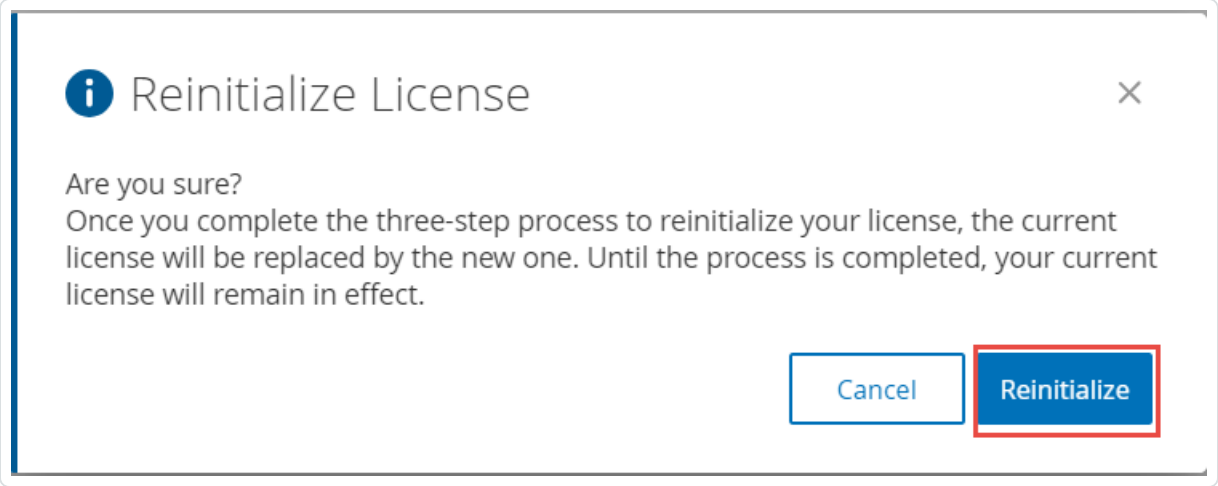
1. Accédez à **Paramètres locaux** > **Configuration système** > **Licence**.



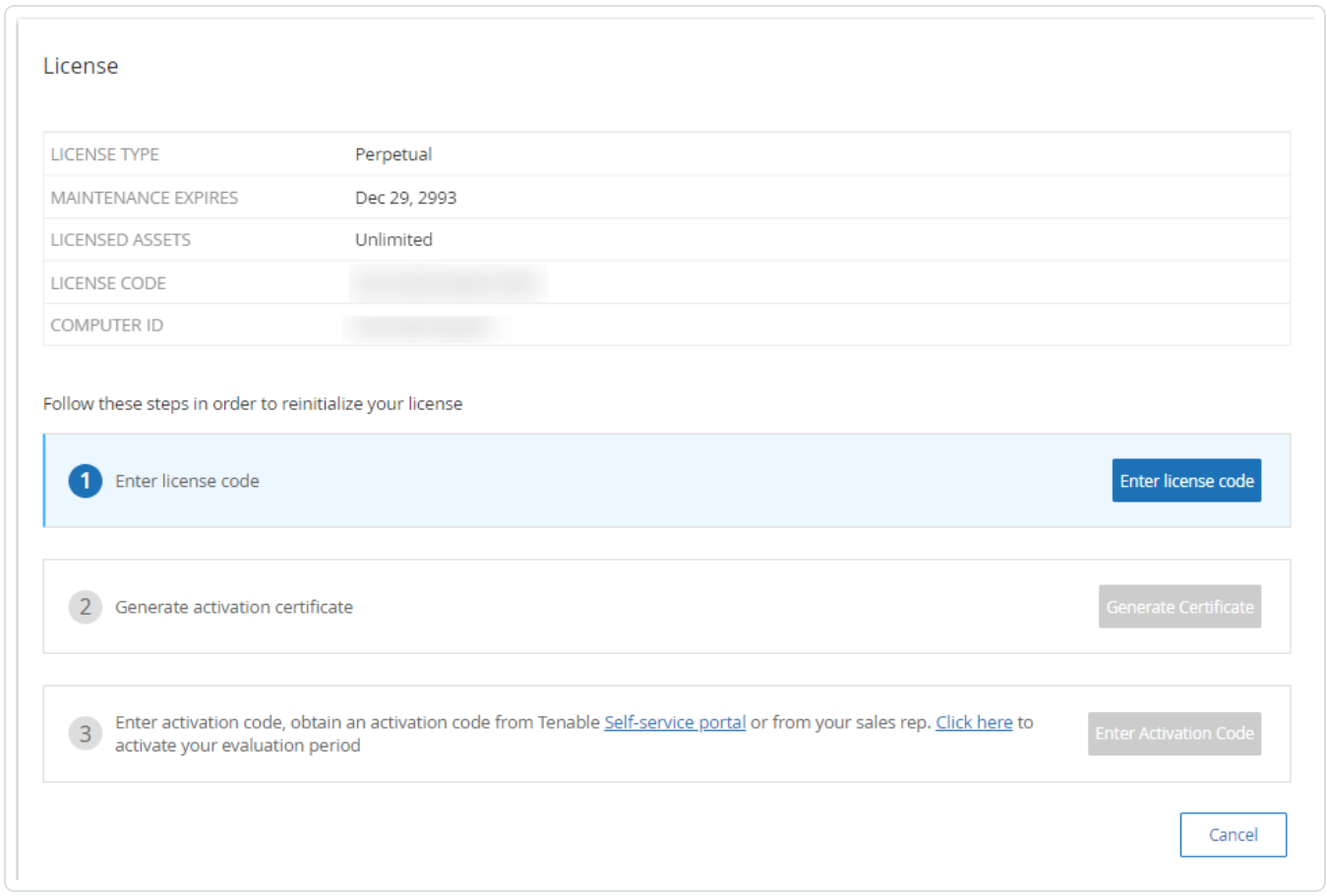
2. Dans le menu **Actions**, sélectionnez **Reinitialiser la licence**.

   Une fenêtre de confirmation apparaît.

3. Cliquez sur **Réinitialiser**.



   La fenêtre **Licence** apparaît avec les trois étapes de réinitialisation.



4. Suivez les étapes de démarrage du système pour activer votre licence. Voir Activer votre licence.

   Après avoir fourni votre **code d'activation**, votre licence actuelle est remplacée par votre nouvelle licence.

Que faire ensuite

Activer le système OT Security

Lancer OT Security

Objectif : démarrer le système et commencer à l'utiliser selon les besoins de votre solution OT Security.

Après avoir configuré Tenable Core + OT Security, activez le système pour commencer à utiliser OT Security.

1. Activer le système OT Security —Activez le système OT Security après avoir activé votre licence.
2. Utiliser OT Security —Configurez vos réseaux surveillés, la séparation des ports, les utilisateurs, les groupes, les serveurs d'authentification, etc. pour commencer à utiliser OT Security.

Activer le système OT Security

Une fois la procédure d'activation de la licence terminée, OT Security affiche le bouton **Activer**.

Activez OT Security pour pouvoir activer les fonctionnalités principales du système, telles que :

- Identification des assets dans le réseau
- Collecte et surveillance de tout le trafic réseau
- Journalisation des « communications » sur le réseau

Vous pouvez afficher toutes les données compilées et analysées à partir de ces fonctionnalités dans l'interface utilisateur.

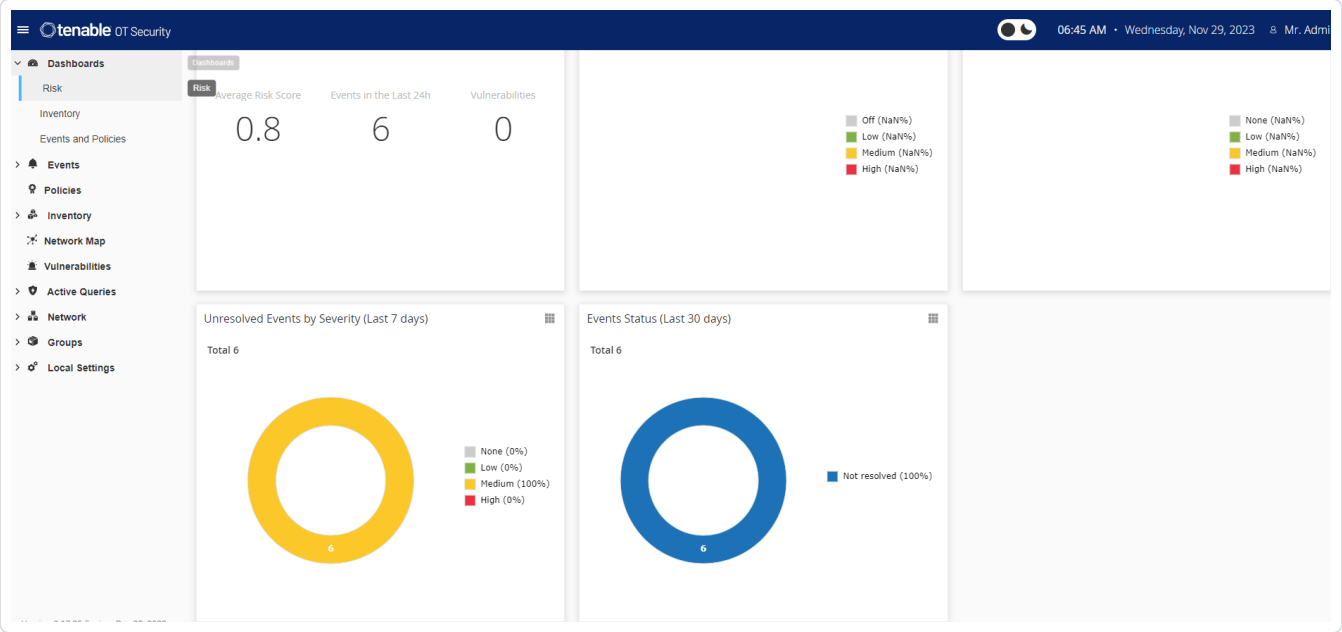
> **Remarque :** ce sont des processus continus qui se poursuivent au fil du temps. Par conséquent, l'affichage de résultats entièrement à jour peut prendre un certain temps.

Vous pouvez configurer et activer des fonctions supplémentaires telles que Requêtes actives dans la fenêtre **Paramètres locaux** de la console de gestion (interface utilisateur). Pour plus d'informations, voir Requêtes actives.

Pour activer OT Security :

1. Cliquez sur **Activer**.

   OT Security active le système et affiche la fenêtre **Dashboard** > **Risques**.



> **Remarque :** il faut quelques minutes au système pour identifier vos assets. Vous devrez peut-être actualiser la page pour commencer à afficher les données.

Commencer à utiliser OT Security

Après l'installation, vous pouvez configurer et utiliser OT Security.

Configurer les réseaux surveillés

Configurez les segments réseau à faire surveiller par OT Security et incluez toutes les zones pertinentes pour votre réseau. Voir Réseaux surveillés.

> **Remarque** : supprimez les réseaux surveillés inutiles. Vous pouvez masquer tous les assets que vous avez ajoutés à partir de ces réseaux. Pour plus d'informations, voir Masquer des assets.

Examiner et configurer les ports

Si vous ne l'avez pas encore fait, vous pouvez choisir de séparer les ports de gestion et de requête active.

Configurer les utilisateurs, les groupes et les serveurs d'authentification

Définissez vos Utilisateurs locaux et vos Groupes d'utilisateurs. Vous pouvez configurer des serveurs d'authentification externes ou utiliser SAML pour faciliter la connexion SSO.

Ajouter des services réseau

Ajoutez vos serveurs DNS et NTP. Vous pouvez également configurer des serveurs de messagerie et Syslog pour récupérer tous les événements critiques.

Activer les requêtes actives

Les requêtes actives représentent l'un des principaux avantages de OT Security. Elles vous permettent d'accéder directement à vos assets pour obtenir les détails et la visibilité les plus précis et quasiment en temps réel. Pour plus d'informations, voir Requêtes actives.

Découverte des assets actifs —Sondez et découvrez de manière proactive les assets silencieux ou ceux que le trafic de surveillance passive ne couvre pas.

Créer des scans Nessus

Configurez les scans Nessus pour les appareils informatiques de votre réseau OT Security. Les scans Tenable Nessus sont sécurisés et n'affectent que les assets informatiques découverts. Pour plus d'informations, voir Configurer les scans de plug-in Nessus.

Définir des sauvegardes

Configurez des sauvegardes système périodiques et choisissez de les enregistrer localement ou de les exporter vers un stockage distant. Pour plus d'informations, voir Application Data Backup and Restore (Sauvegarde et restauration des données d'application).

Obtenir des mises à jour

Assurez-vous de vérifier les mises à jour du flux et du système. Si votre système est hors ligne, assurez-vous d'effectuer périodiquement une mise à jour manuelle. Pour plus d'informations, voir

Mises à jour.

Optimiser

Lorsque OT Security est opérationnel, examinez les événements générés et optimisez vos politiques en fonction des exigences de votre environnement.

Intégrer

Intégrez OT Security à d'autres produits Tenable ou services tiers. Pour plus d'informations, voir Intégrations.

Installer le capteur OT Security

Remarque : cette section décrit la procédure de configuration d'un capteur versions 3.14 et supérieures.

L'installation du capteur OT Security nécessite d'appairer les capteurs avec la plateforme Core industrielle (ICP). Pour appairer les capteurs avec l'ICP OT Security, utilisez à la fois la console de gestion ICP et l'interface utilisateur Tenable Core du capteur.

Vous pouvez activer l'approbation automatique des demandes d'appairage entrantes ou la désactiver et autoriser uniquement l'approbation manuelle de chaque nouvelle demande d'appairage de capteur.

Avant de commencer

Assurez-vous que les conditions suivantes sont remplies :

- Le matériel du capteur est correctement installé (voir Configurer le capteur).
- Le capteur est connecté à votre commutateur réseau (voir Connecter le capteur au réseau).
- Le capteur possède sa propre adresse IPv4 statique (voir Accéder à l'assistant de configuration du capteur).
- Le capteur est connecté à la plateforme Tenable Core et vous disposez d'un nom d'utilisateur et d'un mot de passe pour vous connecter à l'interface utilisateur Core. Pour plus d'informations sur l'utilisation de l'interface utilisateur Tenable Core, voir le Guide de l'utilisateur Tenable Core + Tenable OT Security.
- Vous disposez d'un certificat valide dans la console ICP (voir Certificat).

Remarque : Tenable recommande de créer un utilisateur ICP dédié avec un rôle d'administrateur pour le processus d'appairage des capteurs, afin d'éviter les interruptions de la connectivité (voir Ajout d'utilisateurs locaux). Vous pouvez ajouter un nouvel administrateur pour appairer plusieurs capteurs.

Remarque : pour plus d'informations sur l'application de mises à jour hors ligne à votre machine Tenable Core, voir Update Tenable Core Offline (Mettre à jour Tenable Core hors ligne).

Appairer le capteur

Pour appairer un capteur v.3.14 ou ultérieure avec l'ICP :

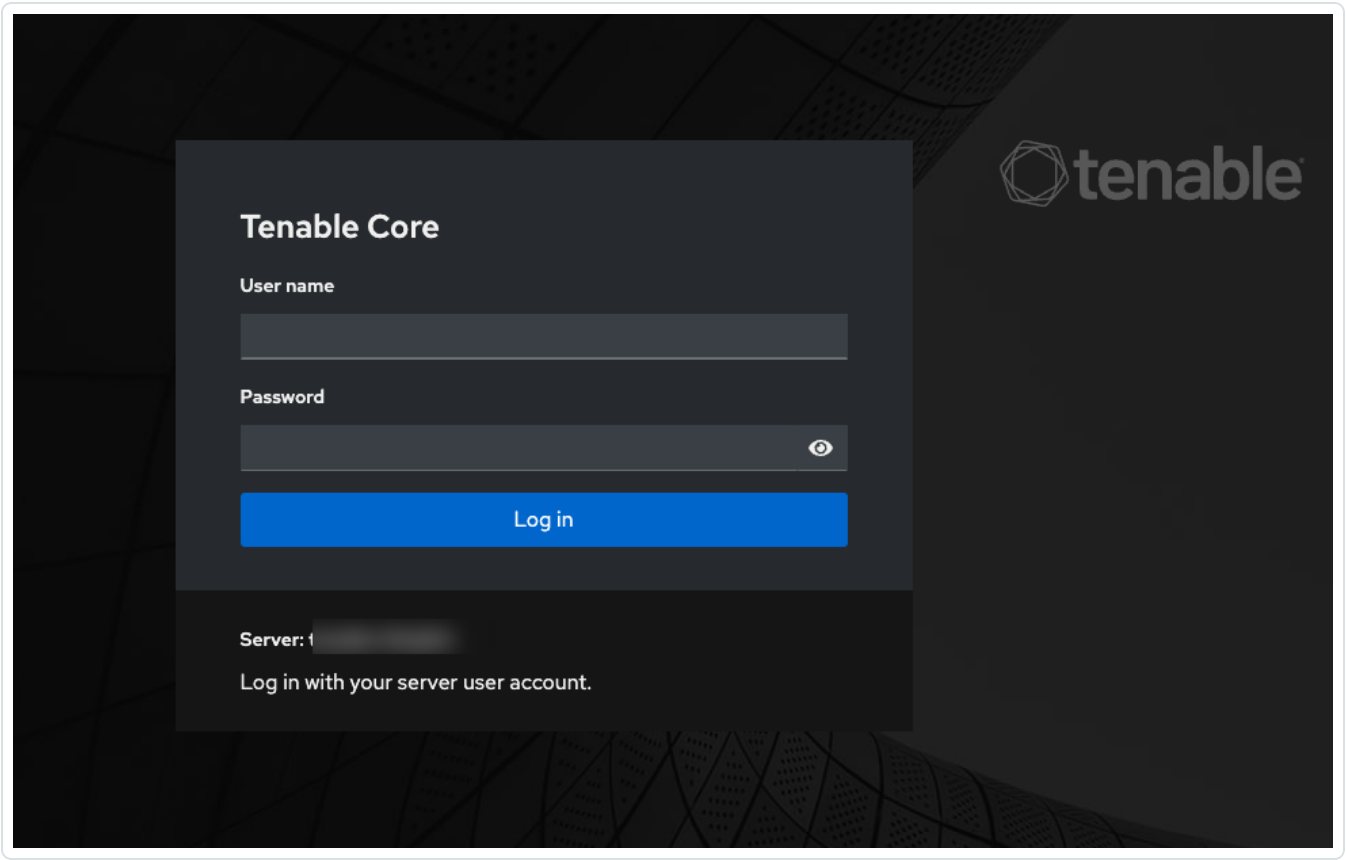
1. Dans la console de gestion ICP (interface utilisateur), accédez à la fenêtre **Paramètres locaux** > **Capteurs**.

2. Pour activer l'approbation automatique de l'appairage de capteurs, vous devez **activer** l'option **Approuver automatiquement les demandes d'appairage des capteurs** en cliquant sur le curseur qui se trouve en haut de la page. Si vous ne le faites pas, vous devrez approuver manuellement toutes les demandes d'appairage.

3. Ouvrez un nouvel onglet, en laissant l'onglet ICP ouvert, puis saisissez **<Sensor IP>:8000** pour ouvrir l'interface utilisateur Tenable Core du capteur.

   Remarque : l'accès à l'interface utilisateur de Tenable Core nécessite la dernière version de Chrome.

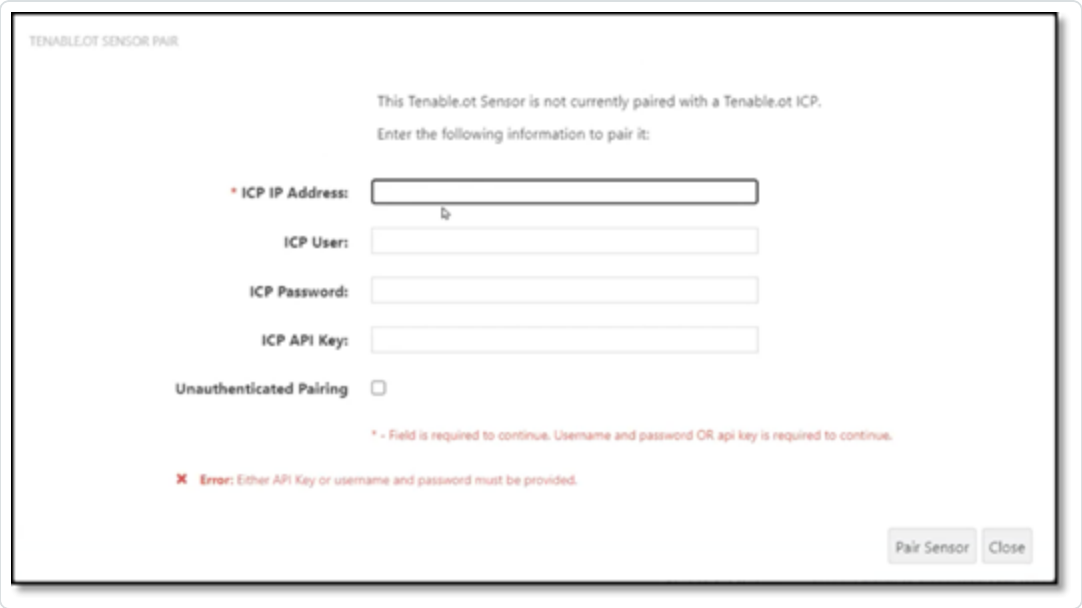
4. Dans la fenêtre de connexion à la console Tenable Core, saisissez votre **nom d'utilisateur** et votre **mot de passe**, cochez la case **Reuse my password for privileged tasks** (Réutiliser mon mot de passe pour les tâches privilégiées) et cliquez sur **Log In** (Connexion).



Important : si vous ne sélectionnez pas **Reuse my password for privileged tasks** (Réutiliser mon mot de passe pour les tâches privilégiées) lors de la connexion, vous ne pourrez pas redémarrer le service des capteurs.

5. Dans la barre de menu de navigation, cliquez sur **OT Security Sensor** (Capteur Tenable OT Security).

   La fenêtre **OT Security Sensor Pair** (Appairage des capteurs Tenable OT Security) apparaît.



Remarque : la fenêtre **Tenable OT Security Sensor Pair** (Appairage des capteurs Tenable OT Security) n'apparaît que lors du premier chargement de la page. Pour ouvrir la fenêtre après cela, cliquez sur le bouton dans la section **Pairing Info** (Informations d'appairage) de la console **Tenable Core**.

6. Dans la zone **ICP IP Address** (Adresse IP de l'ICP), saisissez l'adresse IPv4 de l'ICP avec laquelle vous souhaitez appairer ce capteur.

7. Pour utiliser un appairage non authentifié (non chiffré), sélectionnez **Unauthenticated Pairing** (Appairage non authentifié) et passez à l'étape 8.

   Remarque : les capteurs qui utilisent l'**appairage non authentifié** ne peuvent que scanner passivement leurs segments de réseau, et l'ICP ne peut pas les gérer pour envoyer des requêtes actives.

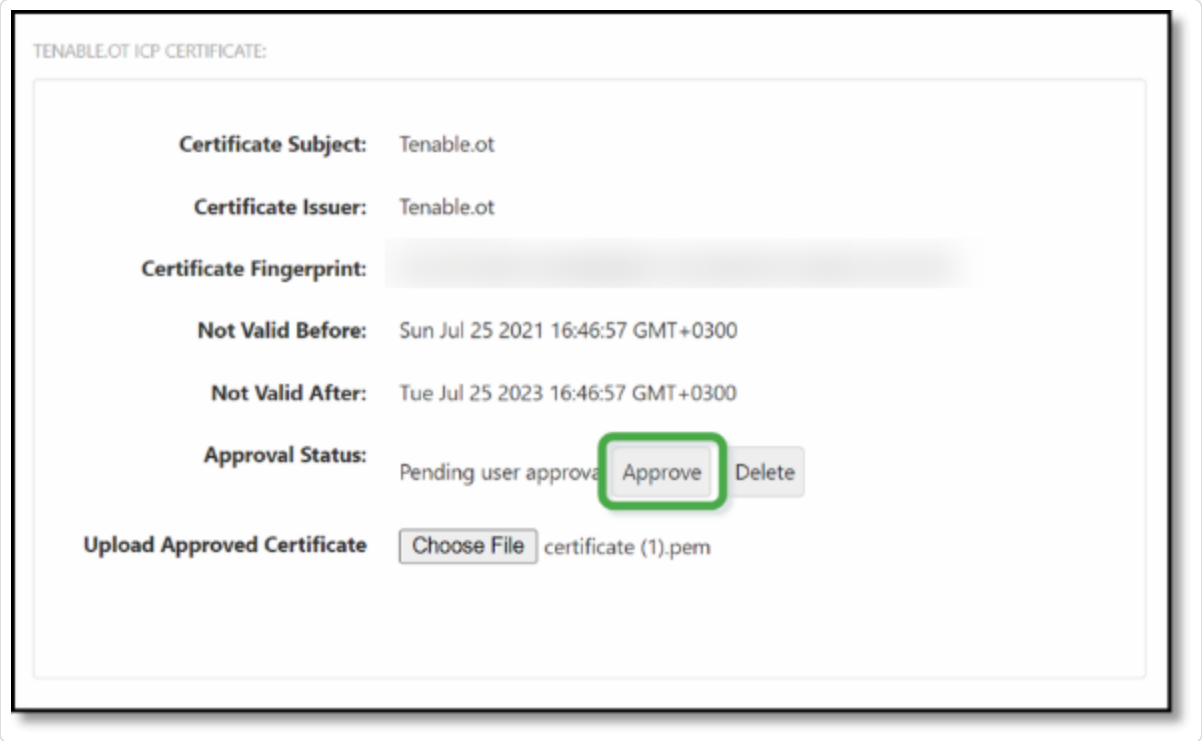
8. Pour authentifier l'appairage, effectuez l'une des opérations suivantes :

   - Saisissez le nom d'utilisateur ICP dans la zone **ICP User** (Utilisateur ICP) et le mot de passe ICP dans la zone **ICP Password** (Mot de passe ICP).
   - Dans la zone **ICP API Key** (clé API ICP), saisissez une clé API pour l'ICP.

   Remarque : Tenable recommande de créer un utilisateur ICP dédié pour appairer les capteurs, afin d'assurer la connectivité pendant le processus d'appairage (voir Ajout d'utilisateurs locaux).

Remarque : la méthode d'authentification basée sur un nom d'utilisateur et un mot de passe offre l'avantage d'utiliser des informations d'authentification qui n'expirent pas, contrairement à une clé API.

9. Cliquez sur **Pair Sensor** (Appairer le capteur).
10. Pour utiliser un certificat proposé par l'ICP :
    a. Dans **Tenable Core**, dans la section **Certificat ICP Tenable**, sous **Statut d'approbation**, attendez que les informations du certificat soient chargées.



    b. Cliquez sur **Approuver** pour approuver le certificat.
    c. Dans la fenêtre **Confirm Accept Tenable OT Security Server Certificate** (Confirmer l'acceptation du certificat du serveur Tenable OT Security), cliquez sur **Accept This Certificate** (Accepter ce certificat).

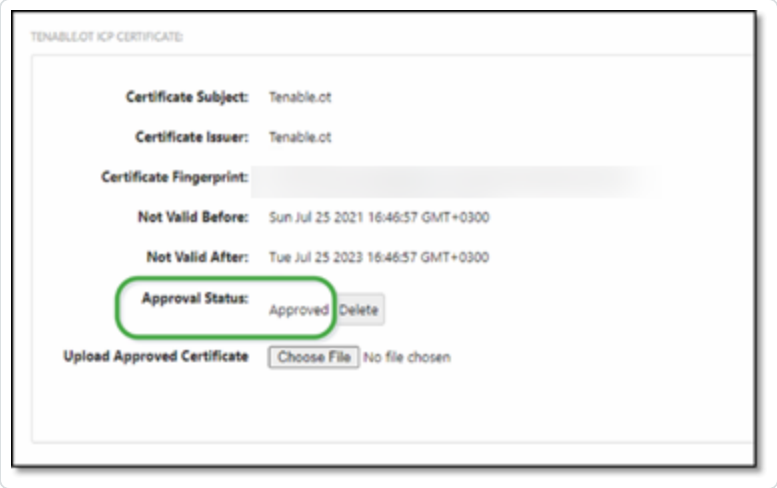
    Si vous préférez importer manuellement un certificat :

    a. Dans la console **Tenable ICP**, suivez la procédure décrite dans la section **Génération d'un certificat HTTPS**.

b. Dans **Tenable Core**, dans la section **Tenable ICP Certificate** (Certificat ICP Tenable), sous **Upload Approved Certificate** (Charger le certificat approuvé), cliquez sur **Choose File** (Choisir un fichier).

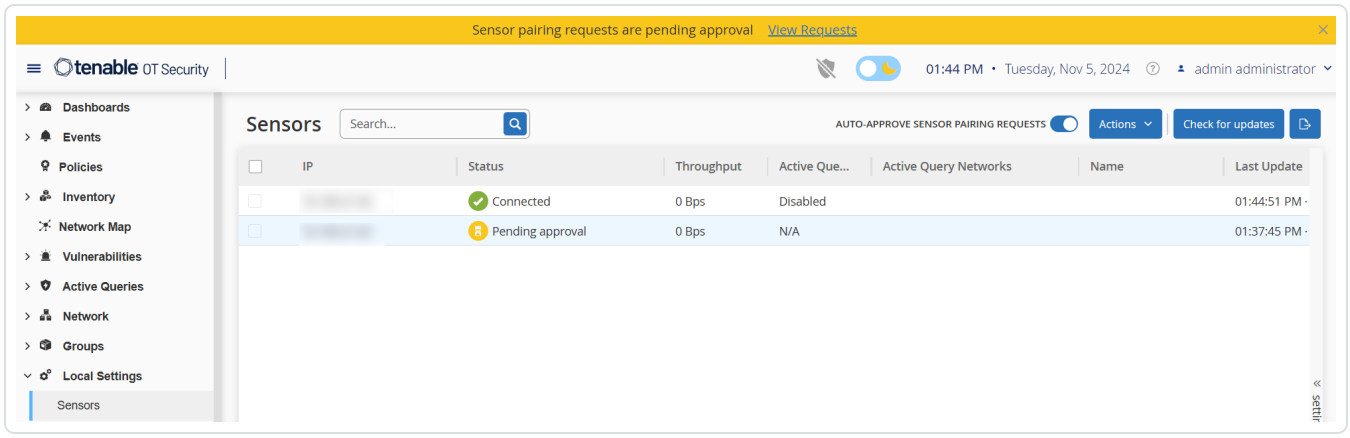
c. Accédez au fichier de certificat `.pem` à charger.

Une fois qu'un certificat valide est chargé, son **statut d'approbation** (Approval Status) dans le tableau **OT Security ICP Certificate** (Certificat ICP Tenable OT Security) apparaît comme **Approved** (Approuvé).

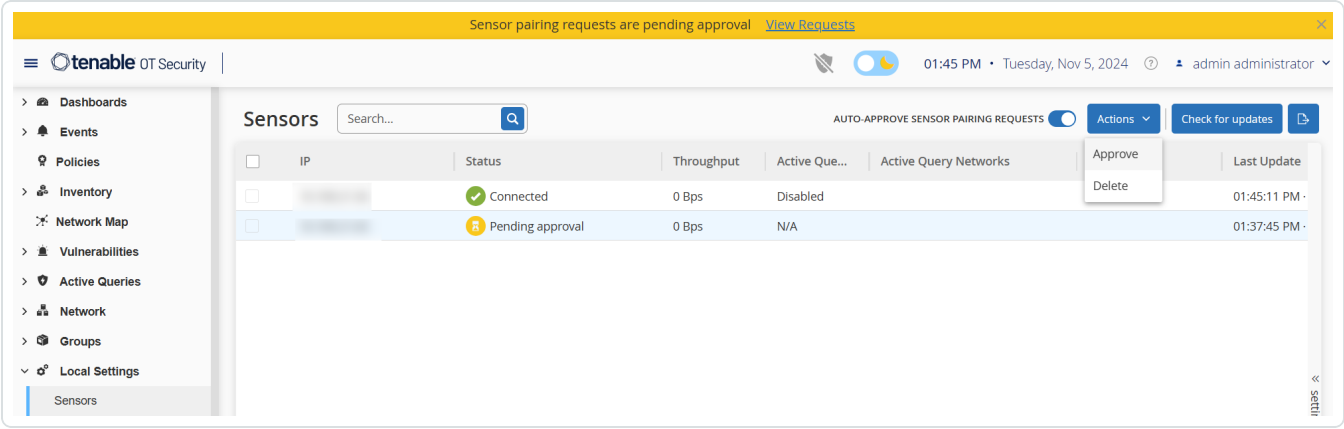


11. Dans l'interface utilisateur ICP, accédez à **Paramètres locaux** > **Capteurs**.

OT Security affiche le nouveau capteur dans le tableau avec le statut **En attente d'approbation**.



12. Cliquez sur la ligne du capteur, puis sur **Actions** (ou effectuez un clic droit sur la ligne) et sélectionnez **Approuver**.



Le **statut** doit passer à **Connecté**, indiquant que l'appairage a réussi. Les autres statuts possibles sont :

- **Connecté (non authentifié)** —Le capteur est connecté en mode non authentifié. Le capteur ne peut exécuter qu'une détection de réseau passive.
- **En pause** —Le capteur est correctement connecté, mais a été mis en pause.
- **Déconnecté** —Le capteur n'est pas connecté. Pour un capteur authentifié, cela peut résulter d'une erreur dans le processus d'appairage. Par exemple : erreur de tunnel ou problème d'API.
- **Connecté (erreur de tunnel)** —L'appairage est réussi, mais la communication sur le tunnel est inopérante. Vérifiez la connectivité du port 28304 entre le capteur et l'ICP. Pour plus d'informations, voir Considérations sur le pare-feu.

Une fois que OT Security a terminé l'appairage d'un capteur authentifié, vous pouvez configurer les requêtes actives pour qu'elles s'exécutent sur le capteur. Voir Requêtes actives.

> **Remarque :** une fois l'appairage terminé, Tenable recommande d'utiliser uniquement la page ICP pour gérer le capteur, et non pas l'interface utilisateur de Tenable Core.

Configurer le capteur

Il existe deux modèles de capteur : le capteur pour montage en rack et le capteur configurable, comme décrit dans OT Security Sensor. Le modèle pour montage en rack peut être monté sur un rack standard de 19 pouces ou posé sur une surface plane. Le modèle configurable peut être installé sur un rail DIN ou monté sur un rack 19 pouces standard (à l'aide du kit d'adaptation « oreilles de montage »).

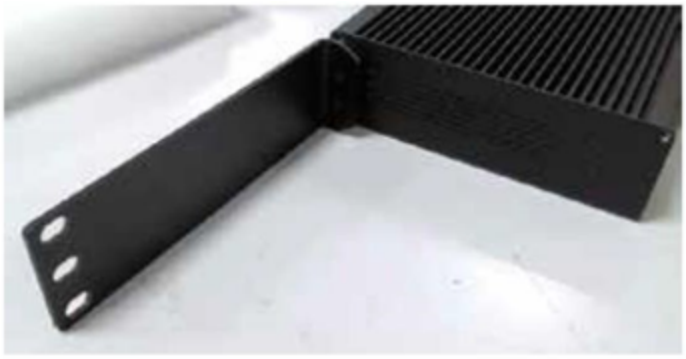
Configurer un capteur pour montage en rack

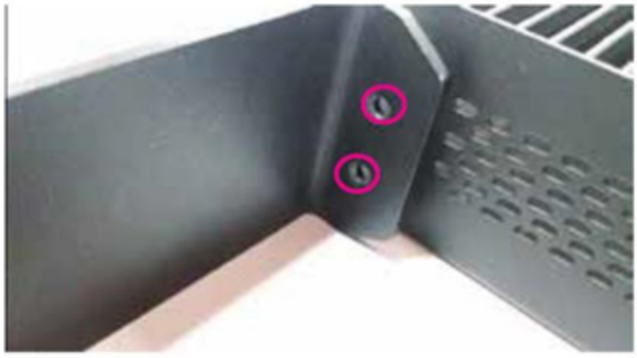
Vous pouvez monter le capteur sur un rack standard de 19 pouces ou le poser sur une surface plane (comme un bureau).

Montage en rack (modèle pour montage en rack)

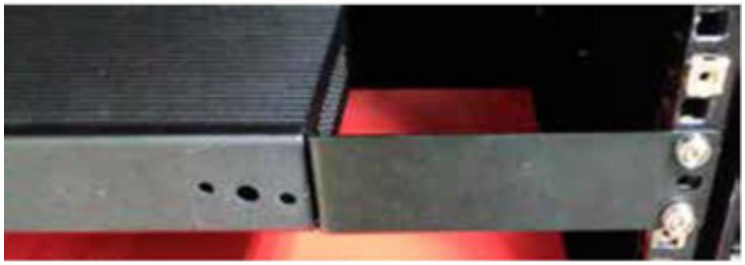
Pour monter le Capteur OT Security sur un rack standard de 19 pouces :

1. Fixez les supports en L aux trous de vis de chaque côté du capteur, comme indiqué dans l'image suivante.





2. Insérez deux vis de chaque côté et fixez-les avec un tournevis pour maintenir les supports en place.
3. Insérez le capteur avec les supports dans un emplacement 1U disponible du rack.
4. Installez l'unité en fixant les supports de montage en rack (fournis) au cadre du rack, à l'aide des vis adéquates (non fournies).



Important :

- Assurez-vous que le rack est électriquement relié à la terre.
- Assurez-vous que l'entrée d'air du ventilateur de refroidissement (situé sur le panneau arrière) et les orifices de ventilation (sur le panneau supérieur) ne sont pas obstrués.

5. Branchez le câble d'alimentation CA (fourni) sur le port d'alimentation du panneau arrière, puis branchez le câble sur l'alimentation CA (secteur).

Surface plane

Pour installer le Capteur OT Security sur une surface plane :

1. Placez le capteur sur une surface sèche, plane et nivelée (un bureau, par exemple).

Important :

- Assurez-vous que le plan de travail est plat et sec.
- Assurez-vous que l'entrée d'air du ventilateur de refroidissement (situé sur le panneau arrière) et les orifices de ventilation (sur le panneau supérieur) ne sont pas obstrués.

2. Si l'unité est placée dans une pile d'autres appliances électriques, assurez-vous qu'il y a suffisamment d'espace derrière le ventilateur de refroidissement (situé sur le panneau arrière) pour permettre une ventilation et un refroidissement appropriés.
3. Branchez le câble d'alimentation CA (fourni) sur le port d'alimentation du panneau arrière, puis branchez le câble sur l'alimentation CA (secteur).

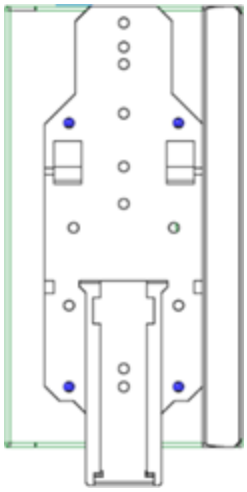
Configurer un capteur configurable

Le capteur configurable peut être installé sur un rail DIN ou monté sur un rack de 19 pouces standard (à l'aide du kit d'adaptation « oreilles de montage »).

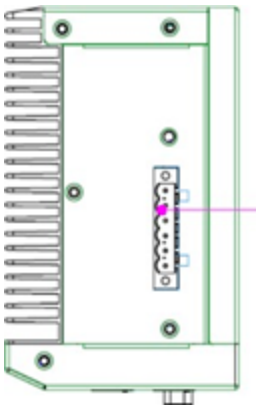
Montage sur rail DIN

Pour monter le capteur OT Security configurable sur un rail DIN standard :

1. Utilisez le support situé à l'arrière du capteur pour le monter sur un rail DIN.



2. Connectez l'alimentation en utilisant l'une des méthodes suivantes :
    - **Alimentation CC** – Connectez le câble d'alimentation CC au capteur en insérant le connecteur Phoenix Contact 12-36 V CC à 6 broches sur le côté du capteur et en serrant les vis intégrées en haut et en bas du connecteur. Ensuite, connectez l'autre extrémité du câble à une source d'alimentation CC.



- **Alimentation CA** – Connectez l'alimentation CA au capteur en insérant le connecteur Phoenix Contact 12-36 V CC à 6 broches sur le côté du capteur et en serrant les vis intégrées en haut et en bas du connecteur.

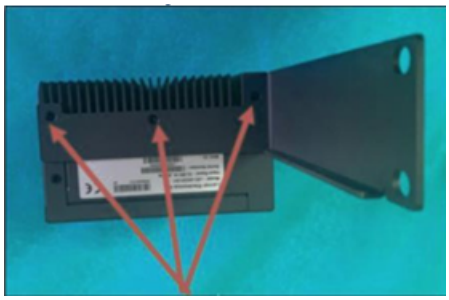
Ensuite, insérez le câble d'alimentation CA (fourni) dans le bloc d'alimentation et branchez l'autre extrémité dans une prise CA.

Montage en rack (modèle configurable)

Un capteur configurable peut être fixé à un rack de montage à l'aide des « oreilles de montage » fournies.

Pour monter le capteur configurable sur un rack standard (19 pouces) :

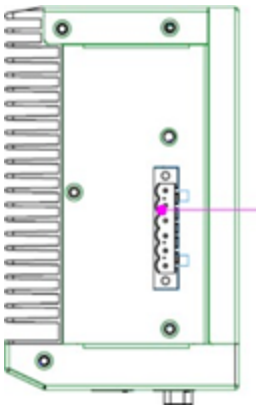
1. Préparez l'unité pour le montage en rack :
    a. Retirez les 3 vis de chaque côté de l'appareil.
    b. Fixez les « oreilles de montage » des deux côtés de l'appareil à l'aide de nouvelles vis (fournies).



2. Insérez l'unité serveur dans un emplacement 1U disponible du rack.

> **Remarque :**
>
> - Assurez-vous que le rack est électriquement relié à la terre.
> - Assurez-vous que l'entrée d'air du ventilateur de refroidissement (situé sur le panneau arrière) et les orifices de ventilation (sur le panneau supérieur) ne sont pas obstrués.

3. Fixez l'unité au rack en fixant les « oreilles de montage » au cadre du rack à l'aide des vis de montage (fournies).
4. Connectez l'alimentation en utilisant l'une des méthodes suivantes :
    - **Alimentation CC** – Connectez le câble d'alimentation CC au capteur en insérant le connecteur Phoenix Contact 12-36 V CC à 6 broches sur le côté du capteur et en serrant les vis intégrées en haut et en bas du connecteur. Ensuite, connectez l'autre extrémité du câble à une source d'alimentation CC.



- **Alimentation CA** – Connectez l'alimentation CA au capteur en insérant le connecteur Phoenix Contact 12-36 V CC à 6 broches sur le côté du capteur et en serrant les vis intégrées en haut et en bas du connecteur.

Ensuite, insérez le câble d'alimentation CA (fourni) dans le bloc d'alimentation et branchez l'autre extrémité dans une prise CA.

Connecter le capteur au réseau

Le Capteur OT Security est utilisé pour collecter et transférer le trafic réseau vers l'appliance OT Security. Pour assurer la surveillance du réseau, connectez l'unité à un port de mise en miroir sur le commutateur réseau, lui-même connecté aux contrôleurs/PLC pertinents.

Pour gérer le capteur, connectez l'unité à un réseau. Il peut s'agir d'un réseau différent de celui utilisé pour surveiller le réseau.

Pour connecter le capteur OT Security à monter en rack au réseau :

1. Sur le Capteur OT Security, connectez le câble Ethernet (fourni) au **port 1**.
2. Connectez le câble à un port standard du commutateur réseau.
3. Sur l'unité, connectez un autre câble Ethernet (fourni) au **port 2**.
4. Connectez le câble à un port de mise en miroir du commutateur réseau.

Pour connecter le capteur OT Security configurable au réseau :

1. Sur le Capteur OT Security, connectez le câble Ethernet (fourni) au **port 1**.
2. Connectez le câble à un port standard du commutateur réseau.
3. Sur l'unité, connectez un autre câble Ethernet (fourni) au **port 3**.
4. Connectez le câble à un port de mise en miroir du commutateur réseau.

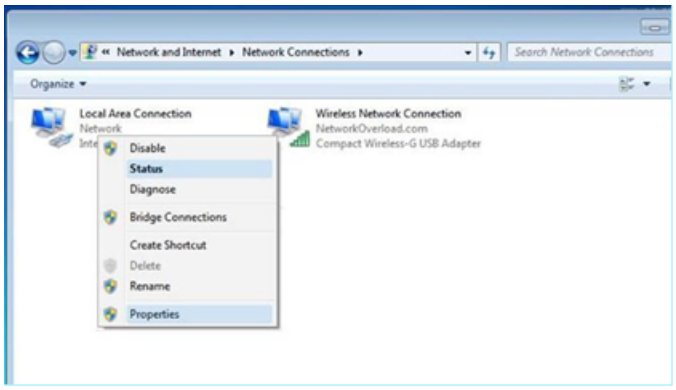
Accéder à l'assistant de configuration du capteur

Pour se connecter à la console de gestion :

1. Effectuez l'une des actions suivantes :
   - Connectez le poste de travail de la console de gestion (PC, ordinateur portable, etc.) directement au port 1du Capteur OT Security à l'aide du câble Ethernet.
   - Connectez le poste de travail de la console de gestion au commutateur réseau.
2. Assurez-vous que le poste de travail de la console de gestion fait partie du même sous-réseau que le Capteur OT Security (qui est 192.168.1.5) ou qu'il peut être routé vers l'unité.
3. Utilisez la procédure suivante pour configurer une adresse IP statique (vous devez configurer une adresse IP statique pour vous connecter au Capteur OT Security) :
   a. Accédez à **Réseau et Internet** > **Centre Réseau et partage** > **Modifier les paramètres de la carte**.

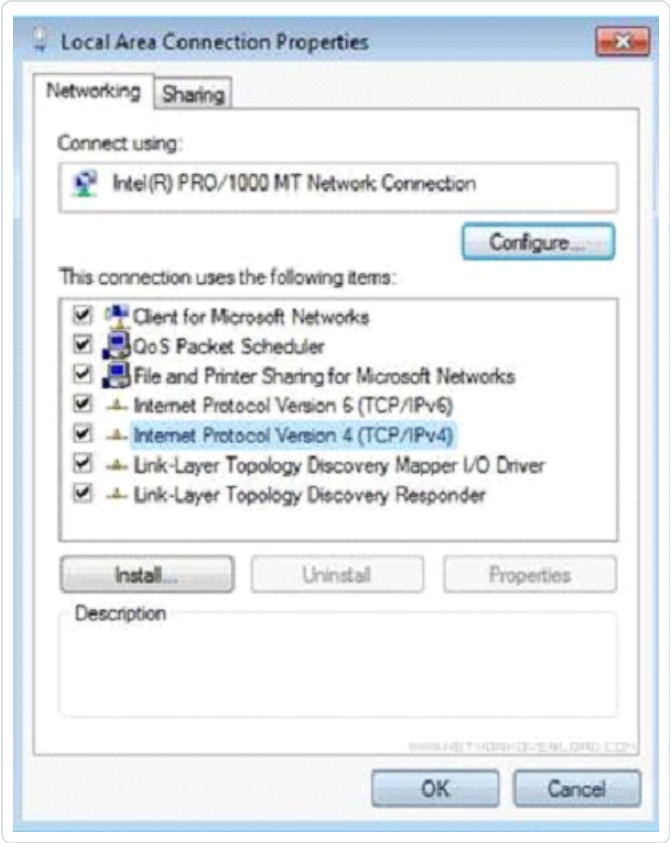
      > **Remarque :** la navigation peut varier légèrement selon la version de Windows.

      La fenêtre **Connexions réseau** apparaît.



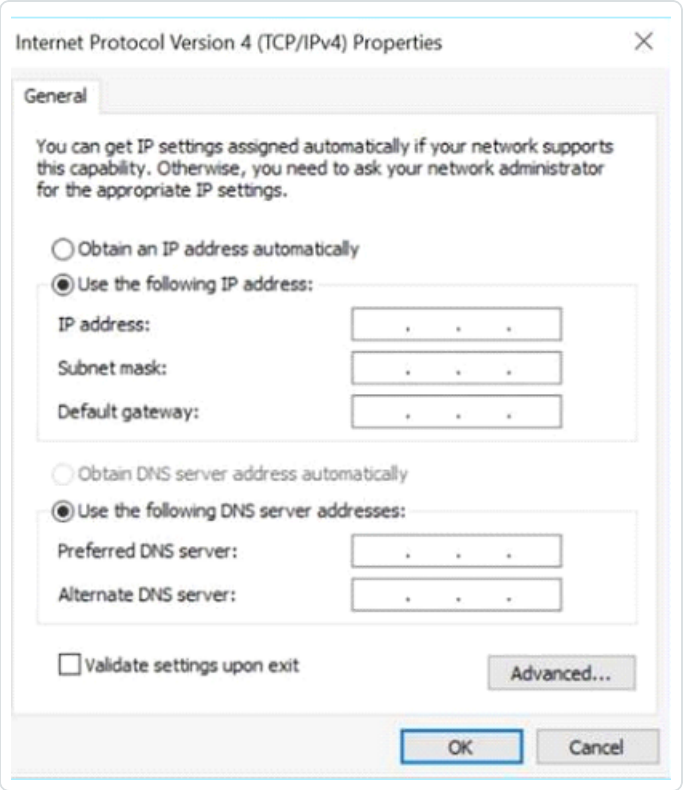
b. Effectuez un clic droit sur **Connexions au réseau local** et sélectionnez **Propriétés**.

La fenêtre **Connexions au réseau local** apparaît.



c. Sélectionnez **Protocole Internet version 4 (TCP/ IPv4)** et cliquez sur **Propriétés**.

La fenêtre **Propriétés d'Internet Protocol Version 4 (TCP/ IPv4)** apparaît.



d. Sélectionnez **Utiliser l'adresse IP suivante**.

e. Dans la zone Adresse IP, saisissez **192.168.1.10**.

f. Dans la zone **Masque de sous-réseau**, saisissez 255.255.255.0.

g. Cliquez sur **OK**.

OT Security applique les nouveaux paramètres.

4. Dans votre navigateur web Chrome, accédez à https://192.168.1.5:8000.

> **Remarque :** l'interface utilisateur n'est accessible qu'à partir d'un navigateur Chrome. Utilisez la dernière version de Chrome.

5. Appairez le capteur.

Restaurer la sauvegarde à l'aide de la CLI

Vous pouvez restaurer votre OT Security à l'aide de la CLI ou via l'interface Tenable Core. Pour plus d'informations sur la restauration d'une sauvegarde via l'interface utilisateur Tenable Core, voir

Restore a Backup (Restaurer une sauvegarde) dans le Guide de l'utilisateur Tenable Core + Tenable OT Security. Pour effectuer une restauration à l'aide de la CLI, effectuez les étapes suivantes.

> **Remarque** : vous ne pouvez restaurer que les sauvegardes effectuées à l'aide de l'utilitaire de sauvegarde Tenable Core. Les sauvegardes plus anciennes de OT Security, antérieures à la version 3.18, ne sont pas compatibles. Si vous essayez de restaurer à partir d'une sauvegarde capturée dans une ancienne version de OT Security, antérieure à la version 3.18, contactez l'assistance pour connaître les instructions et les commandes nécessaires.

Avant de commencer

- Vérifiez que vous disposez bien des fichiers `.tar` de sauvegarde à restaurer.

  > **Remarque** : vous pouvez télécharger les fichiers de sauvegarde OT Security à partir de la page **Backup/ Restore** (Sauvegarder/ Restaurer) dans Tenable Core. Pour plus d'informations, voir Restore a Backup (Restaurer une sauvegarde) dans le Guide de l'utilisateur Tenable Core + Tenable OT Security. Exemple de fichier de sauvegarde OT Security : `tenable-ot-tenable-s2cc78kg-2024-03-21T135648.tar`.

Pour restaurer votre sauvegarde OT Security à l'aide de la CLI :

1. Effectuez l'une des opérations suivantes afin d'accéder au système ICP :
   - Connectez-vous à Tenable Core et accédez au terminal.
   - Connectez-vous à l'aide de SSH.
2. Dans le terminal, exécutez la commande suivante :

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

Où :

- `/home/admin/my-tc-ot-backup.tar` est l'emplacement des fichiers de sauvegarde.

> **Remarque** : le processus est très long car il restaure la sauvegarde avant la fin de la commande. Vous pouvez afficher la progression de la restauration à partir de **Backup/ Restore** (Sauvegarder/ Restaurer) > **Backup/ Restore Logs** (Sauvegarder/ Restaurer les journaux) > **Restore logs** (Restaurer les journaux) dans l'interface utilisateur Tenable Core ou en exécutant la commande suivante :
>
> `journalctl -xf tenablecore.restorelocal@$(systemd-escape /home/admin/my-tc-ot-`

backup.tar)

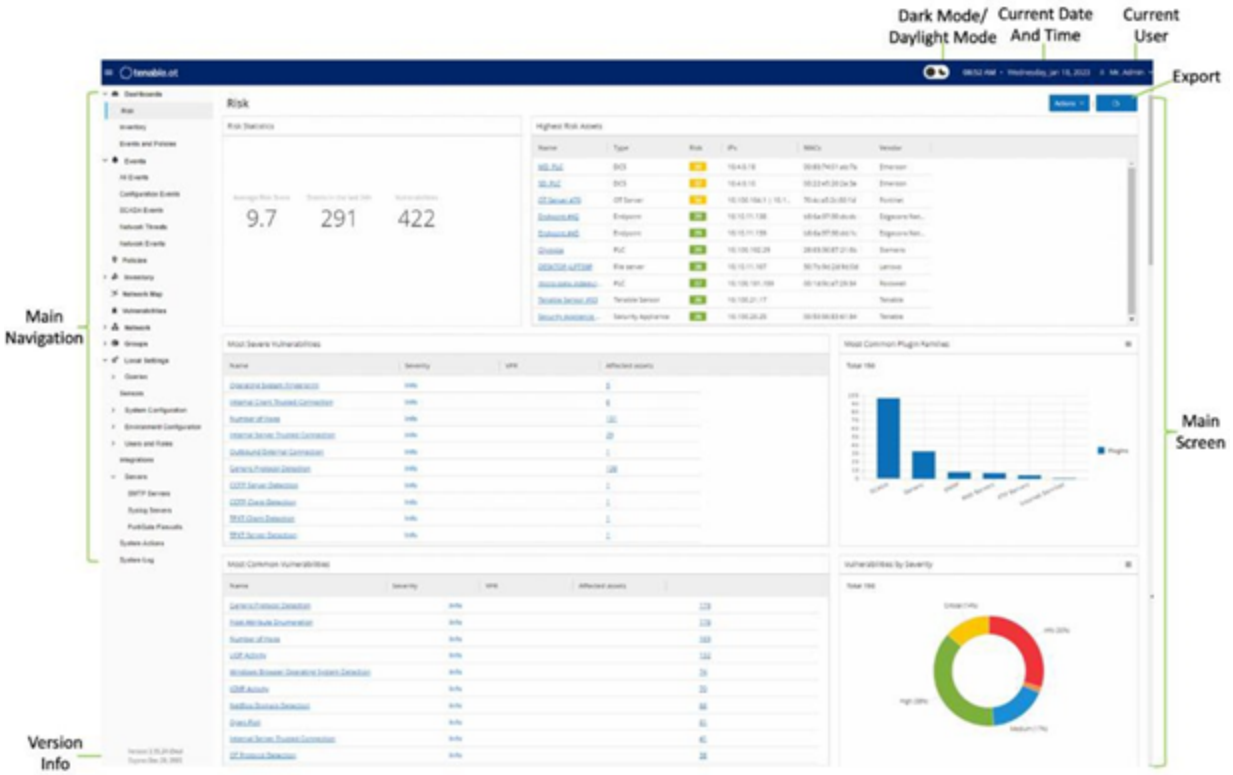
Où : `/home/admin/my-tc-ot-backup.tar` est l'emplacement des fichiers de sauvegarde.

OT Security est restauré et vous pouvez accéder à l'application. Pour vérifier que OT Security est en cours d'exécution, utilisez votre navigateur pour vous connecter à l'interface utilisateur OT Security via le port 443 (HTTPS).

Éléments de l'interface utilisateur de la console de gestion

L'interface utilisateur de la console de gestion permet d'accéder facilement aux données importantes découvertes par OT Security concernant la gestion des assets, l'activité du réseau et les événements de sécurité. Vous pouvez utiliser l'interface utilisateur pour configurer la fonctionnalité de la plateforme OT Security en fonction de vos besoins.

Principaux éléments de l'interface utilisateur



Le tableau suivant décrit les principaux éléments de l'interface utilisateur.

Élément de l'interface utilisateur	Description
Navigation principale	Menu de navigation principal. Cliquez sur l'icône pour afficher/masquer le menu de navigation principal.
Requêtes actives	Indique si les **requêtes actives** sont activées ou désactivées.
Mode sombre/ Mode clair	Permet de basculer la palette de couleurs en mode sombre ou en mode clair.
Date et heure en cours	Affiche la date et l'heure actuelles enregistrées dans le système.
Centre de ressources	Centre de ressources OT Security.
Nom d'utilisateur en cours	Affiche le nom de l'utilisateur actuellement connecté au système. Cliquez sur la flèche du bas pour afficher les options de menu : **À propos** (affiche des informations sur le logiciel) et **Déconnexion**. Après avoir activé OT Security, vous pouvez afficher votre identifiant client Tenable dans la vue **À propos**. Cet identifiant client est requis lorsque vous contactez l'assistance technique ou les équipes en charge de la réussite client.
Informations sur la licence	Affiche la version du logiciel OT Security et la date d'expiration de la licence.
Écran principal	Affiche l'écran que vous avez sélectionné dans la navigation principale.
Exporter	Télécharge un PDF du dashboard.

Activer ou désactiver le mode sombre

Vous pouvez utiliser la palette de couleurs du **mode sombre** sur tous les écrans en activant ce mode.

Pour activer ou désactiver le mode sombre :

1. Cliquez sur le curseur (mode sombre) en haut de la fenêtre.

   OT Security applique le paramètre sélectionné à tous les écrans.

2. Pour restaurer le paramètre Mode clair, cliquez sur le curseur (mode clair).

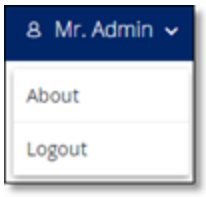
Vérifier la version actuelle du logiciel

Vous pouvez vérifier la version du logiciel en utilisant l'icône de profil utilisateur dans le coin supérieur droit de la barre d'en-tête.

Pour afficher la version actuelle du logiciel :

1. Dans la barre d'en-tête principale, cliquez sur l'icône dans le coin supérieur droit.

   OT Security affiche le menu utilisateur.

2. Cliquez sur **À propos**.

   OT Security affiche la version actuelle du logiciel.

Naviguer dans OT Security

Vous pouvez accéder aux pages principales suivantes à partir du panneau de navigation de gauche :

- **Dashboards** – Affiche des widgets contenant des graphes et des tableaux qui donnent une vue générale de l'inventaire et de la sécurité de votre réseau. Il existe des dashboards distincts pour les risques, l'inventaire, les événements et les politiques. Voir Dashboards.
- **Événements** – Affiche tous les événements qui se sont produits à la suite de violations de politique. La page **Tous les événements** comporte des sections distinctes pour chaque type d'événement. Par exemple : Événements de configuration, Événements SCADA, Menaces réseau ou Événements réseau. Voir Événements.
- **Politiques** – Affichez, modifiez et activez les politiques dans le système. Voir Politiques.
- **Inventaire** – Affiche un inventaire de tous les assets découverts, permettant une gestion complète des assets, la surveillance de l'état de chaque asset et la visualisation des événements associés. La page **Tous les assets** comporte des sections distinctes pour les assets de types spécifiques : Contrôleurs et modules, Assets réseau et IoT. Voir Inventaire.
- **Cartographie du réseau** – Affiche une représentation visuelle des assets du réseau et de leurs connexions. Voir Cartographie du réseau.
- **Vulnérabilités** —Affiche toutes les menaces réseau détectées par OT Security, y compris les CVE, les protocoles vulnérables, les ports ouverts vulnérables, etc., ainsi que les étapes de remédiation recommandées. Voir Vulnérabilités.
- **Requêtes actives** —Vous permet de configurer et d'activer des requêtes actives. Voir Managing Active Queries.
- **Réseau** – Fournit une vue complète du trafic réseau en affichant des données sur les communications qui ont eu lieu entre les assets du réseau au fil du temps. Voir Réseau.

  OT Security affiche les informations réseau dans trois fenêtres distinctes :

  - **Récapitulatif réseau** – Affiche un aperçu du trafic réseau
  - **Captures de paquets** – Affiche des captures de paquets complets du trafic réseau
  - **Communications** – Affiche une liste de toutes les conversations réseau détectées, avec des détails sur la date/heure à laquelle elles se sont produites et les assets impliqués.
- **Groupes** – Affichez, créez et modifiez les groupes utilisés dans Configuration de la politique. Voir Groupes.
- **Paramètres locaux** – Affichez et configurez les paramètres système. Voir Paramètres locaux.

Personnaliser les tableaux

Les pages de OT Security affichent les données sous forme de tableau avec une liste pour chaque élément. Ces tableaux disposent de fonctionnalités de personnalisation standardisées qui vous permettent d'accéder facilement aux informations pertinentes.

Remarque : les exemples présentés ici s'appliquent aux écrans **Tous les événements** et **Tous les assets**, mais une fonctionnalité similaire est disponible pour la plupart des pages. Vous pouvez rétablir les paramètres d'affichage par défaut à tout moment en cliquant sur **Paramètres** > **Réinitialiser le tableau aux valeurs par défaut**.

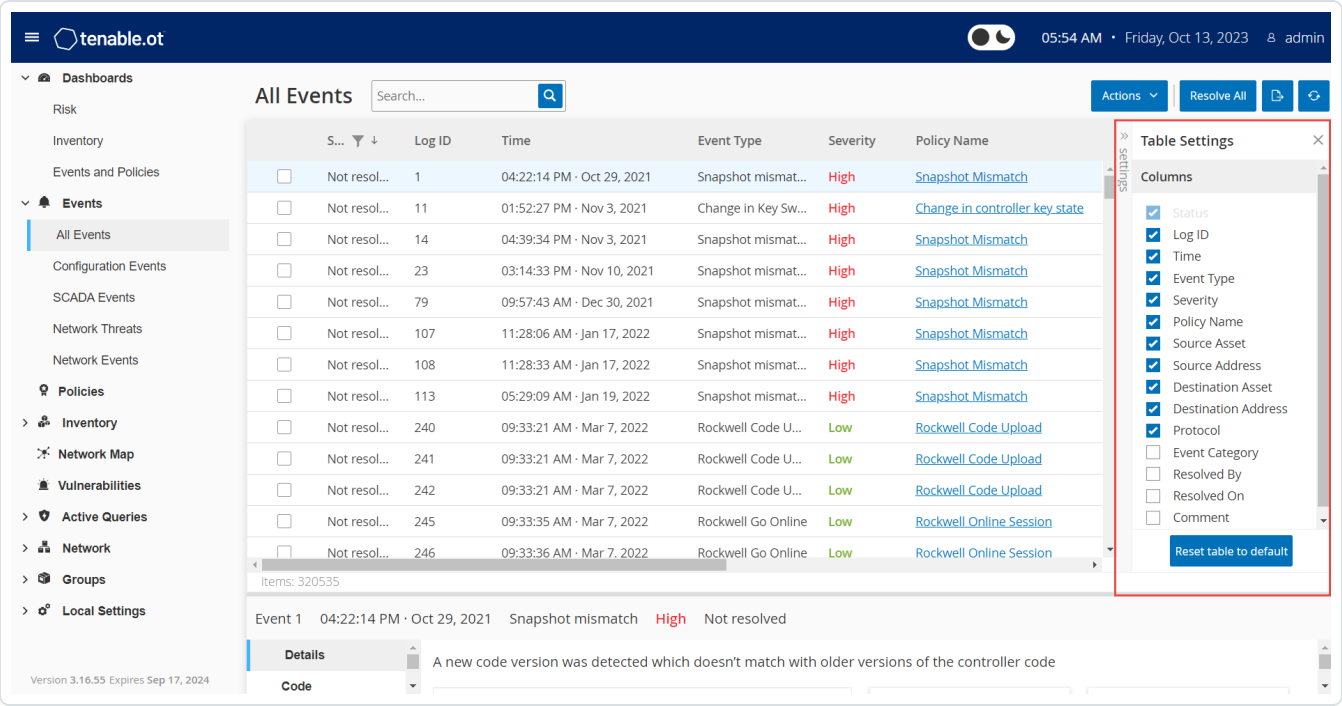
Personnaliser l'affichage des colonnes

Vous pouvez personnaliser les colonnes affichées, ainsi que leur organisation.

Pour sélectionner les colonnes à afficher :

1. À droite du tableau, cliquez sur **Paramètres**.

   Le panneau **Paramètres du tableau** apparaît avec la section **Colonnes**.



2. Dans la section **Colonnes**, cochez la case à côté des colonnes que vous souhaitez afficher.
3. Décochez la case à côté des colonnes que vous souhaitez masquer.

   OT Security affiche uniquement les colonnes sélectionnées.
4. Cliquez sur le signe « **x** » ou sur l'onglet **Paramètres** pour refermer la fenêtre **Paramètres du tableau**.

Pour modifier l'ordre d'affichage des colonnes :

1. Cliquez sur un en-tête de colonne et faites-le glisser vers la position souhaitée.

Regrouper des listes par catégories

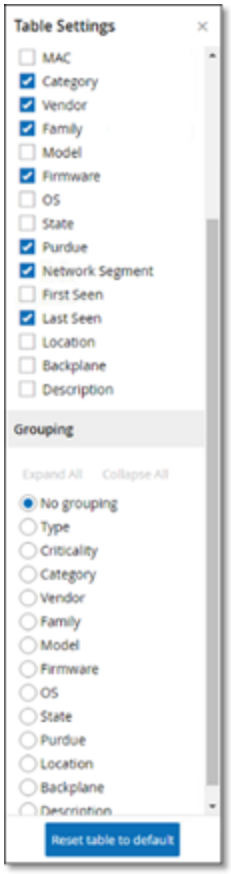
Pour les pages **Inventaire**, vous pouvez regrouper les listes selon divers paramètres pertinents pour cet écran particulier.

Pour regrouper les listes :

1. Cliquez sur l'onglet **Paramètres** le long du bord droit du tableau.

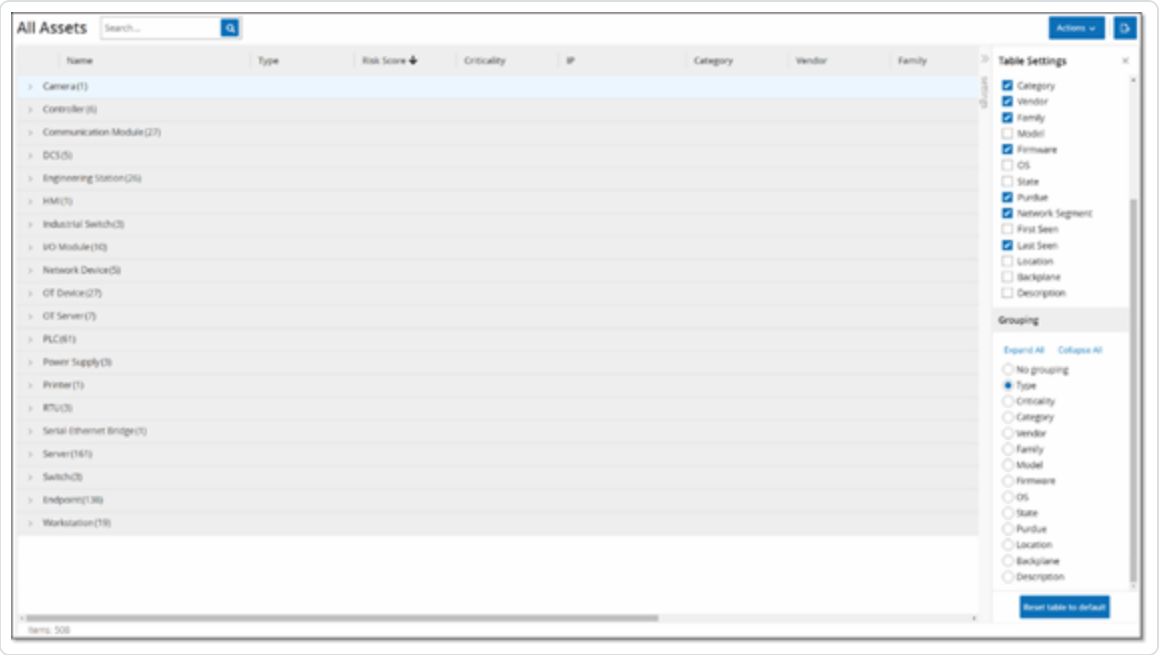
   Le panneau **Paramètres du tableau** apparaît sur le côté droit, en affichant les sections **Colonnes** et **Regroupements**.

2. Faites défiler jusqu'à la section **Regroupements**.

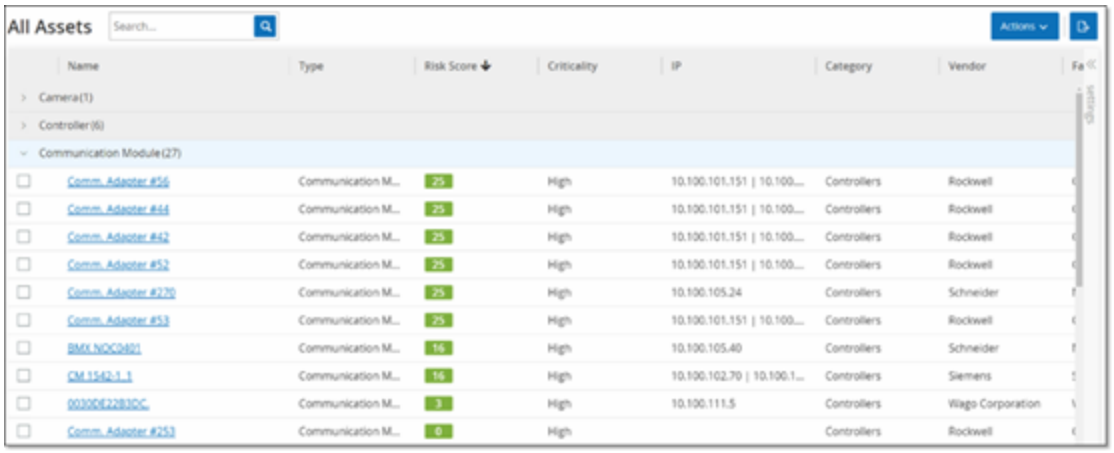


3. Sélectionnez le paramètre selon lequel vous souhaitez regrouper les listes. Par exemple, **Type**.

   OT Security affiche les catégories regroupées.



4. Cliquez sur le signe « **x** » ou sur l'onglet **Paramètres** pour refermer la fenêtre **Paramètres du tableau**.
5. Cliquez sur la flèche à côté d'une catégorie pour afficher toutes les instances de cette catégorie.



Trier des colonnes

Remarque : cette procédure s'applique à toutes les versions.

Pour trier les listes :

1. Cliquez sur un en-tête de colonne pour trier les assets selon ce paramètre. Par exemple, cliquez sur l'en-tête **Nom** pour afficher les noms des assets par ordre alphabétique.
2. Cliquez à nouveau sur l'en-tête de la colonne pour inverser l'ordre d'affichage (passer de A→ Z à Z→ A).

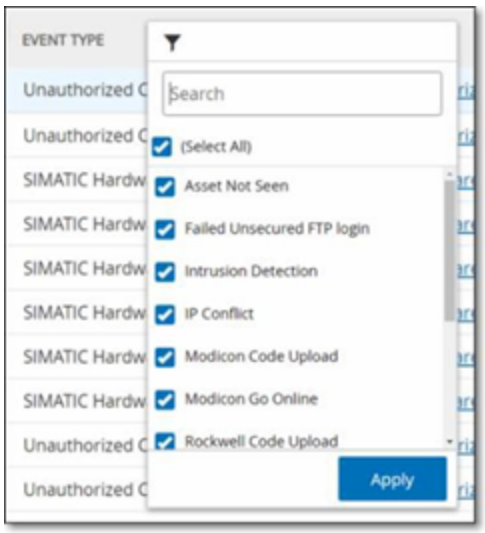
Filtrer les colonnes

Vous pouvez définir des filtres pour un ou plusieurs en-têtes de colonne. Les filtres sont cumulés pour n'afficher que les listes qui répondent à tous les critères de filtrage. Les options de filtrage sont spécifiques à chaque en-tête de colonne. Chaque écran propose une sélection de filtres pertinents. Par exemple, dans la fenêtre **Inventaire des contrôleurs**, vous pouvez filtrer par **nom**, **adresses**, **type**, **fond de panier**, **fournisseur**, etc.

Pour filtrer les listes :

1. Survolez avec la souris un en-tête de colonne pour afficher l'icône de filtre ▼.
2. Cliquez sur l'icône de filtre ▼.

   Une liste d'options de filtrage apparaît. Les options sont spécifiques à chaque paramètre.



3. Sélectionnez les éléments à afficher et décochez les cases de ceux que vous souhaitez masquer.

Remarque : vous pouvez commencer par décocher la case **Tout sélectionner**, puis sélectionnez ce que vous souhaitez afficher.

4. Vous pouvez rechercher dans la liste les filtres que vous souhaitez sélectionner ou non.
5. Cliquez sur **Appliquer**.

   OT Security filtre les listes selon vos critères.

Le bouton de filtre à côté de l'en-tête d'une colonne indique que les résultats sont actuellement filtrés selon ce paramètre.

Pour supprimer les filtres :

1. Cliquez sur le bouton de filtre .
2. Cliquez sur la case **Tout sélectionner** pour effacer toutes les sélections.
3. Cliquez à nouveau sur la case **Tout sélectionner** pour sélectionner tous les éléments.
4. Cliquez sur **Appliquer**.

Recherche

Sur chaque page, vous pouvez rechercher des enregistrements spécifiques.

Pour rechercher dans les listes :

1. Saisissez votre recherche dans la zone **Recherche**.
2. Cliquez sur le bouton .
3. Pour effacer le texte de la recherche, cliquez sur le bouton « **x** ».

Exporter des données

Vous pouvez exporter des données de n'importe quelle liste affichée dans l'interface utilisateur de OT Security (ex. : événements, inventaire, etc.) sous la forme d'un fichier CSV.

Remarque : le fichier exporté contient toutes les données de cette page, même si des filtres ont été appliqués à l'affichage actuel.

Pour exporter des données :

1. Accédez à la page dont vous souhaitez exporter les données.
2. Dans la barre d'en-tête, cliquez sur **Exporter**.

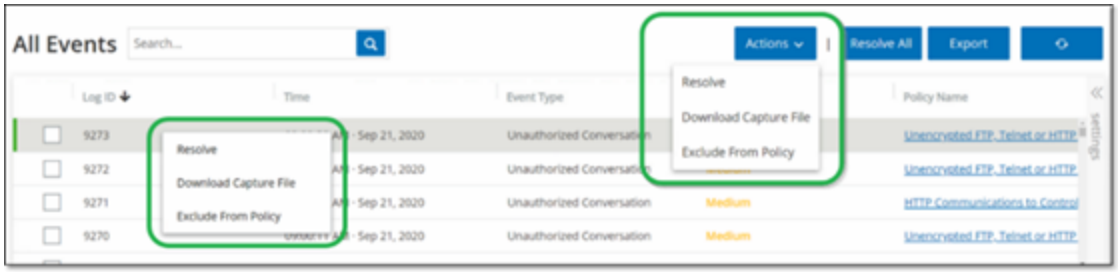
   OT Security télécharge les données au format CSV.

Menu Actions

Chaque écran dispose d'un ensemble d'actions spécifiques aux éléments qui y sont affichés. Par exemple, sur l'écran **Politiques**, vous pouvez **afficher**, **modifier**, **dupliquer** ou **supprimer** une politique. Sur l'écran **Événements**, vous pouvez **résoudre** ou **télécharger le fichier de capture** pour un événement, etc.

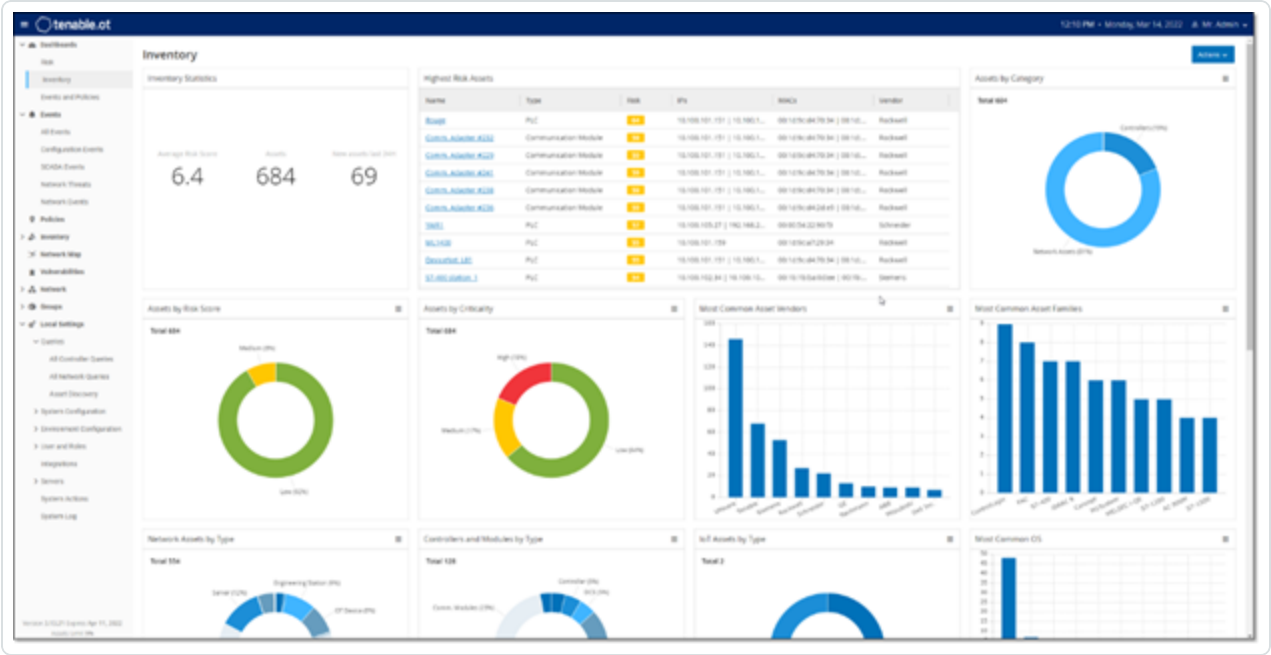
Pour accéder au menu **Actions**, effectuez l'une des actions suivantes :

- Sélectionnez un élément, puis cliquez sur **Actions** dans la barre d'en-tête,
- Effectuez un clic droit sur l'élément, puis sélectionnez **Actions**.



Dashboards

OT Security fournit trois dashboards (**Risque**, **Inventaire** et **Événements et politiques**) pour donner un aperçu de l'inventaire et de la posture de sécurité de votre réseau.



Pour sélectionner un dashboard :

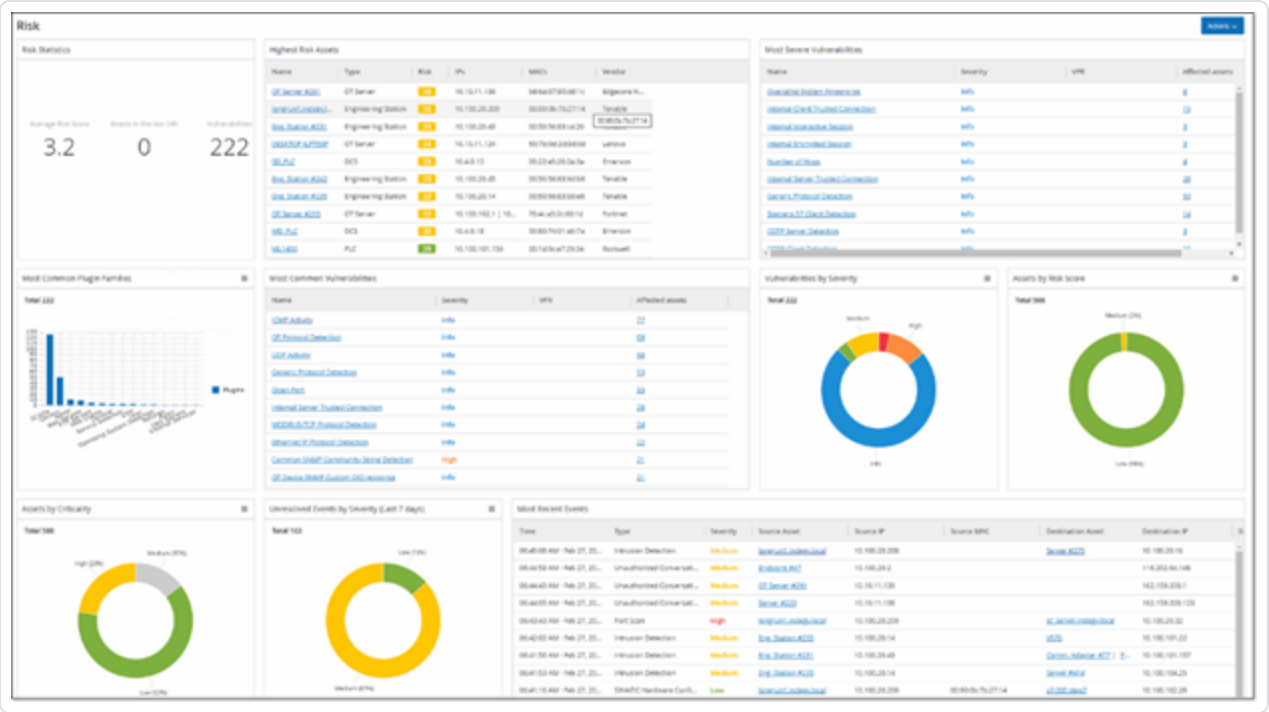
- Dans le menu de navigation principal, cliquez sur **Dashboards**.

Le dashboard **Risques** est la vue par défaut initiale. Cependant, vous pouvez assigner un autre dashboard à la vue par défaut.

Vous pouvez interagir avec les dashboards en ajustant les paramètres d'affichage et en définissant des filtres. Voir Interagir avec les dashboards.

Dashboard Risques

Le dashboard **Risques** fournit des informations sur la cyber-exposition du réseau en se basant sur deux métriques : le score de risque des assets et la gestion des vulnérabilités.

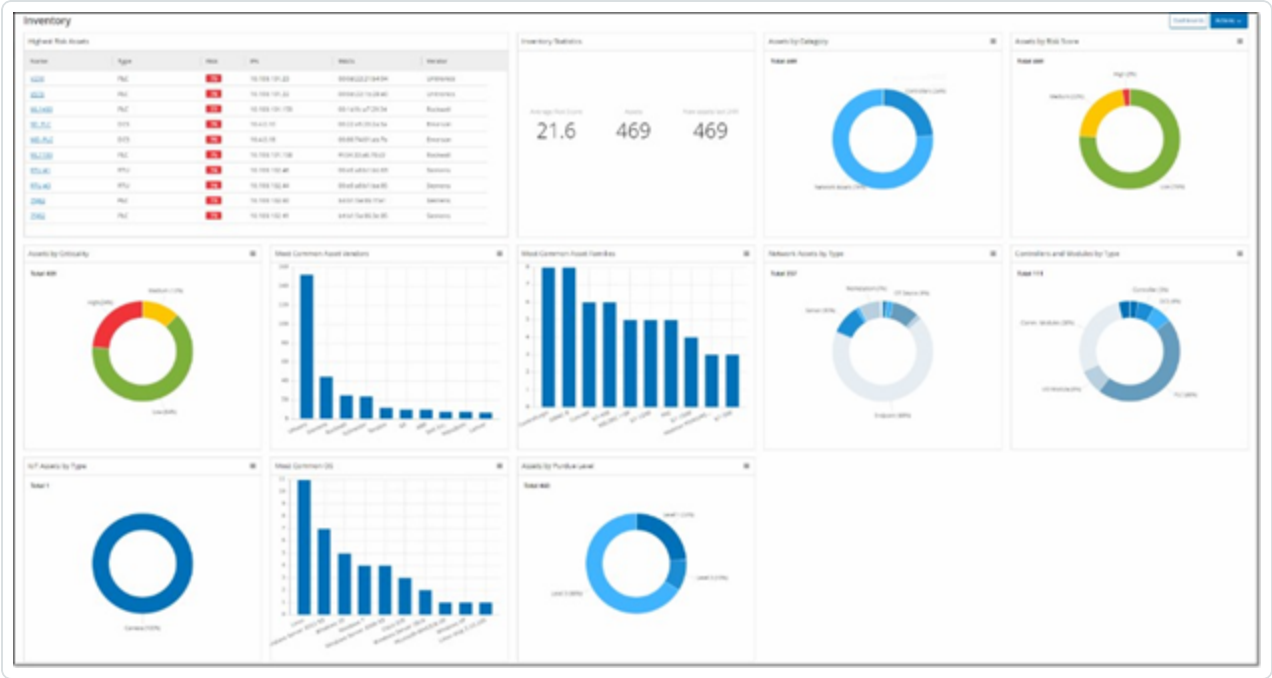


Le dashboard **Risques** affiche des widgets tels que : Statistiques relatives aux risques, Assets par score de risque, Assets par criticité, Événements par sévérité, Vulnérabilités les plus courantes, etc.

En cliquant sur le lien d'un asset ou d'une vulnérabilité, vous accédez à l'élément correspondant sur l'écran **Inventaire** ou **Vulnérabilités**.

Dashboard Inventaire

Le dashboard **Inventaire** offre une visibilité sur l'inventaire des assets, facilitant ainsi leur gestion et leur suivi.

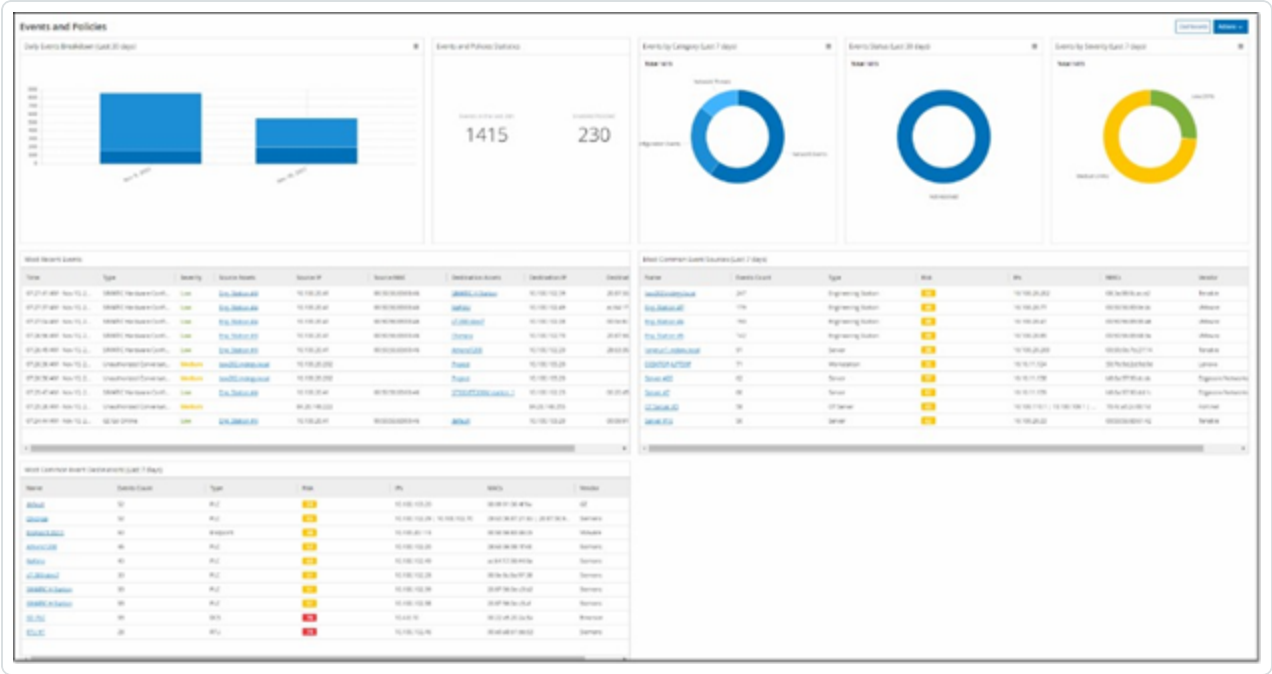


Le dashboard **Inventaire** affiche des widgets tels que : Assets présentant le plus de risque, Statistiques d'inventaire, Assets par score de risque, Contrôleurs et modules par type, Assets par niveau Purdue, etc.

En cliquant sur le lien d'un asset, vous accédez à l'asset correspondant sur l'écran **Inventaire**.

Dashboard Événements et politiques

Le dashboard **Événements et politiques** fournit un moyen de détecter les menaces réseau en surveillant les événements identifiés et les violations de politiques qu'ils génèrent.



Le dashboard **Événements et politiques** affiche des widgets tels que : Répartition des événements quotidiens, Statistiques relatives aux événements et politiques, Statut des événements, Cibles d'événements les plus courantes, etc.

En cliquant sur le lien d'un asset ou d'une événement, vous accédez à l'élément correspondant sur l'écran **Inventaire** ou **Événements**.

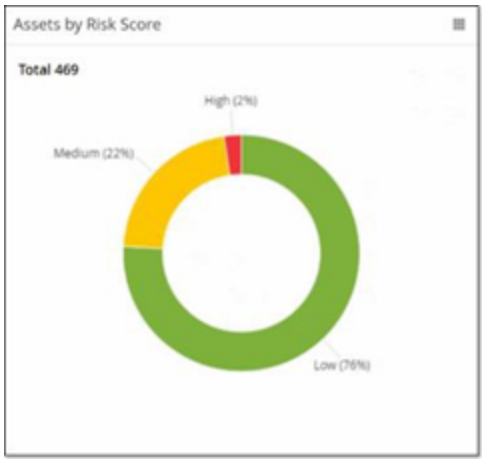
Interagir avec les dashboards

Vous pouvez modifier l'affichage d'un dashboard en interagissant avec les widgets. Vous pouvez afficher les données des dashboards de deux façons : en mode graphique ou en mode tableau. Certains widgets ont un mode d'affichage fixe, d'autres vous permettent de passer d'un mode à l'autre. Les widgets qui présentent un symbole ▦ dans le coin supérieur droit peuvent être visualisés en mode graphique ou en mode tableau. Cliquez sur le symbole tableau/ graphique pour passer d'un mode à l'autre.

> **Remarque :** vous ne pouvez appliquer des filtres qu'en mode tableau.

Mode graphique

Le mode graphique affiche une représentation graphique des données du widget.

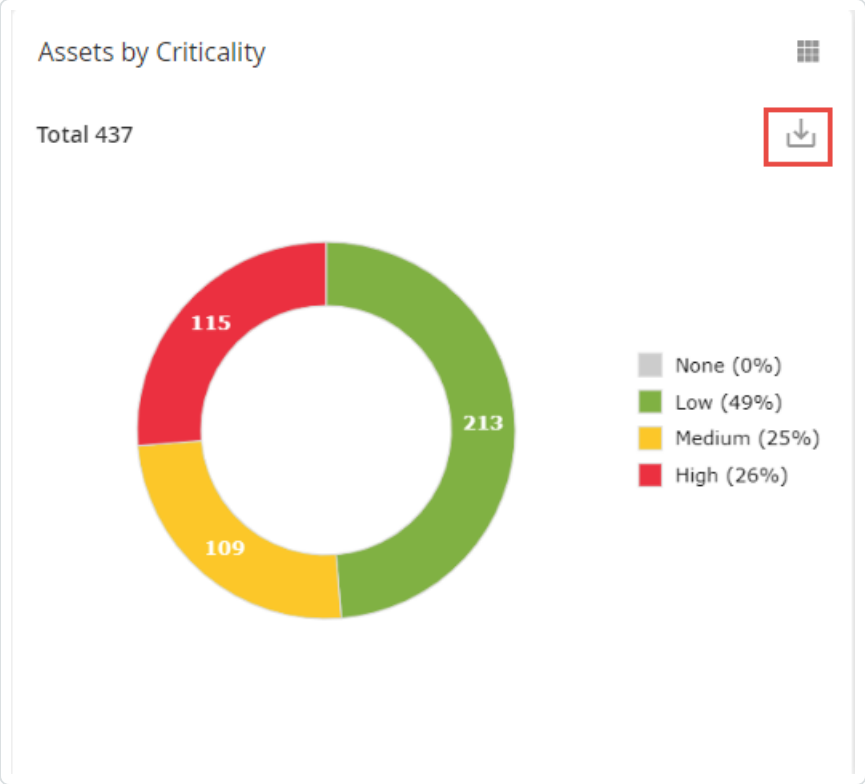


Vous pouvez interagir avec les widgets des manières suivantes :

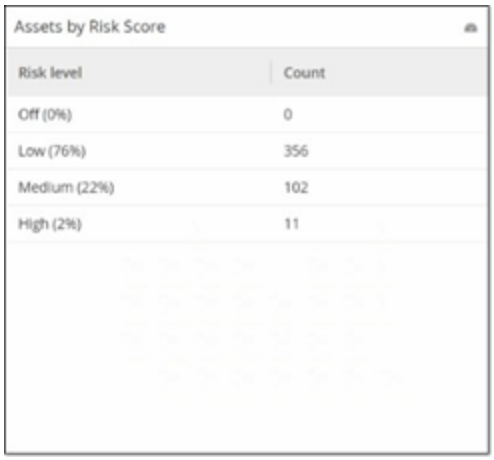
- En survolant un point du graphe avec la souris, vous affichez une fenêtre contextuelle avec des données spécifiques à ce segment du graphe.

- Lorsque vous affichez un widget en mode graphique, vous pouvez télécharger une image du

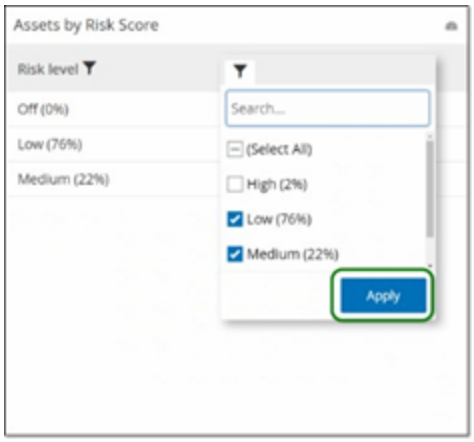
graphe en survolant le widget et en cliquant sur le bouton .



Mode tableau



Lorsque vous affichez un widget en mode tableau, vous pouvez filtrer chaque colonne en survolant l'en-tête de la colonne avec la souris. Cliquez ensuite sur l'icône de filtre, choisissez vos filtres puis cliquez sur **Appliquer**. Les filtres que vous appliquez en mode tableau ne s'appliquent pas au graphe si vous passez en mode graphique.



Modification du dashboard par défaut

Le dashboard Risques est la vue par défaut initiale de la console de gestion. Vous pouvez assigner un autre dashboard à la vue par défaut.

Pour modifier le dashboard affiché par défaut :

1. Accédez au dashboard que vous souhaitez utiliser comme vue par défaut.

2. Cliquez sur **Actions** > **Définir par défaut**.

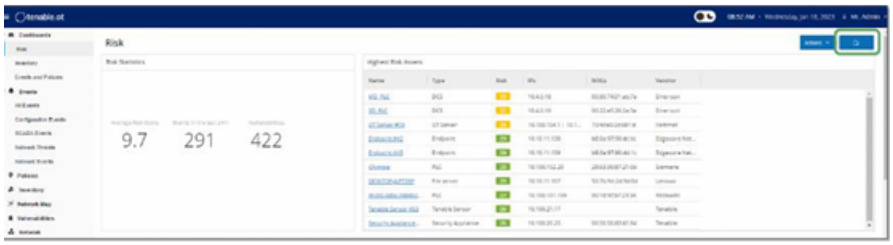
   OT Security met à jour le dashboard par défaut et l'affiche la prochaine fois que vous accédez à la console de gestion

Exporter le dashboard

Le bouton **Exporter** de l'écran Dashboard permet d'exporter un PDF avec chaque widget du dashboard sur une page distincte.

Pour exporter le dashboard :

1. Dans le coin supérieur droit d'un dashboard, cliquez sur **Exporter**.



   Le PDF se télécharge automatiquement dans le dossier de téléchargement par défaut.

   > **Remarque :** assurez-vous de laisser l'onglet Dashboard ouvert dans votre navigateur pendant le téléchargement du PDF (2-3 secondes).

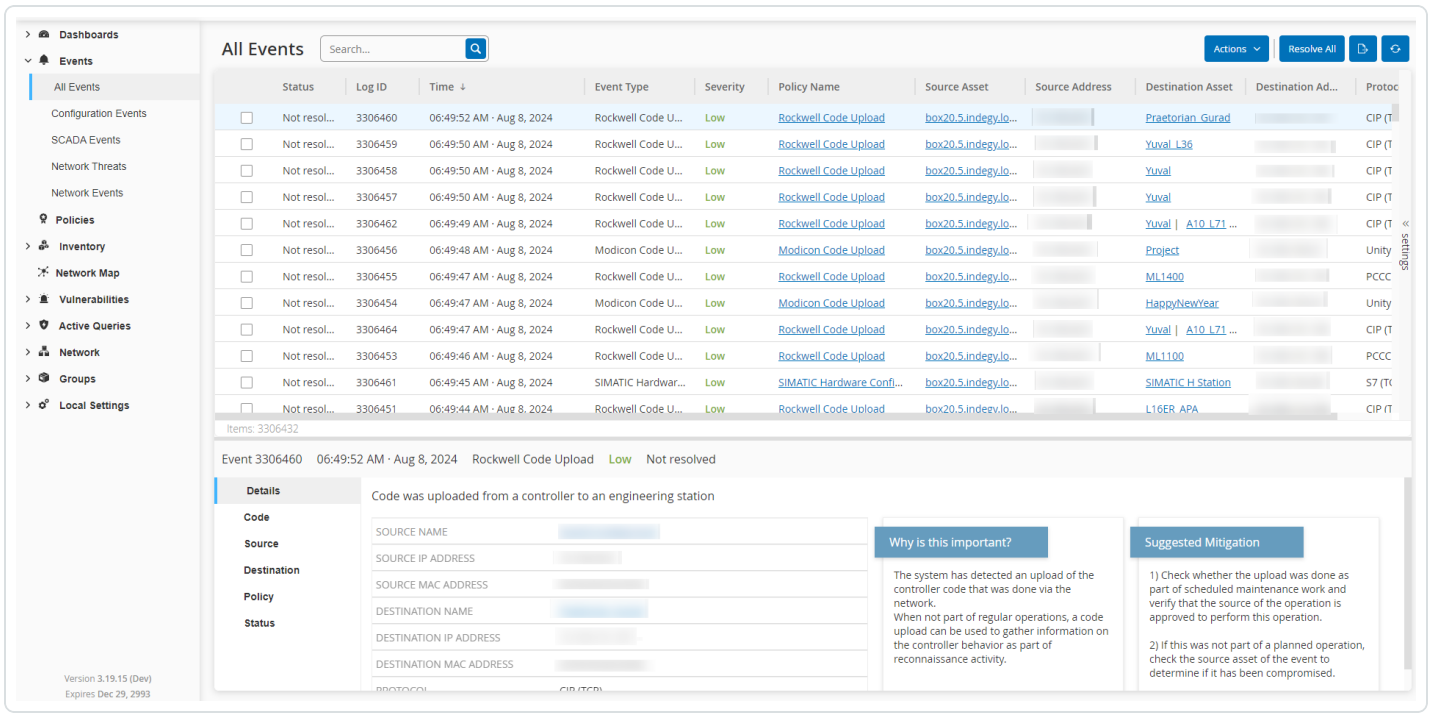
2. Une fois le fichier téléchargé, ouvrez-le pour l'afficher ou le partager.

Événements

Les événements sont des notifications générées dans le système pour attirer l'attention sur une activité potentiellement dangereuse sur le réseau. Les politiques que vous configurez dans le système OT Security génèrent des événements dans l'une des catégories suivantes : Événements de configuration, Événements SCADA, Menaces réseau ou Événements réseau. OT Security attribue un niveau à chaque politique, indiquant la sévérité de l'événement.

Lorsque vous activez une politique, tout événement dans le système qui correspond aux conditions de la politique déclenche une entrée dans le journal d'événement. Plusieurs événements ayant les mêmes caractéristiques sont regroupés en un seul cluster.

Affichage des événements



Tous les événements qui se sont produits dans le système apparaissent sur la page **Tous les événements**. Des sous-ensembles spécifiques d'événements apparaissent sur des fenêtres distinctes pour chacune des catégories d'événements suivantes : **Événements de configuration**, **Événements SCADA**, **Menaces réseau** et **Événements réseau**.

Pour chacune des pages d'événements (Événements de configuration, Événements SCADA, Menaces réseau et Événements réseau), vous pouvez personnaliser les paramètres d'affichage en sélectionnant les colonnes à afficher et la position de chaque colonne. Vous pouvez regrouper les événements en fonction du type d'événement, de la sévérité, du nom de la politique, etc. Vous pouvez également trier et filtrer les listes d'événements, mais aussi effectuer une recherche. Pour plus d'informations sur les fonctionnalités de personnalisation, voir Personnaliser les tableaux (Personnaliser les tables).

Vous pouvez utiliser le bouton **Actions** dans la barre d'en-tête pour effectuer les actions suivantes :

- Résoudre – Marque cet événement comme résolu.
- Télécharger PCAP – Télécharge le fichier PCAP pour cet événement.
- Exclure – Crée une exclusion de politique pour cet événement.

La partie inférieure de la page affiche des informations sur l'événement sélectionné, divisées en onglets. Seuls les onglets correspondant au type de l'événement sélectionné sont affichés. Les

onglets suivants sont affichés pour différents types d'événements : Détails, Code, Source, Cible, Politique, Ports scannés et Statut.

> **Remarque** : vous pouvez faire glisser le séparateur de panneau vers le haut ou vers le bas pour agrandir/réduire l'affichage du panneau inférieur.

Vous pouvez télécharger le fichier de capture de paquet associé à chaque événement. Voir Réseau. Les informations affichées pour chaque liste d'événements sont décrites dans le tableau suivant :

Paramètre	Description
Nom	Le nom de l'appareil sur le réseau. Cliquez sur le nom de l'asset pour afficher l'écran de ses détails. Voir Inventaire.
Adresses	L'adresse IP et/ou MAC de l'asset. **Remarque :** un asset peut avoir plusieurs adresses IP.
Type	Le type d'asset. Voir Types d'assets pour une explication des différents types d'assets.
Fond de panier	L'unité de fond de panier à laquelle le contrôleur est connecté. Des détails supplémentaires sur la configuration du fond de panier sont affichés sur l'écran des détails de l'asset.
Emplacement	Pour les contrôleurs situés sur des fonds de panier, affiche le numéro de l'emplacement auquel le contrôleur est attaché.
Fournisseur	Le fournisseur d'assets.
Famille	Nom de la famille du produit tel que défini par le fournisseur du contrôleur.
Firmware	La version du firmware actuellement installée sur le contrôleur.
Localisation	L'emplacement de l'asset tel que vous le saisissez dans les détails de l'asset OT Security. Voir Inventaire.
Dernière détection	La date et l'heure auxquelles l'appareil a été détecté pour la dernière fois par OT Security. Il s'agit de la dernière fois que l'appareil s'est connecté au réseau ou a effectué une activité.

OS	Le système d'exploitation exécuté sur l'asset.
Identifiant de journal	Identifiant généré par le système pour faire référence à l'événement.
Date/ Heure	La date et l'heure auxquelles l'événement s'est produit.
Type d'événement	Décrit le type d'activité qui a déclenché l'événement. Les événements sont générés par les politiques configurées dans le système. Pour une explication des différents types de politiques, voir Types de politiques.
Sévérité	Affiche le niveau de sévérité de l'événement. Voici une explication des valeurs possibles : Aucun – Aucune raison de s'inquiéter. Info – Aucune raison de s'inquiéter dans l'immédiat. À vérifier au moment opportun. Avertissement – Risque modéré qu'une activité potentiellement dangereuse se soit produite. À traiter au moment opportun. Critique – Risque élevé qu'une activité potentiellement dangereuse se soit produite. À traiter immédiatement.
Nom de la politique	Le nom de la politique qui a généré l'événement. Le nom est un lien vers la liste de politiques.
Asset source	Le nom de l'asset qui a lancé l'événement. Ce champ est un lien vers les listes d'assets.
Adresse source	L'adresse IP ou MAC de l'asset qui a lancé l'événement.
Asset cible	Le nom de l'asset qui a été affecté par l'événement. Ce champ est un lien vers les listes d'assets.
Adresse cible	L'adresse IP ou MAC de l'asset qui a été affecté par l'événement.
Protocole	Lorsque c'est pertinent, montre le protocole utilisé pour la communication qui a généré cet événement.
Catégorie	Affiche la catégorie générale de l'événement.

d'événement	**Remarque :** l'écran Tous les événements affiche tous les types d'événements. Chaque écran d'événement affiche uniquement les événements de la catégorie spécifiée. Les catégories d'événements sont expliquées brièvement ci-dessous (pour une explication plus détaillée, voir Catégories et sous-catégories de politiques) : • Événements de configuration – Cela comprend deux sous-catégories • Événements de validation du contrôleur – Ces politiques concernent les changements ayant lieu au sein des contrôleurs du réseau. • Événements d'activité du contrôleur – Ces politiques concernent les activités qui se produisent sur le réseau (c'est-à-dire les « commandes » mises en œuvre entre les assets du réseau). • Événements SCADA – Ces politiques identifient les modifications apportées au plan de données des contrôleurs. Événements de menaces réseau – Ces politiques identifient le trafic réseau qui indique des menaces d'intrusion. • Événements réseau – Ces politiques concernent les assets du réseau et les flux de communication entre les assets.
Statut	Indique si l'événement a été marqué comme résolu ou non.
Résolu par	Pour les événements résolus, indique quel utilisateur a marqué l'événement comme résolu.
Résolu le	Pour les événements résolus, indique quand l'événement a été marqué comme résolu.
Commentaire	Affiche tous les commentaires qui ont été ajoutés lorsque l'événement a été résolu.

Affichage des détails d'un événement

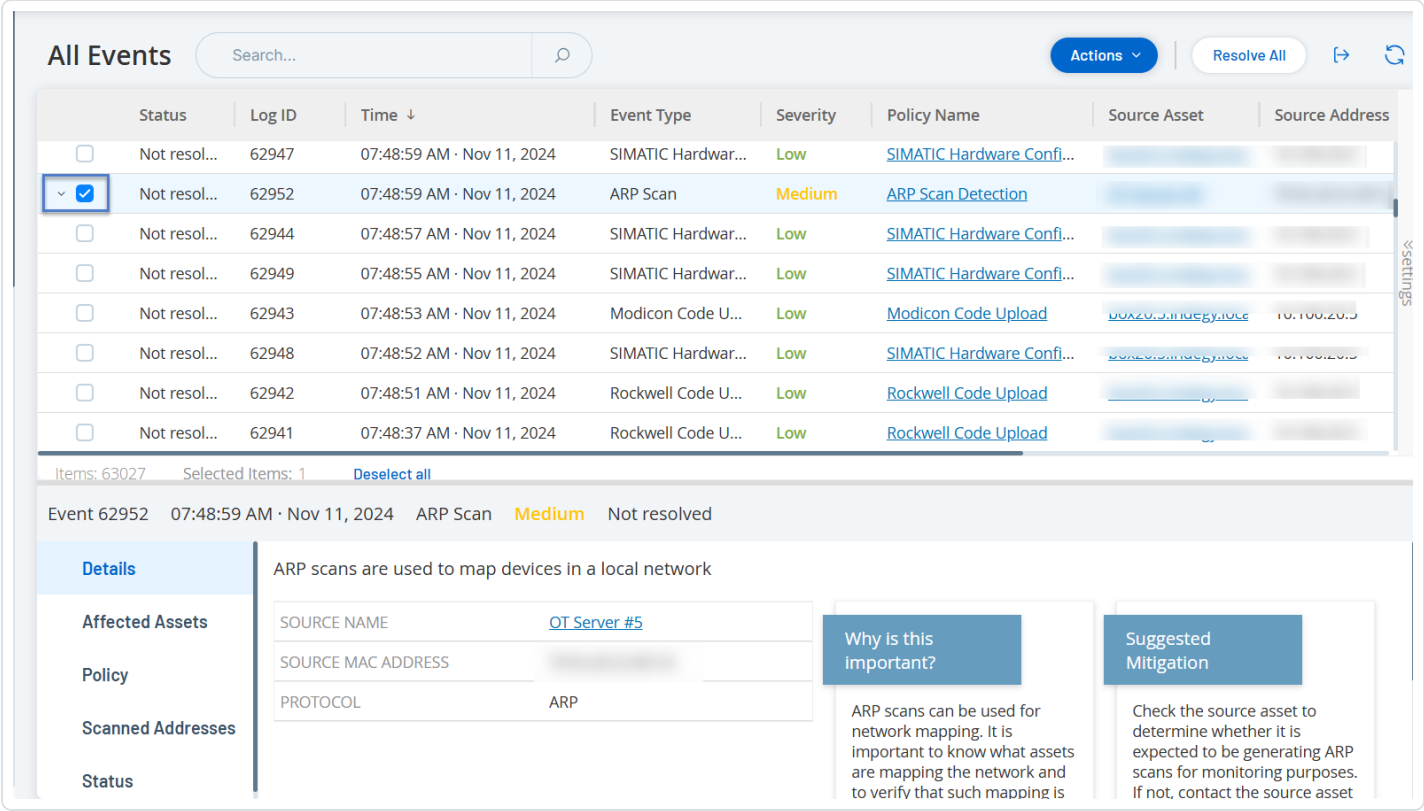
Le bas de la page **Événements** affiche des détails supplémentaires sur l'événement sélectionné. Les informations sont divisées en onglets. Seuls les onglets pertinents pour l'événement sélectionné sont affichés. Les informations détaillées incluent des liens vers des informations supplémentaires sur les entités affectées (asset source, asset cible, politique, groupe, etc.).

- **En-tête** – Affiche un aperçu des informations essentielles sur l'événement.
- **Détails** – Donne une brève description de l'événement ainsi qu'une explication de l'importance de ces informations et des mesures suggérées à prendre pour atténuer les dommages potentiels causés par l'événement. De plus, il affiche les assets sources et cibles qui ont été impliqués dans l'événement.
- **Détails de la règle** (pour les événements de détection d'intrusion) – Affiche des informations sur la règle Suricata qui s'applique à l'événement.
- **Code** – Cet onglet est affiché pour les activités du contrôleur telles que le chargement et le téléchargement de code, la configuration matérielle et la suppression de code. Il affiche des informations détaillées sur le code pertinent, et notamment des blocs de code, des séquences et des tags spécifiques. Les éléments de code sont affichés dans une structure arborescente avec des flèches pour développer/réduire les détails affichés.
- **Source** – Affiche des informations détaillées sur l'asset source pour cet événement.
- **Cible** – Affiche des informations détaillées sur l'asset cible pour cet événement.
- **Asset affecté** – Affiche des informations détaillées sur l'asset affecté par cet événement.
- **Ports scannés** (pour les événements de scan de port) – Affiche les ports qui ont été scannés.
- **Adresse scannée** (pour les événements de scan ARP) – Affiche les adresses qui ont été scannées.
- **Politique** – Affiche des informations détaillées sur la politique qui a déclenché l'événement.
- **Statut** – Indique si l'événement a été marqué comme résolu ou non. Pour les événements résolus, affiche des détails sur l'utilisateur qui l'a marqué comme résolu et quand il a été résolu.

Affichage des clusters d'événements

Pour faciliter le suivi des événements, plusieurs événements aux caractéristiques communes sont regroupés pour former un cluster. Le regroupement est basé sur le type d'événement (c'est-à-dire ceux qui partagent la même politique), les assets source et cible, et la plage temporelle dans laquelle les événements se produisent. Pour plus d'informations sur la configuration des clusters d'événements, voir Groupes d'événements.

Les événements regroupés sont indiqués par une flèche à côté de l'identifiant de journal. Pour afficher le détail des événements d'un cluster, cliquez sur l'enregistrement pour développer la liste.



Résoudre des événements

Lorsqu'un technicien autorisé évalue un événement et prend les mesures nécessaires pour résoudre le problème ou détermine qu'il n'y a pas lieu d'agir, l'événement peut être marqué comme **Résolu**. Lorsqu'un événement faisant partie d'un cluster est résolu, tous les événements de ce cluster sont marqués comme résolus. Vous pouvez sélectionner plusieurs événements et les marquer comme **résolus** en bloc. Vous pouvez également marquer simultanément tous les événements (ou tous les événements d'une catégorie donnée) comme **résolus**.

Résoudre des événements individuels

Pour marquer des événements spécifiques comme résolus :

1. Sur la page **Événements** pertinente (Événements de configuration, Événements SCADA, Menaces réseau ou Événements réseau), cochez la case à côté d'un ou plusieurs événements que vous souhaitez marquer comme **résolus**.
2. Cliquez sur **Actions** dans la barre d'en-tête.

   Un menu déroulant apparaît.

   > **Remarque :** lorsque vous marquez plusieurs événements comme **résolus**, vous devez cliquer sur le bouton **Résoudre** pour résoudre tous les événements sélectionnés, et non sur le bouton **Tout résoudre**. Le bouton **Tout résoudre** est utilisé pour résoudre tous les événements, même ceux qui ne sont pas sélectionnés.

3. Sélectionnez **Résoudre**.

   La fenêtre **Résoudre l'événement** apparaît.

4. (Facultatif) Dans la zone **Commentaire**, vous pouvez ajouter un commentaire pour décrire les mesures d'atténuation prises pour résoudre les problèmes.

5. Cliquez sur **Résoudre**.

   Le statut du ou des événements sélectionnés est marqué comme **Résolu**.

Résoudre tous les événements

L'action **Tout résoudre** s'applique à tous les événements de la page courante en fonction des filtres actuellement appliqués à l'affichage. Par exemple, si la page **Événements de configuration** est ouverte, l'option **Tout résoudre** permet de résoudre les événements de configuration, mais pas les événements SCADA, etc. Pour les événements en cluster, tous les événements du cluster sont marqués comme résolus.

Pour marquer tous les événements comme résolus :

1. Sur la page **Événements** pertinente (Événements de configuration, Événements SCADA, Menaces réseau ou Événements réseau), cliquez sur **Tout résoudre** dans la barre d'en-tête.

   La fenêtre **Résoudre tous les événements** apparaît avec le nombre d'événements à résoudre.

2. (Facultatif) Dans la zone **Commentaire**, vous pouvez ajouter un commentaire sur le groupe d'événements en cours de résolution.
3. Cliquez sur **Résoudre**.

   OT Security affiche un message d'avertissement.
4. Cliquez sur **Résoudre**.

   OT Security marque tous les événements de l'affichage en cours comme **résolus**.

Créer des exclusions de politique

Si une politique génère des événements pour des conditions spécifiques qui ne posent pas de menaces de sécurité, vous pouvez exclure ces conditions de la politique (et ainsi arrêter la génération d'événements pour ces conditions particulières). Par exemple, si vous avez une politique

qui détecte les changements d'état du contrôleur qui se produisent pendant les heures ouvrées, mais que vous déterminez que pour un contrôleur donné, il est normal que l'état change pendant ces périodes, vous pouvez exclure ce contrôleur de la politique.

Vous pouvez créer des exclusions à partir de la page **Événements**, en fonction des événements générés par vos politiques. Vous pouvez spécifier les conditions d'un événement spécifique que vous souhaitez exclure de la politique.

Pour reprendre la génération d'événements pour les conditions spécifiées ultérieurement, vous pouvez supprimer l'exclusion. Voir Politiques.

Pour créer une exclusion de politique :

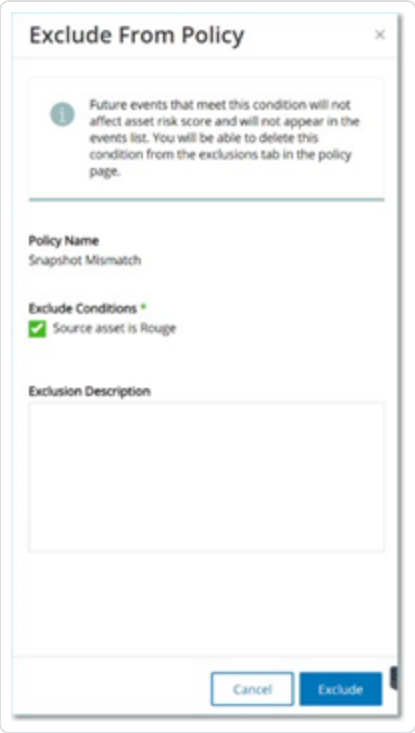
1. Sur la page **Événements** pertinente (Événements de configuration, Événements SCADA, Menaces réseau ou Événements réseau), sélectionnez l'événement pour lequel vous souhaitez créer une exclusion.
2. Dans la barre d'en-tête, cliquez sur **Actions** ou effectuez un clic droit sur l'événement.

   Le menu **Actions** apparaît.
3. Cliquez sur **Exclure de la politique**.

   La fenêtre **Exclure de la politique** apparaît.
4. Dans la section **Condition d'exclusion**, toutes les conditions sont sélectionnées par défaut.

   Les événements qui remplissent l'une des conditions spécifiées sont exclus de la politique. Vous pouvez décocher la case à côté de chaque condition pour laquelle vous souhaitez continuer à générer des événements.

   > **Remarque :** par exemple, dans la fenêtre ci-dessous, pour exclure de cette politique les assets et les adresses IP sources et cibles spécifiés tout en continuant à appliquer cette politique aux communications UDP entre les autres assets du réseau, vous devez désélectionner « Le protocole est UDP ».



Remarque : l'ensemble des conditions qui peuvent être exclues diffère selon le type de politique. Voir le tableau ci-dessous.

5. (Facultatif) Dans la zone **Description de l'exclusion**, vous pouvez ajouter un commentaire sur l'exclusion.
6. Cliquez sur **Exclure**.

   OT Security crée l'exclusion.

   Le tableau suivant indique les conditions pouvant être exclues pour chaque type d'événement.

Catégorie de politique	Type d'événement	Conditions d'exclusion
Activités du contrôleur	Configuration Events (Activities) (Événements de configuration (Activités))	• Asset source • IP source • Asset cible • IP cible

Validation du contrôleur	Change in Key State (Changement d'état de la clé)	Asset source
	Change in Controller State (Changement d'état du contrôleur)	Asset source
	Change in FW version (Changement de version du firmware)	Asset source
	Module not seen (Module non détecté)	Asset source
	Snapshot mismatch (Déviation par rapport à l'instantané)	Asset source
Réseau	Asset Not Seen (Asset non détecté)	Asset source
	Change in USB configuration (Changement dans la configuration USB)	• Asset source • Identifiant du périphérique USB
	IP conflict (Conflit IP)	• Adresses MAC • Adresse IP
	Network Baseline Deviation (Déviation par rapport à la base de référence réseau)	• Asset source • IP source • Asset cible • IP cible • Protocole
	Open Port (Port ouvert)	• Asset source • IP source • Port
	RDP Connection (Connexion RDP)	• Asset source

		• IP source • Asset cible • IP cible
	Unauthorized conversation (Communication non autorisée)	• Asset source • IP source • Asset cible • IP cible • Protocole
	FTP Log In (Failed and Successful) (Connexion FTP (échec et réussite))	• Asset source • IP source • Asset cible • IP cible
	Telnet Log In (Attempt, Failed and Successful) (Connexion Telnet (tentative, échec et réussite))	• Asset source • IP source • Asset cible • IP cible
Menace réseau	Intrusion Detection (Détection d'intrusion)	• Asset source • IP source • Asset cible • IP cible • SID
	ARP Scan (Scan ARP)	• Asset source • IP source

	Port scan (Scan des ports)	• Asset source • IP source
SCADA	Modbus illegal data address (Adresse de données Modbus non valide)	• Asset source • IP source • Asset cible • IP cible
	Modbus illegal data value (Valeur de données Modbus non valide)	• Asset source • IP source • Asset cible • IP cible
	Modbus illegal function (Fonction Modbus non valide)	• Asset source • IP source • Asset cible • IP cible
	Unauthorized write (Écriture non autorisée)	• Asset source • Asset cible • Nom du tag
	IEC60870-5-104 StartDT IEC60870-5-104 StartDT	• Asset source • IP source • Asset cible • IP cible
	IEC60870-5-104 function code based events (Événements basés sur le code de fonction CEI60870-5-104)	• Asset source • IP source

		• Asset cible • IP cible • COT
	DNP3 events (Événements DNP3)	• Asset source • IP source • Asset cible • IP cible • Adresse DNP3 source • Adresse DNP3 cible

Télécharger des fichiers de capture individuels

OT Security stocke les données de capture de paquets associées à chaque événement du réseau. Les données sont stockées sous forme de fichiers PCAP qui peuvent être téléchargés et analysés à l'aide d'outils d'analyse de protocole réseau (par exemple Wireshark, etc.). Vous pouvez également télécharger des fichiers PCAP pour l'ensemble du réseau. Voir Réseau.

Remarque : les fichiers PCAP ne sont disponibles que si la fonction Capture de paquets est activée. Cette fonction peut être activée à partir de l'écran **Paramètres locaux** > **Configuration système** > **Captures de paquets**. Voir Captures de paquets. Les fichiers PCAP ne sont disponibles que pour les événements liés à l'activité du réseau, tels que les activités du contrôleur, les menaces réseau, les événements SCADA et certains types d'événements réseau.

Télécharger un fichier PCAP

Pour télécharger un fichier PCAP :

1. Sur la page **Événements**, cochez la case de l'événement pour lequel vous souhaitez télécharger le fichier PCAP.
2. Cliquez sur **Actions** dans la barre d'en-tête.

Le menu **Actions** apparaît.

3. Sélectionnez **Télécharger le fichier de capture**.

   Le fichier PCAP compressé est téléchargé sur votre ordinateur local.

Créer des politiques FortiGate

L'intégration FortiGate permet d'utiliser certains événements OT Security pour créer des politiques/règles de pare-feu dans le pare-feu FortiGate nouvelle génération. Les types d'événements qui autorisent cette fonctionnalité (événements pris en charge) sont Baseline Deviation (Déviation par rapport à la base de référence), Unauthorized Conversation (Communication non autorisée), Intrusion Detection (Détection d'intrusion) et RDP Connection (authenticated and not authenticated) (Connexion RDP authentifiée et non authentifiée). La politique FortiGate est configurée pour s'appliquer automatiquement aux assets sources et cibles impliqués dans l'événement OT Security. Par défaut, la politique force FortiGate à refuser (c'est-à-dire à bloquer) le trafic du type spécifié. Un administrateur FortiGate peut ajuster les paramètres de politique dans l'application FortiGate.

Avant de suggérer des politiques FortiGate, vous devez configurer l'intégration de votre serveur de pare-feu FortiGate avec OT Security. Voir Pare-feux FortiGate.

Pour suggérer une politique FortiGate :

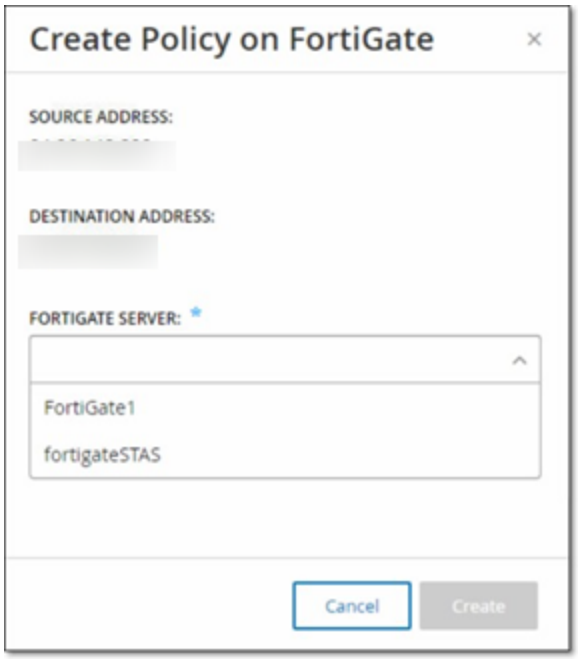
1. Sur la page **Événements** pertinente (Événements de configuration, Événements SCADA, Menaces réseau ou Événements réseau), sélectionnez l'événement pour lequel vous souhaitez créer une politique FortiGate.
2. Dans la barre d'en-tête, cliquez sur **Actions** ou effectuez un clic droit sur l'événement.

   Un menu déroulant apparaît.

3. Sélectionnez **Créer une politique FortiGate**.

   Le panneau **Créer une politique** sur FortiGate apparaît, avec l'**adresse source** et l'**adresse cible** des assets impliqués dans l'événement OT Security déjà remplies.

4. Dans la zone déroulante **Serveur FortiGate**, sélectionnez le serveur souhaité.



5. Cliquez sur **Créer**.

   La politique est créée dans FortiGate et le panneau se referme. Vous pouvez consulter la nouvelle politique dans l'application FortiGate. Un administrateur FortiGate peut ajuster les paramètres selon les besoins.

Politiques

OT Security inclut les politiques qui définissent les types spécifiques d'événements suspects, non autorisés, anormaux ou dignes d'intérêt qui se produisent dans le réseau. Lorsqu'un événement se produit et répond à toutes les conditions de la définition d'une politique, un événement est généré dans le système. Le système consigne les événements et envoie des notifications conformément aux Actions de politique configurées pour la politique.

- **Détection basée sur des politiques** – Déclenche un événement lorsque les conditions précises de la politique, telles que définies par une série de descripteurs d'événements, sont réunies.
- **Détection d'anomalies** – Déclenche un événement lorsque OT Security détecte une activité anormale ou suspecte sur le réseau.

OT Security comporte un ensemble de politiques prédéfinies (prêtes à l'emploi). De plus, vous pouvez modifier les politiques prédéfinies ou établir de nouvelles politiques personnalisées.

Remarque : par défaut, la plupart des politiques sont activées. Pour activer/désactiver des politiques, voir Activer ou désactiver des politiques.

Configuration des politiques

Chaque politique consiste en un ensemble de conditions qui définissent un type de comportement spécifique sur le réseau. Cela inclut des considérations telles que l'activité, les assets impliqués et le moment de l'événement. Un événement est déclenché pour une politique uniquement s'il répond à tous les paramètres définis pour cette politique. Chaque politique a une configuration spécifique d'Actions de politique qui définissent la sévérité, les méthodes de notification et l'enregistrement de l'événement.

Groupes

Les groupes sont un élément essentiel de la définition des politiques dans OT Security. Lors de la configuration d'une politique, chacun des paramètres appartient à un groupe et non pas à des entités individuelles. Cela simplifie considérablement le processus de configuration de la politique. Par exemple, si l'activité Mise à jour du firmware est considérée comme suspecte lorsqu'elle est effectuée sur un contrôleur à certaines heures de la journée (par exemple, pendant les heures ouvrées), au lieu de créer une politique distincte pour chaque contrôleur de votre réseau, vous pouvez créer une politique unique qui s'applique au groupe d'assets nommé Contrôleurs.

La configuration de politique utilise les types de groupes suivants :

- **Groupes d'assets** – Le système est livré avec des groupes d'assets prédéfinis basés sur le type d'asset. Vous pouvez ajouter des groupes personnalisés en fonction d'autres facteurs tels que l'emplacement, le service, la criticité, etc.
- **Segments réseau** – Le système génère automatiquement des segments réseau en fonction du type d'asset et de la plage d'adresses IP. Vous pouvez créer des segments réseau personnalisés pour définir tous les groupes d'assets dont les modèles de communication sont similaires.

- **Groupes de messagerie** – Vous pouvez regrouper plusieurs comptes de messagerie qui reçoivent des notifications par e-mail pour des événements spécifiques. Par exemple, vous pouvez regrouper par rôle, par service, etc.
- **Groupes de ports** – Vous pouvez regrouper des ports utilisés de manière similaire. Il peut s'agir, par exemple, des ports ouverts sur les contrôleurs Rockwell.
- **Groupes de protocoles** – Vous pouvez regrouper des protocoles de communication par type de protocole (par exemple, Modbus), par fabricant (par exemple, Protocoles autorisés par Rockwell), etc.
- **Groupes de planification** – Vous pouvez regrouper plusieurs plages temporelles dans un groupe de planification qui présente une caractéristique commune. Il peut s'agir, par exemple, des heures ouvrées, du week-end, etc.
- **Groupes de tags** – Vous pouvez regrouper les tags qui ont des données opérationnelles similaires au sein de plusieurs contrôleurs. Il pourra s'agir par exemple des tags qui contrôlent la température du four.
- **Groupes de règles** – Vous pouvez regrouper des règles connexes en fonction de leurs identifiants de signature Suricata (SID). Ces groupes sont utilisés comme conditions pour définir des politiques de détection d'intrusion.

Les politiques ne peuvent être définies qu'à l'aide des groupes configurés dans votre système. Le système est livré avec un ensemble de groupes prédéfinis. Vous pouvez modifier ces groupes et ajouter vos propres groupes. Voir Groupes.

Remarque : les paramètres de politique peuvent uniquement être définis à l'aide de groupes. Pour qu'une politique s'applique à une entité individuelle, vous devez configurer un groupe comprenant uniquement cette entité.

Niveaux de sévérité

Chaque politique est associée à un niveau de sévérité spécifique, qui indique le degré de risque posé par la situation qui a déclenché l'événement. Le tableau suivant décrit les différents niveaux de sévérité :

Sévérité	Description

Aucun(e)	L'événement n'est pas préoccupant.
Faible	Aucune raison de s'inquiéter dans l'immédiat. À vérifier au moment opportun.
Moyen	Risque modéré qu'une activité potentiellement dangereuse se soit produite. À traiter au moment opportun.
Élevée	Risque élevé qu'une activité potentiellement dangereuse se soit produite. À traiter immédiatement.

Notifications d'événement

Lorsqu'un événement qui répond à toutes les conditions d'une politique se produit, un événement est généré. La section **Événements** affiche **Tous les événements**. La page **Politique** répertorie l'événement sous la politique qui l'a déclenché, et la page **Inventaire** indique l'événement sous l'asset affecté. De plus, vous pouvez configurer des politiques pour envoyer des notifications d'événements à un SIEM externe à l'aide du protocole Syslog et/ou à des destinataires d'e-mails désignés.

- **Notification Syslog** – Les messages Syslog utilisent le protocole CEF avec des clés standard et des clés personnalisées (configurées pour être utilisées avec OT Security). Pour une explication sur la façon d'interpréter les notifications Syslog, voir le OT Security Syslog Integration Guide (Guide d'intégration Syslog de Tenable OT Security).
- **Notifications par e-mail** – Les e-mails contiennent des détails sur l'événement qui a généré la notification, ainsi que les étapes à suivre pour atténuer la menace.

Catégories et sous-catégories de politiques

Dans OT Security, les politiques sont organisées selon les catégories suivantes :

- **Événements de configuration** – Ces politiques concernent les activités se déroulant sur le réseau. Il existe deux sous-catégories :
  - **Validation du contrôleur** – Ces politiques concernent les changements ayant lieu au sein des contrôleurs du réseau. Cela peut impliquer des modifications de l'état d'un contrôleur, ainsi que des modifications du firmware, des propriétés des assets ou des blocs de code. Les politiques peuvent être limitées à des planifications spécifiques (par

exemple, mise à niveau du firmware pendant une journée de travail) et/ou des contrôleurs spécifiques.

- **Activités du contrôleur** – Ces politiques concernent des commandes d'ingénierie spécifiques qui ont un impact sur l'état et la configuration des contrôleurs. Il est possible de définir des activités spécifiques qui génèrent systématiquement des événements ou de désigner un ensemble de critères pour la génération d'événements. Par exemple, si certaines activités sont effectuées à certains moments et/ou sur certains contrôleurs. La création de listes de blocage et de listes d'autorisations pour les assets, les activités et les calendriers est prise en charge.

- **Événements réseau** – Ces politiques concernent les assets du réseau et les flux de communication entre les assets. Les événements portent sur les assets ajoutés ou supprimés du réseau. Cela inclut également les modèles de trafic jugés anormaux pour le réseau, ou signalés comme préoccupants. Par exemple, si une station d'ingénierie communique avec un contrôleur à l'aide d'un protocole non pré-configuré (par exemple, des protocoles utilisés par des contrôleurs fabriqués par un fournisseur spécifique), la politique déclenche un événement. Vous pouvez limiter ces politiques à des planifications et/ou des assets spécifiques. Les protocoles spécifiques aux fournisseurs sont organisés par fournisseur pour plus de commodité, tandis que n'importe quel protocole peut être utilisé dans une définition de politique.
- **Politiques d'événement SCADA** – Ces politiques détectent les changements dans les valeurs de point de consigne qui peuvent nuire au processus industriel. Ces changements peuvent résulter d'une cyber-attaque ou d'une erreur humaine.
- **Politiques de détection des menaces réseau** – Ces politiques utilisent la détection des menaces OT et IT basée sur les signatures pour identifier le trafic réseau qui indique des menaces d'intrusion. La détection est basée sur des règles cataloguées dans le moteur de détection de menaces Suricata.

Types de politiques

Chaque catégorie et chaque sous-catégorie contiennent différents types de politiques. OT Security fournit des politiques prédéfinies de chaque type. Vous pouvez également créer vos propres politiques personnalisées de chaque type. Les tableaux suivants expliquent les différents types de politiques, regroupés par catégorie.

Événement de configuration – Types d'événement liés aux activités du contrôleur

Les **activités des contrôleurs** sont les activités qui se produisent dans le réseau. Il peut s'agir, par exemple, des « commandes » mises en œuvre entre les assets du réseau. Il existe de nombreux types d'événements liés aux activités des contrôleurs. Le type de contrôleur sur lequel l'activité se produit et l'activité spécifique définissent le type d'activité du contrôleur. Par exemple, arrêt du PLC Rockwell, téléchargement du code SIMATIC, session en ligne Modicon, etc.

Les paramètres de définition de la politique (c'est-à-dire les conditions de la politique) qui s'appliquent aux événements liés aux activités du contrôleur sont : Asset source, Asset cible et Planification.

Événement de configuration – Types d'événements liés à la validation du contrôleur

Le tableau suivant décrit les différents types d'événements liés à la validation du contrôleur.

> **Remarque :** les conditions de politique relatives aux assets affectés, aux sources ou aux cibles peuvent être spécifiées en sélectionnant soit un groupe d'assets, soit un segment réseau.

Type d'événement	Conditions de politique	Description
Change in key switch (Changement dans le commutateur de clé)	Asset affecté, Planification	L'état du contrôleur a été changé via un ajustement de la position de la clé physique. Prend uniquement en charge les contrôleurs Rockwell pour le moment.
Change in state (Changement d'état)	Asset affecté, Planification	Le contrôleur est passé d'un état opérationnel à un autre. Par exemple, en cours d'exécution, arrêté, test, etc.
Change in firmware version (Changement de version du firmware)	Asset affecté, Planification	Une modification a été apportée au firmware exécuté sur le contrôleur.
Module not seen (Module non détecté)	Asset affecté, Planification	Détecte un module précédemment identifié ayant été retiré d'un fond de panier.

New module discovered (Nouveau module découvert)	Asset affecté, Planification	Détecte un nouveau module ajouté à un fond de panier existant.
Snapshot mismatch (Déviation par rapport à l'instantané)	Asset affecté, Planification	L'instantané le plus récent d'un contrôleur (qui capture l'état actuel du programme déployé sur le contrôleur) n'était pas identique à son instantané précédent.

Types d'événements réseau

Le tableau suivant décrit les différents types d'événements réseau.

Remarque : les conditions de politique relatives aux assets affectés, aux sources ou aux cibles peuvent être spécifiées en sélectionnant soit un groupe d'assets, soit un segment réseau.

Type d'événement	Conditions de politique	Description
Asset not seen (Asset non détecté)	Non détecté pendant, Asset affecté, Planification	Détecte les assets précédemment identifiés dans le groupe Asset affecté (Affected Asset) qui sont retirés du réseau pendant la durée spécifiée au cours de la plage temporelle spécifiée.
Rediscovered Asset (Asset redécouvert)	Inactif depuis, Assets affectés, Planification	Détecte un asset qui se met en ligne ou recommence à communiquer après avoir été hors ligne pendant un certain temps.
Change in USB configuration (Changement dans la configuration USB)	Assets affectés, Planification	Détecte lorsqu'un périphérique USB est connecté ou retiré d'un poste de travail Windows. La politique s'applique aux modifications apportées à un asset du groupe des assets affectés au cours de la plage temporelle spécifiée.
IP conflict (Conflit IP)	Planification	Détecte si plusieurs assets présents sur le

		réseau utilisent la même adresse IP. Cela peut indiquer une cyber-attaque ou résulter d'une mauvaise gestion du réseau. La politique s'applique aux conflits IP découverts par OT Security au cours de la plage temporelle spécifiée.
Network Baseline Deviation (Déviation par rapport à la base de référence réseau)	Source, Cible, Protocole, Planification	Détecte les nouvelles connexions entre les assets qui n'ont pas communiqué entre eux pendant l'échantillonnage de la base de référence réseau. Cette option n'est disponible qu'une fois qu'une base de référence réseau a été définie dans le système. Pour définir la base de référence réseau initiale ou pour la mettre à jour, voir Définition d'une base de référence réseau. La politique s'applique à la communication provenant d'un asset du groupe Asset source vers un asset du groupe Asset cible, à l'aide d'un protocole provenant du groupe Protocole, au cours de la plage temporelle spécifiée.
New asset discovered (Nouvel asset découvert)	Asset affecté, Planification	Détecte les nouveaux assets du type spécifié dans le groupe Asset source qui apparaissent sur votre réseau au cours de la plage temporelle spécifiée.
Open Port (Port ouvert)	Asset affecté, Port	Détecte les nouveaux ports ouverts sur votre réseau. Les ports ouverts non utilisés peuvent présenter un risque pour la sécurité. La politique s'applique aux assets du groupe Asset affecté, et aux ports du groupe Port.
Spike in network traffic (Pic de trafic réseau)	Fenêtre temporelle, Niveau de	Détecte les pics anormaux dans le volume du trafic réseau. La politique s'applique aux pics relatifs à la fenêtre temporelle spécifiée et en

	sensibilité, Planification	fonction du niveau de sensibilité spécifié. Elle est également limitée à la plage temporelle spécifiée.
Spike in conversation (Pic de communication)	Fenêtre temporelle, Niveau de sensibilité, Planification	Détecte les pics anormaux du nombre de communications sur le réseau. La politique s'applique aux pics relatifs à la fenêtre temporelle spécifiée et en fonction du niveau de sensibilité spécifié. Elle est également limitée à la plage temporelle spécifiée.
RDP connection (authenticated) (Connexion RDP (authentifiée))	Source, Cible, Planification	Une connexion RDP (connexion bureau à distance) a été établie sur le réseau à l'aide des identifiants d'authentification. La politique s'applique à un asset du groupe Asset source se connectant à un asset du groupe Asset cible, au cours de la plage temporelle spécifiée.
RDP connection (not authenticated) (Connexion RDP (non authentifiée))	Source, Cible, Planification	Une connexion RDP (connexion bureau à distance) a été établie sur le réseau sans utiliser d'identifiants d'authentification. La politique s'applique à un asset du groupe Asset source se connectant à un asset du groupe Asset cible, au cours de la plage temporelle spécifiée.
Unauthorized conversation (Communication non autorisée)	Source, Cible, Protocole, Planification	Détecte les communications envoyées entre assets du réseau. La politique s'applique à la communication provenant d'un asset du groupe Asset source vers un asset du groupe Asset cible, à l'aide d'un protocole provenant du groupe Protocole, au cours de la plage temporelle spécifiée.
Successful unsecured FTP login (Connexion FTP non	Source, Cible, Planification	OT Security considère FTP comme un protocole non sécurisé. Cette politique détecte les connexions réussies à l'aide du protocole FTP.

sécurisée réussie)		
Failed unsecured FTP login (Échec de la connexion FTP non sécurisée)	Source, Cible, Planification	OT Security considère FTP comme un protocole non sécurisé. Cette politique détecte les tentatives de connexion infructueuses à l'aide du protocole FTP.
Successful unsecured Telnet login (Connexion Telnet non sécurisée réussie)	Source, Cible, Planification	OT Security considère Telnet comme un protocole non sécurisé. Cette politique détecte les connexions réussies à l'aide du protocole Telnet.
Failed unsecured Telnet login (Échec de la connexion Telnet non sécurisée)	Source, Cible, Planification	OT Security considère Telnet comme un protocole non sécurisé. Cette politique détecte les tentatives de connexion infructueuses à l'aide du protocole Telnet.
Unsecured Telnet login attempt (Tentative de connexion Telnet non sécurisée)	Source, Cible, Planification	OT Security considère Telnet comme un protocole non sécurisé. Cette politique détecte les tentatives de connexion à l'aide de Telnet (pour lesquelles le statut du résultat n'est pas détecté).

Types d'événements liés aux menaces réseau

Le tableau suivant décrit les différents types d'événements liés aux menaces réseau.

Remarque : les conditions de politique relatives aux assets affectés, aux sources ou aux cibles peuvent être spécifiées en sélectionnant soit un groupe d'assets, soit un segment réseau.

Type d'événement	Conditions de politique	Description
Intrusion Detection (Détection d'intrusion)	Source, Asset affecté, Groupe de règles, Planification	Les politiques de détection d'intrusion détectent les menaces OT et IT basées sur les signatures, afin d'identifier le trafic réseau indiquant des menaces d'intrusion. La détection est basée sur des règles

		cataloguées dans le moteur de détection de menaces Suricata. Les règles sont regroupées en catégories (par exemple, attaques ICS, déni de service, malware, etc.) et sous-catégories (par exemple, attaques ICS – Stuxnet, attaques ICS – Black Energy, etc.). Le système est livré avec un ensemble de groupes prédéfinis de règles associées. Vous pouvez également configurer vos propres regroupements de règles. **Remarque :** vous ne pouvez pas modifier les groupes d'assets **sources** et **cibles** pour les événements du système de détection d'intrusion (IDS).
ARP Scan (Scan ARP)	Asset affecté, Planification	Détecte les scans ARP (activité de reconnaissance du réseau) exécutés sur le réseau. La politique s'applique aux scans diffusés du groupe Asset affecté au cours de la plage temporelle spécifiée.
Port scan (Scan des ports)	Asset source, Asset cible, Planification	Détecte les scans SYN (activité de reconnaissance du réseau) exécutés sur le réseau pour détecter les ports ouverts (vulnérables). La politique s'applique à la communication provenant d'un asset du groupe Asset source vers un asset du groupe Asset cible, au cours de la plage temporelle spécifiée.

Types d'événements SCADA

Le tableau suivant décrit les différents types d'événements SCADA.

Remarque : les conditions de politique relatives aux assets affectés, aux sources ou aux cibles peuvent être spécifiées en sélectionnant soit un groupe d'assets, soit un segment réseau.

Type d'événement	Conditions de politique	Description
Modbus illegal data address (Adresse de données Modbus non valide)	Asset source,	Détecte le code d'erreur

	Asset cible, Planification	« illegal data address » (adresse de données non valide) dans le protocole Modbus. La politique s'applique à la communication provenant d'un asset du groupe Asset source vers un asset du groupe Asset cible, au cours de la plage temporelle spécifiée.
Modbus illegal data value (Valeur de données Modbus non valide)	Asset source, Asset cible, Planification	Détecte le code d'erreur « illegal data value » (valeur de données non valide) dans le protocole Modbus. La politique s'applique à la communication provenant d'un asset du groupe Asset source vers un asset du groupe Asset cible, au cours de la plage temporelle spécifiée.
Modbus illegal function (fonction Modbus non valide)	Asset source, Asset cible, Planification	Détecte le code d'erreur « illegal function » (fonction non valide) dans le protocole Modbus. La politique s'applique à la communication provenant d'un asset du groupe Asset source vers un asset du groupe Asset cible, au cours de la plage temporelle spécifiée.
Unauthorized write (Écriture non autorisée)	Asset source, Groupe de tags, Valeur du tag, Planification	Détecte les écritures non autorisées pour des tags spécifiés sur un contrôleur (actuellement pris en charge pour les contrôleurs Rockwell

		et ST) dans le groupe Asset source spécifié. Vous pouvez configurer la politique pour détecter toute nouvelle écriture, un changement par rapport à une valeur spécifiée ou une valeur en dehors d'une plage spécifiée. La politique s'applique uniquement au cours de la plage temporelle spécifiée.
ABB - Unauthorized write (ABB - Écriture non autorisée)	Asset source, Asset cible, Planification	Détecte les commandes d'écriture envoyées via MMS aux contrôleurs ABB 800xA étant hors de la plage autorisée.
Commandes CEI 60870-5-104 : Start/ Stop Data Transfer (démarrage/ arrêt du transfert de données), Interrogation Command (commande d'interrogation), Counter Interrogation Command (commande d'interrogation de compteur), Clock Synchronization Command (commande de synchronisation d'horloge), Reset Process Command (commande de processus de réinitialisation), Test Command with Time Tag (commande de test avec marqueur temporel)	Asset source, Asset cible, Planification	Détecte les commandes spécifiques envoyées aux unités principales ou subordonnées CEI-104 considérées comme risquées.
DNP3 Commands (Commandes DNP3)	Asset source, Asset cible, Planification	Détecte toutes les commandes principales envoyées via le protocole DNP3. Par exemple,

		Select (Sélection), Operate (Exécution), Warm/Cold Restart (Redémarrage à chaud/à froid), etc. Détecte également les erreurs provenant d'indicateurs internes tels que les codes de fonction non pris en charge et les erreurs de paramètre.

Activer ou désactiver des politiques

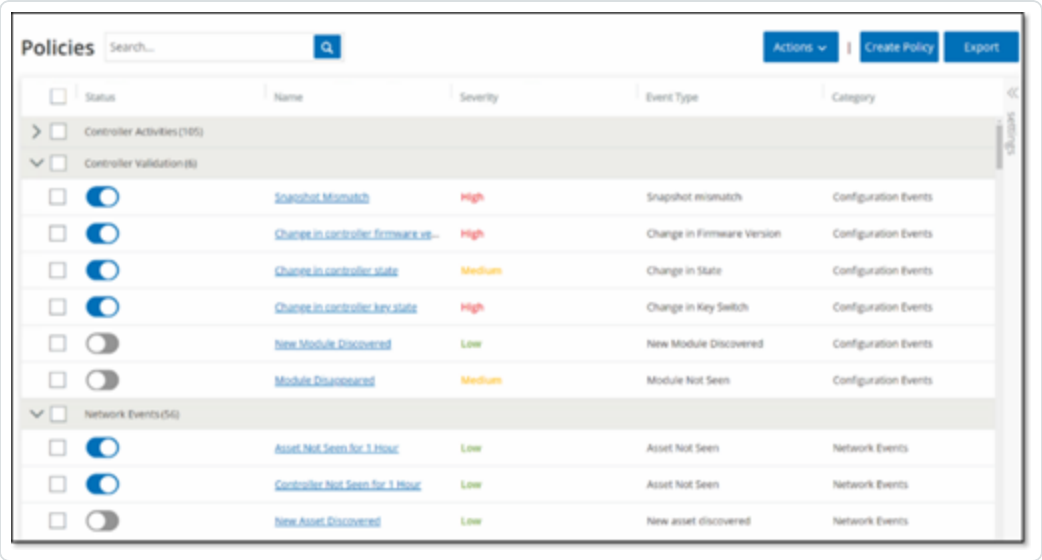
Vous pouvez activer ou désactiver n'importe quelle politique configurée dans votre système (à la fois pré-configurée ou définie par l'utilisateur). Vous pouvez activer et désactiver les politiques individuellement ou en bloc après en avoir sélectionné plusieurs.

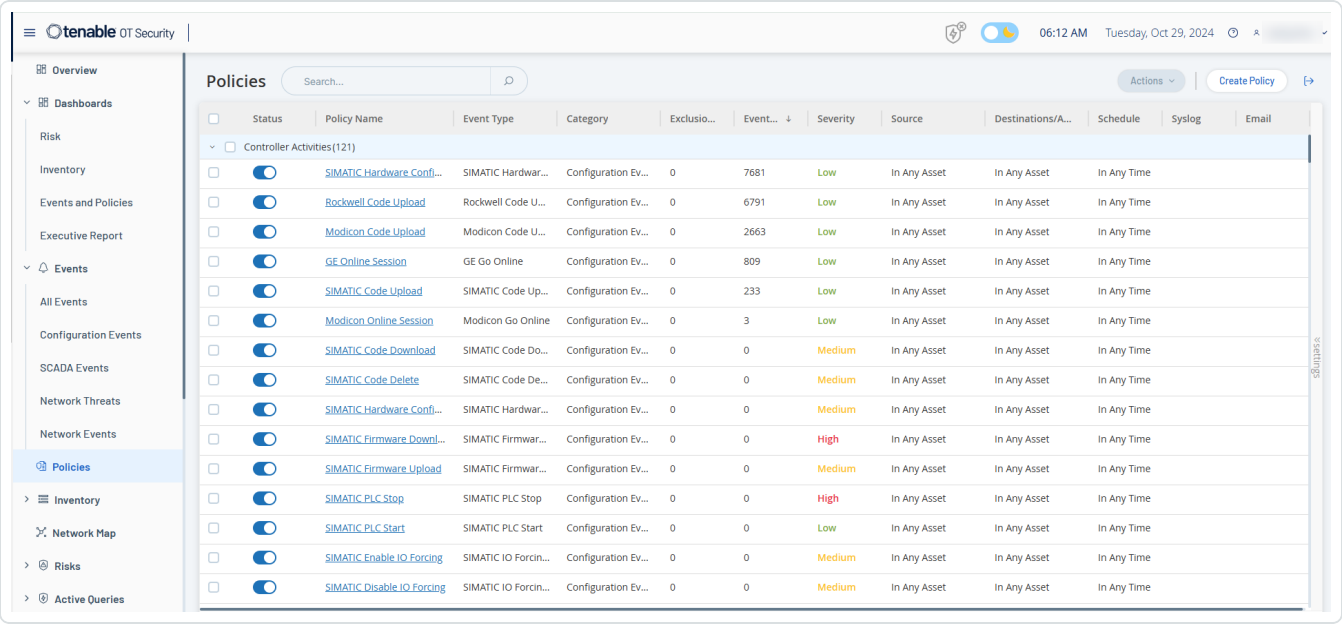
Remarque : la plupart des politiques dépendent de l'utilisation de requêtes pour collecter des données. Si certaines ou toutes les fonctions de requête sont désactivées, les politiques associées ne fonctionnent pas correctement. Vous pouvez activer des requêtes à partir de **Requêtes actives**. Voir Requêtes actives.

Pour activer ou désactiver une politique :

1. Accédez à **Politiques**.

   La page répertorie toutes les politiques configurées dans le système, regroupées par catégorie.



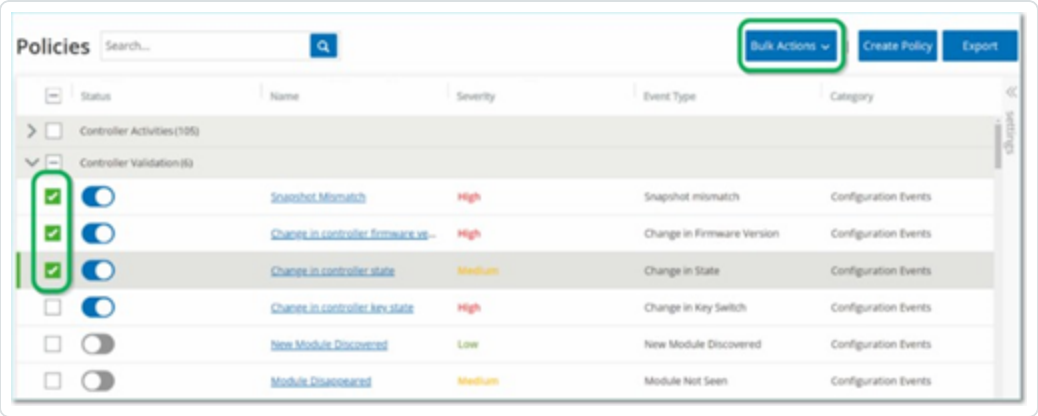


2. Pour activer ou désactiver la politique, cliquez sur le curseur **Statut** à côté de la politique correspondante.

Pour activer ou désactiver plusieurs politiques :

1. Accédez à **Politiques**.

   La page répertorie toutes les politiques configurées dans le système, regroupées par catégorie.



2. Cochez la case à côté de chacune des politiques que vous souhaitez activer ou désactiver. Utilisez l'une des méthodes de sélection suivantes :

   - **Sélection individuelle** – Cochez la case devant chaque politique souhaitée.
   - **Sélection par type** – Cochez la case à côté d'un en-tête de type de politique.
   - **Sélection de toutes les politiques** – Cochez la case dans la barre de titre en haut du tableau.

3. Dans la zone déroulante **Actions en bloc**, sélectionnez l'action souhaitée (**Activer** ou **Désactiver**).

   OT Security active ou désactive les politiques sélectionnées.

Afficher les politiques

L'écran **Politiques** répertorie toutes les politiques configurées dans votre système. Les listes sont regroupées par onglets distincts pour chaque catégorie de politique. La page répertorie les politiques pré-configurées et les politiques définies par l'utilisateur. Chaque politique s'accompagne d'un curseur qui indique son statut actuel, ainsi que de plusieurs paramètres indiquant la configuration de la politique.

Vous pouvez afficher/masquer des colonnes, trier et filtrer les listes d'assets, mais aussi rechercher des mots-clés. Pour plus d'informations sur la personnalisation de la liste, voir Éléments de l'interface utilisateur de la console de gestion.

Les paramètres de politique sont décrits dans le tableau suivant :

Paramètre	Description

Statut	Indique si la politique est activée ou désactivée. Si le système a désactivé automatiquement une politique, car elle générait un trop grand nombre d'événements, une icône d'avertissement apparaît à côté du curseur. Activez ou désactivez une politique à l'aide du curseur de statut.
ID de la politique	Identifiant unique de la politique dans le système. Les ID de politique sont regroupés par catégorie, avec un préfixe différent pour chaque catégorie. Par exemple, P1pour les activités de contrôleur, P2 pour les événements réseau, etc.
Nom	Le nom de la politique.
Sévérité	Le degré de sévérité de l'événement. Les valeurs possibles sont : Aucune, Faible, Moyenne ou Élevée. Voir la section Niveaux de sévérité pour une description des niveaux de sévérité.
Type d'événement	Le type spécifique d'événement qui déclenche cette politique d'événement.
Catégorie	La catégorie générale du type d'événement qui déclenche cette politique d'événement. Les valeurs possibles sont : Événements de configuration, Événements SCADA, Menaces réseau ou Événement réseau. Pour plus d'informations sur les différentes catégories, voir Catégories et sous-catégories de politiques.
Source	Condition de politique. Groupe d'assets source/ segment réseau (c'est-à-dire, l'asset qui a lancé l'activité) auquel la politique s'applique.
Asset cible/ affecté	Condition de politique. Le groupe d'assets cible/ segment réseau (l'asset qui reçoit l'activité) auquel la politique s'applique. Pour les politiques qui impliquent un seul asset (pas de source ni de cible), ce paramètre affiche l'asset affecté par l'événement.
Planification	Condition de politique. Plage temporelle pour laquelle la politique s'applique.
Journal système	Le serveur Syslog (SIEM) où les événements de la politique sont enregistrés.

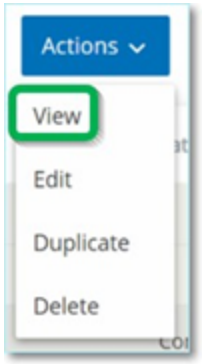
E-mail	Le groupe de messagerie qui envoie les notifications d'événement pour cette politique.
Sous-catégorie	La classification de la sous-catégorie de l'événement. La catégorie Événements de configuration est composée des sous-catégories Activités du contrôleur et Validation du contrôleur. Pour plus d'informations sur les différentes sous-catégories, voir Afficher les politiques.
Nombre d'événements par politique	Répertorie le nombre d'événements générés par chaque politique. Vous pouvez cliquer sur la colonne pour trier les éléments de la liste, afin de traiter les politiques qui ont le plus grand nombre violations/d'événements.
Exclusions	Répertorie le nombre d'exclusions ajoutées à chaque politique. Pour plus d'informations, voir Événements.

Afficher les détails d'une politique

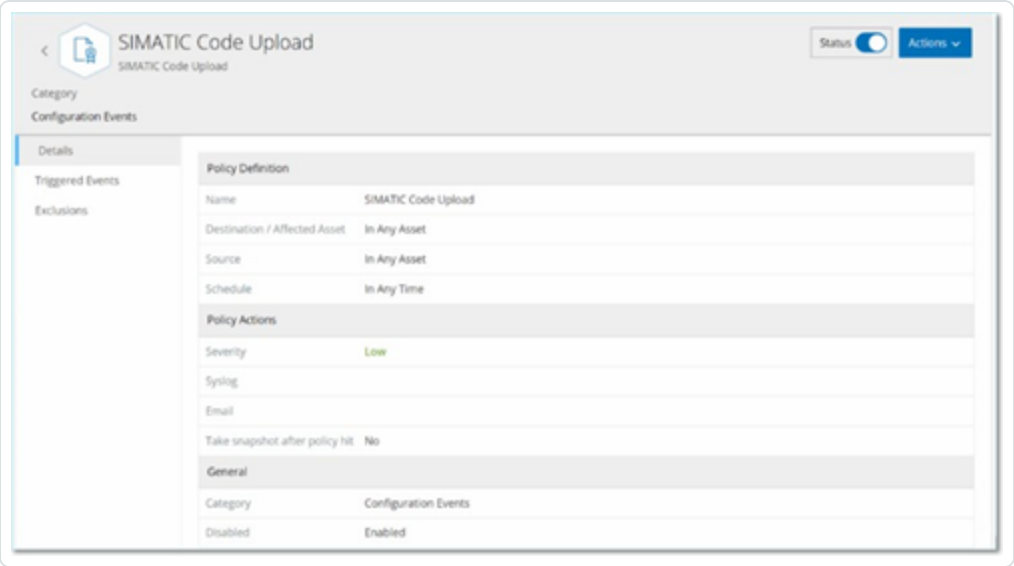
Vous pouvez ouvrir la page des **détails d'une politique** pour afficher des détails supplémentaires sur une politique. Cette page répertorie toutes les conditions et tous les événements déclenchés par la politique.

Pour ouvrir l'écran des **détails de la politique** pour une politique donnée :

1. Sur la page **Politiques**, sélectionnez la politique souhaitée.
2. Dans la zone déroulante **Actions**, sélectionnez **Afficher**.



La page Détails de la politique apparaît pour la politique sélectionnée.



Remarque : vous pouvez également accéder au menu Actions en effectuant un clic droit sur la politique pertinente.

La page des détails de la politique contient les éléments suivants :

- **Barre d'en-tête** – Affiche le nom, le type et la catégorie de la politique. Cette page contient un curseur qui permet d'activer ou de désactiver la politique, ainsi que la liste déroulante des **actions** disponibles (**Modifier**, **Dupliquer** et **Supprimer**).
- **Onglet Détails** – Affiche des détails sur la configuration de la politique dans les sections suivantes :
  - **Définition de la politique** – Affiche toutes les conditions de la politique. Cela inclut tous les champs pertinents selon le type de politique.
  - **Actions de la politique** – Affiche le niveau de sévérité ainsi que la cible (Syslog, e-mail) des notifications d'événement. Indique également si la fonction **Désactiver la politique après la première correspondance** est activée.
  - **Général** – Affiche la catégorie et le statut de la politique.
- **Onglet Événements déclenchés** – Affiche une liste des événements déclenchés par cette politique. L'onglet affiche également des détails sur les assets impliqués dans l'événement et la nature de l'événement. Les informations affichées dans cet onglet

sont identiques à celles dans la page **Événements**, mais seuls les événements de la politique spécifiée sont affichés. Pour une explication des informations sur les événements, voir Affichage des événements.

Onglet **Exclusions** – Si une politique génère des événements pour des conditions spécifiques qui ne posent pas de menaces de sécurité, vous pouvez exclure ces conditions de la politique (et ainsi arrêter la génération d'événements pour ces conditions particulières). Vous pouvez ajouter des exclusions sur la page **Événements**. Voir Événements. L'onglet **Exclusions** affiche toutes les exclusions appliquées à la politique. Pour chaque exclusion, il affiche les conditions spécifiques exclues. À partir de cet onglet, vous pouvez supprimer une exclusion, permettant ainsi au système de reprendre la génération d'événements pour les conditions spécifiées.

Créer des politiques

Vous pouvez créer vos propres politiques basées sur les considérations spécifiques de votre réseau ICS. Vous pouvez déterminer précisément quels types d'événements doivent être portés à l'attention de votre personnel, ainsi que la manière dont les notifications sont transmises. Vous disposez d'une flexibilité totale pour déterminer le degré de précision ou d'étendue de la définition que vous souhaitez donner à chaque politique.

> **Remarque :** les politiques sont définies à l'aide de groupes configurés dans votre système. Si la liste déroulante d'un certain paramètre n'affiche pas le groupe spécifique auquel vous souhaitez que la politique s'applique, vous pouvez créer un nouveau groupe en fonction de vos besoins. Voir Groupes.

La première étape de la création d'une politique est de sélectionner la catégorie et le type de la politique que vous souhaitez créer. L'assistant Créer une politique vous guide tout au long du processus de configuration. Chaque type de politique a son propre ensemble de paramètres de condition pertinents. L'assistant Créer une politique vous montre les paramètres de condition les plus pertinents pour le type de politique sélectionné.

Pour les paramètres Source, Cible et Planification, vous pouvez indiquer s'il faut placer le groupe spécifié sur une liste d'autorisation ou de blocage.

- sélectionnez **Inclure** pour ajouter le groupe à la liste d'autorisation (c'est-à-dire l'inclure dans la politique), OU
- sélectionnez **Exclure** pour ajouter le groupe spécifié à la liste de blocage (c'est-à-dire l'exclure de la politique).

Pour les paramètres de groupe d'assets et de segment réseau (c'est-à-dire les assets sources, cibles et affectés), vous pouvez utiliser des opérateurs logiques (et/ou) pour appliquer la politique à diverses combinaisons ou sous-ensembles de vos groupes prédéfinis. Par exemple, si vous souhaitez qu'une politique s'applique à tout périphérique qui est soit un appareil ICS soit un serveur ICS, sélectionnez Appareil ICS ou Serveurs ICS. Pour qu'une politique s'applique uniquement aux contrôleurs situés dans l'usine A, sélectionnez Contrôleurs et Périphériques de l'usine A.

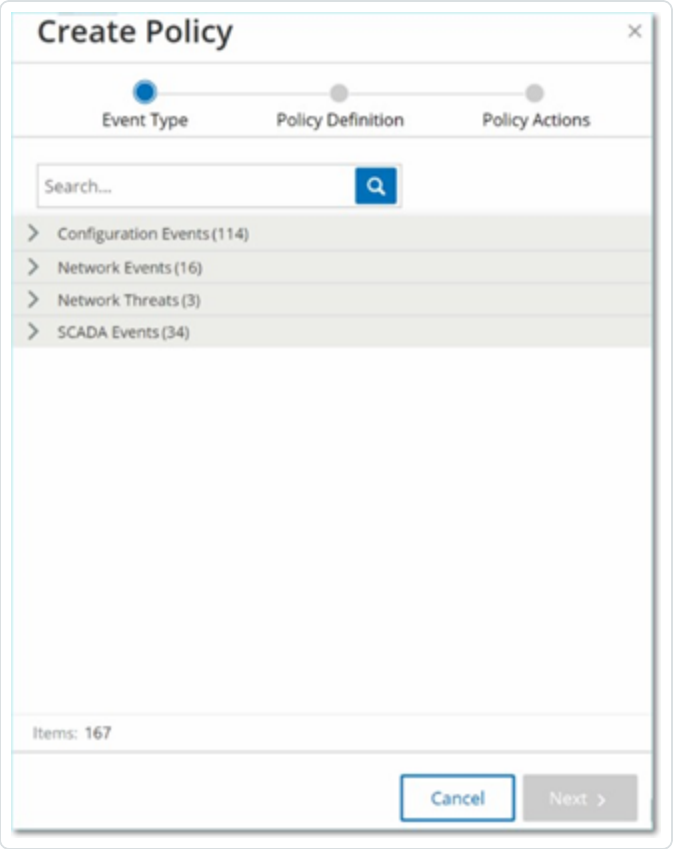
Pour créer une politique avec des paramètres similaires à une politique existante, vous pouvez dupliquer la politique d'origine et apporter les modifications nécessaires. Voir la section Créer des politiques.

> **Remarque :** après avoir créé une politique, si vous constatez qu'elle génère des événements pour des situations qui ne nécessitent pas d'attention, vous pouvez exclure certaines conditions spécifiques de la politique. Voir Événements.

Pour créer une politique :

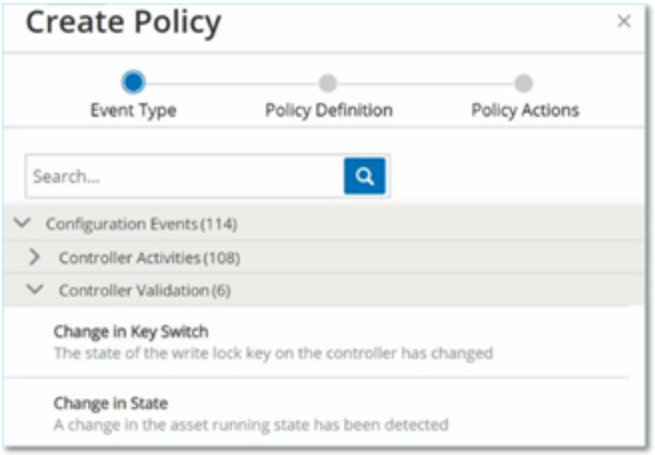
1. Sur l'écran **Politiques**, cliquez sur **Créer une politique**.

   L'assistant **Créer une politique** apparaît.

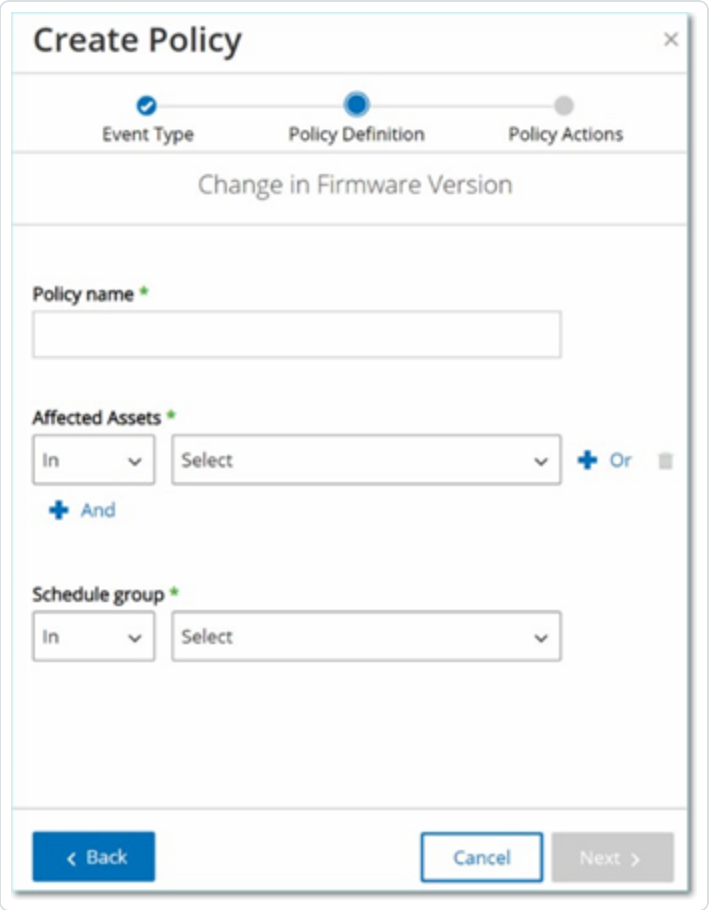


2. Cliquez sur une **catégorie de politique** pour afficher les sous-catégories et/ou les types de politiques.

   Une liste de toutes les sous-catégories et/ou types inclus dans cette catégorie apparaît.



3. Sélectionnez un type de politique.



4. Cliquez sur **Suivant**.

   Une série de paramètres permettant de définir la politique apparaît. Elle comprend toutes les conditions pertinentes pour le type de politique sélectionné.

5. Dans le champ **Nom de la politique**, saisissez un nom pour cette politique.

   > **Remarque :** choisissez un nom décrivant la nature spécifique du type d'événement que la politique est censée détecter.

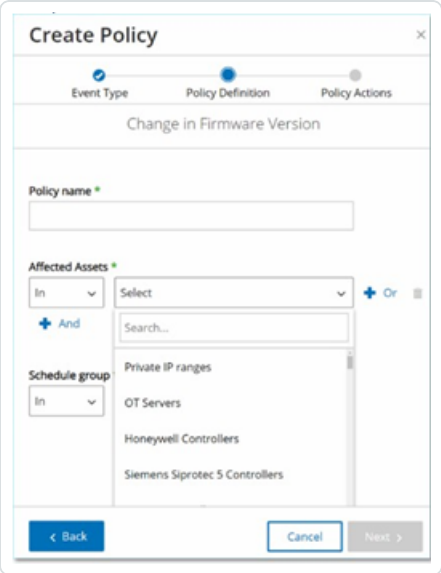
6. Pour chaque paramètre :

   > **Important** : vous ne pouvez pas modifier les groupes d'assets **sources** et **cibles** pour les événements du système de détection d'intrusion (IDS).

a. Lorsque c'est pertinent, sélectionnez **Inclure**, option par défaut, pour ajouter l'élément sélectionné à la liste d'autorisations ou Exclure pour le placer dans la liste de blocage.

b. Cliquez sur **Sélectionner**.

Une liste déroulante des éléments pertinents (par exemple, groupe Asset, Segment réseau, groupe Port, groupe Planification, etc.) apparaît.



c. Sélectionnez l'élément souhaité.

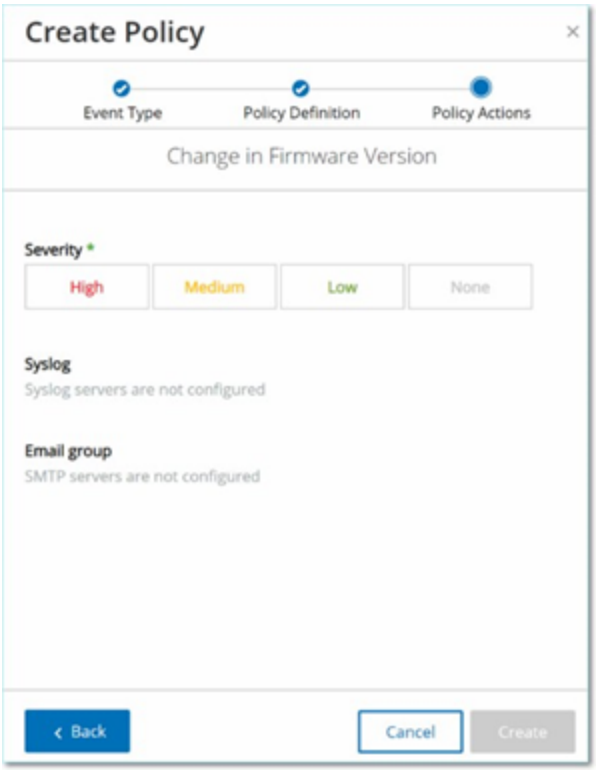
> **Remarque :** si le groupe spécifique auquel vous souhaitez que la politique s'applique n'existe pas, vous pouvez créer un groupe en fonction de vos besoins. Voir Groupes.

d. Pour les paramètres d'asset (c'est-à-dire assets sources, cibles et affectés), si vous souhaitez ajouter un groupe d'assets/segment réseau avec une condition « Ou », cliquez sur le bouton bleu « **+ Ou** » à côté du champ et sélectionnez un autre groupe d'assets/segment réseau.

e. Pour les paramètres d'asset (c'est-à-dire assets sources, cibles et affectés), si vous souhaitez ajouter un groupe d'assets/segment réseau avec une condition « Et », cliquez sur le bouton bleu « **+ Et** » à côté du champ et sélectionnez un autre groupe d'assets/segment réseau.

7. Cliquez sur **Suivant**.

Une série de paramètres d'action de politique (c'est-à-dire les actions exécutées par le système lorsqu'une correspondance de politique se produit) apparaît.



8. Dans la section **Sévérité**, cliquez sur le niveau de sévérité souhaité pour cette politique.
9. Pour envoyer des journaux d'événements à un ou plusieurs serveurs Syslog, dans la section **Syslog**, cochez la case à côté de chaque serveur auquel vous souhaitez envoyer les journaux d'événements.

   Remarque : pour ajouter un serveur Syslog, voir Serveurs Syslog.

10. Pour envoyer des notifications d'événement par e-mail, dans le champ Groupe de messagerie, sélectionnez le groupe de messagerie à notifier dans la liste déroulante.

    Remarque : pour ajouter un serveur SMTP, voir Serveurs SMTP.

11. Dans la section **Actions supplémentaires**, lorsque l'action spécifiée est pertinente :

- Pour désactiver la politique après la première correspondance, cochez la case **Désactiver la politique après la première correspondance**. (Cette action est pertinente pour certains types de politiques d'événements réseau et certains types de politiques d'événements SCADA.)
- Pour lancer automatiquement un instantané de l'asset affecté chaque fois qu'une correspondance avec la politique est détectée, cochez la case **Prendre un instantané après une correspondance avec la politique**. (Cette action est pertinente pour certains types de politiques d'événements de configuration.)

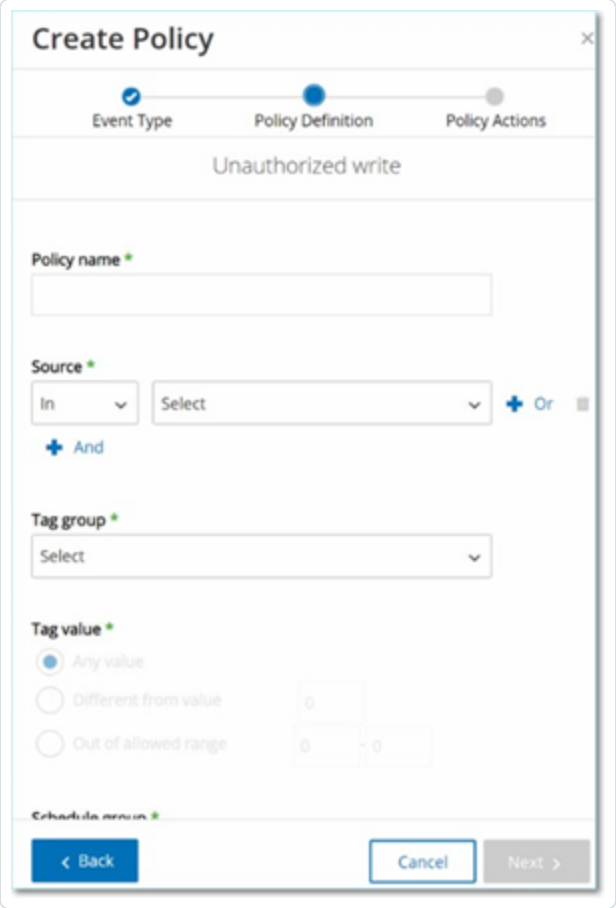
12. Cliquez sur **Créer**. La nouvelle politique est créée et automatiquement activée. La politique apparaît maintenant dans la liste de l'écran Politiques.

Création de politiques d'écriture non autorisée

Ce type de politique détecte les écritures non autorisées sur les tags de contrôleur. La définition de la politique nécessite de spécifier les groupes de tags pertinents et le type d'écriture qui génère une correspondance avec la politique.

Pour établir la définition d'une politique d'écriture non autorisée :

1. Créez une politique d'écriture non autorisée comme décrit dans Créer des politiques.



2. Dans la section Définition de la politique, dans le champ **Groupe de tags**, sélectionnez le groupe de tags auquel cette politique s'applique.
3. Dans la section **Valeur du tag**, sélectionnez l'option souhaitée en cliquant sur le bouton radio et en remplissant les champs requis. Les options sont :
    - **N'importe quelle valeur** – Sélectionnez cette option pour détecter toute modification de la valeur du tag.
    - **Différent de la valeur** – Sélectionnez cette option pour détecter toute valeur autre que la valeur spécifiée. Saisissez la valeur spécifiée dans le champ à côté de cette sélection.
    - **Hors plage autorisée** – Sélectionnez cette option pour détecter toute valeur en dehors de la plage spécifiée. Saisissez les limites inférieure et supérieure de la plage autorisée dans les champs respectifs à côté de cette sélection.

> **Remarque :** les options Différent de la valeur et Hors plage autorisée ne sont disponibles que pour les types de tags standard (par exemple, entier, booléen, etc.), mais pas pour les tags ni les chaînes personnalisés.

4. Effectuez les procédures de création de politique décrites dans Créer des politiques.

Autres actions sur les politiques

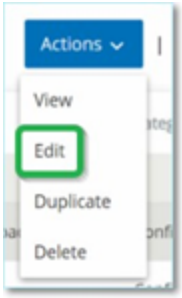
Modifier des politiques

Vous pouvez modifier la configuration des politiques prédéfinies et définies par l'utilisateur. Pour la plupart des politiques, vous pouvez ajuster à la fois les paramètres **Définition de la politique** (conditions de la politique) et les paramètres **Actions de la politique**. Pour les **politiques de détection d'intrusion**, vous pouvez uniquement ajuster les paramètres **Actions de la politique**.

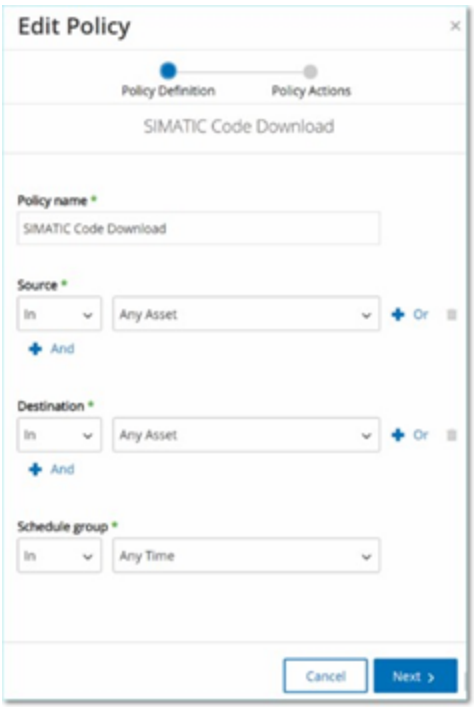
Vous pouvez également modifier les paramètres **Actions de la politique** de plusieurs politiques à la fois.

Pour modifier une politique :

1. Dans la fenêtre **Politiques**, cochez la case à côté de la politique souhaitée.
2. Dans la zone déroulante **Actions**, sélectionnez **Modifier**.



3. La fenêtre **Modifier la politique** apparaît avec la configuration actuelle.



4. Ajustez les paramètres **Définition de la politique** selon vos besoins.

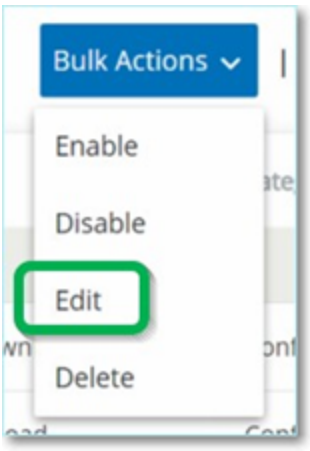
   > **Remarque :** vous ne pouvez pas modifier les groupes d'assets **sources** et **cibles** pour les événements du système de détection d'intrusion (IDS).

5. Cliquez sur **Suivant**.
6. Ajustez les paramètres **Actions de la politique** selon vos besoins.
7. Cliquez sur **Enregistrer**.

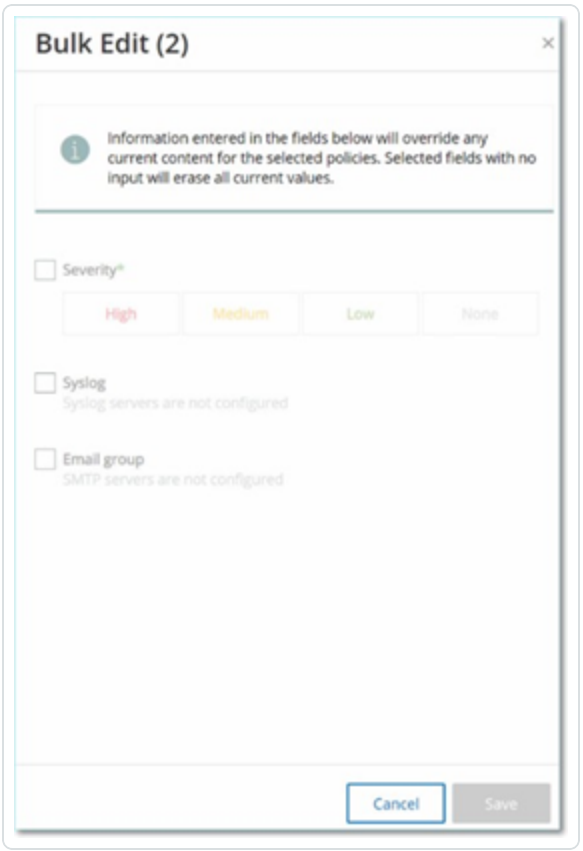
   OT Security enregistre la politique avec la nouvelle configuration.

Pour modifier plusieurs politiques (action en bloc) :

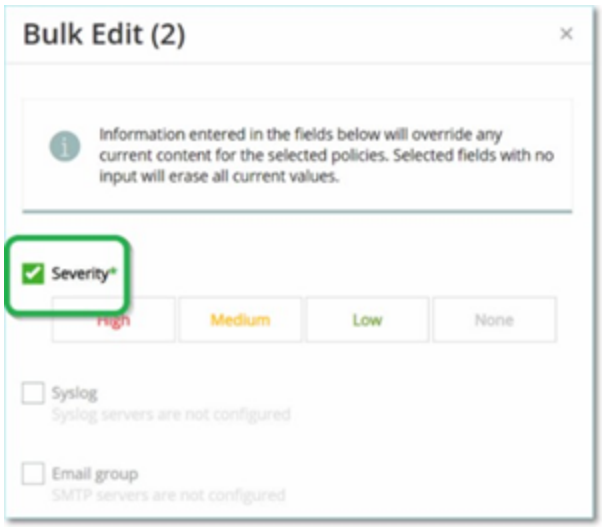
1. Dans la fenêtre **Politiques**, cochez les cases pour deux politiques ou plus.
2. Dans la zone déroulante **Actions en bloc**, sélectionnez **Modifier**.



3. La fenêtre **Modifier en bloc** apparaît avec toutes les actions de politique disponibles pour la modification en bloc.



4. Cochez la case à côté de chacun des paramètres que vous souhaitez modifier : **Sévérité**, **Syslog** et **Groupe de messagerie**.



5. Définissez chaque paramètre selon vos besoins.

   > **Remarque :** les informations saisies dans la fenêtre **Modifier en bloc** remplacent tout contenu actuel pour les politiques sélectionnées. Si vous cochez la case d'un paramètre sans y saisir une sélection, les valeurs actuelles du paramètre sont effacées.

6. Cliquez sur **Enregistrer**.

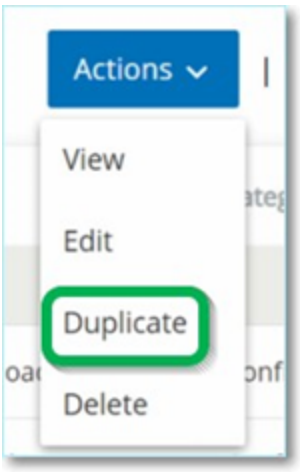
   OT Security enregistre les politiques avec la nouvelle configuration.

Dupliquer des politiques

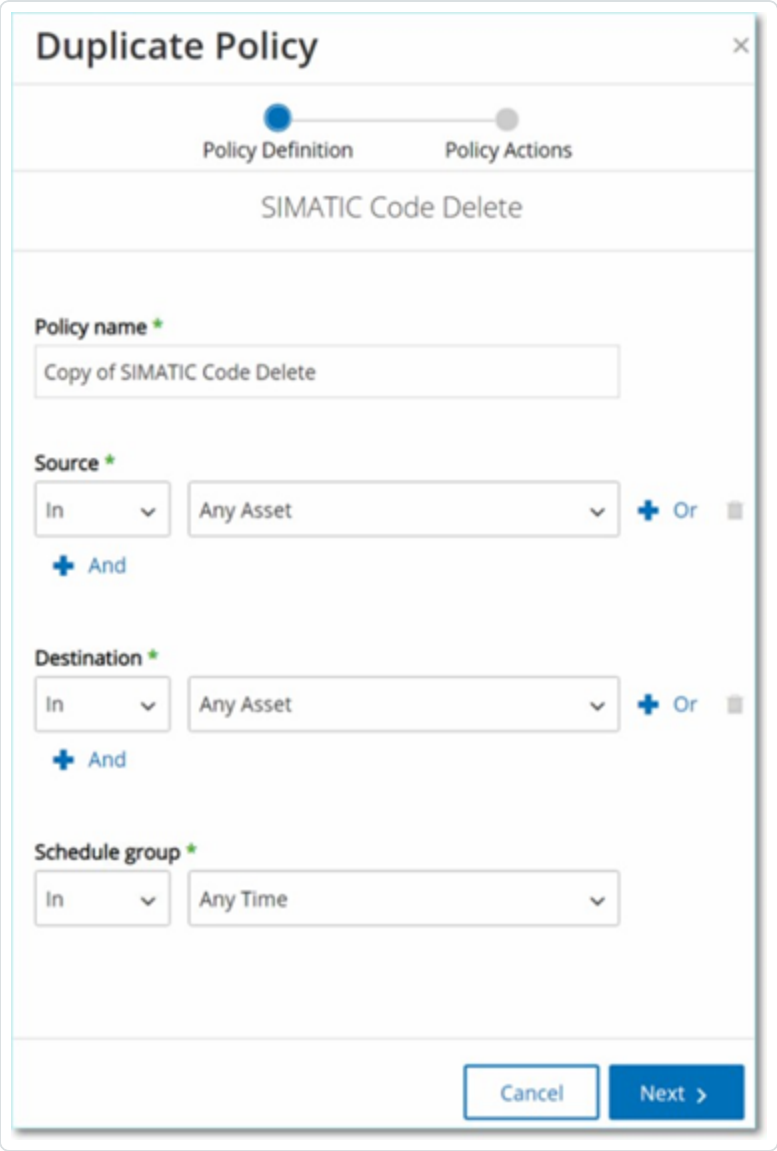
Vous pouvez créer une nouvelle politique similaire à une politique existante en dupliquant la politique d'origine et en effectuant les ajustements souhaités. Vous pouvez dupliquer les politiques prédéfinies et définies par l'utilisateur (à l'exception des **politiques de détection d'intrusion**).

Pour dupliquer une politique :

1. Dans la fenêtre **Politiques**, cochez la case à côté de la politique souhaitée.
2. Dans la zone déroulante **Actions**, sélectionnez **Dupliquer**.



3. La fenêtre **Dupliquer la politique** apparaît avec la configuration actuelle et propose par défaut le nom « *Copie de <Nom de la politique d'origine>* ».



4. Ajustez les paramètres **Définition de la politique** selon vos besoins.
5. Cliquez sur **Suivant**.
6. Ajustez les paramètres **Actions de la politique** selon vos besoins.
7. Cliquez sur **Enregistrer**.

   OT Security enregistre la politique avec la nouvelle configuration.

Supprimer des politiques

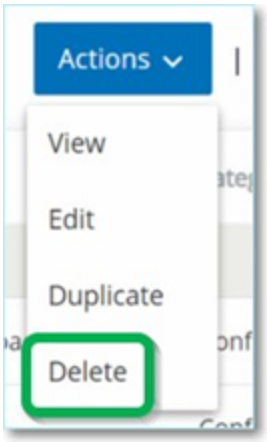
Vous pouvez supprimer une politique du système. Vous pouvez supprimer les politiques prédéfinies et définies par l'utilisateur (à l'exception des **politiques de détection d'intrusion** qui ne peuvent pas être supprimées).

Vous pouvez également supprimer plusieurs politiques à la fois.

Remarque : une fois que vous avez supprimé une politique du système, vous ne pouvez plus la réactiver. Une autre option consiste à la désactiver temporairement à l'aide du **curseur**, et ainsi garder la possibilité de la réactiver plus tard.

Pour supprimer une politique :

1. Dans la fenêtre **Politiques**, cochez la case à côté de la politique souhaitée.
2. Dans la zone déroulante **Actions**, sélectionnez **Supprimer**.



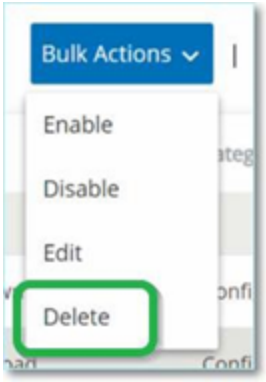
   Une fenêtre de confirmation apparaît.

3. Cliquez sur **Supprimer**.

   OT Security supprime la politique du système.

Pour supprimer plusieurs politiques à la fois :

1. Dans la fenêtre **Politiques**, cochez la case à côté de chacune des politiques souhaitées.
2. Dans la zone déroulante **Actions en bloc**, sélectionnez **Supprimer**.



Une fenêtre de confirmation apparaît.

3. Cliquez sur **Supprimer**.

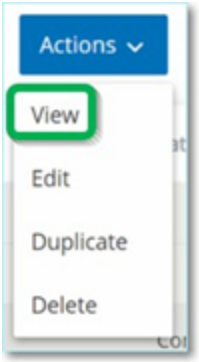
   OT Security supprime les politiques du système.

Supprimer des exclusions de politique

Pour supprimer une exclusion appliquée à une politique donnée, vous pouvez le faire sur l'écran **Politiques**.

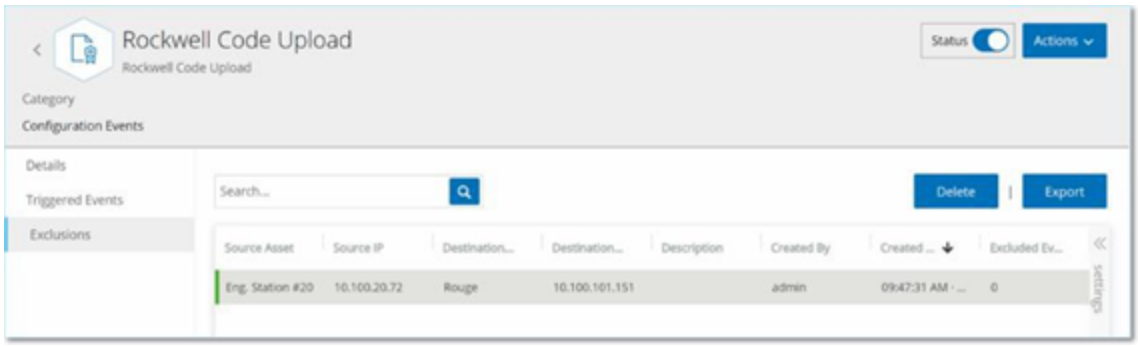
Pour supprimer une exclusion de politique :

1. Dans la fenêtre **Politiques**, sélectionnez la politique souhaitée.
2. Dans la zone déroulante **Actions**, sélectionnez **Afficher**.



> **Remarque :** vous pouvez également accéder au menu Actions en effectuant un clic droit sur la politique pertinente.

3. Cliquez sur l'onglet **Exclusions**.



Une liste d'exclusions apparaît.

4. Sélectionnez l'exclusion de politique que vous souhaitez supprimer.
5. Cliquez sur **Supprimer**.

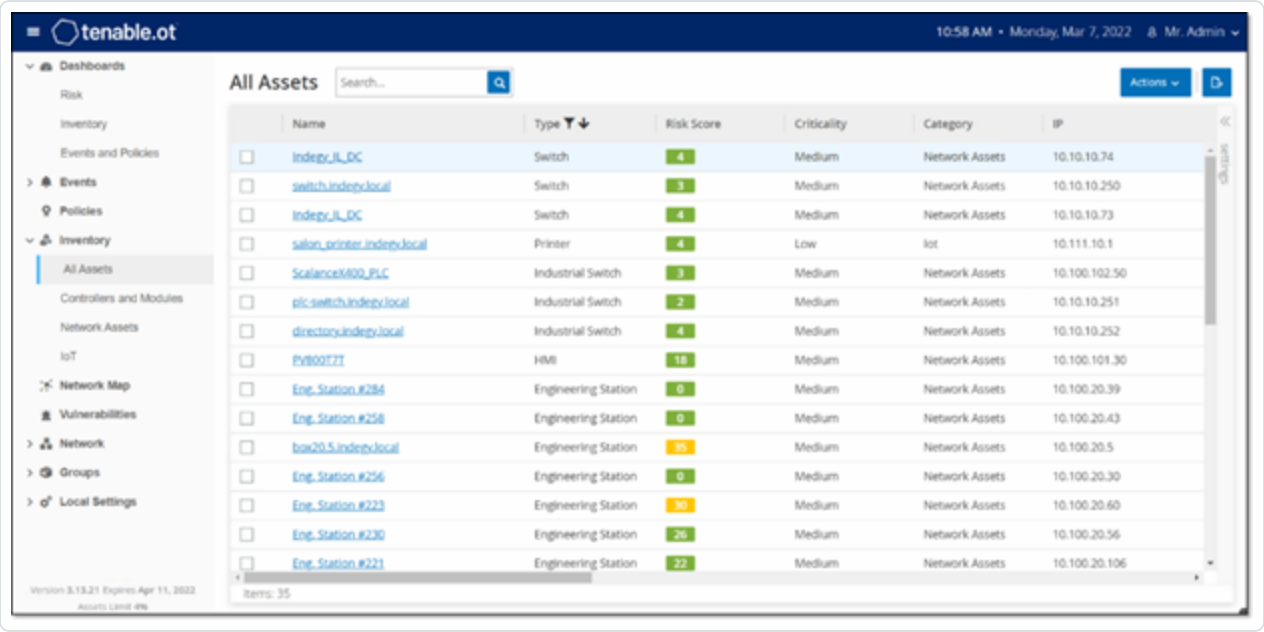
   Une fenêtre de confirmation apparaît.
6. Dans la fenêtre de confirmation, cliquez sur **Supprimer**.

   OT Security supprime l'exclusion du système.

Inventaire

Les fonctions automatisées de découverte, de classification et de gestion des assets de OT Security fournissent un inventaire précis et à jour par le biais d'un suivi continu de toutes les modifications apportées aux appareils. Cela simplifie le maintien de la continuité, de la fiabilité et de la sécurité opérationnelles. Cela joue également un rôle clé dans la planification des projets de maintenance, la priorisation des mises à niveau, les déploiements de correctifs, la réponse aux incidents et les efforts d'atténuation.

Affichage des assets



Tous les assets du réseau apparaissent sur les pages **Inventaire**. Les pages Inventaire contiennent des données détaillées sur l'asset, permettant une gestion complète des assets ainsi que la surveillance de l'état de chaque asset et des événements associés. OT Security collecte ces données à l'aide des fonctionnalités de détection réseau et de requête active. La page **Tout** affiche les données de tous les types d'assets. De plus, des sous-ensembles spécifiques d'assets sont affichés sur des écrans distincts pour chacun des types d'assets suivants : **Contrôleurs et modules**, **Assets réseau** et **IoT**.

> **Remarque :** l'écran Assets réseau comprend tous les types d'assets qui ne sont pas inclus dans les écrans Contrôleurs et modules ou IoT.

Pour chacune des pages d'assets (**Tout**, **Contrôleurs et modules**, **Assets réseau**et **IoT**), vous pouvez personnaliser les paramètres d'affichage en ajustant les colonnes affichées et l'emplacement de chaque colonne. Vous pouvez également trier et filtrer les listes d'assets, mais aussi lancer une recherche. Pour plus d'informations sur la personnalisation des tableaux, voir Éléments de l'interface utilisateur de la console de gestion.

Le tableau suivant décrit les paramètres affichés sur les pages **Inventaire**.

Les paramètres marqués d'un « * » ne sont affichés que sur la page **Contrôleurs**.

Paramètre	Description
Nom	Le nom de l'asset sur le réseau. Cliquez sur le nom de l'asset pour afficher

	ses détails (voir Inventaire).
IP	L'adresse IP de l'asset. **Remarque :** un asset peut avoir plusieurs adresses IP. **Remarque :** les adresses IP étiquetées Direct sont celles avec lesquelles Tenable a établi une connexion directe. S'il n'y a pas d'étiquette, cela signifie que Tenable a découvert l'IP sans communication directe. **Remarque :** les assets peuvent être filtrés par plage d'adresses IP. Pour plus d'informations sur le filtrage, voir Éléments de l'interface utilisateur de la console de gestion.
MAC	L'adresse MAC de l'asset.
Segment réseau	Le segment réseau auquel les adresses IP de cet asset sont attribuées.
Type	Le type d'asset, contrôleur , E/S ou communication, etc. Voir Types d'assets.
Fond de panier*	L'unité de fond de panier à laquelle l'asset est connecté. Des détails supplémentaires sur la configuration du fond de panier sont affichés sur l'écran des détails de l'asset.
Emplacement*	Pour les assets qui se trouvent sur des fonds de panier, affiche le numéro de l'emplacement auquel l'asset est attaché.
Fournisseur	Le fournisseur d'assets.
Famille*	Nom de famille du produit tel que défini par le fournisseur de l'asset.
Firmware	La version du firmware actuellement installée sur l'asset.
Localisation	L'emplacement de l'asset tel que vous le saisissez dans les détails de l'asset OT Security. Voir Modifier les détails de l'asset.
Dernière détection	La date et l'heure auxquelles l'appareil a été détecté pour la dernière fois par OT Security. Il s'agit de la dernière fois que l'appareil s'est connecté au réseau ou a effectué une activité.

OS	Le système d'exploitation exécuté sur l'asset.
Nom du modèle	Le nom du modèle de l'asset.
État*	L'état de l'appareil. Valeurs possibles : • Backup (Sauvegarde) – Le contrôleur s'exécute en tant que sauvegarde d'un contrôleur principal. • Fault (Erreur) – Le contrôleur est en panne. • NoConfig (Pas de config) – Aucune configuration n'a été définie pour le contrôleur. • Running (En cours d'exécution) – Le contrôleur est en cours d'exécution. • Stopped (Arrêté) – Le contrôleur ne fonctionne pas. • Unknown (Inconnu) – L'état est inconnu.
Description	Une brève description de l'asset OT Security, dont les détails ont été configurés par l'utilisateur. Voir Modifier les détails de l'asset.
Risque	Une mesure du degré de risque lié à cet asset sur une échelle de 0 (aucun risque) à 100 (risque extrêmement élevé). Pour une explication de la façon dont le score de risque est calculé, voir Évaluation des risques.
Criticité	Mesure de l'importance de l'asset pour le bon fonctionnement du système. Une valeur est attribuée automatiquement à chaque asset en fonction de son type. Vous pouvez ajuster manuellement la valeur.
Niveau Purdue	Le niveau Purdue de l'asset (0=Processus physique, 1=Appareils intelligents, 2=Systèmes de contrôle, 3=Systèmes d'exploitation de fabrication, 4=Systèmes logistiques d'entreprise).
Champ personnalisé	Vous pouvez créer des champs personnalisés pour étiqueter vos assets avec des informations pertinentes. Le champ personnalisé peut être un lien vers une ressource externe.

Types d'assets

Le tableau suivant décrit les différents types d'assets identifiés par OT Security. Il affiche également l'icône qui représente chaque type d'asset dans la console de gestion de OT Security (par exemple, sur l'écran Cartographie du réseau).

Catégorie	Niveau de criticité/ Niveau Purdue par défaut	Description	Sous-types	
Contrôleurs	High / 1 (Haut / 1)	Un système de contrôle informatique industriel qui surveille en permanence l'état des appareils d'entrée et prend des décisions basées sur un programme personnalisé pour contrôler l'état des appareils de sortie. Cette catégorie comprend tous les types de contrôleurs et leurs composants associés.		Contrôleur
				PLC
				DCS
				IED
				RTU
				Contrôleur BMS
				Robot
				Module de communication
				Module E/S
				CNC
				Alimentation

				Module de fond de panier
Appareils de terrain	High / 1 (Haut / 1)	Appareil industriel (par exemple, capteur, actionneur, moteur électrique) qui utilise des protocoles industriels pour envoyer des informations aux systèmes ICS.		Appareil de terrain
				Wattmètre
				E/S à distance
				Relais
				Onduleur
				Capteur industriel
				Lecteur
				Actionneur
Appareils OT	Medium / 2 (Moyen / 2)	Cette catégorie comprend tous les types d'appareils OT.		Appareil OT
				Routeur

				industriel
				Commutateur industriel
				Passerelle industrielle
				Appareil réseau industriel
				Imprimante industrielle
Serveurs OT	Medium / 2 (Moyen / 2)	Ordinateur/appareil utilisé pour accéder aux données industrielles. Cette catégorie comprend tous les types de serveurs OT et leurs composants associés.		Serveur OT
				Historien opérationnel
				IHM
				Enregistreur de données

Appareils réseau	Medium / 3 (Moyen / 3)	Appareil réseau (par exemple, un commutateur ou un routeur). Cette catégorie comprend tous les types d'appareils réseau et leurs composants associés.		Appareil réseau
				Routeur
				Commutateur
				Pont Série-Ethernet
				Passerelle
				Hub
				Point d'accès sans fil
				Pare-feu

				Convertisseur
				Répétiteur
				Radio
Postes de travail	Low / 3 (Faible / 3)	Un ordinateur connecté au réseau et utilisé pour contrôler les PLC. Cette catégorie comprend tous les types de postes de travail et leurs composants associés.		Poste de travail
				Poste de travail OT
				Station d'ingénierie
				Poste de travail virtuel
Serveurs	Low / 3 (Faible / 3)	Cette catégorie comprend divers types de serveurs		Serveur

		informatiques.		
				Serveur de fichiers
				Serveur web
				Serveur virtuel
				Appliance de sécurité
				TenableICP
				TenableEM
				CapteurTenable
				Contrôleur de domaine
				Internet des objets (IoT)

Internet des objets (IoTs)	Low / 3 (Faible / 3)	Cette catégorie comprend divers types d'appareils interdépendants.		Caméra
				Panneau
				Projecteur
				Appareil VOIP
				Imprimante 3D
				Imprimante
				UPS
				Téléphone IP
				Capteur intelligent
				Lecteur de code-barres

				Système de contrôle d'accès
				Contrôle d'éclairage
				Module HVAC
				SmartHub
				SmartTV
				Appareil médical
				Tablette
				Appareil mobile
				Périphérique de stockage
Terminaux	Low / 3	Une adresse IP non		Terminal

	(Faible / 3)	identifiée sur le réseau.		

Afficher les détails d'un asset

La page des **détails de l'asset** affiche des détails complets sur toutes les données découvertes par OT Security pour un asset sélectionné. Les détails apparaissent dans la barre d'en-tête ainsi que dans plusieurs onglets et sous-sections. Certains ne sont pertinents que pour des types d'assets spécifiques.

Pour accéder à la page des **détails de l'asset** pour un asset spécifique :

1. Effectuez l'une des actions suivantes :
    - Cliquez sur le nom de l'asset sur l'une des pages suivantes où son nom apparaît sous forme de lien : **Inventaire**, **Événements** ou **Réseau**.
    - Sur la page **Inventaire**, cliquez sur **Actions** > **Afficher**.

Les éléments suivants sont inclus dans la fenêtre des **détails de l'asset** (pour les types d'assets pertinents) :

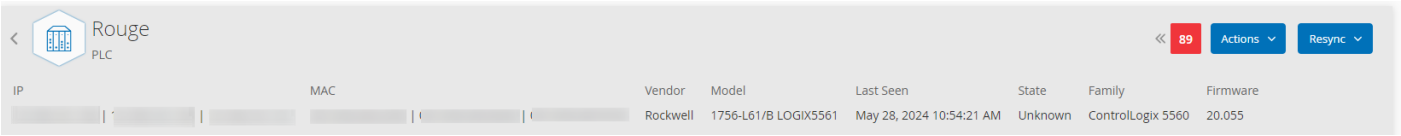
- **Volet d'en-tête** – Affiche un aperçu des informations essentielles sur l'asset et son état actuel. Il contient également un menu Actions qui vous permet de modifier les listes dans lesquelles cet asset est présent.
- **Détails** – Affiche des informations détaillées divisées en sous-sections avec des données spécifiques pertinentes pour différents types d'assets.
- **Révisions de code** (uniquement pour les contrôleurs) – Affiche des informations sur les révisions de code actuelles et précédentes découvertes par la fonction « instantané » de OT Security. Cela inclut des détails sur toutes les modifications spécifiques introduites dans le code, c'est-à-dire les sections (blocs de code/séquences) qui ont été ajoutées, supprimées, ou modifiées.
- **Itinéraire IP** – Affiche toutes les adresses IP actuelles et anciennes liées à l'asset.
- **Vecteurs d'attaque** – Affiche les vecteurs d'attaque vulnérables, c'est-à-dire les routes qu'un attaquant peut utiliser pour accéder à cet asset. Vous pouvez générer un vecteur d'attaque

automatiquement, afin d'afficher le vecteur d'attaque le plus critique. Vous pouvez aussi générer manuellement des vecteurs d'attaque à partir d'assets spécifiques.

- **Ports ouverts** – Affiche des informations sur les ports ouverts sur l'asset.
- **Vulnérabilités** – Affiche les vulnérabilités corrigées et actives identifiées par le système pour l'asset sélectionné, telles que les systèmes d'exploitation Windows obsolètes, l'utilisation de protocoles vulnérables et les ports de communication ouverts connus pour être risqués ou non essentiels pour des types d'appareils spécifiques. Voir Vulnérabilités.
- **Événements** – Une liste d'événements sur le réseau impliquant l'asset.
- **Cartographie du réseau** – Affiche une représentation graphique des connexions réseau de l'asset.
- **Ports du périphérique** (pour les commutateurs réseau) – Affiche des informations sur les ports du commutateur réseau.

Volet d'en-tête

Le volet d'en-tête affiche un aperçu de l'état actuel de l'asset.



L'affichage comprend les éléments suivants :

- **Nom** – Le nom de l'asset.
- < Retour (lien) – Vous renvoie à l'écran à partir duquel vous avez accédé à cet écran d'asset.
- **Type d'asset** – Affiche l'icône et le nom du type d'asset.
- **Aperçu de l'asset** – Affiche des informations essentielles sur l'asset : adresses IP, fournisseur, famille, modèle, firmware et dernière détection (date et heure).
- **Widget Score de risque** – Affiche le score de risque de l'asset. Le score de risque est une évaluation (de 1 à 100) du degré de menace posé à l'asset. Pour une explication de la façon dont la valeur est déterminée, voir Évaluation des risques. Cliquez sur l'indicateur de score de risque pour afficher un widget étendu décrivant de façon exhaustive les facteurs qui permettent d'évaluer le niveau de risque (événements non résolus, vulnérabilités et criticité).

Certains des éléments sont un lien vers l'écran correspondant, qui affiche des détails sur cet élément.

- Menu **Actions** – Vous permet de modifier les détails de l'asset ou d'exécuter un scan Tenable Nessus.
- **Resynchroniser** – Cliquez sur ce bouton pour exécuter manuellement une ou plusieurs des requêtes disponibles pour cet asset. Voir Exécuter une resynchronisation.

Détails

L'onglet **Détails** affiche des détails supplémentaires sur l'asset sélectionné. Les informations sont divisées en sections montrant différents types de données système et de configuration pour l'asset spécifié. OT Security affiche uniquement les sections pertinentes pour l'asset spécifié. La liste suivante répertorie toutes les catégories de section possibles pour différents types d'assets : Vue d'ensemble, Général, Projet, Mémoire, Ethernet, Profinet, OS, Système, Matériel, Appareils et lecteurs, Appareils USB, Logiciel installé, CEI 61850 et Statut de l'interface.

Remarque : OT Security affiche uniquement les détails qu'il extrait de l'asset. Il se peut que les sections ne soient pas toutes affichées pour tous les assets. Par exemple, **Général**, **Informations sur le scan Nessus**.

Le tableau suivant affiche les détails dans la section **Vue d'ensemble** :

Section	Description
Nom	Nom de l'asset obtenu soit par surveillance passive, soit par requête active, ou généré automatiquement à l'aide du type d'asset et d'un identifiant unique.
Description	La description de l'asset de l'utilisateur.
Niveau Purdue	Le niveau du modèle Purdue attribué à l'asset.
État	Statut opérationnel actuel de l'asset. Ce champ est utile pour des types d'assets spécifiques, et en particulier pour les contrôleurs.
IP directe	L'adresse IP présente sur ou configurée pour cet asset ou ce module

	spécifique.
Mac directe	L'adresse Mac présente physiquement sur cet asset ou ce module spécifique, ou configurée pour celui-ci.
IP supplémentaires	Adresses IP associées à d'autres modules partageant un fond de panier ou une infrastructure similaire avec l'asset, et utilisées pour accéder indirectement à l'asset. Par exemple, un PLC (module de contrôleur) peut ne pas disposer de sa propre interface réseau, mais être accessible via une adresse IP configurée sur un module de communication installé dans un emplacement différent. Notez que l'asset peut avoir des connexions autres qu'un fond de panier.
Mac supplémentaires	Adresses Mac associées à d'autres modules partageant un fond de panier ou une infrastructure similaire, et utilisées pour accéder indirectement à l'asset.
Famille	La famille d'appareils ou la ligne de produits à laquelle l'asset appartient.
Fournisseur	Le fabricant ou fournisseur de l'asset.
Nom du modèle	Le numéro de modèle spécifique de l'asset.
Dernière détection	La date et l'heure auxquelles OT Security a détecté l'asset pour la dernière fois. OT Security peut mettre à jour ce champ lors de la relecture d'un PCAP (fichier de capture de trafic) ou de la réalisation d'une analyse similaire.
Première détection	La date et l'heure auxquelles l'asset a été détecté pour la première fois. Cette valeur peut être identique ou antérieure à **Dernière détection**.
Dernière mise à jour	La date et l'heure de la dernière mise à jour des détails de l'asset. **Remarque** : toute modification manuelle des informations de l'asset (la description, par exemple) met à jour cette valeur, que l'asset soit actuellement actif ou récemment détecté.

Sources	Les sources (capteurs, PCAP, interfaces locales, etc.) identifiées ou associées à l'asset.
Segments réseau	Les segments réseau attribués ou associés à l'asset.
Criticité	L'importance de l'asset évalué comme Élevée, Moyenne ou Faible.
Score de risque	Reflète l'impact potentiel du risque associé à l'asset. Le score est affecté par des facteurs tels que la criticité, les vulnérabilités, les événements non résolus (et leur durée), les assets associés (par exemple, via le fond de panier) et d'autres considérations pertinentes.

Pour les assets connectés à un fond de panier, il existe également une section « Vue du fond de panier », qui affiche une représentation graphique de la configuration du fond de panier avec l'emplacement de chaque appareil connecté. Sélectionnez un appareil pour afficher ses détails dans le volet inférieur.

Révisions de code

L'onglet **Révision de code** (pour les contrôleurs uniquement) affiche les différentes versions du code du contrôleur capturées par les « instantanés » de OT Security. Chaque version « instantanée » inclut des informations sur la révision du code au moment où « l'instantané » a été pris, en incluant des détails sur des sections spécifiques (blocs de code/séquences) et des tags. Chaque fois qu'un « instantané » n'est pas identique à « l'instantané » de ce contrôleur, une nouvelle version de la révision de code est créée. Vous pouvez comparer les versions pour voir quelles modifications ont été apportées au code du contrôleur.

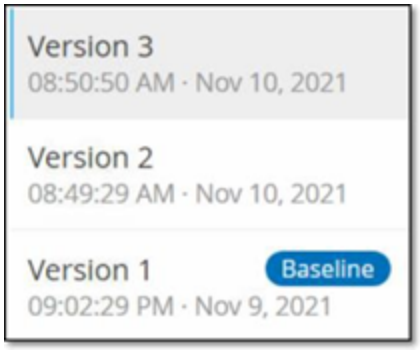
Un instantané peut être déclenché des manières suivantes :

- **Routine** – Les instantanés sont pris à intervalles réguliers, définis par l'utilisateur dans les paramètres du système.
- **Déclenché par une activité** – Le système déclenche un instantané lorsqu'une activité spécifique liée au code est détectée (par exemple, un téléchargement de code).
- **Lancé par l'utilisateur** – L'utilisateur peut déclencher manuellement un instantané en cliquant sur le bouton Prendre un instantané pour un asset spécifique.

Vous pouvez configurer une politique « Déviation par rapport à l'instantané » pour détecter les ajouts, les suppressions ou les modifications apportées au code d'un contrôleur. Voir Événement de configuration – Types d'événement liés aux activités du contrôleur.

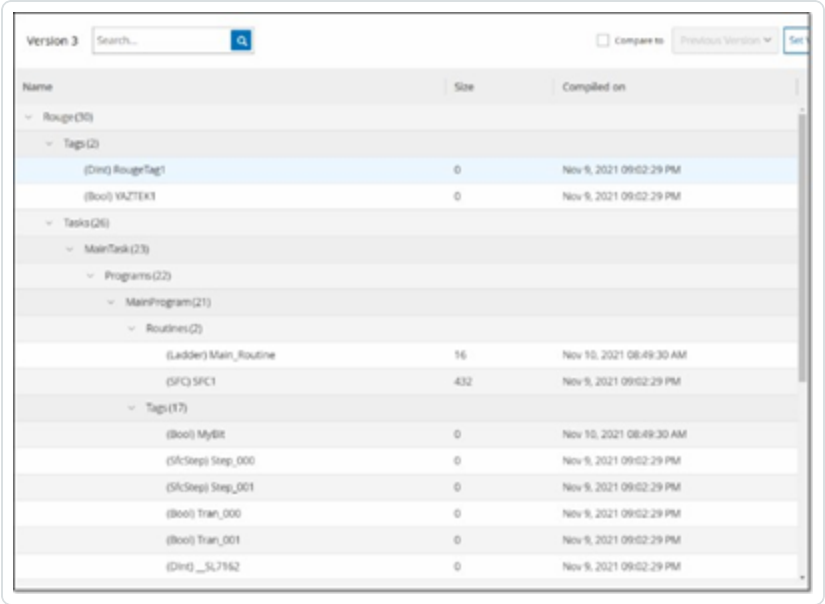
Les sections suivantes décrivent les différentes sections de l'affichage de la révision de code ainsi que la manière de comparer différentes versions « d'instantanés ».

Volet de sélection de version



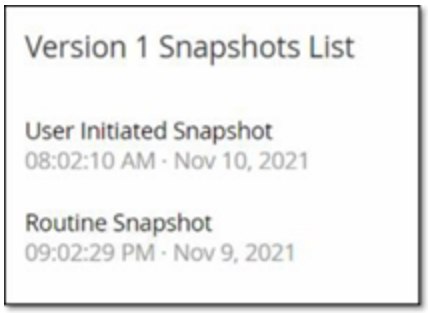
Ce volet affiche une liste de toutes les versions disponibles de la révision de code pour ce contrôleur. Pour chaque version, la date et l'heure de début d'application de la version apparaissent. Une nouvelle version est créée à chaque fois qu'un changement est détecté par rapport au précédent « instantané ». Le tag « Base de référence » indique quelle version est actuellement définie comme version de référence à des fins de comparaison. Sélectionnez une version pour afficher ses révisions de code dans le volet Détails de l'instantané.

Volet des détails d'un instantané



Le volet de détails affiche des informations détaillées sur les blocs de code, les séquences, ainsi que les tags relatifs à la version d'instantané sélectionnée. Les éléments de code sont affichés dans une structure arborescente avec des flèches pour développer/réduire les détails affichés. Pour chaque élément, le nom, la taille et la date de compilation sont affichés. Vous pouvez comparer la version sélectionnée à la version précédente ou à la version « de référence » pour voir quelles modifications ont été apportées. Voir Comparer les versions d'un instantané.

Volet d'historique des versions



Ce volet affiche des détails sur « l'instantané » ayant permis de capturer la version sélectionnée, y compris la méthode par laquelle il a été lancé, ainsi que la date et l'heure de la capture.

Si aucune modification n'a été apportée entre les instantanés, plusieurs instantanés sont regroupés en une seule version. Tous les instantanés identiques sont répertoriés dans le volet d'historique de l'instantané pour cette version.

Comparer les versions d'un instantané

Vous pouvez comparer la version d'un instantané à la version précédente ou à la version de référence. Une fois qu'une comparaison a été lancée, le volet des détails de l'instantané affiche les modifications apportées au code du contrôleur entre les deux instantanés.

Les modifications sont marquées de la manière suivante :

✚ Ajouté – Nouveau code ajouté dans la version sélectionnée.

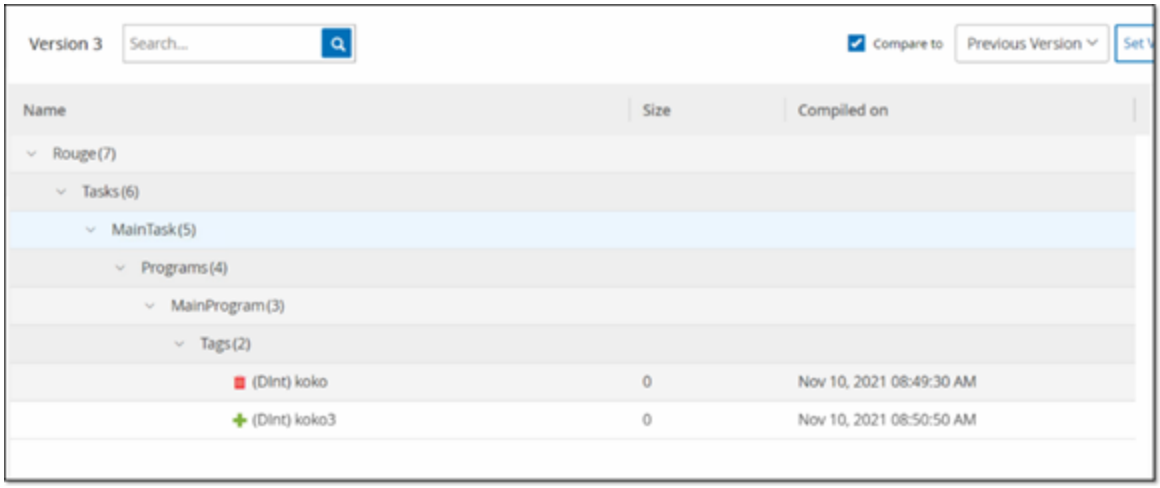
Supprimé – Code supprimé de la version sélectionnée.

Modifié – Code modifié dans la version sélectionnée.

Pour comparer une version d'instantané à la version précédente :

1. Sur l'écran **Inventaire** > **Contrôleurs**, sélectionnez le contrôleur souhaité.
2. Cliquez sur l'onglet **Révision de code**.
3. Dans le volet de **sélection des versions**, sélectionnez la version que vous souhaitez analyser.
4. En haut du volet des **détails de l'instantané**, dans le champ de comparaison, sélectionnez **Version précédente** dans le menu déroulant.
5. Cochez la case **Comparer à**.

   Le volet des détails de l'instantané affiche toutes les différences entre les deux versions. Pour chaque changement, une icône indique le type de changement qui s'est produit.



Pour comparer une version d'instantané à une version ancienne (autre que la version précédente) :

1. Sur l'écran **Inventaire** > **Contrôleurs**, sélectionnez le contrôleur souhaité.
2. Cliquez sur l'onglet **Révision de code**.
3. Dans le volet de **sélection des versions**, sélectionnez la version que vous souhaitez utiliser comme base de comparaison.
4. En haut du volet des **détails de l'instantané**, cliquez sur **Définir la version comme base de référence**.

Le tag **Base de référence** apparaît pour la version sélectionnée, indiquant qu'elle est définie comme version de référence.

> **Remarque :** la définition d'une version comme version de référence n'affecte que les comparaisons effectuées à l'aide de cet écran. Cela n'affecte pas les politiques qui vérifient les déviations par rapport à l'instantané.

5. Dans le volet de **sélection des versions**, sélectionnez la version que vous souhaitez comparer à la version de référence.
6. Cochez la case Comparer à. Dans le champ à côté de cette case, sélectionnez Version de référence dans le menu déroulant.
7. Le volet des détails de l'instantané affiche toutes les différences entre les deux versions. Pour chaque changement, une icône indique le type de changement qui s'est produit.

Créer un instantané

Un instantané peut être lancé manuellement par l'utilisateur. Par exemple, il est recommandé de prendre un instantané avant et après l'intervention d'un technicien sur un contrôleur.

Pour créer un instantané d'un contrôleur :

1. Sur l'écran **Inventaire** > **Contrôleurs**, sélectionnez le contrôleur souhaité.
2. Cliquez sur l'onglet **Révision de code**.
3. Dans le coin supérieur droit du volet des **détails de l'instantané**, cliquez sur **Prendre un instantané**.

   L'instantané lancé par l'utilisateur est créé.
4. Si aucune modification n'est identifiée, un nouvel instantané identifié par l'utilisateur est ajouté au volet d'historique des révisions pour la dernière version. Si des modifications sont identifiées, une nouvelle version est créée indiquant les modifications de révision du code.

Itinéraire IP

L'onglet **Itinéraire IP** affiche toutes les adresses IP pertinentes pour cet asset. La colonne Carte réseau affiche une liste des cartes réseau utilisées par cet asset. Cliquez sur la flèche à côté d'une carte réseau pour développer la liste, afin d'afficher les adresses IP de tous les assets connectés au fond de panier partagé.

Les listes incluent les dates de début et de fin d'utilisation de l'adresse IP. Les options pour la date de fin sont :

- **Active** – L'adresse IP est actuellement utilisée pour cet asset.
- **{date/ heure}** – La dernière date et heure à laquelle l'adresse IP a été active pour cet asset (si elle a été active au cours des 30 derniers jours).
- **{date/ heure} (Inactive)** – La dernière date et heure à laquelle l'adresse IP a été active pour cet asset (si elle a été inactive pendant 30 jours ou plus).
- **Inactive** – L'adresse IP est actuellement utilisée par un autre asset.

Vecteurs d'attaque

Un attaquant peut compromettre un accès critique en profitant d'un « maillon faible » vulnérable dans le réseau pour accéder à l'asset critique. L'asset critique est la cible (destination) de l'attaque, et le vecteur d'attaque est l'itinéraire que l'attaquant utilise pour accéder à cet asset.

Comment déterminer le vecteur d'attaque ?

Une fois l'asset cible spécifié, le système calcule tous les vecteurs d'attaque potentiels qui pourraient permettre l'accès à cet asset et identifie le chemin qui présente le potentiel de risque le plus élevé pour compromettre cet asset. Le calcul prend en compte plusieurs paramètres et utilise une approche basée sur le risque afin d'identifier le vecteur d'attaque le plus critique. Les paramètres incluent :

- Niveau de risque de l'asset
- Longueur du chemin
- Méthode de communication d'asset à asset
- Communication externe (Internet/ Entreprise) et communication interne

Étapes d'atténuation recommandées

Afin de minimiser le risque d'une attaque potentielle utilisant le vecteur sélectionné, les mesures d'atténuation recommandées comprennent ce qui suit :

- Réduire les scores de risque associés et individuels des assets inclus dans le vecteur d'attaque.
- Minimiser ou supprimer l'accès réseau aux réseaux externes (Internet ou réseaux d'entreprise)
- Identifier les canaux de communication tout au long de la chaîne et valider leur pertinence vis-à-vis du processus. Dans le cas où ils ne sont pas essentiels, ils doivent être supprimés (par exemple, fermeture de port ou suppression de service) afin de bloquer le chemin d'attaque potentiel.

Générer des vecteurs d'attaque

Les vecteurs d'attaque doivent être générés manuellement pour chaque asset cible pertinent. Cela se fait dans l'onglet Vecteurs d'attaque pour l'asset cible souhaité. Il existe deux méthodes pour générer des vecteurs d'attaque :

- **Automatique** – OT Security évalue tous les vecteurs d'attaque potentiels et identifie le chemin le plus vulnérable.
- **Manuel** – Vous spécifiez un asset source et OT Security vous montre le chemin potentiel (le cas échéant) qui peut être utilisé pour y accéder.

Pour générer un vecteur d'attaque automatique :

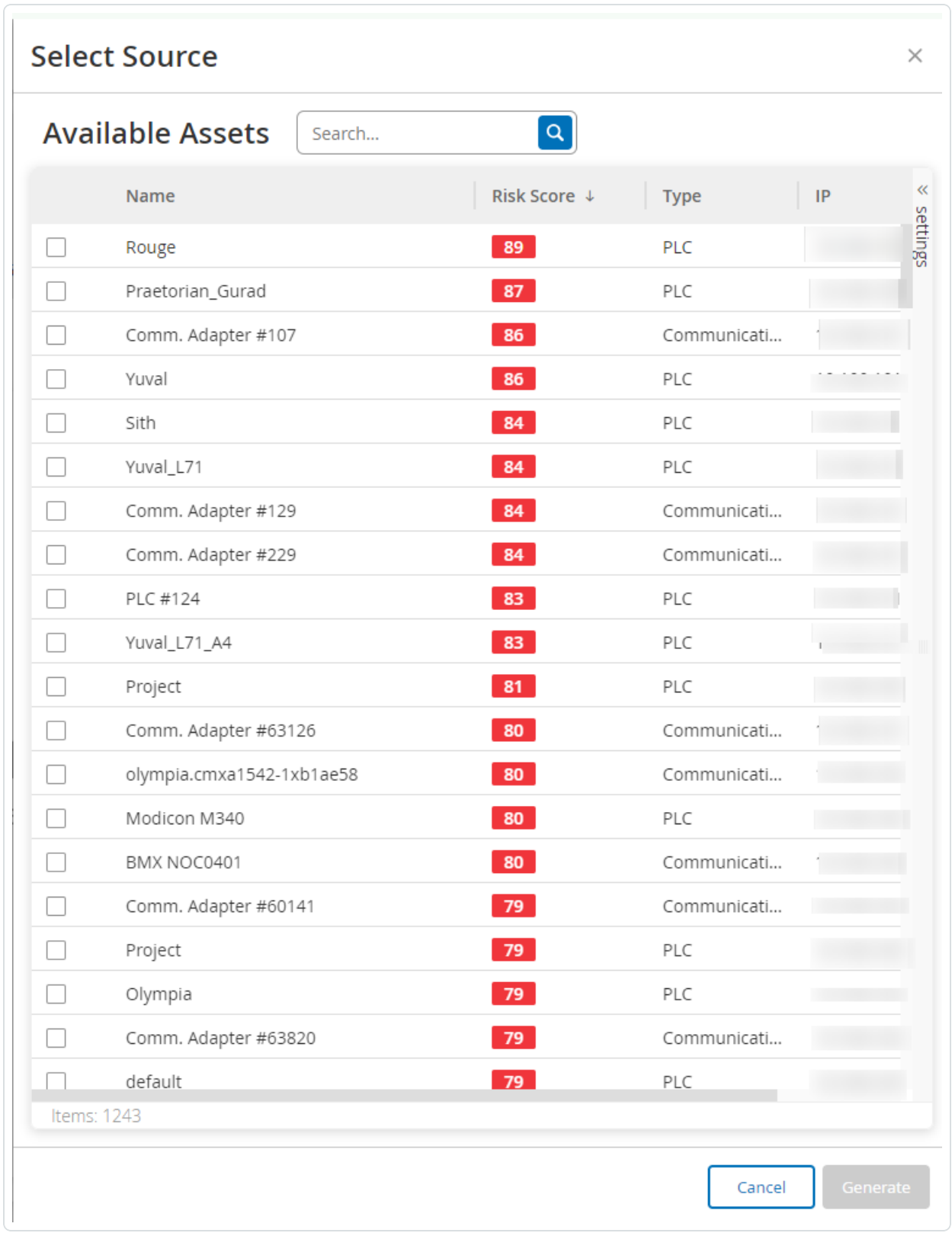
1. Accédez à la page des **détails de l'asset** pour l'asset cible souhaité et cliquez sur l'onglet **Vecteur d'attaque**.
2. Cliquez sur **Générer**, puis sur **Sélectionner la source automatiquement** dans la liste déroulante.

Le vecteur d'attaque est généré automatiquement et apparaît dans l'onglet **Vecteur d'attaque**.

Pour générer un vecteur d'attaque manuel :

1. Accédez à la page des **détails de l'asset** pour l'asset cible souhaité et cliquez sur l'onglet **Vecteur d'attaque**.
2. Cliquez sur **Générer**, puis sur **Sélectionner la source manuellement** dans la liste déroulante.

La fenêtre **Sélectionner la source** apparaît.


Select Source
Available Assets
Search...
Name
Risk Score
Type
IP
settings
Rouge 89 PLC
Praetorian_Gurad 87 PLC
Comm. Adapter #107 86 Communicati...
Yuval 86 PLC
Sith 84 PLC
Yuval_L71 84 PLC
Comm. Adapter #129 84 Communicati...
Comm. Adapter #229 84 Communicati...
PLC #124 83 PLC
Yuval_L71_A4 83 PLC
Project 81 PLC
Comm. Adapter #63126 80 Communicati...
olympia.cmxa1542-1xb1ae58 80 Communicati...
Modicon M340 80 PLC
BMX NOC0401 80 Communicati...
Comm. Adapter #60141 79 Communicati...
Project 79 PLC
Olympia 79 PLC
Comm. Adapter #63820 79 Communicati...
default 79 PLC
Items: 1243
Cancel
Generate

Remarque : par défaut, les assets sources sont triés par score de risque. Vous pouvez régler les paramètres d'affichage ou rechercher l'asset souhaité.

3. Sélectionnez l'asset source souhaité.
4. Cliquez sur **Générer**.

   Le vecteur d'attaque est généré et apparaît dans l'onglet **Vecteur d'attaque**.

Affichage des vecteurs d'attaque

L'onglet Vecteurs d'attaque affiche un diagramme du vecteur d'attaque généré le plus récemment pour l'asset cible spécifié. La case à côté du bouton Générer indique la date et l'heure auxquelles le vecteur d'attaque affiché a été généré. Le diagramme Vecteur d'attaque comprend les éléments suivants :

- Pour chaque asset inclus dans le vecteur d'attaque, le niveau de risque et les adresses IP sont affichés. Cliquez sur une icône d'asset pour afficher des détails supplémentaires sur ses facteurs de risque.
- Pour chaque connexion réseau, le protocole de communication est affiché.
- Les assets qui partagent un fond de panier sont entourés d'un cercle.

Remarque : cliquez sur le bouton d'aide dans le coin supérieur droit de l'onglet Vecteurs d'attaque pour une explication de la fonction Vecteur d'attaque.

Ports ouverts

L'onglet **Ports ouverts** affiche une liste des ports ouverts sur cet asset. Pour chaque port ouvert, des détails sont donnés sur le protocole qu'il utilise, une description de sa fonction, la date et l'heure de la dernière mise à jour des données et la source d'informations (requêtes actives, mappage de port, communications, Tenable Network Monitor ou scans Tenable Nessus) qui indique que le port est ouvert. Une liste distincte des ports ouverts apparaît pour chaque IP disponible pour l'asset (y compris les ports accessibles via un fond de panier partagé). Cliquez sur la flèche à côté d'une adresse IP pour développer la liste et afficher ses ports ouverts.

Il y a une **période d'expiration automatique des ports ouverts**, après laquelle une liste de ports ouverts sera automatiquement supprimée de la liste si aucune autre indication n'a été reçue que le port est toujours ouvert. La durée par défaut est de deux semaines. Pour ajuster la durée de la période d'expiration des ports ouverts, voir Appareil.

Les paramètres de scan des ports ouverts sont configurés dans Requêtes actives. Vous pouvez également exécuter une requête manuelle de l'asset sélectionné pour mettre à jour la liste des ports ouverts.

Pour mettre à jour manuellement la liste des ports ouverts :

1. Dans l'écran **Inventaire** > **Contrôleurs/ Assets réseau**, sélectionnez l'asset souhaité.

   L'écran des **détails de l'asset** apparaît.

2. Cliquez sur l'onglet **Ports ouverts**.

3. Dans le coin supérieur droit du volet Ports ouverts, cliquez sur **Mettre à jour les ports ouverts**.

   Un nouveau scan est exécuté, mettant à jour les ports ouverts affichés pour ce contrôleur.

Actions supplémentaires dans l'onglet Ports ouverts

Dans l'onglet Ports ouverts d'un asset spécifique, vous pouvez effectuer les actions supplémentaires suivantes pour un port ouvert spécifique.

- Scanner – Lance un scan du port sélectionné.
- Afficher – Affiche des détails et des diagnostics supplémentaires sur l'appareil en accédant à l'interface web de l'appareil.

Pour lancer un scan sur un port spécifique :

1. Dans l'écran **Inventaire** > **Contrôleurs/ Assets réseau**, sélectionnez l'asset souhaité.

   L'écran des **détails de l'asset** apparaît.

2. Cliquez sur l'onglet **Ports ouverts**.
3. Sélectionnez un port spécifique.
4. Cliquez sur le menu **Actions**.
5. Dans le menu déroulant, sélectionnez **Scanner**.

   OT Security exécute un scan sur le port sélectionné.

Pour afficher le portail de l'asset :

> **Remarque :** cette option n'est disponible que lorsque le port 80 (utilisé pour l'accès au Web) est l'un des ports ouverts.

1. Dans l'écran **Inventaire** > **Contrôleurs/ Assets réseau**, sélectionnez l'asset souhaité.

   L'écran des **détails de l'asset** apparaît.

2. Cliquez sur l'onglet **Ports ouverts**.
3. Sélectionnez un port spécifique.
4. Cliquez sur le menu **Actions**.
5. Dans le menu déroulant, sélectionnez **Afficher**.

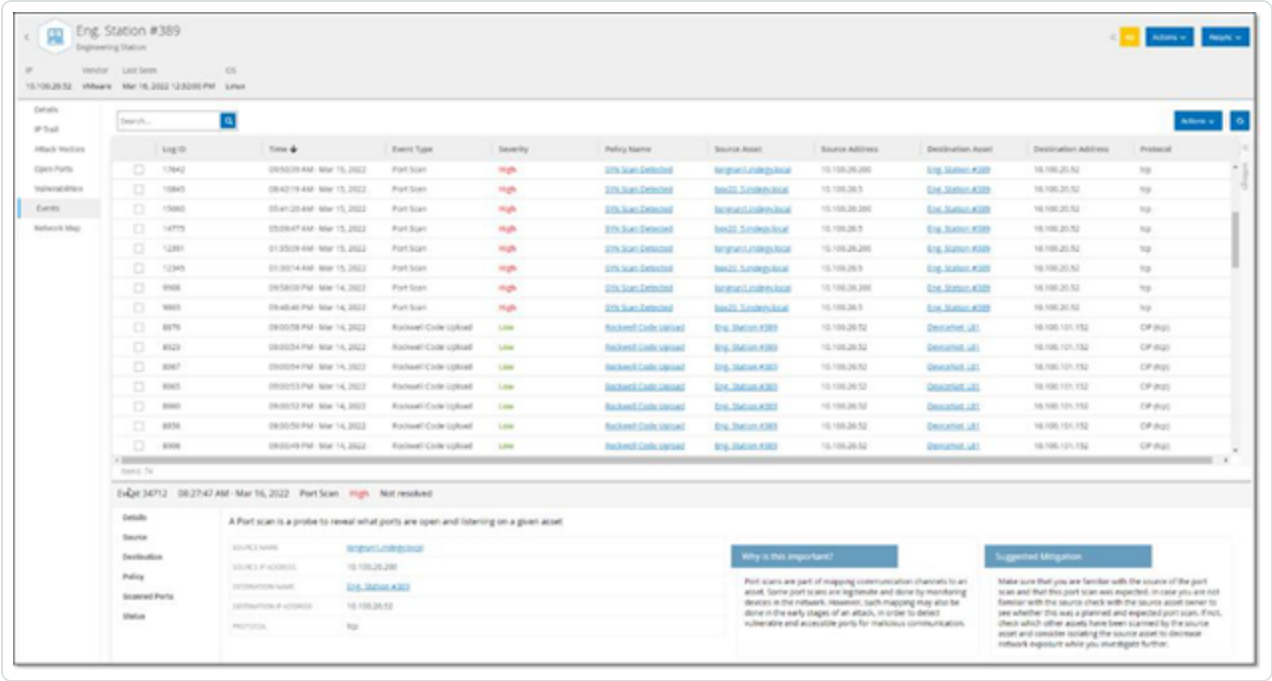
   Un nouvel onglet de navigateur s'ouvre et affiche le portail de cet asset.

Vulnérabilités

L'onglet **Vulnérabilités** affiche la liste de toutes les vulnérabilités qui affectent l'asset spécifié, telles qu'elles sont détectées par les plug-ins OT Security. Le système identifie les vulnérabilités, telles que les systèmes d'exploitation Windows obsolètes, l'utilisation de protocoles vulnérables et les ports de communication ouverts connus pour être risqués ou non essentiels pour des types d'appareils spécifiques. Les vulnérabilités sont répertoriées en deux catégories : **Actives** et **Corrigées**. Chaque liste affiche des détails sur la nature de la menace et sa sévérité. Les informations contenues dans cet onglet sont identiques à celles de la page **Vulnérabilités**, mais seules les vulnérabilités pertinentes pour l'asset spécifié sont affichées. Pour une explication des informations sur les vulnérabilités, voir Vulnérabilités.

Événements

L'onglet **Événements** affiche la liste détaillée des événements du réseau impliquant l'asset, tels que détectés par les plug-ins OT Security. Vous pouvez personnaliser les paramètres d'affichage en ajustant les colonnes affichées et l'emplacement de chaque colonne. Les événements peuvent être regroupés selon différentes catégories (par exemple, Type d'événement, Sévérité, Nom de la politique). Vous pouvez également trier et filtrer les listes d'événements, mais aussi effectuer une recherche. Pour une explication des fonctionnalités de personnalisation, voir Éléments de l'interface utilisateur de la console de gestion.



La partie inférieure de la page affiche des informations détaillées sur l'événement sélectionné, divisées en onglets. Seuls les onglets correspondant au type de l'événement sélectionné sont affichés. Pour plus d'informations sur les événements, voir Événements.

Un bouton **Actions** en haut du volet vous permet d'effectuer l'action suivante sur le ou les événements sélectionnés :

- **Résoudre** – Marque cet événement comme résolu.
- **Télécharger le fichier de capture** – Télécharge le fichier PCAP pour cet événement.
- **Exclure de la politique** – Crée une exclusion de politique pour cet événement.

Des informations détaillées sur ces actions sont fournies dans le chapitre Événements.

Les informations affichées pour chaque liste d'événements sont décrites dans le tableau suivant :

Paramètre	Description
Identifiant de journal	Identifiant généré par le système pour faire référence à l'événement.
Date/ Heure	La date et l'heure auxquelles l'événement s'est produit.
Type d'événement	Décrit le type d'activité qui a déclenché l'événement. Les événements sont générés par les politiques configurées dans le système. Pour une explication des différents types de politiques, voir Types de politiques.
Sévérité	Affiche le niveau de sévérité de l'événement. Voici une explication des valeurs possibles : • Aucun – Aucune raison de s'inquiéter. • Info – Aucune raison de s'inquiéter dans l'immédiat. À vérifier au moment opportun. • Avertissement – Risque modéré qu'une activité potentiellement dangereuse se soit produite. À traiter au moment opportun. • Critique – Risque élevé qu'une activité potentiellement dangereuse se soit produite. À traiter immédiatement.
Nom de la politique	Le nom de la politique qui a généré l'événement. Le nom est un lien vers la liste de politiques.
Asset source	Le nom de l'asset qui a lancé l'événement. Ce champ est un lien vers les listes d'assets.
Adresse source	L'adresse IP ou MAC de l'asset qui a lancé l'événement.
Adresse source	L'adresse IP ou MAC de l'asset qui a lancé l'événement.
Asset cible	Le nom de l'asset qui a été affecté par l'événement. Ce champ est un lien vers les listes d'assets.
Adresse cible	L'adresse IP ou MAC de l'asset qui a été affecté par l'événement.
Protocole	Lorsque c'est pertinent, montre le protocole utilisé pour la communication

	qui a généré cet événement.
Catégorie d'événement	Affiche la catégorie générale de l'événement. REMARQUE : l'écran Tous les événements affiche tous les types d'événements. Chaque écran d'événement affiche uniquement les événements de la catégorie spécifiée. Les catégories d'événements sont expliquées brièvement ci-dessous (pour une explication plus détaillée, voir Catégories et sous-catégories de politiques) : • Événements de configuration – Cela comprend deux sous-catégories • Événements de validation du contrôleur – Ces politiques concernent les changements ayant lieu au sein des contrôleurs du réseau. • Événements d'activité du contrôleur – Ces politiques concernent les activités qui se produisent sur le réseau (c'est-à-dire les « commandes » mises en œuvre entre les assets du réseau). • Événements SCADA – Ces politiques identifient les modifications apportées au plan de données des contrôleurs. • Événements de menaces réseau – Ces politiques identifient le trafic réseau qui indique des menaces d'intrusion. • Événements réseau – Ces politiques concernent les assets du réseau et les flux de communication entre les assets.
Statut	Indique si l'événement a été marqué comme résolu ou non.
Résolu par	Pour les événements résolus, indique quel utilisateur a marqué l'événement comme résolu.
Résolu le	Pour les événements résolus, indique quand l'événement a été marqué comme résolu.
Commentaire	Affiche tous les commentaires qui ont été ajoutés lorsque l'événement a été résolu.

Cartographie du réseau

L'onglet **Cartographie du réseau** affiche une représentation graphique des connexions réseau de l'asset. Cette vue affiche toutes les connexions établies par l'asset sélectionné au cours des 30 derniers jours.

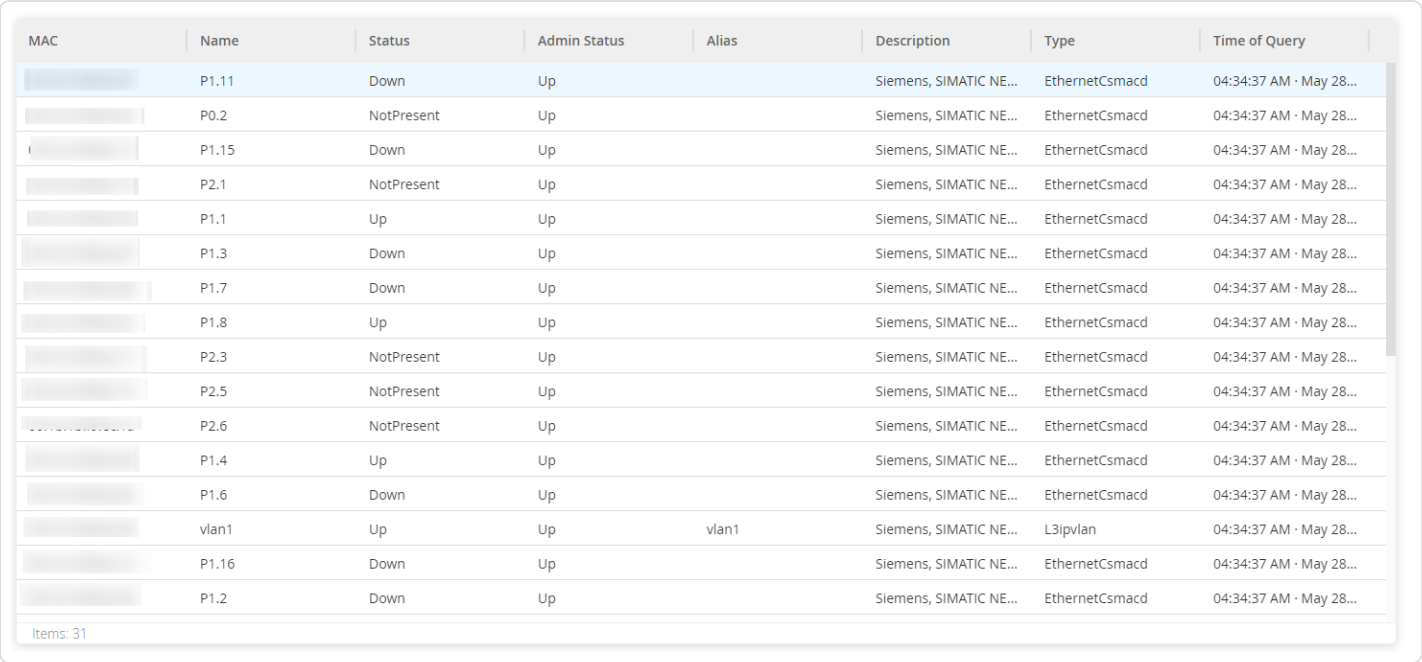
Les informations affichées dans cet onglet sont similaires aux informations affichées sur l'écran **Cartographie du réseau**, mais elles sont ici limitées aux connexions impliquant cet asset spécifique. Cet écran affiche aussi les connexions à des assets individuels et non à des groupes d'assets comme indiqué sur l'écran Cartographie du réseau principal. Pour une explication des informations affichées dans cet onglet, voir Cartographie du réseau.

Pour afficher la cartographie du réseau pour tous les assets, cliquez sur le bouton **Accéder à la cartographie du réseau**. Lorsque vous cliquez dessus, la cartographie du réseau effectue un zoom avant dynamique et se concentre sur cet asset pour afficher ses connexions à d'autres groupes d'assets.

Cliquer sur l'un des assets connectés sur la cartographie affiche les détails de cet asset, et cliquer sur le lien dans le nom de l'asset vous amène à l'écran Détails de l'asset sélectionné.

Ports du périphérique

L'onglet **Ports du périphérique** est disponible pour les commutateurs réseau et contient des détails sur leurs ports. OT Security collecte ces données en adressant des requêtes SNMP aux commutateurs. Les informations fournies pour chaque port sont l'adresse MAC, le nom, le statut de la connexion (actif ou inactif), l'alias et la description.



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

Remarque : activez cette fonctionnalité dans votre compte pour que l'onglet soit visible. Pour activer cette fonctionnalité, contactez l'Assistance Tenable.

Modifier les détails de l'asset

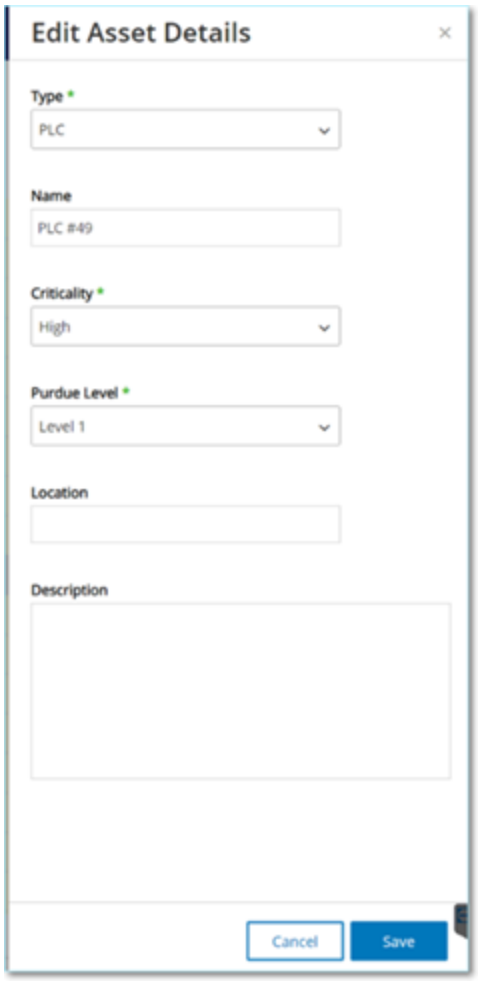
OT Security identifie automatiquement le type et le nom de l'asset en fonction de ses données internes et de son activité sur le réseau. Si le système n'a pas pu collecter ces informations ou si vous pensez que l'identification automatique n'est pas précise, vous pouvez modifier ces paramètres soit directement via l'interface utilisateur, soit en chargeant un fichier CSV. Vous pouvez également ajouter une description générale de l'asset et une description de l'emplacement de l'unité.

Modifier les détails d'un asset via l'interface utilisateur

Pour modifier les détails d'un asset unique :

1. Sous **Inventaire**, cliquez sur **Contrôleurs** ou **Assets réseau**.
2. Sélectionnez l'asset souhaité.
3. Cliquez sur le bouton **Actions** dans la barre d'en-tête.
4. Dans le menu déroulant, sélectionnez **Modifier**.

   La fenêtre **Modifier les détails de l'asset** apparaît.



5. Dans la zone **Type**, sélectionnez le type d'asset dans la liste déroulante.
6. Dans la zone **Nom**, saisissez un nom qui identifiera l'asset dans l'interface utilisateur de OT Security.
7. Dans la zone **Criticité**, saisissez le niveau de criticité de cet asset pour le système.
8. Dans la zone **Niveau Purdue**, saisissez le niveau Purdue en fonction du type d'asset.
9. Dans la zone **Fond de panier** (pour les contrôleurs), saisissez le nom du fond de panier sur lequel l'asset est installé.
10. Dans la zone **Localisation**, saisissez une description de l'emplacement de l'asset. Ce champ n'est pas obligatoire. Les données sont affichées dans le tableau des assets ainsi que sur l'écran des détails de l'asset.

11. Dans la zone **Description**, saisissez une description de l'asset. Ce champ n'est pas obligatoire. Les données sont affichées sur la page des détails de l'asset.
12. Cliquez sur **Enregistrer**.

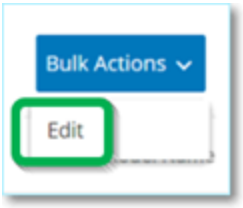
    OT Security enregistre les détails modifiés.

Pour modifier plusieurs assets (action en bloc) :

1. Sous **Inventaire**, cliquez sur **Contrôleurs** ou **Assets réseau**.
2. Cochez la case à côté de chacun des assets souhaités.

   > **Remarque :** vous pouvez également sélectionner plusieurs assets en appuyant sur la touche Maj et en cliquant sur chacun des assets souhaités.

3. Cliquez sur le menu **Actions en bloc** et sélectionnez **Modifier** dans la liste déroulante.

   L'écran **Modifier en bloc** apparaît avec les paramètres disponibles pour la modification en bloc.

4. Cochez la case à côté de chacun des paramètres que vous souhaitez modifier (Type, Criticité, Niveau Purdue, Segments réseau, Localisation et Description).

   > **Remarque :** lorsque vous modifiez des segments réseau en bloc, filtrez d'abord vos assets par **type**, puis sélectionnez les assets que vous souhaitez modifier en bloc. Les assets avec plusieurs adresses IP ne peuvent pas être inclus dans une modification en bloc pour les segments réseau ; vous devez modifier chaque asset manuellement.

5. Réglez chaque paramètre selon vos besoins.

   > **Remarque :** les informations saisies dans les champs de modification en bloc remplacent tout contenu actuel pour l'asset sélectionné. Si vous cochez la case d'un paramètre sans y saisir une sélection, les valeurs actuelles du paramètre sont effacées.

6. Cliquez sur **Enregistrer**.

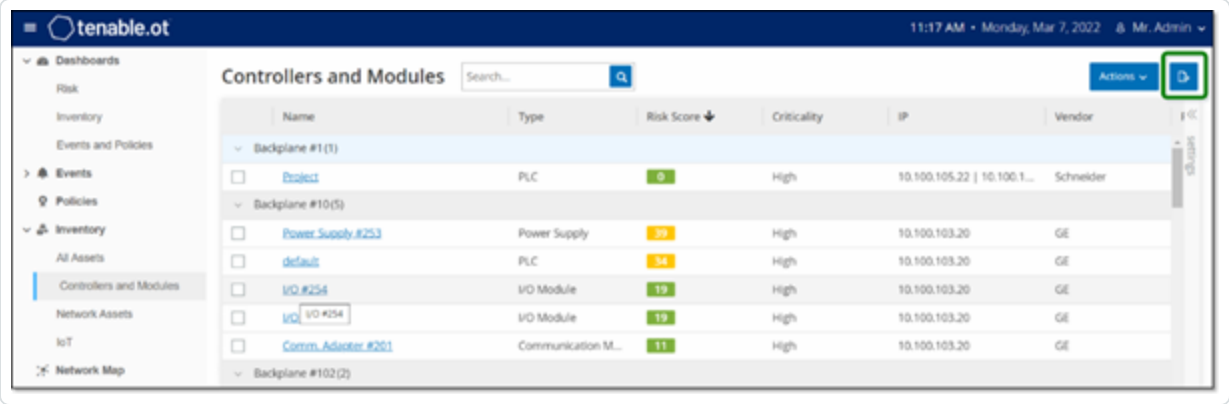
   OT Security enregistre les assets avec la nouvelle configuration.

Modifier les détails d'un asset en téléchargeant un fichier CSV

Cette méthode de modification des détails des assets vous permet d'en modifier un grand nombre grâce à un fichier CSV, plutôt que de les modifier manuellement dans l'interface utilisateur. Les détails suivants peuvent être modifiés à l'aide de cette méthode : Type, Nom, Criticité, Niveau Purdue, Localisation, Description et tous les champs personnalisés.

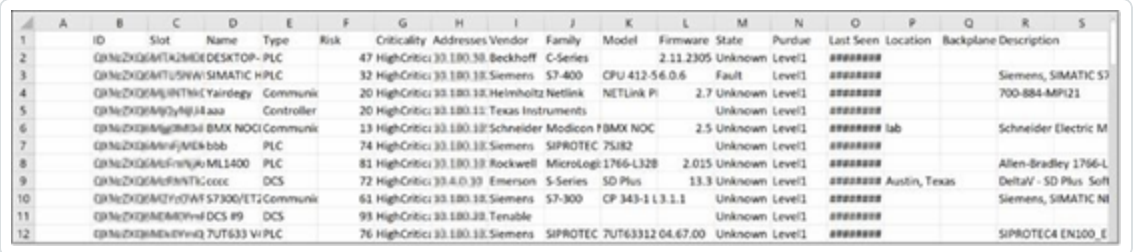
Pour modifier les détails d'un élément via un fichier CSV :

1. Sous **Inventaire**, cliquez sur **Tous les assets**, **Contrôleurs** et **Modules** ou **Assets réseau**.
2. Cliquez sur le bouton **Exporter**.



   Un fichier CSV de l'inventaire est téléchargé.

3. Accédez au fichier qui vient d'être téléchargé et ouvrez-le.



4. Modifiez les paramètres autorisés en modifiant le contenu des cellules. Les paramètres autorisés sont : Type, Nom, Criticité, Niveau Purdue, Localisation, Description et les champs personnalisés.

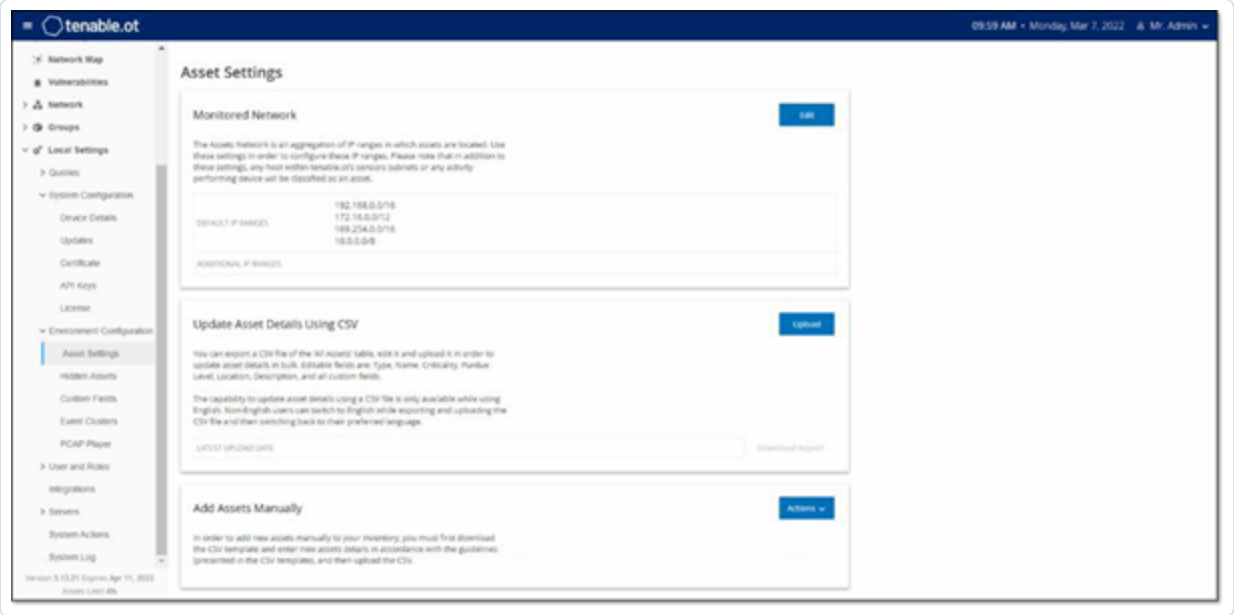
   Remarque : vous devez saisir des données valides pour les paramètres qui nécessitent des options spécifiques (par exemple, Type, Criticité, Niveau Purdue). Sinon, l'asset correspondant ne pourra pas être mis à jour.

5. Enregistrez le fichier au format CSV.

   Remarque : seuls les assets que vous modifiez sont mis à jour dans le système. Les assets qui ne sont pas inclus dans le fichier CSV ou les lignes que vous n'avez pas modifiées resteront inchangés dans le système. Il n'est pas possible de supprimer des assets à l'aide de cette méthode.

6. Sous **Paramètres locaux**, accédez à **Configuration de l'environnement** > **Paramètres de l'asset**.

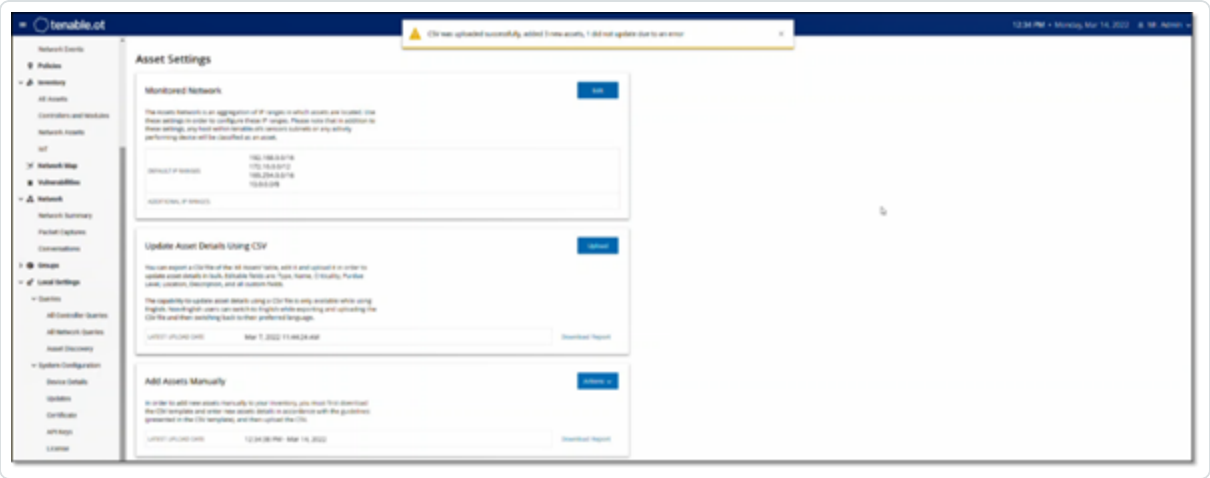
   La page **Paramètres de l'asset** apparaît.



7. Dans la section **Mettre à jour les détails d'un asset à l'aide d'un fichier CSV**, cliquez sur **Charger**.

8. Suivez les invites de navigation de votre appareil pour charger le fichier CSV que vous venez d'enregistrer.

   Un message de confirmation apparaît et précise le nombre de lignes mises à jour.



   Le champ **Date du dernier chargement** dans la section « Mettre à jour les détails d'un asset à l'aide d'un fichier CSV » est mis à jour.

9. Pour voir plus d'informations sur les résultats du chargement, dans la section **Mettre à jour les détails d'un asset à l'aide d'un fichier CSV**, cliquez sur **Télécharger le rapport**.

   OT Security télécharge un fichier CSV qui répertorie les identifiants d'assets mis à jour et ceux dont la mise à jour a échoué.

Masquer des assets

Vous pouvez masquer un ou plusieurs assets de l'inventaire. Un asset qui a été masqué n'est pas affiché dans l'inventaire et est supprimé des groupes. Cependant, les événements et l'activité sur le réseau sont toujours affichés pour l'asset masqué.

Vous pouvez restaurer un asset masqué à partir de la page **Paramètres locaux** > **Configuration de l'environnement** > **Assets masqués**.

Pour masquer un ou plusieurs assets :

1. Sous **Inventaire**, cliquez sur **Contrôleurs** ou **Assets réseau**.
2. Cochez la case à côté du ou des assets que vous souhaitez supprimer.

3. Cliquez sur **Actions** dans la barre d'en-tête.

   Un menu apparaît.

4. Sélectionnez **Masquer l'asset**.

   La page **Assets masqués** apparaît.

5. (Facultatif) Dans la zone **Commentaires**, ajoutez des commentaires sur les assets.

   > **Remarque** : les commentaires apparaissent dans la liste des assets supprimés sur la page **Paramètres locaux** > **Configuration de l'environnement** > **Assets masqués**.

6. Cliquez sur **Masquer**.

   OT Security masque les assets sur les pages **Inventaire** et **Groupes**.

Effectuer un scan Tenable Nessus spécifique à un asset

Tenable Nessus est un outil qui scanne les appareils informatiques pour détecter les vulnérabilités. OT Security vous permet d'exécuter le **Basic Network Scan** (Scan réseau de base) de Tenable Nessus sur des assets informatiques spécifiques au sein de votre réseau OT. Il s'agit d'un scan actif de l'ensemble du système qui rassemble des informations supplémentaires à propos des vulnérabilités sur les serveurs et les appareils réseau. Ce scan utilise les informations d'authentification WMI et SNMP, si elles sont disponibles. Cette action n'est disponible que pour les machines PC concernées. Vous pouvez accéder aux résultats du scan à partir de la page Vulnérabilités. Vous pouvez également créer des scans personnalisés pour exécuter un ensemble spécifique de plug-ins Tenable Nessus sur un ensemble particulier d'assets réseau. Voir Tenable NessusScans de plug-in Nessus.

Le scan Nessus dans OT Security utilise les mêmes paramètres de politique qu'un scan réseau de base dans Tenable Nessus, Tenable Security Center et Tenable Vulnerability Management. La seule différence réside dans les options de performance de OT Security. Voici les options de performance pour le scan Nessus dans OT Security. Ces options s'appliquent également au scan Nessus de base que vous lancez à partir de la page **Gestion des requêtes actives**.

- 5 hôtes simultanés (max.)
- 2 vérifications simultanées par hôte (max.)
- 15 secondes de délai d'expiration pour la lecture réseau

Remarque : Tenable Nessus est un outil invasif qui fonctionne mieux dans les environnements informatiques. Tenable ne recommande pas de l'utiliser sur les appareils OT, car cela peut interférer avec leur fonctionnement.

Pour lancer un scan Tenable Nessus sur des assets spécifiques :

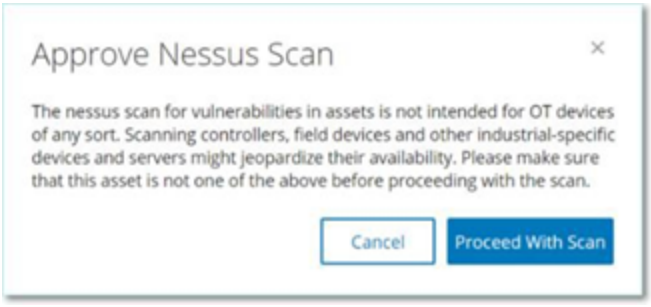
1. Accédez à **Inventaire** > **Assets réseau**.

   La page **Assets réseau** apparaît.

2. Cochez la case à côté du ou des assets que vous souhaitez scanner.

3. Dans le coin supérieur droit, cliquez sur **Actions** > **Scan Nessus**.

   La boîte de dialogue **Approuver le scan Nessus** apparaît.

4. Cliquez sur **Procéder au scan**.

   OT Security exécute le scan Nessus.

Exécuter une resynchronisation

La fonction Resynchroniser lance une ou plusieurs requêtes au réseau et au contrôleur, afin de capturer des informations à jour pour cet asset. Vous pouvez exécuter toutes les requêtes disponibles ou bien des requêtes spécifiques.

Voici les requêtes disponibles pour la fonction Resynchroniser :

- **Scan du fond de panier** —Découvre les modules et leurs spécifications au sein d'un fond de panier.
- **Scan DNS** —Recherche les noms DNS des assets du réseau.

- **Requête de détails** —Récupère les détails du matériel et du firmware du contrôleur. Le résultat apparaît dans le champ **Firmware** de la page **Assets** > **Contrôleurs et modules**.
- **Requête d'identification** —Utilise plusieurs protocoles pour identifier l'asset.
- **Requête NetBIOS** —Envoie un paquet Netbios Unicast qui est utilisé pour classer et détecter les machines Windows sur le réseau.
- **Requête SNMP (pour les assets compatibles SNMP)** —Récupère les détails de configuration des assets compatibles SNMP.
- **État** —Détecte l'état actuel de l'asset (**En cours d'exécution**, **Arrêté**, **En panne**, **Inconnu** et **Test**).
- **ARP** —Récupère l'adresse MAC des nouvelles adresses IP détectées sur le réseau. Le résultat apparaît dans la section **Détails** > **Vue d'ensemble**.

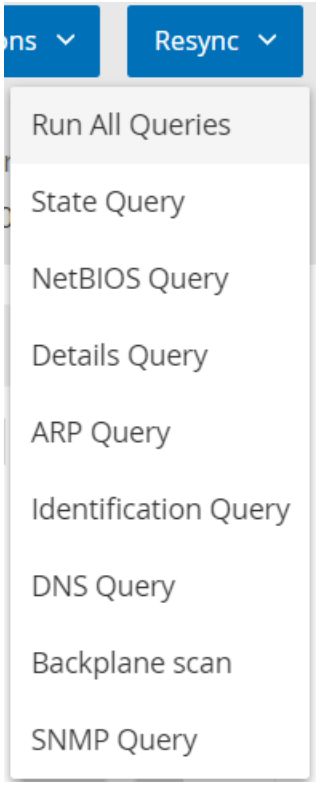
Le bouton **Resynchroniser** peut être désactivé dans des conditions spécifiques. Les raisons possibles incluent :

- L'appareil est inaccessible ou ne dispose pas de requêtes disponibles.
- L'autorisation configurée sur la page **Requêtes actives** peut empêcher des comptes non-administrateurs de lancer certaines requêtes.
- Les requêtes ne sont pas activées sur ce déploiement OT Security.
- Toutes les requêtes de la section **Requêtes actives** > **Manuelles** sont désactivées.
- L'asset n'a pas d'adresse IP connue pour les requêtes.

Pour resynchroniser les données d'un asset :

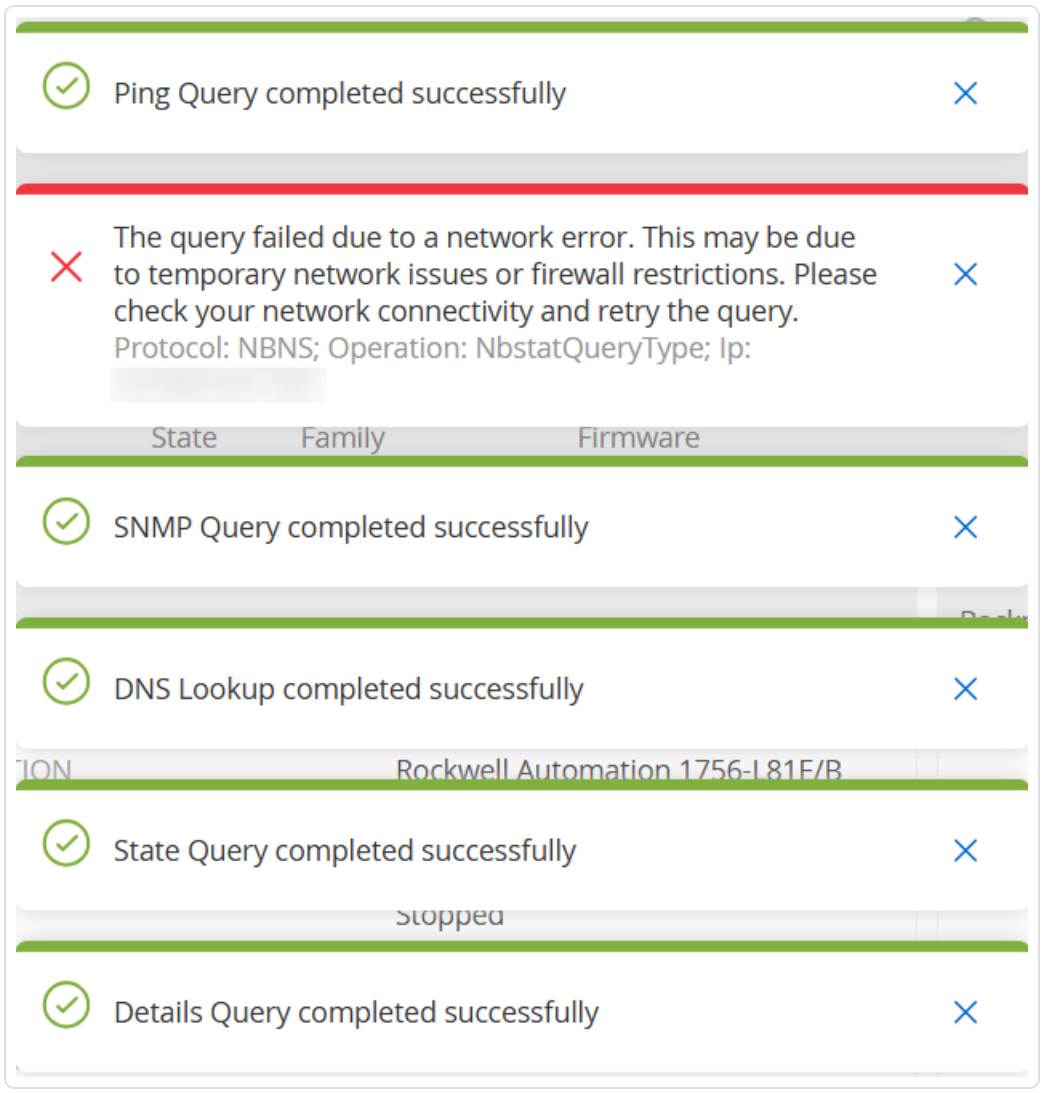
1. Sur la page **Détails de l'asset** de l'asset souhaité, en haut à droite, cliquez sur **Resynchroniser**.

   Une liste déroulante de requêtes apparaît.



2. Cliquez sur la requête que vous souhaitez exécuter ou cliquez sur **Exécuter toutes les requêtes** pour exécuter toutes les requêtes disponibles.

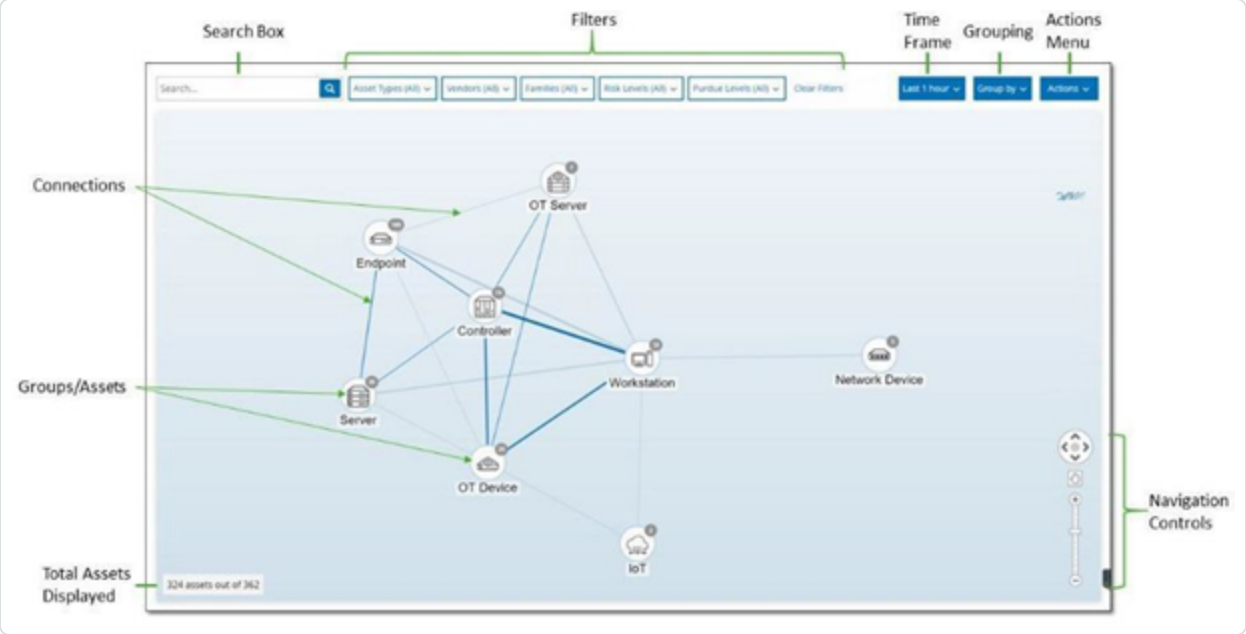
   Au fur et à mesure que chaque requête est exécutée, une notification apparaît avec son statut.



Pour chaque requête terminée, les données système de cet asset sont mises à jour par OT Security en fonction des nouvelles données.

Cartographie du réseau

L'écran **Cartographie du réseau** offre une représentation visuelle des assets du réseau et de leurs connexions au fil du temps, que les fonctionnalités de détection du réseau de OT Security ont détectés. La détection réseau offre une visibilité approfondie et en temps réel sur toutes les activités sur le réseau opérationnel, en se concentrant sur les activités d'ingénierie des plans de contrôle, telles que les chargements et téléchargements de firmware, les mises à jour de code et les modifications de configuration effectués sur les protocoles propriétaires et spécifiques aux fournisseurs. La cartographie du réseau affiche les assets par groupes d'assets associés ou comme assets individuels.



La **cartographie du réseau** affiche tous les assets et toutes les connexions que Tenable a découverts au cours de la période spécifiée.

La **cartographie du réseau** affiche les détails suivants :

- **Zone de recherche** – Saisissez du texte pour rechercher des assets dans l'affichage. La cartographie du réseau affiche les résultats de la recherche en mettant en évidence tous les groupes qui correspondent au texte de recherche. Vous pouvez explorer chaque groupe pour voir les assets pertinents.
- **Filtres** – Filtrez l'affichage de la carte selon une ou plusieurs des catégories pertinentes : **Type d'asset**, **Fournisseurs**, **Familles**, **Niveaux de risque**, **Niveaux Purdue**. Pour une explication des

différents types d'assets, voir Types d'assets.

- **Période** – La cartographie du réseau affiche les assets et les connexions réseau détectées pendant la plage temporelle spécifiée. La période par défaut est définie sur les **30 derniers jours**. Dans la zone déroulante de période, sélectionnez une autre période.
- **Regroupements** – Vous pouvez spécifier la catégorie de regroupement dans l'affichage. Les options sont : **Type d'asset**, **Niveau Purdue**, **Niveau de risque** ou **Pas de regroupement**. L'option **Réduire tous les groupes** conserve la sélection de regroupement actuelle, mais réduit tous les autres groupes ouverts.
- **Actions** – Vous pouvez sélectionner les actions suivantes dans le menu déroulant :
  - **Définir comme base de référence** – Définit la base de référence utilisée pour détecter une activité réseau anormale. Voir Définir une base de référence réseau.
  - **Organisation automatique** – Optimise automatiquement l'affichage de la cartographie pour les entités actuellement affichées.
- **Groupes/ Assets** – Chaque groupe d'assets est représenté par une icône sur la carte, et chaque type d'asset est symbolisé par une icône spécifique comme décrit dans Types d'assets. Pour les groupes, le nombre situé en haut de l'icône indique le nombre d'assets dans le groupe. Vous pouvez afficher successivement les icônes de chaque sous-groupe pour parvenir aux icônes d'assets individuels. La couleur du cadre autour d'un asset indique son niveau de risque (rouge, jaune, vert).

  > **Remarque :** vous pouvez faire glisser les groupes et les assets et les repositionner, pour obtenir une meilleure vue des assets et de leurs connexions.

- **Connexions** – Chaque communication entre des groupes d'assets et/ou des assets individuels, selon le degré de granularité actuellement affiché dans la carte. L'épaisseur de la ligne indique le volume de communication via cette connexion.
- **Total des assets affichés** – Affiche le nombre d'assets détectés sur le réseau (et affichés sur la carte) en fonction de la période et des filtres d'assets spécifiés. Ce nombre est affiché par rapport au nombre total d'assets détectés dans votre réseau.
- **Commandes de navigation** – Vous pouvez effectuer un zoom avant ou un zoom arrière sur l'affichage et naviguer pour afficher les éléments souhaités à l'aide des commandes à l'écran

ou des commandes de souris standard.

Regroupements d'assets

La page **Cartographie du réseau** peut afficher des assets regroupés selon de nombreuses catégories différentes. Elle indique les connexions entre les groupes d'assets. Vous pouvez cliquer sur un asset pour accéder aux éléments du groupe. Plusieurs groupes peuvent être détaillés simultanément. OT Security contient plusieurs couches de groupes intégrés, de sorte que chaque exploration successive délivre une vue plus détaillée des assets inclus.

Voici les regroupements qui peuvent être appliqués à l'affichage principal et les options de développement détaillé pour cette sélection.

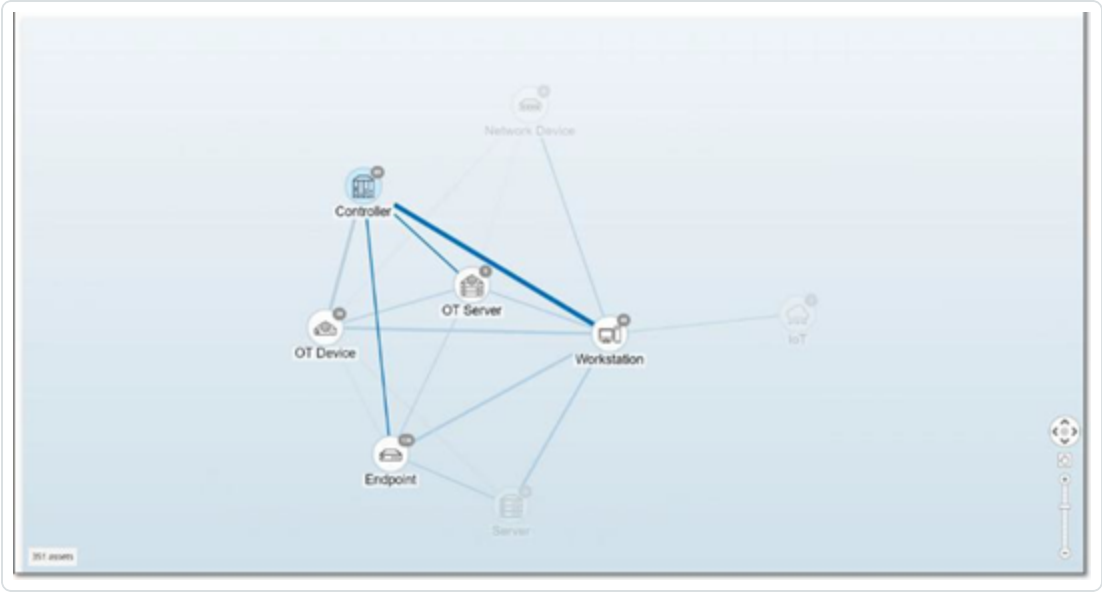
Lorsque la cartographie affiche les groupes par **type d'asset** (par défaut), la hiérarchie détaillée est la suivante : **Type d'asset** > **Fournisseur** > **Famille** > **Asset individuel**.

Lorsque la cartographie affiche les groupes par **niveau de risque** ou **niveau Purdue**, un niveau supplémentaire figure **au-dessus** du regroupement par type d'asset pour afficher la hiérarchie suivante : **Niveau Purdue/ Niveau de risque** > **Type d'asset** > **Fournisseur** > **Famille** > **Asset individuel**. Chaque niveau est représenté par un cercle entourant les groupes/ assets inclus.

L'exemple suivant montre comment vous pouvez détailler l'affichage :

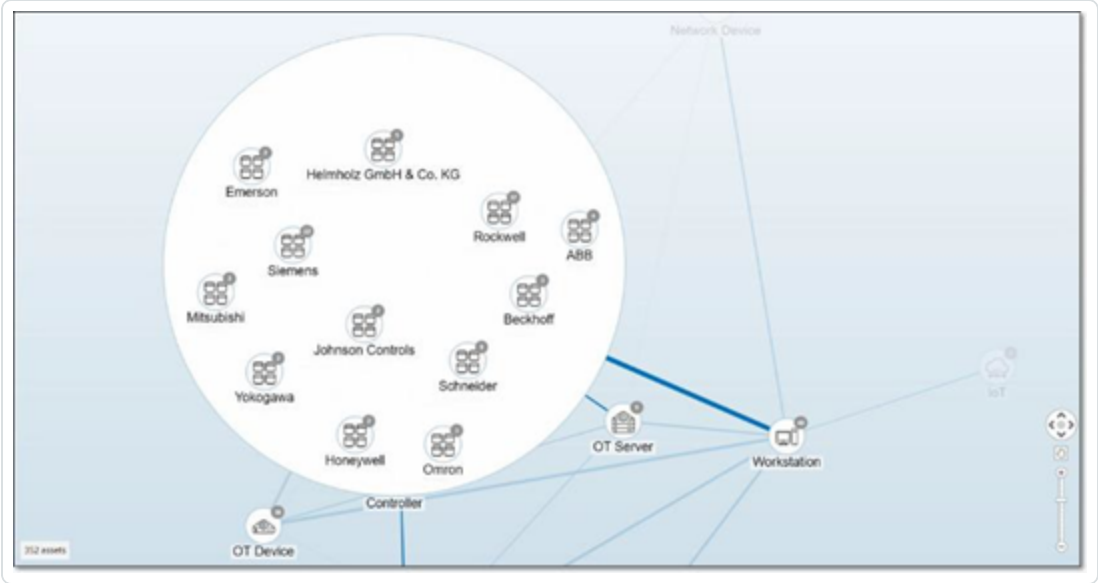
Pour détailler un groupe de types d'assets :

1. Par défaut, lorsque vous ouvrez l'écran **Cartographie du réseau**, il regroupe les assets par type.

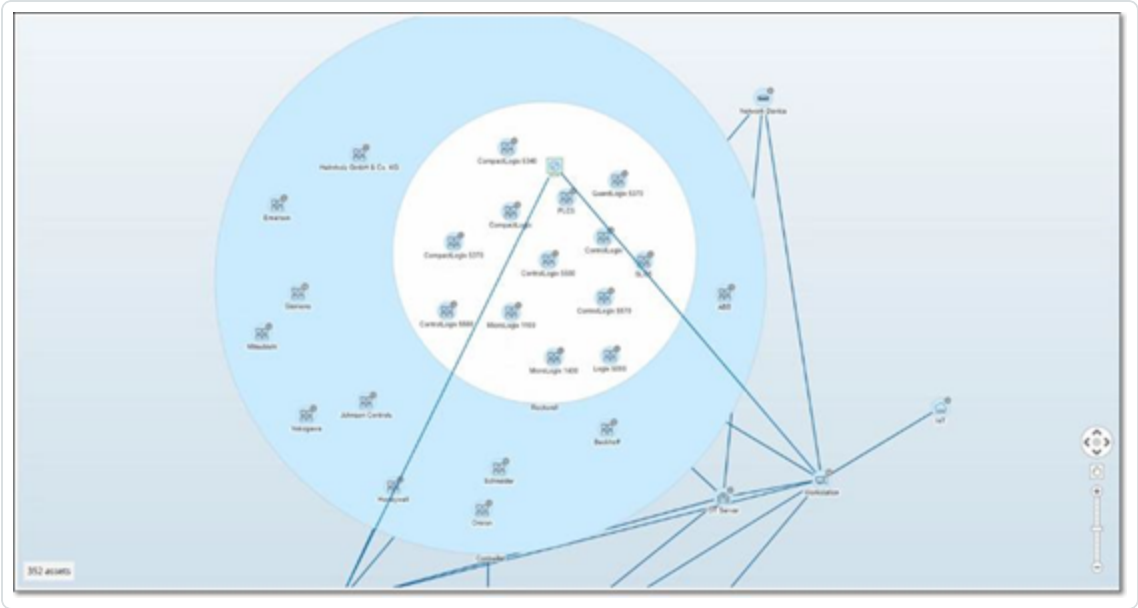


2. Double-cliquez sur l'icône du groupe que vous souhaitez détailler (par exemple Contrôleur).

   Le groupe est développé, affichant les groupes de fournisseurs qu'il contient.

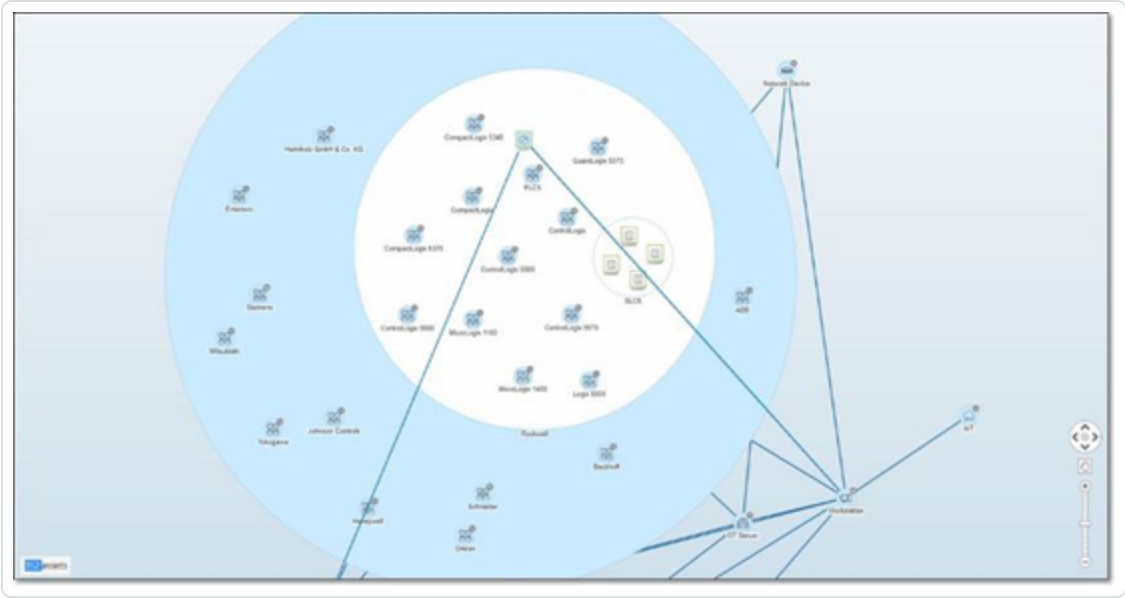


3. Pour aller plus loin, cliquez sur un groupe de fournisseurs (par exemple Rockwell).



4. Pour aller encore plus loin, cliquez sur un groupe de famille (par exemple SLC5).

   Les assets individuels du groupe apparaissent.



5. Maintenant, vous pouvez cliquer sur un asset pour afficher ses détails et ses connexions. Voir Inventaire.

Pour réduire l'affichage :

1. Cliquez sur **Grouper par**.
2. Cliquez sur **Réduire tous les groupes**.

   L'affichage retourne alors aux groupes de niveau supérieur.

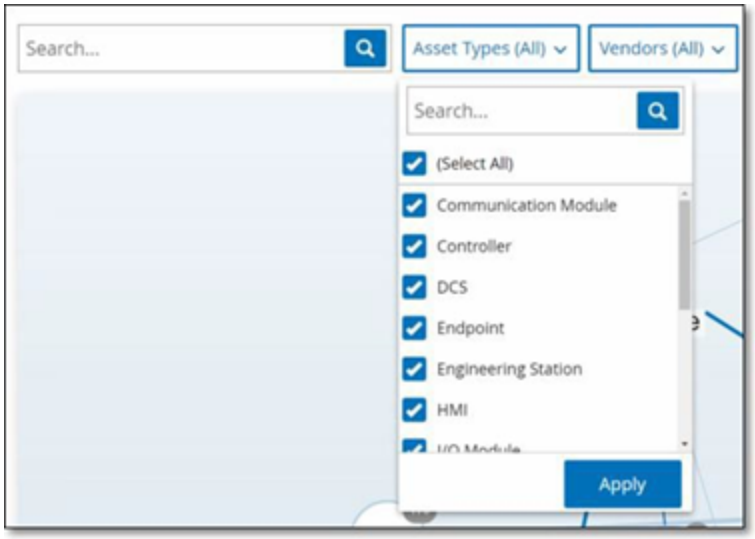
Pour supprimer tous les regroupements :

1. Cliquez sur le bouton **Grouper par**.
2. Sélectionnez **Pas de regroupement**.

   La carte affiche tous les assets uniques sans les regrouper.

Application de filtres à l'affichage de la cartographie

Vous pouvez filtrer l'affichage de la cartographie selon une ou plusieurs des catégories spécifiées : Type d'asset, Fournisseurs, Familles, Niveaux de risque, Niveaux Purdue.



Pour appliquer des filtres à la carte :

1. Cliquez sur la catégorie de filtre souhaitée.
2. Cochez ou décochez les cases de chaque élément que vous souhaitez inclure ou exclure de l'affichage.

   Remarque : par défaut, tous les éléments sont inclus dans le filtre.

3. Vous pouvez décocher la case **Tout sélectionner** pour désélectionner toutes les valeurs, puis ajouter les valeurs souhaitées.
4. Vous pouvez effectuer une recherche de filtre dans la zone dédiée pour trouver une valeur spécifique.
5. Répétez le processus pour chaque catégorie de filtre, si nécessaire.
6. Cliquez sur **Appliquer**.

   La carte affiche uniquement les éléments sélectionnés.

Affichage des détails d'un asset

Vous pouvez cliquer sur un asset de base pour afficher ses informations de base et ses activités sur le réseau, notamment le niveau de risque, l'adresse IP, le type d'asset, le fournisseur et la famille. La carte affiche les connexions de l'asset sélectionné vers tous les autres assets qui communiquent avec lui. Vous pouvez ensuite cliquer sur le lien du nom de l'asset pour accéder à l'écran des **détails de l'asset** qui contient plus de détails sur l'asset.

Définir une base de référence réseau

Une base de référence réseau est une cartographie de toutes les communications qui ont eu lieu entre les assets du réseau pendant une période spécifiée. La base de référence réseau est utilisée

par les politiques de déviation de la base de référence réseau, qui alertent en cas de communications anormales sur le réseau. Voir Types d'événements réseau.

Les assets qui n'ont pas communiqué pendant l'échantillonnage de la référence de base déclenchent une alerte pour chaque communication (en supposant qu'elle se situe dans le cadre des conditions de politique spécifiées). Pour pouvoir créer des politiques de déviation de la base de référence réseau, vous devez créer une base de référence réseau dans l'écran **Cartographie du réseau**. Vous pouvez mettre à jour la référence de base réseau à tout moment en définissant une nouvelle référence de base réseau.

Pour définir une base de référence réseau :

1. Dans l'écran **Cartographie du réseau**, sélectionnez la plage temporelle des communications à inclure dans la base de référence réseau en utilisant la **sélection de période** en haut de l'écran.

   La **cartographie du réseau** apparaît pour la période sélectionnée.

2. Dans le coin supérieur droit, sélectionnez **Actions** > **Définir comme base de référence**.

   OT Security configure la nouvelle base de référence réseau dans le système et l'applique à toutes les politiques de déviation de la base de référence réseau.

Vulnérabilités

OT Security identifie les différents types de menaces qui affectent les assets dans votre réseau. Au fur et à mesure que des informations sur de nouvelles vulnérabilités sont découvertes et diffusées dans le domaine public, le personnel de recherche de Tenable conçoit des programmes pour permettre à Tenable Nessus de les détecter.

Ces programmes sont nommés Plug-ins et sont écrits dans le langage de script propriétaire de Tenable Nessus, appelé Tenable Nessus Attack Scripting Language (NASL). Les plug-ins détectent les CVE ainsi que les autres menaces pesant sur les assets de votre réseau (par exemple, systèmes d'exploitation obsolètes, utilisation de protocoles vulnérables, ports ouverts vulnérables, etc.).

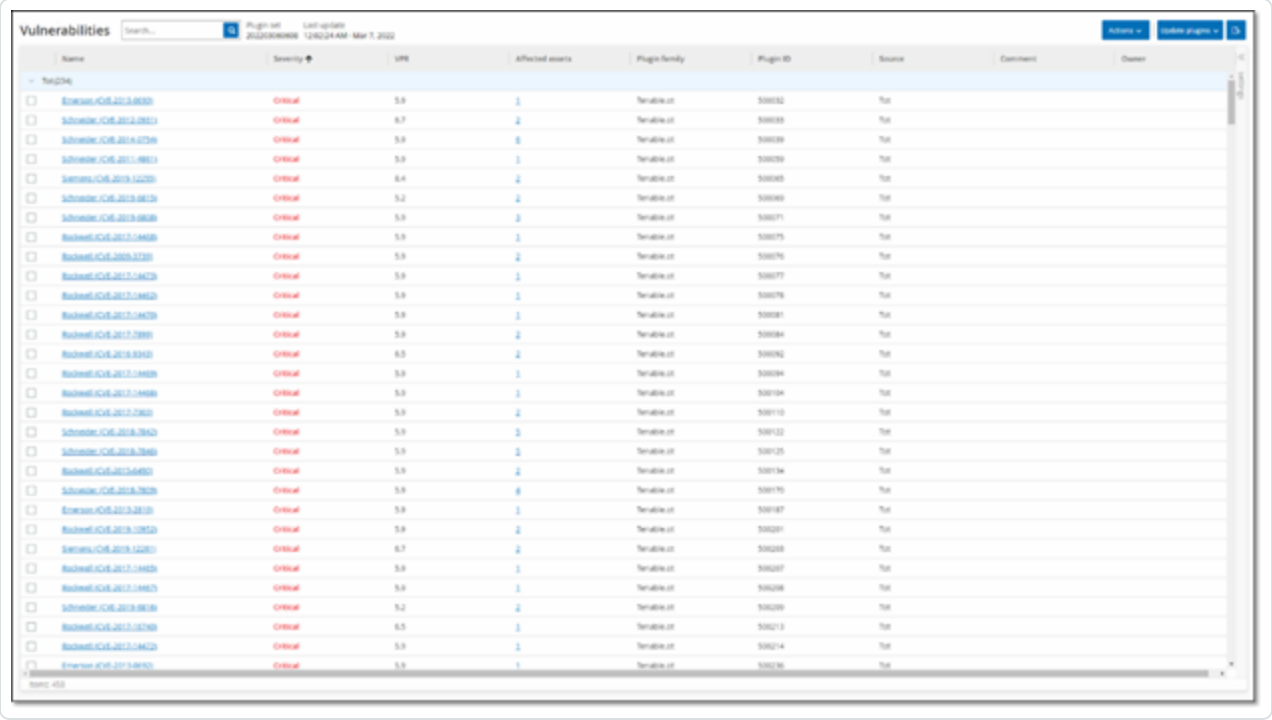
Les plug-ins contiennent des informations sur la vulnérabilité, un ensemble générique d'actions de remédiation et l'algorithme pour tester la présence du problème de sécurité.

Pour plus d'informations sur la mise à jour de votre ensemble de plug-ins, voir Configuration de l'environnement.

Vulnérabilités

La page **Vulnérabilités** affiche une liste de toutes les vulnérabilités détectées par les plug-ins Tenable qui affectent votre réseau et vos assets.

Vous pouvez personnaliser les paramètres d'affichage en ajustant les colonnes affichées et l'emplacement de chaque colonne. Pour une explication des fonctionnalités de personnalisation, voir Éléments de l'interface utilisateur de la console de gestion.



La page **Vulnérabilités** affiche les détails suivants :

Paramètre	Description
Nom	Nom de la vulnérabilité. Le nom est un lien qui permet d'afficher la liste complète des vulnérabilités.
Sévérité	Ce score indique la sévérité de la menace détectée par ce plug-in. Les valeurs possibles sont : Info, Faible, Moyenne, Élevée ou Critique.

VPR	Le classement VPR (Vulnerability Priority Rating) est un indicateur dynamique du niveau de sévérité, qui est constamment mis à jour en fonction de l'exploitabilité actuelle de la vulnérabilité. Tenable génère cette valeur en tant que sortie du service Predictive Prioritization de Tenable qui évalue l'impact technique et la menace posée par la vulnérabilité. Les valeurs VPR vont de 0,1 à 10,0, une valeur plus élevée représentant une plus grande probabilité d'exploitation.
ID de plug-in	L'identifiant unique du plug-in.
Assets affectés	Nombre d'assets de votre réseau qui sont affectés par cette vulnérabilité.
Famille de plug-ins	La famille (groupe) à laquelle ce plug-in est associé.
Commentaire	Vous pouvez ajouter librement des commentaires sur ce plug-in.

Détails du plug-in

Pour afficher les détails d'un plug-in :

1. Sur la ligne de la vulnérabilité dont vous souhaitez afficher les détails, cliquez sur le nom de la vulnérabilité.

   La fenêtre des détails de la vulnérabilité apparaît.

Cette fenêtre contient les détails suivants :

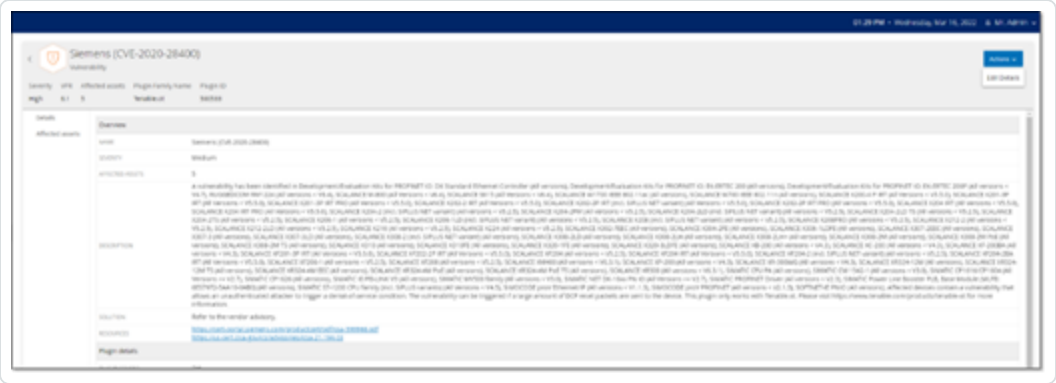
- **Barre d'en-tête** – Affiche des informations de base sur la vulnérabilité spécifiée. Dans le menu **Actions**, sélectionnez **Modifier les détails** pour modifier les détails de la vulnérabilité. Voir Modifier les détails d'une vulnérabilité.
- **Onglet Détails** – Affiche la description complète de la vulnérabilité et fournit des liens vers les ressources pertinentes.
- **Onglet Assets affectés** – Affiche la liste de tous les assets affectés par la vulnérabilité spécifiée. Chaque liste contient des informations détaillées sur l'asset, ainsi qu'un lien pour afficher la fenêtre des détails de l'asset.

Modifier les détails d'une vulnérabilité

Pour modifier les détails d'une vulnérabilité :

1. Sur la page des **détails de la vulnérabilité** pertinente, cliquez sur le bouton **Actions** dans le coin supérieur droit.

   Le menu **Actions** apparaît.

2. Cliquez sur **Modifier les détails**.

   Le panneau **Modifier les détails de la vulnérabilité** apparaît.

3. Dans la zone **Commentaires**, saisissez des commentaires sur la vulnérabilité.
4. Dans la zone **Propriétaire**, saisissez le nom de la personne désignée pour traiter la vulnérabilité.
5. Cliquez sur **Enregistrer**.

Afficher la sortie d'un plug-in

La sortie du plug-in d'un asset apporte du contexte ou explique la raison pour laquelle un plug-in donné est signalé pour un asset.

Pour afficher les détails d'une sortie de plug-in à partir de la page Vulnérabilités :

1. Accédez à **Vulnérabilités**.

   La page **Vulnérabilités** apparaît.
2. Dans la liste des vulnérabilités, sélectionnez celles dont vous souhaitez afficher les détails et effectuez l'une des opérations suivantes :

- Cliquez sur le lien de la vulnérabilité.
- Effectuez un clic droit sur la vulnérabilité et sélectionnez **Afficher**.
- Dans la zone déroulante **Actions**, sélectionnez **Afficher**.

La page des détails de la vulnérabilité apparaît avec le panneau **Sortie du plug-in** et affiche les informations suivantes :

- Date de la correspondance
- Source
- Port
- Sortie du plug-in

> **Remarque :** les plug-ins n'offrent pas tous une sortie de plug-in.

Pour afficher les détails d'une sortie de plug-in à partir de la page Inventaires :

1. Accédez à **Inventaires** > **Tous les assets**.

   La page **Inventaires** apparaît.

2. Dans la liste des assets, sélectionnez celui dont vous voulez afficher les détails et exécutez l'une des opérations suivantes :
   - Cliquez sur le lien de l'asset.
   - Effectuez un clic droit sur l'asset et sélectionnez **Afficher**.
   - Cochez la case à côté de l'asset, puis sélectionnez **Afficher** dans la liste déroulante **Actions**.

   La page des détails de l'asset apparaît.

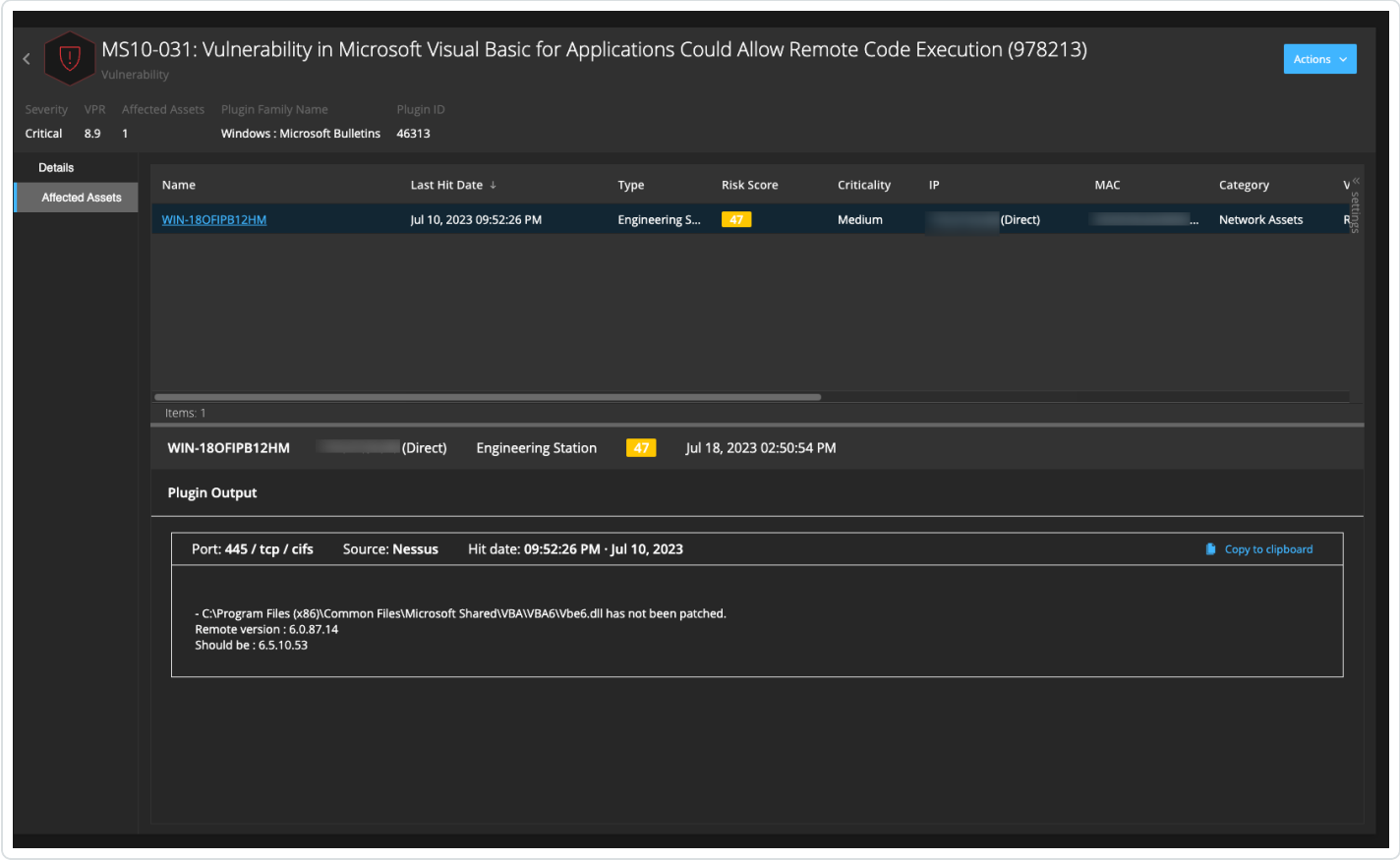
3. Cliquez sur l'onglet **Vulnérabilités**.

   La liste des vulnérabilités apparaît et affiche le panneau **Sortie du plug-in** avec les informations suivantes :

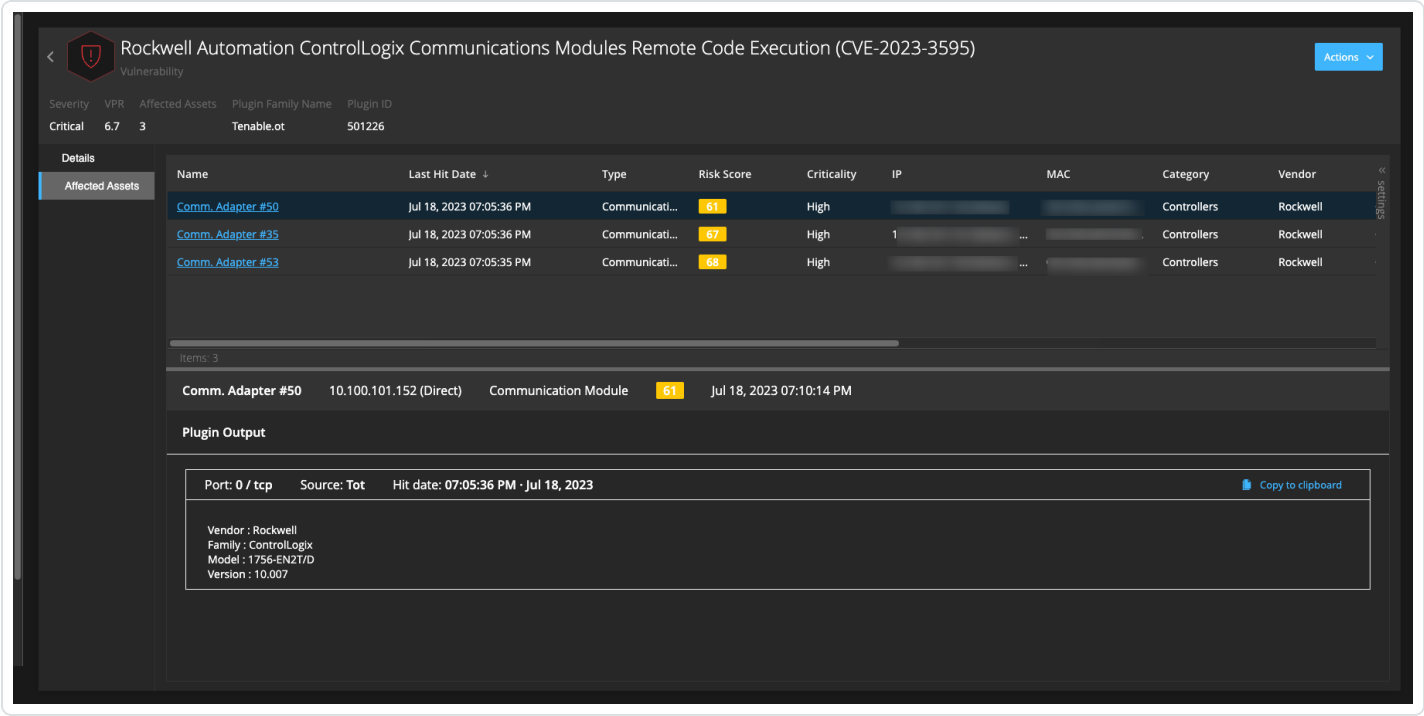
- Date de la correspondance
- Source
- Port
- Sortie du plug-in

> **Remarque :** les plug-ins n'offrent pas tous une sortie de plug-in.

Exemple de sortie d'un plug-in Tenable Nessus



Exemple de sortie d'un plug-in OT Security

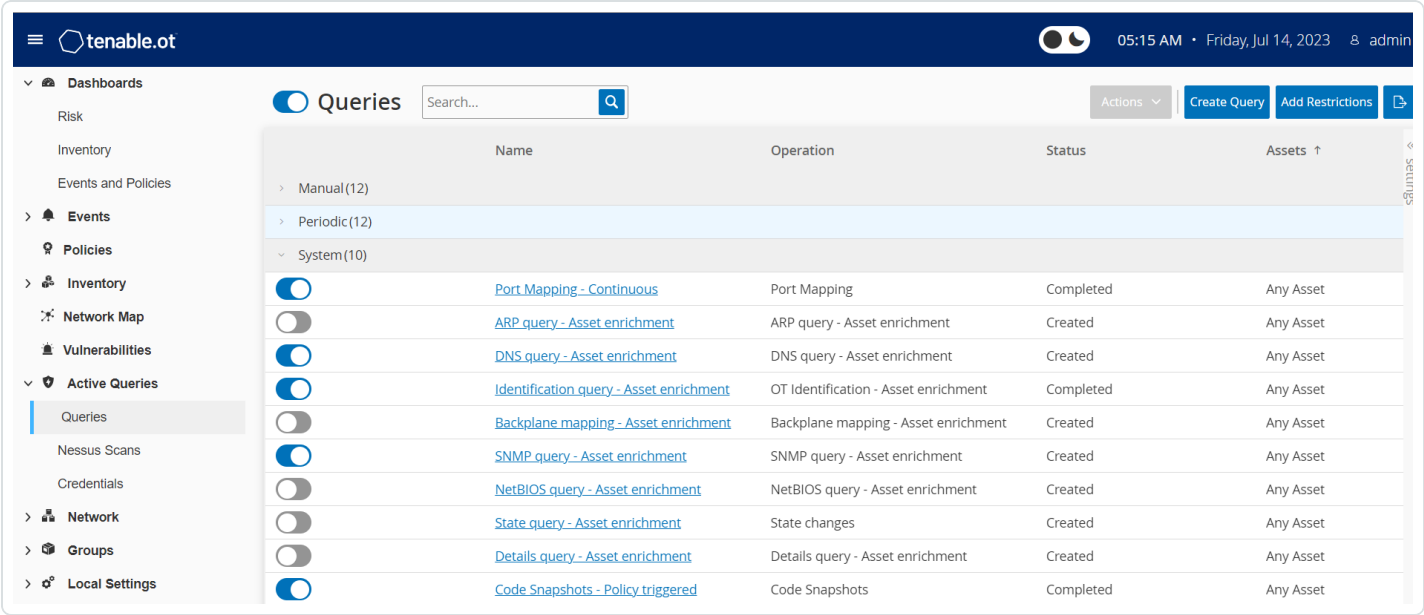


Requêtes actives

La fenêtre **Requêtes** de OT Security vous permet de configurer et d'activer les fonctionnalités de requêtes. Pour une explication générale de la technologie liée aux requêtes, voir Technologies OT Security. Dans le cadre de la configuration initiale, Tenable recommande d'activer toutes les fonctionnalités de requête. À tout moment, vous pouvez activer/désactiver n'importe laquelle des fonctions de requête. Vous pouvez également ajuster les paramètres pour définir quand et comment les requêtes sont exécutées.

En plus des requêtes automatiques qui sont exécutées périodiquement, vous pouvez lancer des requêtes à la demande en cliquant sur le curseur à côté de la requête.

Remarque : la désactivation des requêtes peut empêcher d'identifier certains assets. OT Security assure le suivi des appareils par le biais d'une surveillance passive et de requêtes actives.



Vous pouvez activer et configurer des requêtes à partir de la page **Requêtes actives** > **Requêtes**. Trois options sont disponibles pour contrôler les requêtes actives de manière granulaire : **Manuelles**, **Périodiques** et **Système**.

Manuelles – Cette option contrôle les requêtes que vous pouvez exécuter lors de l'examen d'un seul asset en utilisant l'option **Resynchroniser** pour cet asset. Les requêtes manuelles vous permettent de contrôler la fonctionnalité du produit pour des types de requêtes spécifiques lors de l'examen d'un seul asset surveillé. L'activation des options de resynchronisation vous permet d'exécuter ces requêtes lors de l'examen d'un asset. Pour plus d'informations sur l'option **Resynchroniser**, voir Exécuter une resynchronisation.

Périodiques – Il s'agit des requêtes qui s'exécutent selon une fréquence que vous définissez. Une fois activée, la requête s'exécute selon la planification que vous spécifiez dans la colonne **Répéter** de cette page. Vous pouvez exécuter toutes les requêtes périodiques sur demande en cliquant dessus avec le bouton droit et en sélectionnant **Exécuter maintenant**. Cela n'affecte pas la planification ou l'heure définie de la prochaine requête. Toutes les requêtes que vous créez manuellement peuvent être définies comme des requêtes périodiques.

Système – Il s'agit des requêtes que OT Security traite automatiquement en fonction de certains critères ou conditions. Par exemple, les requêtes basées sur l'enrichissement des assets sont exécutées chaque fois que Tenable observe pour la première fois un appareil de manière passive ou active. Grâce à l'enrichissement des assets, OT Security prend les empreintes digitales de l'appareil et l'identifie dès qu'il apparaît sur le réseau. L'enrichissement des assets contrôle également les

Instantanés déclenchés par la politique sous le contrôle de la configuration des politiques des événements basés sur des contrôleurs.

> **Remarque :** si vous utilisez l'enrichissement des assets, veillez à activer ces requêtes :
>
> - Mappage de ports —Continu
> - Requête d'identification —Enrichissement d'asset

Le tableau Requêtes affiche les informations suivantes :

Colonne	Description
Curseur d'activation ou de désactivation	Cliquez sur le curseur à côté du nom de la requête pour activer ou désactiver la requête.
Nom	Nom de la requête.
Opération	Type de requête : requête de découverte, périodique ou système.
Statut	État de la requête : **Créée**, **En cours**, **En préparation**, **Terminée** et **Échec**.
Assets	Groupes d'assets que cette requête doit interroger. **Remarque :** vous pouvez créer vos propres groupes d'assets pour les utiliser dans les requêtes que vous configurez.

Créer une requête

Vous pouvez créer des requêtes pour différents projets et fonctions, afin de contrôler quelle requête s'exécute et quand.

Par exemple, vous pouvez configurer des requêtes personnalisées pour les scénarios suivants :

- Différentes intervalles de maintenance pour différents secteurs de l'usine
- Différents projets et criticité variable pour différents assets
- Différentes requêtes pour les fonctions OT et les fonctions IT.

Pour créer une requête :

1. Accédez à **Requêtes actives** > **Requêtes**.

   La fenêtre **Requêtes** apparaît.

2. Cliquez sur **Créer une requête**.

   Le panneau **Créer une requête** apparaît.

3. Sélectionnez le type de requête requis parmi l'une des options suivantes :

   - **Découverte** il s'agit des requêtes qui détectent les assets en direct sur le réseau que OT Security surveille.
     - La **découverte** des assets utilise le protocole ICMP (Internet Control Message Protocol) ou ping pour détecter les adresses IP actives et qui répondent.
     - Le **suivi des assets actifs** tente régulièrement d'interroger un asset connu et surveillé pour déterminer s'il est toujours opérationnel et disponible.
     - La **découverte des contrôleurs** envoie un ensemble de paquets multicast au réseau pour que les contrôleurs ou les appareils ICS répondent directement à OT Security en donnant leurs informations.
   - **IT** —Il s'agit des requêtes qui récupèrent des points de données supplémentaires à partir d'assets de type IT surveillés que OT Security a observés. À l'exception de NetBIOS, ces requêtes de type IT nécessitent des informations d'authentification.
     - La **requête NetBIOS** tente de découvrir tous les appareils qui écoutent NetBIOS dans la plage de diffusion de Capteur OT Security ou de OT Security lui-même. Ce type de requête permet d'identifier les appareils Windows à proximité.
     - La **requête SNMP** utilise les informations d'authentification SNMP v2 ou SNMP v3 qui sollicitent l'infrastructure réseau ou les appareils en réseau qui prennent en charge le protocole SNMP, pour obtenir leurs détails d'identification. OT Security demande la description du système SNMP et d'autres paramètres pour ajouter un contexte à l'asset et créer son empreinte digitale.
     - La **requête de détails WMI** récupère divers points de données importants à partir des systèmes Windows. Le système interrogé doit disposer d'un compte Windows

(local ou domaine) avec les autorisations suffisantes pour interroger le service WMI (Windows Management Instrumentation).

- Les requêtes d'**état USB WMI** déterminent si des supports amovibles tels que des clés USB ou des disques durs portables sont connectés à l'appareil Windows, comme une station de travail ingénieur ou un serveur d'ingénierie. Cette requête est étroitement liée à la politique de **changement de la configuration USB sur les machines Windows**, car il s'agit d'une condition préalable au bon fonctionnement de cette politique.

- **OT** —Ces requêtes interrogent les contrôleurs et les appareils intégrés en toute sécurité pour obtenir plus d'informations en utilisant leurs protocoles propriétaires. OT Security exécute des requêtes en lecture seule pour collecter des informations sur les appareils. Dans certains cas, OT Security ne demande pas seulement les détails d'identification des appareils, et peut afficher des informations, telles que l'état de fonctionnement du PLC ou d'autres modules connectés au fond de panier. OT Security tente d'interroger les appareils qui écoutent les protocoles propriétaires que OT Security prend en charge.

4. Cliquez sur **Suivant**.

   Le panneau **Définition de la requête** apparaît.

5. Dans la zone **Nom**, saisissez le nom de la requête.

6. Dans la zone **Description**, saisissez la description de la requête.

7. Dans la zone déroulante **Assets**, sélectionnez les assets.

   > **Remarque :** vous pouvez également utiliser la zone de **recherche** pour rechercher un asset.

8. Dans la section **Répéter chaque**, saisissez un nombre et sélectionnez **Jours** ou **Semaines** dans la zone déroulante. Pour certaines requêtes, vous pouvez également définir des **minutes** et des **heures**.

   Si vous sélectionnez **Semaines**, indiquez les jours de la semaine d'exécution des requêtes.

9. Dans la zone **À**, définissez l'heure d'exécution des requêtes (au format heure, minutes, secondes) en cliquant sur l'icône d'horloge et en sélectionnant l'heure, ou en saisissant l'heure manuellement.

10. Cliquez sur le curseur **Requête d'état** pour activer la requête.
11. (Uniquement pour la découverte des assets) Dans la zone **Plages d'adresses IP**, saisissez les adresses IP des assets.
12. (Uniquement pour les requêtes de découverte) Dans la zone déroulante **Nombre d'assets à interroger simultanément**, sélectionnez le nombre d'assets. Les options disponibles sont : 10 assets, 20 assets ou 30 assets.
13. (Uniquement pour les requêtes de découverte) Dans la zone déroulante **Temps entre les requêtes de découverte**, sélectionnez l'intervalle entre les requêtes de découverte. Les options disponibles sont : 1seconde, 2 secondes ou 3 secondes.

Ajouter des restrictions

Vous pouvez empêcher les requêtes de s'exécuter sur certains assets, tels que des plages d'adresses IP, des serveurs OT, des tablettes, des dispositifs médicaux, des contrôleurs de domaine, etc.

Pour ajouter des restrictions :

1. Accédez à **Requêtes actives** > **Requêtes**.

   La fenêtre **Requêtes** apparaît.
2. Dans la zone déroulante **Assets bloqués**, sélectionnez les assets à bloquer.

   Remarque : vous pouvez utiliser la zone de recherche pour rechercher des assets.
3. Dans la zone déroulante **Clients restreints**, sélectionnez les clients requis.
4. Dans la zone déroulante **Période d'indisponibilité**, sélectionnez la durée de blocage des assets. Les options disponibles sont : **None** (Aucune), **Working Hours** (Heures ouvrées).
5. Cliquez sur **Enregistrer**.

   OT Security applique les restrictions aux clients et aux assets.

Afficher une requête

Pour afficher les détails d'une requête :

1. Accédez à **Requêtes actives** > **Requêtes**.

   La fenêtre **Requêtes** apparaît.

2. Sur la ligne de la requête à afficher, effectuez l'une des opérations suivantes :

   - Effectuez un clic droit sur la requête et sélectionnez **Afficher**.
   - Sélectionnez la requête puis, dans le menu **Actions**, sélectionnez **Afficher**.

   Une fenêtre apparaît avec les détails de la requête.

Modifier une requête

Pour modifier les détails d'une requête :

1. Accédez à **Requêtes actives** > **Requêtes**.

   La fenêtre **Requêtes** apparaît.

2. Dans la liste des requêtes, sélectionnez celle que vous souhaitez modifier et effectuez l'une des opérations suivantes :

   - Effectuez un clic droit sur la requête et sélectionnez **Modifier**.
   - Sélectionnez la requête, puis dans le menu **Actions**, sélectionnez **Modifier**.

   Le panneau **Modifier la requête** apparaît.

   > **Remarque :** vous pouvez également modifier une requête à partir de la page **Détails de la requête**.

3. Modifiez la requête selon les besoins.
4. Cliquez sur **Enregistrer**.

Dupliquer une requête

> **Remarque :** vous ne pouvez dupliquer que les requêtes **périodiques**.

1. Accédez à **Requêtes actives** > **Requêtes**.

   La fenêtre **Requêtes** apparaît.

2. Dans la liste des requêtes, sélectionnez celle que vous souhaitez dupliquer et procédez de l'une des manières suivantes :

   - Effectuez un clic droit sur la requête et sélectionnez **Dupliquer**.
   - Sélectionnez la requête, puis dans le menu **Actions**, sélectionnez **Dupliquer**.

   Le panneau **Dupliquer la requête** apparaît avec les détails de la requête.

   > **Remarque :** vous pouvez également dupliquer une requête à partir de la page des détails de la requête.

3. Renommez la requête et modifiez les détails selon les besoins.

4. Cliquez sur **Enregistrer**.

   OT Security enregistre la requête dans le tableau Requêtes.

Exécuter une requête

Vous pouvez exécuter des requêtes périodiques, si nécessaire.

> **Remarque :** l'option **Exécuter maintenant** n'est disponible que pour les requêtes **périodiques**.

Pour exécuter une requête :

1. Accédez à **Requêtes actives** > **Requêtes**.

   La fenêtre **Requêtes** apparaît.

2. Dans la liste des requêtes, sélectionnez celle que vous souhaitez exécuter et exécutez l'une des actions suivantes :

   - Effectuez un clic droit sur la requête et sélectionnez **Exécuter maintenant**.
   - Sélectionnez la requête, puis dans le menu **Actions**, sélectionnez **Exécuter maintenant**.

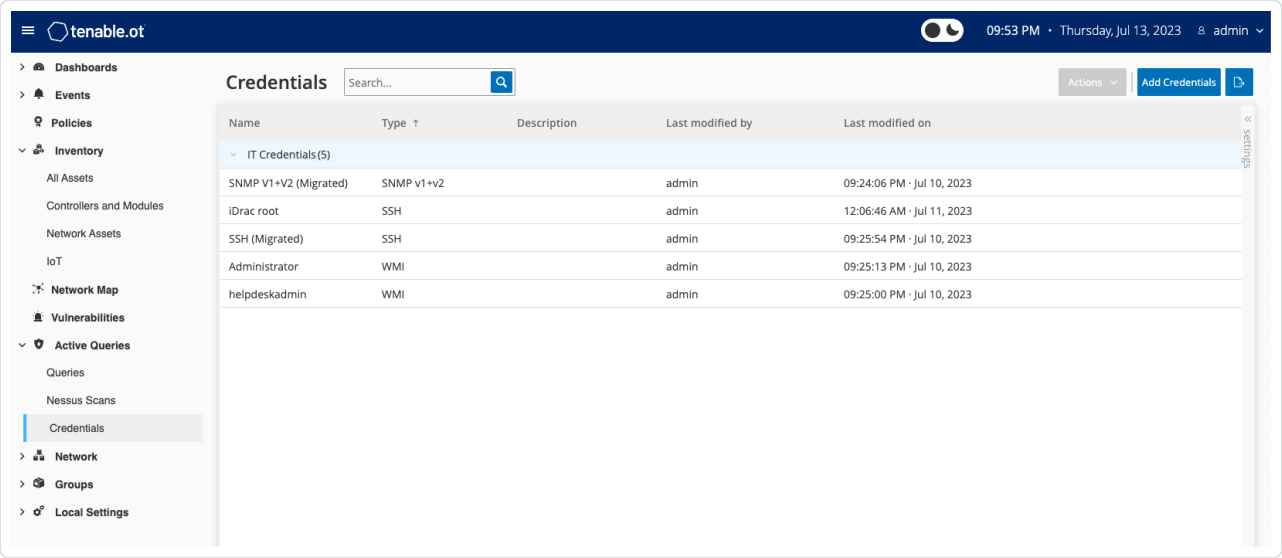
   Un message demande de confirmer l'exécution de la requête.

3. Cliquez sur **OK**.

   OT Security exécute la requête sélectionnée.

Informations d'authentification

Utilisez la page **Informations d'authentification** pour configurer les identifiants des appareils lorsqu'ils sont nécessaires. Lorsqu'ils communiquent dans leurs protocoles réseau natifs ou des protocoles propriétaires, les appareils n'ont pas besoin d'informations d'authentification. Cependant, certains appareils pris en charge par OT Security peuvent nécessiter des informations d'authentification pour permettre la découverte des assets.



Ajouter des informations d'authentification

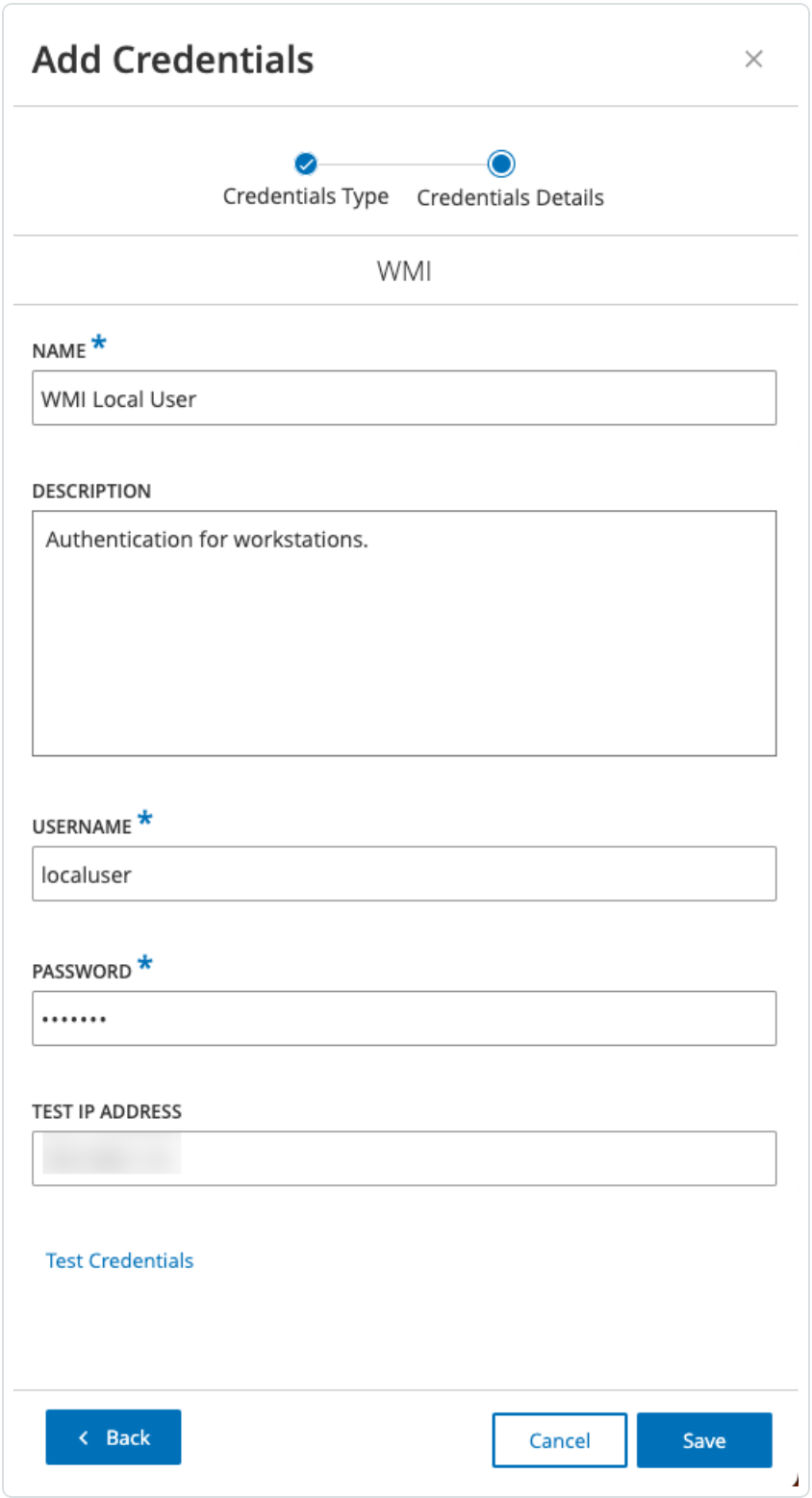
Pour ajouter des informations d'authentification :

1. Accédez à **Requêtes actives** > **Informations d'authentification**.

   La page **Informations d'authentification** apparaît.

2. Dans le coin supérieur droit, cliquez sur **Ajouter des informations d'authentification**.

Le panneau **Ajouter des informations d'authentification** apparaît.



3. Dans la section **Type d'informations d'authentification**, cliquez pour sélectionner le type d'appareil. Les options disponibles sont les suivantes :
    - ABB RTU 500
    - Bachmann
    - Concept
    - Sel
    - SicamA8000
    - SIPROTEC 5
    - SNMP v1+v2
    - SNMP v3
    - SSH
    - WMI
4. Cliquez sur **Suivant**.

    Le panneau **Détails des informations d'authentification** apparaît.
5. Fournissez les informations suivantes :
    - **Nom** : nom des informations d'authentification.
    - **Description** : description des informations d'authentification.
    - **Nom d'utilisateur** : nom d'utilisateur de l'appareil.
    - **Mot de passe** : mot de passe de l'appareil.
    - **Adresse IP de test** : adresse IP de l'appareil.
6. Cliquez sur **Tester les informations d'authentification** pour vérifier si OT Security peut accéder à l'appareil à l'aide des informations d'authentification.
7. Cliquez sur **Enregistrer**.

    OT Security enregistre les informations d'authentification. Elles figurent sur la page **Informations d'authentification**.

Modifier des informations d'authentification

Vous pouvez modifier les détails des informations d'authentification.

Modifier les informations d'authentification :

1. Accédez à **Requêtes actives** > **Informations d'authentification**.

   La page **Informations d'authentification** apparaît.

2. Effectuez l'une des actions suivantes :

   - Effectuez un clic droit sur les informations d'authentification requises et sélectionnez **Modifier**.
   - Sélectionnez les informations d'authentification, puis dans le menu **Actions**, sélectionnez **Modifier**.

   Le panneau **Modifier les informations d'authentification** apparaît.

3. Modifiez les détails selon les besoins.
4. Cliquez sur **Enregistrer**.

Supprimer des informations d'authentification

Vous pouvez supprimer les informations d'authentification dont vous n'avez plus besoin.

Pour supprimer des informations d'authentification :

1. Accédez à **Requêtes actives** > **Informations d'authentification**.

   La page **Informations d'authentification** apparaît.

2. Effectuez l'une des actions suivantes :

   - Effectuez un clic droit sur les informations d'authentification requises et sélectionnez **Supprimer**.
   - Sélectionnez les informations d'authentification requises, puis dans le menu **Actions**, sélectionnez **Supprimer**.

   OT Security supprime les informations d'authentification sélectionnées.

Comptes WMI

Pour permettre à OT Security d'effectuer des requêtes WMI (Windows Management Instrumentation), vous pouvez configurer un compte WMI. OT Security utilise les requêtes WMI pour obtenir plus d'informations sur les systèmes Windows.

OT Security repose sur les mêmes méthodes WMI que Tenable Nessus lors de l'exécution de requêtes WMI. Pour configurer un compte WMI pour le scan, voir la section Enable Windows Logins for Local and Remote Audits (Activer les connexions Windows pour les audits locaux et à distance) dans le Guide de l'utilisateur Tenable Nessus.

Créer des scans des plug-ins Nessus

Le scan de plug-in Nessus lance un scan Nessus avancé qui exécute une liste définie par l'utilisateur de plug-ins sur les assets spécifiés dans la liste de CIDR et d'adresses IP.

OT Security exécute le scan sur les assets réactifs au sein des CIDR désignés. Cependant, afin de protéger vos appareils OT, OT Security scanne uniquement les assets réseau confirmés dans la plage donnée (hors PLC). OT Security exclut les assets de type **Endpoint** (Terminal) du scan.

Le scan Nessus dans OT Security utilise les mêmes paramètres de politique qu'un scan réseau de base dans Tenable Nessus, Tenable Security Center et Tenable Vulnerability Management. La seule différence réside dans les options de performance de OT Security. Voici les options de performance pour le scan Nessus dans OT Security. Ces options s'appliquent également au scan Nessus de base que vous lancez à partir de la page **Inventaire** > **Tous les assets**.

- 5 hôtes simultanés (max.)
- 2 vérifications simultanées par hôte (max.)
- 15 secondes de délai d'expiration pour la lecture réseau

Remarque : Tenable Nessus est un outil invasif qui fonctionne mieux dans les environnements informatiques. Tenable ne recommande pas d'utiliser Tenable Nessus sur les appareils OT, car cela peut interférer avec leur fonctionnement.

Pour exécuter un scan Nessus de base sur un asset, voir Effectuer un scan Tenable Nessus spécifique à un asset.

Remarque : vous pouvez exécuter le scan de base sur des assets de type **Endpoint** (Terminal).

Créer un scan de plug-in Nessus

Pour créer un scan de plug-in Nessus :

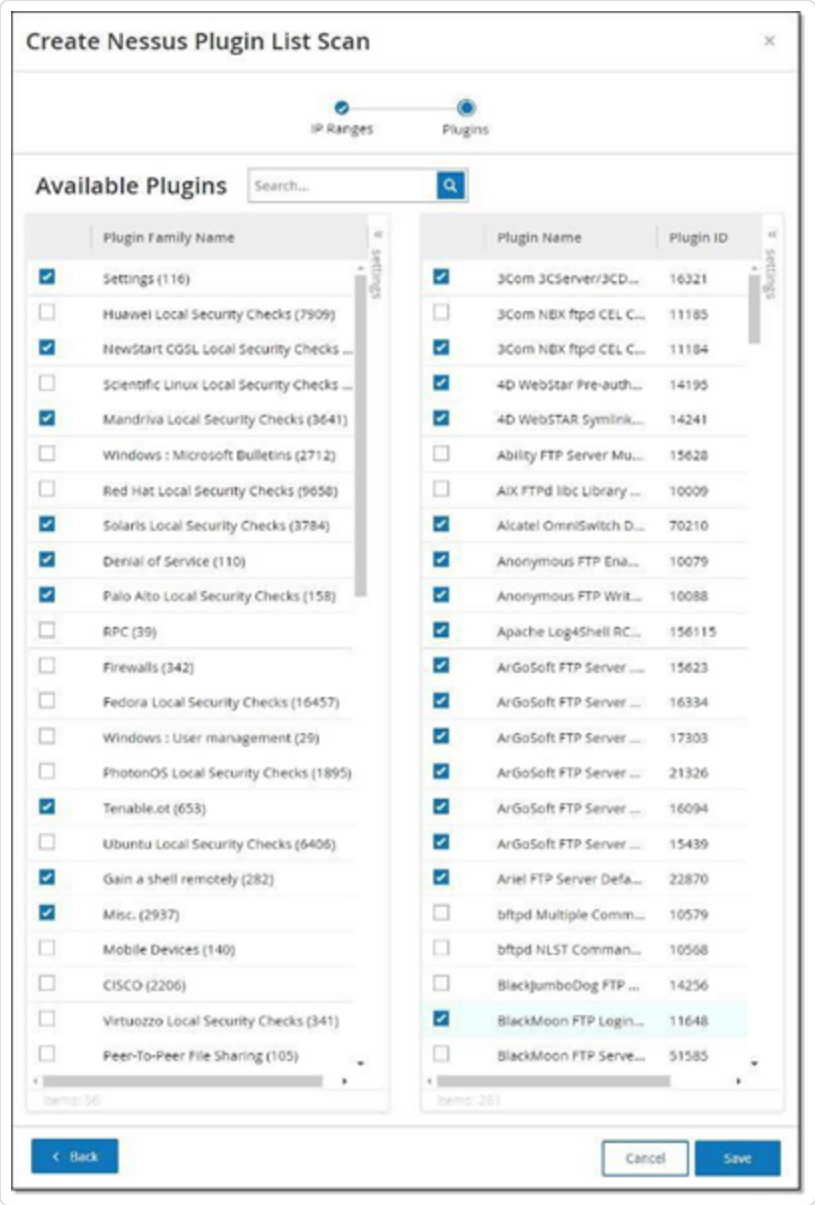
1. Accédez à **Requêtes actives** > **Scans Nessus**.
2. Dans le coin supérieur droit, cliquez sur **Créer un scan**.

   Le panneau **Créer un scan de la liste des plug-ins Nessus** apparaît.

3. Dans la zone **Nom**, saisissez le nom du scan Nessus.

4. Dans la zone **Plages d'adresses IP**, saisissez une plage d'adresses IP ou de CIDR.
5. Cliquez sur **Suivant**.

   Le volet **Plug-ins** apparaît.



Remarque : OT Security ne répertorie que les plug-ins spécifiques à l'appareil. Votre licence doit être à jour pour recevoir de nouveaux plug-ins. Pour mettre à jour votre licence, voir Mettre à jour la licence.

6. Dans la colonne **Nom de la famille du plug-in**, sélectionnez les familles de plug-ins requises pour les inclure dans le scan. Dans la colonne de droite, décochez les cases de certains plug-ins au besoin.

   Remarque : pour plus d'informations sur les familles de plug-ins Tenable Nessus, voir https://fr.tenable.com/plugins/nessus/families.

7. Cliquez sur **Enregistrer**.

   Le nouveau scan Nessus apparaît sur la page **Scans Nessus**.

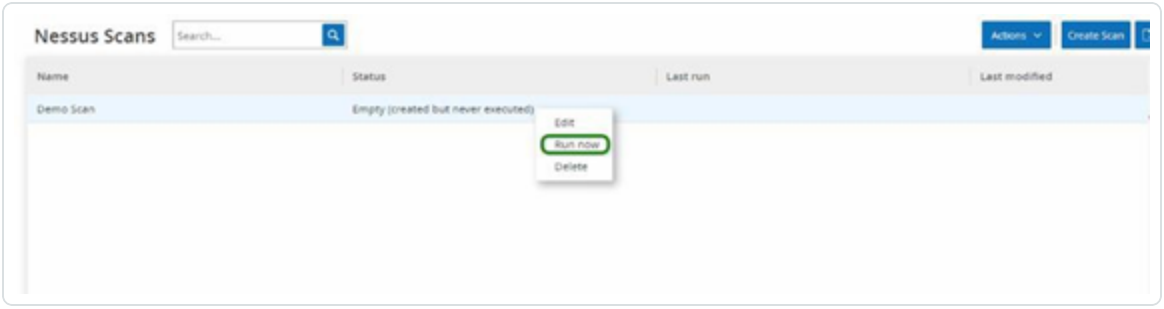
   Remarque : pour modifier ou supprimer un scan Tenable Nessus existant, effectuez un clic droit sur le scan et sélectionnez **Modifier** ou **Supprimer**.

Exécuter un scan de plug-in Nessus

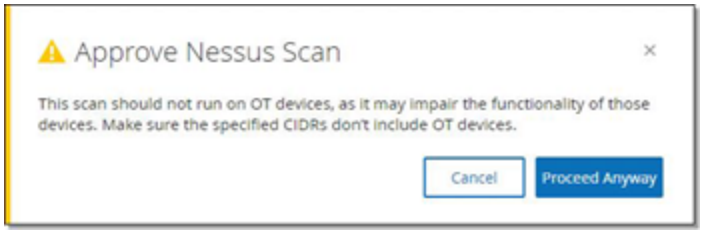
Pour exécuter un scan de plug-in Nessus :

1. Sur la page **Scans Nessus**, effectuez l'une des actions suivantes :

   - Effectuez un clic droit sur le scan et sélectionnez **Exécuter maintenant**.
   - Sélectionnez le scan que vous souhaitez exécuter et cliquez sur **Actions** > **Exécuter maintenant**.

   La boîte de dialogue **Approuver le scan Nessus** apparaît.

2. Si vous savez qu'aucun appareil OT n'est inclus dans le scan, cliquez sur **Continuer quand même**.

   La boîte de dialogue se referme et OT Security enregistre le scan.

3. Pour exécuter le scan, effectuez de nouveau un clic droit sur la ligne du scan et sélectionnez **Exécuter maintenant**.

   La boîte de dialogue **Approuver le scan Nessus** réapparaît.

4. Cliquez sur **Continuer quand même**.

   OT Security exécute maintenant le scan. Vous pouvez mettre en pause/reprendre, interrompre ou annuler les scans en fonction de leur statut en cours.

Réseau

OT Security surveille toutes les activités de votre réseau et affiche les données correspondantes sur les pages suivantes :

- **Récapitulatif réseau** – Affiche un aperçu du trafic réseau.
- **Captures de paquets** – Affiche une liste des fichiers PCAP capturés par le système. Voir Captures de paquets.
- **Communications** – Affiche une liste de toutes les conversations détectées sur le réseau, avec des détails sur la date et l'heure à laquelle elles se sont produites, les ressources impliquées, etc. Voir Communications

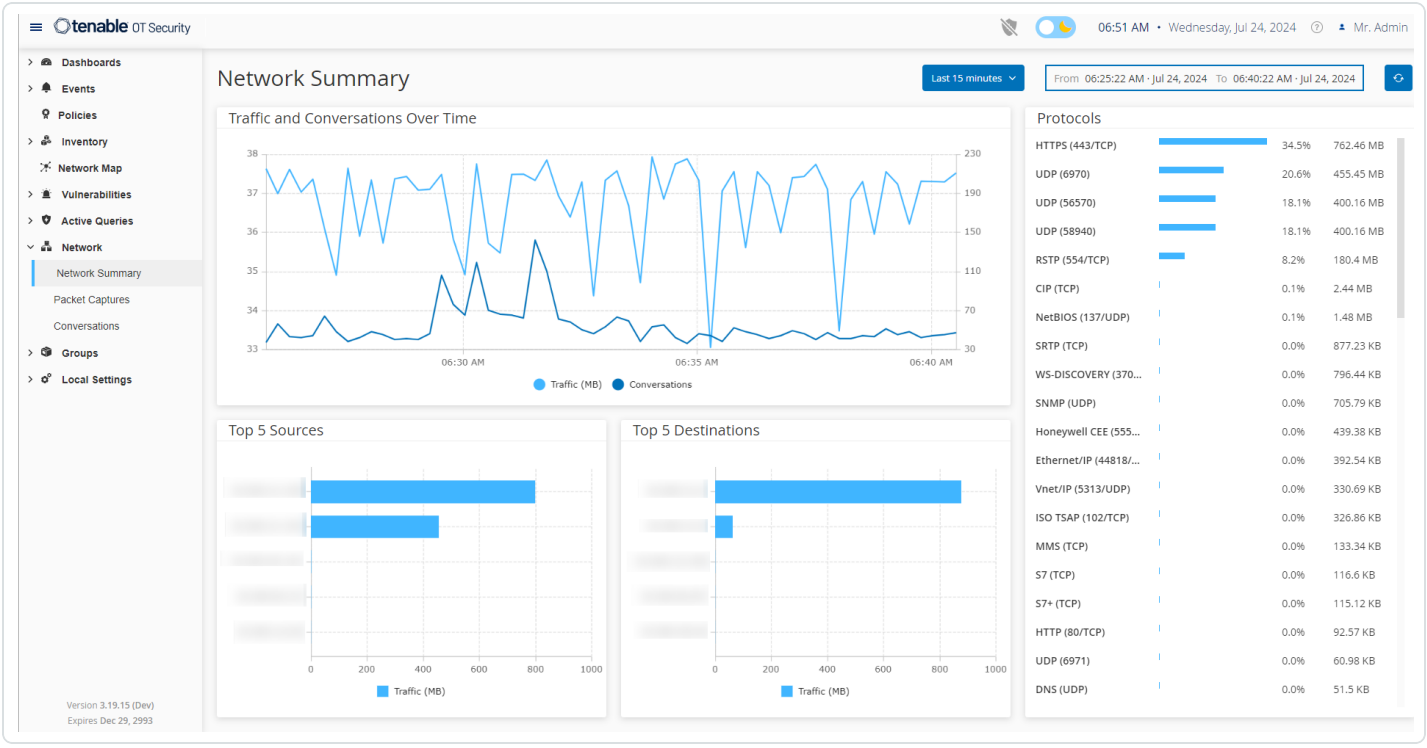
Pour accéder à la page **Réseau** :

1. Dans le volet de navigation de gauche, sélectionnez **Réseau**.

   La page **Récapitulatif réseau** apparaît.

Récapitulatif réseau

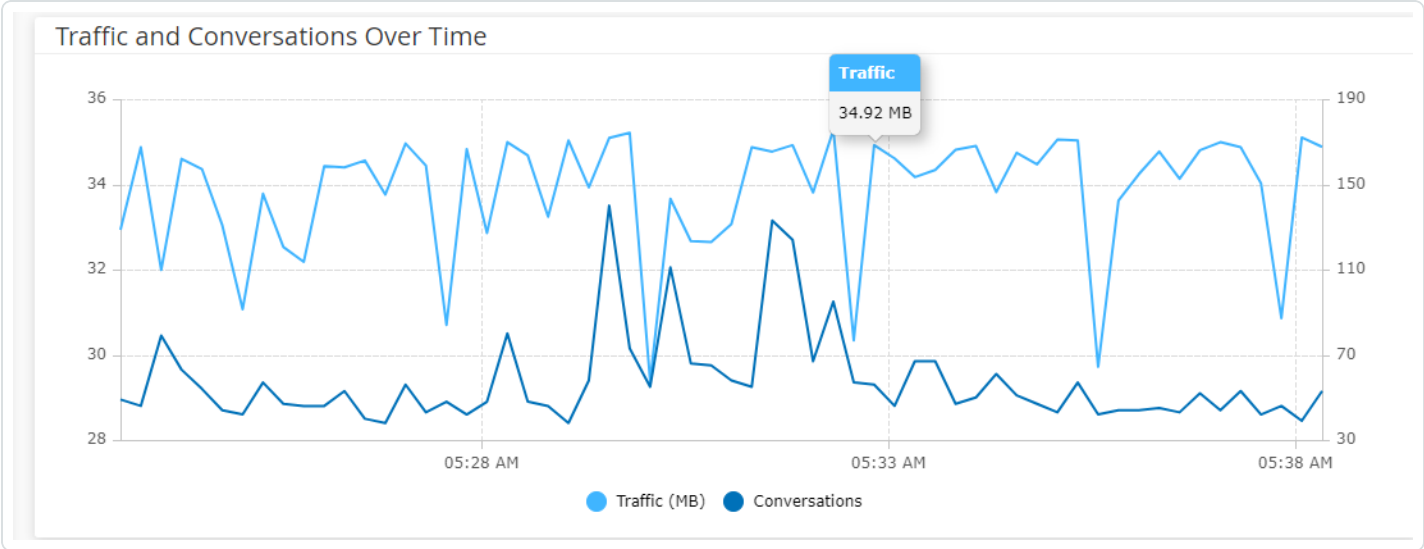
La page **Récapitulatif réseau** affiche des graphes visuels qui résument l'activité du réseau. Vous pouvez afficher les données associées à une période spécifique.



Interagissez avec les widgets suivants pour afficher des détails supplémentaires.

Trafic et communications au fil du temps

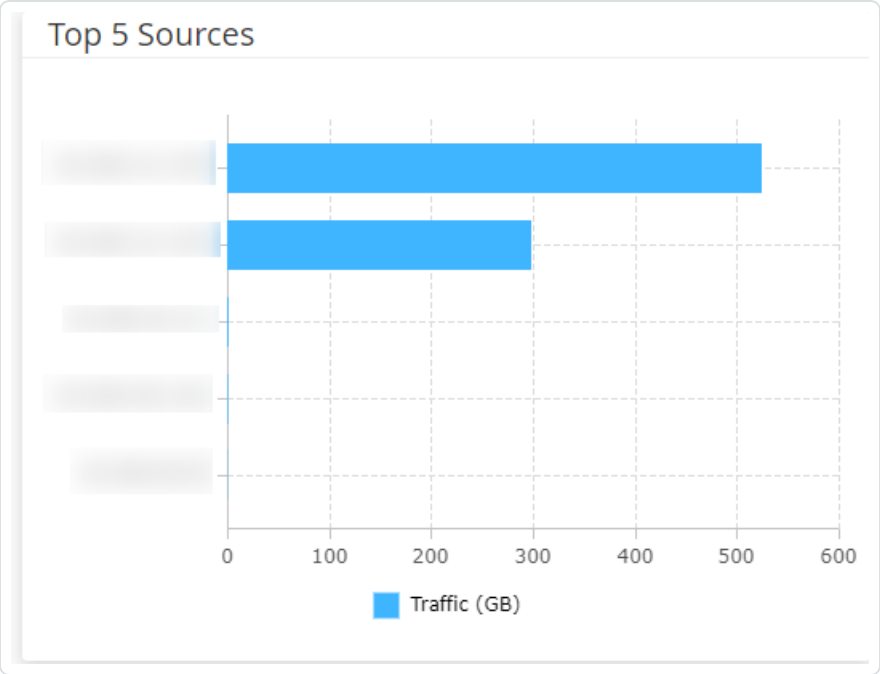
Un graphique en courbe affiche le volume de trafic (exprimé en Ko/Mo/Go) et le nombre de communications survenues sur le réseau au fil du temps. La légende apparaît en haut du graphe. Survolez un point du graphe avec la souris pour afficher des données spécifiques sur le trafic et les communications survenues pendant ce segment temporel.



Remarque : la longueur du segment temporel est ajustée en fonction de l'échelle de temps affichée dans le graphe. Par exemple, les données d'une période de 15 minutes affichent chaque minute séparément, tandis qu'une période de 30 jours affiche les données pour des segments de 6 heures.

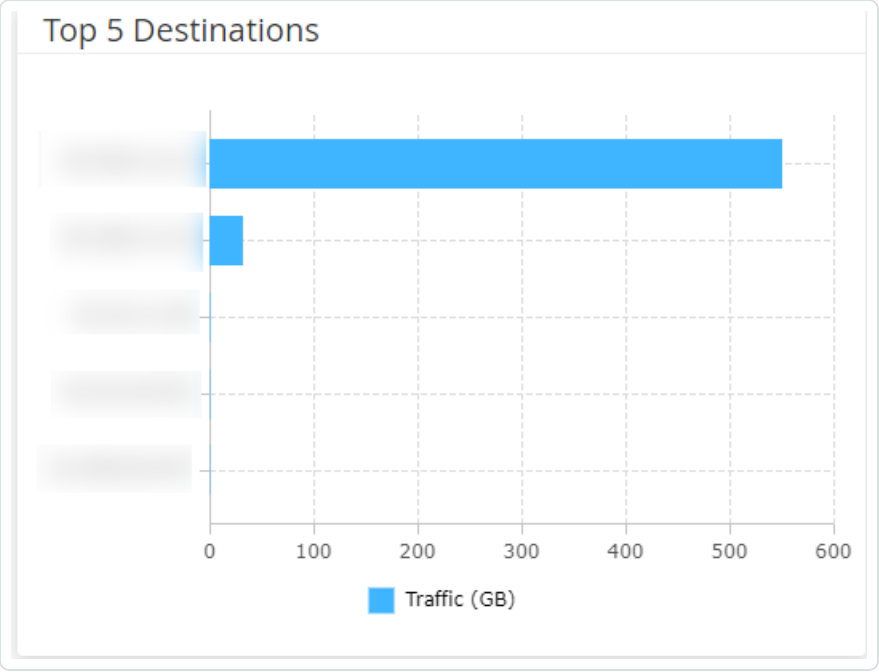
Top 5 sources

Le widget « Top 5 sources » affiche le nombre de communications et le volume de trafic de chacun des cinq principaux assets qui ont envoyé des communications via le réseau pendant une période spécifique. Vous pouvez identifier les assets sources par leurs adresses IP. Survolez l'histogramme pour afficher le nombre de communications et le volume de trafic provenant de cet asset.



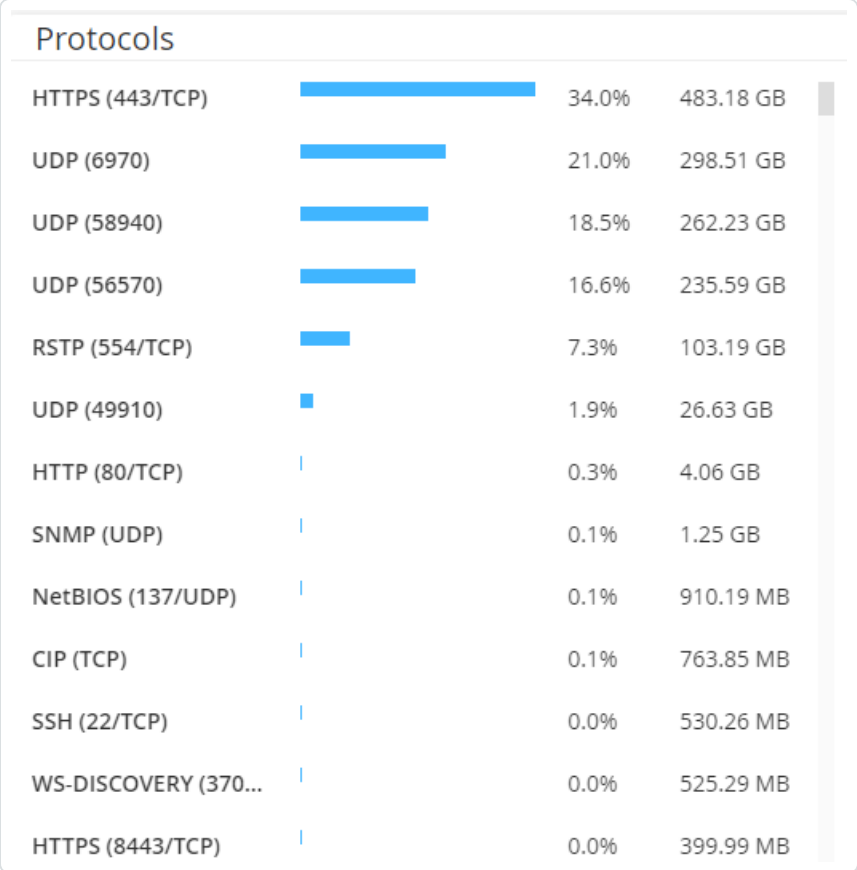
Top 5 cibles

Le widget « Top 5 cibles » affiche le nombre de communications et le volume de trafic de chacun des cinq principaux assets qui ont reçu des communications via le réseau pendant une période spécifique. Vous pouvez identifier les assets sources par leurs adresses IP. Survolez l'histogramme pour afficher le nombre de communications et le volume de trafic reçus par cet asset.



Protocoles

Le widget **Protocoles** affiche des données sur l'utilisation de divers protocoles de communication au sein du réseau pendant une période spécifique.



Les protocoles sont répertoriés du plus utilisé (en haut) au moins utilisé (en bas). Chaque protocole affiche les informations suivantes :

- Un histogramme indiquant le taux d'utilisation, avec une barre pleine indiquant l'utilisation la plus élevée et des barres partielles indiquant l'étendue de l'utilisation par rapport au protocole le plus utilisé.
- Le pourcentage d'utilisation
- Le volume total de communication

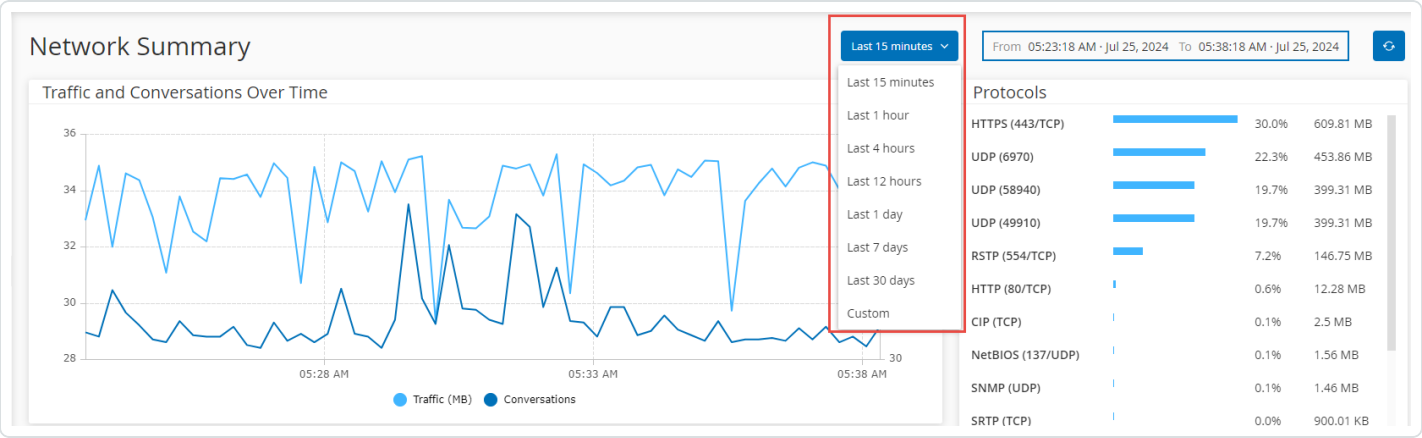
Définir la période

La page **Récapitulatif réseau** affiche les données qui représentent l'activité dans le réseau pendant une période spécifique. La barre d'en-tête indique la plage temporelle des données affichées. La période par défaut correspond aux **15 dernières minutes**. La barre d'en-tête indique également les dates/heures de début et de fin de la période.

Pour définir une période :

Dans la barre d'en-tête, cliquez sur le sélecteur de période. La période par défaut correspond aux **15 dernières minutes**.

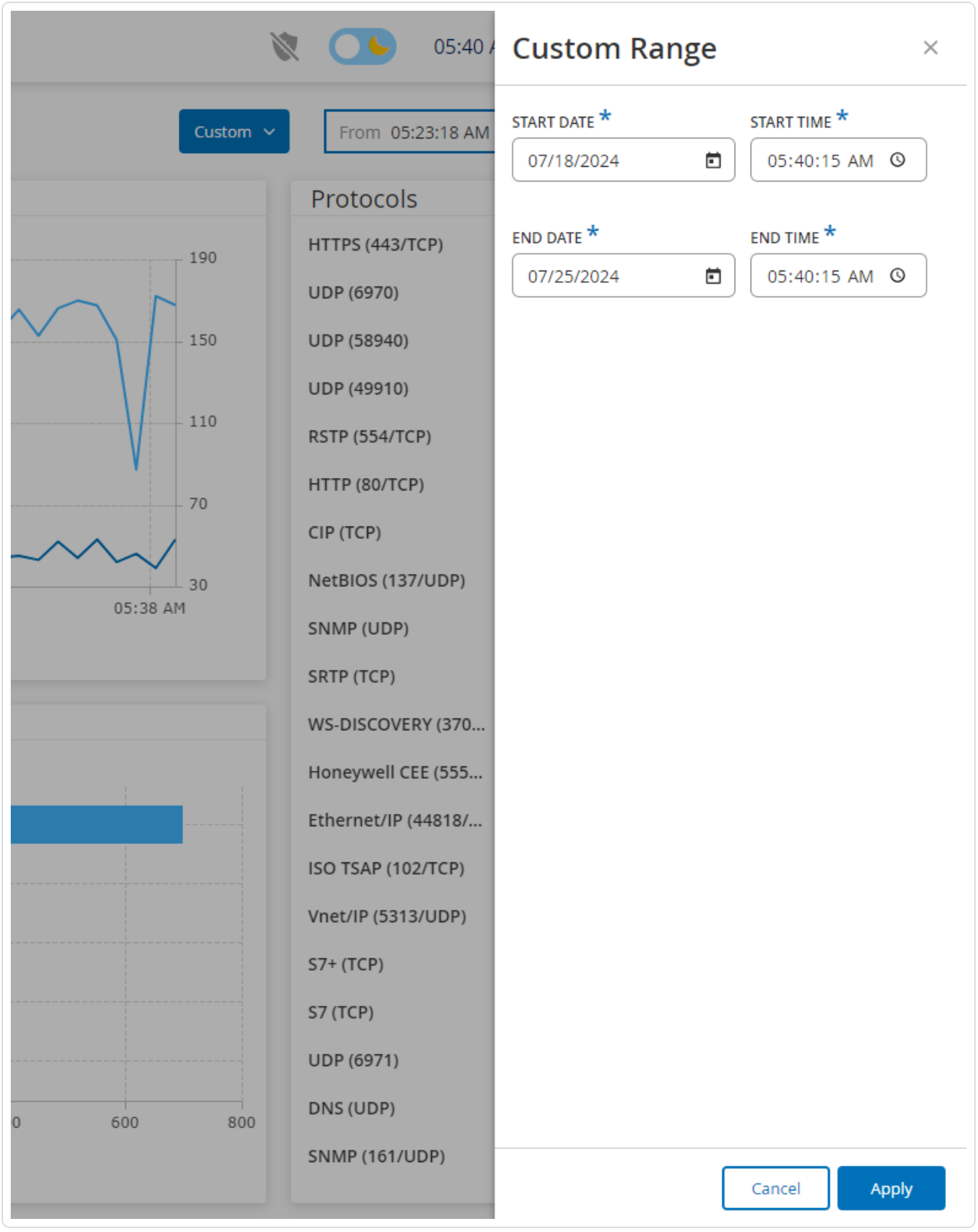
La zone déroulante répertorie les options disponibles.



Sélectionnez une plage temporelle en procédant de l'une des manières suivantes :

- Sélectionnez une plage temporelle prédéfinie en cliquant dessus. Les options sont : 15 dernières minutes, Dernière heure, 4 dernières heures, 12 dernières heures, Dernier jour, 7 derniers jours ou 30 derniers jours.
- Définissez une plage temporelle personnalisée :
- Cliquez sur **Personnalisée**.

  La fenêtre **Plage personnalisée** apparaît.



- Indiquez la **date de début**, l'**heure de début**, la **date de fin** et l'**heure de fin**.

- Cliquez sur **Appliquer**.

  Une fois que vous avez défini la période, la barre d'en-tête affiche les dates/heures de début et de fin à côté de la sélection de la période. OT Security actualise la page pour afficher les données dans la période choisie.

Captures de paquets

OT Security stocke des fichiers contenant des captures de paquets d'activités sur le réseau. Les données sont stockées sous forme de fichiers PCAP (capture de paquet) qui peuvent être analysés à l'aide d'outils d'analyse de protocole réseau tels que Wireshark. Cela permet une analyse approfondie des événements critiques. Lorsque la capacité de stockage du système est dépassée (1,8 To), le système supprime les anciens fichiers.

La page **Captures de paquets** affiche tous les fichiers PCAP du système. La section **Terminé** dresse la liste de tous les fichiers terminés disponibles au téléchargement. La section **En cours** affiche des détails sur la capture de paquets en cours.

La barre d'en-tête affiche le plus ancien fichier capturé encore disponible. Elle propose également une option pour télécharger des fichiers et pour arrêter manuellement la capture de paquets en cours.

Dans le tableau des captures de paquets, vous pouvez afficher ou masquer les colonnes, trier et filtrer les listes et rechercher des mots-clés. Pour plus d'informations sur la personnalisation des tableaux, voir Personnaliser les tableaux.

> **Remarque :** vous pouvez également télécharger le fichier PCAP d'un événement à partir de la page **Événements**. Voir Télécharger des fichiers.

Paramètres de capture de paquets

La liste Capture de paquet affiche les détails suivants :

Paramètre	Description
Date/ heure de début	La date et l'heure auxquelles la capture de paquets a commencé.

Date/ heure de fin	La date et l'heure auxquelles la capture de paquets a pris fin.
Statut	Le statut de la capture : **Terminé** ou **En cours**.
Capteur	Le capteur OT Security qui a capturé le paquet. Pour les paquets capturés directement par l'appliance OT Security, la valeur affichée est `local`.
Nom du fichier	Le nom du fichier.
Taille du fichier	La taille du fichier, donnée en Ko/Mo.

Filtrer l'affichage de la capture de paquets

Vous pouvez filtrer l'affichage de la capture de paquets pour rechercher un fichier PCAP en fournissant les paramètres d'heure de début et/ou d'heure de fin.

Pour filtrer les captures de paquets :

1. Accédez à **Réseau** > **Captures de paquets**.
2. Pour filtrer par heure de début, survolez **Heure de début** et cliquez sur l'icône ▽.

   Un menu déroulant apparaît.

   1. Pour définir le filtre :

      a. Dans le menu déroulant, sélectionnez le filtre requis : **N'importe quand (par défaut)**, **Début antérieur à** ou **Début postérieur à**.

      b. Si vous sélectionnez **Début antérieur à** ou **Début postérieur à**, une fenêtre contenant les zones **Date** et **Heure** apparaît pour vous permettre de choisir la date et l'heure souhaitées.

      c. Cliquez sur **Appliquer**.
3. Pour filtrer par heure de fin, survolez **Heure de fin** et cliquez sur l'icône ▽.

   Un menu déroulant apparaît.

1. Pour définir le filtre :

    a. Sélectionnez le filtre requis : **N'importe quand (par défaut)**, **Fin antérieure à** ou **Fin postérieure à**.

    b. Si vous sélectionnez **Fin antérieure à** ou **Fin postérieure à**, une fenêtre contenant les zones **Date** et **Heure** apparaît pour vous permettre de choisir la date et l'heure souhaitées.

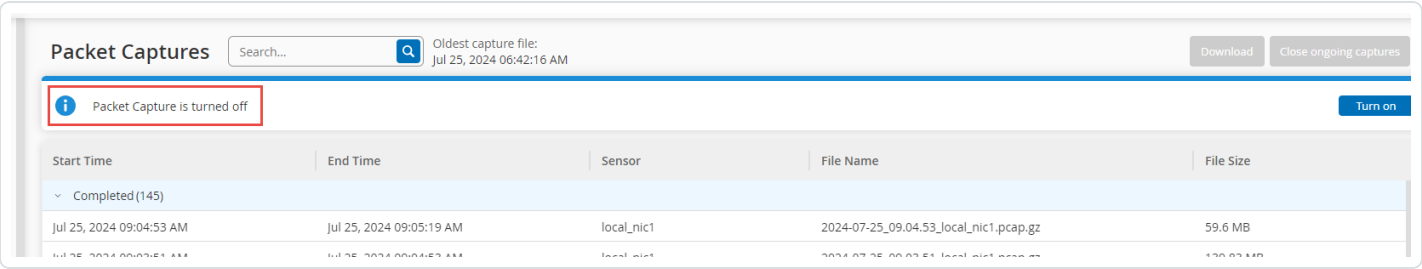
    c. Cliquez sur **Appliquer**.

    OT Security applique le filtre et affiche uniquement les fichiers générés dans la période spécifiée.

Activer ou désactiver les captures de paquets

Vous pouvez activer ou désactiver la fonction de capture de paquets dans **Paramètres locaux** > **Configuration système** > **Appareil**.

Si la fonction **Capture de paquets** est désactivée, l'écran **Captures de paquets** affiche un message vous informant qu'elle est désactivée.



Important : vous pouvez activer (mais pas désactiver) la capture de paquets à partir de l'écran **Réseau** > **Capture de paquets**.

Pour activer la capture de paquets :

1. Accédez à **Réseau** > **Captures de paquets**.
2. Dans la barre d'**en-tête**, cliquez sur **Activer**.

    OT Security lance la capture de paquets.

Télécharger des fichiers

Vous pouvez télécharger n'importe lequel des fichiers PCAP **terminés** sur votre ordinateur local. Vous pouvez ensuite l'analyser à l'aide d'outils d'analyse de protocole réseau tels que Wireshark.

Les captures de fichiers qui sont toujours en cours ne sont pas encore disponibles au téléchargement. Vous pouvez fermer manuellement une capture en cours pour fermer le fichier en cours et commencer à capturer des informations sur un nouveau fichier.

Pour télécharger un fichier terminé :

1. Accédez à **Réseau** > **Captures de paquets**.
2. Sélectionnez le fichier requis dans les listes de capture de paquets.
3. Dans la barre d'**en-tête**, cliquez sur **Télécharger**.

   OT Security télécharge le fichier PCAP au format zip sur votre ordinateur local.

Pour fermer manuellement la capture de paquets en cours :

1. Accédez à **Réseau** > **Captures de paquets**.
2. Dans la barre d'**en-tête**, cliquez sur **Fermer les captures en cours**.

   OT Security arrête la capture en cours et le fichier devient disponible au téléchargement. OT Security lance automatiquement une nouvelle capture de paquets.

Communications

Les communications sur le réseau ont lieu entre deux assets – une source et une cible. Par exemple, il pourra s'agir d'une interaction entre un poste d'ingénierie et un PLC, ou entre deux serveurs. La page **Communications** affiche une liste des communications actuelles et passées, avec des informations détaillées sur chacune d'entre elles.

Vous pouvez effectuer les actions suivantes à partir de la page **Communications** :

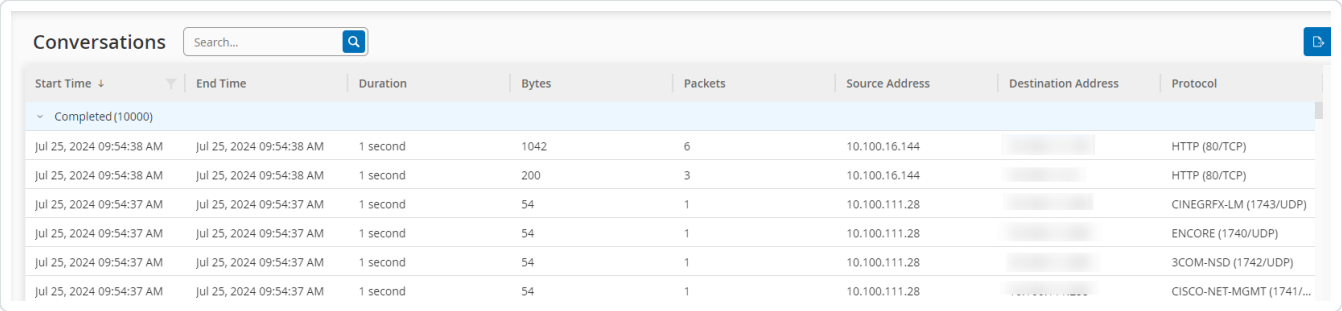
- **Rechercher** – Utilisez la zone de **recherche** pour retrouver des communications spécifiques en saisissant des informations d'identification.
- **Exporter** – Utilisez le bouton Exporter pour exporter toutes les données de l'onglet **Communications** vers votre ordinateur local sous forme de fichier `.csv`.

  Remarque : le tableau Communications affiche les 10 000 dernières communications réseau.

Pour accéder à la page **Communications** :

1. Accédez à **Réseau** > **Communications**.

   La page **Communications** apparaît.



   La page Communications affiche les détails suivants :

Paramètre	Description
Date/ heure de début	L'heure à laquelle la communication a démarré.
Date/ heure de fin	L'heure à laquelle la communication a pris fin. Affiche **En cours** pour les communications qui sont toujours en cours.
Durée	La durée de la communication.
Paquets	Le nombre de paquets de données envoyés pendant la communication.
Adresse source	L'adresse IP de l'asset qui a envoyé les données.
Adresse cible	L'adresse IP de l'asset qui a reçu les données.
Protocole	Le protocole utilisé pour la communication.

Groupes

Les groupes sont des éléments indispensables dans l'élaboration des politiques. Lorsque vous configurez une politique, vous définissez chaque condition à l'aide de groupes et non pas d'entités individuelles. OT Security est livré avec quelques groupes prédéfinis. Vous pouvez également créer

vos propres groupes personnalisés. Pour fluidifier la modification et la création de politiques, Tenable recommande de configurer à l'avance les groupes dont vous avez besoin.

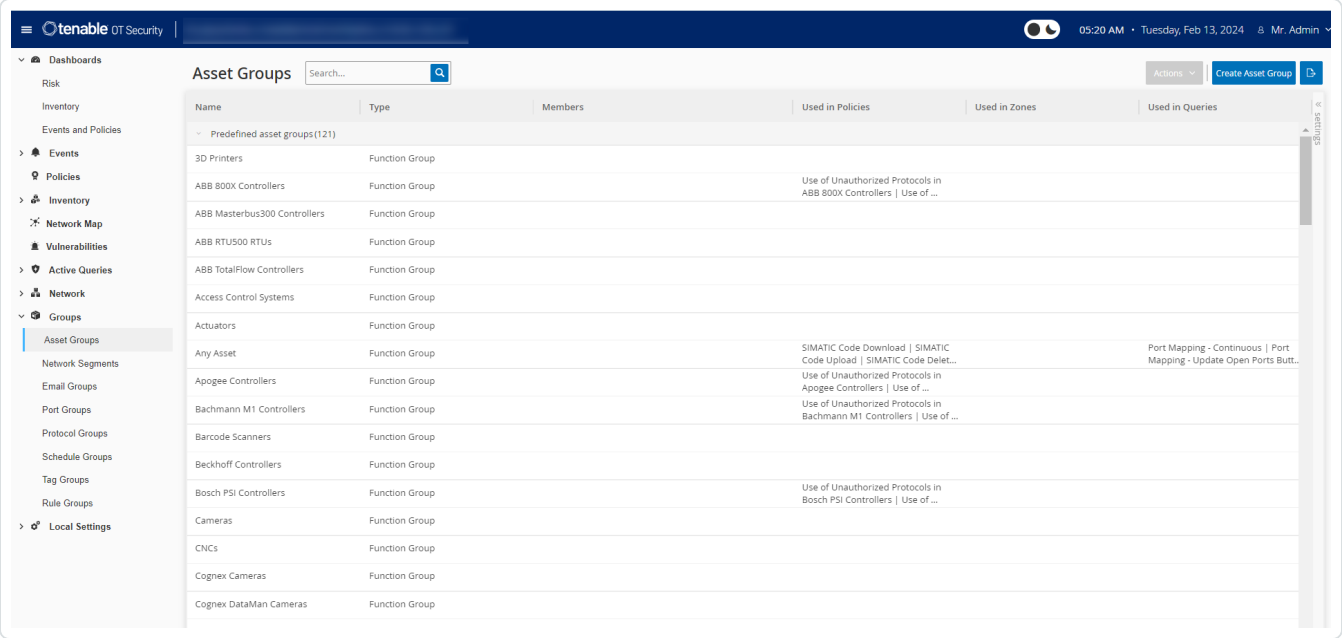
> **Remarque :** vous ne pouvez définir des paramètres de politique qu'en utilisant des groupes. Pour qu'une politique s'applique à une entité particulière, vous devez configurer un groupe comprenant uniquement cette entité.

Afficher les groupes

Pour afficher les groupes :

1. Dans la barre de navigation de gauche, cliquez sur **Groupes**.

   La section **Groupes** se développe pour afficher les types de groupes.



Sous **Groupes**, vous pouvez afficher tous les groupes configurés dans votre système. Les groupes sont divisés en deux catégories :

- **Groupes prédéfinis** – Ils sont préconfigurés ; vous ne pouvez pas les modifier.
- **Groupes définis par l'utilisateur** – Vous pouvez créer et modifier ces groupes.

Il existe plusieurs types de groupes, chacun étant utilisé pour la configuration de divers types de politiques. Chaque type de groupe est affiché sur un écran séparé sous Groupes. Les types de groupes sont :

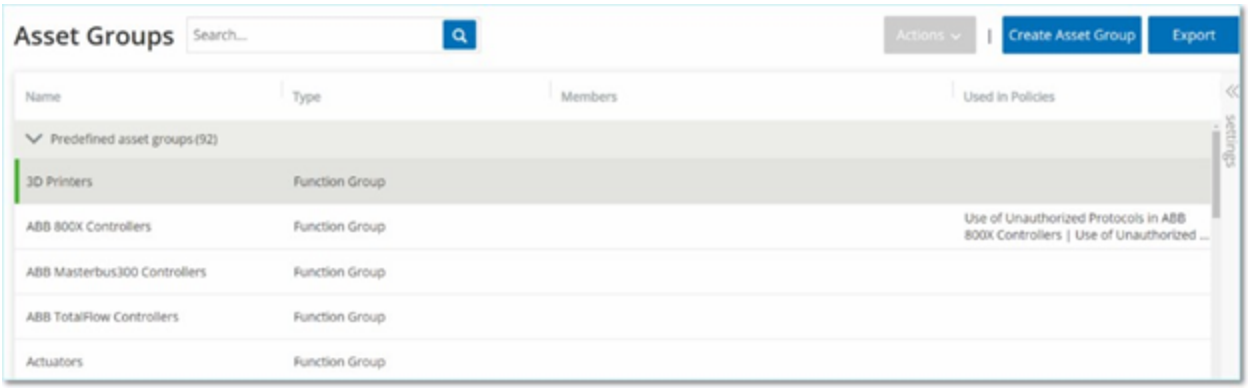
- **Groupes d'assets** – Les assets sont des entités matérielles du réseau. Les groupes d'assets sont utilisés comme condition pour un grand nombre de types de politiques.
- **Segments réseau** – La segmentation du réseau est une méthode de création de groupes d'assets réseau associés, qui permet d'isoler logiquement un groupe d'assets d'un autre.
- **Groupes de messagerie** – Groupes d'e-mails qui sont notifiés lorsqu'un événement lié à une politique se produit. Utilisés pour tous les types de politiques.
- **Groupes de ports** – Groupes de ports utilisés par les assets du réseau. Utilisés pour les politiques qui identifient les ports ouverts.
- **Groupes de protocoles** – Groupes de protocoles par lesquels les communications sont menées entre les assets du réseau. Utilisés comme condition de politique pour les **événements réseau**.
- **Groupes de planification** – Les groupes de planification sont des plages temporelles utilisées pour configurer la date et l'heure auxquelles l'événement spécifié doit se produire pour remplir les conditions de la politique.
- **Groupes de tags** – Les tags sont des paramètres dans les contrôleurs qui contiennent des données opérationnelles spécifiques. Les groupes de tags sont utilisés comme condition de politique pour les événements SCADA.
- **Groupes de règles** – Les groupes de règles comprennent un ensemble de règles associées, reconnues par leurs identifiants de signature (SID) Suricata. Ces groupes sont utilisés comme conditions pour définir des politiques de détection d'intrusion.

La procédure de création de chaque type de groupe est décrite dans les sections suivantes. De plus, vous pouvez afficher, modifier, dupliquer ou supprimer un groupe existant. Voir Actions sur les groupes.

Groupes d'assets

Les assets sont des entités matérielles du réseau. Le regroupement d'assets similaires vous permet de créer des politiques qui s'appliquent à tous les assets du groupe. Par exemple, vous pouvez utiliser un groupe d'assets nommé Contrôleur pour créer une politique qui alerte en cas de modification apportée au firmware d'un contrôleur. Les groupes d'assets sont utilisés comme condition pour un grand nombre de types de politiques. Les groupes d'assets peuvent être utilisés pour spécifier l'asset source, l'asset cible ou l'asset affecté pour différents types de politiques.

Afficher les groupes d'assets



L'écran **Groupes d'assets** affiche tous les groupes d'assets actuellement configurés dans le système. L'onglet **Groupes d'assets prédéfinis** affiche les groupes intégrés au système qui ne peuvent pas être modifiés, dupliqués ou supprimés. L'onglet **Groupes d'assets définis par l'utilisateur** contient les groupes personnalisés créés par l'utilisateur. Vous pouvez modifier, dupliquer ou supprimer ces groupes.

Le tableau Groupes d'assets affiche les informations suivantes :

Paramètre	Description
Statut	Indique si la politique est activée ou désactivée. Si le système désactive automatiquement la politique, car elle générait un trop grand nombre d'événements, une icône d'avertissement apparaît. Activez ou désactivez une politique à l'aide du curseur de statut.
Nom	Le nom de la politique.
Sévérité	Le degré de sévérité de l'événement. Les valeurs possibles sont : Aucune, Faible, Moyenne ou Élevée. Voir la section Niveaux de sévérité pour plus d'informations.

Type d'événement	Le type spécifique d'événement qui déclenche cette politique d'événement.
Catégorie	La catégorie du type d'événement qui déclenche cette politique d'événement. Les valeurs possibles sont : Événements de configuration, Événements SCADA, Menaces réseau ou Événement réseau. Pour une explication des différentes catégories, voir Catégories et sous-catégories de politiques.
Source	Une condition de politique. Le groupe d'assets source auquel la politique s'applique. Un groupe d'assets est l'asset qui a lancé l'activité.
Nom	Nom utilisé pour identifier le groupe.
Type	Type de groupe. Les options sont : • **Function** (Fonction) – Un groupe d'assets prédéfini créé pour remplir une fonction spécifique. • **Sélection d'assets** – Des assets spécifiés sont inclus dans le groupe. • **Liste d'IP** – Assets avec l'adresse IP spécifiée. • **Plage IP** – Assets au sein de la plage d'adresses IP spécifiée.
Membres	Affiche la liste des assets inclus dans ce groupe. Aucune valeur n'est affichée pour les groupes de type Function Groups (Groupes de fonction). **Remarque :** s'il n'y a pas assez de place pour afficher tous les assets de cette ligne, cliquez sur le menu **Actions** du tableau > **Afficher** > onglet **Membres**.
Utilisé dans les politiques	Affiche le nom de chaque politique qui utilise ce groupe d'assets dans sa configuration. **Remarque :** pour afficher plus de détails sur les politiques dans lesquelles le groupe est utilisé, cliquez sur le menu **Actions** du tableau > **Afficher** > onglet **Utilisé dans les politiques**.
Utilisé dans des requêtes	Affiche le nom de la requête qui utilise le groupe d'assets.

Les procédures de création de chaque type de groupes d'assets sont décrites dans la section suivante. De plus, vous pouvez afficher, modifier, dupliquer ou supprimer un groupe existant. Voir Actions sur les groupes.

Créer des groupes d'assets

Vous pouvez créer des groupes d'assets personnalisés pour les utiliser dans la configuration de politiques. Le regroupement d'assets similaires vous permet de créer des politiques qui s'appliquent à tous les assets du groupe.

Il existe trois types de groupes d'assets définis par l'utilisateur :

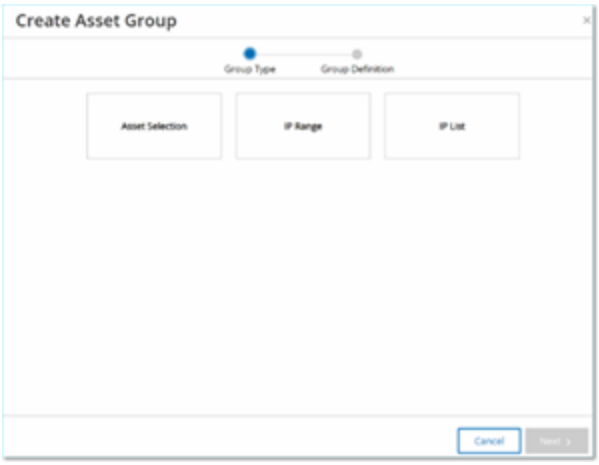
- **Sélection d'assets** – Indique des assets spécifiques inclus dans le groupe.
- **Liste d'IP** – Indique les adresses IP des assets inclus dans le groupe.
- **Plage IP** – Indique les plages d'adresses IP des assets inclus dans le groupe.

Il existe différentes procédures pour créer chaque type de groupe d'assets.

Pour créer un groupe d'assets de type Sélection d'assets :

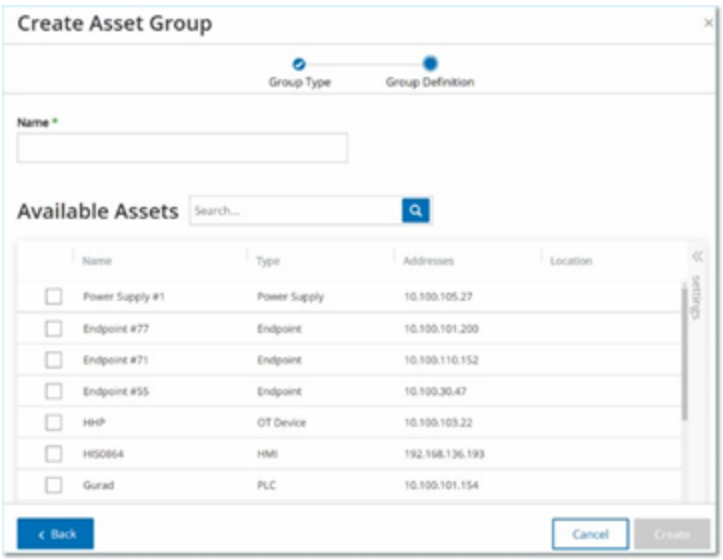
1. Accédez à **Groupes** > **Groupes d'assets**.
2. Cliquez sur **Créer un groupe d'assets**.

   Le panneau **Créer un groupe d'assets** apparaît.



3. Cliquez sur **Sélection d'assets**.
4. Cliquez sur **Suivant**.

La liste des **assets disponibles** apparaît.



5. Dans la zone **Nom**, saisissez le nom du groupe.

   Choisissez un nom qui décrit un élément commun catégorisant les assets inclus dans le groupe.

6. Cochez la case à côté de chaque asset à inclure dans le groupe.

7. Cliquez sur **Créer**.

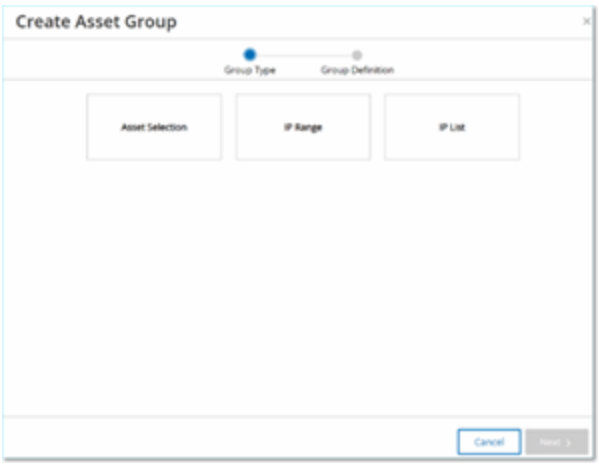
   OT Security crée le groupe d'assets et l'affiche sur l'écran **Groupes d'assets**. Vous pouvez désormais utiliser ce groupe lors de la configuration des politiques.

Pour créer un groupe d'assets de type Plage IP :

1. Accédez à **Groupes** > **Groupes d'assets**.

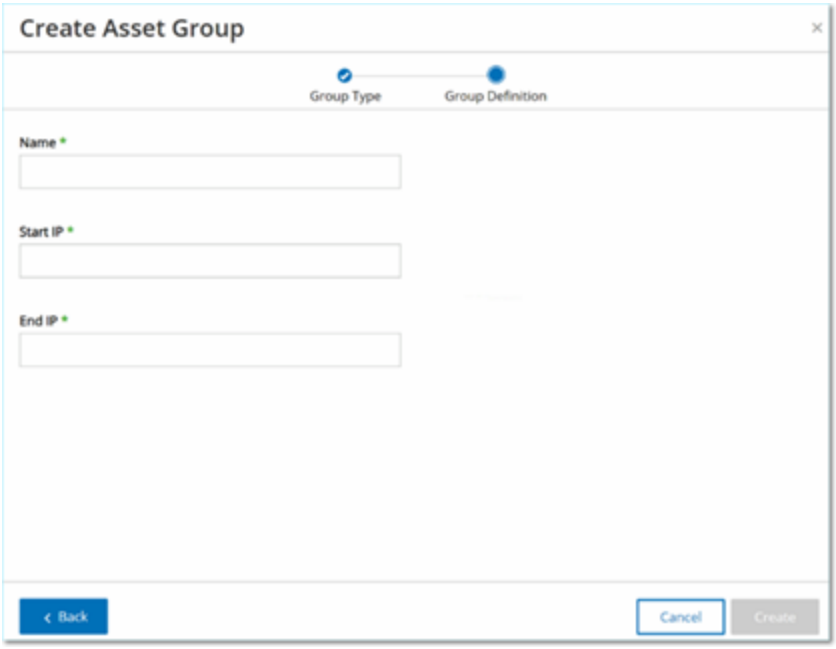
2. Cliquez sur **Créer un groupe d'assets**.

   Le panneau **Créer un groupe d'assets** apparaît.



3. Cliquez sur **Plage IP**.
4. Cliquez sur **Suivant**.

   Le panneau de sélection de la plage d'adresses IP apparaît.



5. Dans la zone **Nom**, saisissez le nom du groupe.

   Choisissez un nom qui décrit un élément commun catégorisant les assets inclus dans le groupe.

6. Dans la zone **Adresse IP de début**, saisissez l'adresse IP débutant la plage à inclure.

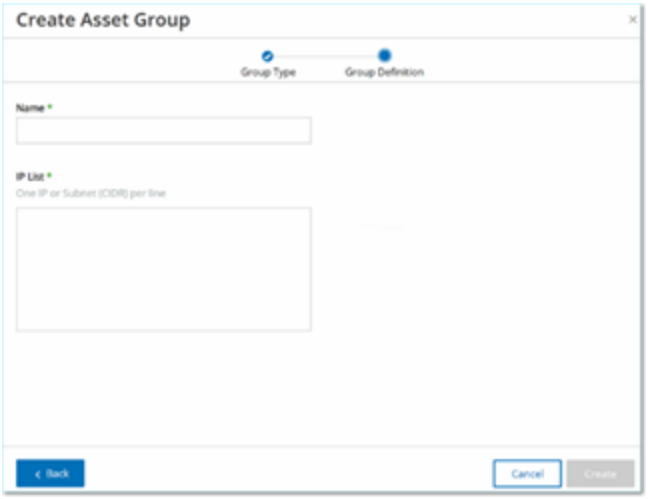
7. Dans la zone **Adresse IP de fin**, saisissez l'adresse IP finissant la plage à inclure.
8. Cliquez sur **Créer**.

   OT Security crée le groupe d'assets et l'affiche sur l'écran **Groupes d'assets**. Vous pouvez désormais utiliser ce groupe lors de la configuration des politiques.

Pour créer un groupe d'assets de type Liste d'IP :

1. Accédez à **Groupes** > **Groupes d'assets**.
2. Cliquez sur **Créer un groupe d'assets**.

   Le panneau **Créer un groupe d'assets** apparaît.



3. Cliquez sur **Liste d'IP**.
4. Cliquez sur **Suivant**.

   Le panneau **Liste d'IP** apparaît.
5. Dans la zone **Nom**, saisissez le nom du groupe.

   Choisissez un nom qui décrit un élément commun catégorisant les assets inclus dans le groupe.
6. Dans la zone **Liste d'IP**, saisissez une adresse IP ou un sous-réseau à inclure dans le groupe.
7. Pour ajouter d'autres assets au groupe, saisissez chaque adresse IP ou sous-réseau supplémentaire sur une ligne distincte.

8. Cliquez sur **Créer**.

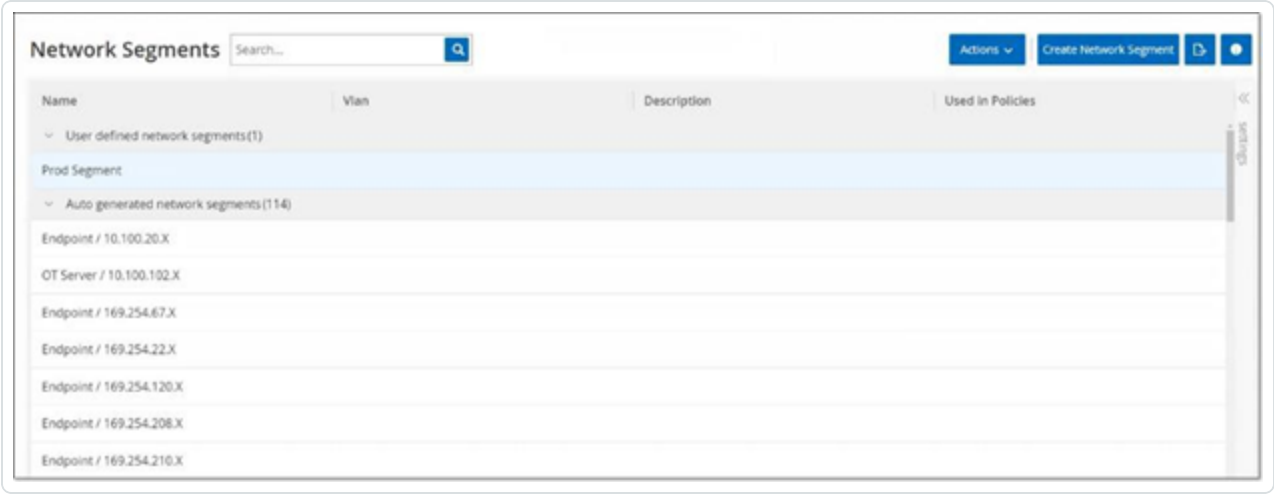
   OT Security crée le groupe d'assets et l'affiche sur l'écran **Groupes d'assets**. Vous pouvez désormais utiliser ce groupe lors de la configuration des politiques.

Segments réseau

Grâce à la segmentation du réseau, vous pouvez créer des groupes d'assets réseau associés, afin d'isoler logiquement les groupes d'assets les uns des autres. OT Security attribue automatiquement à un segment réseau chaque adresse IP associée à un asset de votre réseau. Pour les assets avec plus d'une adresse IP, chaque adresse IP est associée à un segment réseau. Chaque segment généré automatiquement inclut tous les assets d'une catégorie spécifique (contrôleur, serveurs OT, appareils réseau, etc.) qui ont des adresses IP avec la même adresse réseau de classe C (les IP ont les mêmes premiers 24 bits).

Vous pouvez créer des segments réseau définis par l'utilisateur et préciser les assets affectés à ce segment. Sur l'écran **Inventaire**, une colonne indique le segment réseau pour chaque asset, facilitant ainsi le tri et le filtrage de vos assets par segment réseau.

Afficher les segments réseau



L'écran **Segments réseau** affiche tous les segments réseau actuellement configurés dans le système. L'onglet **Segments réseau générés automatiquement** contient les segments réseau générés automatiquement par le système. L'onglet **Segments réseau définis par l'utilisateur** contient les segments réseau personnalisés qui ont été créés par l'utilisateur.

Le tableau Segments réseau affiche les détails suivants :

Paramètre	Description
Nom	Le nom utilisé pour identifier le segment réseau.
VLAN	Le numéro de VLAN du segment réseau. (Facultatif)
Description	Une description du segment réseau. (Facultatif)
Utilisé dans les politiques	Affiche les noms des politiques qui s'appliquent à ce segment réseau. **Remarque :** pour afficher plus de détails sur les politiques dans lesquelles le segment réseau est utilisé, cliquez sur **Actions** > **Afficher** > onglet **Utilisé dans les politiques**.

Vous pouvez afficher, modifier, dupliquer ou supprimer un segment réseau existant. Pour plus d'informations, voir Actions sur les groupes.

Créer des segments réseau

Vous pouvez créer des segments réseau pour les utiliser dans la configuration des politiques. Le regroupement de segments réseau similaires vous permet de créer des politiques qui définissent le trafic réseau acceptable pour les assets de ce segment.

Pour créer un segment réseau :

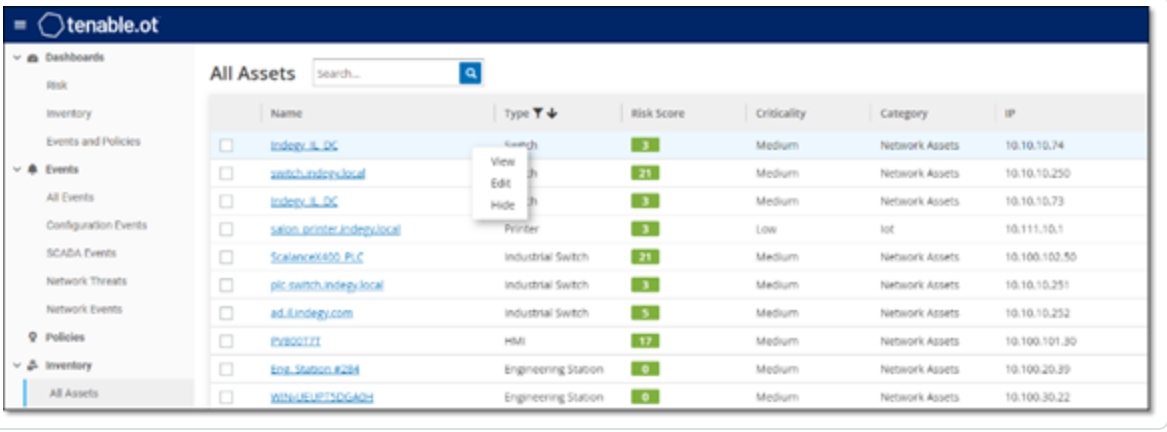
1. Accédez à **Groupes** > **Segments réseau**.
2. Cliquez sur **Créer un segment réseau**.

   Le panneau **Créer un segment réseau** apparaît.

3. Dans le champ **Nom**, saisissez le nom du segment réseau.
4. (Facultatif) Dans la zone **VLAN**, saisissez un numéro de VLAN pour ce segment réseau.
5. (Facultatif) Dans la zone **Description**, saisissez la description du segment réseau.
6. Cliquez sur **Créer**.

   OT Security crée le segment réseau et l'affiche dans la liste des segments réseau.
7. Pour affecter les assets au segment réseau nouvellement créé :
   a. Accédez à **Inventaire** > **Tous les assets**.
   b. Effectuez l'une des actions suivantes :

- Effectuez un clic droit sur l'asset à assigner au segment réseau nouvellement créé et sélectionnez **Modifier**.
- Survolez l'asset à attribuer, puis dans le menu **Actions**, sélectionnez **Modifier**.



La fenêtre **Modifier les détails de l'asset** apparaît.

8. Dans la zone déroulante **Segments réseau**, sélectionnez le segment réseau requis.

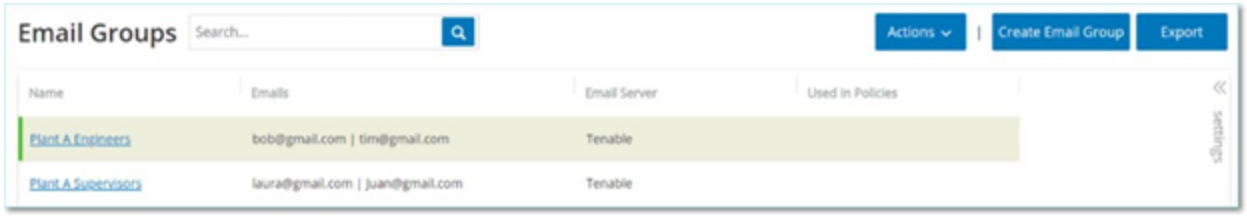
Remarque : certains assets disposent de plusieurs adresses IP associées. Vous pouvez sélectionner le segment réseau requis pour chacun d'eux.

OT Security applique le segment réseau à l'asset et l'affiche dans la colonne **Segment réseau**. Vous pouvez désormais utiliser ce segment réseau lors de la configuration des politiques.

Groupes de messagerie

Les groupes de messagerie sont des groupes contenant les adresses e-mail de parties concernées. Les groupes de messagerie sont utilisés pour préciser les destinataires des notifications d'événement déclenchées par des politiques spécifiques. Par exemple, le regroupement par rôle ou par service (entre autres) vous permet d'envoyer aux parties concernées les notifications liées à des politiques d'événements spécifiques.

Afficher des groupes de messagerie



L'écran **Groupes de messagerie** affiche tous les groupes de messagerie actuellement configurés dans le système.

Le tableau Groupes de messagerie affiche les informations suivantes :

Remarque : vous pouvez afficher des détails supplémentaires sur un groupe spécifique en sélectionnant le groupe et en cliquant sur **Actions** > **Afficher**.

Paramètre	Description
Nom	Nom utilisé pour identifier le groupe.
E-mails	La liste des adresses e-mails incluses dans le groupe. **Remarque :** s'il n'y a pas assez de place pour afficher tous les membres de ce

	groupe, cliquez sur **Actions** > **Afficher** > onglet **Membres**.
Serveur de messagerie	Le nom du serveur SMTP utilisé pour envoyer des e-mails au groupe.
Utilisé dans les politiques	Affiche les noms des politiques pour lesquelles des notifications sont envoyées à ce groupe. **Remarque :** pour afficher plus de détails sur les politiques dans lesquelles le groupe est utilisé, cliquez sur **Actions** > **Afficher** > onglet **Utilisé dans les politiques**.

De plus, vous pouvez afficher, modifier, dupliquer ou supprimer un groupe existant. Pour plus d'informations, voir Actions sur les groupes.

Créer des groupes de messagerie

Vous pouvez créer des groupes de messagerie personnalisés à utiliser dans la configuration des politiques. En regroupant les adresses e-mails associées, vous pouvez configurer les notifications d'événement de politique à envoyer à tout le personnel concerné.

Remarque : vous ne pouvez attribuer qu'un seul groupe de messagerie à chaque politique. Par conséquent, il est utile de créer à la fois des groupes larges et inclusifs ainsi que des groupes spécifiques et limités, afin de pouvoir affecter le groupe approprié à chaque politique.

Pour créer un groupe de messagerie :

1. Accédez à **Groupes** > **Groupes de messagerie**.
2. Cliquez sur **Créer un groupe de messagerie**.

   Le panneau **Créer un groupe de messagerie** apparaît.

3. Dans la zone **Nom**, saisissez le nom du groupe.
4. Dans la zone déroulante **Serveur SMTP**, sélectionnez le serveur utilisé pour envoyer les notifications par e-mail.

   Remarque : si aucun serveur SMTP n'a été configuré dans le système, vous devez d'abord en configurer un avant de pouvoir créer un groupe de messagerie. Voir Serveurs SMTP.

5. Dans la zone **E-mails** , saisissez l'adresse e-mail de chaque membre du groupe sur une ligne distincte.
6. Cliquez sur **Créer**.

   OT Security crée le groupe de messagerie et l'affiche sur la page **Groupes de messagerie**. Vous pouvez désormais utiliser ce groupe lors de la configuration des politiques.

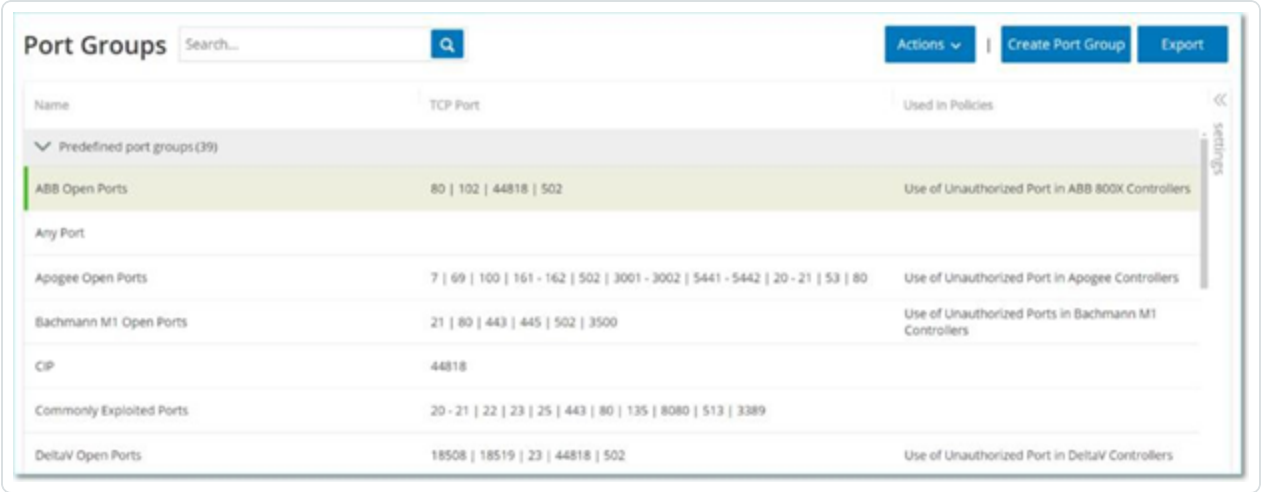
Groupes de ports

Les groupes de ports sont des groupes de ports utilisés par les assets du réseau. Les groupes de ports sont utilisés comme condition pour définir les politiques d'événement réseau **Port ouvert**, qui détectent les ports ouverts sur le réseau.

L'onglet **Prédéfinis** affiche les groupes de ports prédéfinis dans le système. Ces groupes comprennent les ports censés être ouverts sur les contrôleurs d'un fournisseur spécifique. Par exemple, le groupe Siemens PLC Open Ports (Ports Ouverts Siemens PLC) comprend : 20, 21, 80, 102, 443 et 502. Cela permet la configuration de politiques détectant les ports qui ne sont pas censés être ouverts pour les contrôleurs de ce fournisseur. Ces groupes ne peuvent pas être modifiés, dupliqués ni supprimés.

L'onglet **Définis par l'utilisateur** contient les groupes personnalisés créés par l'utilisateur. Vous pouvez modifier, dupliquer ou supprimer ces groupes.

Afficher les groupes de ports



Le tableau Groupes de ports affiche les détails suivants :

Paramètre	Description
Nom	Nom utilisé pour identifier le groupe.
Port TCP	La liste des ports et/ou des plages de ports inclus dans le groupe. **Remarque :** s'il n'y a pas assez de place pour afficher tous les membres du groupe, vous pouvez les afficher sur **Actions** > **Afficher** > onglet **Membres**.

Utilisé dans les politiques	Affiche le nom de chaque politique qui utilise ce groupe de ports dans sa configuration. **Remarque :** pour afficher plus d'informations sur les politiques dans lesquelles le groupe est utilisé, cliquez sur **Actions** > **Afficher** > onglet **Utilisé dans les politiques**.

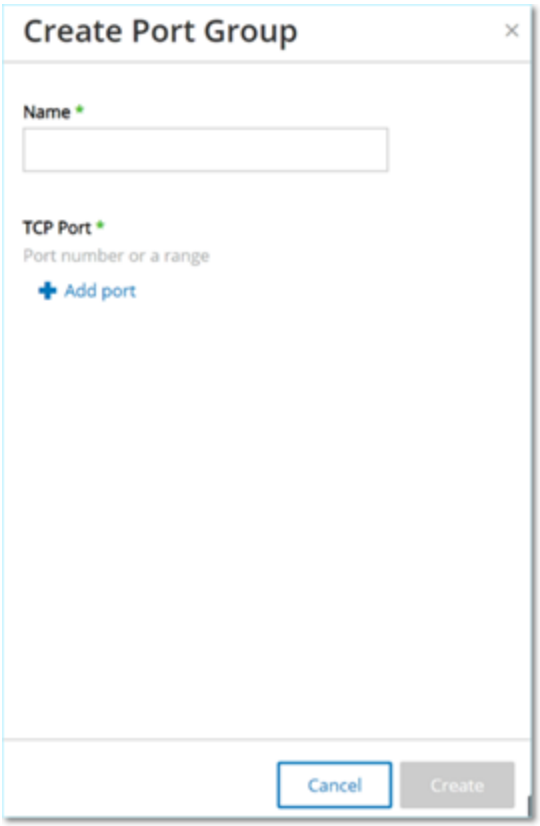
Créer des groupe de ports

Vous pouvez créer des groupes de ports personnalisés pour les utiliser dans la configuration des politiques. Le regroupement de ports similaires permet de créer des politiques qui alertent sur les ports ouverts posant un risque de sécurité spécifique.

Pour créer un groupe de ports :

1. Accédez à **Groupes** > **Groupes de ports**.
2. Cliquez sur **Créer un groupe de ports**.

   Le panneau **Créer un groupe de ports** apparaît.



3. Dans la zone **Nom**, saisissez le nom du groupe.
4. Dans la zone **Port TCP**, saisissez un port ou une plage de ports à inclure dans le groupe.
5. Pour ajouter des ports au groupe :
    a. Cliquez sur **+ Ajouter un port**.

        Une nouvelle zone de sélection de port apparaît.

    b. Dans la zone **Numéro de port**, saisissez un port ou une plage de ports à inclure dans le groupe.
6. Cliquez sur **Créer**.

    OT Security crée le groupe de ports et l'affiche dans la liste des groupes de ports. Vous pouvez désormais utiliser ce groupe lors de la configuration des politiques.

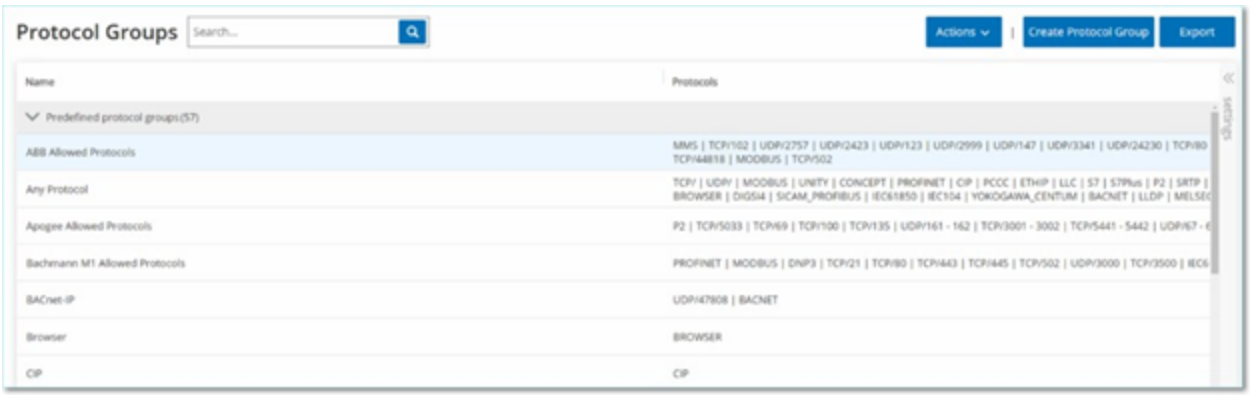
Groupes de protocoles

Il s'agit des protocoles utilisés pour les communications entre les assets du réseau. Les groupes de protocoles sont une condition des politiques réseau. Ils définissent également les protocoles utilisés entre des assets donnés qui déclenchent une politique.

OT Security est livré avec un ensemble de groupes de protocoles prédéfinis qui comprennent des protocoles associés. Ces groupes sont disponibles pour une utilisation dans les politiques. Vous pouvez modifier ou supprimer ces groupes. Les protocoles peuvent être regroupés en fonction des protocoles autorisés par un fournisseur spécifique.

Par exemple, les protocoles autorisés par Schneider incluent : 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). Ils peuvent être également regroupés par type de protocole (Modbus, PROFINET, CIP, etc.). Vous pouvez également créer vos propres groupes de protocole.

Afficher les groupes de protocoles



L'écran **Groupes de protocoles** affiche tous les groupes de protocoles actuellement configurés dans le système. L'onglet **Prédéfinis** affiche les groupes prédéfinis dans le système. Vous ne pouvez pas modifier ni supprimer ces groupes, mais vous pouvez les dupliquer. L'onglet **Définis par l'utilisateur** contient les groupes personnalisés que vous créez. Vous pouvez modifier, dupliquer ou supprimer ces groupes.

Le tableau Groupes de protocoles affiche les détails suivants :

Paramètre	Description
Nom	Nom utilisé pour identifier le groupe.
Protocoles	Liste des protocoles inclus dans le groupe. **Remarque :** s'il n'y a pas assez de place pour afficher tous les membres du groupe, cliquez sur **Actions** > **Afficher** > onglet **Membres**.
Utilisé dans les politiques	Affiche le nom de chaque politique qui utilise ce groupe de protocoles dans sa configuration. **Remarque :** pour afficher plus de détails sur les politiques dans lesquelles ce groupe est utilisé, cliquez sur **Actions** > **Afficher** > onglet **Utilisé dans les politiques**.

Créer des groupes de protocoles

Vous pouvez créer des groupes de protocoles personnalisés pour les utiliser dans la configuration de politiques. Le regroupement de protocoles similaires permet de créer des politiques qui définissent les protocoles suspects.

Pour créer un groupe de protocoles :

1. Accédez à **Groupes** > **Groupes de protocoles**.
2. Cliquez sur **Créer un groupe de protocoles**.

   Le panneau **Créer un groupe de protocoles** apparaît.

3. Dans la zone **Nom**, saisissez le nom du groupe.
4. Dans la zone déroulante **Protocoles**, sélectionnez un type de protocole.
5. Si le protocole sélectionné est TCP ou UDP, saisissez un numéro de port ou une plage de ports dans la zone **Port**.

   Pour les autres types de protocoles, vous n'avez pas à saisir de valeur dans la zone **Port**.
6. Pour ajouter des protocoles au groupe :
   a. Cliquez sur **+ Ajouter un protocole**.

      Une nouvelle zone **Sélection** apparaît.

   b. Remplissez la nouvelle zone **Sélection** en suivant les étapes 4 et 5.

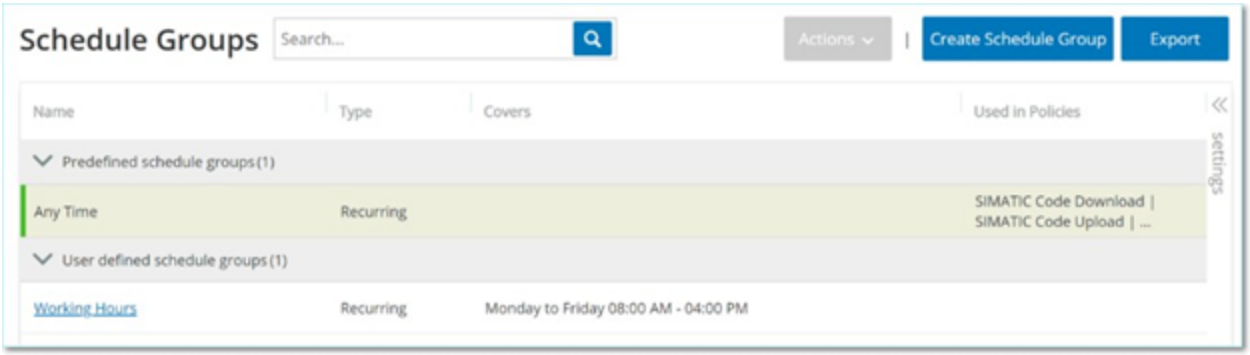
7. Cliquez sur **Créer**.

   OT Security crée le groupe de protocoles et l'affiche dans la liste des groupes de protocoles. Vous pouvez désormais utiliser ce groupe lors de la configuration des politiques.

Groupe de planification

Un groupe de planification définit une ou plusieurs plages temporelles dont les caractéristiques particulières rendent les activités qui se produisent pendant cette période dignes d'intérêt. Par exemple, certaines activités sont censées avoir lieu pendant les heures ouvrées, tandis que d'autres activités sont censées avoir lieu pendant les temps d'arrêt.

Afficher les groupes de planification



L'écran **Groupes de planification** affiche tous les groupes de planification actuellement configurés dans le système. L'onglet **Groupes de planification prédéfinis** affiche les groupes prédéfinis dans le système. Vous ne pouvez pas modifier, dupliquer ou supprimer ces groupes. L'onglet **Groupes de planification définis par l'utilisateur** contient les groupes personnalisés que vous avez créés. Vous pouvez modifier, dupliquer ou supprimer ces groupes.

Le tableau Groupes de planification affiche les détails suivants :

Paramètre	Description
Nom	Nom utilisé pour identifier le groupe.
Type	Type de groupe. Les options sont : • **Function** (Fonction) – Un groupe de planification prédéfini qui a été

	créé pour remplir une fonction donnée. • **Recurring** (Récurrent) – Pour une planification quotidienne ou hebdomadaire. Par exemple, une planification « Heures ouvrées » peut être définie du lundi au vendredi de 9h00 à 17h00. • **Interval** (Intervalle) – Un groupe de planification pour une date ou une plage de dates spécifiques. Par exemple, une planification « Rénovation d'usine » peut être définie par la période du 1er juin au 15 août.
Couverture	Un résumé des paramètres de planification. **Remarque :** s'il n'y a pas assez de place pour afficher tous les membres du groupe, cliquez sur **Actions** > **Afficher** > onglet **Membres**.
Utilisé dans les politiques	Affiche l'ID de chaque politique qui utilise le groupe de planification dans sa configuration. **Remarque :** pour afficher plus de détails sur les politiques dans lesquelles ce groupe est utilisé, cliquez sur **Actions** > **Afficher** > onglet **Utilisé dans les politiques**.

Créer des groupes de planification

Vous pouvez créer des groupes de planification personnalisés à utiliser dans la configuration des politiques. Définissez une plage temporelle ou un groupe de plages temporelles avec des caractéristiques communes qui mettent en évidence les événements qui se produisent pendant cette période.

Il existe deux types de groupes de planification :

- **Recurring** (Récurrent) – Pour une planification hebdomadaire. Par exemple, une planification « Heures ouvrées » peut être définie du lundi au vendredi de 9h00 à 17h00.
- **Once** (Ponctuel) – Planifications pour une date ou une plage de dates spécifiques. Par exemple, une planification « Rénovation d'usine » peut être définie par la période du 1er juin au 15 août. Il existe différentes procédures pour créer chaque type de groupe de planification.

Il existe différentes procédures pour créer chaque type de groupe de planification.

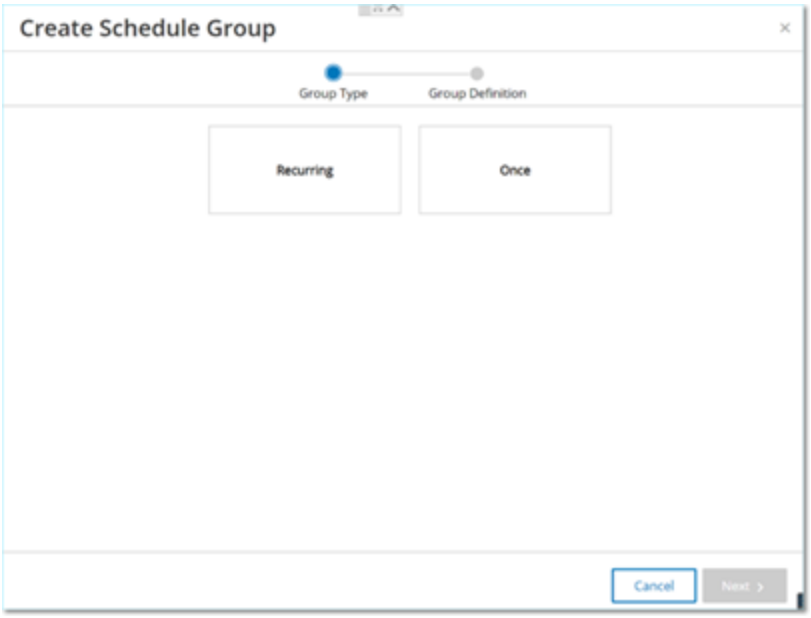
Pour créer un groupe de planification de type Récurrent :

1. Accédez à **Groupes** > **Groupes de planification**.

   La page **Groupes de planification** apparaît.

2. Cliquez sur **Créer un groupe de planification**.

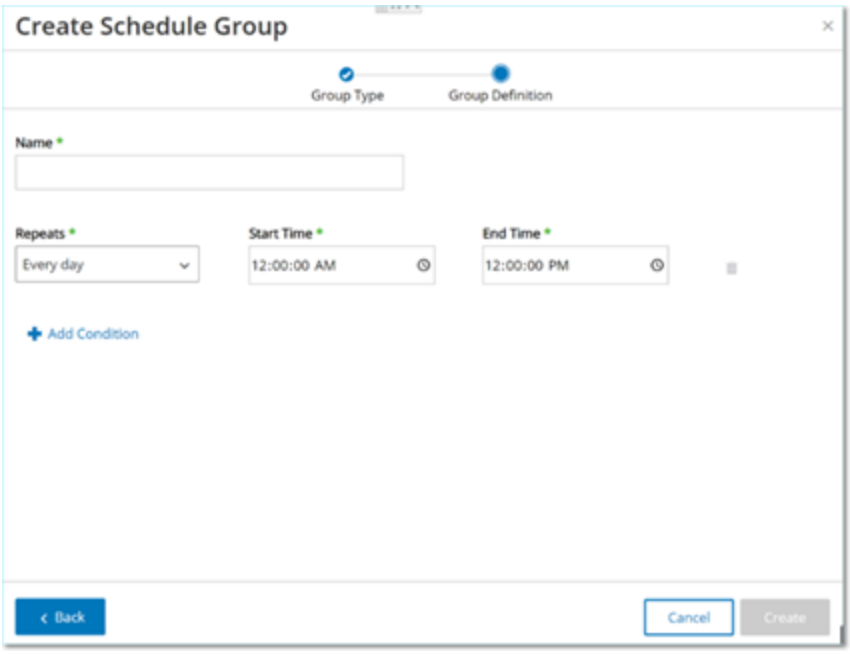
   Le panneau **Créer des groupes de planification** apparaît.



3. Cliquez sur **Récurrent**.

4. Cliquez sur **Suivant**.

   Les paramètres de définition d'un groupe de planification récurrent apparaissent.



5. Dans la zone **Nom**, saisissez le nom du groupe.
6. Dans la zone **Répéter**, sélectionnez les jours de la semaine à inclure dans le groupe de planification.

   Les options sont : Tous les jours, Du lundi au vendredi ou un jour spécifique de la semaine.

   > **Remarque :** pour inclure des jours spécifiques de la semaine, par exemple, le lundi et le mercredi, vous devez ajouter une condition distincte pour chaque jour.

7. Dans la zone **Heure de début**, saisissez le début de la plage temporelle (sous la forme heure, minutes, secondes) incluse dans le groupe de planification.
8. Dans la zone **Heure de fin**, saisissez la fin de la plage temporelle (sous la forme heures, minutes, secondes) incluse dans le groupe de planification.
9. Pour ajouter des conditions (c'est-à-dire des plages temporelles) au groupe de planification :
   a. Cliquez sur **+ Ajouter une condition**.

      Une nouvelle ligne de paramètres de sélection de planification apparaît.

   b. Remplissez les champs comme décrit ci-dessus aux étapes 5 à 7.
10. Cliquez sur **Créer**.

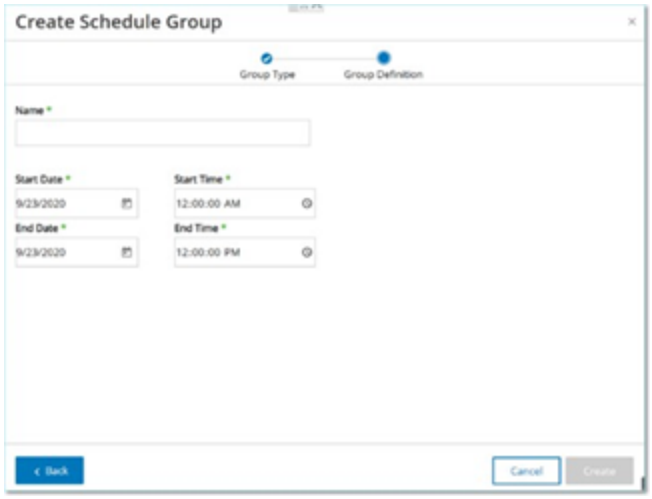
OT Security crée le groupe de planification et l'affiche dans la liste des groupes de planification. Vous pouvez désormais utiliser ce groupe lors de la configuration des politiques.

Pour créer un groupe de planification ponctuel :

1. Accédez à **Groupes** > **Groupes de planification**.
2. Cliquez sur **Créer un groupe de planification**.

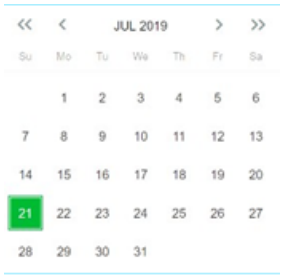
   La page **Créer un groupe de planification** apparaît.
3. Sélectionnez **Plage temporelle**.
4. Cliquez sur **Suivant**.

   Les paramètres de définition d'un groupe de planification pour une page temporelle apparaissent.



5. Dans la zone **Nom**, saisissez le nom du groupe.
6. Dans la zone **Date de début**, cliquez sur l'icône du calendrier .

   Une fenêtre de calendrier apparaît.



7. Sélectionnez la date à laquelle le groupe de planification commence La date actuelle est la valeur par défaut.
8. Dans la zone **Heure de début**, saisissez le début de la plage temporelle (sous la forme heure, minutes, secondes) incluse dans le groupe de planification.
9. Dans la zone **Date de fin**, cliquez sur l'icône du calendrier .

   Une fenêtre de calendrier apparaît.
10. Sélectionnez la date à laquelle le groupe de planification prend fin (par défaut : la date actuelle).
11. Dans la zone **Heure de fin**, saisissez la fin de la plage temporelle (sous la forme heures, minutes, secondes) incluse dans le groupe de planification.
12. Cliquez sur **Créer**.

    OT Security crée le groupe de planification et l'affiche dans la liste des groupes de planification. Vous pouvez désormais utiliser ce groupe lors de la configuration des politiques.

Groupes de tags

Les tags sont des paramètres dans les contrôleurs qui contiennent des données opérationnelles spécifiques. Les groupes de tags sont utilisés comme condition pour les **politiques d'événements SCADA**. Le regroupement de tags aux rôles similaires permet de créer des politiques qui détectent les modifications suspectes du paramètre spécifié. Par exemple, en regroupant des tags qui contrôlent la température des fours, vous pouvez créer une politique qui détecte les changements de température qui pourraient être nocifs pour les fours.

Afficher les groupes de tags

La page **Groupes de tags** affiche tous les groupes de tags actuellement configurés dans le système.

Le tableau Groupes de tags affiche les détails suivants :

Paramètre	Description
Nom	Nom utilisé pour identifier le groupe.
Type	Le type de données du tag. Les valeurs possibles sont : Bool, Dint, Float, Int, Long, Short, Unknown (pour les tags d'un type que OT Security n'a pas pu identifier) ou Any Type (qui peut inclure des tags de différents types)
Contrôleur	Le contrôleur sur lequel le tag est surveillé.
Tags	Affiche chaque tag inclus dans le groupe ainsi que le nom du contrôleur dans lequel il se trouve. **Remarque :** s'il n'y a pas assez de place pour afficher tous les tags, cliquez sur **Actions** > **Afficher** > onglet **Membres**.
Utilisé dans les politiques	Affiche l'ID de chaque politique qui utilise le groupe de planification dans sa configuration. **Remarque :** pour afficher plus de détails sur les politiques dans lesquelles ce groupe est utilisé, cliquez sur **Actions** > **Afficher** > onglet **Utilisé dans les politiques**.

Vous pouvez afficher, modifier, dupliquer ou supprimer un groupe existant. Voir Actions sur les groupes.

Créer des groupes de tags

Vous pouvez créer des groupes de tags personnalisés à utiliser dans la configuration des politiques. Le regroupement de tags similaires permet de créer des politiques qui s'appliquent à tous les tags du groupe. Sélectionnez les tags de type similaire et nommez-les de manière à représenter l'élément commun des tags.

Vous pouvez également créer des groupes qui incluent des tags de différents types en sélectionnant l'option **Any Type** (Tout type). Dans ce cas, les politiques appliquées à ce groupe peuvent uniquement détecter les modifications apportées à **N'importe quelle valeur** pour les tags spécifiés, mais elles ne peuvent pas être définies pour détecter des valeurs spécifiques.

Vous pouvez modifier, dupliquer ou supprimer les groupes de tags.

Pour créer un groupe de tags :

1. Accédez à **Groupes** > **Groupes de tags**.
2. Cliquez sur **Créer un groupe de tags**.

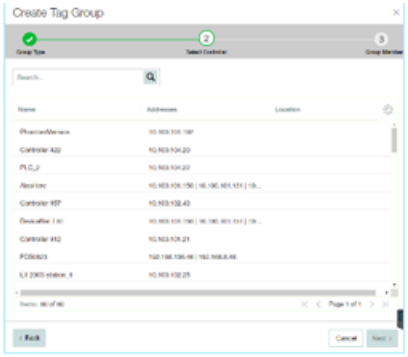
   Le panneau **Créer un groupe de tags** apparaît.

3. Sélectionnez un type de tag.

   Les options sont : Bool, Dint, Float, Int, Long, Short ou Any Type (qui peut inclure des tags de différents types)

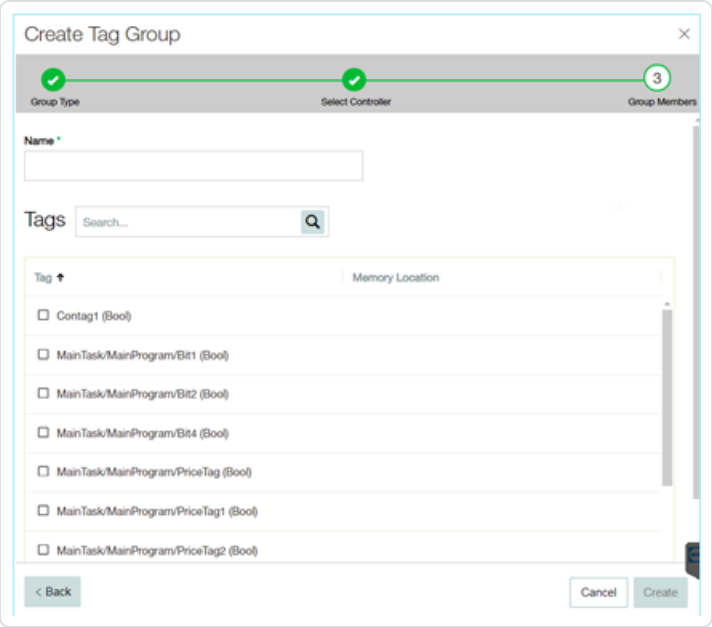
4. Cliquez sur **Suivant**.

   Une liste des contrôleurs de votre réseau apparaît.



5. Sélectionnez un contrôleur pour lequel vous souhaitez inclure des tags dans le groupe.
6. Cliquez sur **Suivant**.

   Une liste de tags du type spécifié sur le contrôleur spécifié apparaît.



7. Dans la zone **Nom**, saisissez le nom du groupe.
8. Cochez la case à côté des tags que vous souhaitez inclure dans le groupe.
9. Cliquez sur **Créer**.

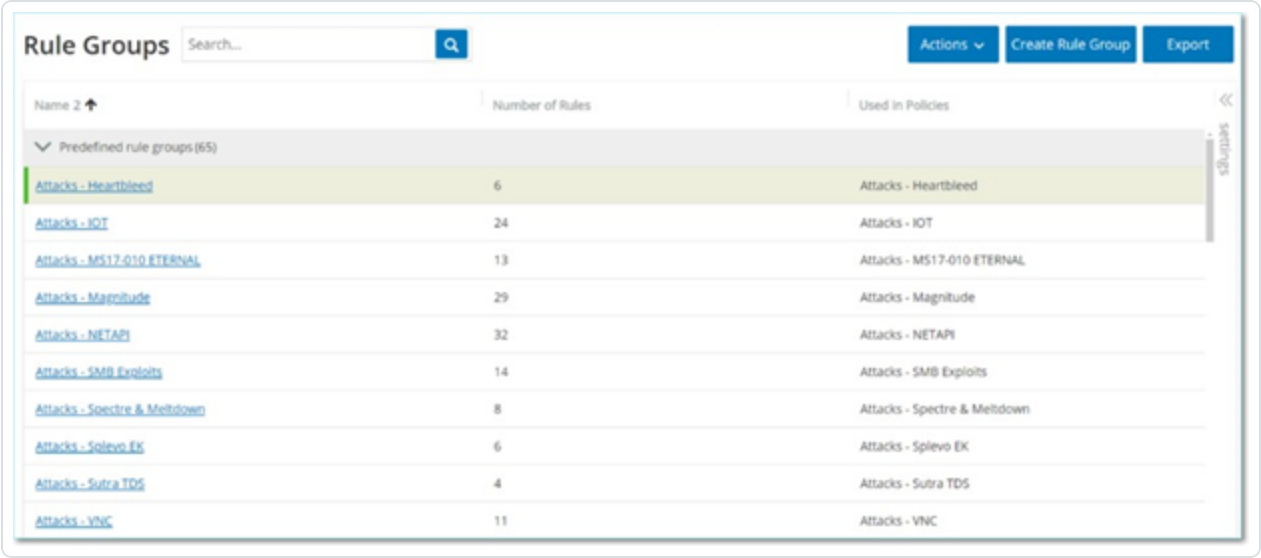
   OT Security crée le groupe de tags et l'affiche dans la liste des groupes de tags. Vous pouvez désormais utiliser ce groupe lors de la configuration des politiques d'événement SCADA.

Groupes de règles

Les groupes de règles sont constitués d'un ensemble de règles associées identifiées par leur ID de signature Suricata (SID). Ces groupes sont utilisés comme conditions pour définir des politiques de détection d'intrusion.

OT Security fournit un ensemble de groupes prédéfinis de vulnérabilités associées. De plus, vous pouvez sélectionner des règles spécifiques dans notre référentiel de vulnérabilités afin de créer vos propres groupes de règles personnalisés.

Afficher les groupes de règles



L'écran **Groupes de règles** affiche tous les groupes de règles actuellement configurés dans le système. L'onglet Prédéfinis affiche les groupes prédéfinis dans le système. Vous ne pouvez pas modifier, dupliquer ou supprimer ces groupes. L'onglet **Définis par l'utilisateur** contient les groupes personnalisés créés par l'utilisateur. Vous pouvez modifier, dupliquer ou supprimer ces groupes.

Le tableau Groupes de règles affiche les détails suivants :

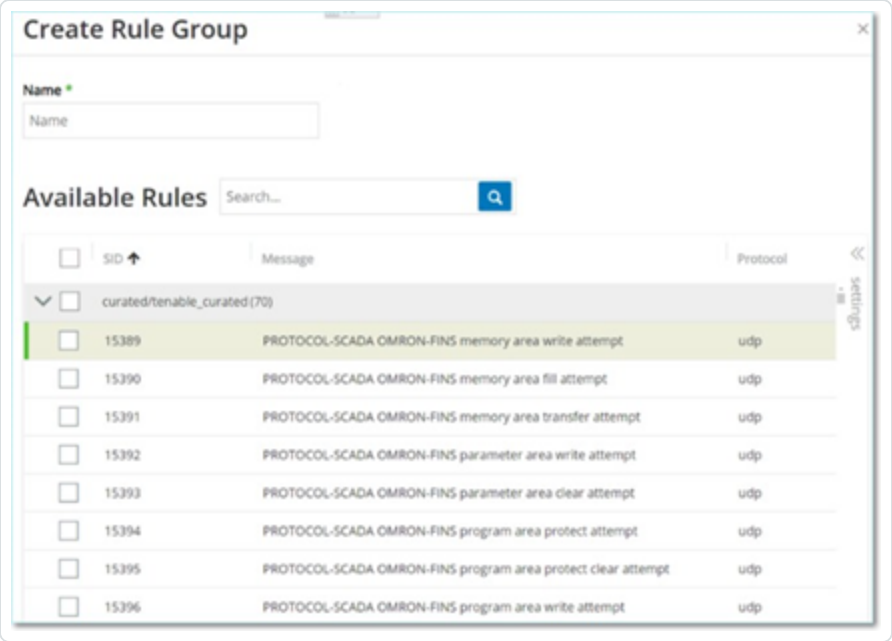
Paramètre	Description
Nom	Nom utilisé pour identifier le groupe.
Nombre de règles	Le nombre de règles (SID) qui composent ce groupe de règles.
Utilisé dans les politiques	Affiche l'identifiant de chaque politique qui utilise ce groupe de règles dans sa configuration. **Remarque :** pour afficher plus de détails sur les politiques dans lesquelles ce groupe est utilisé, cliquez sur **Actions** > **Afficher** > onglet **Utilisé dans les politiques**.

Créer des groupes de règles

Pour créer un groupe de règles :

1. Accédez à **Groupes** > **Groupes de règles**.
2. Cliquez sur **Créer un groupe de règles**.

   Le panneau **Créer un groupe de règles** apparaît.



3. Dans la zone **Nom**, saisissez le nom du groupe.
4. Dans la section **Règles disponibles**, cochez la case à côté des règles que vous souhaitez inclure dans le groupe.

   > **Remarque :** utilisez la zone de recherche pour trouver les règles souhaitées.

5. Cliquez sur **Créer**.

   OT Security crée le groupe de règles et l'affiche dans la liste des groupes de règles. Vous pouvez désormais utiliser ce groupe lors de la configuration des politiques de détection d'intrusion.

Actions sur les groupes

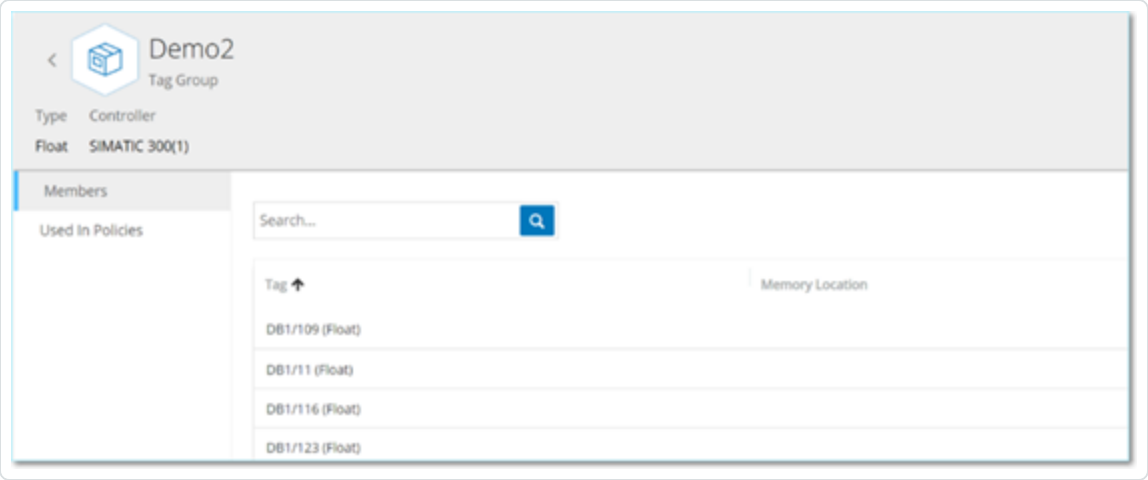
Lorsque vous sélectionnez un groupe dans n'importe quel écran de groupe, utilisez le menu **Actions** en haut de l'écran pour effectuer les actions suivantes :

- **Afficher** – Affiche des détails sur le groupe sélectionné, tels que les entités incluses dans le groupe et les politiques qui utilisent le groupe comme condition. Voir Afficher les détails d'un groupe
- **Modifier** – Modifie les détails du groupe. Voir Modifier un groupe
- **Dupliquer** – Crée un groupe avec une configuration similaire au groupe spécifié. Voir Dupliquer un groupe
- **Supprimer** – Supprime le groupe du système. Voir Supprimer un groupe

> **Remarque :** vous ne pouvez pas modifier ni supprimer de groupes prédéfinis. Certains groupes prédéfinis ne peuvent pas non plus être dupliqués. Le menu **Actions** est également accessible en effectuant un clic droit sur un groupe.

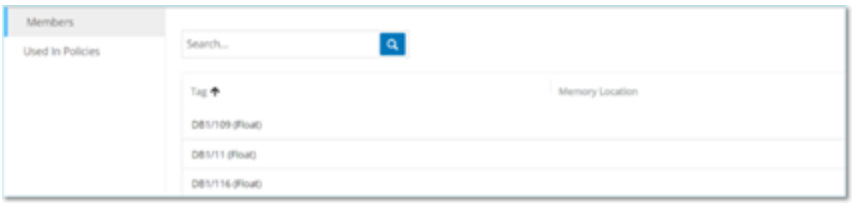
Afficher les détails d'un groupe

Lorsque vous sélectionnez un groupe et cliquez sur **Actions** > **Afficher**, l'écran Détails du groupe apparaît pour le groupe sélectionné.



L'écran **Détails du groupe** comporte une barre d'en-tête qui affiche le nom et le type du groupe. Il comporte deux onglets :

- **Membres** – Affiche une liste de tous les membres du groupe.

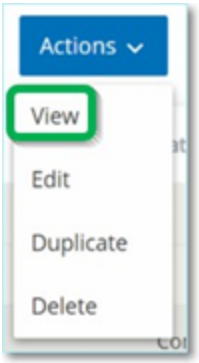


- **Utilisé dans les politiques** – Affiche une liste pour chaque politique pour laquelle le groupe spécifié est utilisé comme condition. Un curseur permet d'activer/désactiver la politique dans les différentes listes. Pour plus d'informations, voir Afficher les politiques.

Pour afficher les détails d'un groupe :

1. Dans **Groupes**, sélectionnez le type de groupe souhaité.
2. Effectuez l'une des actions suivantes :
   - Cliquez sur **Actions**.
   - Effectuez un clic droit sur le groupe requis.

     Un menu apparaît.
3. Sélectionnez **Afficher**.



   L'écran des détails du groupe apparaît.

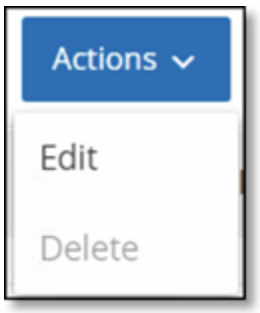
Modifier un groupe

Vous pouvez modifier les détails d'un groupe existant.

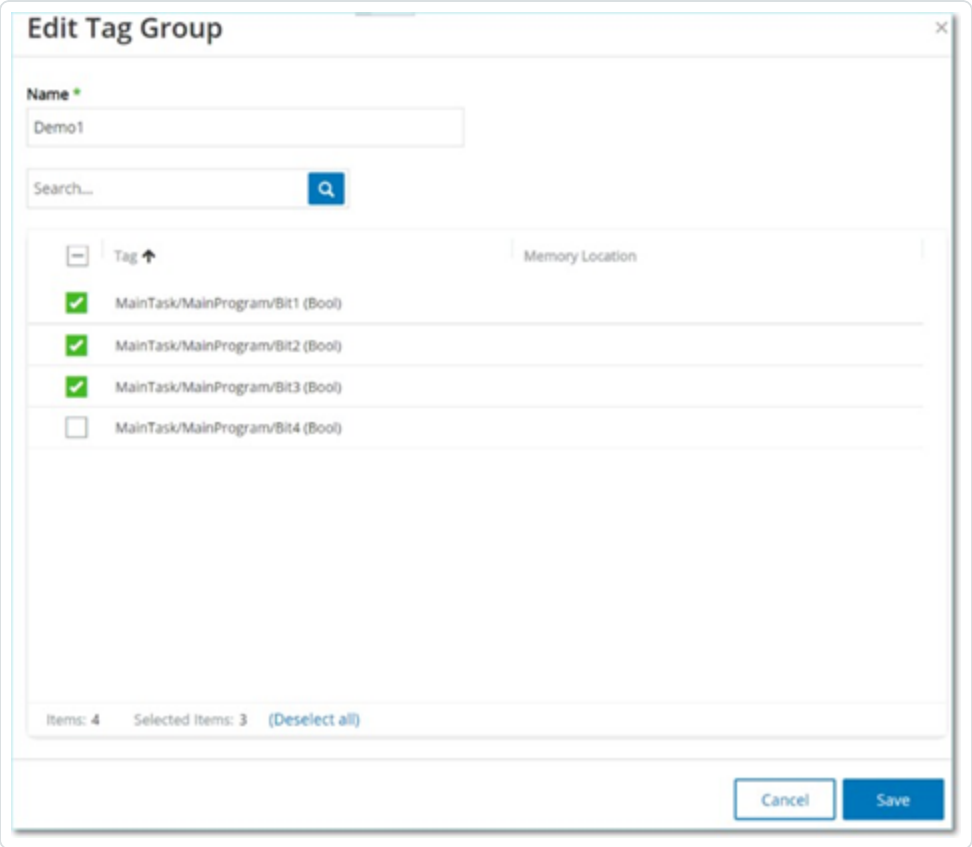
Pour afficher les détails d'un groupe :

1. Sous **Groupes**, sélectionnez le type de groupe souhaité.
2. Effectuez l'une des actions suivantes :
    - Cliquez sur **Actions**.
    - Effectuez un clic droit sur le groupe requis.

      Un menu apparaît.
3. Sélectionnez **Modifier**.



4. La fenêtre **Modifier le groupe** apparaît et affiche les paramètres pertinents pour le type de groupe spécifié.



5. Modifiez le groupe selon les besoins.
6. Cliquez sur **Enregistrer**.

   OT Security enregistre le groupe avec les nouveaux paramètres.

Dupliquer un groupe

Pour créer un groupe avec des paramètres similaires à un groupe existant, vous pouvez dupliquer le groupe existant. Lorsque vous dupliquez un groupe, le nouveau groupe est enregistré sous un nouveau nom, en plus du groupe d'origine.

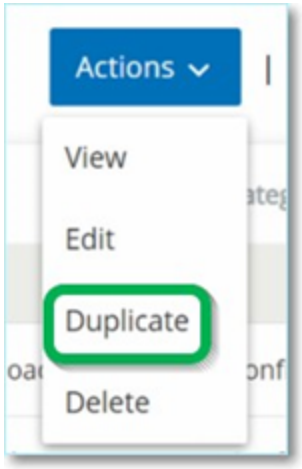
Pour dupliquer un groupe :

1. Sous **Groupes**, sélectionnez le type de groupe souhaité.
2. Sélectionnez le groupe existant sur lequel vous souhaitez baser le nouveau groupe.
3. Effectuez l'une des actions suivantes :

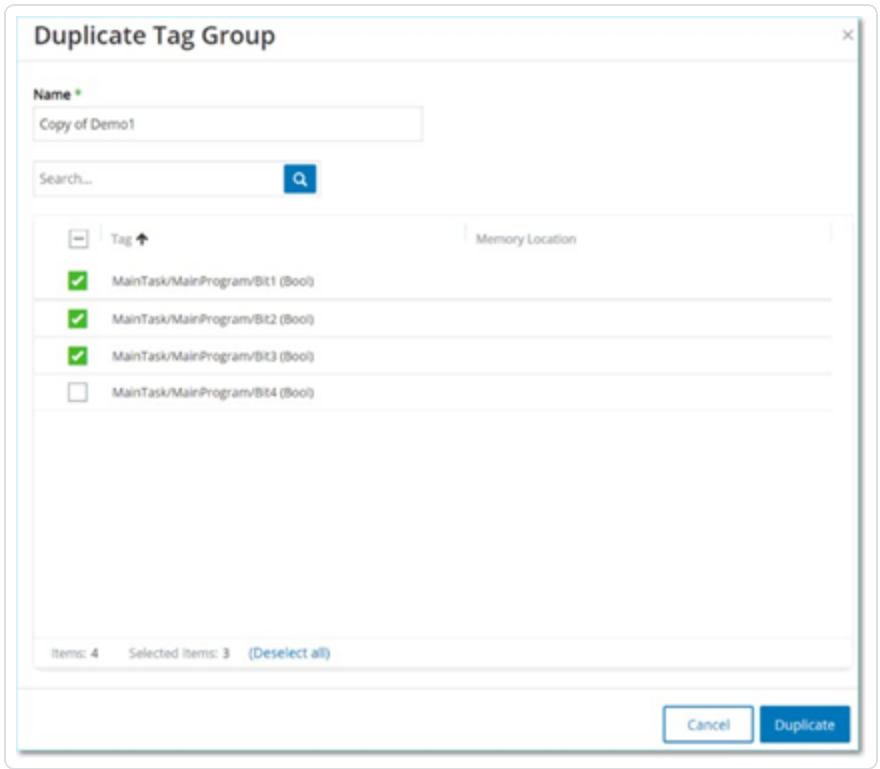
- Cliquez sur **Actions**.
- Effectuez un clic droit sur le groupe requis.

  Un menu apparaît.

4. Sélectionnez **Dupliquer**.



La fenêtre **Dupliquer le groupe** apparaît et affiche les paramètres pertinents pour le type de groupe spécifié.



5. Dans la zone **Nom**, saisissez le nom du groupe. Par défaut, le nouveau groupe est nommé « Copie de » suivi du nom du groupe d'origine.
6. Apportez les modifications souhaitées aux paramètres du groupe.
7. Cliquez sur **Dupliquer**.

   OT Security enregistre le nouveau groupe avec les nouveaux paramètres, en plus du groupe existant.

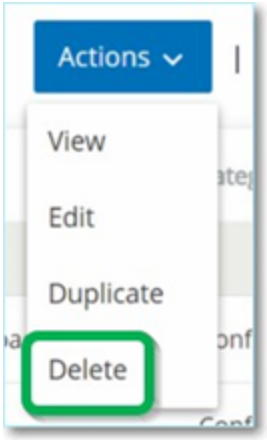
Supprimer un groupe

Vous pouvez supprimer des groupes définis par l'utilisateur, mais pas des groupes prédéfinis. Vous ne pouvez pas supprimer une politique définie par l'utilisateur si elle est utilisée comme condition pour des politiques.

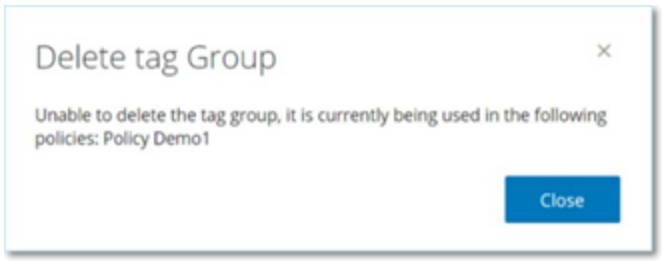
Pour supprimer un groupe :

1. Sous **Groupes**, sélectionnez le type de groupe souhaité.
2. Sélectionnez le groupe que vous souhaitez supprimer.
3. Effectuez l'une des actions suivantes :
   - Cliquez sur **Actions**.
   - Effectuez un clic droit sur le groupe requis.

     Un menu apparaît.
4. Sélectionnez **Supprimer**.



Une fenêtre de confirmation apparaît.



5. Cliquez sur **Supprimer**.

   OT Security supprime définitivement le groupe du système.

Paramètres locaux

La section **Paramètres locaux** dans OT Security comprend la plupart des pages de configuration pour OT Security. Les pages suivantes sont disponibles sous **Paramètres locaux** :

Requêtes actives – Activez/désactivez les fonctions de requête et ajustez leur fréquence et leurs paramètres. Voir Requêtes actives.

Capteurs – Affichez et gérez les capteurs, approuvez ou supprimez les demandes d'appairage entrantes des capteurs et configurez les requêtes actives effectuées par les capteurs. Voir Capteurs.

Configuration système

- **Appareil** – Affichez et modifiez les détails de l'appareil et les informations réseau. Par exemple, l'heure système et la déconnexion automatique (c'est-à-dire le délai d'inactivité).

  > **Remarque** : vous pouvez configurer les serveurs DNS dans Tenable Core. Pour plus d'informations, voir Manually Configure a Static IP Address (Configurer manuellement une adresse IP statique) dans le Guide de l'utilisateur de Tenable Core + Tenable OT Security.

- **Configuration des ports** – Affichez la configuration des ports de l'appareil. Pour plus d'informations sur la configuration des ports, voir Appareil.
- Mises à jour **– Effectuez des mises à jour des plug-ins soit automatiquement, soit manuellement via le cloud, soit hors ligne.**
- **Certificat** – Affichez les informations sur votre certificat HTTPS et assurez une connexion sécurisée en générant un nouveau certificat HTTPS dans le système ou en important le vôtre. Voir Configuration système.
- **Clés API** – Générez des clés API pour permettre aux applications tierces d'accéder à OT Security via l'API. Tous les utilisateurs peuvent créer des clés API. La clé API a les mêmes autorisations que l'utilisateur qui l'a créée, en fonction de son rôle. Une clé API est affichée une seule fois, lorsqu'elle est générée pour la première fois ; vous devez l'enregistrer dans un emplacement sécurisé pour une utilisation ultérieure. Voir Générer des clés API.
- **Licence** – Affichez, mettez à jour et renouvelez votre licence. Voir Licence.

Configuration de l'environnement

- **Paramètres de l'asset**
  - **Réseau surveillé** – Affichez et modifiez l'agrégation des plages d'adresses IP dans lesquelles le système classe les assets. Voir Réseaux surveillés.
  - **Mettre à jour les détails d'un asset à l'aide d'un fichier CSV** – Mettez à jour les détails de vos assets à l'aide d'un modèle CSV.
  - **Ajouter des assets manuellement** – Ajoutez de nouveaux assets à votre liste d'assets à l'aide d'un modèle CSV. Voir Ajouter des assets manuellement.

  Remarque : le nombre maximal de plages d'adresses IP pouvant être envoyées au Tenable Network Monitor est 128 ; Tenable vous recommande donc de ne pas dépasser cette limite. Outre les plages d'adresses IP spécifiées, tout hôte au sein des sous-réseaux de la plateforme OT Security ou tout appareil exécutant une activité sera classé comme un asset.

  - **Assets masqués** – Affiche une liste des assets masqués dans le système. Il s'agit des assets supprimés des listes d'assets. Voir Inventaire. Vous pouvez restaurer les assets masqués à partir de cette page.
  - **Champs personnalisés** – Vous pouvez créer des champs personnalisés pour étiqueter vos assets avec des informations pertinentes. Le champ personnalisé peut être un lien vers une ressource externe.
  - **Clusters d'événements** – Vous permet de regrouper plusieurs événements similaires qui se produisent dans une plage temporelle désignée afin de les surveiller. Voir Groupes d'événements.
  - **Lecteur PCAP** – Vous permet d'importer un fichier PCAP contenant une activité réseau enregistrée et de le « lire » sur OT Security, en chargeant les données dans votre système. Voir Lecteur PCAP.
- **Utilisateurs et rôles** – Affichez, modifiez et exportez des informations sur tous les comptes utilisateur.
  - **Paramètres de l'utilisateur** – Affichez et modifiez les informations sur l'utilisateur actuellement connecté au système (nom complet, nom d'utilisateur et mot de passe) et modifiez la langue utilisée dans l'interface utilisateur (anglais, japonais, chinois, français ou allemand).

- **Utilisateurs locaux** – Un utilisateur administrateur peut créer des comptes utilisateur locaux pour des utilisateurs spécifiques et attribuer un rôle au compte. Voir Gestion des utilisateurs.
- **Groupes d'utilisateurs** – Un utilisateur administrateur peut afficher, modifier, ajouter et supprimer des groupes d'utilisateurs. Voir Gestion des utilisateurs.
- **Serveurs d'authentification** – Les informations d'authentification de l'utilisateur peuvent éventuellement être attribuées à l'aide d'un serveur LDAP tel qu'Active Directory. Dans ce cas, les privilèges utilisateurs sont gérés sur l'Active Directory. Voir Gestion des utilisateurs.

- **Intégrations** – Configurez l'intégration avec d'autres plates-formes. OT Security prend actuellement en charge l'intégration avec le pare-feu Palo Alto Networks nouvelle génération (NGFW) et Aruba ClearPass, ainsi qu'avec d'autres produits Tenable (Tenable Security Center et Tenable Vulnerability Management). Voir Intégrations.
- **Serveurs** – Affichez, créez et modifiez les serveurs configurés dans votre système. Des écrans séparés sont affichés pour :
  - **Serveurs SMTP** – Les serveurs SMTP permettent d'envoyer des notifications d'événement par e-mail.
  - **Serveurs Syslog** – Les serveurs Syslog permettent aux journaux d'événements d'être enregistrés sur un SIEM externe.
  - **Pare-feu FortiGate** – L'intégration OT Security-FortiGate vous permet d'envoyer des suggestions de politique de pare-feu à un pare-feu FortiGate en fonction des événements réseau de OT Security.
- **Actions système** – Affiche un sous-menu des activités du système. Le sous-menu comprend les options suivantes :
  - **Sauvegarde système** —À partir de la version 3.18, vous pouvez effectuer une sauvegarde et restaurer votre OT Security en utilisant la page **Backup/ Restore** (Sauvegarder/ Restaurer) dans Tenable Core. Pour plus d'informations, voir Application Data Backup and Restore (Sauvegarde et restauration des données d'application). Pour restaurer à l'aide de la CLI, voir Restaurer la sauvegarde à l'aide de la CLI.

- **Exporter les paramètres** – Exporte les paramètres de configuration de la plateforme OT Security sous forme de fichier `.ndg` vers l'ordinateur local. Cela sert de sauvegarde en cas de réinitialisation du système ou en cas d'importation vers une nouvelle plateforme OT Security.
- **Importer les paramètres** – Importe les paramètres de configuration de la plateforme OT Security enregistrés sous forme de fichier `.ndg` sur l'ordinateur local.
- **Télécharger les données de diagnostic** – Crée un fichier avec des données de diagnostic sur la plateforme OT Security et le stocke sur l'ordinateur local.
- **Redémarrer** – Redémarre la plateforme OT Security. Ceci est nécessaire pour activer certains changements de configuration.
- **Désactiver** – Désactive toutes les activités de surveillance. Vous pouvez réactiver les activités de surveillance à tout moment.
- **Arrêter** – Arrête la plateforme OT Security. Pour mettre l'appliance OT Security sous tension, appuyez sur le bouton d'alimentation.
- **Réinitialisation d'usine** – Rétablit tous les paramètres d'usine par défaut.

  > **Attention** : cette opération est irréversible et toutes les données du système sont perdues.

- **Journal système** – Affiche le journal de tous les événements système qui se sont produits dans le système. Par exemple, Politique activée, Politique modifiée, Événement résolu, etc. Vous pouvez exporter le journal dans un fichier CSV ou l'envoyer à un serveur Syslog. Voir Journal système.

Capteurs

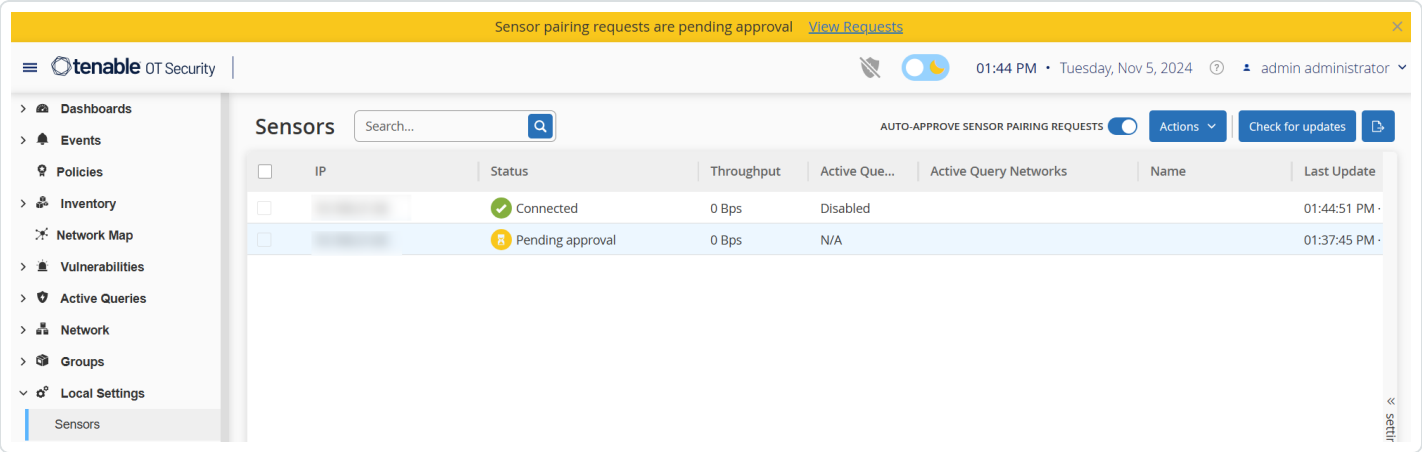
Une fois que les capteurs sont appairés à l'aide de l'interface utilisateur Tenable Core, vous pouvez approuver les nouveaux appairages et afficher et gérer les capteurs à l'aide des fonctions **Modifier**, **Mettre en pause** et **Supprimer** du menu **Actions**. Vous pouvez également choisir d'activer l'approbation automatique des demandes d'appairage des capteurs à l'aide du curseur **Approuver automatiquement les demandes d'appairage des capteurs**.

Remarque : les modèles de capteurs antérieurs à la version 2.214 n'apparaissent pas sur la page Capteurs ICP. Cependant, ils peuvent toujours être utilisés en mode non authentifié.

Remarque : vous pouvez appairer un nombre illimité de capteurs avec ICP, mais le volume de trafic SPAN (analyseur de port commuté) total combiné par appliance est plafonné. Par exemple, si vous disposez de dix capteurs, chacun transmettant entre 10 Mbit/s et 20 Mbit/s, le trafic global ne devra pas dépasser la limite de l'ICP. Pour plus d'informations, voir System and License Requirements (Configuration requise et exigences de licence) dans le Guide de l'utilisateur Tenable Core + OT Security.

Afficher les capteurs

Le tableau Capteurs affiche une liste de tous les capteurs v. 2.214 et ultérieures sur le système.



Le tableau Capteurs contient les détails suivants :

Paramètre	Description
IP	Adresse IPv4 du capteur.
Statut	Statut du capteur : **Connecté**, **Connecté (non authentifié)**, **En attente d'approbation**, **Déconnecté** ou **En pause**. **Important** : une fois appairés, tous les capteurs affichent le statut **En pause**. • Pour modifier le statut des capteurs authentifiés : Dans OT Security, effectuez un clic droit sur les capteurs et activez-les en faisant passer l'état de **En pause** à **Connecté**. • Pour modifier le statut des capteurs non authentifiés :

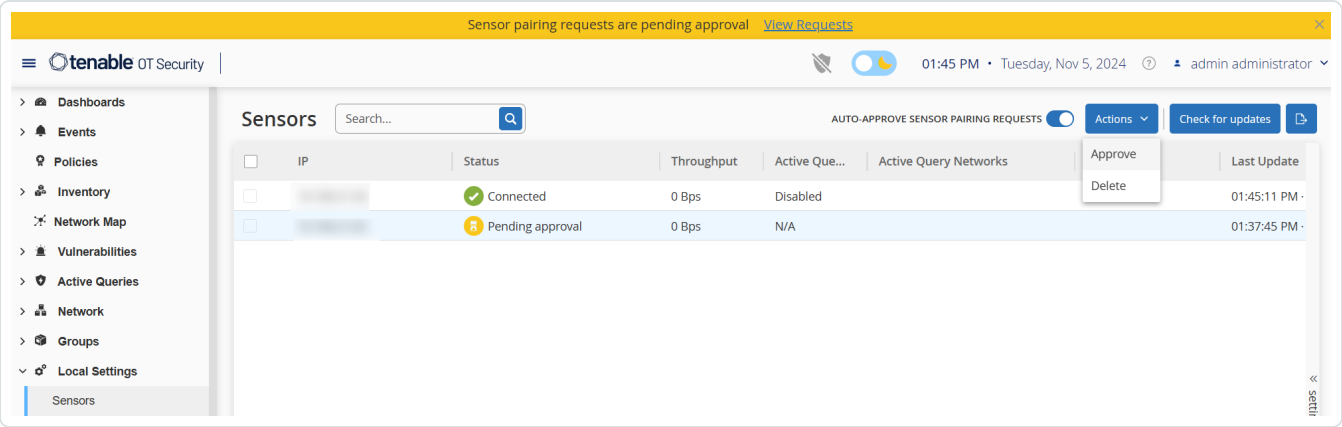
	Dans Tenable Core + Capteur OT Security, accédez à la section **Capteur OT Security** > **Pairing Info (Informations d'appairage)**, puis cliquez sur **Resume Data Transfer (Reprendre le transfert de données)** pour modifier le **statut de la connexion**.
Requêtes actives	La capacité du capteur à envoyer des requêtes actives : **Activé**, **Désactivé**, **N/ A**)
Réseaux de requêtes actives	Les segments réseau auxquels le capteur est affecté.
Nom	Le nom du capteur dans le système.
Dernière mise à jour	La date et l'heure auxquelles les informations du capteur ont été mises à jour pour la dernière fois.
Identifiant du capteur	L'identifiant universel unique (UUID) du capteur, une valeur de 128 bits utilisée pour identifier de manière unique un objet ou une entité sur Internet.
Version	La version du capteur.
Débit	Une mesure de la quantité de données transitant par le capteur (en kilo-octets par seconde).

Approuver manuellement les demandes entrantes d'appairage des capteurs

Si le paramètre **Approuver automatiquement les demandes d'appairage des capteurs** est **désactivé**, les demandes entrantes d'appairage des capteurs doivent être approuvées manuellement avant toute connexion.

Pour approuver manuellement une demande entrante d'appairage des capteurs :

1. Accédez à **Paramètres locaux** > **Capteurs**.
2. Cliquez sur une ligne du tableau dont le statut est **En attente d'approbation**.
3. Cliquez sur **Actions** > **Approuver**, ou effectuez un clic droit et sélectionnez **Approuver** dans le menu contextuel.



Remarque : pour supprimer un capteur, cliquez sur **Actions** > **Supprimer**, ou effectuez un clic droit et sélectionnez **Supprimer**.

Configuration des requêtes actives

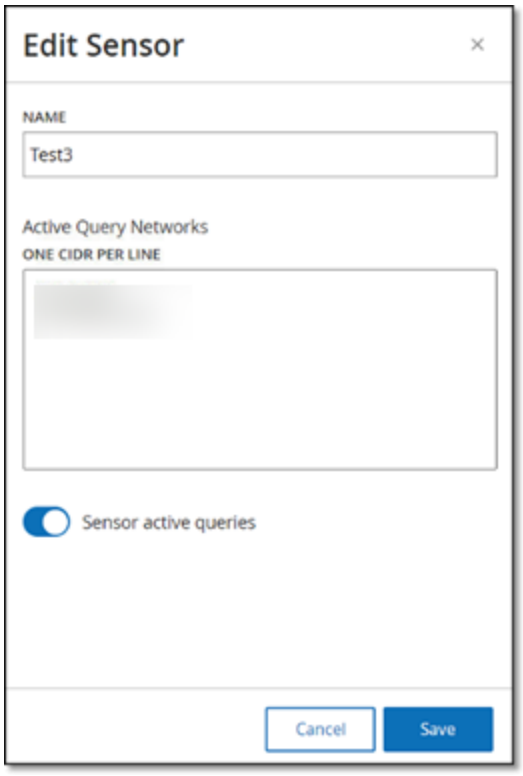
Une fois qu'un capteur est connecté en mode authentifié, il peut être configuré pour effectuer des requêtes actives dans les segments réseau auxquels il est affecté. Vous devez spécifier les segments réseau qu'il doit interroger.

Remarque : les capteurs effectuent une détection de réseau passive sur tous les segments disponibles indépendamment de cette configuration.

Pour configurer les requêtes actives :

1. Sous **Paramètres locaux**, accédez à **Configuration système** > **Capteurs**.
2. Cliquez sur une ligne du tableau dont le statut est **Connecté**.
3. Cliquez sur **Actions** > **Modifier**, ou effectuez un clic droit et sélectionnez **Modifier**.

   Le panneau **Modifier le capteur** apparaît.



4. Pour renommer le capteur, modifiez le texte dans la zone **Nom**.
5. Dans la zone **Réseaux de requêtes actives**, ajoutez ou modifiez les segments de réseau pertinents auxquels le capteur envoie des requêtes actives, en utilisant la notation CIDR et en ajoutant chaque sous-réseau sur une ligne distincte.

   > **Remarque :** les requêtes ne peuvent être effectuées que sur les CIDR inclus dans les plages de réseau surveillées. Veillez à n'ajouter que les CIDR accessibles via ce capteur. L'ajout de CIDR inaccessibles peut interférer avec la capacité de l'ICP à interroger ces segments par d'autres moyens.

6. Cliquez sur le curseur **Requêtes actives du capteur** pour activer les requêtes actives.
7. Cliquez sur **Enregistrer**.

   Le panneau se referme. Dans le tableau **Capteurs**, dans la colonne **Requêtes actives**, les capteurs activés affichent désormais **Activé**.

Mettre à jour les capteurs

À partir de la version 3.16, le Capteur OT Security reçoit les mises à jour logicielles et de sécurité de l'ICP qui le gère. Une fois qu'un capteur est appairé avec l'authentification, il utilise le site pour recevoir toutes les mises à jour nécessaires du système d'exploitation et du logiciel. Il suffit au capteur d'atteindre OT Security pour recevoir les mises à jour du logiciel. OT Security vous permet de mettre à jour tous vos capteurs à partir de la page centralisée **Capteurs**.

Remarque : OT Security utilise le fichier ISO hors ligne pour les mises à jour centralisées. Pour mettre à jour de manière centralisée tous les capteurs authentifiés attachés à une ICP, placez le fichier ISO hors ligne de l'ICP ou du capteur sous `/srv/tenablecore/offlineiso/tenable-offline-updates.iso` sur l'ICP.

Si le capteur nécessite une mise à jour, vous recevez une alerte pendant les opérations suivantes :

- Démarrage.
- Fin d'appairage entre le capteur et l'ICP.
- Vérification régulière.
- Utilisation de l'option **Rechercher les mises à jour**.

Remarque : le capteur doit être appairé à OT Security avec l'authentification pour que la mise à jour à distance soit possible. Pour plus d'informations sur l'appairage, voir Appairage des capteurs avec l'ICP.

Pour mettre à jour le capteur authentifié version 3.16 ou ultérieure avec l'ICP :

1. Accédez à **Paramètres locaux** > **Capteurs**.

   La page **Capteurs** apparaît.

2. Consultez la colonne **Version** pour déterminer si la version est à jour ou nécessite d'être mise à jour.

3. Si la version doit être mise à jour, effectuez l'une des opérations suivantes :

   #### Pour mettre à jour un seul capteur :

   - Effectuez un clic droit sur le capteur et sélectionnez **Mettre à jour**.
   - Cochez la case à côté du capteur puis, dans le menu **Actions**, sélectionnez **Mettre à jour**.

   #### Pour mettre à jour plusieurs capteurs :

- Sélectionnez les capteurs à mettre à jour, puis sélectionnez **Mettre à jour** dans le menu **Actions**.

OT Security met à jour les capteurs sélectionnés.

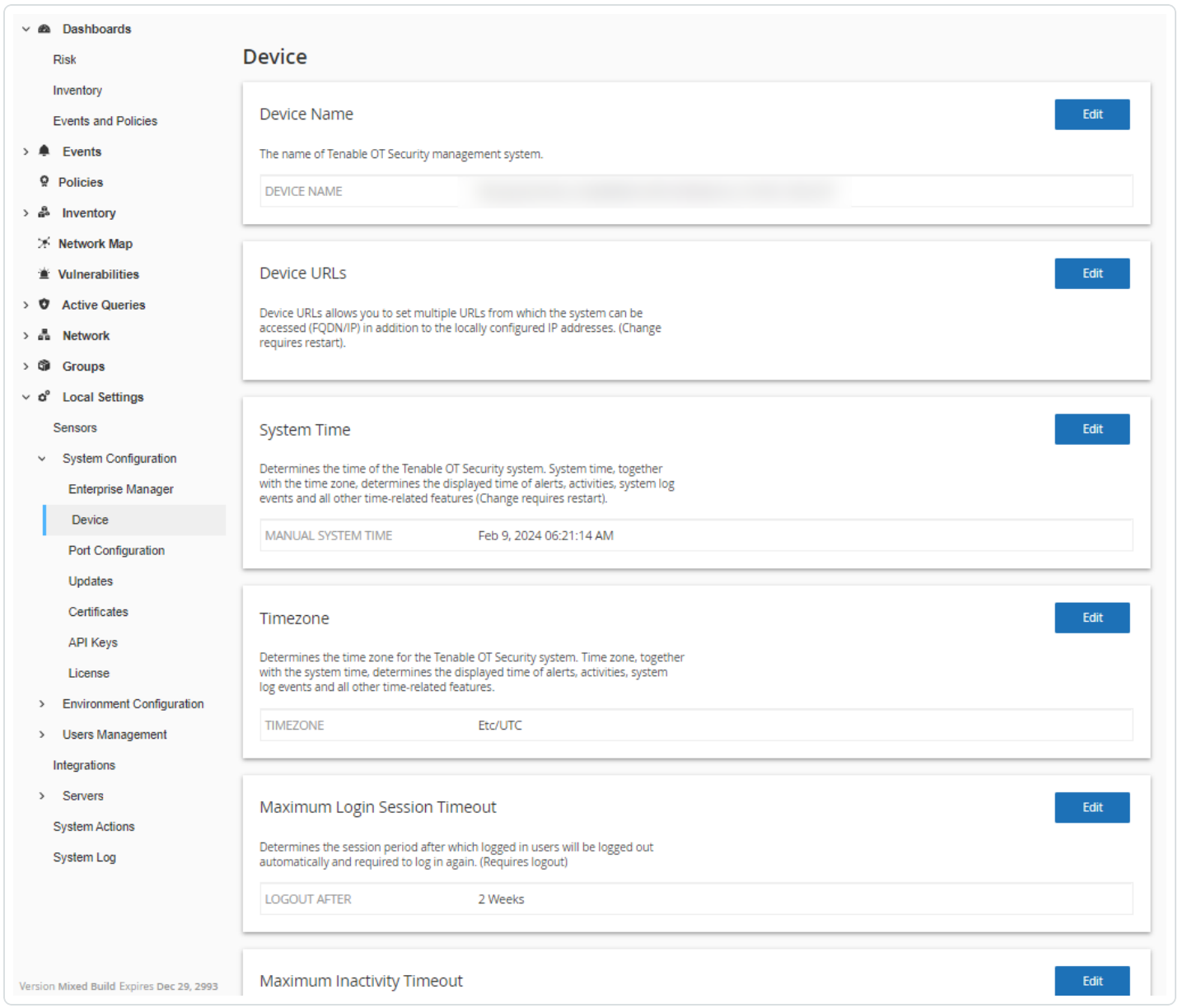
> **Remarque :** pendant la mise à jour, le capteur peut être indisponible.

Configuration système

Les pages **Configuration système** de OT Security vous permettent de configurer automatiquement et d'effectuer manuellement les mises à jour des plug-ins. Elle permettent également d'afficher et de mettre à jour les détails concernant votre appareil, le certificat HTTPS, les clés API et la licence.

Appareil

La page **Appareil** affiche des informations détaillées sur votre configuration OT Security. Vous pouvez afficher et modifier la configuration sur cette page.



Nom de l'appareil

Identifiant unique pour l'appliance OT Security.

URL de l'appareil

Vous permet de définir l'URL unique permettant d'accéder au système (FQDN).

Remarque : la modification de l'URL de l'appareil est un changement critique. Le nouveau FQDN n'est plus jamais présenté. Si vous ne notez pas la chaîne exacte, l'interface utilisateur devient inaccessible. Veillez à vérifier la résolution avant de continuer.

Heure système

L'heure et la date correctes sont définies automatiquement, mais peuvent être modifiées.

Remarque : la définition de la date et de l'heure est essentielle pour un enregistrement précis des journaux et des alertes.

Fuseau horaire

Dans la liste déroulante, sélectionnez le fuseau horaire local correspondant à l'emplacement du site. Pour modifier le fuseau horaire, cliquez sur **Modifier**.

Délai d'attente maximal pour la session de connexion

Période de session après laquelle les utilisateurs sont déconnectés automatiquement et doivent se reconnecter. Pour modifier le délai d'attente pour la session de connexion, cliquez sur **Modifier**. Options disponibles pour la période : 30 minutes, 1heure, 4 heures, 12 heures, 1jour, 1semaine et 2 semaines.

Délai maximal d'inactivité

Période d'inactivité après laquelle les utilisateurs connectés sont déconnectés automatiquement et doivent se reconnecter. Pour modifier la période d'inactivité, cliquez sur **Modifier**.

Période d'expiration des ports ouverts

Détermine la période après laquelle les listes de ports ouverts sont supprimées de l'écran des **détails de l'asset** en l'absence de signal indiquant que le port est toujours ouvert. La valeur par défaut est de deux semaines. Pour plus d'informations, voir Inventaire.

Requêtes Ping

L'activation des requêtes Ping active la réponse automatique de la plateforme OT Security aux requêtes Ping.

Pour activer les requêtes Ping, cliquez sur le curseur à côté de **Requêtes Ping**.

Capture de paquets

L'activation de la capacité de capture de paquets complets active l'enregistrement continu des captures de paquets complets de tout le trafic sur le réseau. Cela permet des capacités étendues de dépannage et d'investigation forensique. Lorsque la capacité de stockage dépasse 1,8 To, le système supprime les anciens fichiers. Vous pouvez afficher et télécharger les fichiers disponibles sur la page **Réseau** > **Captures de paquets**. Voir la section Réseau.

Pour activer les captures de paquets, cliquez sur le curseur à côté de **Capture de paquet**.

Remarque : vous pouvez arrêter la fonction de capture de paquet à tout moment en **désactivant** la fonction avec le curseur.

Approuver automatiquement les demandes d'appairage des capteurs

L'activation de l'approbation automatique des demandes d'appairage de capteur entrantes garantit que toutes les demandes d'appairage de capteur sont approuvées sans administrateur supplémentaire. Si cette option n'est pas sélectionnée, une approbation manuelle finale est requise pour qu'un nouveau capteur puisse se connecter à votre réseau.

Pour activer l'approbation automatique des demandes d'appairage entrantes des capteurs, cliquez sur le curseur **Approuver automatiquement les demandes d'appairage entrantes des capteurs**.

Bannière de classification

Ajoutez une bannière à OT Security pour indiquer les données accessibles via le logiciel.

Pour ajouter une bannière, cliquez sur **Modifier**. Après avoir ajouté la bannière, cliquez pour activer le curseur **Bannière de classification**.

Activer les statistiques d'utilisation

L'option **Activer les statistiques d'utilisation** précise si Tenable collecte des données de télémétrie anonymes sur votre déploiement OT Security. Lorsqu'elle est activée, Tenable collecte des informations de télémétrie qui ne peuvent pas être attribuées à un individu spécifique ; elles ne sont collectées qu'au niveau de l'entreprise. Ces informations ne comprennent aucune donnée personnelle ni information personnelle identifiable (IPI). Les informations de télémétrie comprennent, sans s'y limiter, les données concernant les pages visitées, les rapports et dashboards utilisés et les fonctionnalités configurées. Tenable utilise ces données dans le but d'améliorer votre expérience utilisateur pour les futures versions OT Security et à d'autres fins

commerciales, dans le respect des dispositions de l'accord-cadre de Tenable. Ce paramètre est activé par défaut.

Pour activer la collecte des informations de télémétrie, cliquez sur **Activer les statistiques d'utilisation**.

> **Remarque :** vous pouvez interrompre le partage des statistiques d'utilisation à tout moment en cliquant sur le curseur.

GraphQL Playground

IDE GraphQL utilisable dans le navigateur. Activez ou désactivez ce curseur pour utiliser le playground en production afin de tester vos requêtes API.

Configuration des ports

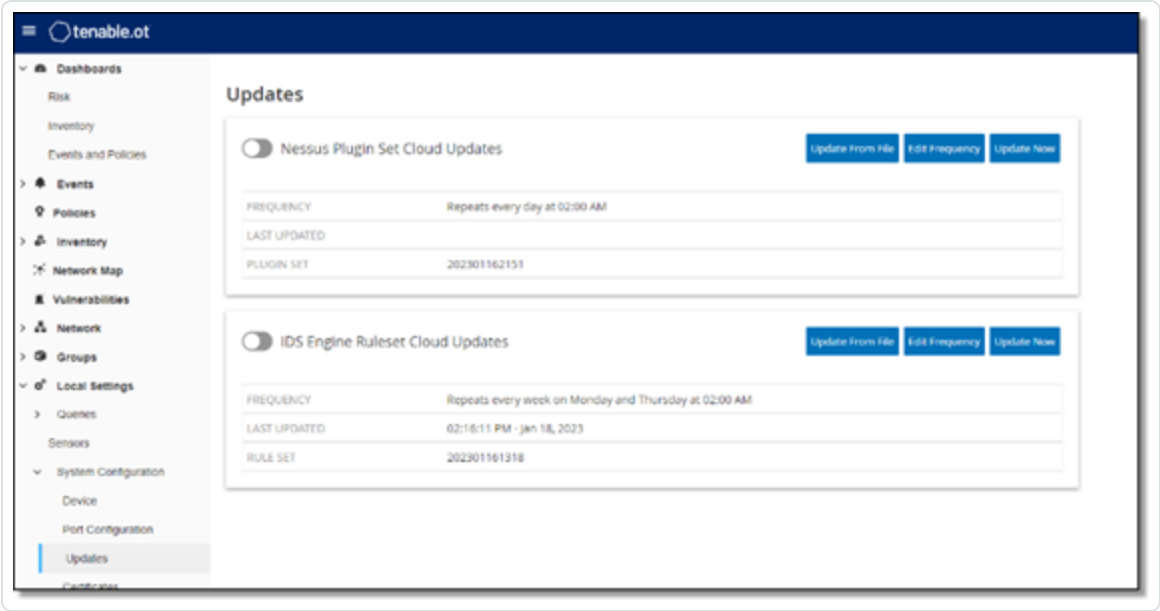
La page **Configuration des ports** montre la manière dont les ports de l'appareil sont configurés. Pour plus d'informations sur la configuration des ports, voir Appareil.

Mises à jour

La mise à jour des plugins Tenable Nessus et de l'ensemble de règles du moteur du système de détection d'intrusion (IDS) vers les dernières versions garantit que OT Security surveille vos assets

pour toutes les dernières vulnérabilités connues. Vous pouvez effectuer les mises à jour via le cloud, à la fois automatiquement et manuellement, et également hors ligne.

Remarque : pour plus d'informations sur la mise à jour de Tenable Core, voir Manage Updates (Gérer les mises à jour) dans le Guide de l'utilisateur Tenable Core + OT Security.



Remarque : vous pouvez également effectuer les mises à jour via **Vulnérabilités** > **Mettre à jour les plug-ins**.

Remarque : si la licence utilisateur expire, l'option de téléchargement des nouvelles mises à jour est bloquée, et les plug-ins ne peuvent pas être mis à jour.

Mises à jour de l'ensemble de plug-ins Tenable Nessus

Configurer des mises à jour cloud automatiques des plug-ins

Si vous disposez d'une connexion Internet, vous pouvez mettre à jour les plug-ins via le cloud. Lorsque vous activez les mises à jour automatiques, les plug-ins sont mis à jour à l'heure et selon la fréquence définies par vos soins (par défaut : tous les jours à 02:00).

Pour activer les mises à jour automatiques des plug-ins :

1. Accédez à **Paramètres locaux** > **Configuration système** > **Mises à jour**.

   La fenêtre **Mises à jour** apparaît. La section **Mises à jour des services cloud de l'ensemble de plug-ins Nessus** indique le numéro de votre ensemble de plug-ins, la date de la dernière mise à jour et le calendrier de mise à jour.

2. Cliquez sur le curseur **Mises à jour des services cloud de l'ensemble de plug-ins Nessus** pour activer les mises à jour automatiques.

Modifier la fréquence des mises à jour des plug-ins

Pour modifier le calendrier des mises à jour automatiques des plug-ins :

1. Accédez à **Paramètres locaux** > **Configuration système** > **Mises à jour**.

   La fenêtre **Mises à jour** apparaît. La section **Mises à jour des services cloud de l'ensemble de plug-ins Nessus** indique le numéro de votre ensemble de plug-ins, la date de la dernière mise à jour et le calendrier de mise à jour.

2. Cliquez sur **Modifier la fréquence**.

   Le panneau latéral **Modifier la fréquence** apparaît.

3. Dans la section **Répéter chaque**, définissez l'intervalle de temps auquel vous souhaitez mettre à jour les plug-ins, en saisissant un nombre et en sélectionnant une unité de temps (jours ou semaines) dans le menu déroulant.

   Si vous sélectionnez **Semaines**, sélectionnez le ou les jours de la semaine où vous souhaitez effectuer une mise à jour hebdomadaire des plug-ins.

4. Dans la section **À**, définissez l'heure à laquelle vous souhaitez mettre à jour les plug-ins (heure, minutes, secondes) en cliquant sur l'icône d'horloge et en sélectionnant l'heure, ou en saisissant l'heure manuellement.

5. Cliquez sur **Enregistrer**.

   Un message apparaît pour confirmer que la fréquence a bien été mise à jour.

Mettre à jour manuellement les plug-ins via le cloud

Pour mettre à jour manuellement les plug-ins :

1. Accédez à **Paramètres locaux** > **Configuration système** > **Mises à jour**.

   La page **Mises à jour** apparaît avec la section **Mises à jour des services cloud de l'ensemble de plug-ins Nessus**, en indiquant le numéro de votre ensemble de plug-ins, la date de la dernière mise à jour et le calendrier de mise à jour.

2. Cliquez sur **Mettre à jour maintenant**.

   Un message confirme que la mise à jour est en cours. Une fois la mise à jour terminée, l'**ensemble de plug-ins** affiche le numéro de l'ensemble de plug-ins actuel.

   > **Conseil** : pendant la **mise à jour de l'ensemble de plug-ins**, maintenez la fenêtre du navigateur ouverte et n'actualisez pas la page.

Mises à jour hors ligne

Si vous ne disposez pas d'une connexion Internet sur votre appareil OT Security, vous pouvez mettre à jour manuellement les plug-ins en téléchargeant le dernier ensemble de plug-ins depuis le portail Tenable Community puis en chargeant le fichier.

Pour mettre à jour les plug-ins sans connexion Internet :

1. Accédez à **Paramètres locaux** > **Configuration système** > **Mises à jour**.

   La page **Mises à jour** apparaît. La section **Mises à jour des services cloud de l'ensemble de plug-ins Nessus** indique le numéro de votre ensemble de plug-ins, la date de la dernière mise à jour et le calendrier de mise à jour.

2. Cliquez sur **Mettre à jour à partir du fichier**.

La fenêtre **Mettre à jour à partir du fichier** apparaît.

3. Si vous ne l'avez pas encore fait, cliquez sur le lien pour télécharger le dernier fichier de plug-in, puis revenez à la fenêtre **Mettre à jour à partir du fichier**.

   > **Remarque :** le téléchargement du dernier fichier de plug-in à partir du lien n'est possible que via une connexion Internet, par exemple avec un PC connecté à Internet.

4. Cliquez sur **Parcourir** et accédez au fichier d'ensemble de plug-ins que vous avez téléchargé à partir du portail client de OT Security.
5. Cliquez sur **Mettre à jour**.

Mises à jour de l'ensemble de règles du moteur IDS

Configurer les mises à jour cloud automatiques de l'ensemble de règles du moteur IDS

Si vous disposez d'une connexion Internet, vous pouvez mettre à jour l'ensemble de règles du moteur IDS via le cloud. Lorsque vous activez les mises à jour automatiques, l'ensemble de règles du moteur IDS peut être mis à jour à l'heure et selon la fréquence définies par vos soins (par défaut : toutes les semaines, le mardi et le jeudi à 02:00).

Pour activer les mises à jour automatiques de l'ensemble de règles du moteur IDS :

1. Accédez à **Paramètres locaux** > **Configuration système** > **Mises à jour**.

   La page **Mises à jour** apparaît. La section **Mises à jour cloud de l'ensemble de règles du moteur IDS** indique le numéro de votre ensemble de règles, la date de la dernière mise à jour et le calendrier de mise à jour.

2. Cliquez sur le curseur **Mises à jour cloud de l'ensemble de règles du moteur IDS** pour activer les mises à jour automatiques.

Modifier la fréquence des mises à jour de l'ensemble de règles du moteur IDS

Pour modifier le calendrier des mises à jour automatiques de l'ensemble de règles du moteur IDS :

1. Accédez à **Paramètres locaux** > **Configuration système** > **Mises à jour**.

   La page **Mises à jour** apparaît. La section **Mises à jour cloud de l'ensemble de règles du moteur IDS** indique le numéro de votre ensemble de règles, la date de la dernière mise à jour et le calendrier de mise à jour.

2. Cliquez sur **Modifier la fréquence**.

   Le panneau latéral **Modifier la fréquence** apparaît.

3. Dans la section **Répéter chaque**, définissez l'intervalle de temps auquel vous souhaitez mettre à jour l'ensemble de règles en saisissant un nombre et en sélectionnant une unité de temps (jours ou semaines) dans le menu déroulant.

   Si vous sélectionnez **Semaines**, sélectionnez le ou les jours de la semaine où vous souhaitez effectuer une mise à jour hebdomadaire de l'ensemble de règles.

4. Dans la section **À**, définissez l'heure à laquelle vous souhaitez mettre à jour l'ensemble de règles du moteur IDS (heure, minutes, secondes) en cliquant sur l'icône d'horloge et en sélectionnant l'heure, ou en saisissant l'heure manuellement.

5. Cliquez sur **Enregistrer**.

   Un message apparaît pour confirmer que la fréquence a bien été mise à jour.

Mettre à jour manuellement l'ensemble de règles du moteur IDS

Pour mettre à jour manuellement l'ensemble de règles du moteur IDS :

1. Accédez à **Paramètres locaux** > **Configuration système** > **Mises à jour**.

   La page **Mises à jour** apparaît. La section **Mises à jour cloud de l'ensemble de règles du moteur IDS** indique le numéro de votre ensemble de règles, la date de la dernière mise à jour et le calendrier de mise à jour.

2. Cliquez sur **Mettre à jour maintenant**.

   Un message confirme que la mise à jour est en cours. Une fois la mise à jour terminée, la zone **Ensemble de règles** affiche le numéro de l'ensemble de règles actuel du moteur IDS.

Mises à jour hors ligne

Si vous ne disposez pas d'une connexion Internet sur votre appareil OT Security, vous pouvez mettre à jour manuellement l'ensemble de règles du moteur IDS en téléchargeant le dernier ensemble de règles depuis le portail client de Tenable puis en chargeant le fichier.

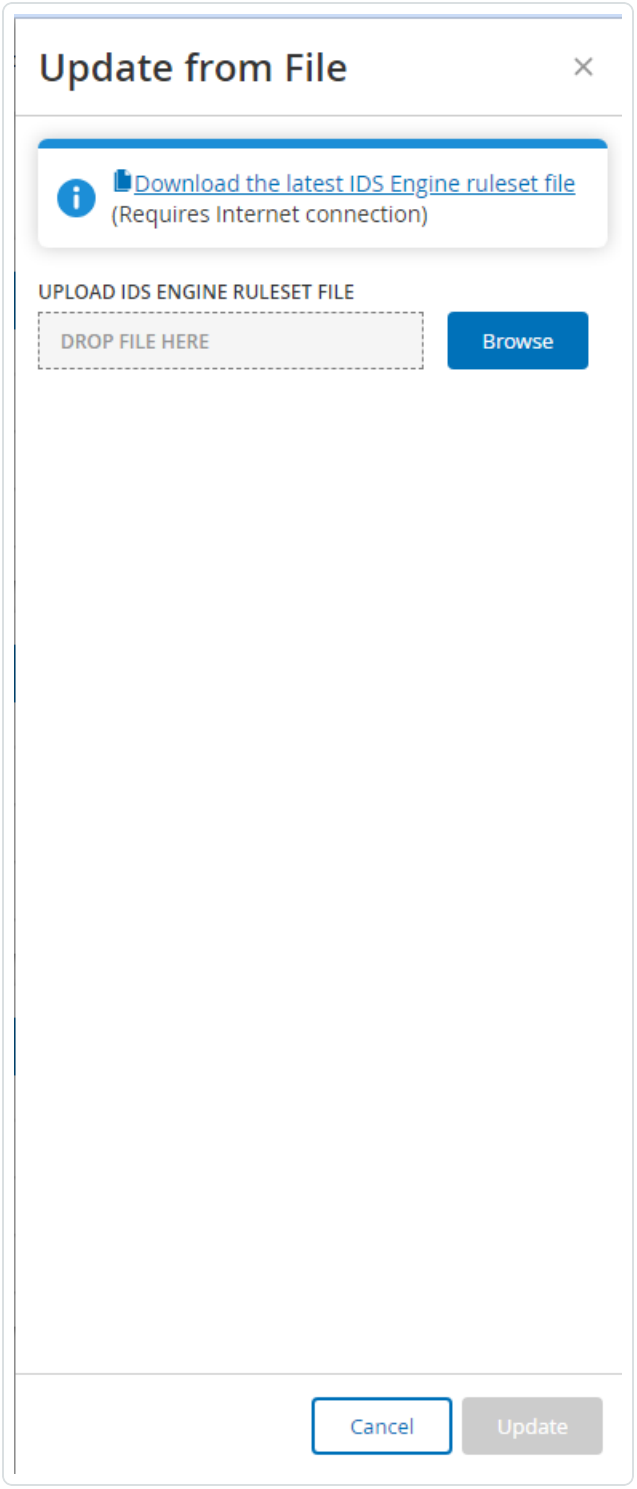
Pour mettre à jour l'ensemble de règles du moteur IDS hors ligne :

1. Accédez à **Paramètres locaux** > **Configuration système** > **Mises à jour**.

   La fenêtre **Mises à jour** apparaît. La section **Mises à jour cloud de l'ensemble de règles du moteur IDS** indique le numéro de votre ensemble de règles, la date de la dernière mise à jour et le calendrier de mise à jour.

2. Cliquez sur **Mettre à jour à partir du fichier**.

   La fenêtre **Mettre à jour à partir du fichier** apparaît.



3. Si vous ne l'avez pas encore fait, cliquez sur le lien pour télécharger le dernier fichier d'ensemble de règles du moteur IDS.

Remarque : le téléchargement du dernier fichier d'ensemble de règles du moteur IDS à partir du lien n'est possible que via une connexion Internet, par exemple, avec un PC connecté à Internet.

4. Cliquez sur **Parcourir** et accédez au fichier d'ensemble de règles du moteur IDS que vous avez téléchargé à partir du portail client de OT Security.
5. Cliquez sur **Mettre à jour**.

Certificats

Générer un certificat HTTPS

Le certificat HTTPS garantit que le système utilise une connexion sécurisée à l'appliance et au serveur OT Security. Le certificat initial est valide deux ans. Vous pouvez générer un nouveau certificat auto-signé à tout moment. Le nouveau certificat est valable un an.

Remarque : le nouveau certificat généré remplace le certificat actuel.

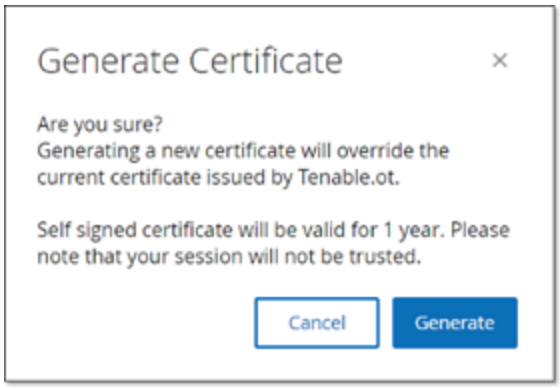
Pour générer un certificat auto-signé :

1. Accédez à **Paramètres locaux** > **Configuration système** > **Certificats**.

   La fenêtre **Certificats** apparaît.

2. Dans le menu **Actions**, sélectionnez **Générer un certificat auto-signé**.

   La fenêtre de confirmation de génération du certificat apparaît.



3. Cliquez sur **Générer**.

   OT Security génère le certificat auto-signé et peut être affiché sur la page **Paramètres locaux** > **Configuration système** > **Certificat**.

Charger un certificat HTTPS

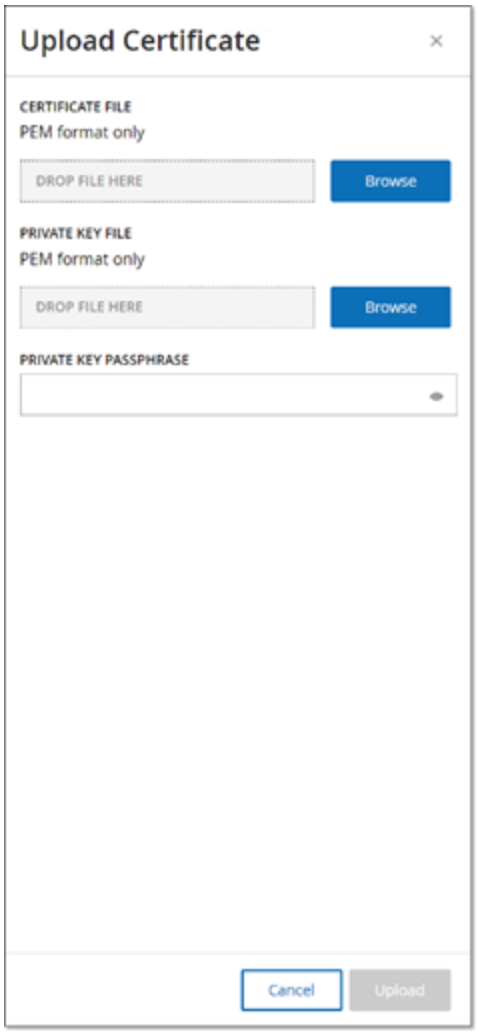
Pour charger un certificat HTTPS :

1. Accédez à **Paramètres locaux** > **Configuration système** > **Certificats**.

   La fenêtre **Certificats** apparaît.

2. Dans le menu **Actions**, sélectionnez **Charger un certificat**.

   Le panneau latéral **Charger un certificat** apparaît.



3. Dans la section **Fichier de certificat**, cliquez sur **Parcourir** et accédez au fichier de certificat à charger.
4. Dans la section **Fichier de clé privée**, cliquez sur **Parcourir** et accédez au fichier de clé privée à charger.
5. Dans la zone **Mot de passe de la clé privée**, saisissez le mot de passe de la clé privée.
6. Cliquez sur **Charger** pour charger les fichiers.

   Le panneau latéral se referme.

   Remarque : après avoir remplacé le certificat, Tenable recommande de recharger l'onglet du navigateur pour s'assurer que la mise à jour du certificat HTTP a réussi. Si le chargement a échoué, OT Security affiche un message d'avertissement.

Générer des clés API

La génération d'une clé API peut faciliter l'intégration de OT Security à d'autres outils et systèmes de sécurité au sein de votre organisation.

Pour générer des clés API dans OT Security :

1. Accédez à **Paramètres locaux** > **Configuration système** > **Clés API**.

   La page **Clés API** apparaît.

2. Dans le coin supérieur droit, cliquez sur **Générer une clé**.

   Le panneau **Générer une clé** apparaît.

3. Dans la zone **Période d'expiration**, sélectionnez le nombre de jours après lequel la clé API peut expirer.

4. Dans la zone **Description**, saisissez la description de la clé API.

5. Cliquez sur **Générer**.

   Le panneau **Générer une clé** apparaît avec l'**ID** et la **clé API**.

6. Cliquez sur le bouton pour copier la clé API.

7. Cliquez sur **Terminé**.

   La page **Clés API** apparaît avec l'ID de la clé API nouvellement ajoutée.

Appairer l'ICP avec Enterprise Manager

Remarque : ce flux est disponible pour OT Security 3.18 et versions ultérieures.

Vous pouvez appairer votre plateforme Core industrielle (ICP) avec OT Security EM et gérer tous vos sites.

Remarque : une fois appairées avec EM, toutes les mises à jour doivent être effectuées au niveau EM, afin que les sites et leurs capteurs reçoivent les dernières mises à jour de version.

Avant de commencer

Assurez-vous que :

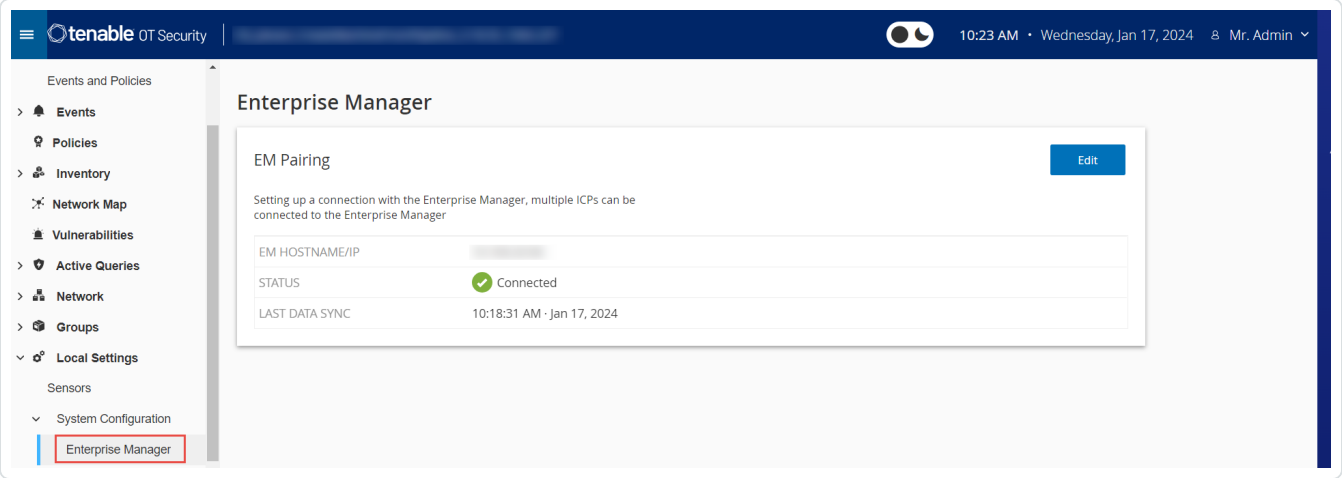
- OT Security EM peut se connecter à l'ICP via l'API.
- Assurez-vous que les ports TCP 443 et TCP 28305 sont ouverts pour la communication de l'ICP vers OT Security EM.
- Il doit y avoir des connexions HTTPS entre l'ICP et OT Security EM.
- (Facultatif) Générez une clé API dans OT Security EM.

> **Remarque** : cela n'est nécessaire que lorsque l'appairage se fait à l'aide de l'option de la clé API.

Pour appairer l'ICP avec OT Security EM :

1. Dans OT Security, accédez à **Paramètres locaux** > **Configuration système** > **Enterprise Manager**.

   La page **Enterprise Manager** s'affiche.



2. Dans la section **Appairage d'EM**, cliquez sur **Démarrer l'appairage**.

   Le panneau **Configuration de l'appairage d'EM** apparaît.

3. Sélectionnez l'une des options suivantes :

   - **Appairer à l'aide du nom d'utilisateur et du mot de passe**
   - **Appairer à l'aide de la clé secrète de l'API**

Si vous sélectionnez...	Action

Appairer à l'aide du nom d'utilisateur et du mot de passe	1. Dans la zone **Nom d'hôte/ adresse IP**, saisissez le nom d'hôte ou l'adresse IP de l'EM. 2. Dans la zone **Nom d'utilisateur**, saisissez le nom d'utilisateur de l'administrateur de l'EM. 3. Dans la zone **Mot de passe**, saisissez le mot de passe de l'EM. 4. Dans la zone **Empreinte du certificat d'EM**, collez le certificat que vous avez copié à partir de la page **Certificats** d'EM. **Conseil** : vous pouvez ignorer cette étape et approuver manuellement le certificat à partir de la page **Appairage d'EM**. **Remarque** : vous pouvez accéder à la page **Certificats** à partir de **Paramètres locaux** > **Configuration système** dans OT Security EM.
Appairer à l'aide d'une clé API	1. Dans la zone **Nom d'hôte/ adresse IP**, saisissez le nom d'hôte ou l'adresse IP de l'EM. 2. Dans la zone **Clé secrète de l'API**, collez la clé API que vous avez copiée à partir d'EM. 3. Dans la zone **Empreinte du certificat d'EM**, collez le certificat que vous avez copié à partir de la page **Certificats** d'EM. **Conseil** : vous pouvez ignorer cette étape et approuver manuellement le certificat à partir de la page **Appairage d'EM**. **Remarque** : vous pouvez accéder à la page **Certificats** à partir de **Paramètres locaux** >

	Configuration système dans OT Security EM.

4. Cliquez sur **Appairer**.

   OT Security affiche la page **Appairage d'EM** avec le statut d'appairage.

   Remarque : le statut peut apparaître comme **Attente de l'approbation de certificat** (si le certificat n'est pas fourni) ou **En attente d'approbation d'EM** (si l'approbation automatique des demandes d'appairage est désactivée).

5. (Facultatif) Si le statut affiche **Attente de l'approbation de certificat** :

   a. Cliquez sur **Afficher le certificat**.

      Le panneau **Approuver le certificat** apparaît.

   b. Vérifiez si l'empreinte numérique visible sur le panneau est la même que celle de la page **Certificats** d'EM.

      Cliquez sur **Approuver**.

      OT Security approuve le certificat et affiche la page Appairage d'EM dont le statut est passé à **En attente d'approbation d'EM**.

6. Si le statut affiche **En attente d'approbation d'EM**, cela indique que l'option **Approuver automatiquement les demandes d'appairage ICP** est désactivée. Procédez comme suit :

   Conseil : pour approuver automatiquement les demandes d'appairage dans OT Security EM, activez l'option **Approuver automatiquement les demandes d'appairage ICP** sur la page **ICP** de OT Security EM.

   a. Dans OT Security EM, dans la barre de navigation de gauche, sélectionnez **ICP**.

      La page **ICP** apparaît.

   b. Survolez la ligne du système à appairer, puis effectuez l'une des actions suivantes :

      - Effectuez un clic droit dans la colonne **Statut** et sélectionnez **Approuver**.
      - Dans le coin supérieur droit, cliquez sur **Actions** > **Approuver**.

   OT Security EM approuve l'appairage et affiche le statut **Connecté**.

Conseil : une fois l'appairage terminé, OT Security EM affiche les éléments suivants :

- Les données de l'ICP sur les **dashboards** EM.
- L'ICP nouvellement appairée sur la page **ICP**.
- Accédez à l'ICP en cliquant sur son nom sur la page **ICP** . L'instance de l'ICP accessible à partir d'EM présente l'étiquette **ICP** dans l'en-tête. Pour plus d'informations, voir ICPs (ICP) dans le Guide de l'utilisateur Tenable OT Security Enterprise Manager.

Dans OT Security, la page **Enterprise Manager** affiche le statut **Connecté**. Vous pouvez cliquer sur **Modifier** pour modifier la configuration de l'appairage d'EM.

Déconnecter l'appairage ICP avec Enterprise Manager

Vous pouvez déconnecter l'appairage ICP d'EM ou de l'ICP lorsque l'appairage n'est plus nécessaire.

Pour déconnecter un appairage ICP de OT Security EM :

1. Dans OT Security EM, dans la barre de navigation de gauche, sélectionnez **ICP**.

   La page **ICP** apparaît.

2. Survolez la ligne de l'ICP à supprimer, puis effectuez l'une des actions suivantes :

   - Effectuez un clic droit dans la colonne **Statut** et sélectionnez **Supprimer**.
   - Cliquez sur la ligne de l'ICP. La ligne est alors mise en surbrillance et le bouton **Actions** est activé.

3. Cliquez sur **Supprimer**.

OT Security EM déconnecte l'appairage avec OT Security.

Pour déconnecter un appairage ICP de OT Security :

1. Dans OT Security, accédez à **Paramètres locaux** > **Configuration système** > **Enterprise Manager**.

   La page **Enterprise Manager** s'affiche.

2. Dans la section Appairage d'EM, cliquez sur **Modifier**.

Le panneau **Appairage d'EM** apparaît.

3. Cliquez sur **Aucun appairage**.
4. Cliquez sur **Appairer**.

   OT Security déconnecte l'appairage avec OT Security EM.

Licence

Lorsque vous devez mettre à jour ou réinitialiser votre licence OT Security, contactez votre responsable de compte Tenable. Une fois que votre responsable de compte Tenable a mis à jour votre licence, vous pouvez la mettre à jour ou la réinitialiser. Pour plus d'informations, voir le Activation de licence OT Security.

Configuration de l'environnement

Paramètres des assets

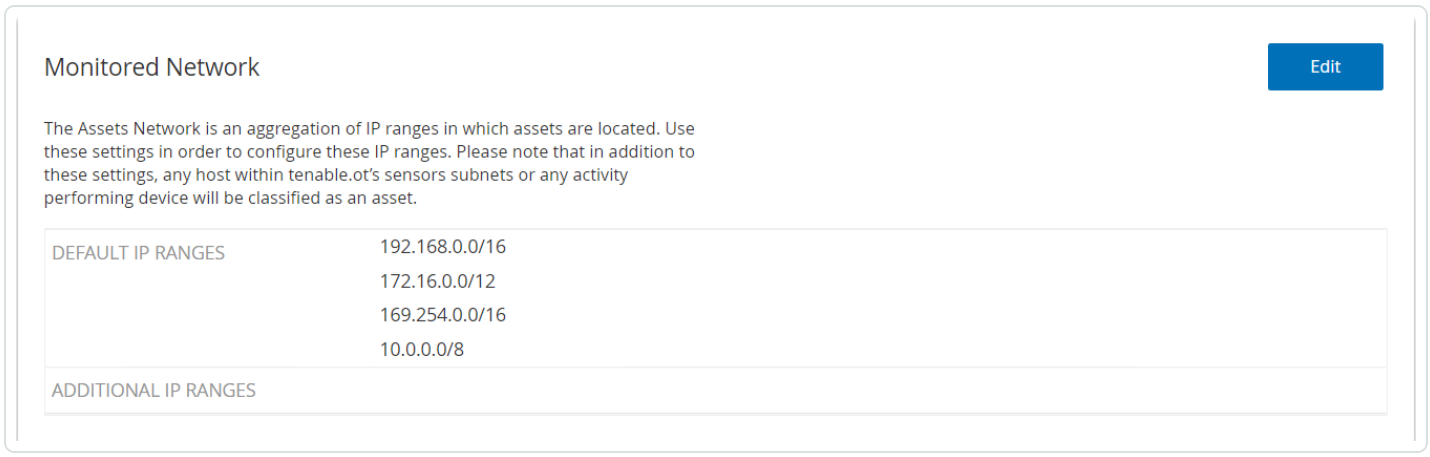
La page **Paramètres des assets** comprend les sections suivantes :

- Réseaux surveillés
- Mettre à jour les détails des assets à l'aide d'un fichier CSV
- Ajouter des assets manuellement
- Récupérer une adresse IP pour les assets IoT

Réseaux surveillés

La configuration du réseau surveillé contient un ensemble de plages d'adresses IP (CIDR/sous-réseaux) qui définissent les limites de surveillance pour OT Security. OT Security ignore les assets en dehors des plages configurées.

Par défaut, OT Security configure trois plages publiques par défaut : 10.0.0.0/8, 172.16.0.0/12 et 192.168.0.0/16, ainsi que la plage de lien local de 169.254.0.0/16 (APIPA).



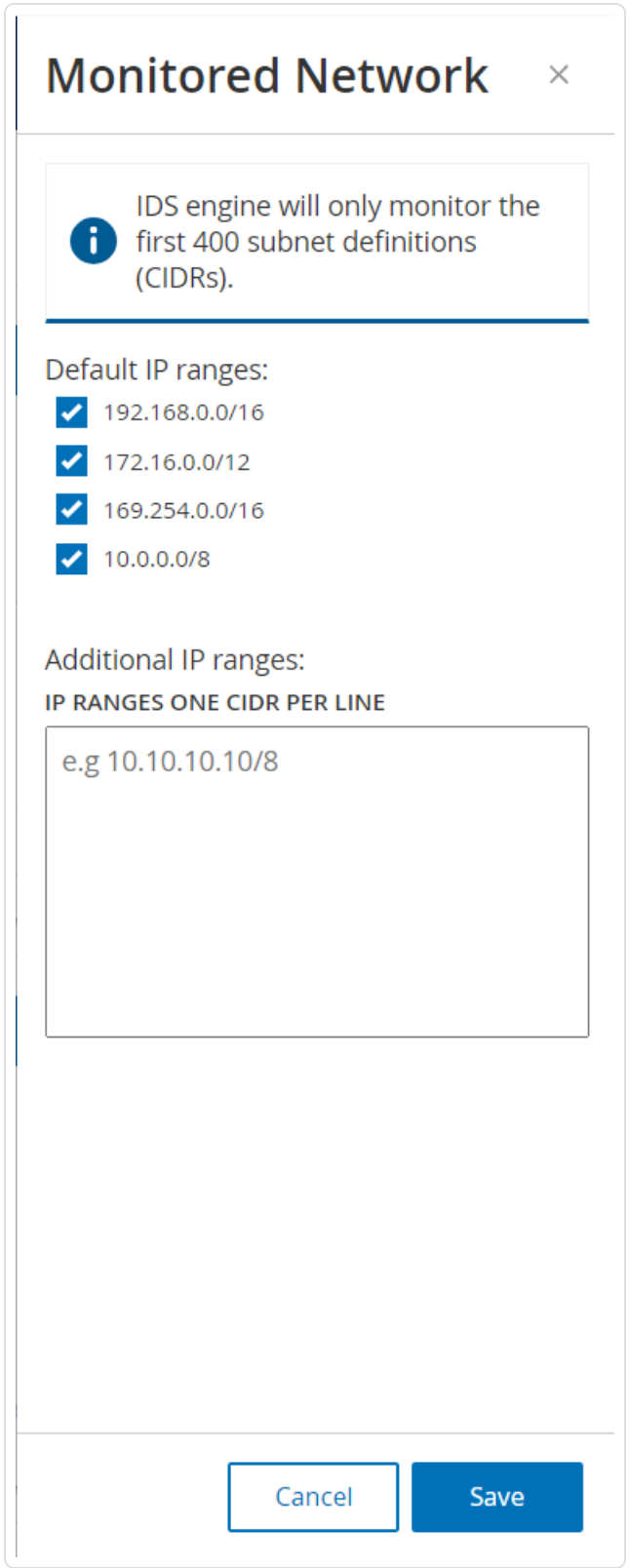
Pour désactiver l'une des plages par défaut ou pour ajouter des plages appropriées à votre réseau :

1. Sous **Paramètres locaux**, accédez à **Configuration de l'environnement** > **Paramètres de l'asset**.

   La fenêtre **Paramètres de l'asset** apparaît.

2. Dans la section **Réseau surveillé**, cliquez sur **Modifier**.

Le panneau **Réseau surveillé** apparaît.



3. Sélectionnez les **Plages d'adresses IP par défaut** requises et/ou ajoutez des **Plages d'adresses IP supplémentaires** (une plage d'adresses IP par ligne) dans la zone de texte désignée.
4. Cliquez sur **Enregistrer**.

   OT Security enregistre la configuration du réseau surveillé.

Mettre à jour les détails des assets à l'aide d'un fichier CSV

Vous pouvez exporter un fichier CSV issu du tableau « Tous les assets », le modifier, puis l'importer. Les champs modifiables incluent : **Type**, **Nom**, **Criticité**, **Niveau Purdue**, **Localisation**, **Description** et tous les champs personnalisés.

Vous pouvez mettre à jour les détails d'un asset à l'aide d'un fichier CSV uniquement lorsque la langue est définie sur l'anglais. Les utilisateurs non anglophones peuvent temporairement passer à l'anglais lors de l'exportation et du chargement du fichier CSV, puis rétablir leur langue préférée.

Pour charger le fichier CSV des détails de l'asset :

1. Accédez à **Configuration de l'environnement** > **Paramètres de l'asset**.
2. Accédez à la section **Mettre à jour les détails d'un asset à l'aide d'un fichier CSV**.
3. Cliquez sur **Charger**.
4. Accédez à l'emplacement où se trouve le fichier CSV et chargez-le.

Ajouter des assets manuellement

Pour suivre votre inventaire, vous souhaiterez peut-être afficher d'autres assets que vous possédez, même s'ils n'ont pas encore été détectés par OT Security. Vous pouvez ajouter manuellement ces assets à votre inventaire en téléchargeant et en modifiant un fichier CSV, puis en chargeant le fichier sur le système. Vous ne pouvez charger que les assets dont l'adresse IP n'est pas déjà utilisée par un asset existant dans le système. Si le système détecte un asset qui communique sur le réseau avec la même adresse IP, il utilise les informations récupérées sur l'asset détecté et remplace les informations précédemment chargées. Le système commence à voir l'asset comme un élément normal lorsqu'il détectera ses communications sur le réseau.

Les adresses IP des assets chargés sont comptabilisées dans la licence du système.

Les assets chargés affichent un score de risque de 0 jusqu'à ce que OT Security les détecte.

> **Remarque :** lorsque des assets sont ajoutés manuellement, aucun événement n'est détecté pour ces assets jusqu'à ce que OT Security détecte leur communication sur le réseau.

Pour ajouter des assets manuellement :

1. Sous **Paramètres locaux**, accédez à **Configuration de l'environnement** > **Paramètres de l'asset**.

   L'écran **Paramètres de l'asset** apparaît.

2. Dans **Ajouter des assets manuellement**, cliquez sur le bouton **Actions** et dans le menu déroulant, sélectionnez **Télécharger le modèle CSV**.

   OT Security télécharge le modèle de document tot_Assets.

3. Ouvrez le document modèle tot_Assets.

4. Modifiez le modèle tot_Assets en suivant précisément les instructions trouvées dans le fichier, en ne laissant que les en-têtes de colonne (Nom, Type, etc.) et les valeurs que vous saisissez.

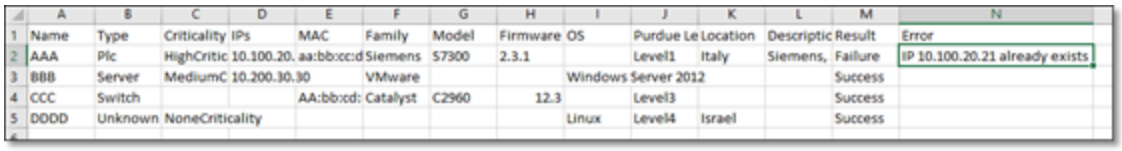
5. Enregistrez le fichier modifié.

6. Revenez à l'écran **Paramètres des assets**.

7. Depuis le menu **Actions**, sélectionnez **Charger un fichier CSV**, accédez au fichier CSV souhaité et ouvrez-le pour le charger.

8. Dans **Ajouter des assets manuellement**, cliquez sur **Télécharger le rapport**.

   Un fichier CSV avec un rapport apparaît, indiquant les réussites et les échecs dans la colonne Result (Résultat). Les détails des erreurs sont affichés dans la colonne Erreur.



	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	

Groupes d'événements

Pour faciliter le suivi des événements, plusieurs événements aux caractéristiques communes sont regroupés pour former un cluster. Le clustering est basé sur le type d'événement (c'est-à-dire, les événements qui ont une même politique en commun), les assets sources et cibles, etc.

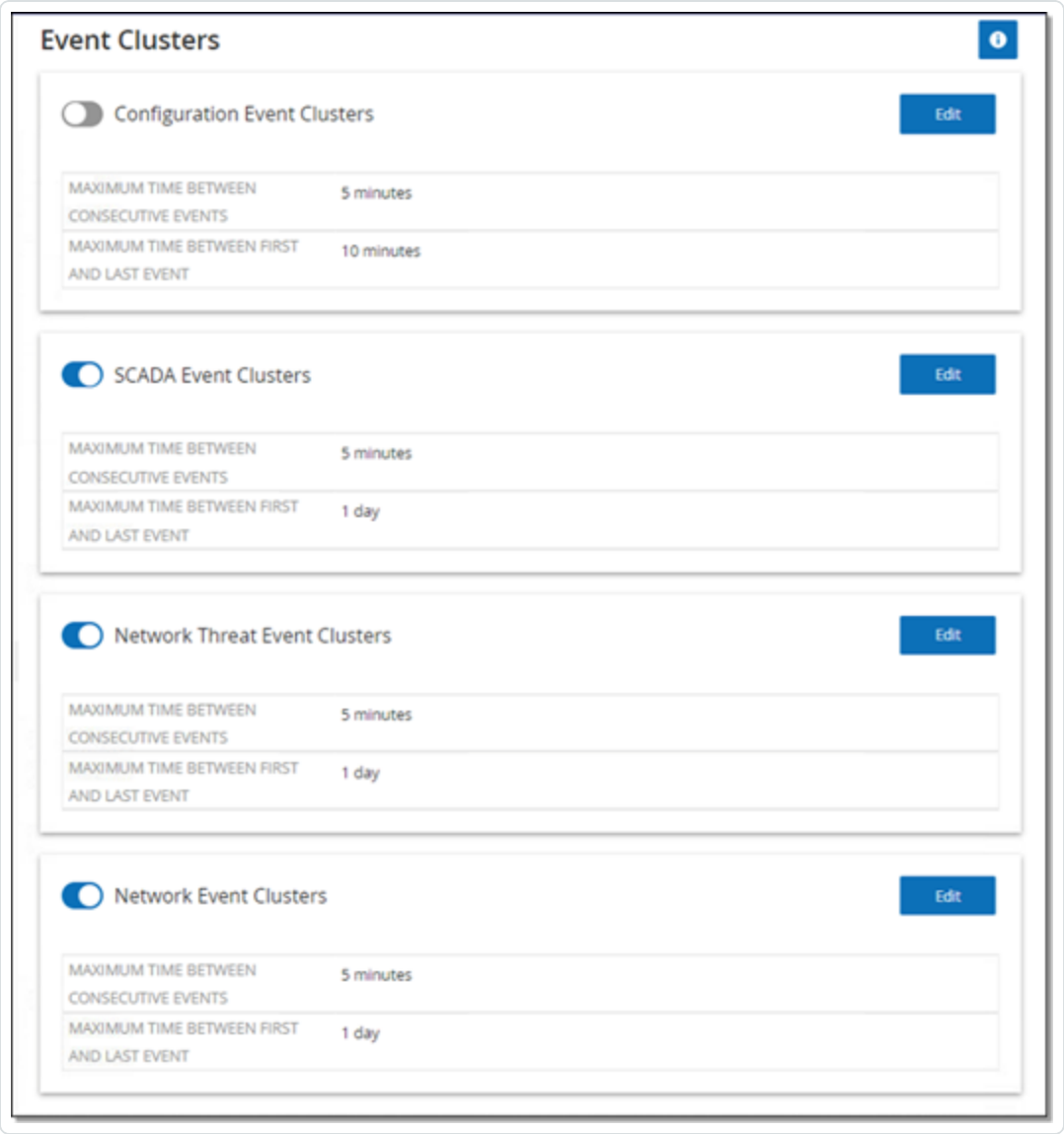
Pour regrouper des événements dans un cluster, ils doivent être générés dans les intervalles de temps configurés suivants :

- **Temps maximal entre événements consécutifs** – Définit l'intervalle de temps maximal entre les événements. Au-delà de ce délai, les événements consécutifs ne sont pas mis en cluster.
- **Temps maximum entre le premier et le dernier événement** – Définit l'intervalle de temps maximal pour que tous les événements soient affichés dans un cluster. Un événement généré après cet intervalle de temps ne fait pas partie du cluster.

Pour activer le clustering :

1. Accédez à **Paramètres locaux** > **Configuration de l'environnement** > **Clusters d'événements**.

   La page **Clusters d'événements** apparaît.

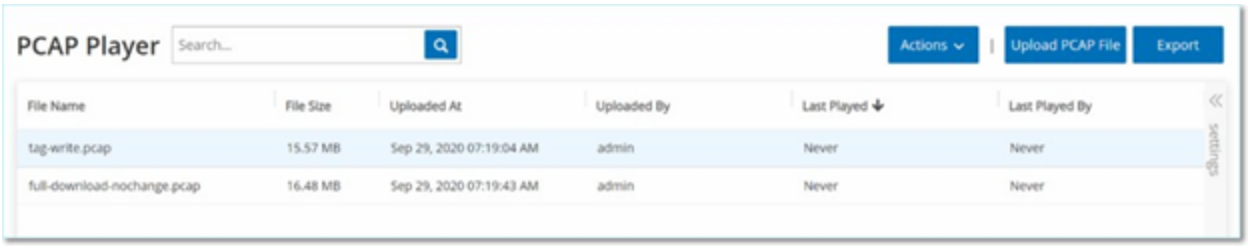


2. Cliquez sur le curseur pour activer les catégories souhaitées pour le clustering.
3. Pour configurer les intervalles de temps pour une catégorie, cliquez sur **Modifier**.

   La fenêtre **Modifier la configuration** apparaît.
4. Saisissez la valeur numérique requise dans la zone numérique et l'unité de temps dans la zone déroulante.

   Remarque : pour plus d'informations sur le clustering et les intervalles de temps, cliquez sur l'icône .
5. Cliquez sur **Enregistrer**.

Lecteur PCAP



OT Security permet de charger un fichier PCAP (capture de paquet) contenant l'activité réseau enregistrée et de le « lire » sur OT Security. Lorsque vous « lisez » un fichier PCAP, OT Security surveille le trafic réseau et enregistre toutes les informations sur les assets détectés, l'activité réseau et les vulnérabilités comme si le trafic se produisait au sein de votre réseau. Vous pouvez utiliser cette fonctionnalité à des fins de simulation ou pour analyser le trafic en dehors du réseau que OT Security surveille, des usines distantes, par exemple.

Remarque : le lecteur PCAP prend en charge ces types de fichiers : `.pcap`, `.pcapng`, `.pcap.gz`,`.pcapng.gz`. Vous pouvez utiliser des fichiers qui ont été enregistrés par une instance de OT Security ou d'autres outils de surveillance du réseau.

Charger un fichier PCAP

Pour charger un fichier PCAP :

1. Accédez à **Paramètres locaux** > **Configuration de l'environnement** > **Lecteur PCAP**.
2. Cliquez sur **Charger le fichier PCAP**.

   L'**explorateur de fichiers** apparaît.
3. Sélectionnez l'enregistrement PCAP souhaité.
4. Cliquez sur **Ouvrir**.

   OT Security charge le fichier PCAP sur le système.

Lire un fichier PCAP

Pour lire un fichier PCPAP :

1. Accédez à **Paramètres locaux** > **Configuration de l'environnement** > **Lecteur PCAP**.
2. Sélectionnez l'enregistrement PCAP à lire.
3. Cliquez sur **Actions** > **Lire**.

   L'assistant **Lire le PCAP** apparaît.
4. Dans la zone déroulante **Vitesse de lecture**, sélectionnez la vitesse de lecture du fichier par le système.

   Les options sont : 1X, 2X, 4X, 8X ou 16X.

   > **Remarque :** la lecture d'un fichier PCAP injecte des données dans le système. Cette opération est irréversible ou ne peut pas être arrêtée une fois lancée.
5. Cliquez sur **Lire**.

   Le système lit le fichier PCAP. Toute l'activité du réseau dans le fichier PCAP est enregistrée dans le système et les assets identifiés par le système sont ajoutés à l'inventaire des assets.

   > **Remarque :** vous ne pouvez pas lire un autre fichier PCAP pendant qu'un fichier est en cours de lecture.

Gestion des utilisateurs

L'accès à la console OT Security est contrôlé par des comptes utilisateur qui désignent les autorisations disponibles pour l'utilisateur. Les autorisations de l'utilisateur sont déterminées par les groupes d'utilisateurs auxquels ils sont affectés. Chaque groupe d'utilisateurs se voit attribuer un rôle qui définit l'ensemble des autorisations qui sont disponibles pour ses membres. Ainsi, par exemple, si le groupe d'utilisateurs Opérateurs de site a le rôle Opérateur de site, tous les utilisateurs affectés à ce groupe ont l'ensemble d'autorisations associé au rôle Opérateur de site.

Le système est livré avec un ensemble de groupes d'utilisateurs pré-définis, correspondant à chacun des rôles disponibles, à savoir **Administrators** (Groupe d'utilisateurs > rôle **Administrator**), **Site Operators** (Groupe d'utilisateurs > rôle **Site Operator**), etc. Vous pouvez également créer des groupes d'utilisateurs personnalisés et spécifier leurs rôles.

Il existe trois méthodes pour créer des utilisateurs dans le système :

- **Ajouter des utilisateurs locaux** – Créez des comptes utilisateur afin d'autoriser les utilisateurs individuels à accéder au système. Affectez des utilisateurs à des groupes d'utilisateurs qui définissent leurs rôles.
- **Serveurs d'authentification** – Utilisez les serveurs d'authentification de votre organisation (par ex. Active Directory, LDAP) pour autoriser les utilisateurs à accéder au système. Vous pouvez attribuer des rôles OT Security en fonction de vos groupes existants dans Active Directory.
- **SAML** – Configurez une intégration avec votre fournisseur d'identité (par exemple, Microsoft Entra ID) et affectez des utilisateurs à votre application OT Security.

Utilisateurs locaux

Groupes d'utilisateurs

Rôles d'utilisateur

Zones

Serveurs d'authentification

SAML

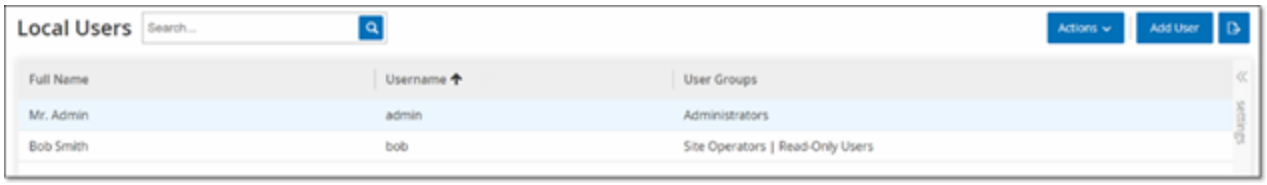
Utilisateurs locaux

Un utilisateur administrateur peut créer de nouveaux comptes utilisateur et modifier les comptes existants. Chaque utilisateur est affecté à un ou plusieurs groupes d'utilisateurs qui déterminent son ou ses rôles.

> **Remarque :** les utilisateurs peuvent être ajoutés aux groupes d'utilisateurs lors de la création ou de la modification de leur compte ou du groupe d'utilisateurs.

Afficher les utilisateurs locaux

La fenêtre **Utilisateurs locaux** affiche la liste de tous les utilisateurs locaux du système.



La fenêtre **Utilisateurs locaux** affiche les détails suivants :

Paramètre	Description
Nom complet	Le nom complet de l'utilisateur.
Nom d'utilisateur	Le nom d'utilisateur de l'utilisateur, pour la connexion.
Groupes d'utilisateurs	Les groupes d'utilisateurs auxquels l'utilisateur est affecté.

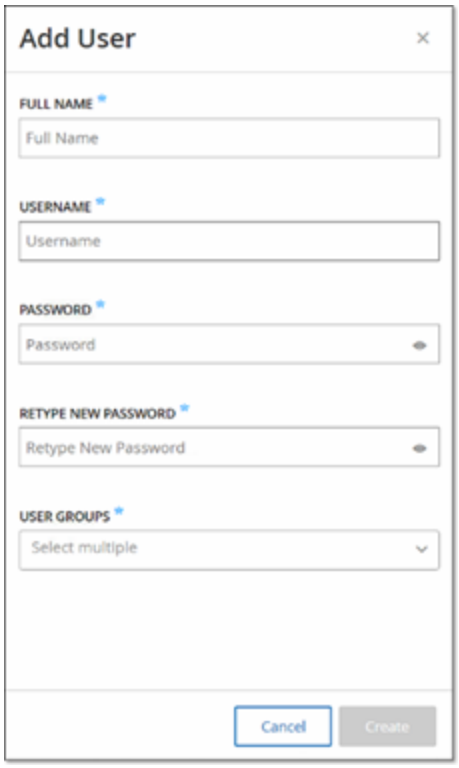
Ajouter des utilisateurs locaux

Vous pouvez créer des comptes utilisateur afin d'autoriser des utilisateurs à accéder au système. Chaque utilisateur doit être affecté à un ou plusieurs groupes d'utilisateurs.

Pour créer un compte utilisateur :

1. Accédez à **Paramètres locaux** > **Gestion des utilisateurs** > **Utilisateurs locaux**.
2. Cliquez sur **Ajouter un utilisateur**.

   Le panneau **Ajouter un utilisateur** apparaît.



3. Dans la zone **Nom complet**, saisissez les prénom et nom de famille.

   Remarque : le nom que vous saisissez apparaît dans la barre d'en-tête lorsque l'utilisateur est connecté.

4. Dans la zone **Nom d'utilisateur**, saisissez le nom d'utilisateur à utiliser pour la connexion au système.

5. Dans la zone **Mot de passe**, saisissez un mot de passe.

6. Dans la zone **Confirmer le mot de passe**, saisissez le même mot de passe.

   Remarque : il s'agit du mot de passe que l'utilisateur utilise pour la première connexion. Il peut le modifier dans la fenêtre **Paramètres** après s'être connecté au système.

7. Dans la zone déroulante **Groupes d'utilisateurs**, cochez la case de chaque groupe d'utilisateurs à affecter à l'utilisateur.

   Remarque : le système est livré avec un ensemble de groupes d'utilisateurs pré-définis, correspondant à chacun des rôles disponibles, à savoir **Administrators** (Groupe d'utilisateurs > rôle

Administrator), Site **Operators** (Groupe d'utilisateur > rôle **Site Operator**), etc. Pour une explication des rôles disponibles, voir Utilisateurs locaux.

8. Cliquez sur **Créer**.

   OT Security crée le nouveau compte utilisateur dans le système et l'ajoute à la liste des utilisateurs dans l'onglet **Utilisateurs locaux**.

Actions supplémentaires sur les comptes utilisateur

Modifier un compte utilisateur

Vous pouvez affecter un utilisateur à des groupes utilisateur supplémentaires ou retirer l'utilisateur d'un groupe.

Pour modifier les groupes utilisateur d'un utilisateur :

1. Accédez à **Paramètres locaux** > **Gestion des utilisateurs** > **Utilisateurs locaux**.

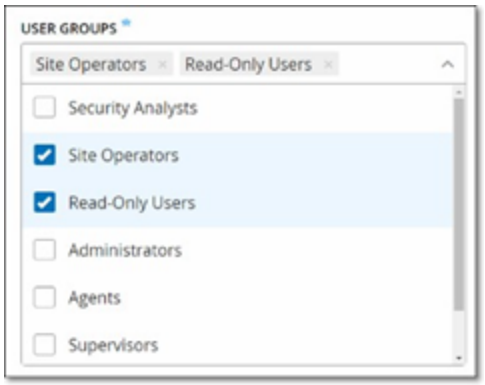
   La page **Utilisateurs locaux** apparaît.

2. Effectuez un clic droit sur l'utilisateur et sélectionnez **Modifier l'utilisateur**.

   Remarque : vous pouvez également sélectionner un utilisateur, puis **Modifier l'utilisateur** dans le menu **Actions**.

3. Le volet **Modifier l'utilisateur** apparaît, indiquant les groupes d'utilisateurs auxquels l'utilisateur est affecté.

4. Dans la zone déroulante **Groupes d'utilisateurs**, sélectionnez ou désélectionnez les groupes d'utilisateurs requis.



5. Cliquez sur **Enregistrer**.

Modifier le mot de passe d'un utilisateur

Remarque : cette procédure permet à un administrateur de changer le mot de passe de n'importe quel compte du système. Un utilisateur peut modifier son propre mot de passe en accédant à **Paramètres locaux** > **Utilisateur**.

Pour modifier le mot de passe d'un utilisateur :

1. Accédez à **Paramètres locaux** > **Gestion des utilisateurs** > **Utilisateurs locaux**.

   La page **Utilisateurs locaux** apparaît.

2. Effectuez un clic droit sur l'utilisateur et sélectionnez **Réinitialiser le mot de passe**.

   Remarque : vous pouvez également sélectionner un utilisateur, puis sélectionner **Réinitialiser le mot de passe** dans le menu **Actions**.

   La fenêtre **Réinitialiser le mot de passe** apparaît.

3. Dans la zone **Nouveau mot de passe**, saisissez un mot de passe.
4. Dans la zone **Confirmer le nouveau mot de passe**, ressaisissez le même nouveau mot de passe.
5. Cliquez sur **Réinitialiser**.

   OT Security applique le nouveau mot de passe au compte utilisateur spécifié.

Supprimer des utilisateurs locaux

Pour supprimer un compte utilisateur :

1. Accédez à **Paramètres locaux** > **Gestion des utilisateurs** > **Utilisateurs locaux**.

   La page **Utilisateurs locaux** apparaît.
2. Effectuez un clic droit sur l'utilisateur et sélectionnez **Supprimer l'utilisateur**.

   > **Remarque :** vous pouvez également sélectionner un utilisateur, puis **Supprimer l'utilisateur** dans le menu **Actions**.

   Une fenêtre de confirmation apparaît.
3. Cliquez sur **Supprimer**.

   OT Security supprime le compte utilisateur du système.

Groupes d'utilisateurs

Un utilisateur administrateur peut créer de nouveaux groupes d'utilisateurs et modifier les groupes existants. Chaque utilisateur est affecté à un ou plusieurs groupes d'utilisateurs qui déterminent son ou ses rôles.

Le système est livré avec un ensemble de groupes d'utilisateurs pré-définis, correspondant à chacun des rôles disponibles, à savoir Administrators (Groupe d'utilisateurs > rôle Administrator), Site Operators (Groupe d'utilisateurs > rôle Site Operator), etc. Pour une explication des rôles disponibles, voir Rôles d'utilisateur.

Affichage des groupes d'utilisateurs

La page Groupes d'utilisateurs affiche une liste de tous les groupes d'utilisateurs du système.

Elle contient les informations suivantes :

Paramètre	Description
Nom	Le nom du groupe d'utilisateurs.
Membres	Une liste de tous les membres affectés au groupe.
Rôle	Le rôle donné à ce groupe. Pour une explication des autorisations associées à chaque rôle, voir Tableau des rôles d'utilisateurs.

Ajouter des groupes d'utilisateurs

Vous pouvez créer des groupes d'utilisateurs et affecter des utilisateurs à ce groupe.

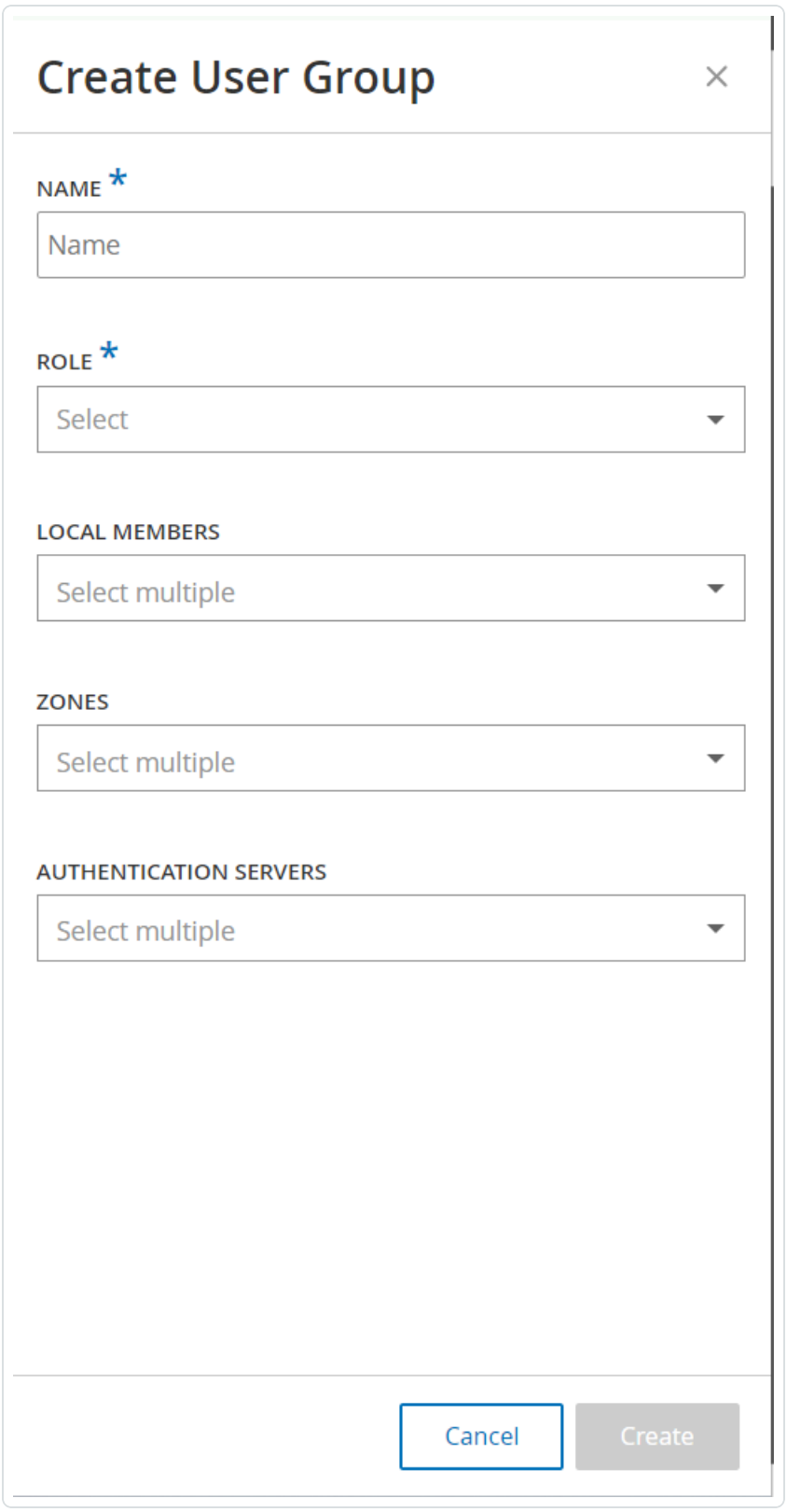
Pour créer un groupe d'utilisateurs :

1. Accédez à **Paramètres locaux** > **Gestion des utilisateurs** > **Groupes d'utilisateurs**.

   L'écran **Groupes d'utilisateurs** apparaît.

2. Cliquez sur **Créer un groupe d'utilisateurs**.

   Le volet **Créer un groupe d'utilisateurs** apparaît.



3. Dans la zone **Nom**, saisissez le nom du groupe.

4. Dans la zone déroulante **Rôle**, sélectionnez le rôle que vous souhaitez affecter à ce groupe. Les rôles disponibles sont les suivants :
    - Lecture seule
    - Analyste sécurité
    - Responsable sécurité
    - Opérateur de site
    - Superviseur
5. Dans la zone déroulante **Membres locaux**, sélectionnez les comptes utilisateur à affecter au groupe.
6. Dans la zone déroulante **Zones**, sélectionnez les zones à affecter au groupe d'utilisateurs.
7. Dans la zone déroulante **Serveurs d'authentification**, sélectionnez les serveurs à affecter au groupe d'utilisateurs.
8. Cliquez sur **Créer**.

    OT Security crée le groupe d'utilisateurs dans le système et l'ajoute à la liste des groupes affichés sur l'écran **Groupes d'utilisateurs**.

Actions supplémentaires sur les groupes d'utilisateurs

Modifier des groupes d'utilisateurs

Vous pouvez modifier les paramètres, ajouter ou supprimer des membres à un groupe d'utilisateurs existant en modifiant le groupe.

> **Remarque :** vous pouvez également sélectionner un utilisateur, puis **Supprimer l'utilisateur** dans le menu **Actions**.

Pour modifier un groupe d'utilisateurs :

1. Accédez à **Paramètres locaux** > **Gestion des utilisateurs** > **Groupes d'utilisateurs**.

    L'écran **Groupes d'utilisateurs** apparaît.

2. Effectuez l'une des actions suivantes :

   - Effectuez un clic droit sur le groupe d'utilisateurs et sélectionnez **Modifier**.
   - Sélectionnez le groupe d'utilisateurs que vous souhaitez modifier. Le menu **Actions** apparaît. Sélectionnez **Actions** > **Modifier**.

   Le volet **Modifier le groupe d'utilisateur** apparaît, indiquant les paramètres du groupe.

3. Modifiez le **nom** et le **rôle**. Vous pouvez également sélectionner ou effacer des utilisateurs pour les ajouter ou les supprimer dans le groupe.

4. Modifiez les paramètres selon les besoins.
5. Cliquez sur **Enregistrer**.

Supprimer des groupes d'utilisateurs

Remarque : vous ne pouvez supprimer qu'un groupe d'utilisateurs auquel aucun utilisateur n'est actuellement affecté. Si des utilisateurs sont affectés à un groupe, vous devez d'abord retirer les utilisateurs du groupe avant de pouvoir le supprimer.

Pour supprimer un groupe d'utilisateurs :

1. Accédez à **Paramètres locaux** > **Gestion des utilisateurs** > **Groupes d'utilisateurs**.

   L'écran **Groupes d'utilisateurs** apparaît.

2. Effectuez l'une des actions suivantes :

- Effectuez un clic droit sur le groupe d'utilisateur et sélectionnez **Supprimer**.
- Sélectionnez le groupe d'utilisateurs que vous souhaitez supprimer. Le menu **Actions** apparaît. Sélectionnez **Actions** > **Supprimer**.

Une fenêtre de confirmation apparaît.

3. Cliquez sur **Supprimer**.

   OT Security supprime le **groupe d'utilisateurs**.

Rôles d'utilisateur

Les rôles suivants sont disponibles :

- **Administrators** (Administrateurs) – Dispose du maximum de privilèges pour effectuer toutes les tâches opérationnelles et administratives dans le système, y compris la création de comptes utilisateur.
- **Read-Only Users** (Utilisateurs en lecture seule) – Peut afficher les données (inventaire des assets, événements, trafic réseau) mais ne peut pas agir dans le système.
- **Security Analysts** (Analystes sécurité) – Peut afficher les données dans le système et résoudre les événements de sécurité.
- **Security Managers** (Responsables sécurité) – Peut gérer toutes les fonctionnalités liées à la sécurité, y compris la configuration des politiques, l'affichage des données dans le système et la résolution des événements.
- **Site Operators** (Opérateurs de site) – Peut afficher les données dans le système et gérer l'inventaire des assets.
- **Supervisors** (Superviseurs) – Dispose de tous les privilèges pour effectuer toutes les tâches opérationnelles du système ainsi que certaines tâches administratives limitées (à l'exception de la création de nouveaux utilisateurs et d'autres activités sensibles).

Tableau des rôles d'utilisateurs

Le tableau suivant donne une répartition détaillée des autorisations précisément activées pour chaque rôle.

Autorisation	Administrateur	Administrateur

	(local)	(externe/ AD)
Événements		
Afficher les événements	✓	✓
Résoudre	✓	✓
Télécharger le fichier de capture	✓	✓
Exclure de la politique	✓	✓
Tout résoudre	✓	✓
Exporter	✓	✓
Créer une politique sur FortiGate	✓	✓
Actualiser	✓	✓
Politiques		
Afficher les politiques	✓	✓
Activer/ Désactiver	✓	✓
Afficher l'action	✓	✓
Modifier	✓	✓
Dupliquer	✓	✓
Supprimer	✓	✓
Créer une politique	✓	✓
Exporter	✓	✓
Assets		
Afficher les assets	✓	✓
Afficher l'action	✓	✓

Modifier	✓	✓
Supprimer	✓	✓
Importer (charger de nouveaux assets via csv)	✓	✓
Masquer	✓	✓
Exporter	✓	✓
Resynchroniser	✓	✓
Scan Nessus	✓	✓
Prendre un instantané (un seul asset)	✓	✓
Mettre à jour les ports ouverts (un seul asset)	✓	✓
Mettre à jour l'état des ports (un seul asset)	✓	✓
Afficher dans le navigateur (un seul asset)	✓	✓
Afficher dans la carte des assets principaux (un seul asset)	✓	✓
Générer un vecteur d'attaque (un seul asset)	✓	✓
Vulnérabilités (Plug-ins)		
Afficher les correspondances de plug-in	✓	✓
Afficher l'action	✓	✓
Modifier le commentaire	✓	✓
Mettre à jour l'ensemble de plug-ins	✓	✓

Exporter	✓	✓
Réseau		
Activer la capture de paquets	✓	✓
Fermer les captures en cours	✓	✓
Télécharger le fichier PCAP	✓	✓
Exporter le tableau des communications	✓	✓
Définir comme base de référence	✓	✓
Générer une cartographie	✓	✓
Actualiser la cartographie	✓	✓
Groupes		
Afficher les groupes	✓	✓
Afficher l'action	✓	✓
Modifier	✓	✓
Dupliquer	✓	✓
Supprimer	✓	✓
Créer un groupe	✓	✓
Exporter	✓	✓
Rapport		
Afficher les rapports	✓	✓
Générer	✓	✓
Télécharger	✓	✓
Exporter	✓	✓

Segments réseau		
Afficher les segments réseau	✓	✓
Modifier	✓	✓
Supprimer	✓	✓
Créer	✓	✓
Exporter	✓	✓
En savoir plus	✓	✓
Paramètres locaux		
Requêtes	✓	✓
Configuration système – Détails de l'appareil	✓	✓
Configuration système – Capteurs	✓	✓
Configuration système – Configuration des ports	✓	✓
Configuration système –Mises à jour	✓	✓
Configuration système – Certificat (HTTPS)	✓	✓
Configuration système – Clés API	✓	✗
Configuration système – Licence	✓	✓
Configuration de l'environnement – Paramètres de l'asset	✓	✓
Configuration de l'environnement – Assets masqués	✓	✓
Configuration de l'environnement – Champs personnalisés	✓	✓

Configuration de l'environnement – Clusters d'événements	✓	✓
Configuration de l'environnement – Lecteur PCAP	✓	✓
Utilisateurs et rôles – Paramètres de l'utilisateur	✓	✓
Utilisateurs et rôles – Utilisateurs locaux	✓	✗
Utilisateurs et rôles – Groupes d'utilisateurs	✓	✗
Utilisateurs et rôles – Active Directory	✓	✗
Intégrations	✓	✓
Serveurs	✓	✓
Actions système	✓	✓ sans réinitialisation des paramètres d'usine
Journal système	✓	✓
Activer (lors de la configuration et après la désactivation)	✓	✓
Supprimer les assets	✓	✓

Autorisation	Superviseur	Responsable sécurité	Analyste sécurité	Opérateur de site	Lecture seule
Événements					
Afficher les événements	✓	✓	✓	✓	✓
Résoudre	✓	✓	✓	✗	✗
Télécharger le	✓	✓	✓	✓	✓

fichier de capture					
Exclure de la politique	✓	✓	✗	✗	✗
Tout résoudre	✓	✓	✓	✗	✗
Exporter	✓	✓	✓	✓	✓
Créer une politique sur FortiGate	✓	✓	✗	✗	✗
Actualiser	✓	✓	✓	✓	✓
Politiques					
Afficher les politiques	✓	✓	✓	✓	✓
Activer/ Désactiver	✓	✓	✗	✗	✗
Afficher l'action	✓	✓	✓	✓	✓
Modifier	✓	✓	✗	✗	✗
Dupliquer	✓	✓	✗	✗	✗
Supprimer	✓	✓	✗	✗	✗
Créer une politique	✓	✓	✗	✗	✗
Exporter	✓	✓	✓	✓	✓
Assets					
Afficher les assets	✓	✓	✓	✓	✓

Afficher l'action	✓	✓	✓	✓	✓
Modifier	✓	✗	✗	✓	✗
Supprimer	✓	✗	✗	✓	✗
Importer (charger de nouveaux assets via csv)	✓	✗	✗	✓	✗
Masquer	✓	✗	✗	✓	✗
Exporter	✓	✓	✓	✓	✓
Resynchroniser	✓	✓	✓	✓	✗
Scan Nessus	✓	✓	✓	✓	✗
Prendre un instantané (un seul asset)	✓	✓	✓	✓	✗
Mettre à jour les ports ouverts (un seul asset)	✓	✓	✓	✗	✗
Mettre à jour l'état des ports (un seul asset)	✓	✓	✓	✗	✗
Afficher dans le navigateur (un seul asset)	✓	✓	✓	✓	✓
Afficher dans la carte des assets principaux (un seul asset)	✓	✓	✓	✓	✓

Générer un vecteur d'attaque (un seul asset)	✓	✓	✓	✓	✓
Vulnérabilités (Plug-ins)					
Afficher les correspondances de plug-in	✓	✓	✓	✓	✓
Afficher l'action	✓	✓	✓	✓	✓
Modifier le commentaire	✓	✓	✓	✗	✗
Mettre à jour l'ensemble de plug-ins	✓	✓	✗	✗	✗
Exporter	✓	✓	✓	✓	✓
Réseau					
Activer la capture de paquets	✓	✗	✗	✗	✗
Fermer les captures en cours	✓	✓	✓	✓	✗
Télécharger le fichier PCAP	✓	✓	✓	✓	✓
Exporter le tableau des communications	✓	✓	✓	✓	✓
Définir comme	✓	✓	✗	✗	✗

base de référence					
Générer une cartographie	✓	✓	✓	✓	✓
Actualiser la cartographie	✓	✓	✓	✓	✓
Groupes					
Afficher les groupes	✓	✓	✓	✓	✓
Afficher l'action	✓	✓	✓	✓	✓
Modifier	✓	✓	✗	✗	✗
Dupliquer	✓	✓	✗	✗	✗
Supprimer	✓	✓	✗	✗	✗
Créer un groupe	✓	✓	✗	✗	✗
Exporter	✓	✓	✓	✓	✓
Rapport					
Afficher les rapports	✓	✓	✓	✓	✓
Générer	✓	✓	✓	✓	✓
Télécharger	✓	✓	✓	✓	✓
Exporter	✓	✓	✓	✓	✓
Segments réseau					
Afficher les segments réseau	✓	✓	✓	✓	✓

Modifier	✓	✓	✗	✗	✗
Supprimer	✓	✓	✗	✗	✗
Créer	✓	✓	✗	✗	✗
Exporter	✓	✓	✓	✓	✓
En savoir plus	✓	✓	✓	✓	✓
Paramètres locaux					
Requêtes	✓	✗	✗	✗	✗
Configuration système – Détails de l'appareil	✓	✗	✗	✗	✗
Configuration système – Capteurs	✓	✓ (Aucune action)	✓ (Aucune action)	✓ (Aucune action)	✓ (Aucune action)
Configuration système – Configuration des ports	✓	✗	✗	✗	✗
Configuration système –Mises à jour	✓	✗	✗	✗	✗
Configuration système – Certificat (HTTPS)	✗	✗	✗	✗	✗
Configuration système – Clés API	✓ (Utilisateurs locaux	✓ (Utilisateurs locaux	✓ (Utilisateurs locaux	✓ (Utilisateurs locaux	✓ (Utilisateurs locaux

	uniquement)	uniquement)	uniquement)	uniquement)	uniquement)
Configuration système – Licence	✗	✗	✗	✗	✗
Configuration de l'environnement – Paramètres de l'asset	✓	✗	✗	✗	✗
Configuration de l'environnement – Assets masqués	✓	✓ - pas de restauration	✓ - pas de restauration	✓	✓ - pas de restauration
Configuration de l'environnement – Champs personnalisés	✓	✗	✗	✗	✗
Configuration de l'environnement – Clusters d'événements	✓	✗	✗	✗	✗
Configuration de l'environnement – Lecteur PCAP	✓	✗	✗	✗	✗
Utilisateurs et rôles – Paramètres de l'utilisateur	✓	✗	✗	✗	✗
Utilisateurs et rôles –	✗	✗	✗	✗	✗

Utilisateurs locaux					
Utilisateurs et rôles – Groupes d'utilisateurs	✗	✗	✗	✗	✗
Utilisateurs et rôles – Active Directory	✗	✗	✗	✗	✗
Intégrations	✗	✗	✗	✗	✗
Serveurs	✓	✓ (Aucune action)	✓ (Aucune action)	✓ (Aucune action)	✓ (Aucune action)
Actions système	✓ sauvegarde et diagnostics uniquement	✓ diagnostics uniquement	✗	✗	✗
Journal système	✓	✓	✓	✓	✓ pas de journal syslog
Activer (lors de la configuration et après la désactivation)	✗	✗	✗	✗	✗
Supprimer les assets	✓	✗	✗	✗	✗

Zones

Les zones contrôlent les assets, les événements et les vulnérabilités qu'un groupe d'utilisateurs donné peut afficher. Un groupe d'utilisateurs spécifique ne peut afficher que les assets et les vulnérabilités, événements et connexions associés qui se trouvent dans sa zone. Vous pouvez attribuer des comptes non-administrateurs à un groupe et à une zone spécifiques pour limiter leur visibilité aux assets en question.

Créer des zones

Pour créer des zones :

1. Accédez à **Paramètres locaux** > **Gestion des utilisateurs** > **Zones**.

   La page **Zones** apparaît.

2. Dans le coin supérieur droit, cliquez sur **Créer**.

   Le panneau **Créer une zone** apparaît.

3. Dans la zone **Nom**, saisissez le nom de la zone.

4. Dans la zone **Groupes d'assets**, sélectionnez les groupes à affecter à la zone. Vous pouvez utiliser la zone de recherche pour rechercher un groupe d'assets spécifique.

5. Dans la zone **Groupes d'assets**, sélectionnez les groupes d'utilisateurs à affecter à la zone.

6. (Facultatif) Dans la zone **Description**, saisissez la description de la zone.

7. Cliquez sur **Créer**.

   OT Security crée la zone qui apparaît ensuite sur la page **Zones**.

Afficher des zones

1. Accédez à **Paramètres locaux** > **Gestion des utilisateurs** > **Zones**.

   La page **Zones** apparaît. La page **Zones** affiche les zones sous forme de tableau et fournit les détails suivants.

Colonne	Description
Nom	Le nom de la zone.

Groupes d'assets	Les groupes d'assets affectés à la zone.
Groupes d'utilisateurs	Les groupes d'utilisateurs affectés à la zone.
Description	Une description de la zone.
Dernière modification par	L'utilisateur qui a modifié la zone en dernier.
Dernière modification le	La date à laquelle la zone a été modifiée pour la dernière fois.

Modifier une zone

1. Accédez à **Paramètres locaux** > **Gestion des utilisateurs** > **Zones**.

   La page **Zones** apparaît.

2. Cliquez sur la ligne de la zone à modifier et effectuez l'une des opérations suivantes :

   - Effectuez un clic droit sur la zone et sélectionnez **Modifier**.
   - Cliquez sur **Actions** > **Modifier** dans la barre d'en-tête.

   Le panneau **Modifier la zone** apparaît.

3. Modifiez la configuration selon les besoins.
4. Cliquez sur **Enregistrer**.

   OT Security met à jour la zone.

Dupliquer une zone

1. Accédez à **Paramètres locaux** > **Gestion des utilisateurs** > **Zones**.

   La page **Zones** apparaît.

2. Cliquez sur la ligne de la zone à dupliquer et effectuez l'une des opérations suivantes :

   - Effectuez un clic droit sur la zone et sélectionnez **Dupliquer**.
   - Cliquez sur **Actions** > **Dupliquer** dans la barre d'en-tête.

Le panneau **Dupliquer la zone** apparaît.

3. Dans la zone **Nom**, saisissez le nom de la zone.

   La valeur par défaut est le nom de la zone d'origine avec le préfixe « Copie de ».

4. Modifiez la configuration selon les besoins.

5. Cliquez sur **Dupliquer**.

   OT Security crée un double de la zone.

Supprimer une zone

Vous pouvez supprimer les zones dont vous n'avez plus besoin.

Remarque : vous ne pouvez pas supprimer une zone si des groupes d'utilisateurs lui sont associés.

1. Accédez à **Paramètres locaux** > **Gestion des utilisateurs** > **Zones**.

   La page **Zones** apparaît.

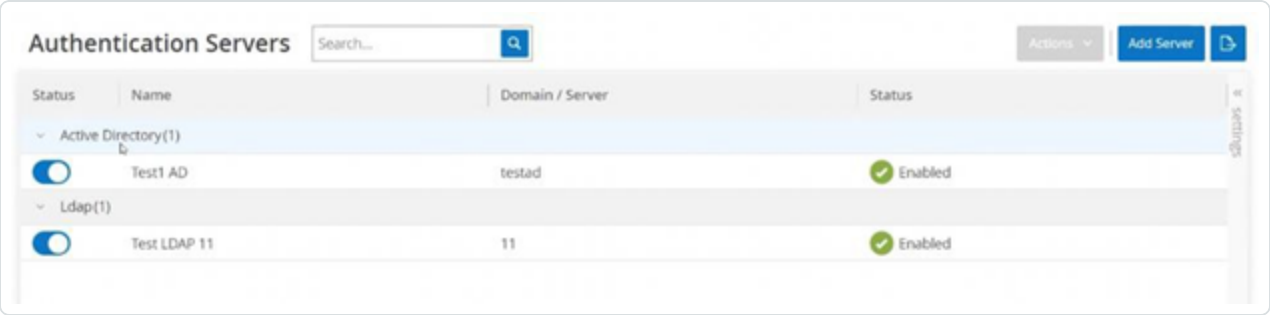
2. Cliquez sur la ligne de la zone à supprimer et effectuez l'une des opérations suivantes :

   - Effectuez un clic droit sur la zone et sélectionnez **Supprimer**.
   - Cliquez sur **Actions** > **Supprimer** dans la barre d'en-tête.

   OT Security supprime la zone.

Serveurs d'authentification

La page **Serveurs d'authentification** affiche vos intégrations existantes avec des serveurs d'authentification. Vous pouvez ajouter un serveur en cliquant sur le bouton **Ajouter un serveur**.



Active Directory

Vous pouvez intégrer OT Security à l'Active Directory de votre organisation. Cela permet aux utilisateurs de se connecter à OT Security à l'aide de leurs identifiants Active Directory. La configuration implique la définition de l'intégration, puis le mappage des groupes au sein de votre AD aux groupes d'utilisateurs dans OT Security.

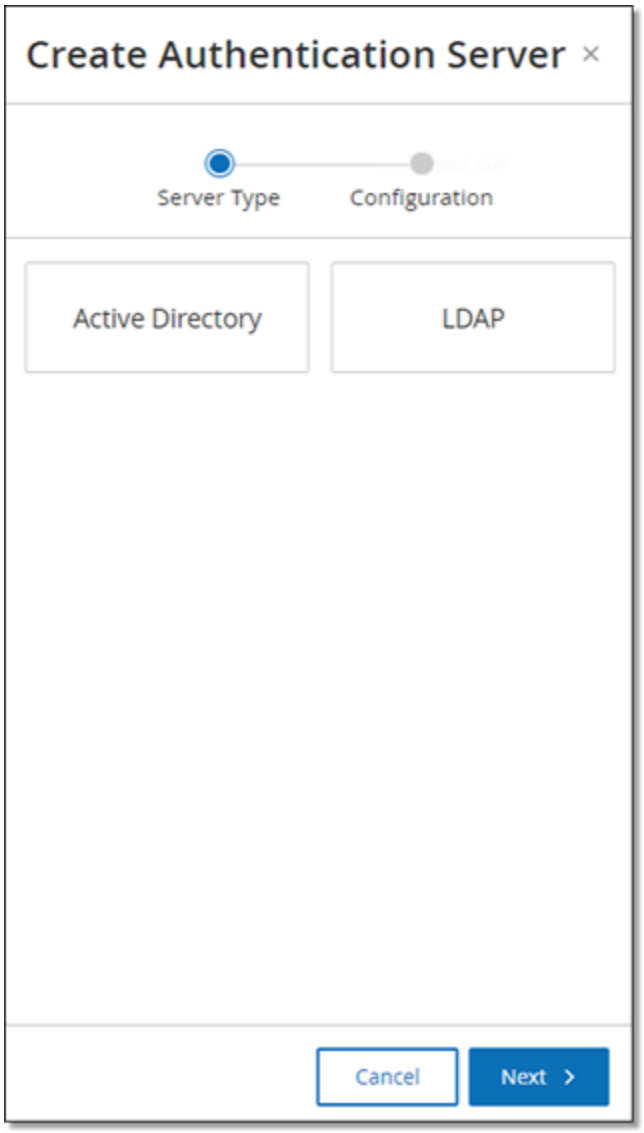
Remarque : le système est fourni avec des groupes d'utilisateurs prédéfinis qui correspondent à chacun des rôles disponibles, à savoir **Administrateurs (Groupe d'utilisateurs** > **rôle Administrateur**), **Opérateurs de site (Groupe d'utilisateurs** > **rôle Opérateur de site**), etc. Pour une explication des rôles disponibles, voir Serveurs d'authentification.

Pour configurer Active Directory :

1. En option, vous pouvez obtenir un certificat CA auprès de l'autorité de certification ou de l'administrateur réseau de votre organisation et le charger sur votre ordinateur local.
2. Accédez à **Paramètres locaux** > **Gestion des utilisateurs** > **Serveurs d'authentification**.

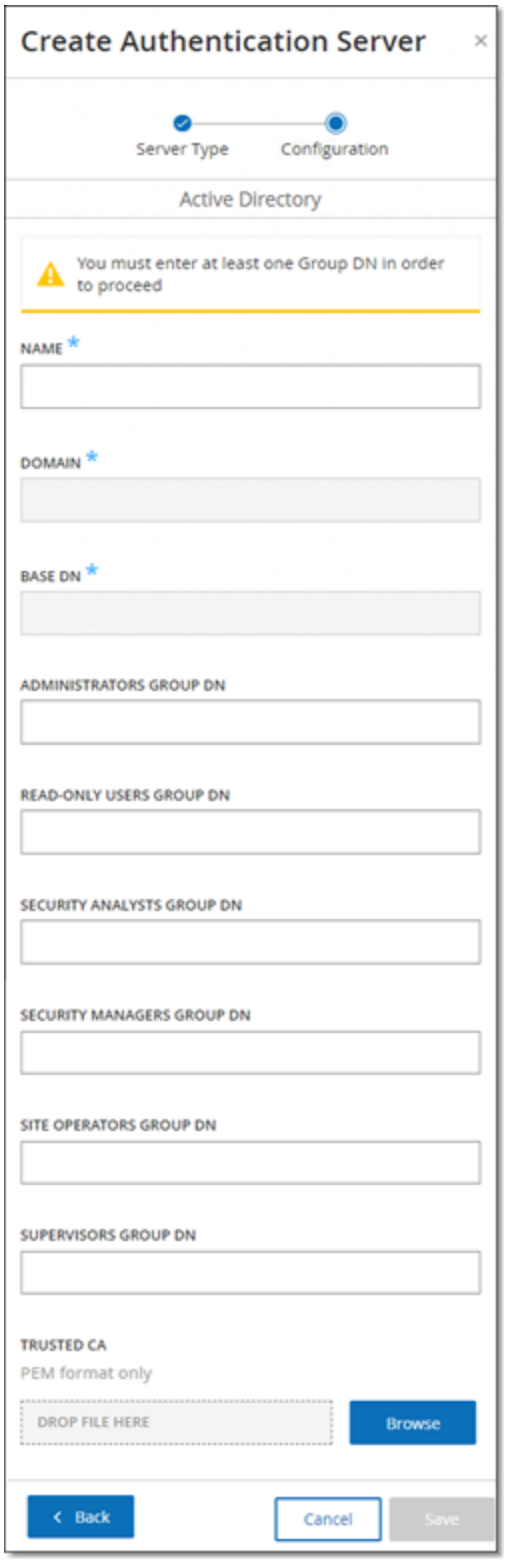
   La fenêtre **Serveurs d'authentification** apparaît.
3. Cliquez sur **Ajouter un serveur**.

   Le panneau **Créer un serveur authentification** apparaît avec le volet **Type de serveur**.



4. Cliquez sur **Active Directory**, puis sur **Suivant**.

   Le volet de configuration d'**Active Directory** apparaît.



5. Dans la zone **Nom**, saisissez le nom à utiliser sur l'écran de connexion.

6. Dans la zone **Domaine**, saisissez le FQDN du domaine de l'organisation (par exemple, société.com).

   Remarque : si vous ne connaissez pas votre nom de domaine, vous pouvez le trouver en saisissant la commande « set » dans l'invite de commandes ou Windows CMD. La valeur donnée pour l'attribut « USERDNSDOMAIN » est le nom de domaine.

7. Dans la zone **DN de base**, saisissez le nom distinctif du domaine. Le format de cette valeur est « DC={domaine de second niveau},DC={domaine de premier niveau} » (par exemple DC=société,DC=com).

8. Pour chacun des groupes que vous souhaitez mapper d'un groupe AD à un groupe d'utilisateurs OT Security, saisissez le DN du groupe AD dans la zone appropriée.

   Par exemple, pour affecter un groupe d'utilisateurs au groupe d'utilisateurs Administrateurs, saisissez le DN du groupe Active Directory auquel vous souhaitez attribuer des privilèges d'administrateur dans la zone **DN du groupe Administrateurs**.

   Remarque : si vous ne connaissez pas le DN du groupe auquel vous souhaitez attribuer des privilèges OT Security, vous pouvez afficher la liste de tous les groupes configurés dans votre infrastructure Active Directory qui contiennent des utilisateurs, en entrant la commande `dsquery group -name Users*` dans l'invite de commande ou Windows CMD. Saisissez le nom du groupe que vous souhaitez attribuer dans le même format que celui dans lequel il est affiché (par exemple « CN=IT_Admins,OU=Groupes,DC=Société,DC=Com »). Le DN de base doit également être inclus à la fin de chaque DN.

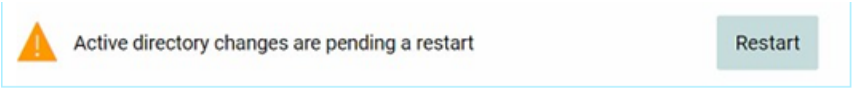
   Remarque : ces champs sont facultatifs. Si un champ est vide, aucun utilisateur AD n'est affecté à ce groupe d'utilisateurs. Vous pouvez configurer une intégration sans groupe mappé, mais dans ce cas, aucun utilisateur ne peut accéder au système tant que vous n'avez pas ajouté au moins un ping de mappage de groupe.

9. (Facultatif) Dans la section **CA de confiance**, cliquez sur **Parcourir** et accédez au fichier contenant le certificat CA de votre organisation (que vous avez obtenu de votre autorité de certification ou de votre administrateur réseau)

10. Cochez la case **Activer Active Directory**.

11. Cliquez sur **Enregistrer**.

    Un message vous invite à redémarrer l'unité afin d'activer Active Directory.



12. Cliquez sur **Redémarrer**.

    L'unité redémarre. Au redémarrage, OT Security active les paramètres d'Active Directory. Tout utilisateur affecté aux groupes désignés peut accéder à la plateforme OT Security à l'aide de ses identifiants d'entreprise.

    > **Remarque :** pour vous connecter à l'aide d'Active Directory, le nom d'utilisateur principal (UPN) doit être utilisé sur la page de connexion. Dans certains cas, cela revient simplement à ajouter @<domaine>.com au nom d'utilisateur.

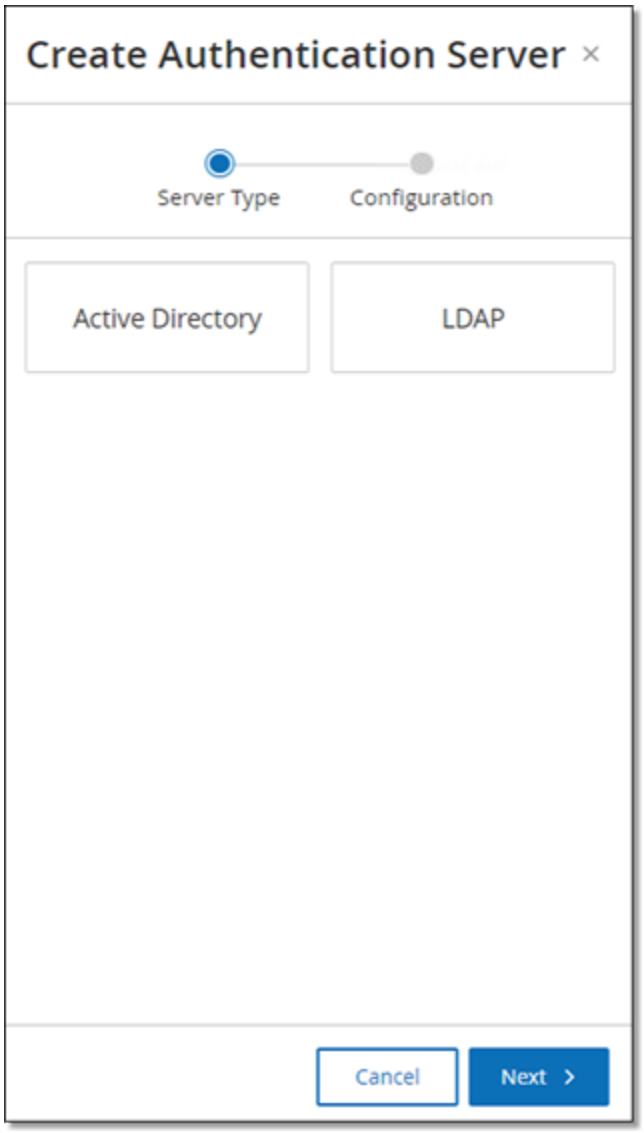
LDAP

Vous pouvez intégrer OT Security au LDAP de votre organisation. Ainsi, les utilisateurs peuvent se connecter à OT Security en utilisant leurs informations d'authentification LDAP. La configuration implique la définition de l'intégration, puis le mappage des groupes au sein de votre AD aux groupes d'utilisateurs dans OT Security.

Pour configurer LDAP :

1. Accédez à **Paramètres locaux** > **Gestion des utilisateurs** > **Serveurs d'authentification**.
2. Cliquez sur **Ajouter un serveur**.

   Le panneau **Ajouter un serveur d'authentification** apparaît avec le **Type de serveur**.



3. Sélectionnez **LDAP**, puis cliquez sur **Suivant**.

   Le volet **Configuration LDAP** apparaît.

4. Dans la zone **Nom**, saisissez le nom à utiliser sur l'écran de connexion.

   > **Remarque :** le nom de connexion doit être distinctif et indiquer qu'il est utilisé pour LDAP. Dans le cas où LDAP et Active Directory sont configurés, seul le nom de connexion différencie les différentes configurations sur l'écran de connexion.

5. Dans la zone **Serveur**, saisissez le FQDN ou l'adresse de connexion.

Remarque : si vous utilisez une connexion sécurisée, Tenable recommande d'utiliser le FQDN et non pas une adresse IP, afin que le certificat sécurisé fourni soit vérifié.

Remarque : si un nom d'hôte est utilisé, il doit figurer dans la liste des serveurs DNS du système OT Security. Voir Configuration système > Appareil.

6. Dans la zone **Port**, saisissez 389 pour utiliser une connexion non sécurisée, ou 636 pour utiliser une connexion SSL sécurisée.

   Remarque : si le port 636 est choisi, un certificat est requis pour terminer l'intégration.

7. Dans la zone **DN de l'utilisateur**, saisissez le DN avec les paramètres au format DN. Par exemple, pour le nom de serveur adsrv1tenable.com, le DN de l'utilisateur peut être `CN=Administrateur,CN=Utilisateurs,DC=adsrv1,DC=tenable,DC=com`.

8. Dans la zone **Mot de passe**, saisissez le mot de passe du DN de l'utilisateur.

   Remarque : la configuration OT Security avec LDAP ne fonctionne que si le mot de passe du DN de l'utilisateur est valide. Par conséquent, en cas de changement ou d'expiration du mot de passe du DN de l'utilisateur, la configuration OT Security doit également être mise à jour.

9. Dans la zone **DN de base de l'utilisateur**, saisissez le nom de domaine de base au format DN. Par exemple, pour le nom de serveur adsrv1tenable.com, le DN de base de l'utilisateur est `OU=Utilisateurs,DC=adsrv1,DC=tenable,DC=com`.

10. Dans la zone **DN de base du groupe**, saisissez le nom de domaine de base du groupe au format DN. Par exemple, pour le nom de serveur adsrv1tenable.com, le DN de base du groupe est `OU=Groupes,DC=adsrv1,DC=tenable,DC=com`.

11. Dans la zone **Ajout de domaine**, saisissez le domaine par défaut qui est ajouté à la demande d'authentification dans le cas où l'utilisateur n'a pas appliqué un domaine dont il est membre.

12. Dans les zones appropriées de nom de groupe, saisissez les noms de groupe Tenable que doit utiliser l'utilisateur avec la configuration LDAP.

13. Si vous utilisez le port 636 pour la configuration, sous **CA de confiance**, cliquez sur **Parcourir** et accédez à un fichier de certificat PEM valide.

14. Cliquez sur **Enregistrer**.

OT Security démarre le serveur en mode **désactivé**.

15. Pour appliquer la configuration, **activez** le curseur.

    La boîte de dialogue **Redémarrage du système** apparaît.

16. Cliquez sur **Redémarrer maintenant** pour redémarrer et appliquer la configuration immédiatement, ou sur **Redémarrer ultérieurement** pour continuer temporairement à utiliser le système sans la nouvelle configuration.

    > **Remarque :** l'activation/la désactivation de la configuration LDAP n'est pas terminée tant que le système n'a pas redémarré. Si vous ne redémarrez pas le système immédiatement, cliquez sur le bouton **Redémarrer** sur la bannière en haut de l'écran lorsque vous êtes prêt à redémarrer.

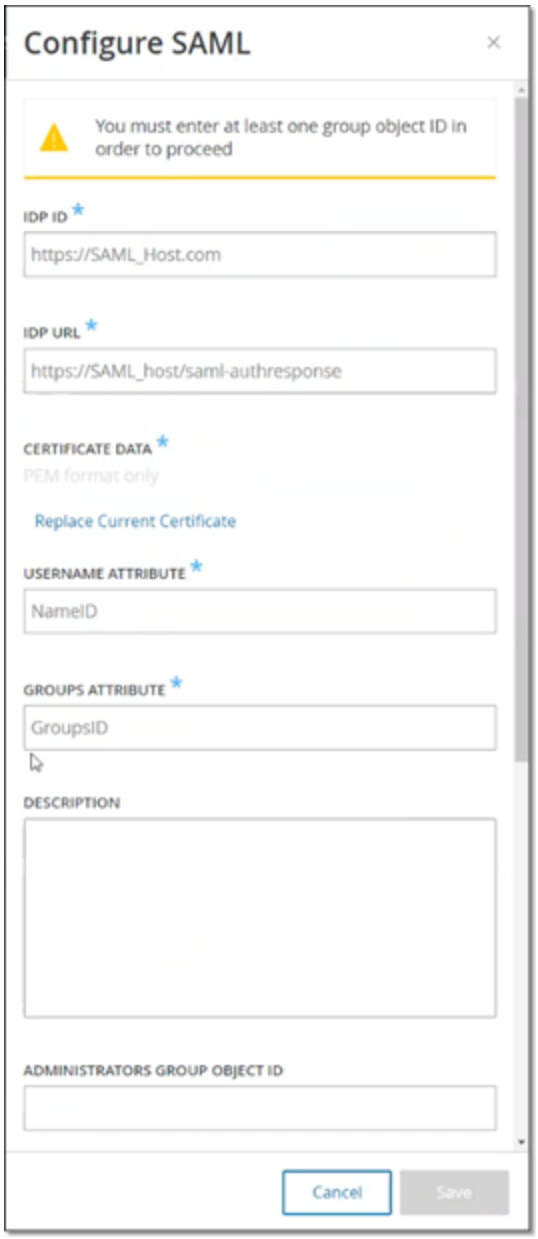
SAML

Vous pouvez intégrer OT Security au fournisseur d'identité de votre organisation (par exemple, Microsoft Azure). Cela permet aux utilisateurs de s'authentifier via leur fournisseur d'identité. La configuration implique la mise en place de l'intégration en créant une application OT Security au sein de votre fournisseur d'identité. Ensuite, vous devrez saisir des informations sur votre application OT Security nouvellement créée, puis charger le certificat de votre fournisseur d'identité à la page **SAML** de OT Security, et enfin mapper les groupes de votre fournisseur d'identité aux groupes d'utilisateurs dans OT Security. Pour accéder à un tutoriel détaillé sur l'intégration de OT Security à Microsoft Azure, voir Annexe – Intégration SAML pour Microsoft Azure.

Pour configurer SAML :

1. Accédez à **Paramètres locaux** > **Gestion des utilisateurs** > **SAML**.
2. Cliquez sur **Configurer.**.

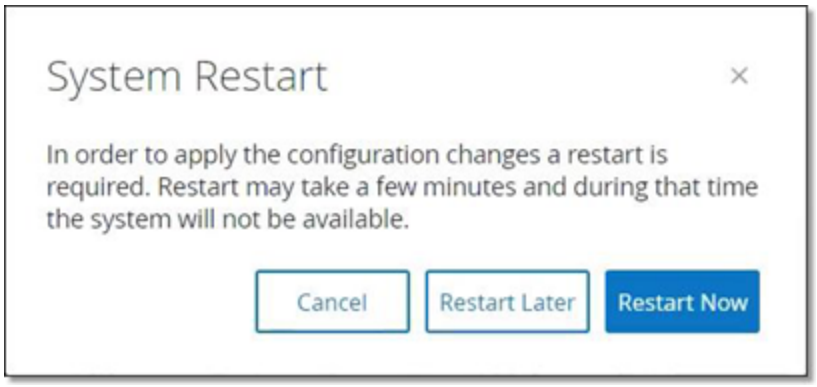
   Le panneau **Configurer SAML** apparaît.



3. Dans la zone **ID IDP**, saisissez l'identifiant du fournisseur d'identité de l'application OT Security.
4. Dans la zone **URL IDP**, saisissez l'URL du fournisseur d'identité de l'application OT Security.
5. Dans **Données de certificat**, cliquez sur **Déposer le fichier ici**, accédez au fichier de certificat du fournisseur d'identité que vous avez téléchargé pour l'utiliser avec l'application OT Security et ouvrez-le.
6. Dans la zone **Attribut de nom d'utilisateur**, saisissez l'attribut de nom d'utilisateur du fournisseur d'identité pour l'application OT Security.

7. Dans la zone **Attribut de nom d'utilisateur**, saisissez l'attribut des groupes du fournisseur d'identité de l'application OT Security.
8. (Facultatif) Dans la zone **Description**, saisissez la description de la requête.
9. Pour chaque mappage de groupe que vous souhaitez configurer, accédez à l'**ID d'objet de groupe** du fournisseur d'identité d'un groupe d'utilisateurs et saisissez-le dans le champ **ID d'objet de groupe** souhaité pour le mapper au groupe d'utilisateurs OT Security souhaité.
10. Cliquez sur **Enregistrer** pour enregistrer et refermer le panneau latéral.
11. Dans la fenêtre **SAML**, cliquez sur le curseur **Connexion unique SAML** pour activer la connexion authentifiée unique.

    La fenêtre de notification de **redémarrage du système** apparaît.



12. Cliquez sur **Redémarrer maintenant** pour redémarrer le système et appliquer la configuration SAML immédiatement, ou cliquez sur **Redémarrer ultérieurement** pour retarder l'application de la configuration SAML au prochain redémarrage du système. Si vous choisissez de redémarrer le système plus tard, OT Security affiche la bannière suivante jusqu'à ce que le redémarrage soit terminé :

    Au redémarrage, les paramètres seront activés et tout utilisateur affecté aux groupes désignés pourra accéder à la plateforme OT Security à l'aide de ses identifiants de fournisseur d'identité.

Intégrations

Vous pouvez configurer des intégrations à d'autres plateformes prises en charge, afin de permettre à OT Security de se synchroniser avec vos autres plateformes de cyber-sécurité.

Produits Tenable

Vous pouvez intégrer OT Security à Tenable Security Center et Tenable Vulnerability Management. OT Security partage des données avec les autres plateformes via ces intégrations. Les données synchronisées incluent les vulnérabilités OT, ainsi que les données découvertes par les scans Tenable Nessus IT lancés à partir de OT Security.

Remarque : OT Security n'envoie pas de données pour les assets **masqués** à Tenable Security Center ni à Tenable Vulnerability Management via l'intégration.

Remarque : pour intégrer les plateformes, OT Security doit pouvoir accéder à Tenable Security Center et/ou Tenable Vulnerability Management via le port 443. Tenable recommande de créer un utilisateur spécifique sur Tenable Security Center et/ou Tenable Vulnerability Management pour l'utiliser comme utilisateur d'intégration à OT Security.

Tenable Security Center

Pour intégrer Tenable Security Center, créez un **référentiel universel** dans Tenable Security Center pour stocker les données OT Security et notez l'ID de référentiel. Pour plus d'informations, voir Universal Repositories (Référentiels universels).

Remarque : Tenable recommande de créer un utilisateur spécifique sur Tenable Security Center qui sera utilisé pour l'intégration à OT Security. L'utilisateur doit avoir le rôle de Responsable sécurité/ Analyste sécurité ou Analyste vulnérabilité et être affecté au groupe « Accès complet ».

Pour effectuer l'intégration à Tenable Security Center :

1. Accédez à **Paramètres locaux** > **Intégrations**.

   La page **Intégrations** s'affiche.

2. Dans le coin supérieur droit, cliquez sur **Ajouter un module d'intégration**.

   Le panneau **Ajouter un module d'intégration** apparaît.

3. Dans la section **Type de modules**, sélectionnez Tenable Security Center.

4. Cliquez sur **Suivant**.

   Le panneau **Définition des modules** apparaît avec les champs pertinents.

5. Dans la zone **Nom d'hôte/ adresse IP**, saisissez le nom d'hôte ou l'adresse IP de votre Tenable Security Center.
6. Dans la zone **Nom d'utilisateur**, saisissez l'ID utilisateur du compte.
7. Dans la zone **Mot de passe**, saisissez le mot de passe de votre compte.
8. Dans **ID de référentiel**, fournissez l'ID de référentiel universel.
9. Dans la zone déroulante **Fréquence de synchronisation**, définissez la fréquence de synchronisation des données.
10. Cliquez sur **Enregistrer**.

    OT Security crée l'intégration et affiche la nouvelle intégration sur la page Intégrations.

11. Effectuez un clic droit sur la nouvelle intégration et cliquez sur **Synchroniser**.

Tenable Vulnerability Management

Remarque : vous devez d'abord générer une clé API dans la console Tenable Vulnerability Management (**Paramètres** > **Mon compte** > **Clés API** > **Générer**). Vous recevez une **clé d'accès** et une **clé secrète** que vous saisissez dans la console OT Security lors de la configuration de l'intégration.

Pour effectuer l'intégration à Tenable Vulnerability Management :

1. Accédez à **Paramètres locaux** > **Intégrations**.

   La page **Intégrations** s'affiche.

2. Dans le coin supérieur droit, cliquez sur **Ajouter un module d'intégration**.

   Le panneau **Ajouter un module d'intégration** apparaît.

3. Dans la section **Type de modules**, sélectionnez Tenable Vulnerability Management.
4. Cliquez sur **Suivant**.

   Le panneau **Définition des modules** apparaît avec les champs pertinents.

5. Dans la zone **Clé d'accès**, saisissez la clé d'accès.
6. Dans la zone **Clé secrète**, saisissez la clé secrète.
7. Dans la zone déroulante **Fréquence de synchronisation**, sélectionnez la fréquence de synchronisation des données.

Tenable One

Pour effectuer l'intégration à Tenable One, suivez les étapes de la section Intégration à Tenable One.

Palo Alto Networks – Pare-feu de nouvelle génération (NGFW)

Vous pouvez partager les informations d'inventaire d'assets découvertes par OT Security avec votre système Palo Alto.

Pour intégrer OT Security à vos pare-feux de nouvelle génération (NGFW) Palo Alto Networks :

1. Accédez à **Paramètres locaux** > **Intégrations**.

   La page **Intégrations** s'affiche.
2. Dans le coin supérieur droit, cliquez sur **Ajouter un module d'intégration**.

   Le panneau **Ajouter un module d'intégration** apparaît.
3. Dans la section **Type de modules**, sélectionnez Palo Alto Networks NGFW.
4. Cliquez sur **Suivant**.
5. Dans la zone **Nom d'hôte/ adresse IP**, saisissez le nom d'hôte ou l'adresse IP de votre compte Palo Alto NGFW.
6. Dans la zone **Nom d'utilisateur**, saisissez le nom d'utilisateur de votre compte NGFW.
7. Dans la zone **Mot de passe**, saisissez le mot de passe de votre compte NGFW.
8. Cliquez sur **Enregistrer**.

   OT Security enregistre l'intégration.

Aruba – Gestionnaire de politiques ClearPass

Vous pouvez partager les informations d'inventaire d'assets découvertes par OT Security avec votre système Aruba.

Pour intégrer OT Security à votre compte Aruba ClearPass :

1. Accédez à **Paramètres locaux** > **Intégrations**.

   La page **Intégrations** s'affiche.

2. Dans le coin supérieur droit, cliquez sur **Ajouter un module d'intégration**.

   Le panneau **Ajouter un module d'intégration** apparaît.

3. Dans la section **Type de modules**, sélectionnez Aruba Networks ClearPass.

4. Cliquez sur **Suivant**.

5. Dans la zone **Nom d'hôte/ adresse IP**, saisissez le nom d'hôte ou l'adresse IP de votre compte Aruba Networks ClearPass.

6. Dans la zone **Nom d'utilisateur**, saisissez le nom d'utilisateur de votre compte Aruba Networks ClearPass.

7. Dans la zone **Mot de passe**, saisissez le mot de passe de votre compte Aruba Networks ClearPass.

8. Dans la zone **ID client**, saisissez l'ID client de votre compte Aruba Networks ClearPass.

9. Dans la zone **Code secret du client API**, saisissez le code secret du client API de votre compte Aruba Networks ClearPass.

10. Cliquez sur **Enregistrer**.

    OT Security enregistre l'intégration.

Intégration à Tenable One

Vous pouvez intégrer OT Security à Tenable One pour envoyer des assets et des données de scores de risque à Tenable Vulnerability Management. Pour effectuer l'intégration à Tenable One, vous devez d'abord générer une clé de liaison dans Tenable Vulnerability Management et la fournir à OT Security. Tenable One est mis à jour périodiquement et reçoit toutes les modifications apportées aux assets depuis la synchronisation précédente.

Avant de commencer

- Vérifiez que vous disposez de la clé de liaison générée dans Tenable Vulnerability Management. Pour plus d'informations, voir OT Connectors (Connecteurs OT) dans le Guide de l'utilisateur Tenable Vulnerability Management.

  Remarque : une clé de liaison générée dans Tenable Vulnerability Management ne peut être utilisée que pour un seul site OT Security.

Pour effectuer l'intégration à Tenable One :

1. Accédez à **Paramètres locaux** > **Intégrations**.

   La page **Intégrations** s'affiche.

2. Dans le coin supérieur droit, cliquez sur **Ajouter un module d'intégration**.

   Le panneau **Ajouter un module d'intégration** apparaît.

3. Dans la section **Type de modules**, cliquez sur **Tenable One**.

4. Cliquez sur **Suivant**.

   La section **Définition des modules** s'affiche.

5. Dans la zone **Site cloud**, saisissez le nom du site cloud.

   Remarque : le nom du site cloud apparaît dans la fenêtre **Ajouter un connecteur OT** dans Tenable Vulnerability Management après la génération de la clé de liaison.

6. Dans la zone **Clé de liaison**, indiquez la clé de liaison que vous avez générée à partir de Tenable Vulnerability Management.

7. Cliquez sur **Enregistrer**.

   OT Security affiche un message indiquant que l'intégration a réussi. Une fois l'intégration terminée, vous pouvez visualiser le site lié sur la page **Intégrations**. Dans Tenable One, la page **Capteurs** > **Connecteurs OT** affiche le nom de l'appareil configuré pour ce site dans OT Security.

   Pour connaître le nom d'appareil d'un site, voir la section **Nom de l'appareil** sur la page **Configuration système** > **Appareil**.

Remarque : si vous modifiez le nom du site dans OT Security après l'appairage, vous pouvez modifier manuellement le nom du capteur dans Tenable Vulnerability Management pour qu'il corresponde au nouveau nom du site. Vous pouvez également supprimer l'intégration sur OT Security et Tenable Vulnerability Management, et procéder à un nouvel appairage pour mettre à jour automatiquement le nom du site.

Pour plus d'informations sur la procédure complète de déploiement et gestion des licences de Tenable OT Security pour Tenable One, voir le Guide de déploiement de Tenable One.

Serveurs

Vous pouvez configurer des serveurs SMTP et des serveurs Syslog dans le système pour permettre aux notifications d'événement d'être envoyées par e-mail et/ou connectées à un SIEM. Vous pouvez également configurer des pare-feu FortiGate afin d'envoyer des suggestions de politique de pare-feu à FortiGate en fonction des événements réseau de OT Security.

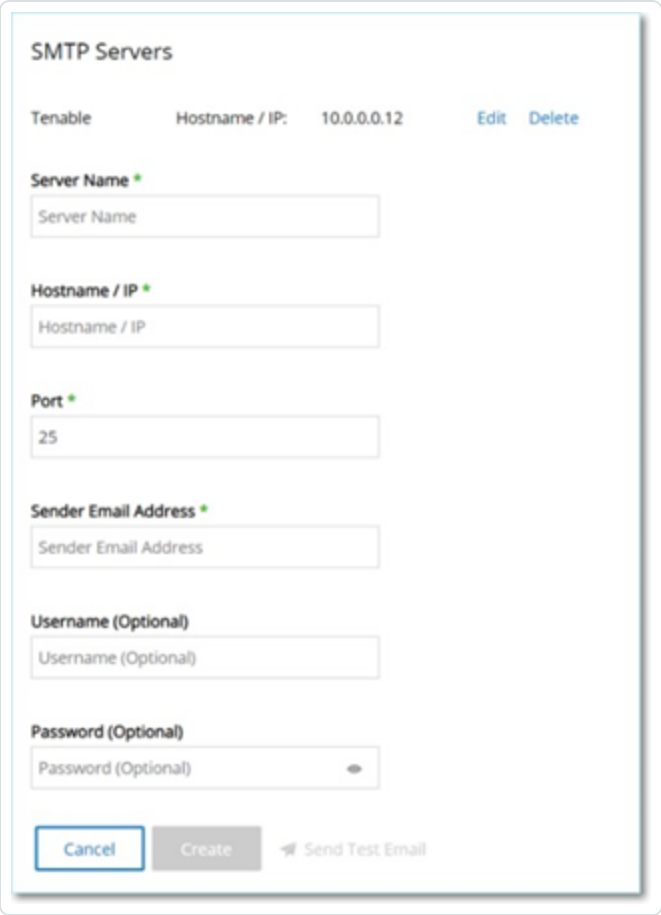
Serveurs SMTP

Pour envoyer les notifications d'événement par e-mail aux parties pertinentes, vous devez configurer un serveur SMTP dans le système. Si vous ne configurez pas de serveur SMTP, le système ne peut pas envoyer de notifications par e-mail chaque fois que des événements sont générés. Dans tous les cas, tous les événements peuvent être visualisés dans la console de gestion (interface utilisateur) sur l'écran des **événements**.

Pour configurer un serveur SMTP :

1. Accédez à **Paramètres locaux** > **Serveurs** > **Serveurs SMTP**.
2. Cliquez sur **Ajouter un serveur SMTP**.

   La fenêtre de configuration des **serveurs SMTP** apparaît.



3. Dans la zone **Nom du serveur**, saisissez le nom d'un serveur SMTP à utiliser pour les notifications par e-mail.
4. Dans la zone **Nom d'hôte/ adresse IP**, saisissez le nom d'hôte ou l'adresse IP du serveur SMTP.
5. Dans la zone **Port**, saisissez le numéro de port sur lequel le serveur SMTP doit écouter les événements (port 25, par défaut).
6. Dans la zone **Adresse e-mail de l'expéditeur**, saisissez l'adresse e-mail qui apparaît comme expéditeur de l'e-mail de notification d'événement.
7. (Facultatif) Dans les zones **Nom d'utilisateur** et **Mot de passe**, saisissez le nom d'utilisateur et le mot de passe à utiliser pour accéder au serveur SMTP.
8. Pour envoyer un e-mail de test afin de vérifier que la configuration est correcte, cliquez sur **Envoyer un e-mail de test**, puis saisissez l'adresse e-mail de destination et vérifiez la boîte de réception pour déterminer si l'e-mail a été reçu. Si tel n'est pas le cas, identifiez la cause du

problème et résolvez-le.

9. Cliquez sur **Enregistrer**.

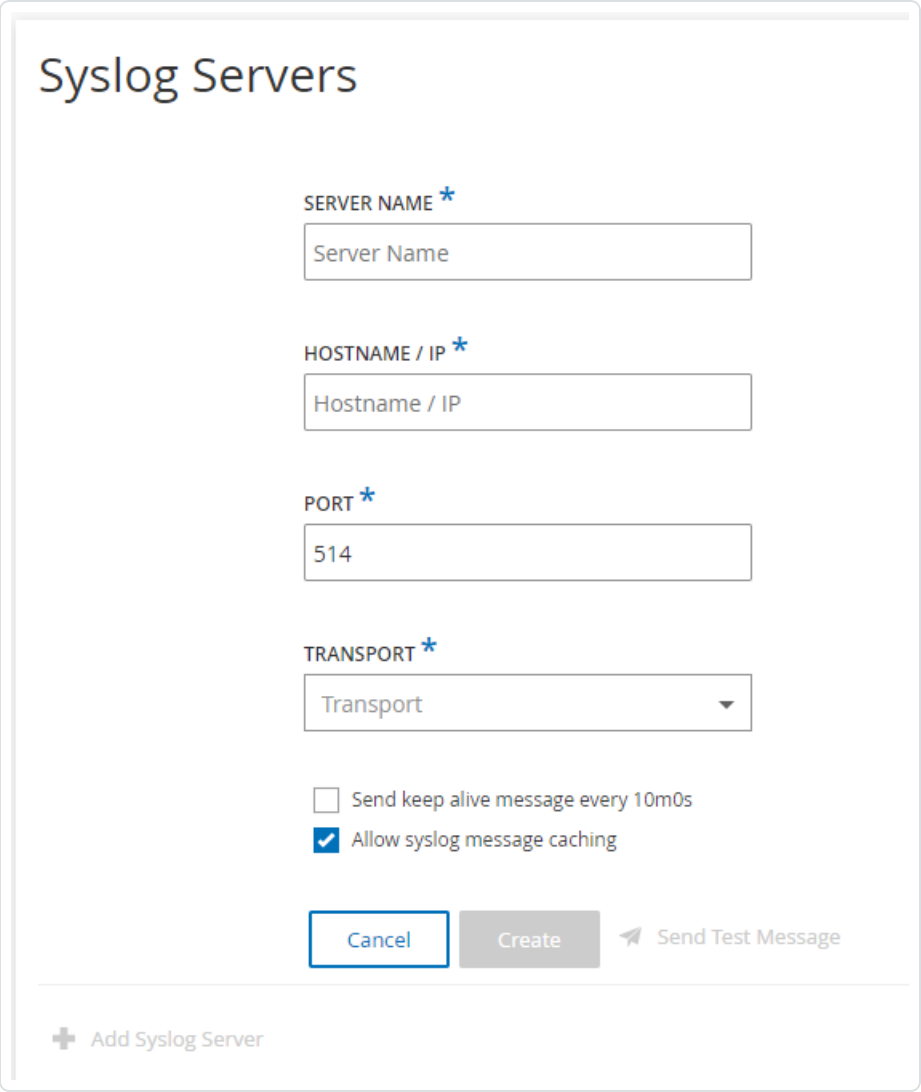
   Vous pouvez configurer des serveurs SMTP supplémentaires en répétant la procédure.

Serveurs Syslog

Pour collecter les événements des journaux sur un serveur externe, vous devez configurer un serveur Syslog dans le système. Si vous ne souhaitez pas configurer de serveur Syslog, les journaux d'événements ne sont enregistrés que sur la plateforme OT Security.

Pour configurer un serveur Syslog :

1. Accédez à **Paramètres locaux** > **Serveurs** > **Serveurs Syslog**.
2. Cliquez sur **+ Ajouter un serveur Syslog**. La fenêtre de configuration **Serveurs SMTP** apparaît.



3. Dans la zone **Nom du serveur**, saisissez le nom du serveur Syslog à utiliser pour consigner les événements système.
4. Dans la zone **Nom d'hôte/ adresse IP**, saisissez le nom d'hôte ou l'adresse IP du serveur Syslog.
5. Dans la zone **Port**, saisissez le numéro de port du serveur Syslog auquel les événements doivent être envoyés. Port par défaut : 514.
6. Dans la zone déroulante **Transport**, sélectionnez le protocole de transport à utiliser. Les options sont TCP ou UDP.
7. Pour envoyer un message de test pour vérifier que la configuration a réussi, cliquez sur **Envoyer un message de test** et vérifiez si le message est arrivé. Si tel n'est pas le cas,

déterminez la cause du problème et résolvez-le.

8. (Facultatif) Sélectionnez l'option **Envoyer un message de présence toutes les 10m0s** pour vérifier la connexion à des intervalles fréquents.
9. (Facultatif) Pour TCP Syslog, sélectionnez l'option **Autoriser la mise en cache des messages Syslog** pour mettre en cache les événements lorsque la connexion est interrompue et les envoyer une fois la connexion rétablie.

   > **Remarque** : les messages syslog UDP n'ont aucune connaissance de l'état et peuvent être perdus si la connexion est interrompue.

10. Cliquez sur **Enregistrer**.

    Vous pouvez configurer des serveurs Syslog supplémentaires en répétant la procédure.

Pare-feux FortiGate

Pour configurer un serveur FortiGate :

1. Accédez à **Paramètres locaux** > **Serveurs** > **Pare-feux FortiGate**.
2. Cliquez sur **Ajouter un pare-feu**.

   La fenêtre de configuration **Ajouter un pare-feu FortiGate** apparaît.

3. Dans la zone **Nom du serveur**, saisissez le nom du serveur FortiGate à utiliser.
4. Dans la zone **Nom d'hôte/ adresse IP**, saisissez le nom d'hôte ou l'adresse IP du serveur FortiGate.
5. Dans la zone **Clé API**, saisissez le jeton API que vous avez généré à partir de FortiGate.

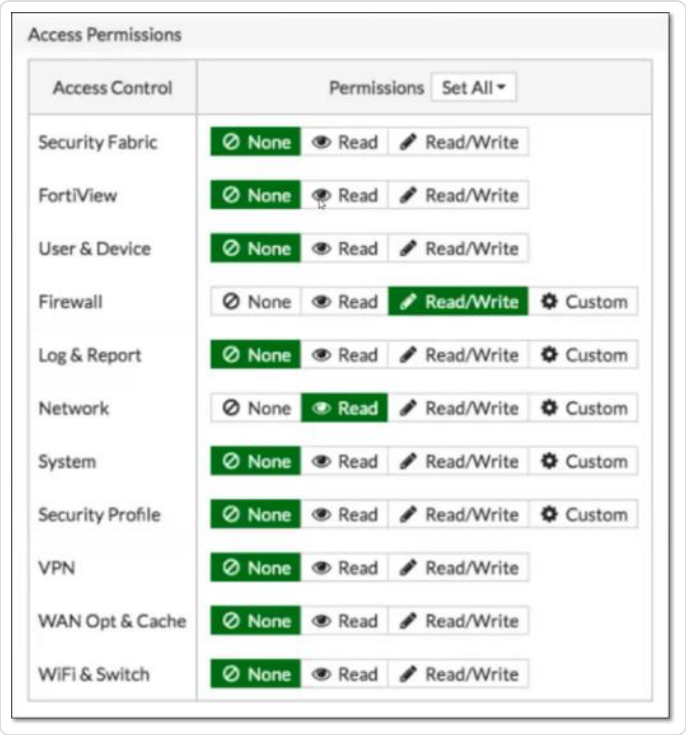
   > **Remarque :** pour les instructions de génération d'un jeton API FortiGate, voir https://registry.terraform.io/providers/fortinetdev/fortios/latest/docs/guides/fgt_token.

6. Cliquez sur **Ajouter**.

   OT Security crée le serveur FortiGate Firewall.

   > **Remarque :** pour l'adresse source (qui est nécessaire pour garantir que le jeton API ne puisse être utilisé qu'à partir d'hôtes de confiance), utilisez l'adresse IP de votre unité OT Security.

   Lors de la création d'un profil d'administrateur pour OT Security, veillez à appliquer les autorisations d'accès en fonction des paramètres suivants :



Journal système

La page **Journal système** affiche le journal de tous les événements système (par exemple, politique activée, politique modifiée, événement résolu, etc.) qui se sont produits sur le système. Ce journal inclut à la fois les événements déclenchés par l'utilisateur et les événements système qui se produisent automatiquement (par exemple, la stratégie s'est automatiquement désactivée en raison d'un trop grand nombre de correspondances). Le journal n'inclut pas les événements générés par des politiques, qui sont affichés sur l'écran **Événements**. Vous pouvez exporter les journaux dans un fichier CSV. Vous pouvez également configurer le système pour envoyer les événements du journal système à un serveur Syslog.

Chaque événement consigné contient les détails suivants :

Paramètre	Description
Date/ Heure	La date et l'heure de l'événement.
Événement	Une brève description de l'événement qui s'est produit.
Nom d'utilisateur	Le nom de l'utilisateur qui a lancé l'événement. Pour les événements qui se produisent automatiquement, aucun nom d'utilisateur n'est donné.

Envoi du journal système à un serveur Syslog

Pour configurer le système pour qu'il envoie les événements système à un serveur Syslog :

1. Accédez à l'écran **Paramètres locaux** > **Journal système**.
2. Dans le coin supérieur droit, cliquez sur la zone déroulante pour afficher la liste des serveurs.

   Remarque : pour ajouter un serveur Syslog, voir Serveurs Syslog.
3. Sélectionnez le serveur souhaité.

   OT Security envoie les événements du journal système au serveur Syslog spécifié.

Annexe – Intégration SAML pour Microsoft Azure

OT Security prend en charge l'intégration à Azure via le protocole SAML. Cela permet aux utilisateurs Azure affectés à OT Security de se connecter à OT Security via SSO. Vous pouvez utiliser le mappage de groupe pour attribuer des rôles dans OT Security en fonction des groupes auxquels les utilisateurs sont attribués dans Azure.

Cette section explique le processus complet de configuration d'une intégration SSO de OT Security à Azure. La configuration implique la mise en place de l'intégration en créant une application OT Security dans Azure. Vous pouvez ensuite fournir des informations sur cette application OT Security nouvellement créée et charger le certificat de votre fournisseur d'identité sur la page OT Security SAML. La configuration est complète lorsque vous mappez les groupes de votre fournisseur d'identité aux groupes d'utilisateurs dans OT Security.

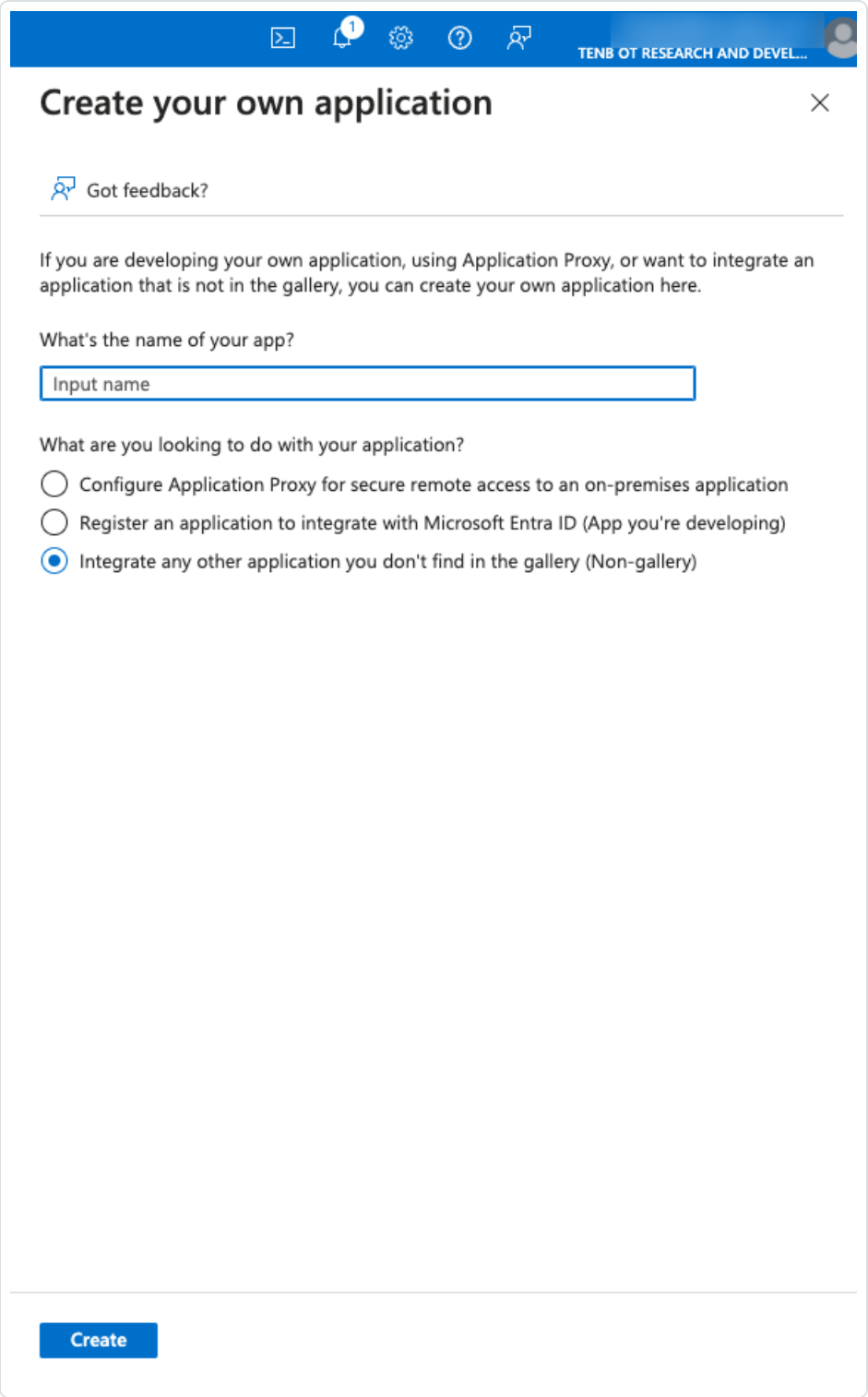
Pour mettre en place la configuration, vous devez être connecté en tant qu'utilisateur administrateur dans Microsoft Azure et OT Security.

Étape 1– Création de l'application Tenable dans Azure

Pour créer l'application Tenable dans Azure :

1. Dans Azure, accédez à Microsoft Entra ID > **Applications d'entreprise** et cliquez sur **+ Nouvelle application.**

   La page **Parcourir la galerie Microsoft Entra ID** apparaît.



2. Cliquez sur **+ Créer votre propre application**.

   Le panneau latéral **Créer votre propre application** apparaît.

3. Dans le champ **Quel est le nom de votre application ?**, saisissez un nom pour l'application (par exemple, Tenable_OT), sélectionnez l'option par défaut **Intégrer une autre application que vous ne trouvez pas dans la galerie**, puis cliquez sur **Créer** pour ajouter l'application.

Étape 2 – Configuration initiale

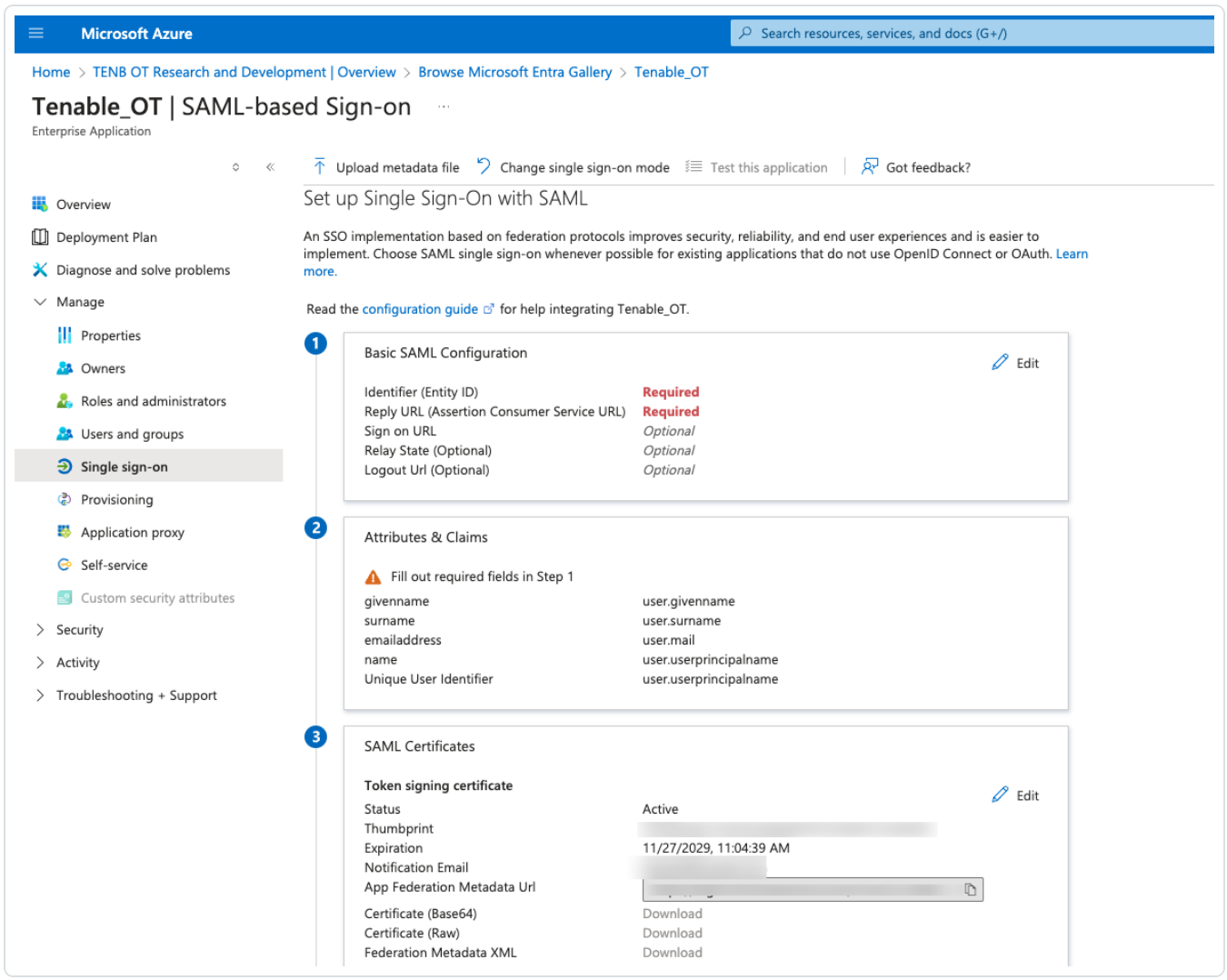
Cette étape est la configuration initiale de l'application OT Security dans Azure, consistant à créer des valeurs temporaires pour les valeurs de la configuration SAML de base, l'**identificateur** et l'**URL de réponse**, afin de permettre le téléchargement du certificat requis.

> **Remarque :** configurez uniquement les paramètres mentionnés dans cette procédure. Conservez les valeurs par défaut pour les autres paramètres.

Pour réaliser la configuration initiale :

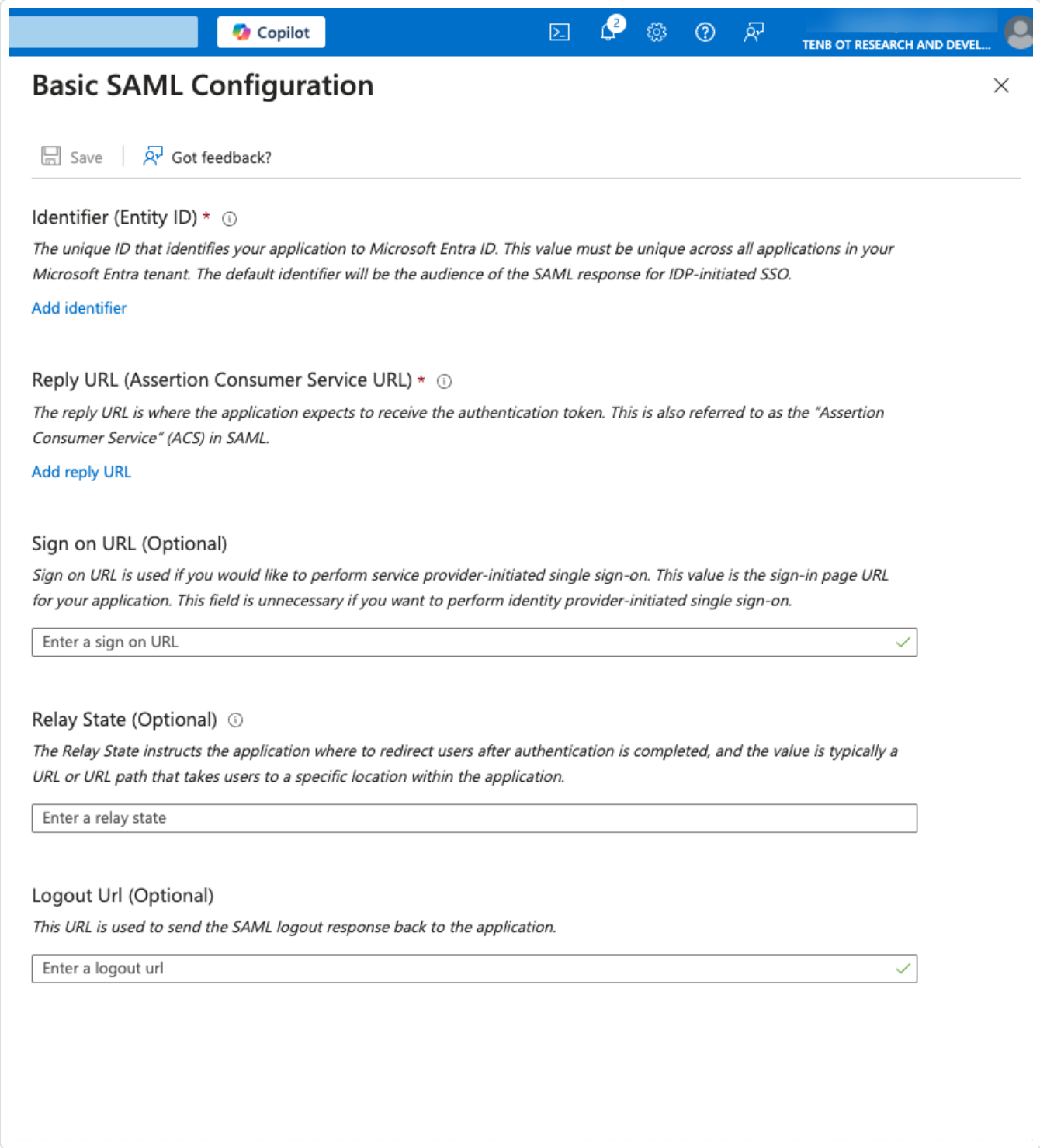
1. Dans le menu de navigation de Azure, cliquez sur **Authentification unique**, puis sélectionnez SAML comme méthode d'authentification unique.

   La page **Authentification basée sur SAML** apparaît.



2. Dans la section 1– **Configuration SAML de base**, cliquez sur **Modifier** .

   Le panneau latéral **Configuration SAML de base** apparaît.



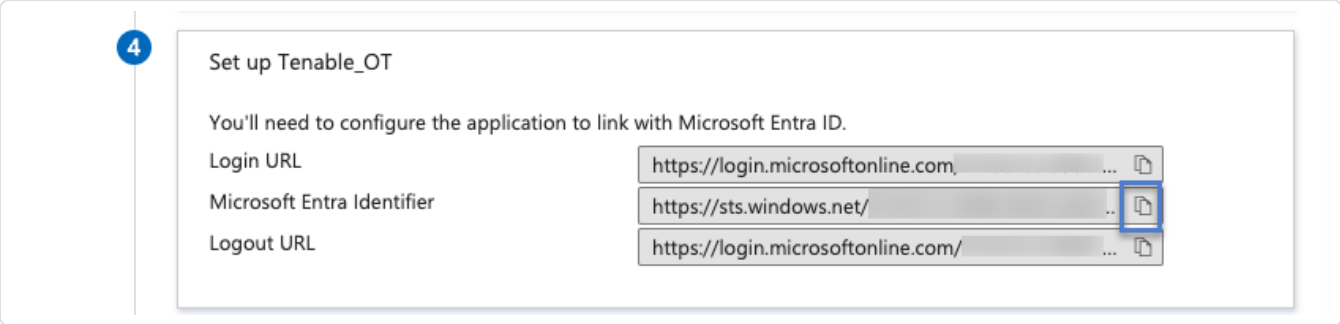
3. Dans la zone **Identificateur (ID de l'entité)**, saisissez un identifiant temporaire pour l'application Tenable (par exemple : `tenable_ot`.

4. Dans la zone **URL de réponse (URL du service consommateur d'assertion)**, saisissez une URL valide (par exemple : `https://OT Security`.

   > **Remarque :** l'**identificateur** et l'**URL de réponse** sont des valeurs temporaires que vous pouvez modifier plus tard dans le processus de configuration.

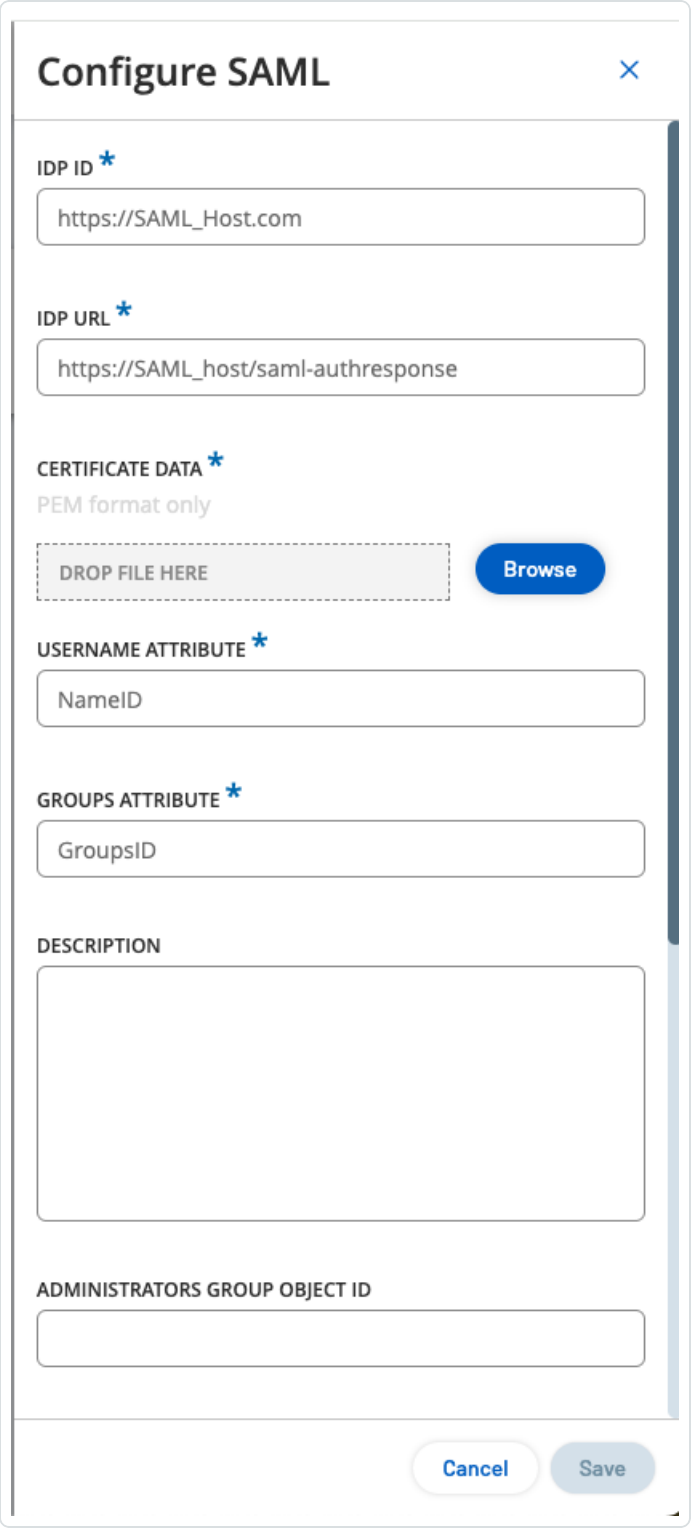
5. Cliquez sur **Enregistrer** pour enregistrer les valeurs temporaires et refermer le panneau latéral **Configuration SAML de base** .

6. Dans la section 4 – **Configurer**, cliquez sur le bouton pour copier l'**identifiant Microsoft Entra ID**.



7. Basculez vers la console OT Security et accédez à **Gestion des utilisateurs** > **SAML**.

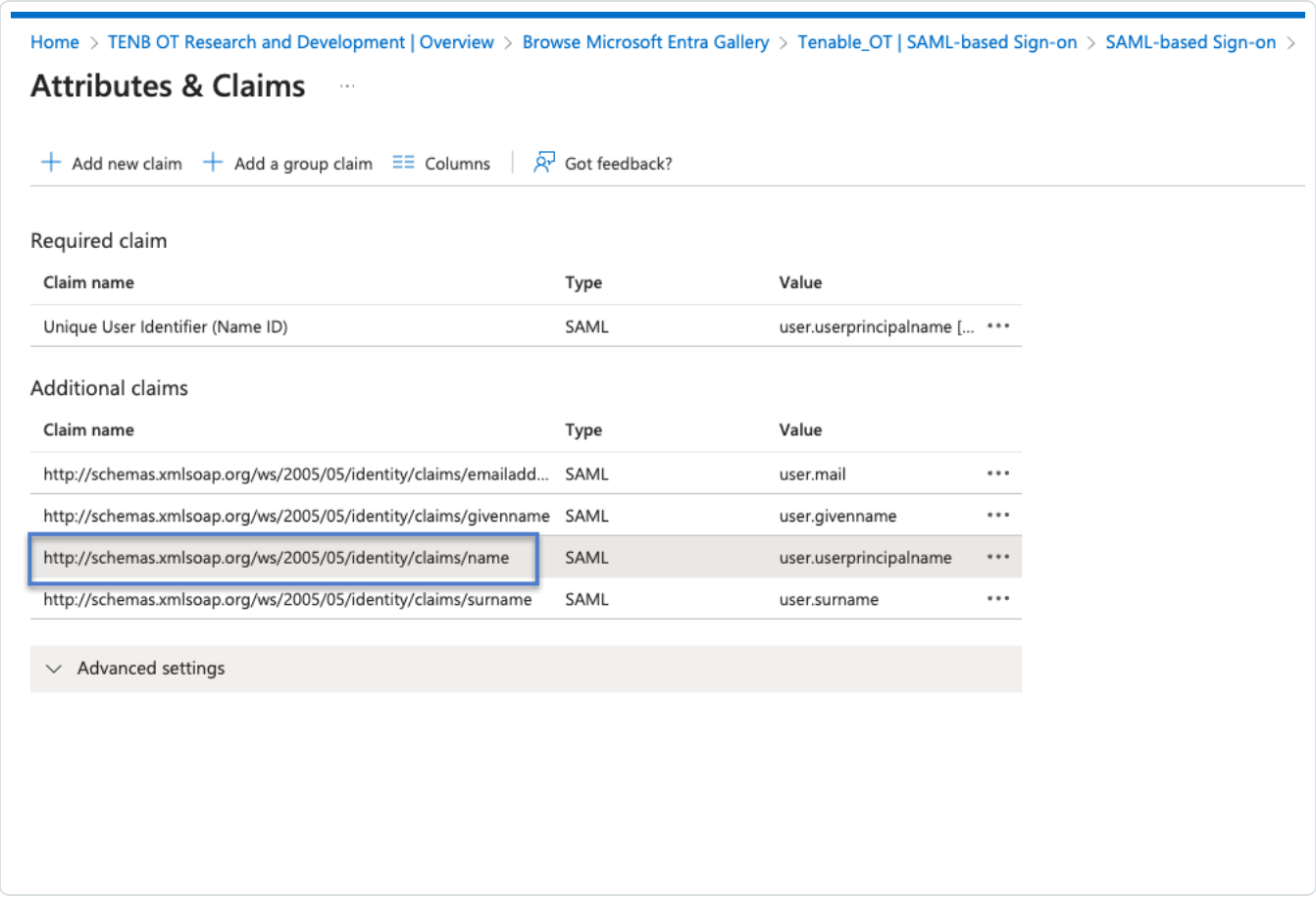
8. Cliquez sur **Configurer** pour afficher le panneau latéral **Configurer SAML** , puis collez la valeur copiée dans la zone **ID de l'IDP**.



9. Dans la console Microsoft Azure, cliquez sur le bouton pour copier l'**URL de connexion**.

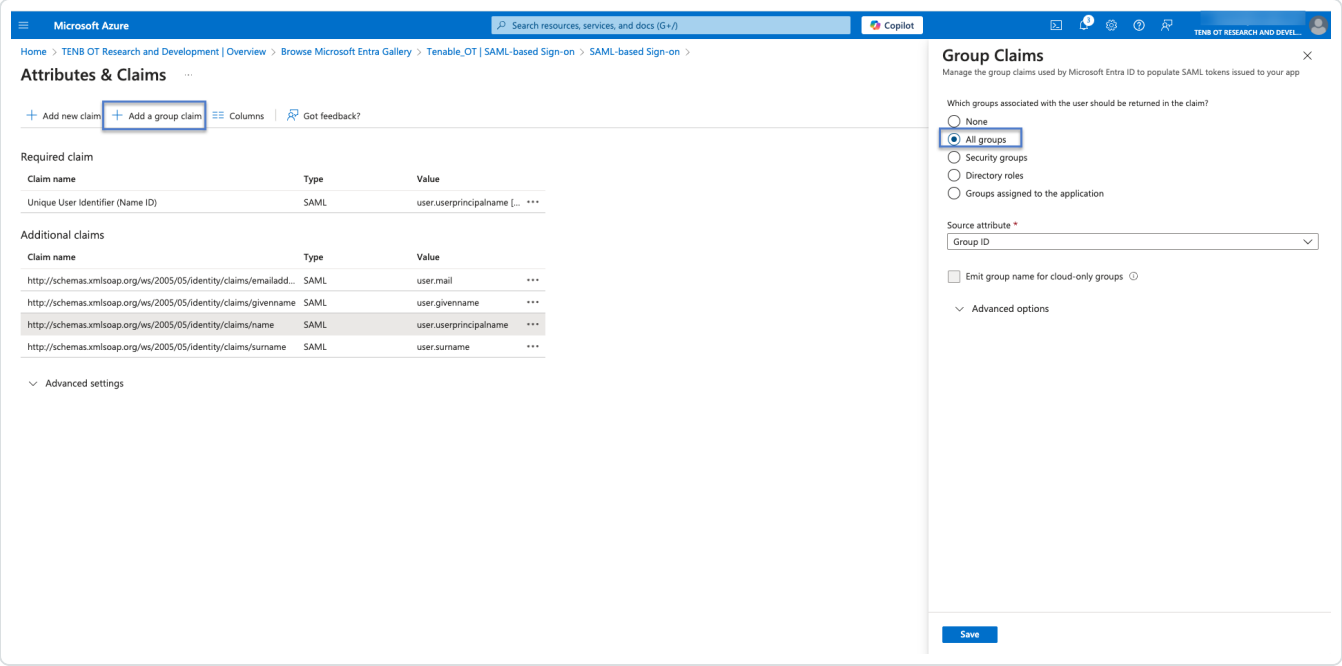
10. Revenez à la console OT Security et collez la valeur copiée dans la zone **URL de l'IDP**.

11. Dans la console Azure, dans la section 3 – **Certificats SAML**, pour **Certificat (Base64)**, cliquez sur **Télécharger**.
12. Revenez à la console OT Security et dans la section **Données de certificat**, cliquez sur **Parcourir**, puis accédez au fichier de certificat de sécurité et sélectionnez-le.
13. Dans la console Azure, dans la section 2 – **Attributs et revendications**, cliquez sur **Modifier**.
14. Dans la section **Revendications supplémentaires**, sélectionnez et copiez l'URL du **nom de la revendication** qui correspond à la **valeur user.userprincipalname**.



15. Revenez à la console OT Security et collez cette URL dans la zone **Attribut de nom d'utilisateur**.
16. Dans la console Azure, cliquez sur **+ Ajouter une revendication de groupe**.

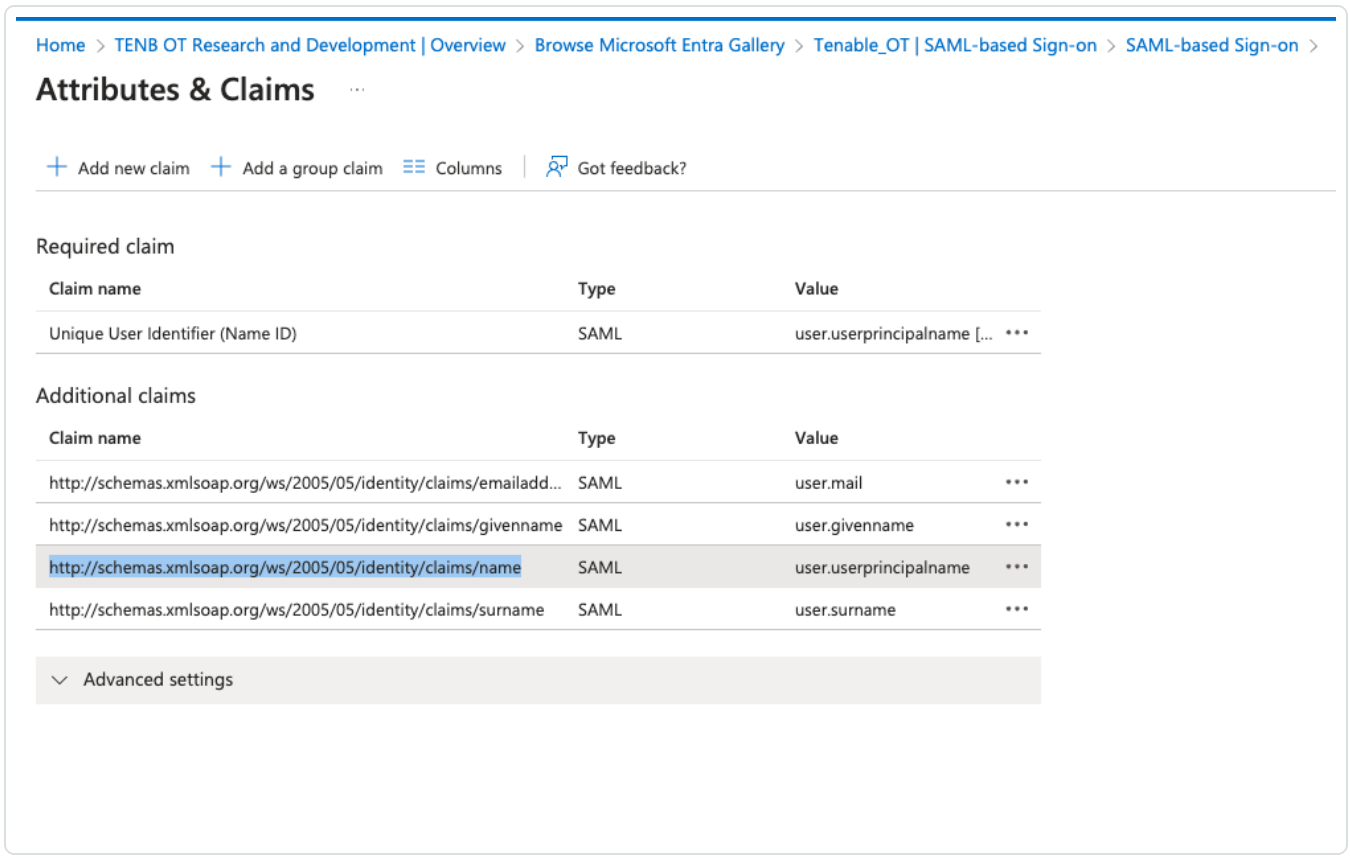
    Le panneau latéral **Revendications de groupe** apparaît.



17. Dans la section **Quels groupes associés à l'utilisateur doivent être retournés dans la revendication ?**, sélectionnez **Tous les groupes** et cliquez sur **Enregistrer**.

> **Remarque :** si vous activez les paramètres de groupes dans Azure, vous pouvez sélectionner **Groupes attribués à l'application** au lieu de **Tous les groupes**. Dans ce cas, Azure fournit uniquement les groupes d'utilisateurs attribués à l'application.

18. Dans la section **Revendications supplémentaires**, mettez en surbrillance et copiez l'URL du **nom de la revendication** associée à la **valeur user.groups [All]**.



19. Revenez à la console OT Security et collez cette URL dans la zone **Attribut des groupes**.
20. (Facultatif) Ajoutez une description de la configuration SAML dans la zone **Description**.

Étape 3 – Mappage des utilisateurs Azure aux groupes Tenable

Au cours de cette étape, vous assignez les utilisateurs Azure à l'application OT Security. Les autorisations accordées à chaque utilisateur sont désignées par mappage entre les groupes Azure auxquels ils sont affectés et un groupe d'utilisateurs OT Security prédéfini, auquel est associé un rôle et un ensemble d'autorisations. Les groupes d'utilisateurs prédéfinis de OT Security sont les suivants : Administrateurs, Utilisateurs en lecture seule, Analystes sécurité, Gestionnaires de sécurité, Opérateurs de site et Superviseurs. Pour plus d'informations, voir Gestion des utilisateurs. Chaque utilisateur Azure doit être affecté à au moins un groupe mappé à un groupe d'utilisateurs OT Security.

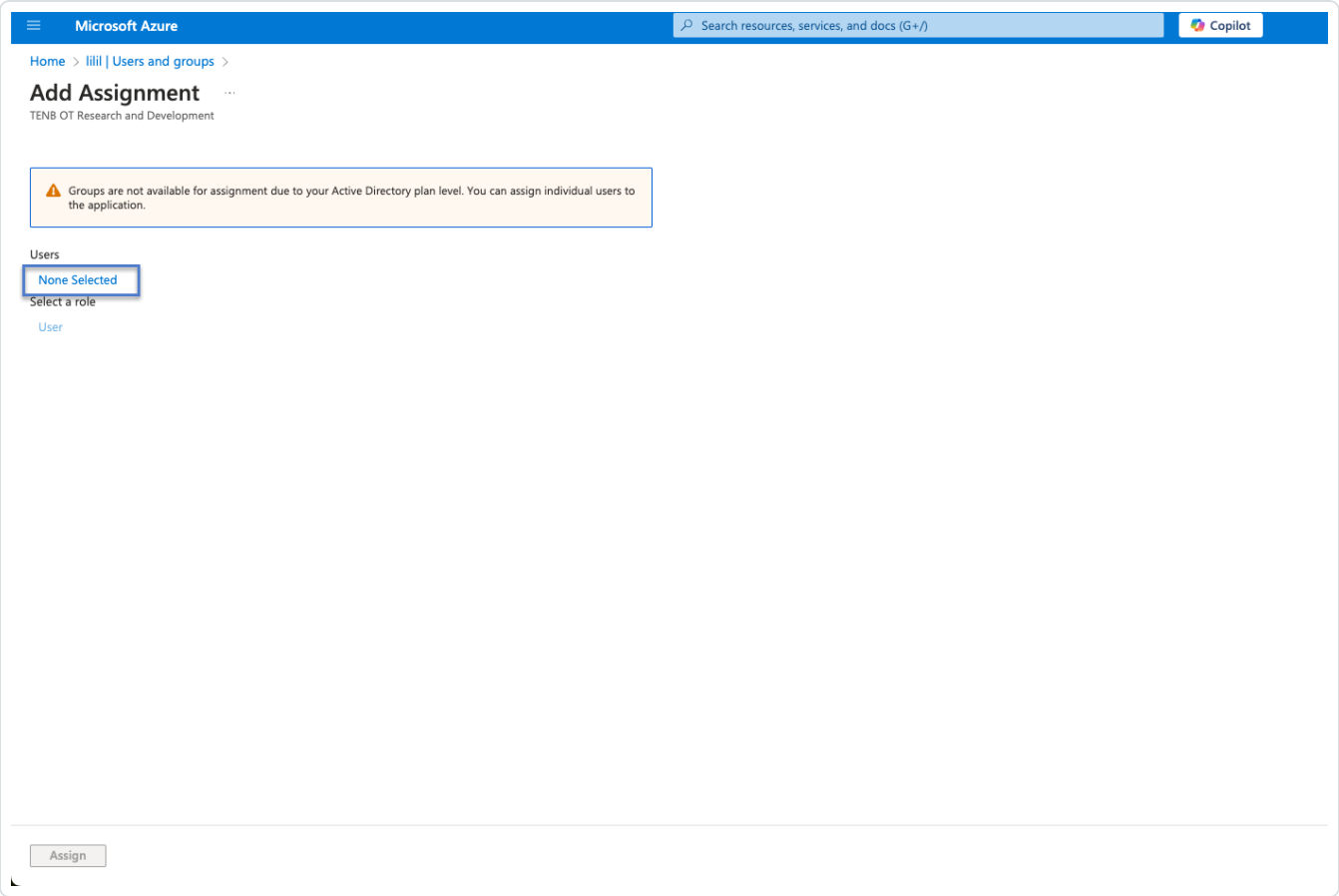
Remarque : les administrateurs connectés via SAML sont considérés comme des administrateurs (externes) et ne bénéficient pas de tous les privilèges des administrateurs locaux. Les utilisateurs affectés

plusieurs groupes d'utilisateurs reçoivent les autorisations les plus élevées possibles parmi leurs roupes.

Pour mapper des utilisateurs Azure à OT Security :

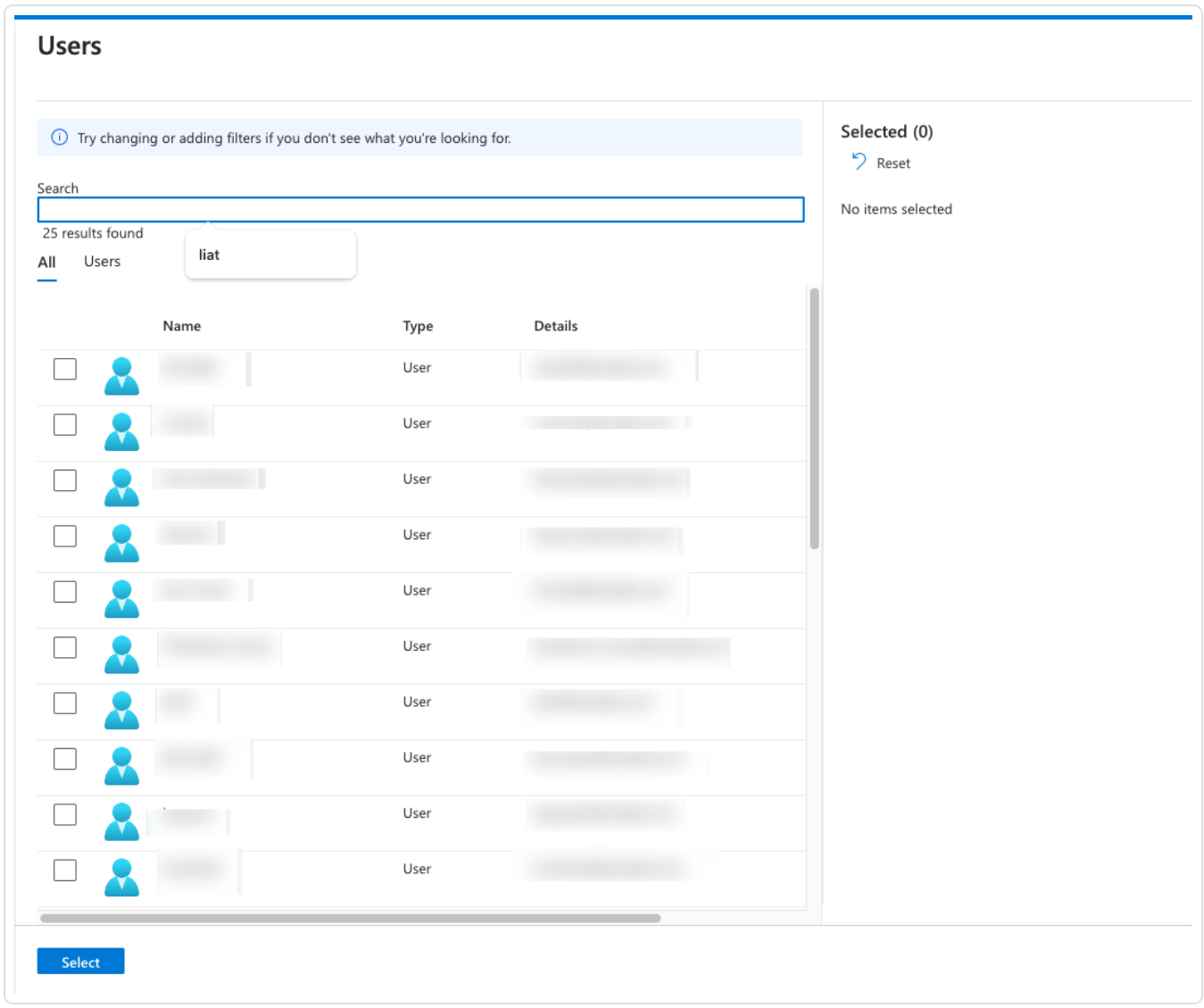
1. Dans Azure, accédez à la page **Utilisateurs et groupes** et cliquez sur **+ Ajouter un utilisateur/ groupe**.
2. Sur la page **Ajouter une attribution**, sous **Utilisateurs**, cliquez sur **Aucune sélection**.

   La page **Utilisateurs** apparaît.



> **Remarque :** si vous activez les paramètres de groupes dans Azure et que vous sélectionnez **Groupes attribués à l'application** au lieu de **Tous les groupes**, vous pouvez attribuer des groupes plutôt que des utilisateurs individuels.

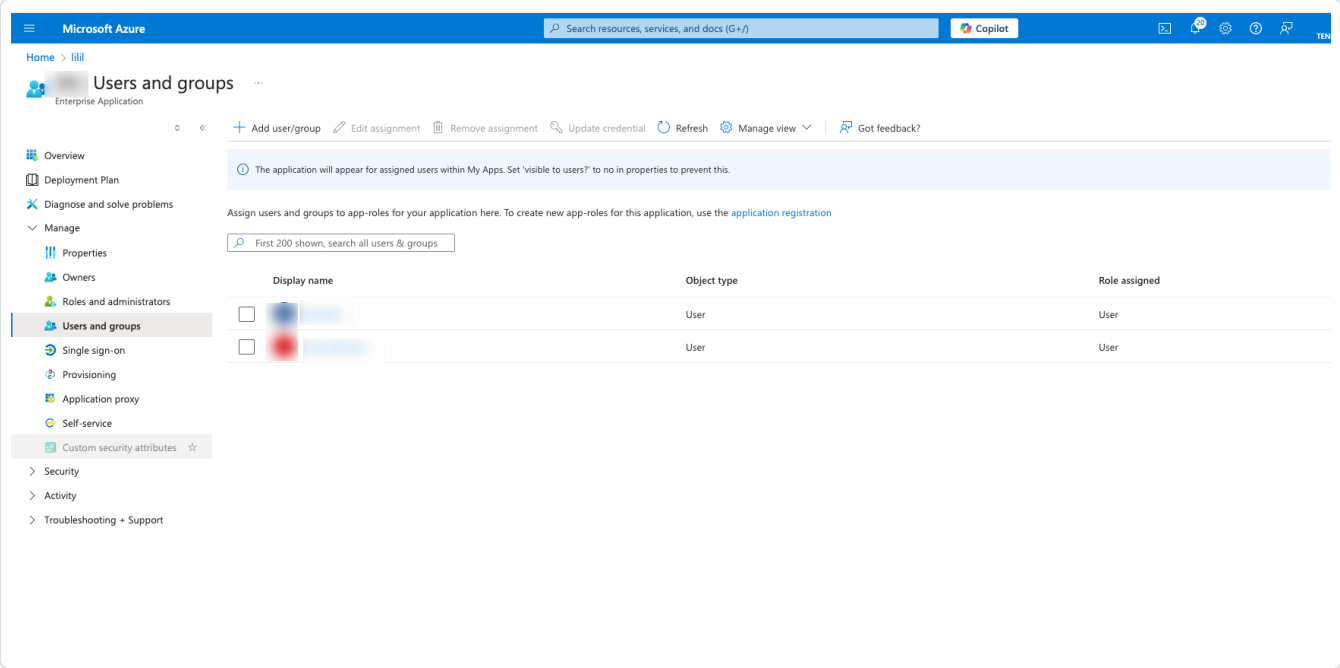
3. Recherchez et sélectionnez tous les utilisateurs requis, puis cliquez sur **Sélectionner**.



4. Cliquez sur **Attribuer** pour les affecter à l'application.

   La page **Utilisateurs et groupes** apparaît.

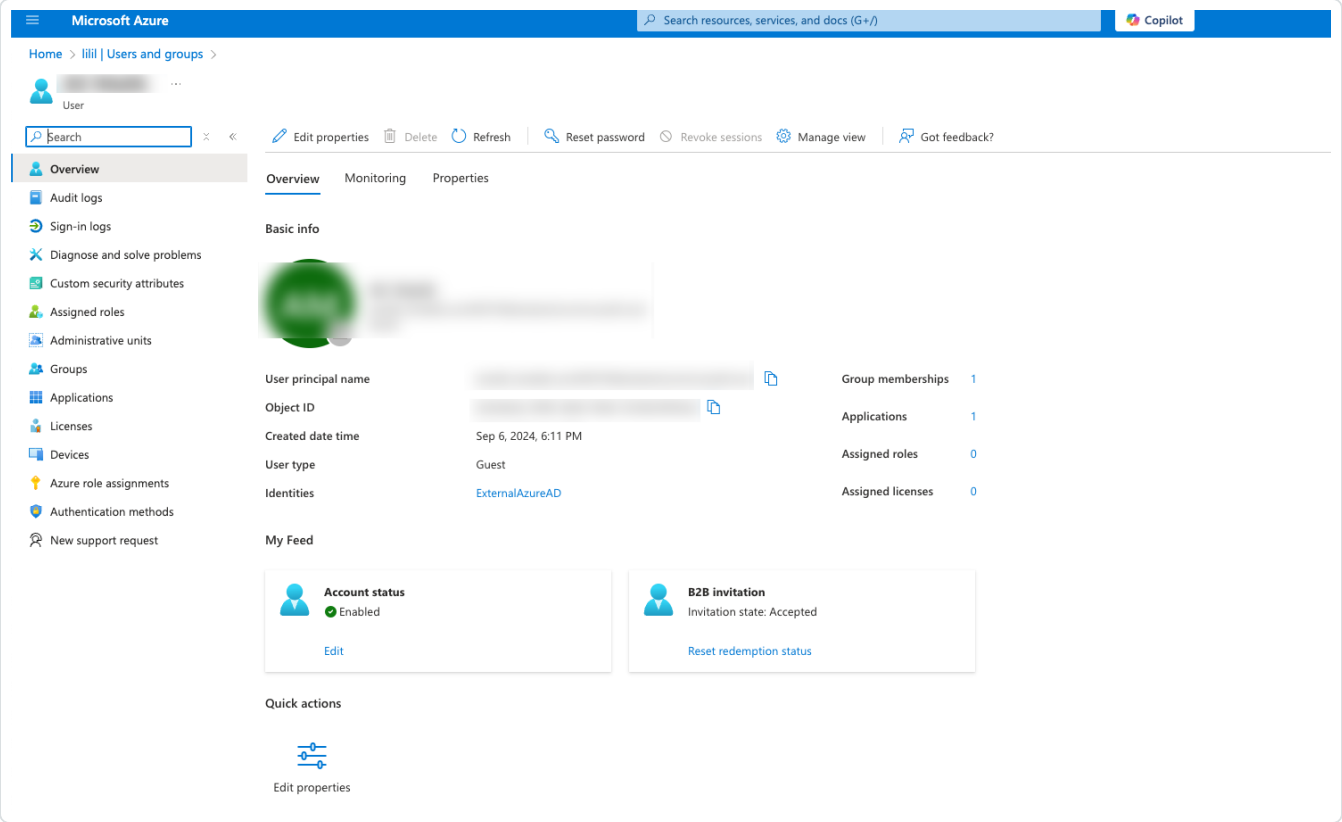
5. Cliquez sur le **nom d'affichage** d'un utilisateur (ou groupe) pour afficher le profil de cet utilisateur (ou groupe).



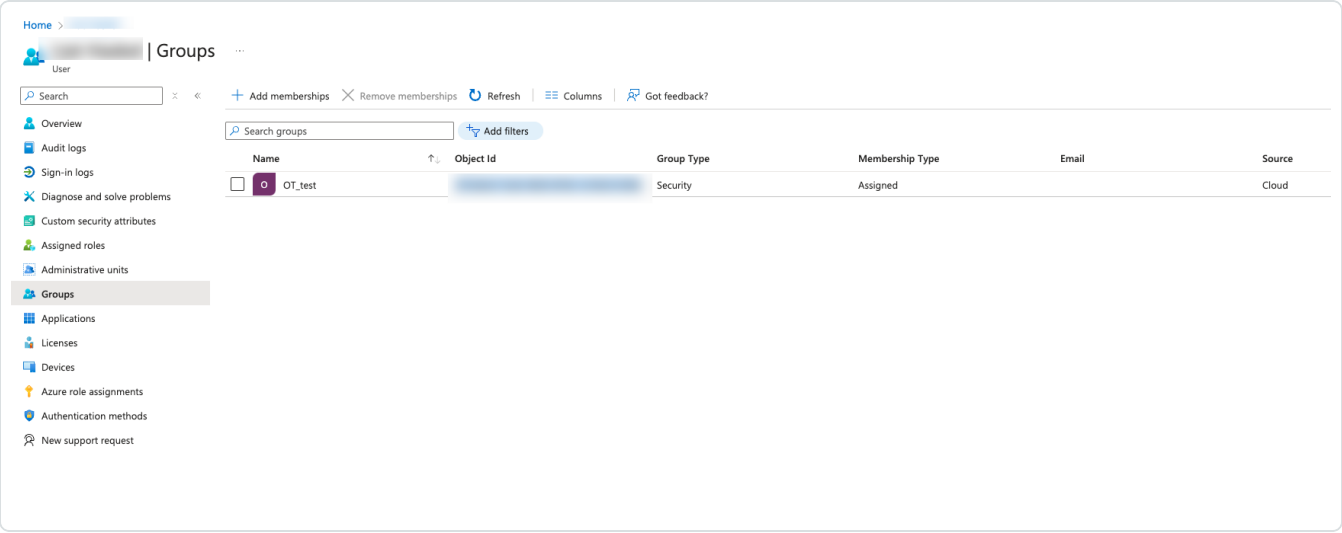
La page **Profil** apparaît.

6. Dans la barre de navigation de gauche, sélectionnez **Groupes**.

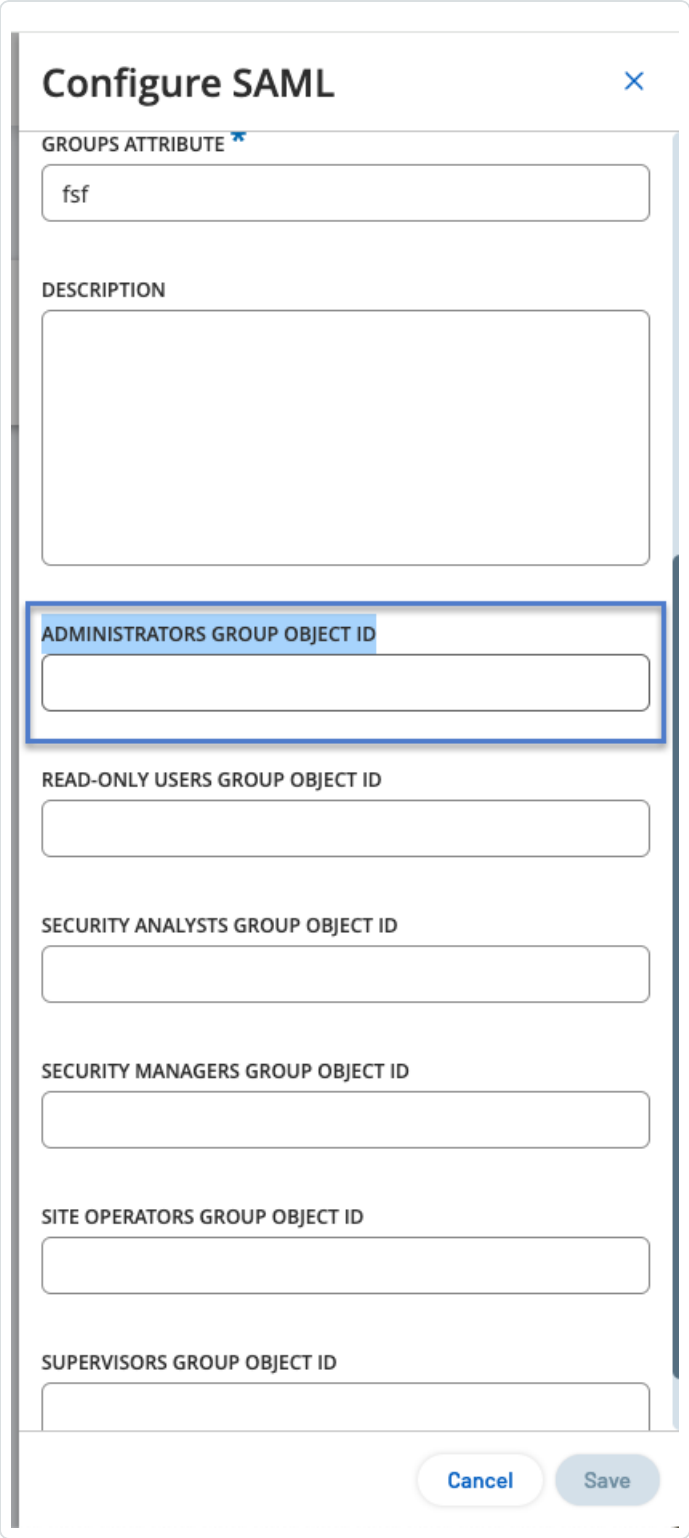
   La page **Groupes** apparaît.



7. Dans la colonne **ID d'objet**, sélectionnez et copiez la valeur du groupe qui sera mappé à Tenable.



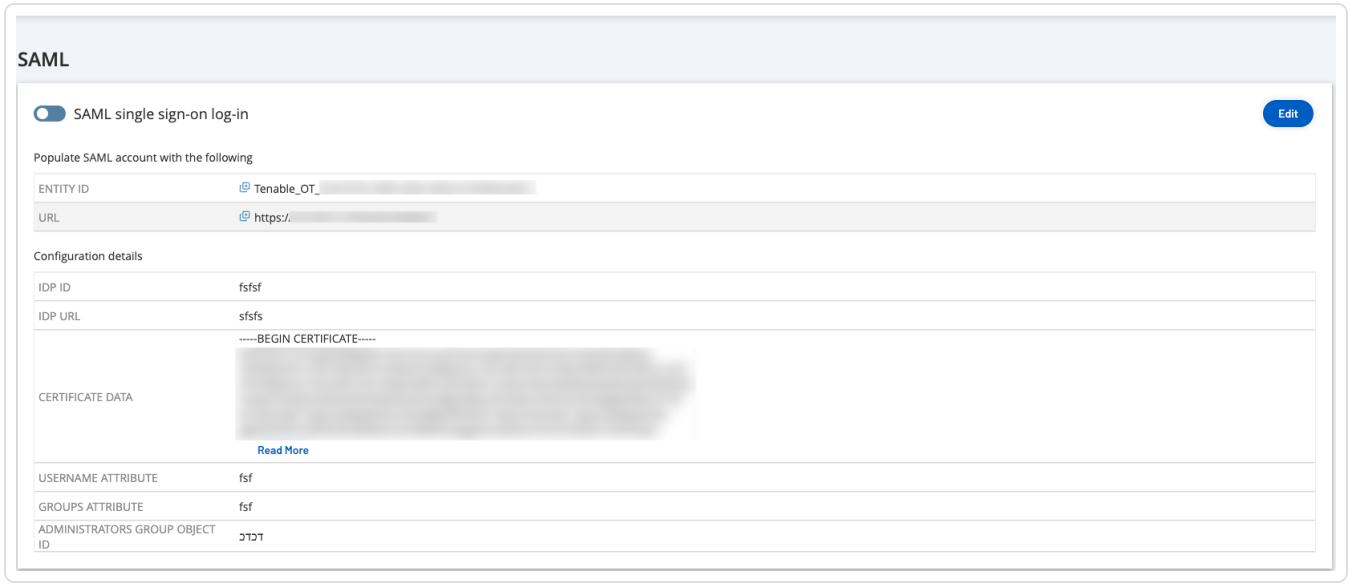
8. Revenez à la console OT Security et collez la valeur copiée dans la zone **ID d'objet de groupe** correspondante. Par exemple, l'**ID d'objet du groupe Administrateurs**.



9. Répétez les étapes 1à 7 pour chaque groupe à mapper à un groupe d'utilisateurs distinct dans OT Security.

10. Cliquez sur **Enregistrer** pour enregistrer et refermer le panneau latéral.

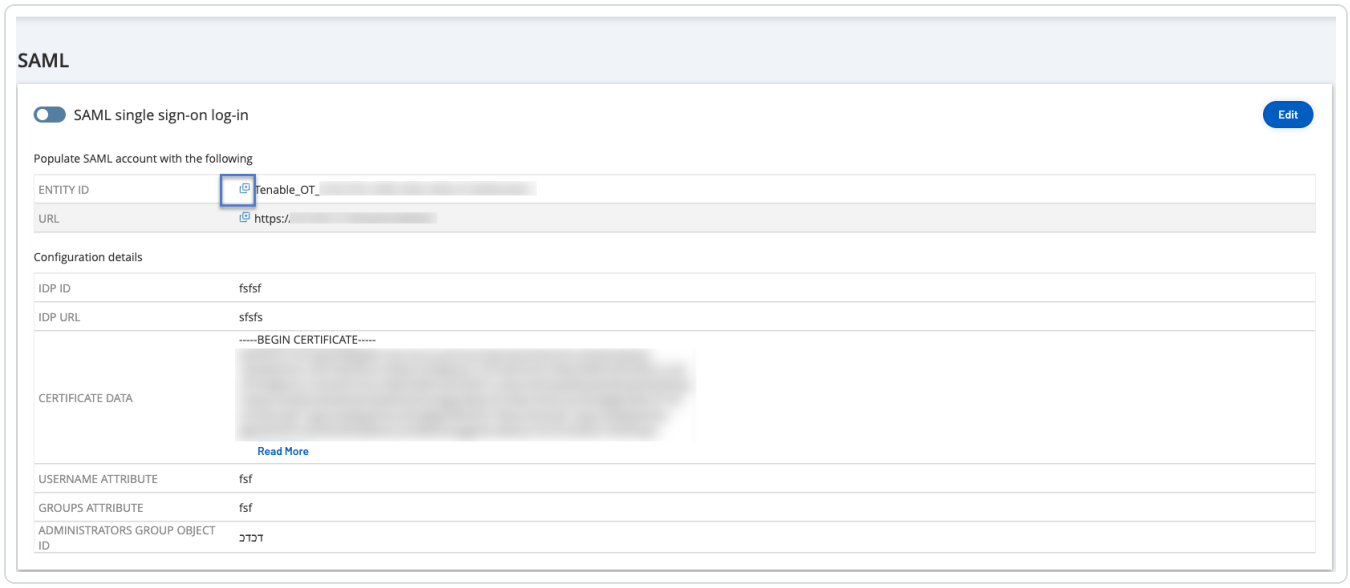
    La page SAML apparaît dans la console OT Security avec les informations configurées.



Étape 4 – Finalisation de la configuration dans Azure

Pour finaliser la configuration dans Azure :

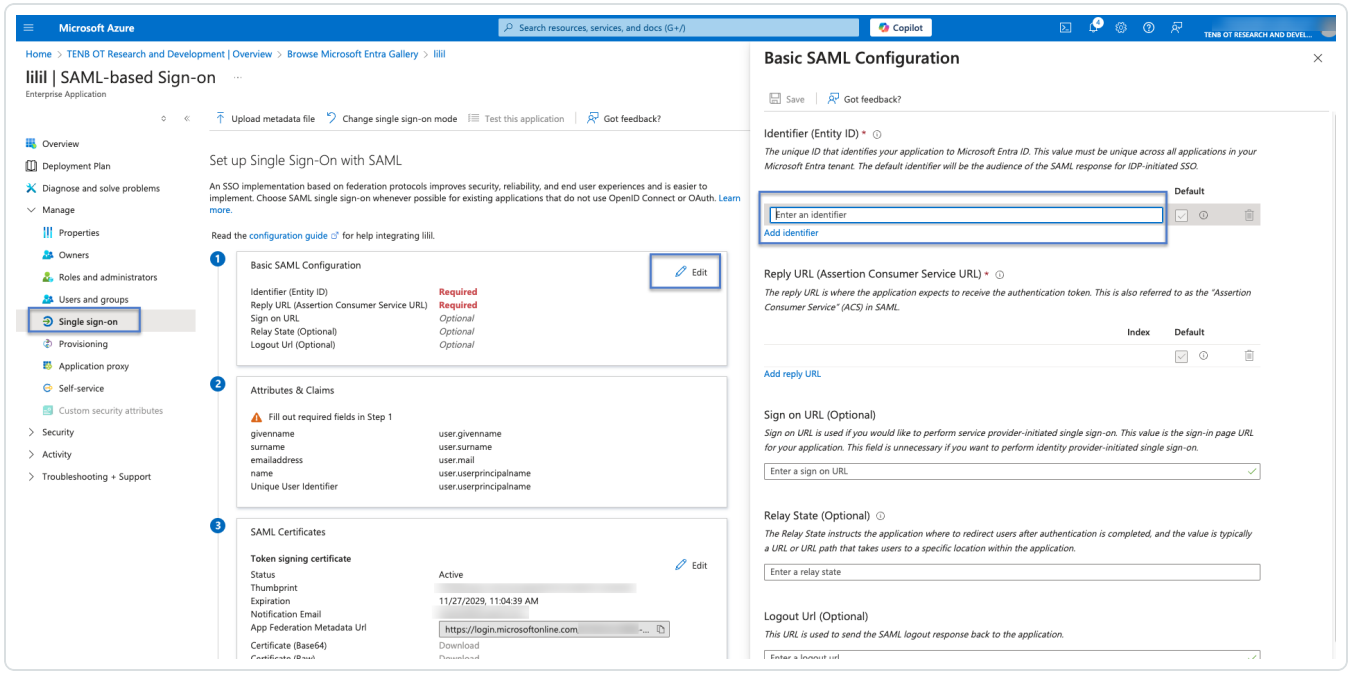
1. Sur la page OT Security **SAML**, cliquez sur le bouton pour copier l'**ID de l'entité**.



2. Dans la console Azure, cliquez sur **Authentification unique** dans le menu de navigation de gauche.

   La page **Authentification basée sur SAML** apparaît.

3. Dans la section 1– **Configuration SAML de base**, cliquez sur **Modifier** et collez la valeur copiée dans la zone **Identificateur (ID de l'entité)** en remplaçant la valeur temporaire que vous avez saisie précédemment.



4. Basculez vers OT Security et, sur la page **SAML**, cliquez sur le bouton pour copier l'**URL**.

5. Basculez vers la console Azure et, dans la section **Configuration SAML de base**, collez l'URL copiée dans la zone **URL de réponse (URL du service consommateur d'assertion)** en remplaçant l'URL temporaire que vous avez saisie précédemment.

6. Cliquez sur **Enregistrer** pour enregistrer la configuration et refermer le panneau latéral.

   La configuration est terminée et la connexion apparaît sur la page **Applications Azure Enterprise**.

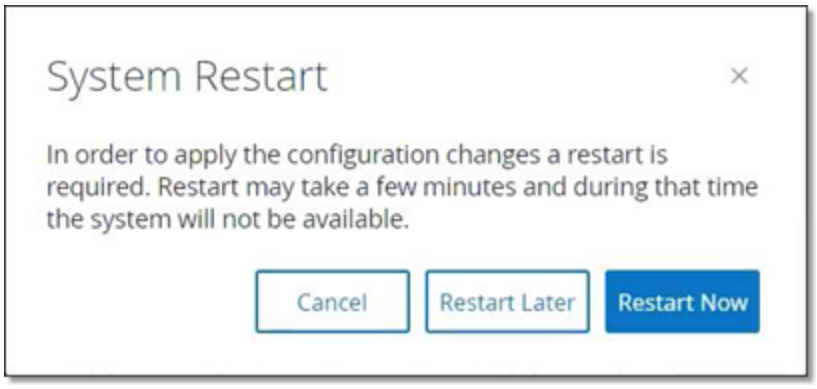
Étape 5 – Activation de l'intégration

Pour activer l'intégration SAML, vous devez redémarrer OT Security. Vous pouvez redémarrer le système immédiatement ou choisir de le redémarrer plus tard.

Pour activer l'intégration :

1. Dans la console OT Security, sur la page **SAML**, cliquez sur le curseur **Connexion unique SAML** pour activer SAML.

   La fenêtre de notification de **redémarrage du système** apparaît.

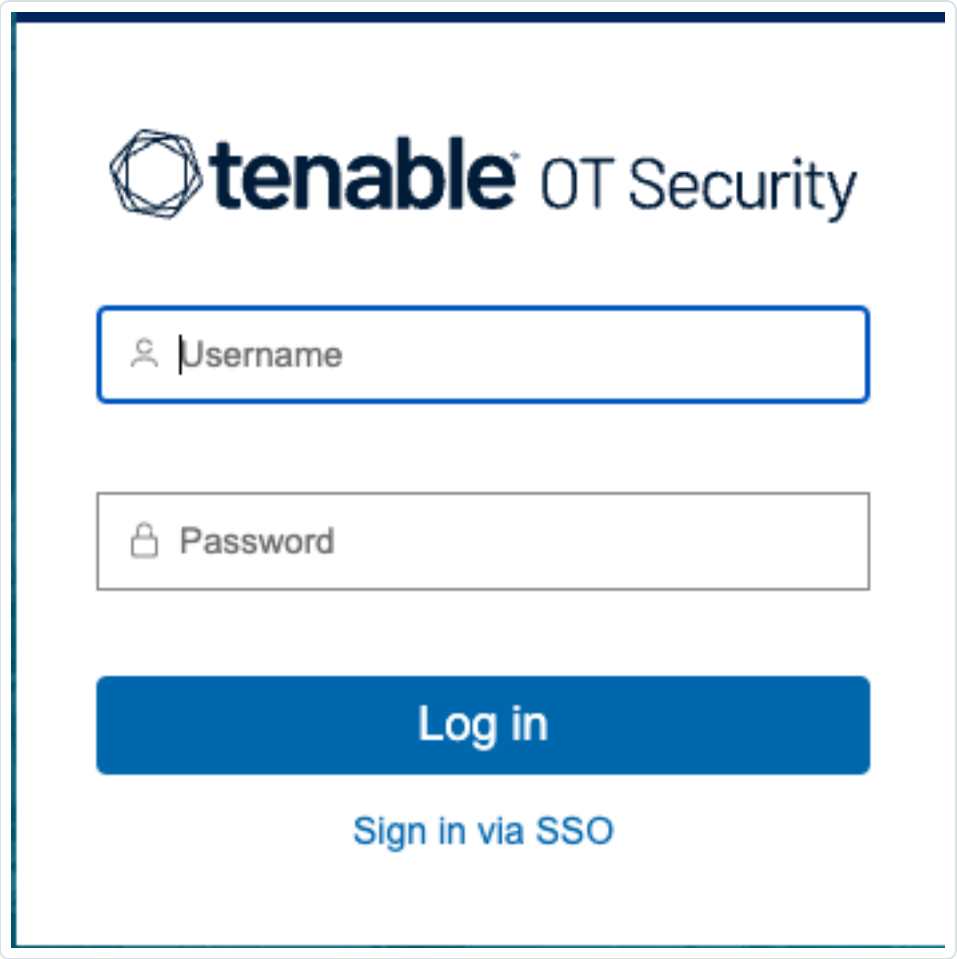
2. Cliquez sur **Redémarrer maintenant** pour redémarrer le système et appliquer la configuration SAML immédiatement, ou cliquez sur **Redémarrer ultérieurement** pour retarder l'application de la configuration SAML au prochain redémarrage du système. Si vous choisissez de redémarrer plus tard, la bannière suivante apparaît jusqu'à ce que le redémarrage soit terminé :

Se connecter via SSO

Après le redémarrage, la fenêtre de connexion OT Security comporte un nouveau lien **Sign in via SSO** (Se connecter via SSO) sous le bouton **Se connecter**. Les utilisateurs Azure affectés à OT Security peuvent se connecter à OT Security à l'aide de leur compte Azure.

Pour se connecter via SSO :

1. Dans la fenêtre de connexion OT Security, cliquez sur le lien **Sign in via SSO** (Se connecter via SSO).



Si vous êtes déjà connecté à Azure, vous êtes dirigé directement vers la console OT Security ; sinon, vous êtes redirigé vers la page de connexion Azure.

Si vous possédez plusieurs comptes, OT Security vous redirige vers la page Microsoft **Choisir un compte**, où vous pouvez sélectionner le compte souhaité pour la connexion.