

Guide de l'utilisateur Tenable OT Security 4.7

Dernière révision : 2 juillet 2026



Table des matières

Bienvenue dans Tenable OT Security	26
Premiers pas avec OT Security	27
Technologies OT Security	28
Architecture de la solution	29
Composants de la plateforme OT Security	29
Composants réseau	30
Spécifications matérielles Tenable OT Security	31
Spécifications pour l'ICP et les capteurs	31
ICP normale	31
XL ICP	32
ICP-Mini	34
Capteur	35
Éléments système	36
Assets	36
Politiques et événements	37
Détection basée sur des politiques	37
Détection des anomalies	38
Catégories de politiques	39
Groupes	40



Événements	41
Composants de licence OT Security	41
Gestion des licences Tenable OT Security	41
Comment les assets sont comptabilisés	42
Composants Tenable OT Security	42
Récupération de licences	43
Dépassement de la limite de licences	43
Licences expirées	44
Playbooks opérationnels	44
Conditions préalables	44
Workflows opérationnels	45
Prioriser et atténuer les vulnérabilités	45
Objectif	45
Conditions préalables	46
Étape 1 : Afficher le dashboard Risques	46
Étape 2 : Prioriser par sévérité et criticité des assets	46
Étape 3 : Analyser les options de remédiation	47
Résultat	49
Investiguer les menaces réseau et y répondre	49
Objectif	49
Conditions préalables	49



Étape 1 : Surveiller les alertes d'événements	50
Étape 2 : Analyser les données de conversation	50
Étape 3 : Lancer la réponse	51
Résultat	52
Messages d'erreur	52
Premiers pas avec OT Security	66
Vérifier les conditions préalables	68
Installer l'ICP OT Security	69
Utiliser OT Security	70
Intégrer OT Security à Tenable One	71
Conditions préalables	75
Configuration matérielle requise	75
Configuration requise pour les appliances virtuelles	76
Exigences de licence	76
Exigences système	76
Configuration matérielle requise pour OT Security	77
Configuration du matériel virtuel OT Security	78
Configuration requise pour les capteurs virtuels OT Security	78
Conditions de stockage requises	78
Espace disque requis	79
Directives sur les exigences système de l'ICP	79



Configuration requise pour les partitions de disque	80
Configuration requise de l'interface réseau	81
Configuration requise pour les NIC	81
Exigences d'accès	82
Configuration Internet requise	82
Configuration de ports requise	83
Trafic entrant	83
Trafic sortant	84
Considérations sur le réseau	84
Interface de gestion et des requêtes actives	84
Séparation des rôles de gestion et de requête active (port fractionné)	85
Interfaces de surveillance	85
Considérations sur le pare-feu	86
Plateforme OT Security Core	86
Capteurs OT Security	88
Requête active	89
Intégrations OT Security	95
Agent OT	96
IoT Connector Agent	96
Installer l'ICP OT Security	97
Installer une appliance matérielle ICP OT Security	97



Nouvelle installation Tenable Core + Tenable OT Security sur le matériel fourni par Tenable	99
Installer une appliance virtuelle ICP OT Security	106
Connecter OT Security au réseau	108
Gestion et requête active	108
Surveillance du réseau	109
Configurer l'ICP OT Security	110
Configurer Tenable Core	110
Configuration initiale via l'interface utilisateur Tenable Core	111
Configuration initiale via la CLI (facultatif)	115
Installer OT Security sur Tenable Core	124
Configurer les paramètres OT Security à l'aide de l'assistant de configuration	131
Se connecter à la console de gestion OT Security	132
Informations utilisateur	136
Appareil	138
Connecter et configurer la séparation des ports de gestion et de requête active	139
Activation de licence OT Security	140
Activer votre licence OT Security	141
Mettre à jour votre licence	144
Mettre à jour votre licence en mode hors ligne	151
Réinitialiser votre licence	157



Lancer OT Security	159
Activer le système OT Security	160
Commencer à utiliser OT Security	162
Configurer les réseaux surveillés	162
Examiner et configurer les ports	162
Configurer les utilisateurs, les groupes et les serveurs d'authentification	163
Ajouter des services réseau	163
Activer les requêtes actives	163
Créer des scans Nessus	163
Définir des sauvegardes	163
Obtenir des mises à jour	163
Optimiser	164
Intégrer	164
Installer le capteur OT Security	164
Appairer le capteur	165
Configurer le capteur	171
Configurer un capteur configurable	172
Montage sur rail DIN	172
Montage en rack (modèle configurable)	173
Connecter le capteur au réseau	175
Accéder à l'assistant de configuration du capteur	176



Établissement de la connexion à la console et de la configuration initiale	179
Connexion physique	180
Identifier le port COM (Windows)	180
Configurer un terminal (PuTTY)	181
Établir une connexion	182
Configuration réseau initiale	182
Accéder à l'interface utilisateur	183
Câbles console à connecter au Capteur OT Security	183
Restaurer la sauvegarde à l'aide de la CLI	185
Éléments de l'interface utilisateur de la console de gestion	187
Principaux éléments de l'interface utilisateur	187
Activer ou désactiver le mode sombre	189
Vérifier la version actuelle du logiciel	189
Accéder au Centre de ressources	190
Naviguer dans OT Security	191
Personnaliser les tableaux	193
Personnaliser l'affichage des colonnes (version 3.19 et antérieures)	193
Personnaliser l'affichage des colonnes (version 4.0 et ultérieures)	194
Regrouper des listes par catégories (version 3.19 et antérieures)	195
Regrouper des listes par catégories (version 4.0 et ultérieures)	197
Trier des colonnes	199



Filtrer les colonnes (version 3.19 et antérieures)	199
Filtrer les colonnes (version 4.0 et ultérieures)	200
Enregistrer un filtre	202
Modifier les filtres enregistrés	204
Créer une copie du filtre enregistré	204
Supprimer tous les filtres	205
Voir les filtres enregistrés	205
Modifier le nom du filtre enregistré	206
Supprimer un filtre enregistré	208
Effectuer une recherche (version 3.19 et antérieures)	209
Effectuer une recherche (version 4.0 et ultérieures)	209
Exporter des données	210
Menu Actions	210
Actions en bloc	211
Vue d'ensemble de OT Security	212
Générer un rapport exécutif	215
Inventaire	217
Affichage des assets	217
Types d'assets	221
Afficher les détails d'un asset	235
Volet d'en-tête	237



Détails	238
Vue du fond de panier	240
Informations sur le scan Nessus	241
CEI 61850	243
Révisions de code	243
Volet de sélection de version	245
Volet des détails d'un instantané	245
Volet d'historique des versions	246
Comparer les versions d'un instantané	247
Créer un instantané	249
Itinéraire IP	249
Vecteurs d'attaque	250
Comment déterminer le vecteur d'attaque ?	250
Étapes d'atténuation recommandées	251
Générer des vecteurs d'attaque	251
Affichage des vecteurs d'attaque	254
Ports ouverts	255
Mettre à jour les ports ouverts	256
Actions supplémentaires dans l'onglet Ports ouverts	256
Exécuter un scan	256
Afficher le portail de l'asset	257



Vulnérabilités	257
Événements	258
Cartographie du réseau	262
Ports du périphérique	263
Assets associés	264
Détails de l'asset imbriqué	265
CEI 61850	267
Sources	269
Modifier les détails de l'asset	271
Modifier les détails d'un asset via l'interface utilisateur	271
Modifier les détails d'un asset en téléchargeant un fichier CSV	273
Masquer des assets	276
Exporter les diagnostics	277
Exporter un rapport de diagnostic d'asset	277
Exporter le rapport de diagnostic Tenable OT Security (Tenable Core)	278
Fusionner des assets	279
Processus de fusion d'assets	283
Conflits de fusion et fusion forcée	284
Comment corriger une fusion accidentelle	284
Effectuer un scan Tenable Nessus spécifique à un asset	284
Exécuter une resynchronisation	286



Vulnérabilités	289
Afficher les vulnérabilités	290
Détails du plug-in	292
Modifier les détails d'une vulnérabilité	292
Afficher la sortie d'un plug-in	293
Afficher une sortie de plug-in à partir de la page Vulnérabilités	293
Afficher une sortie de plug-in à partir de la page Inventaire	294
Exemple de sortie d'un plug-in Tenable Nessus	295
Exemple de sortie d'un plug-in OT Security	296
Détections	297
Afficher les détails des détections	301
Violations de politique	303
Menu Actions	307
Résoudre une détection	307
Exclure de la politique	307
Télécharger le dernier fichier de capture	308
Détails du plug-in	308
Rechercher des événements	308
Dashboard Conformité	309
Événements	314
Affichage des événements	314



Affichage des détails d'un événement	319
Affichage des clusters d'événements	320
Créer des exclusions de politique	321
Télécharger des fichiers de capture individuels	328
Créer des politiques FortiGate	329
Réseau	331
Récapitulatif réseau	331
Trafic et communications au fil du temps	332
Top 5 sources	333
Top 5 cibles	334
Protocoles	335
Définir la période	336
Captures de paquets	338
Paramètres de capture de paquets	338
Filtrer l'affichage de la capture de paquets	339
Activer ou désactiver les captures de paquets	340
Télécharger des fichiers	341
Communications	342
Cartographie du réseau	343
Regroupements d'assets	346
Appliquer des filtres à l'affichage de la cartographie	349



Afficher les détails d'un asset	350
Définir une base de référence réseau	351
Collecte de données	353
Politiques	353
Configuration des politiques	353
Groupes	354
Niveaux de sévérité	355
Notifications d'événement	356
Catégories et sous-catégories de politiques	356
Types de politiques	358
Événement de configuration - Types d'événement liés aux activités du contrôleur	358
Événement de configuration - Types d'événements liés à la validation du contrôleur	358
Types d'événements réseau	359
Types d'événements liés aux menaces réseau	363
Types d'événements SCADA	364
Activer ou désactiver des politiques	367
Afficher les politiques	369
Afficher les détails d'une politique	371
Créer des politiques	373
Création de politiques d'écriture non autorisée	384
Autres actions sur les politiques	385



Modifier des politiques	385
Dupliquer des politiques	387
Supprimer des politiques	387
Supprimer des exclusions de politique	388
Gérer les requêtes actives	389
Créer des requêtes personnalisées	393
Ajouter des restrictions	395
Modifier la variante de requête	397
Dupliquer une variante de requête	398
Exécuter une variante de requête	398
Télécharger le journal de requête	399
Types de requêtes de découverte	400
Informations d'authentification	402
Ajouter des informations d'authentification	403
Modifier des informations d'authentification	406
Supprimer des informations d'authentification	407
Comptes WMI	407
Créer des scans des plug-ins Nessus	407
Créer un scan de plug-in Nessus	410
Exécuter un scan de plug-in Nessus	415
Créer des scans OTD	415



Sources de données	418
Capteurs	419
Afficher les capteurs	420
Approuver manuellement les demandes entrantes d'appairage des capteurs	422
Configuration des requêtes actives	423
Mettre à jour les capteurs	425
Agents OT	426
Afficher les agents OT	427
Installer l'agent OT	429
Configurer l'agent OT	436
Exécuter des scans à l'aide d'un agent OT	438
Abandonner un scan	439
Mettre à jour l'agent OT	440
Supprimer un agent OT	442
Installer des agents OT à l'aide de la CLI	443
Activer, désactiver ou définir des scans planifiés pour les agents OT	445
Comparaison de l'agent OT et du capteur	447
Interface de l'agent OT Tenable	449
Panneau de contrôle	450
Dashboard	452
Scans disponibles	453



Changer de zone réseau	453
Scans	454
Charger les fichiers de scan	455
Exécuter des scans	456
Exécutions	456
Télécharger les résultats du scan	458
Journal système	458
Paramètres	460
Gérer le site	460
Appairage en ligne de l'ICP	460
Localisation	467
Gérer les connecteurs IoT	467
Configuration requise pour l'IoT Connector Agent	468
Moteur de connecteurs IoT	468
Ajouter des connecteurs IoT	468
Afficher les assets liés au connecteur IoT	470
Tester la connexion IoT	471
Modifier un connecteur IoT	471
Supprimer un connecteur IoT	472
Installer l'IoT Connector Agent sous Windows	472
Lecteur PCAP	474



Charger un fichier PCAP	475
Lire un fichier PCAP	475
Chargements manuels	476
Mettre à jour les détails des assets à l'aide d'un fichier CSV	476
Ajouter des assets manuellement	477
Fichiers SCD	478
Fichiers de projet Rockwell	480
Paramètres	482
Configuration système	486
Appareil	486
Nom du site	489
URL de l'appareil	489
Délai d'attente maximal pour la session de connexion	489
Délai maximal d'inactivité	489
Période d'expiration des ports ouverts	489
Capture de paquets	489
Approuver automatiquement les demandes d'appairage des capteurs	490
Bannière de classification	490
Activer les statistiques d'utilisation	490
GraphQL Playground	491
Configuration des ports	491



Définir les préférences du dashboard Conformité	491
Mises à jour	493
Mises à jour de l'ensemble de plug-ins Tenable Nessus	494
Configurer des mises à jour cloud automatiques des plug-ins	494
Modifier la fréquence des mises à jour des plug-ins	495
Mettre à jour manuellement les plug-ins via le cloud	496
Mises à jour hors ligne	496
Mises à jour de l'ensemble de règles du moteur IDS	499
Configurer les mises à jour cloud automatiques de l'ensemble de règles du moteur IDS	499
Modifier la fréquence des mises à jour de l'ensemble de règles du moteur IDS	499
Mettre à jour manuellement l'ensemble de règles du moteur IDS	500
Mises à jour hors ligne	501
Mises à jour cloud du DFE	503
Configurer des mises à jour cloud automatiques du DFE	503
Modifier la fréquence des mises à jour du DFE	503
Mettre à jour manuellement le DFE via le cloud	504
Mises à jour hors ligne	504
Mises à jour du moteur OT Discovery (OTD)	507
Certificats	508
Générer un certificat HTTPS	508



Charger un certificat HTTPS	509
Générer des clés API	510
Appairer l'ICP avec Enterprise Manager	511
Déconnecter l'appairage ICP avec Enterprise Manager	515
Déconnecter un appairage ICP de OT Security EM	515
Déconnecter un appairage ICP de OT Security	516
Licence	516
Paramètres de l'environnement	516
Définitions de réseau	516
Surveillance passive	517
Réseaux internes dupliqués	517
Ajouter un réseau dupliqué	517
Actions sur les réseaux internes dupliqués	524
Découvrir de nouveaux assets via SNMP	526
Récupérer une adresse IP pour les assets IoT	526
Groupes d'événements	526
Réseaux surveillés	527
Ajouter des sous-réseaux	529
Modifier un sous-réseau	531
Effectuer un scan à l'aide d'agents OT portables	531
Concepts clés	532



États de l'agent	532
Workflow de scan d'agent à l'état portable	533
Conditions préalables	533
Étape 1 : Définir le scan OT Discovery	533
Étape 2 : Lier le sous-réseau et la zone de réseaux	534
Étape 3 : Synchroniser la configuration avec l'agent	535
Étape 4 : Exécuter le scan	536
Étape 5 : Charger les résultats	536
Réseaux surveillés	537
Ajouter des sous-réseaux	539
Modifier un sous-réseau	540
Zones de réseaux	541
Afficher les zones de réseaux	542
Ajouter des zones de réseaux distante	543
Déplacer des sources vers une zone de réseaux	544
Modifier une zone de réseaux distante	546
Supprimer une zone de réseaux distante	547
Gestion des utilisateurs	548
Utilisateurs locaux	549
Afficher les utilisateurs locaux	549
Ajouter des utilisateurs locaux	550



Actions supplémentaires sur les comptes utilisateur	551
Groupes d'utilisateurs	553
Affichage des groupes d'utilisateurs	554
Ajouter des groupes d'utilisateurs	554
Actions supplémentaires sur les groupes d'utilisateurs	557
Rôles d'utilisateur	559
Zones	587
Créer des zones	587
Afficher des zones	588
Modifier une zone	589
Supprimer une zone	590
Serveurs d'authentification	590
Active Directory	590
LDAP	593
SAML	595
Groupes	597
Afficher les groupes	597
Groupes d'assets et tags	599
Tags	599
Afficher les groupes d'assets et les tags	602
Créer des groupes d'assets	604



Créer des groupes et des tags d'assets	608
Groupes de messagerie	609
Afficher des groupes de messagerie	610
Créer des groupes de messagerie	611
Groupes de ports	612
Afficher les groupes de ports	612
Créer des groupe de ports	613
Groupes de protocoles	614
Afficher les groupes de protocoles	614
Créer des groupes de protocoles	615
Groupe de planification	616
Afficher les groupes de planification	616
Créer des groupes de planification	617
Groupes de tags de contrôleur	620
Afficher les groupes de tags de contrôleur	620
Créer des groupes de tags de contrôleur	621
Groupes de règles	623
Afficher les groupes de règles	623
Créer des groupes de règles	624
Actions sur les groupes	624
Afficher les détails d'un groupe	625



Modifier un groupe	626
Dupliquer un groupe	627
Supprimer un groupe	628
Intégrations	628
Produits Tenable	629
Tenable Security Center	629
Tenable Vulnerability Management	630
Tenable One	631
Palo Alto Networks - Pare-feu de nouvelle génération (NGFW)	631
Aruba - Gestionnaire de politiques ClearPass	632
Intégration à Tenable One	633
Configurer l'intégration SAML pour Tenable One	636
Serveurs	647
Serveurs SMTP	647
Serveurs Syslog	648
Pare-feux FortiGate	651
Journal système	653
Annexe - Intégration SAML pour Microsoft Azure	654
Étape 1 - Création de l'application Tenable dans Azure	655
Étape 2 - Configuration initiale	657
Étape 3 - Mappage des utilisateurs Azure aux groupes Tenable	664



Étape 4 - Finalisation de la configuration dans Azure	670
Étape 5 - Activation de l'intégration	672
Se connecter via SSO	673



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

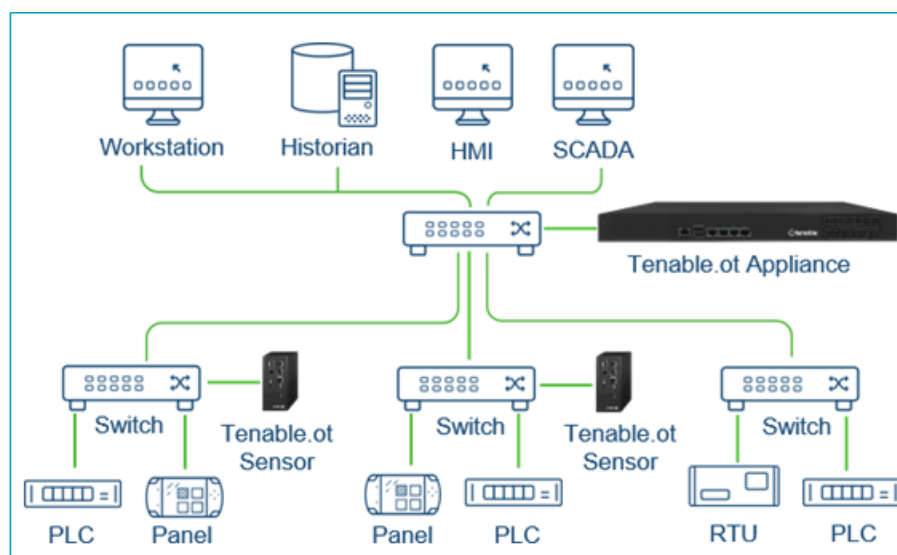
Remarque : dans ce document, l'appliance OT Security est appelée ICP (plateforme Core industrielle).

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 spécifiques¹.

¹Par 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 et les capteurs

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

ICP normale

Catégorie	ICP normale
-----------	-------------



Processeur	Intel® Xeon™ D-218dIT, 2,0 GHz
Cœurs	14
RAM	64 Go
Stockage	SSD 256 Go NVMe 800 Go Disque dur 2 To
Réseau (cuivre Ethernet)	4 x 1 Gbit/s
Réseau (fibre Ethernet)	N/A
Alimentation	Unique 110-220 V
Format	1U demi-profondeur
Dimensions (L x l x h)	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)
Humidité relative	8~90 % sans condensation
Débit SPAN maximal	500 Mbit/s

XL ICP

Catégorie	XL ICP
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 prend en charge le chiffrement complet et il est 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)	Largeur* : 482,0 mm (18,98 po) x hauteur : 42,8 mm (1,69 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

ICP-Mini

Catégorie	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
--------------------	------------

Capteur

Catégorie	Capteur
Processeur	Intel® Core™ 13-8145UE, 2,2 GHz
Cœurs	2
RAM	4 Go
Stockage	SATA M.2 128 Go
Réseau (cuivre)	2 x 1 Gbit/s
Réseau (fibre)	S/O
Alimentation	Bornier 12~28 VCC
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
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 et les serveurs. 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 et ports ouverts vulnérables). 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.

Important ! Pour acheter des produits Tenable, contactez votre représentant Tenable.

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.

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.

Playbooks opérationnels

Les playbooks opérationnels sont des guides conçus pour vous permettre d'obtenir des résultats de sécurité spécifiques à l'aide de workflows pratiques. Quel que soit votre rôle dans l'organisation OT, ces playbooks fournissent des procédures standardisées pour sécuriser vos environnements de systèmes de contrôle industriels (ICS) et SCADA (Supervisory Control and Data Acquisition).

Ces playbooks utilisent les capacités de détection multi-moteurs de OT Security ; ils combinent l'inventaire des assets, la gestion des vulnérabilités et la détection des menaces pour vous aider à conserver une posture résiliente.

Chaque workflow inclut les éléments suivants :

- Un objectif à atteindre.
- Le parcours étape par étape dans l'interface OT Security.
- Le résultat mesurable obtenu après l'exécution du workflow.

Conditions préalables

Avant d'exécuter ces playbooks, assurez-vous que votre réseau dispose des éléments suivants :



- Découverte des assets : assurez-vous que OT Security surveille au moins un segment réseau à l'aide de la découverte passive ou des requêtes actives afin d'alimenter l'inventaire.
- Autorisations utilisateur : vérifiez que vous disposez des rôles utilisateur nécessaires pour afficher les dashboards et lancer des scans.

Workflows opérationnels

Pour démarrer, explorez les workflows suivants :

- Prioriser et atténuer les vulnérabilités - Priorisez la remédiation en fonction des niveaux de menace réels (classement VPR) plutôt que des scores CVSS.
- Investiguer les menaces réseau et y répondre - Détectez et investiguez les anomalies, les malwares ou les scans réseau non autorisés.

Prioriser et atténuer les vulnérabilités

OT Security identifie les menaces telles que les CVE, les protocoles vulnérables et les ports ouverts. Il utilise le Classement VPR (Vulnerability Priority Rating) afin de générer des scores de risque pour chaque vulnérabilité. Les équipes peuvent ainsi se concentrer sur les vulnérabilités à haut risque activement exploitables, plutôt que sur les failles dont le score CVSS (Système commun d'évaluation des vulnérabilités) est le plus élevé.

Le VPR correspond au score calculé par Tenable en fonction de l'impact technique et de la threat intelligence associés à une vulnérabilité. Pour plus d'informations sur le score VPR et sur ses différences avec le score CVSS, voir cet [article de blog](#).

Objectif

Passez d'une approche réactive cherchant à « tout corriger » à une stratégie basée sur le risque : identifiez et corrigez les vulnérabilités qui présentent la plus grande menace réelle pour l'environnement opérationnel.



Conditions préalables

- OT Security doit avoir identifié des assets via la découverte passive ou active.
- (Facultatif) Intégration à Tenable Vulnerability Management ou à Tenable Security Center pour un score unifié.

Étape 1 : Afficher le dashboard Risques

1. Connectez-vous à OT Security.
2. Dans le menu de navigation de gauche, cliquez sur Risques > Détections.

La page Détections apparaît sur l'onglet Vulnérabilités par défaut, et affiche toutes les menaces réseau, y compris les CVE et les protocoles vulnérables.

The screenshot shows the 'Findings' dashboard in OT Security. The left sidebar contains a navigation menu with 'Inventory', 'Risks', 'Vulnerabilities', 'Findings' (selected), 'Compliance', 'Events', 'All Events', 'Configuration Events', 'SCADA Events', 'Network Threats', 'Network Events', 'Network', 'Network Summary', and 'Packet Captures'. The main content area is titled 'Findings' and includes a notification banner about enabling automatic cloud updates for the Nessus Plugin Set. Below the banner, there are tabs for 'Vulnerabilities' and 'Policy Violations'. A search bar contains the text 'PLC' and a '+ Add Filter' button. The main table displays '1586 Vulnerability Findings' and is filtered by 'Group By'. The table has columns for 'Affected Asset', 'IP', 'Severity', 'Plugin Name', 'Protocol', and 'Port'. The 'Severity' column is sorted in descending order, showing 'Critical' findings. The table lists several findings for Rockwell Automation Logix Controllers, all with a severity of 'Critical' and a port of '0'.

Affected Asset	IP	Severity	Plugin Name	Protocol	Port
36		Critical	Rockwell Automation Logix Controllers ...	TCP	0
A10_L81E		Critical	Rockwell Automation Logix Controllers ...	TCP	0
cnet_net		Critical	Rockwell Automation Logix Controllers ...	TCP	0
PLC #80		Critical	Rockwell Automation Logix Controllers ...	TCP	0
L16ER_APA		Critical	Rockwell Automation Logix Controllers ...	TCP	0
L43S_TN		Critical	Rockwell Automation Logix Controllers ...	TCP	0
PLC #124		Critical	Rockwell Automation Logix Controllers ...	TCP	0

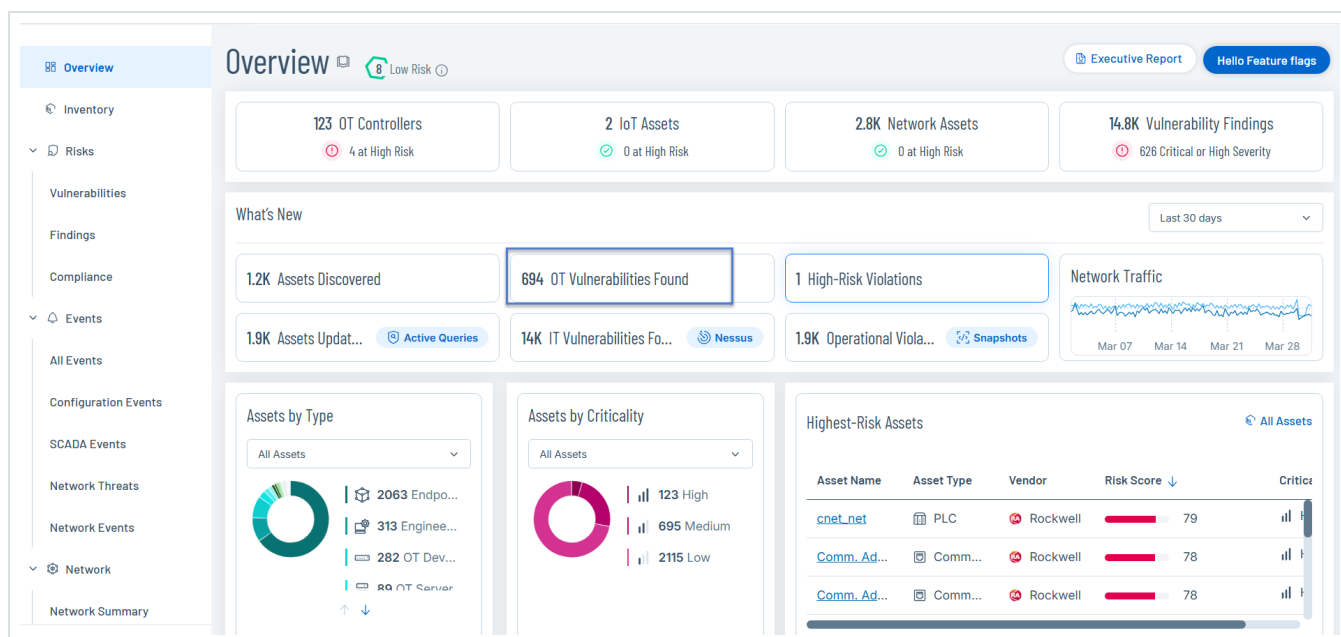
Étape 2 : Prioriser par sévérité et criticité des assets



1. Triez la liste des vulnérabilités par VPR ou sévérité (critique ou élevée) pour identifier les menaces les plus urgentes.
2. Utilisez le bouton Ajouter un filtre pour filtrer la vue et vous concentrer sur des catégories d'assets critiques, comme les contrôleurs (PLC) ou les stations d'ingénierie.

La liste Vulnérabilités affiche les résultats filtrés.

3. Vous pouvez également consulter le widget Vulnérabilités sur le dashboard Vue d'ensemble pour consulter la répartition des sévérités selon le type d'asset.



- Cliquez sur le widget Vulnérabilités OT pour accéder à la page Détections.

Étape 3 : Analyser les options de remédiation

1. Sur la page Détections, cliquez sur un asset spécifique pour ouvrir le panneau Détails de l'asset.
2. Cliquez sur une vulnérabilité spécifique pour examiner les informations détaillées et les suggestions d'atténuation fournies pour la CVE ou la vulnérabilité en question.

Findings

You can enable automatic cloud updates for the Nessus Plugin Set

Vulnerabilities Policy Violations

Search... + Add Filter

First Hit Last 7 days Status Active, Resurfaced Plugin Source Tot Severity Low, Medium, High +1

Remove All Filters Save Filter

694 Vulnerability Findings Group By

Affected Asset	IP	Severity
L36		Critical
A10_L81E		Critical
cnet_net		Critical
PLC #80		Critical

Rockwell Automation Logix Controllers Insufficiently Protected Credentials (CVE-2021-22681)

Plugin Source Tot Plugin ID 500451 Last Hit 10:45:32 AM - Mar 31, 2026

VPR 7.4/10 CVSSv3 9.8/10 Asset Criticality High

Description to verify Logix controllers are communicating with Rockwell... Show More

Solution The following text was originally created by the Cybersecurity and Infrastructure Security Agency (CISA). The original can be found at CISA.gov... Show More

Resources <https://us-cert.cisa.gov/ics/advisories/icsa-21-056-03>
<https://www.rockwellautomation.com/en-us/support/advisory.PN1550.html>
<http://www.nessus.org/u?8402eb8>
<http://www.nessus.org/u?46bc36f8>

VPR key drivers

VPR Score 7.4

- Sur la page Détections, cliquez sur le bouton Exporter pour exporter les données et les partager avec d'autres équipes et parties prenantes.

Findings

License expired—Nessus plugin set updates are not available. [Update license](#)

Vulnerabilities Policy Violations

Search... + Add Filter Status Active, Resurfaced Severity Low, Medium, High +1

Remove All Filters Save Filter

13068 Vulnerability Findings Group By

Affected Asset	IP	Severity	VPR	Plugin Name	Protocol
		Critical	10	Rockwell Automation Stratix 5800 & 52...	TCP
L36		Critical	7.4	Rockwell Automation Logix Controllers ...	TCP
A10_L81E		Critical	7.4	Rockwell Automation Logix Controllers ...	TCP



Conseil : si vous avez intégré OT Security à Tenable One ou Tenable Security Center, vous pouvez approfondir l'analyse des détections dans ces applications. Pour plus d'informations sur l'intégration avec Tenable One ou Tenable Security Center, voir [Intégrations](#).

Résultat

Vous disposez d'une liste hiérarchisée de vulnérabilités pertinentes pour votre environnement, ce qui permet d'optimiser l'allocation des ressources de maintenance de manière à réduire les risques les plus importants.

Investiguer les menaces réseau et y répondre

OT Security utilise plusieurs moteurs de détection - anomalies comportementales, détection basée sur les signatures (Suricata) et règles basées sur des politiques - pour identifier le trafic typique des cyber-attaques.

Objectif

Détecter et investiguer les activités réseau suspectes, telles que les scans non autorisés, la propagation de malware ou les anomalies de protocole, afin d'éviter toute perturbation des opérations.

Conditions préalables

Vous devez disposer des autorisations requises pour afficher les événements.

Vous devez configurer ce qui suit :

- Configurez la surveillance du réseau. Voir [Réseaux surveillés](#).
- Activez les politiques de détection. Voir [Activer ou désactiver des politiques](#).



- (Facultatif) Activez la capture PCAP pour l'analyse forensique. Voir [Télécharger des fichiers de capture individuels](#).

Étape 1 : Surveiller les alertes d'événements

1. Connectez-vous à OT Security.
2. Dans le volet de navigation de gauche, cliquez sur Événements.
3. Sélectionnez Menaces réseau ou Événements réseau pour afficher les alertes liées aux tentatives d'intrusion ou aux anomalies du trafic.

Overview

Inventory

Risks

Vulnerabilities

Findings

Compliance

Events

All Events

Configuration Events

SCADA Events

Network Threats

Network Events

> Network

> Data Collection

Version 4.6.23, Expires Apr 2, 2026

All event actions are now available in Policy Violation Findings view [Go to Policy Violation Findings](#)

Network Events

Search...

Actions

Status	Log ID	Time	Event Type	Severity	Policy Name	Source Asset	Source Address
☐ Not resolved	9018	12:00:46 PM · Feb 18, 2026	Failed Unsecured...	Medium	Failed unsecured FTP login	Eng. Station #4	
☐ Not resolved	4	11:18:44 AM · Feb 3, 2026	Unauthorized Co...	Medium	Conversation in a Comm...	DESKTOP-JLPT59P	
☐ Not resolved	3	11:18:28 AM · Feb 3, 2026	Unauthorized Co...	Medium	Conversation in a Comm...	DESKTOP-JLPT59P	
☐ Not resolved	2	11:18:33 AM · Feb 3, 2026	Unauthorized Co...	Medium	Conversation in a Comm...	DESKTOP-JLPT59P	
☐ Not resolved	2632	12:19:26 PM · Feb 6, 2026	Failed Unsecured...	Medium	Failed unsecured FTP login	Eng. Station #12	
☐ Not resolved	10273	05:38:52 PM · Feb 19, 2026	Failed Unsecured...	Medium	Failed unsecured FTP login	OT Device #219	

Items: 10445

Event 9018 12:00:46 PM · Feb 18, 2026 Failed Unsecured FTP login Medium Not resolved

Details

An attempt to log in using FTP has failed

Source

Source Name [Eng. Station #4](#)

Destination

Source IP Address

Destination Name [Server #11](#)

Policy

Destination IP Address

Status

Why is this important?

A failed log-in attempt may be a human error, but might also suggest an attacker who is implementing brute force to access the server.

Suggested Mitigation

1) Track the station and user that attempted access and verify that it wasn't done by a malicious actor.

4. Triez les événements par sévérité (élevée ou critique) afin de mettre en évidence les menaces immédiates.

Étape 2 : Analyser les données de conversation

1. Sélectionnez un événement particulier pour afficher le volet Détails de l'événement.
2. Identifiez les assets sources et cibles impliqués dans l'activité suspecte.



Event 9018 12:00:46 PM · Feb 18, 2026 Failed Unsecured FTP login Medium Not resolved			
Details	Name	Eng_Station #4	Asset Criticality
Source	Type	Engineering Station	Vendor
Destination	Risk Score	53	Purdue Level
Policy	IPs		Location
Status	MACs		Description

3. Accédez à la page Réseau > Conversations pour afficher les flux de trafic spécifiques entre ces assets.

Events	Conversations							
	Search...							
All Events	Start Time	End Time	Duration	Bytes	Packets	Source Address	Destination Ad...	Protocol
Configuration Events	Completed (10000)							
SCADA Events	Mar 6, 2026 12:59:59 PM	Mar 6, 2026 01:01:28 PM	1 minute	484	13			DNS (53/UDP)
Network Threats	Mar 6, 2026 12:59:59 PM	Mar 6, 2026 01:01:28 PM	1 minute	568	15			DNS (53/UDP)
Network Events	Mar 6, 2026 12:59:55 PM	Mar 6, 2026 12:59:59 PM	4 seconds	1440	16			NTP (123/UDP)
Network	Mar 6, 2026 12:59:55 PM	Mar 6, 2026 01:00:55 PM	1 minute	1500	30			CINEGRFX-LM (17...
	Mar 6, 2026 12:59:55 PM	Mar 6, 2026 01:00:55 PM	1 minute	1500	30			ENCORE (1740/U...
Network Summary	Mar 6, 2026 12:59:55 PM	Mar 6, 2026 01:00:55 PM	1 minute	1500	30			CISCO-NET-MGM...
Packet Captures	Mar 6, 2026 12:59:55 PM	Mar 6, 2026 01:00:55 PM	1 minute	1500	30			3COM-NSD (1742...
Conversations	Mar 6, 2026 12:59:49 PM	Mar 6, 2026 12:59:49 PM	1 second	2916	12			BROWSER (138/U...
Network Map	Mar 6, 2026 12:59:49 PM	Mar 6, 2026 01:00:01 PM	12 seconds	3605	20			HTTPS (443/TCP)
Data Collection	Mar 6, 2026 12:59:48 PM	Mar 6, 2026 12:59:48 PM	1 second	3888	16			BROWSER (138/U...
	Mar 6, 2026 12:59:48 PM	Mar 6, 2026 12:59:48 PM	1 second	2916	12			BROWSER (138/U...
Settings	Mar 6, 2026 12:59:48 PM	Mar 6, 2026 12:59:48 PM	1 second	2430	10			BROWSER (138/U...
	Mar 6, 2026 12:59:47 PM	Mar 6, 2026 12:59:47 PM	1 second	129	1			PANDO-PUB (768...
System Configuration	Mar 6, 2026 12:59:42 PM	Mar 6, 2026 01:00:42 PM	1 minute	1320	24			TRIPE (4070/UDP)
	Mar 6, 2026 12:59:42 PM	Mar 6, 2026 01:00:42 PM	1 minute	864	12			CISCO-SCCP (200...

4. Si elle est disponible, utilisez la vue Captures de paquets (PCAP) pour analyser les données de trafic brutes et obtenir des preuves forensique. Voir [Télécharger des fichiers de capture individuels](#).

Étape 3 : Lancer la réponse

- Examinez la limitation suggérée dans la section Détails de l'événement et prenez des mesures (isolez l'asset compromis, par exemple).



- Si l'événement s'avère être un faux positif, modifiez la configuration de la politique pour affiner la détection et réduire le bruit. Voir [Politiques](#).
- Dans Détections > Violations de politique, marquez l'événement comme résolu pour l'effacer de la file d'attente active. Voir [Violations de politique](#).

Résultat

Vous pouvez identifier rapidement le « qui, quoi, où et quand » d'un incident de sécurité et ainsi minimiser le temps moyen de réponse (MTTR).

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	HostUnreachableError	Impossible	Impossible	Vérifiez les



requêtes actives		d'atteindre une cible de requête. Vérifiez votre routage.	d'accéder à l'appareil. Cela peut être dû à un problème de connectivité réseau. Veuillez vérifier les paramètres de votre réseau ou de votre pare- feu, puis réessayez.	paramètres de connectivité réseau et du pare-feu, puis renvoyez la requête 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	Renvoyez la requête après un certain temps.



			lancer la requête plus tard.	
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. Veuillez vérifier votre connectivité réseau, puis renvoyer la requête.	Vérifiez votre connectivité réseau, puis renvoyez 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	Vérifiez si l'appareil cible est compatible ou renvoyez la requête après un certain temps.



			sur l'appareil ou à un problème temporaire du réseau. Veuillez vérifier la compatibilité de l'appareil ou renvoyer la requête plus tard.	
Gestion des requêtes actives	AuthenticationError	Des identifiants d'authentification non valides ont été utilisés dans la requête.	Échec de l'authentification auprès de l'appareil. Les informations d'identification sont peut-être incorrectes ou manquantes. Veuillez vérifier vos informations d'identification.	Vérifiez vos informations d'authentification et renvoyez la requête.



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 ou plage d'adresses IP).	La requête active n'a trouvé aucun appareil accessible dans la plage cible. Des restrictions appliquées par les utilisateurs	Il se peut que les appareils cibles ne soient pas accessibles en raison de restrictions appliquées par l'utilisateur. Revoyez vos paramètres



			pourraient bloquer certains appareils (bloc CIDR, liste d'assets ou plage d'adresses IP). Veuillez vérifier votre sélection et vos contrôles d'accès.	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. Un problème s'est peut-être produit lors du démarrage ou après la réinitialisation.	Le service de connecteur IoT n'est pas disponible ou a rencontré un problème. Réessayez plus tard. Si le problème persiste, contactez l'assistance.	Le service de connecteur IoT est peut-être temporairement indisponible. Renvoyez la requête après un certain temps. Si le problème persiste, contactez l'assistance technique.
IoT	lotConnectorSecureModeError	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	Réinstallez l'agent IoT sur le système distant et relancez la connexion.



			connexions.	
IoT	lotConnectorIpAlreadyExists	L'utilisateur essaie d'ajouter un connecteur avec une adresse IP qui existe déjà.	Échec de la création du connecteur. L'adresse IP fournie est déjà utilisée par un autre connecteur. Veuillez fournir une adresse IP unique, puis réessayer.	Fournissez une adresse IP unique et essayez d'ajouter le 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.	Générez un nouveau certificat de sécurité et essayez d'appairer l'ICP à EM. Si le problème persiste, contactez l'administrateur du serveur.



			ur 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, puis réessayer.	Fournissez l'adresse IP ou le nom d'hôte du serveur auquel vous souhaitez vous connecter, puis réessayez.
Appairage du serveur : (EM, serveur externe, FW)	MissingPassword	Uniquement via l'API	Les informations d'authentifica tion fournies sont incomplètes. Veuillez saisir le mot de passe du	Fournissez un nom d'utilisateur et le mot de passe du serveur, puis réessayez.



			serveur d'appairage et réessayer.	
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'identification de



			l'appairage avec ce serveur. Veuillez supprimer la clé API ou les informations d'identification de l'utilisateur, puis réessayer.	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	Charger un fichier de configuration



			joint. Veuillez charger un fichier de configuration valide au format pris en charge pour continuer.	valide.
Flux OT: PII/Suricata/Ne ssus	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/Ne ssus	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/Ne ssus	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.

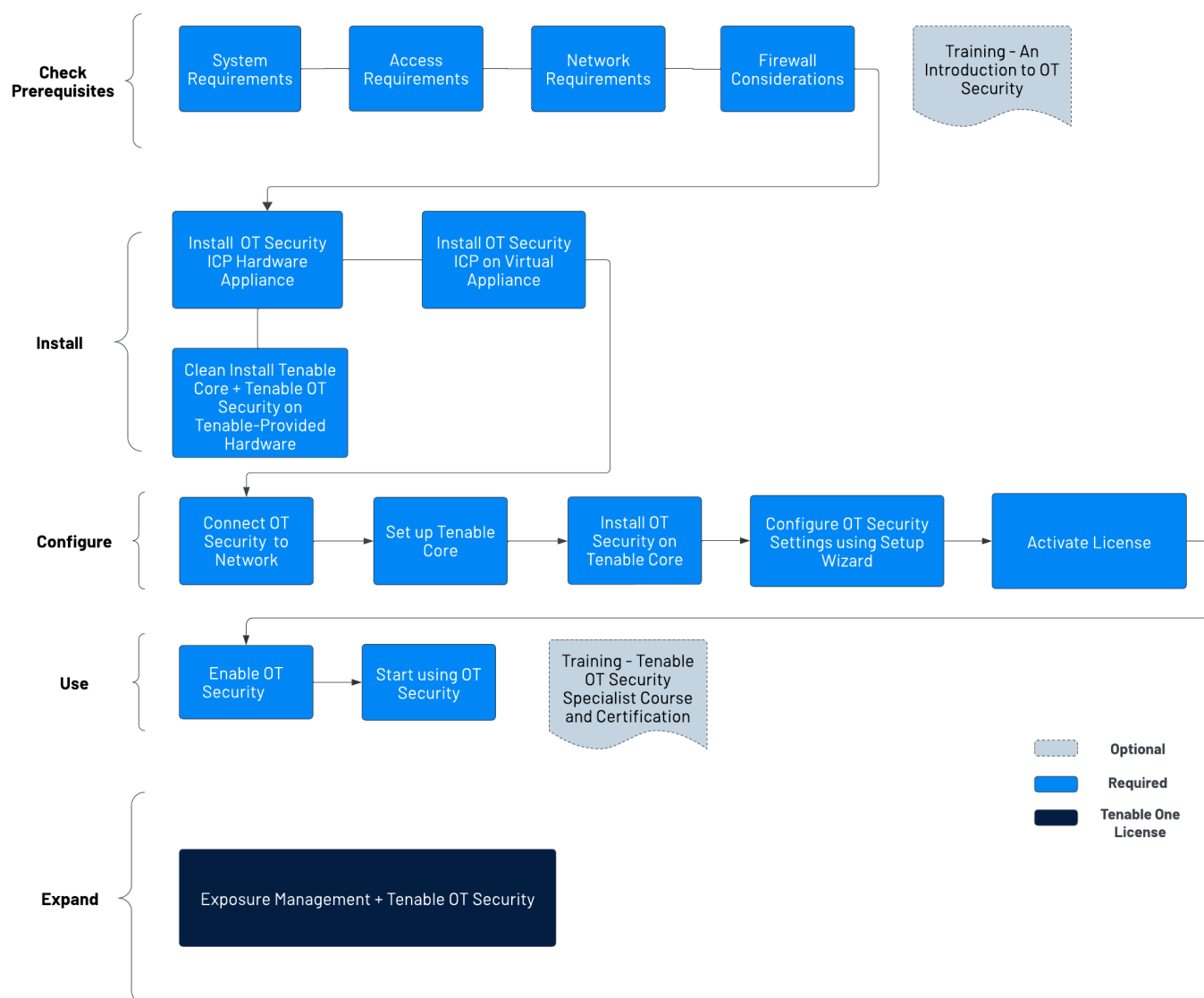


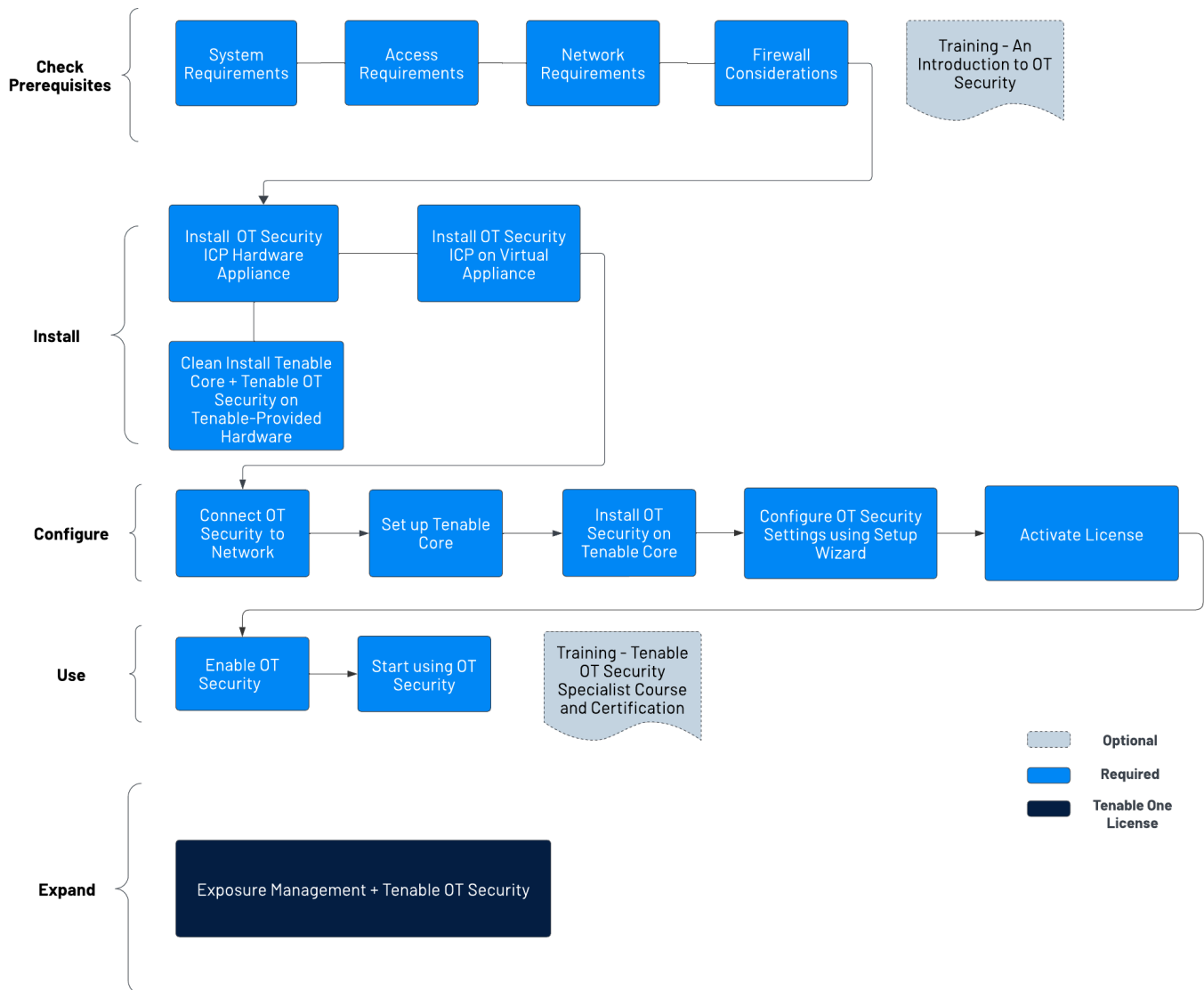
Flux OT: PII/Suricata/Ne ssus	UpdateAlreadyInProgre ss	L'utilisateur exécute actuellement une mise à jour alors qu'une tâche est déjà en cours. Une seule mise à jour peut être exécutée à la fois.	Une mise à jour est déjà en cours pour cet appareil. Veuillez attendre que la mise à jour en cours soit terminée avant d'en tenter une autre.	Attendez que la mise à jour en cours soit terminée avant de réessayer.
Flux OT: PII/Suricata/Ne ssus	OlderVersionUpdateAtt empt	L'utilisateur tente de revenir à une version antérieure.	Échec du téléchargem ent du fichier en raison d'une version active plus récente. Assurez- vous d'avoir le fichier le plus à jour et essayez de le télécharger à nouveau.	Assurez-vous que le fichier que vous essayez de charger est la dernière version.

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, System Time 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 et les serveurs d'authentification pour commencer à utiliser OT Security.

Conseil : pour acquérir une expérience pratique et pour obtenir la certification de spécialiste Tenable OT Security, suivez la Formation Specialist 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 :

- Accédez à **Exposure View** (Vue de l'exposition) pour révéler les niveaux de risque convergés et découvrir 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 :
 - Affichez et gérez les fiches de cyber-exposition.
 - Affichez le score CES et les données sur les tendances du score CES pour les fiches d'exposition Globale et Technologies opérationnelles.
 - Affichez les données de l'accord de niveau de service (SLA) de remédiation.
 - Afficher les données sur les performances des tags.
- Accédez à la page **Exposure Signals** (Signaux de cyber-exposition) afin de générer des signaux d'exposition qui utilisent des requêtes pour rechercher des *violations* d'assets. En termes simples, si un asset est impacté par une faiblesse liée à la requête, il est considéré comme une *violation*. Cela vous permet de gagner en visibilité sur vos scénarios de risque les plus critiques.
 - Recherchez les principales menaces actives de votre environnement grâce aux flux à jour de Tenable Research.
 - Affichez, générez et interagissez avec les données des requêtes et les violations des assets impactés.



- Créez des signaux d'exposition personnalisés pour afficher les risques et les faiblesses spécifiques à l'entreprise
- Accédez à la page **Inventaire** pour enrichir 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 :
 - Affichez les données de l'onglet **Assets** et interagissez avec elles :
 - Examinez vos assets AD pour comprendre la nature stratégique de l'interface. Cela devrait vous aider à choisir les fonctionnalités à utiliser dans Tenable Exposure Management et dans quelles circonstances les utiliser.
 - Familiarisez-vous avec la recherche globale d'assets, ses objets et ses propriétés. Ajoutez des requêtes personnalisées aux favoris pour les réutiliser ultérieurement.
 - Recherchez les appareils, les comptes utilisateur, les logiciels, les assets cloud, les applications SaaS, les réseaux et leurs faiblesses.
 - Explorez la page des **détails de l'asset** pour consulter les propriétés de l'asset et toutes les vues contextuelles associées.
 - Affichez les données de l'onglet **Faiblesses** et interagissez avec elles :
 - Visualisez le contexte clé des faiblesses liées à une vulnérabilité ou à une mauvaise configuration pour prendre les décisions les plus efficaces en matière de remédiation.
 - Affichez les données de l'onglet **Logiciel** et interagissez avec elles :
 - Bénéficiez d'une visibilité totale sur les logiciels déployés au sein de votre entreprise pour mieux comprendre les risques associés.



- Identifiez quels logiciels sont susceptibles d'être obsolètes et quels composants logiciels pourraient prochainement arriver en fin de vie (EoL).
- Affichez les données de l'onglet **Détections** et interagissez avec elles :
 - Affichez les instances de faiblesses (vulnérabilités ou mauvaises configurations) apparaissant sur un asset, identifiées de manière unique par ID de plug-in, port et protocole.
 - Examinez les informations sur ces détections (descriptions, assets affectés, criticité, etc.) pour identifier les risques de sécurité potentiels, assurer la visibilité sur les ressources sous-utilisées et soutenir les efforts de conformité.
- Accédez à la page **Chemin d'attaque** pour optimiser la priorisation des risques en exposant les chemins d'attaque à risque qui traversent la surface d'attaque, notamment les applications web, IT, OT, IoT, les identités et ASM, afin d'éviter tout impact significatif. Simplifiez la réduction des risques en identifiant des points d'étranglement afin de perturber les chemins d'attaque grâce à des conseils adaptés, et approfondissez votre expertise grâce aux informations exploitables de l'IA (non pris en charge dans les environnements **FedRAMP**).
 - Affichez l'onglet **Dashboard** 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 techniques d'attaque 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 les chemins menant à vos assets les plus précieux, c'est-à-dire ceux avec un classement ACR de 7 ou plus.



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

- Dans l'onglet **Top Attack Techniques** (Principales techniques d'attaque), 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 techniques d'attaque qui vous aideront à comprendre et à traiter les inconnues qui favorisent et amplifient l'impact des menaces sur vos assets et vos informations.
- Dans l'onglet **Top Attack Paths** (Chemins d'attaque principaux), générez des requêtes de chemin d'attaque pour afficher vos assets dans le cadre de chemins d'attaque potentiels :
 - Generate an Attack Path with a Built-in Query (Générer un chemin d'attaque à l'aide d'une requête intégrée)
 - Generate an Attack Path Query with the Attack Path Query Builder (Générer une requête de chemin d'attaque à l'aide du générateur de requêtes de chemin d'attaque)
 - Generate an Asset Query with the Asset Query Builder (Générer une requête d'asset à l'aide du générateur de requêtes d'asset)

Vous pouvez ensuite afficher 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.

- Interagissez avec l'onglet **MITRE ATT&CK Heatmap** (Carte thermique MITRE ATT&CK), sélectionnez l'option de carte thermique ICS pour vous concentrer sur les tactiques et techniques ICS (systèmes de contrôle industriels)
- Affichez les données de l'onglet **Tags** et interagissez avec elles :



- Créez un tag dynamique pour vos assets OT, où :
 - Opérateur = type de système hôte
 - Valeur = PLC
- Créez et gérez des tags pour mettre en évidence ou combiner différentes classes d'assets.
- Affichez la page des détails du tag pour obtenir plus d'informations sur les tags associés à vos assets.

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

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.



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 pré-imagées qui simplifient le déploiement et réduisent le temps de configuration. Vous pouvez également vous procurer votre propre matériel et lui appliquer l'image ISO Tenable. Si vous fournissez votre matériel ou choisissez d'utiliser le matériel Tenable, reportez-vous aux [spécifications matérielles Tenable OT Security](#) (en anglais) pour obtenir des conseils. Tous les composants de OT Security, l'ICP, Enterprise Manager (EM) et le capteur peuvent être exécutés sur n'importe quel matériel conforme 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	205 Go

Configuration requise pour les capteurs virtuels OT Security

Scénario d'installation	Processeur	Mémoire	Espace disque
Capteur	2 processeurs virtuels	4 Go de RAM	Disque dur 60 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 : $(23 \times 2) \times 2,7 = 124$ 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	Minimum 205 Go	Minimum deux interfaces réseau
50-150 Mbit/s	16	32 Go de RAM	Minimum 205 Go	Minimum deux interfaces réseau
150-300 Mbit/s	32	64 Go de RAM	Minimum 205 Go	Minimum deux interfaces réseau
300 Mbit/s à 1 Go	32-64	128 Go de RAM ou plus	Minimum 205 Go	Minimum deux interfaces réseau

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 : Tenable ne requiert 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*.

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

Exigences d'accès

Votre déploiement Tenable Core + Capteur OT Security 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 pouvoir 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 `sensor.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.
	Microsoft Hyper-V	fichier .zip	
Cloud	Amazon Web Services (AWS)	S/O	Un accès Internet est requis pour déployer ou mettre à jour Tenable Core.
Cloud	Microsoft Azure	S/O	
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 Tenable Core + Capteur Tenable OT Security 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. 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 (par défaut).
TCP 8090	Communications HTTPS entrantes pour la restauration des sauvegardes. Communications entrantes avec le serveur de chargement de fichiers.

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 <code>appliance.cloud.tenable.com</code> et <code>sensor.cloud.tenable.com</code> 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) nécessite quelques connexions réseau, appelées rôles d'interface.

Interface de gestion et des requêtes actives



Il s'agit d'une interface configurée avec une adresse IP qui autorise l'accès au réseau pour gérer et configurer l'appliance. Cet interface permet à l'appliance d'atteindre les assets du réseau pour les requêtes actives (recommandé, mais facultatif),

Séparation des rôles de gestion et de requête active (port fractionné)

Vous pouvez diviser les rôles de gestion et de requête active entre deux interfaces distinctes. Cela permet, par exemple, d'établir une connexion à un réseau IT à des fins de gestion et une connexion distincte à un réseau OT pour accéder aux assets OT à l'aide d'une requête active.

Pour cela, préparez et connectez deux interfaces distinctes, chacune dédiée à l'un des rôles.

La connectivité de gestion de base à l'ICP via l'interface de requête active est autorisée et opérationnelle tant que le système ICP autorise la connectivité réseau.

Pour finaliser la configuration d'OT Security, vous avez besoin d'une connectivité de gestion. Vous pouvez configurer le fractionnement de port et la connectivité de requête active plus tard.

Sur les appliances matérielles fournies par Tenable, OT Security est automatiquement installé avec les rôles d'interface par défaut (rôles de gestion et de requête active combinés).

Remarque : lors de la configuration de l'adresse IP pour les deux interfaces, Tenable recommande de configurer uniquement une passerelle par défaut pour l'interface dédiée au rôle de gestion. Vous pouvez spécifier une passerelle dédiée pour la requête active lors de la configuration d'un port fractionné.

Interfaces de surveillance

Il est possible d'utiliser une ou plusieurs interfaces réseau pour la surveillance passive du réseau.

Les interfaces de surveillance passive (SPAN) :

- Surveillent et collectent passivement le trafic à des fins d'analyse
- Doivent être connectées 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.



Remarque : le trafic qui ne peut pas être directement surveillé par les interfaces de l'appliance peut être collecté à l'aide des capteurs OT ou de la configuration d'analyseur de ports encapsulé à distance (ERSPAN).

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.

Remarque : pour que les mises à jour centralisées d'EM fonctionnent, l'ICP doit pouvoir accéder aux ports 28305 et 8000 (TCP).

Sens du flux	Port	Communique avec	Usage
Entrant	TCP 443	Interface web pour l'appliance OT Security	Accès du navigateur à OT Security
Entrant	TCP 8000	Interface web pour Tenable Core	Accès par navigateur à Tenable 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 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*	<u>Divers protocoles industriels</u>	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	Serveur AD	Authentification AD LDAP



Sens du flux	Port	Communique avec	Usage
	636		
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



Sens du flux	Port	Communique avec	Usage
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 28304 (SSH) TCP 443 (HTTPS)	ICP/OT Security Connexions SSH pour l'appairage des capteurs. 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.

Remarque : OT Security prend en charge les requêtes sur ces protocoles, mais il est possible que certains ne s'appliquent pas à votre environnement. Pour des résultats optimaux, veillez à ouvrir autant de ports répertoriés que possible entre OT Security (ou les capteurs OT Security) et les appareils distants à proximité. Cette action accroît la précision de l'identification et des requêtes.

Protocole	Port	Communique avec	Usage
ICMP		Générique/Divers	Découverte/ping des assets au niveau du réseau
TCP	21	Générique/Divers	Transfert de fichiers FTP
TCP/UDP	53	Serveurs DNS	Requêtes de résolution du système de noms de domaine (DNS)
TCP	80	Générique/Divers	Empreinte digitale HTTP et accès à l'interface web
TCP	102	Appareils Siemens	Protocole MMS (Manufacturing Message Specification), chevauche la norme CEI 61850
TCP	102	Appareils Siemens	CEI 61850/MMS pour les sous-stations et les appareils SCADA
TCP	102	Appareils Siemens	Communication S7/S7+/MMS pour les appareils d'automatisation
UDP	111	Appareils Emerson Ovation	Inscription/découverte du service RPC pour Ovation
TCP	135	Appareils Windows	Requêtes WMI pour la gestion des



Protocole	Port	Communique avec	Usage
			systèmes et réseaux
UDP	137	Générique/Divers	Service de nom NetBIOS (MBNS) pour la découverte de réseau Windows
UDP	138	Générique/Divers	Service de datagramme NetBIOS (NBT) pour le partage de fichiers/d'imprimantes Windows
UDP	161	Générique/Divers	Interrogation SNMP et communication de traps
TCP	443	Générique/Divers	Empreinte digitale HTTPS et services web sécurisés
TCP	445	Appareils Windows	Requêtes WMI/SMB pour la gestion des systèmes (remplace 135 dans certains cas)
TCP	502	Appareils OT	Communication Modbus TCP avec les PLC et les compteurs
UDP	1069	Caméras Cognex	Protocole de découverte du système de vision Cognex
TCP	1911	Contrôleurs BMS	Protocole non chiffré Niagara FOX
TCP	1962	Appareils Phoenix Contact	Ingénierie et contrôle de la communication PC Worx
TCP/UDP	2001	Appareils Profinet	Communication entre appareils



Protocole	Port	Communique avec	Usage
			Profinet pour les contrôleurs et les modules E/S
TCP	2001	Appareils Siemens	SICAM/PROFINET (appareils hérités et sous-stations)
TCP	2222	Appareils Rockwell	Protocole PCCC pour les communications ControlLogix/PLC
TCP	2404	Appareils SCADA	CEI 60870-5-104 pour les communications entre RTU et sous-stations
TCP	3389	Appareils Windows	RDP (Remote Desktop Protocol)
TCP	3500	Appareils Bachmann M1	Communication du contrôleur Bachmann M1
TCP	4000	Appareils Emerson	Données/contrôle du contrôleur Emerson ROC 4000
TCP	4444	Schneider Electric	Contrôleurs SmartX (EcoTrusture Building Operation)
UDP	4800	Appareils Moxa	Protocole de découverte des appareils Moxa
TCP	4911	Contrôleurs BMS	Protocole sécurisé (TLS/SSL) Niagara FOX
TCP	5001	Appareils Bosch	Bosch PSI (Programmable System Interface)



Protocole	Port	Communique avec	Usage
TCP	5002	Appareils Mitsubishi	Protocole MC sur TCP pour PLC MELSEC
TCP	5007	Appareils Mitsubishi	Port de communication supplémentaire pour PLC MELSEC
UDP	5009	Appareils Mitsubishi	Diffusion du localisateur MELSEC (découverte de l'appareil)
TCP	5033	Appareils Siemens	Protocole P2 (utilisé dans les anciens systèmes d'automatisation Siemens)
TCP	5050	Appareils Saia-Burgers	Communication des contrôleurs Saia PCD
TCP	5094	HAR-IP	HAR-IP sur TCP pour l'instrumentation intelligente
TCP	5313	Yokogawa DCS	Interface d'ingénierie CENTUM DCS
TCP	5432	Appareils SEL (Schweitzer)	Accès à la base de données PostgreSQL pour les appareils à source d'énergie
TCP	6626	Appareils WAGO	Communication et programmation des E/S WAGO
TCP	7700	Schneider Electric	Wattmètres et systèmes de gestion de l'énergie ION
TCP	8000, 8008, 8080, 8443,	Générique/Divers	Ports alternatifs HTTP/HTTPS courants



Protocole	Port	Communique avec	Usage
	8800		
TCP	9940	Yokogawa DCS	Statut et diagnostic CENTUM
UDP	12321	Appareils Honeywell	Découverte/redondance UDP Honeywell FTE
TCP	18245	Appareils Schneider	Protocole SRTP (Schneider Real-Time Protocol) pour les PLC M340/M580
TCP	18507	Appareils Emerson	ROC/Calculateurs de débit Emerson (protocole ACE)
TCP	18508	Appareils Emerson	Service de mise à niveau des micrologiciels Emerson (UPGD)
TCP	20256	Appareils GE	Protocole PCOM pour Proficy iFix/CIMPLICITY SCADA
TCP	20547	Procon	Interface de gestion à distance PROCON OS
TCP	24576	Appareils ABB	Protocole ABB Network Control (ABB_NC) pour l'automatisation des sous-stations
TCP	34964	Appareils Siemens	PROFINET Connection Management (PROFINET CM)
TCP	39329	Appareils Emerson	Ovation/Systèmes de contrôle basés sur VME



Protocole	Port	Communique avec	Usage
TCP/UDP	44818	Appareils OT	Protocole CIP (Common Industrial Protocol) pour les appareils Rockwell
UDP	47808	Contrôleurs BMS	Communication BACnet/IP pour les appareils d'automatisation des bâtiments
TCP/UDP	48898	Appareils Beckhoff	Protocole ADS/TwinCAT pour les communications des contrôleurs et de l'ingénierie
UDP	48899	Appareils Beckhoff	Découverte ADS/AMS (IPC TwinCAT/Beckhoff)
TCP	50000	Appareils Siemens	Communication des relais SIPROTEC 4
TCP	51966	Appareils Honeywell	Communications Honeywell FTE (Fault Tolerant Ethernet)
TCP	55553	Appareils Honeywell	Communications CEE (Control Execution Environment) dans Experion PKS
TCP	55565	Appareils Honeywell	Communications FTE (Fault Tolerant Ethernet) pour la redondance dans Experion PKS

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

Agent OT

Sens du flux	Port	Communique avec	Usage
Sortant	443	OT Security	Premier appairage avec un agent OT.
Sortant	28306	OT Security	Connexion à l'agent OT.

IoT Connector Agent

Sens du flux	Port	Communique avec	Usage
Sortant	TCP 10146 (port sécurisé)	Connecteur IoT	Connecte l'ICP à l'IoT Connector Agent
Sortant	TCP 10104 (port non sécurisé)	Connecteur IoT	Connecte l'ICP à l'IoT Connector Agent



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'apppliance OT Security sur une surface plane :

1. Placez l'apppliance 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	2.75 GB	Mar 15, 2024	Checksum	
OVA Specifications:					
◦ CPU: 4					
◦ Memory: 16384 MB					
◦ Disk: 205 GB					
◦ Includes Tenable.ot 3.18.51					
  Tenable-Core-OL8-Tenable.ot-20240404.iso	Tenable Core Tenable.ot Installation ISO	958 MB	Apr 4, 2024	Checksum	
◦ Requires an internet connection					
◦ Installs the latest version of Tenable.ot and the latest system packages					
  Tenable-Core-OL8-Tenable.ot-offline-20240404.iso	Tenable Core Tenable.ot Self-Contained Installation ISO	3.32 GB	Apr 4, 2024	Checksum	
◦ Includes Tenable.ot 3.18.51					

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

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



ISOHybrid image detected



The image you have selected is an 'ISOHybrid' image. This means it can be written either in ISO Image (file copy) mode or DD Image (disk image) mode. Rufus recommends using ISO Image mode, so that you always have full access to the drive after writing it. However, if you encounter issues during boot, you can try writing this image again in DD Image mode.

Please select the mode that you want to use to write this image:

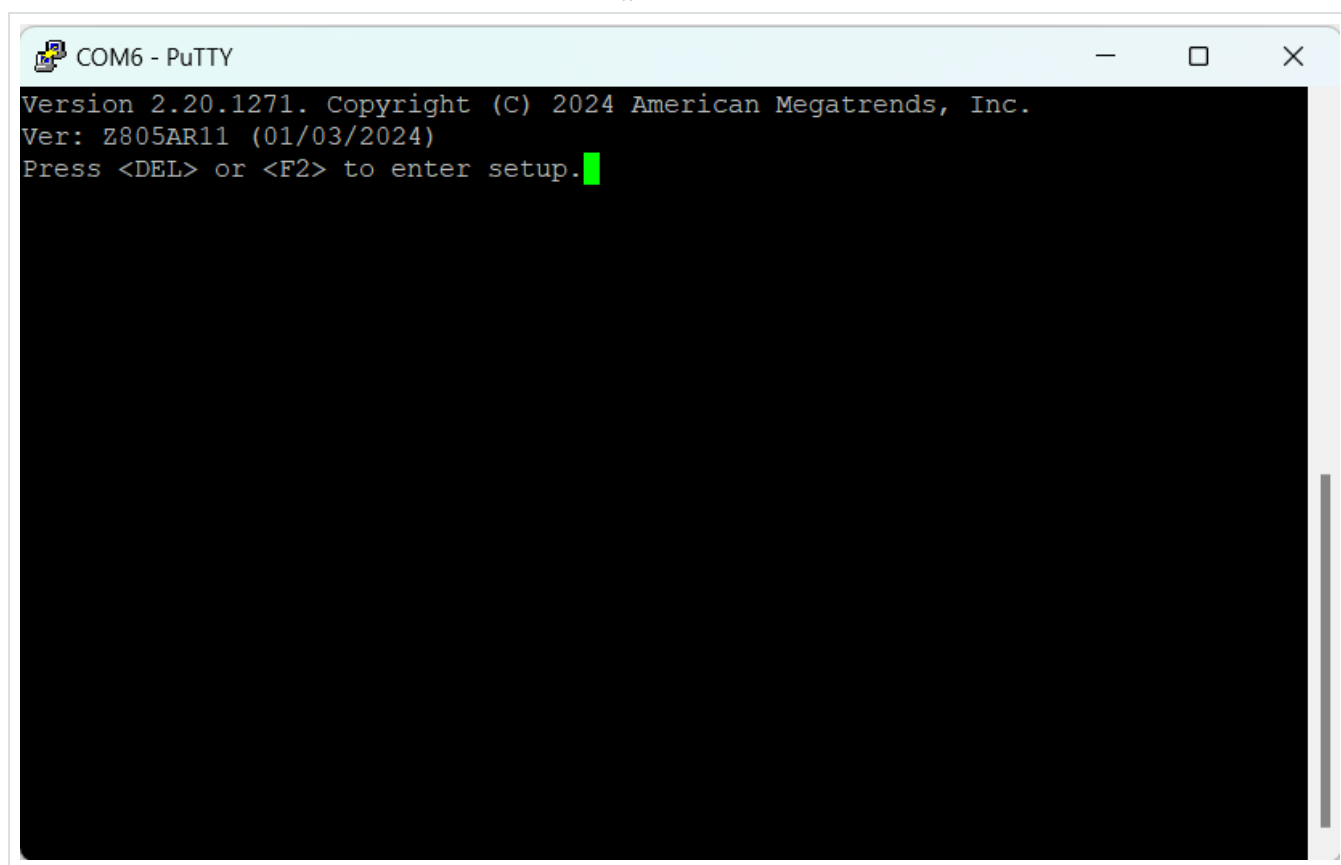
☐ Write in ISO Image mode (Recommended)

☒ Write in DD Image mode

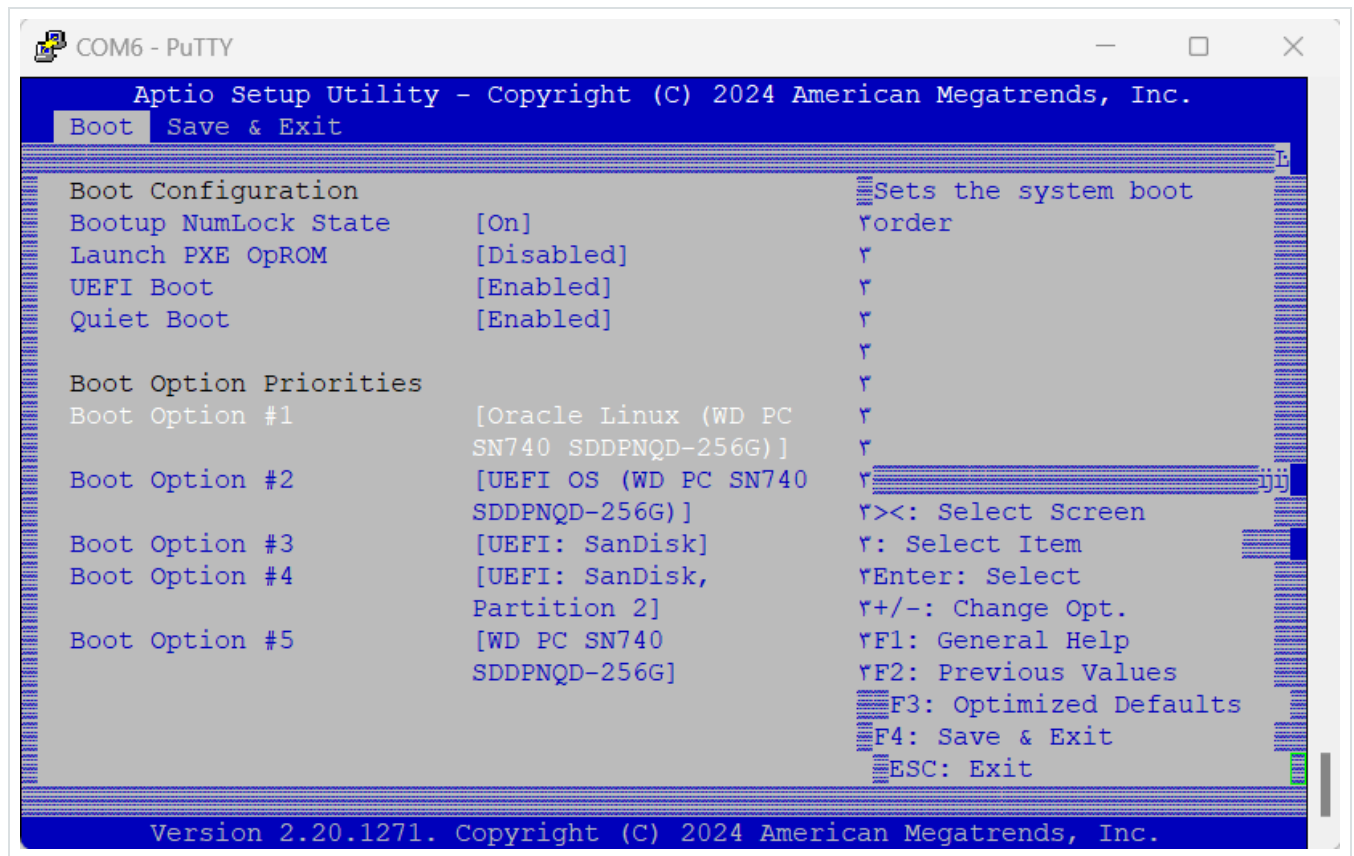
OK

Cancel

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.

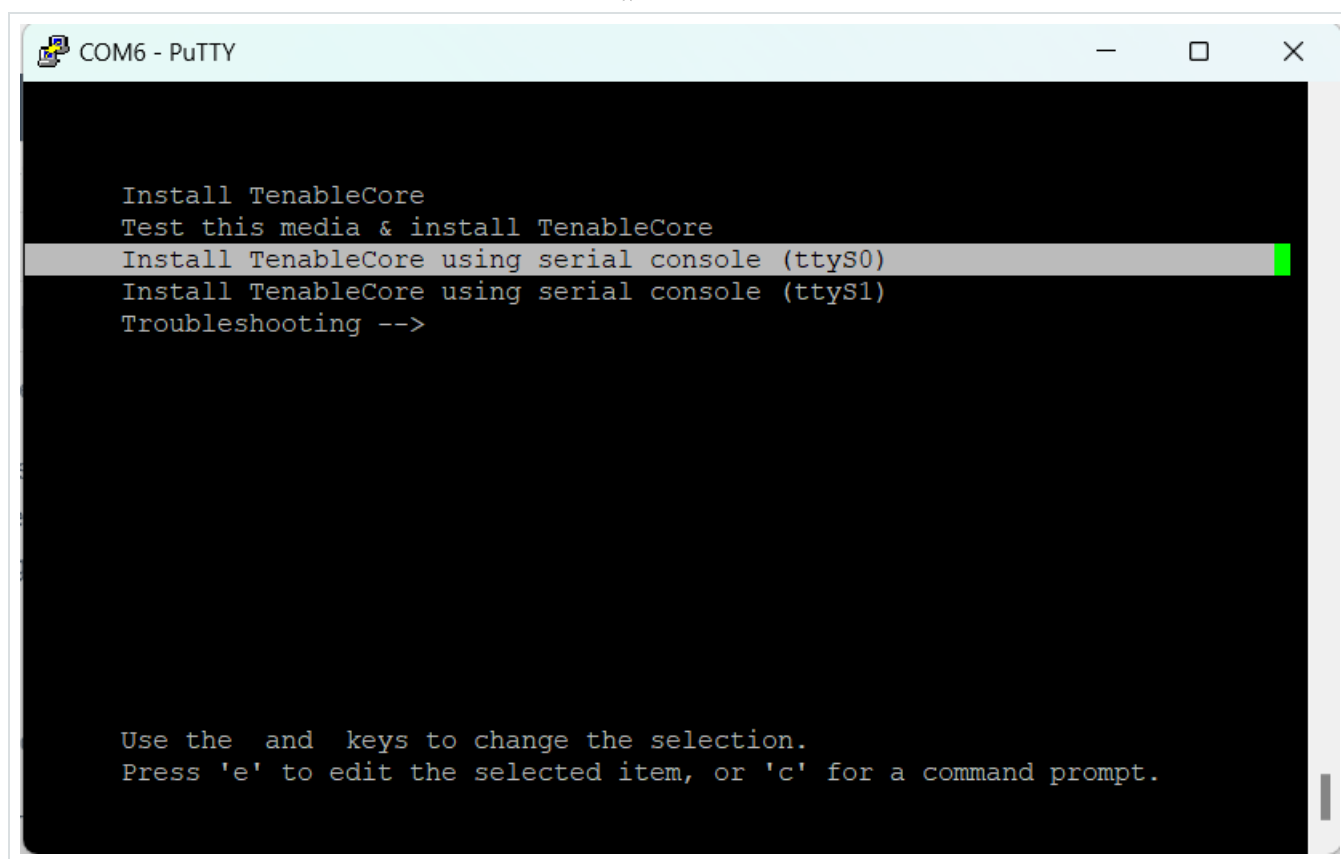


5. Lorsque vous y êtes invité, appuyez sur pour accéder à la configuration.
6. Dans la configuration du système, utilisez les touches de direction pour accéder à la section Boot (Démarrage).



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).



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. Veuillez à préparer votre infrastructure réseau en conséquence. Pour plus d'informations, voir [Considérations sur le réseau](#).

Gestion et requête active

Connectez l'interface réseau sélectionnée à une interface de commutateur réseau configurée pour autoriser la connectivité de gestion à l'ICP si nécessaire.

Veillez à configurer une adresse IP et d'autres paramètres de connectivité sur l'interface d'appliance OT Security sélectionnée via Tenable Core.



Si vous souhaitez séparer les rôles de gestion et de requête active, assurez-vous que chaque interface sélectionnée est connectée à son interface de commutateur dédiée. Attribuez des adresses IP à chacune et configurez les interfaces de commutateur selon les besoins pour autoriser l'accessibilité du réseau pour les deux fonctionnalités.

Pour plus d'informations, voir [Séparation des rôles de gestion et de requête active \(port fractionné\)](#).

Surveillance du réseau

Connectez une ou plusieurs des interfaces d'appliance sélectionnées pour la surveillance passive du réseau à une interface de destination de mise en miroir des ports (SPAN/RSPAN) configurée sur un commutateur réseau. Vous devez configurer la mise en miroir des ports pour permettre une visibilité adéquate des protocoles et des communications du réseau OT.

Remarque : vous pouvez utiliser des capteurs OT ou la configuration d'analyseur de ports encapsulé à distance (ERSPAN) pour capturer le trafic qui ne peut pas être directement surveillé par les interfaces de l'appliance.

Pour connecter l'appliance OT Security au réseau :

Sur une appliance matérielle :

Les appliances matérielles fournies par Tenable peuvent être livrées avec divers nombres et types (RJ45 ou SFP) d'interfaces réseau. Les interfaces par défaut sélectionnées pour chaque rôle sont pré-installées sur OT Security. Vous pourrez modifier cette configuration ultérieurement, si nécessaire.

Sur le matériel non fourni par Tenable, vous devez sélectionner des interfaces pour chaque rôle avant de lancer manuellement le processus d'installation d'OT Security. Veillez à utiliser correctement les interfaces disponibles pour chaque rôle.

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. Vous pouvez ajouter des adaptateurs/interfaces réseau supplémentaires pendant le déploiement ou à un stade ultérieur.

Si vous avez déployé une appliance virtuelle personnalisée à l'aide du fichier .iso ou .zip (Hyper-V), configurez le nombre requis d'interfaces réseau.

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 l'interface utilisateur Tenable Core

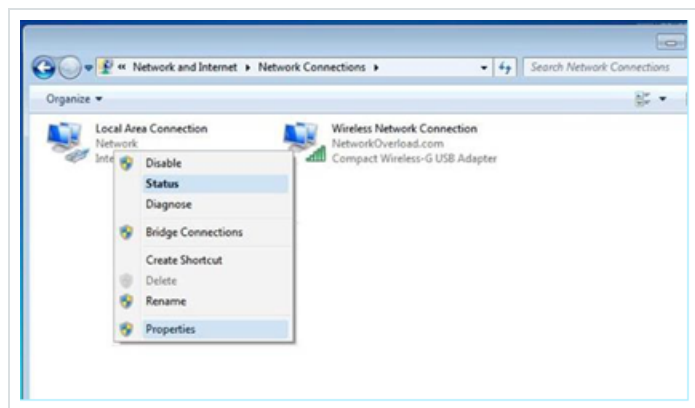
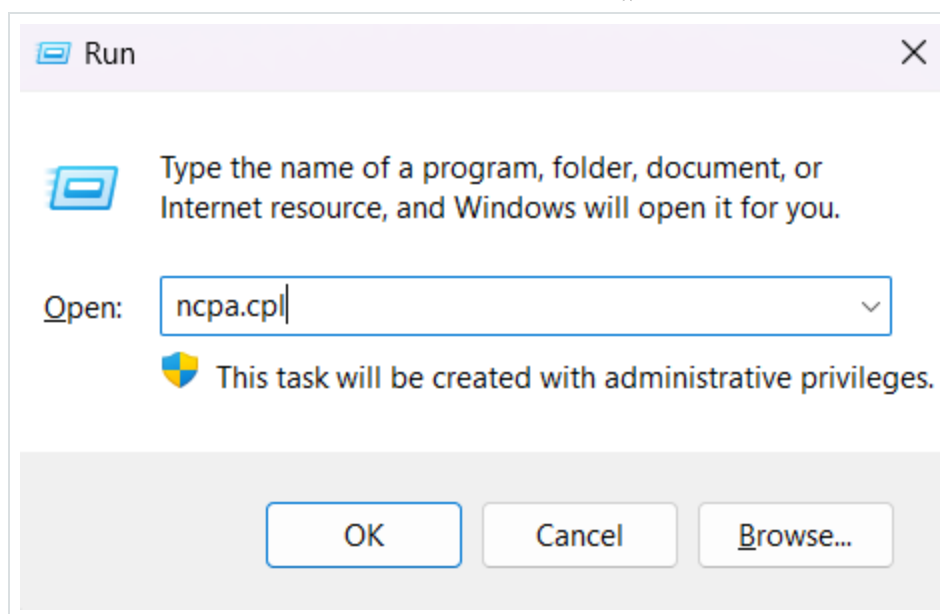
Pour terminer la configuration initiale via l'interface utilisateur Tenable Core (disponible sur <https://<mgmt-IP>:8000>), vous avez besoin d'une connexion réseau fonctionnelle à l'appliance.

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 :

- Port système 1 – Interface de gestion par défaut, pré-configurée avec l'adresse IP 192.168.1.5/24
- Port 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.

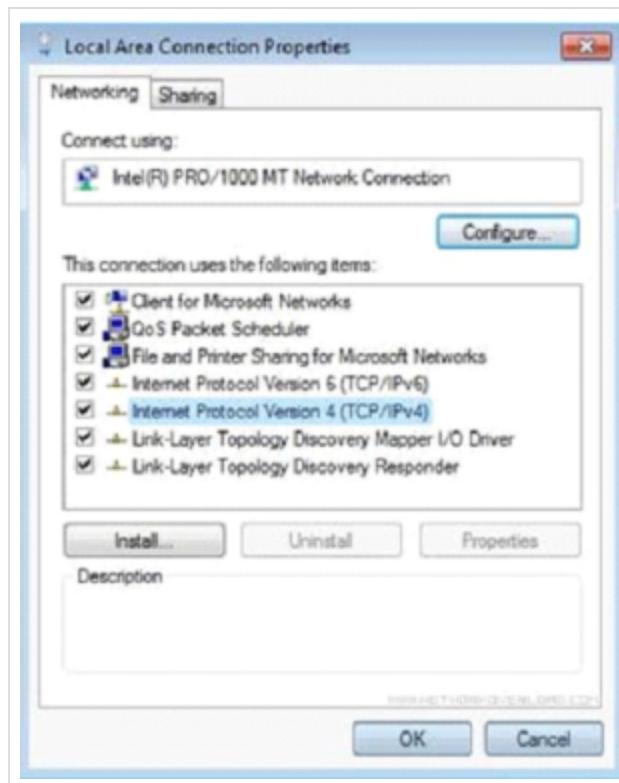
Pour vous connecter à Tenable Core directement via votre PC ou votre ordinateur portable :

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.cp1` pour ouvrir Connexions réseau.



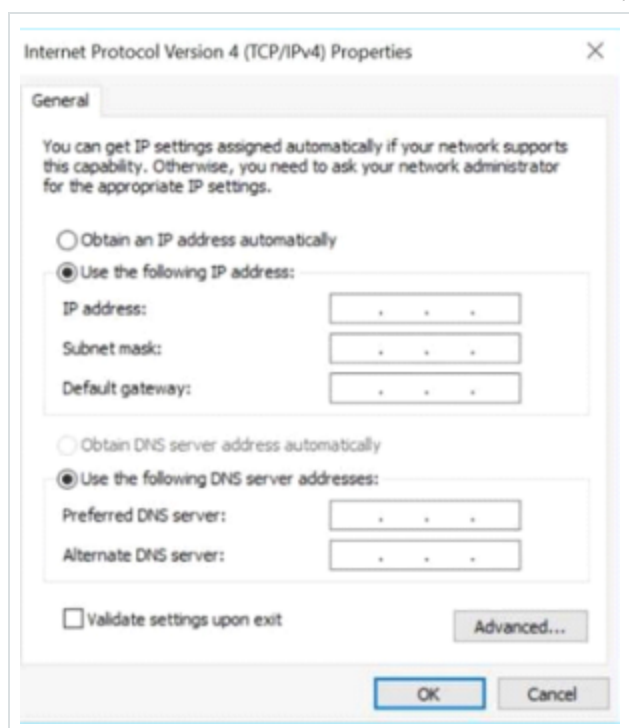
3. Effectuez un clic droit sur votre connexion réseau (appelée Connexion au réseau local) et sélectionnez Propriétés.

La fenêtre Propriétés de la connexion au réseau local apparaît.

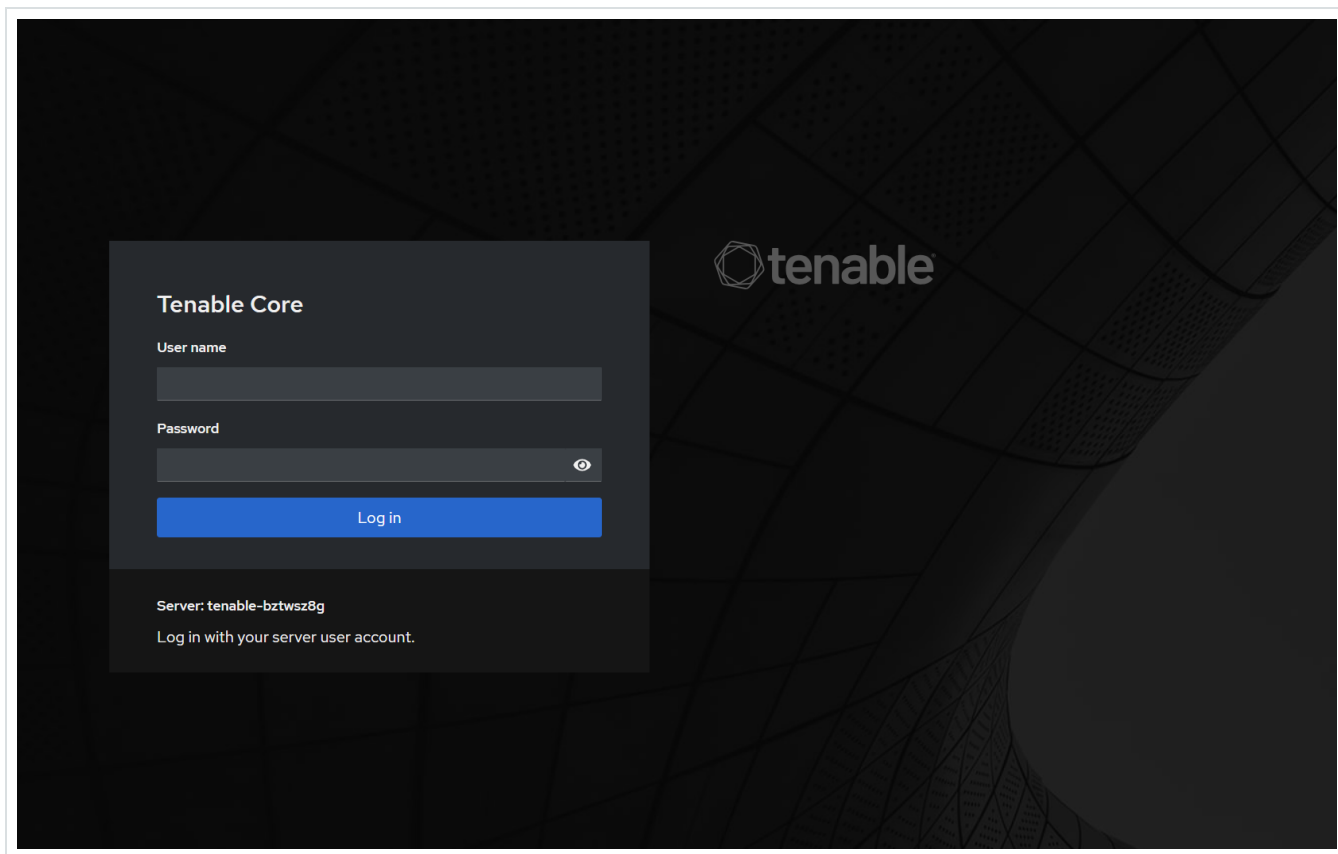


4. Sélectionnez Protocole Internet version 4 (TCP/IPv4) et cliquez sur Propriétés.

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 système 1 ou 192.168.3.10 pour l'adresse par défaut du Port système 4.
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, [connectez-vous à Tenable Core](#), activez l'accès administratif et [modifiez la configuration réseau](#) (documentation en anglais).

Configuration initiale via la CLI (facultatif)



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

1. Connectez-vous à l'apppliance 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.

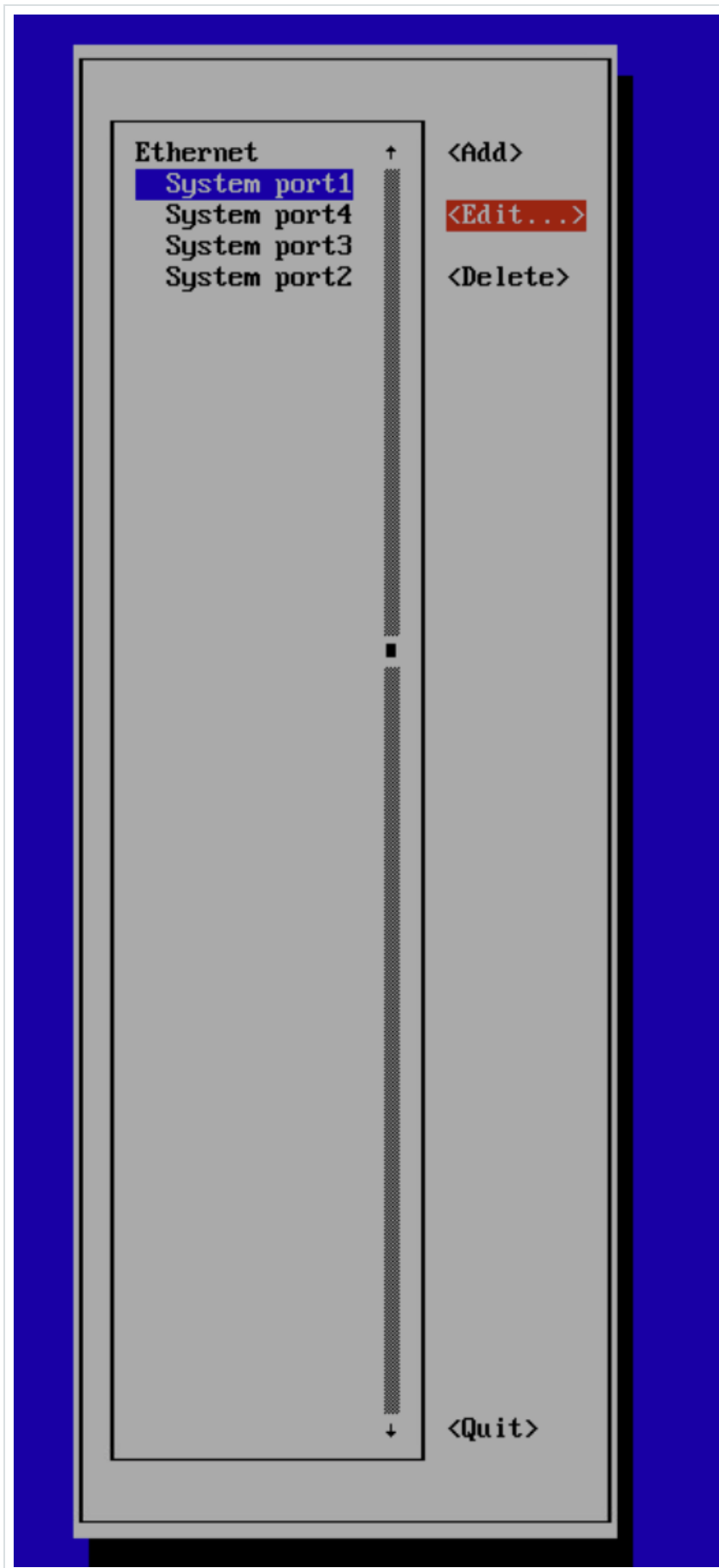
```
#####  
This system is restricted to authorized users only. Individuals attempting  
unauthorized access will be prosecuted. Continued access indicates  
your acceptance of this notice.  
#####  
Web console: https://tenable-...:8000/  
tenable-... : login: wizard  
Password:  
#####  
This system is restricted to authorized users only. Individuals attempting  
unauthorized access will be prosecuted. Continued access indicates  
your acceptance of this notice.  
#####  
Would you like to configure a static address? (y/n) █
```

3. (Facultatif) Pour configurer l'adresse IP de gestion, saisissez y (oui).

Remarque : si vous choisissez d'ignorer cette étape, vous pouvez toujours accéder à cette option à l'aide de la commande `sudo nmtui`.



- a. Sélectionnez Port système 1 (ou Port système 3 si vous utilisez la configuration en port fractionné).





b. Appuyez sur Entrée.flèche du

La fenêtre Edit Connection (Modifier la connexion) apparaît.



Edit Connection

Profile nameSystem port1

Deviceens192 (00:50:56:A7:29:9E)

= ETHERNET

Show

IPv4 CONFIGURATIONManual

Hide

Addresses10.1.2.5/24RemoveAdd...

Gateway10.1.2.254

DNS servers1.1.1.1RemoveAdd...

Search domainsAdd...

Routing (No custom routes) Edit...

Never use this network for default route

Ignore automatically obtained routes

Ignore automatically obtained DNS parameters

Require IPv4 addressing for this connection

= IPv6 CONFIGURATIONIgnore

Show

Automatically connect

Available to all users

CancelOK



- c. Dans la zone IPV4 Configuration (Configuration IPV4), remplacez l'option <Automatic> (Automatique) par <Manual> (Manuel).

Remarque :

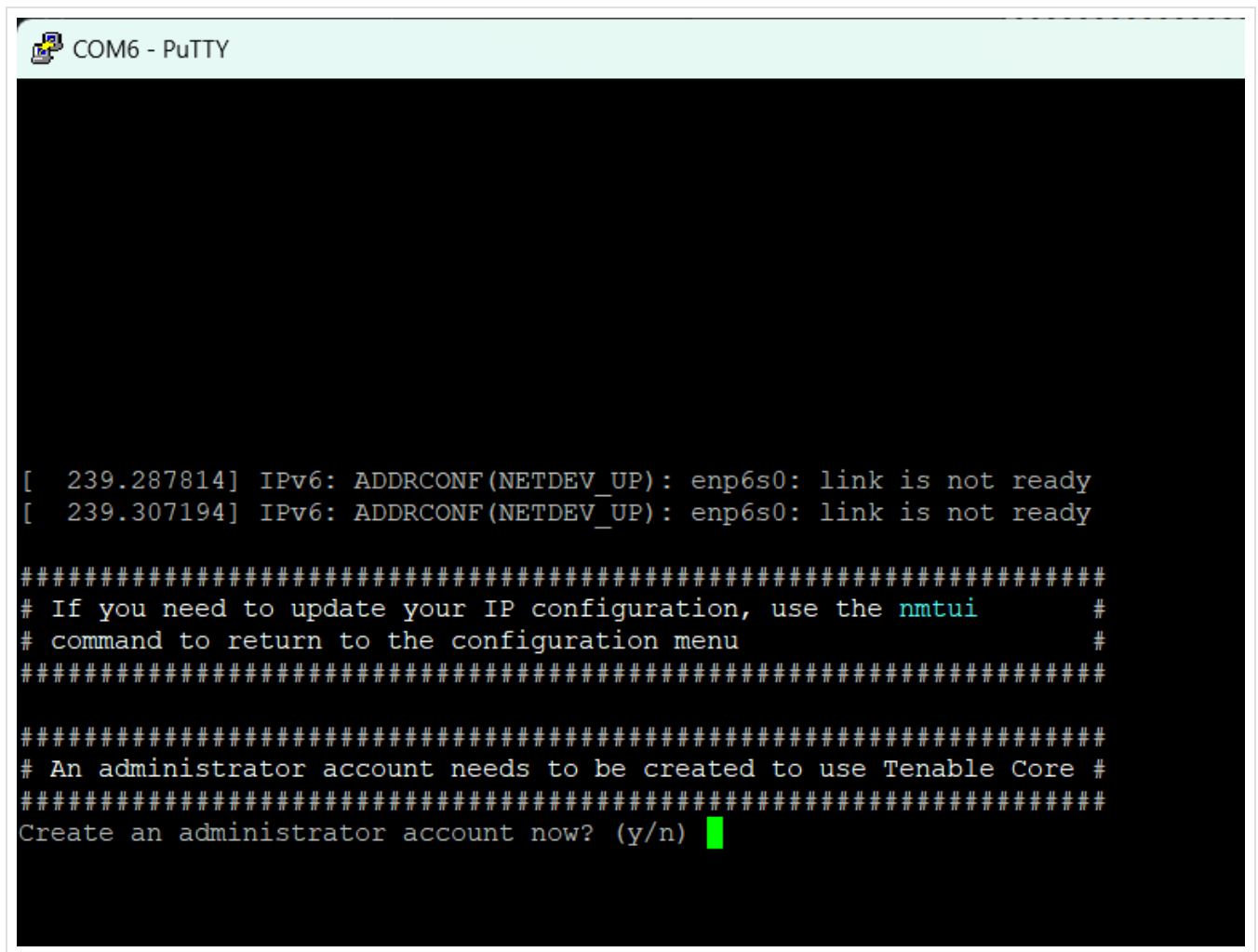
- Sur les machines virtuelles et le matériel non fourni par Tenable, le port 1 est défini par défaut sur Automatic IPv4 configuration (Configuration IPv4 automatique) (DHCP).
- Sur les appliances fournies par Tenable, le port 1 est défini par défaut sur la valeur 192.168.1.5/24. Vous pouvez utiliser ce port pour configurer et connecter directement l'appliance pour la configuration initiale, puis le modifier plus tard via l'onglet Networking (Mise en réseau) de l'interface utilisateur Tenable Core ou la commande `sudo nmtui` de la CLI.

- d. Naviguez à l'aide des touches de direction et configurez votre adresse IP, votre passerelle par défaut et vos serveurs DNS. Vous pourrez modifier cette configuration ultérieurement.
- e. 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.

4. Sélectionnez <Quit> (Quitter).

La fenêtre du terminal Network Manager (Gestionnaire réseau) apparaît et invite à créer un compte administrateur.



```
COM6 - PuTTY

[ 239.287814] IPv6: ADDRCONF(NETDEV_UP): enp6s0: link is not ready
[ 239.307194] IPv6: ADDRCONF(NETDEV_UP): enp6s0: link is not ready

#####
# If you need to update your IP configuration, use the nmtui      #
# command to return to the configuration menu                    #
#####

#####
# An administrator account needs to be created to use Tenable Core #
#####
Create an administrator account now? (y/n) █
```

5. 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.



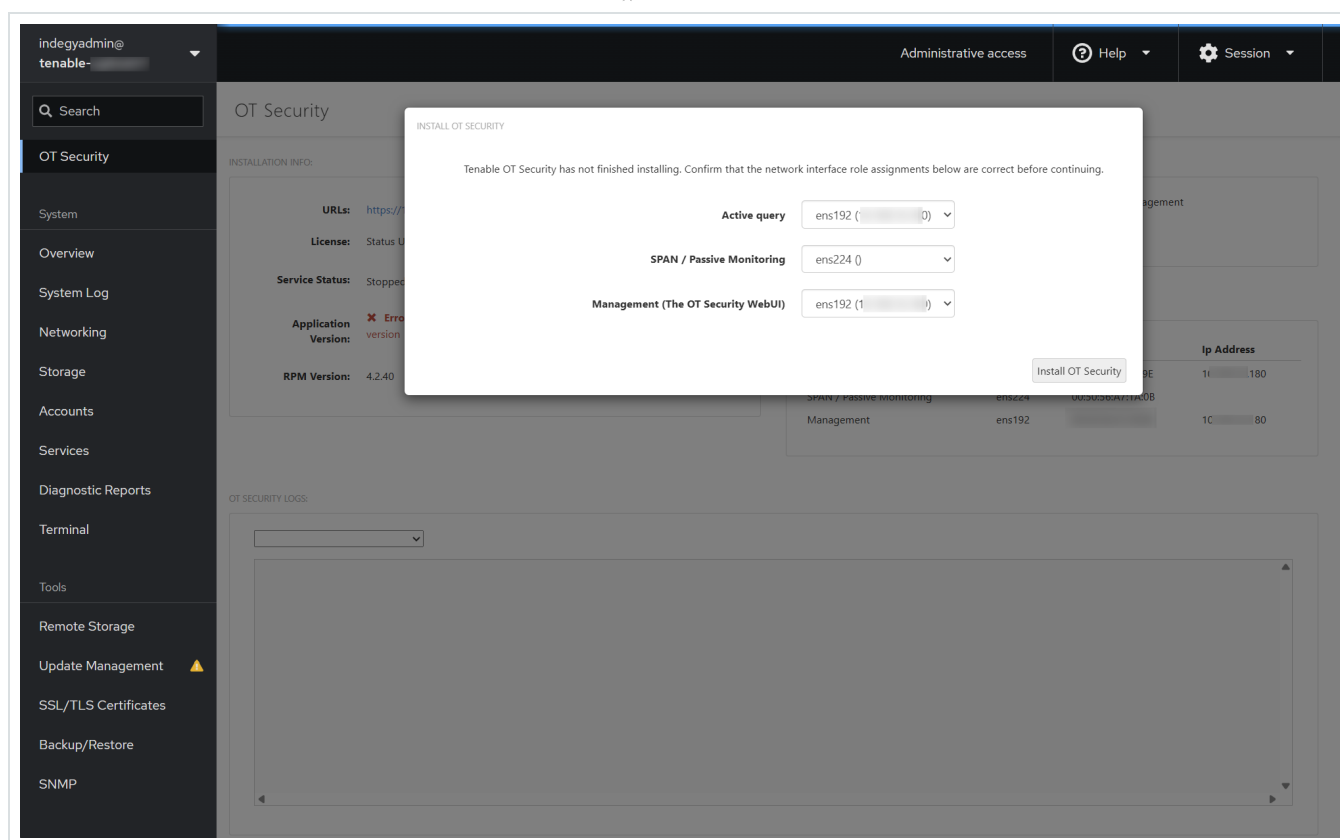
```
COM6 - PuTTY

[ 239.287814] IPv6: ADDRCONF(NETDEV_UP): enp6s0: link is not ready
[ 239.307194] IPv6: ADDRCONF(NETDEV_UP): enp6s0: link is not ready

#####
# If you need to update your IP configuration, use the nmtui      #
# command to return to the configuration menu                    #
#####

#####
# An administrator account needs to be created to use Tenable Core #
#####
Create an administrator account now? (y/n)
Creating a new administrator account
Username:tenableot
Password for tenableot:
Confirm password:
Account created for tenableot. Log in as tenableot to continue configuration
█
```

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



Sur les machines virtuelles et le matériel non fourni par Tenable, une invite apparaît sur la page Tenable Core > **OT Security** pour installer OT Security.

Que faire ensuite

Installer OT Security sur Tenable Core

Installer OT Security sur Tenable Core

Les appliances matérielles fournies par Tenable sont livrées avec l'application OT Security pré-installée. Lors du déploiement de OT Security sur du matériel personnalisé ou sur une machine virtuelle, il est nécessaire de lancer le processus d'installation manuellement.

Remarque : avant de lancer l'installation de l'application OT Security, attribuez des rôles pour chaque interface. Veillez à configurer les interfaces dans Tenable Core et à préparer l'infrastructure réseau pour permettre une connectivité appropriée. Pour plus d'informations, voir Considérations sur le réseau et Connecter OT Security au réseau.



Avant de commencer

- Assurez-vous de disposer d'un accès administrateur.
- Assurez-vous de disposer d'un accès SSH ou Cockpit sur les appliances virtuelles et physiques Tenable Core.

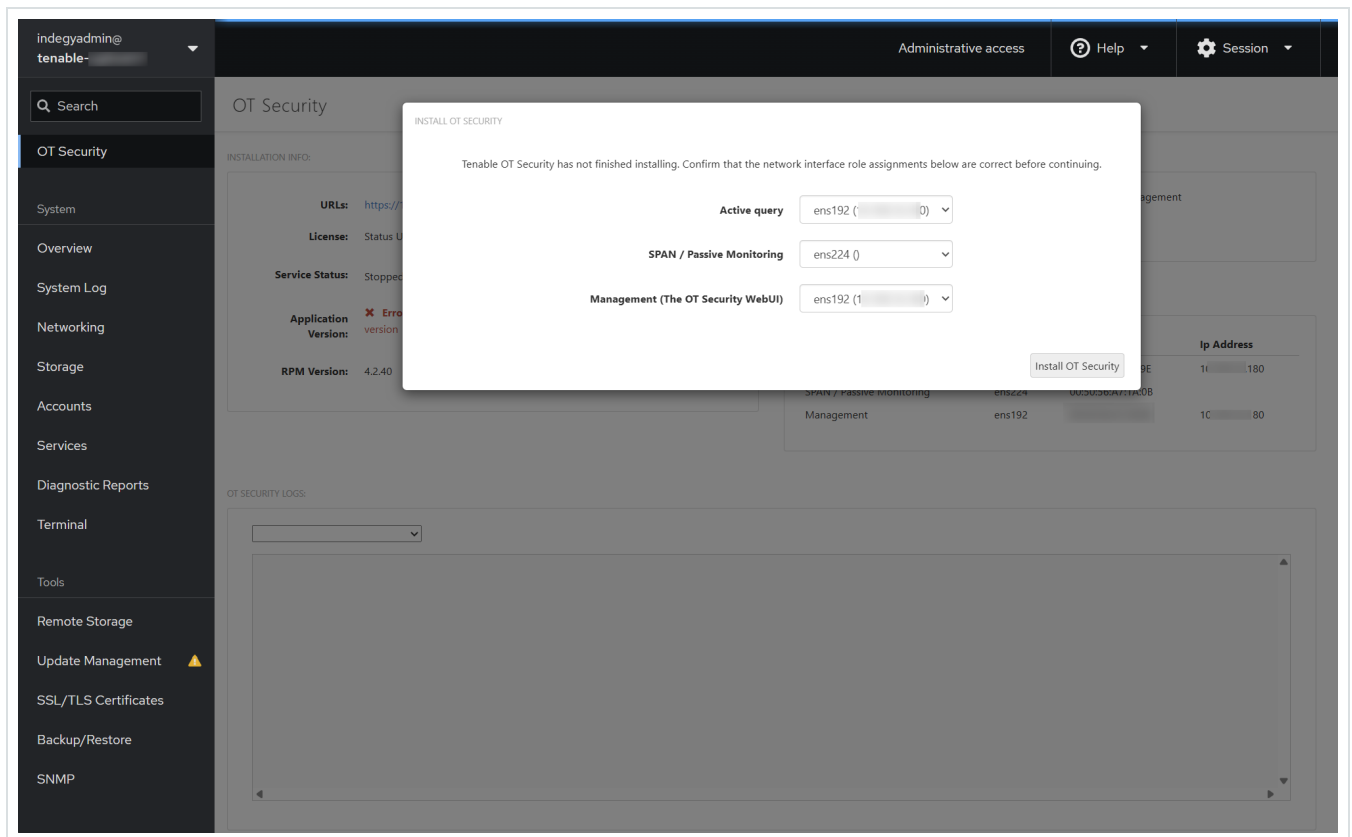
Remarque : les comptes administrateurs peuvent devenir inaccessibles si vous ne vous connectez pas et ne mettez pas régulièrement à jour votre mot de passe. Si un compte administrateur est verrouillé en raison de l'expiration du mot de passe, vous pouvez le déverrouiller à l'aide de l'utilitaire de déverrouillage à distance. Cet utilitaire permet à une ICP de déverrouiller ses capteurs connectés à distance et à un Enterprise Manager (EM) OT Security de faire de même avec ses ICP connectées, dans le cas où le compte est verrouillé. Pour plus d'informations sur l'utilitaire, voir l'article de la base de connaissances : [Leveraging the Remote Unlock Feature in Tenable Core](#) (Utilisation de la fonction de déverrouillage à distance dans Tenable Core).

Pour installer OT Security sur Tenable Core :

1. Connectez-vous à Tenable Core depuis votre navigateur web Chrome : `https://<mgmt-ip>:8000`.
2. Accédez à **OT Security**.

La page OT Security apparaît.

Remarque : sur les machines virtuelles et le matériel non fourni par Tenable, vous êtes invité à installer OT Security.



3. Cliquez sur **Install Tenable OT Security** (Installer Tenable OT Security).

Tenable Core lance l'installation et affiche une bannière jaune contenant le message : OT Security is being installed or upgraded and will be available again when the operation completes (OT Security est en cours d'installation ou de mise à niveau et sera à nouveau disponible une fois l'opération terminée).

indegyadmin@tenable-yg6sek17

Search

OT Security

System

Overview

System Log

Networking

Storage

Accounts

Services

Dagnostic Reports

Terminal

Tools

Remote Storage

Update Management

SSL/TLS Certificates

Backup/Restore

SNMP

Administrative access

Help

Session

OT Security is being installed or upgraded and will be available again when the operation completes

OT Security

URLs:https://:443

License:Status Unavailable (not-found)

Service Status:Stopped

StartRestart

Application Version:

✖ Error: OT Security install is not complete enough to determine application version

RPM Version:4.2.40

OT Security is configured to use ens192 for both active queries and management

Change split-port settings

ASSIGNED NETWORK INTERFACE ROLES:

Role	Interface	Mac Address	Ip Address
Active query	ens192		
SPAN / Passive Monitoring	ens224		
Management	ens192		1

OT SECURITY LOGS:

OT Security installation/upgrade

Last 24 hours

Priority

Only emergency

Identifiertenable.ot-install.sh

Filters

priority:7 identifier:tenable.ot-install.sh

Pause

July 23, 2025

1:14 PM DEBU[23/07/2025 06:14:14.830-04:00] Deploying File from /tmp/dataToDeploy515938476 to /etc/sysconfig/iptables

1:14 PM DEBU[23/07/2025 06:14:14.830-04:00] Executing template /opt/indegyl/manufacturing/templates/iptables.t

1:14 PM INFO[23/07/2025 06:14:14.830-04:00] [Deploy] Running SetIpTables

tenable.ot-install.sh

tenable.ot-install.sh

tenable.ot-install.sh

Une fois l'installation terminée, la bannière jaune disparaît et le statut de la licence passe de Unavailable (Indisponible) à Uninitialized (Non initialisée).

- 127 -

indegyadmin@tenable-

Administrative access

Help

Session

Q Search

OT Security

System

Overview

System Log

Networking

Storage

Accounts

Services

Diagnostic Reports

Terminal

Tools

Remote Storage

Update Management

SSL/TLS Certificates

Backup/Restore

SNMP

OT Security

INSTALLATION INFO:

URLs: https://10.443

License: Uninitialized

Service Status: Running Stop Restart

Application Version: 4.2.40
Installed: 7/23/2025, 1:14:48 PM

RPM Version: 4.2.40

SPLIT-PORT CONFIGURATION INFO:

OT Security is configured to use ens192 for both active queries and management

Change split-port settings

ASSIGNED NETWORK INTERFACE ROLES:

Role	Interface	Mac Address	Ip Address
Active query	ens192	00:00:00:00:00:00	10.44.3.1
SPAN / Passive Monitoring	ens224	00:00:00:00:00:00	
Management	ens192	00:00:00:00:00:00	10.44.3.1

OT SECURITY LOGS:

OT Security installation/upgrade

Last 24 hours

Priority Only emergency

Identifier tenable.ot-install.sh

Filters priority:7 identifier:tenable.ot-install.sh

July 23, 2025

1:15 PM Starting OT Security

1:15 PM DEBU[23/07/2025 06:15:07.843-04:00] Starting service anthology.service

1:15 PM INFO[23/07/2025 06:15:07.827-04:00] [Finalize] Running StartService

4. (Facultatif) Sélectionnez les rôles d'interface.

Remarque : vous pouvez choisir de conserver la configuration par défaut. La configuration des interfaces par défaut inclut Port 1 : gestion + requête active et Port 2 : surveillance passive.

The screenshot displays the OT Security web interface. On the left is a dark sidebar with a search bar and a menu containing: OT Security, System, Overview, System Log, Networking, Storage, Accounts, Services, Diagnostic Reports, Terminal, Tools, Remote Storage, and Update Management. The main content area is titled 'OT Security' and includes a top navigation bar with 'Administrative access', 'Help', and 'Session'.

The main content is divided into three sections:

- INSTALLATION INFO:** Displays 'URLs: https://[redacted]:443', 'License: Active, will expire in 353750 days', 'Service Status: Running' with 'Stop' and 'Restart' buttons, 'Application Version: 4.3.24', and 'RPM Version: 4.3.24'.
- SPLIT-PORT CONFIGURATION INFO:** States 'OT Security is configured to use nic0 for both active queries and management' and includes a 'Change split-port settings' button.
- ASSIGNED NETWORK INTERFACE ROLES:** A table with columns 'Role', 'Interface', 'Mac Address', and 'Ip Address'.

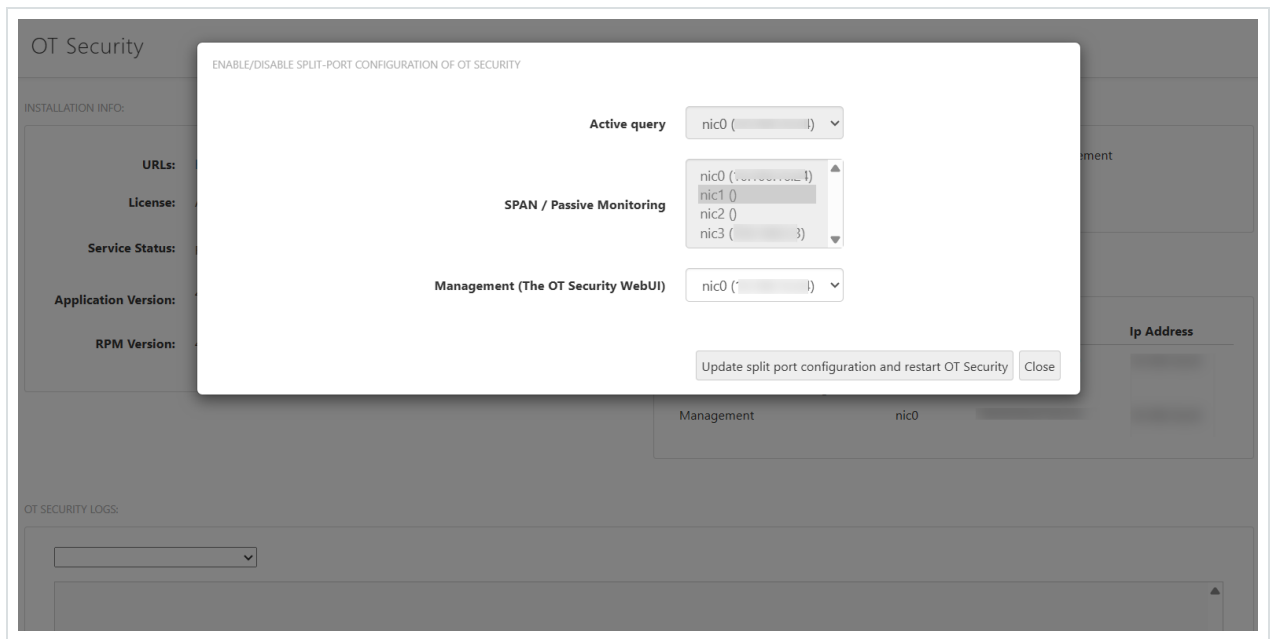
The table data is as follows:

Role	Interface	Mac Address	Ip Address
Active query	nic0	[redacted]	[redacted]
SPAN / Passive Monitoring	nic1	[redacted]	[redacted]
Management	nic0	[redacted]	[redacted]

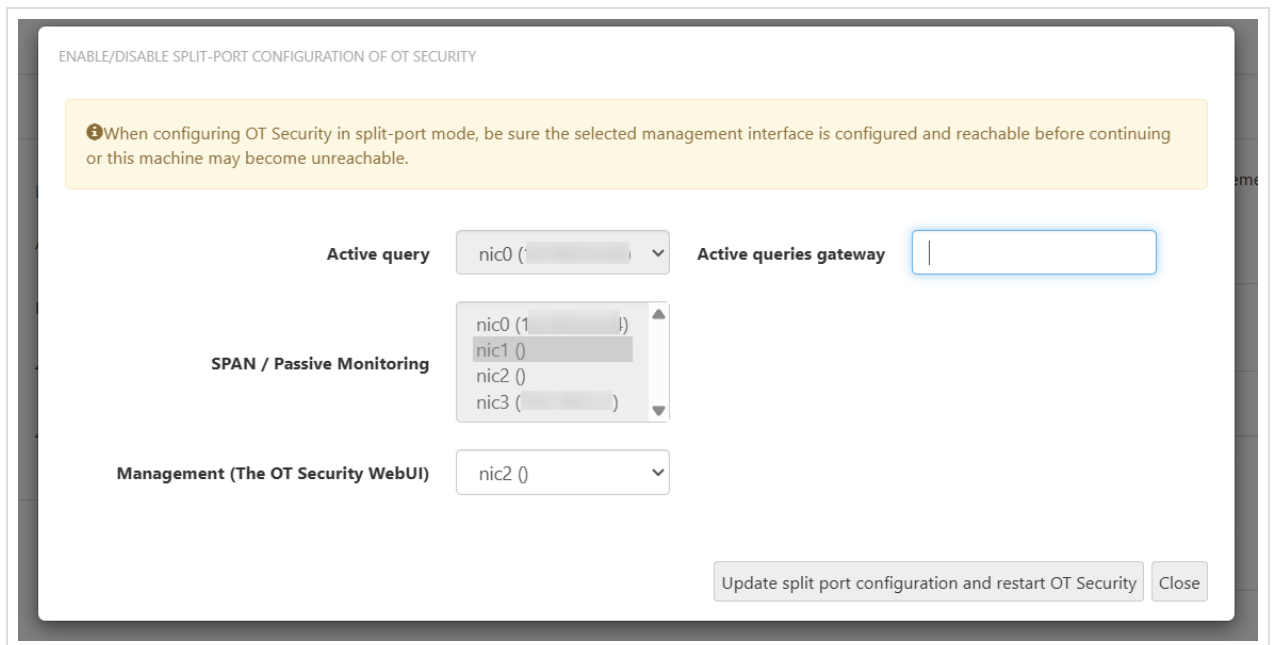
At the bottom, there is an 'OT SECURITY LOGS' section with a dropdown menu and a large empty log area.

- a. Dans la section Split Port Configuration Info (Informations de configuration des ports fractionnés), cliquez sur Change split-port settings (Modifier les paramètres des ports fractionnés).

La fenêtre Enable/Disable Split Configuration of **OT Security** (Activer/Désactiver la configuration fractionnée d'OT Security) apparaît.



- b. Dans la zone Management (The OT Security Web UI) (Gestion [interface utilisateur web OT Security]), déplacez le port de gestion vers une autre interface, par exemple le port 3.



- c. (Facultatif) Dans la zone Active queries gateway (Passerelle des requêtes actives), fournissez l'adresse IP de la passerelle.

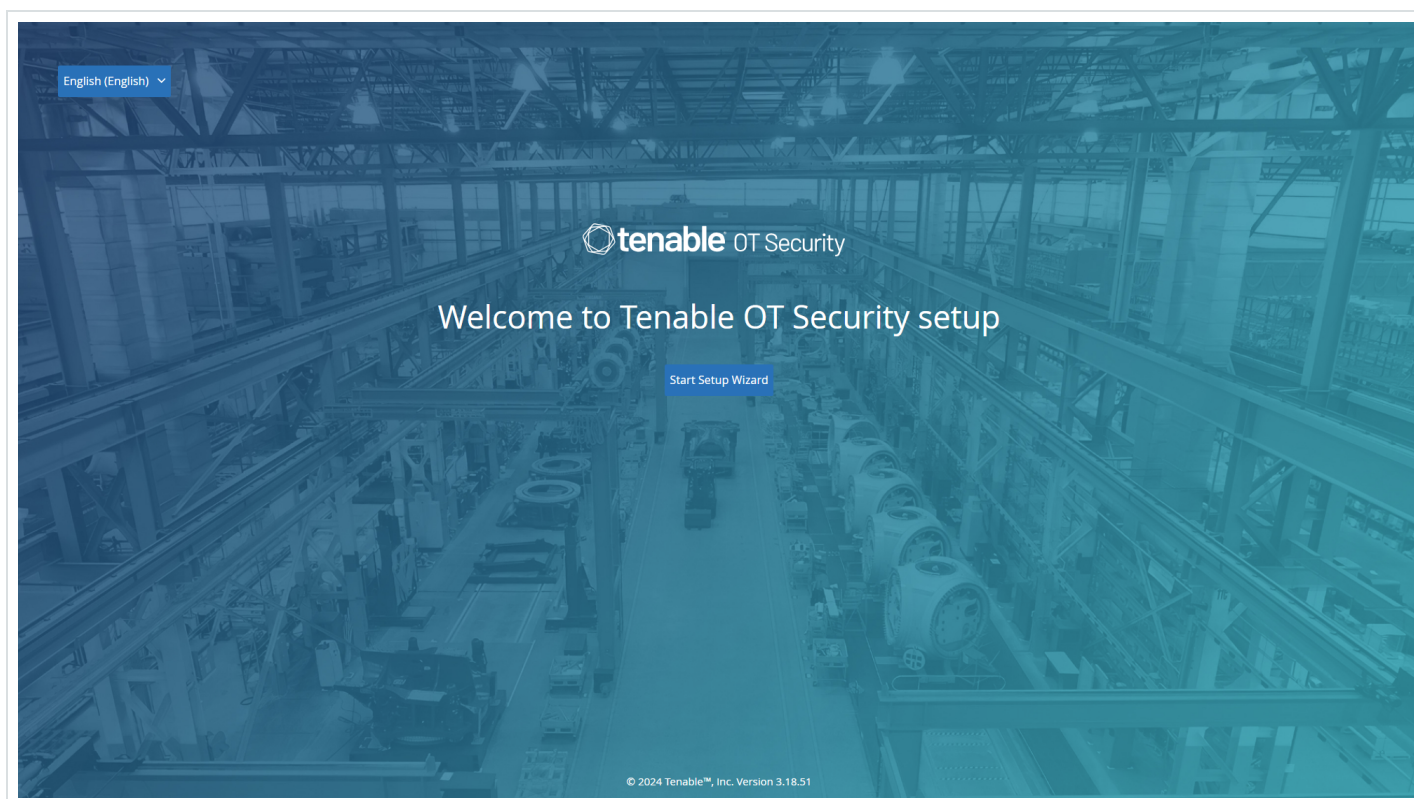


- d. Cliquez sur Update split-port configuration and restart OT Security (Mettre à jour la configuration des ports fractionnés et redémarrer OT Security).

Tenable Core procède à un redémarrage ou à une installation selon les besoins.

Attention : n'installez pas d'autres mises à jour et ne redémarrez pas à ce stade. Le processus d'installation peut prendre un certain temps. N'interrompez pas le processus d'installation.

Une fois l'installation terminée, vous pouvez cliquer sur le lien dans la zone URLs (URL) pour vous connecter à l'interface utilisateur OT Security.



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. [Connecter et configurer la séparation des ports de gestion et de requête active](#)

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 ou ordinateur portable) directement au port 1 de l'appliance OT Security à l'aide du câble Ethernet.
 - Connectez le poste de travail de la console de gestion au commutateur réseau.

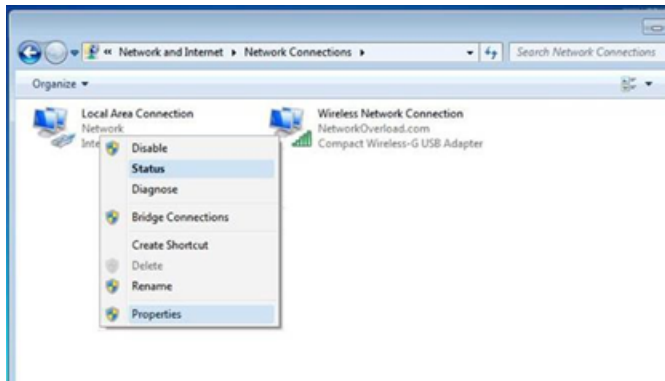
Remarque : vérifiez que le poste de travail de la console de gestion fait partie du même sous-réseau que l'appliance OT Security (192.168. 1.0/24) ou qu'elle est routable vers l'unité.

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.

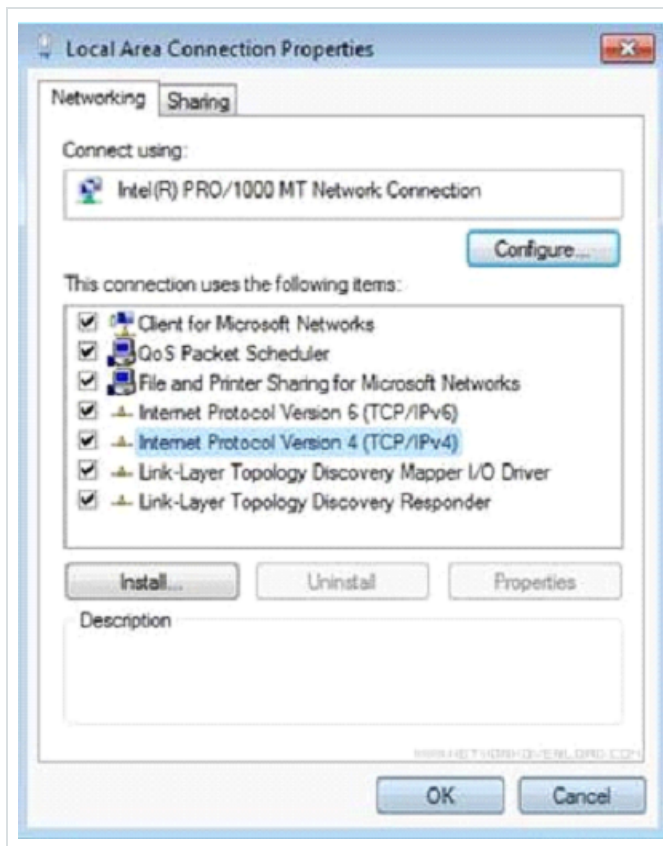
L'écran Connexions réseau apparaît.



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

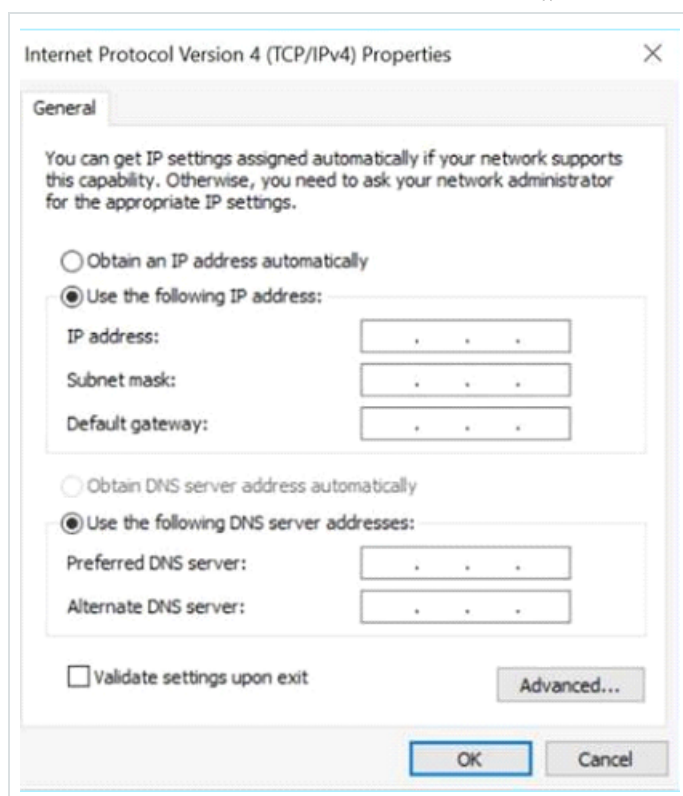
- b. Effectuez un clic droit sur Connexions au réseau local et sélectionnez Propriétés.

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, saisissez à nouveau le 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).



English (English) ▼

tenable OT Security

© 2025 Tenable™, Inc. Version 4.2.40 (Dev)

Set-up Wizard

User Info — Device

SITE NAME *
The name of the site where the Tenable OT Security ICP device is installed

Site

☒ Enable Usage Statistics

Enable this option to turn on telemetry and to access the OT Security Resource Center. After enabling or disabling, refresh your browser for the change to take effect. Note: When enabled, Tenable collects anonymous telemetry data from your account. This information cannot be attributed to a specific individual; it does not include Personal Data. We analyze this data in-house and also send it to third-party partners for analytics and optimization. We use this data to identify ways of improving the user experience in future Tenable OT Security releases. We may also use the data for other reasonable business purposes in accordance with the Tenable Master Agreement. You can disable this option at any time, in order to stop sharing usage statistics with Tenable.

< Back Complete and Restart

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

1. Dans la zone Nom du site, indiquez le nom du site où vous avez installé OT Security.
2. (Facultatif) Cliquez sur le curseur Activer les statistiques d'utilisation pour autoriser OT Security à collecter des données de télémétrie et à accéder au Centre de ressources.
3. Cliquez sur Terminer et redémarrer.

OT Security redémarre.

Que faire ensuite

- Connecter et configurer la séparation des ports de gestion et de requête active
- Activation de licence OT Security

Connecter et configurer la séparation des ports de gestion et de requête active

Cette étape est facultative. Si vous avez sélectionné l'option Port fractionné (pour séparer le rôle d'interface de requêtes actives du rôle de gestion), vous pouvez désormais connecter l'interface



secondaire de l'apppliance OT Security à son interface de commutateur réseau appropriée, à condition que vous ne l'ayez pas fait dans Tenable Core.

Pour plus d'informations, voir [Séparation des rôles de gestion et de requête active \(port fractionné\)](#).

Pour connecter le port de gestion :

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

Activation de licence OT Security

Rôle utilisateur OT Security requis : Administrateur

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. 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.

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

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.

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.

5. 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.

La page du portail Account Management (Gestion des comptes) apparaît.

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

6. Dans le volet de navigation de gauche, cliquez sur Products (Produits).

La page My Products (Mes produits) apparaît.

7. Recherchez votre produit à l'aide du code de licence à 20 chiffres de OT Security.

Le produit OT Security apparaît avec le code de licence spécifique.

8. Cliquez sur l'onglet Sites.



L'onglet Sites apparaît.

9. 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.

Conseil : utilisez le champ Label (Étiquette) pour indiquer le nom de l'appareil ou de l'ICP et différencier plus facilement les différents sites.

- 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 f.
- 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).

10. Revenez à l'instance OT Security.

11. À l'étape 3 Saisir le code d'activation, cliquez sur Saisir le code d'activation.

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

12. 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.



13. Cliquez sur Activer.

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

14. Cliquez sur Activer.

OT Security est maintenant activé et prêt à être utilisé.

15. 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).

16. 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. Lorsque vous mettez à jour votre licence, vous utilisez votre code de licence existant à 20 chiffres.

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 **locaux > Configuration système > Licence**.

La fenêtre Licence apparaît.



License

Actions ▾

LICENSE TYPE	Subscription
SUBSCRIPTION EXPIRES	Sep 17, 2024
LICENSED ASSETS	43/100 (43%)
LICENSE CODE	
COMPUTER ID	

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

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

License

LICENSE TYPE	Perpetual
MAINTENANCE EXPIRES	Dec 29, 2993
LICENSED ASSETS	Unlimited
LICENSE CODE	
COMPUTER ID	

Follow these steps in order to update your license

✓

Certificate was generated successfully

Generate certificate

2

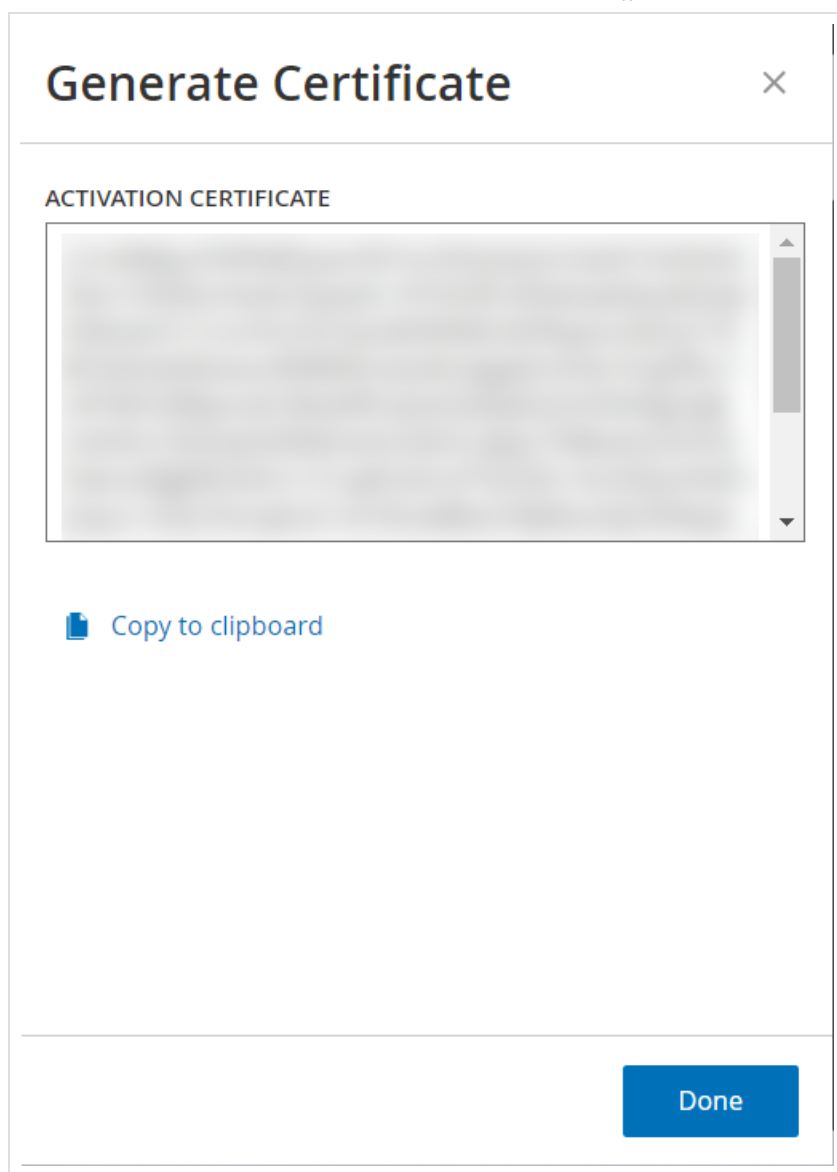
Enter activation code, obtain an activation code from Tenable [Self-service portal](#) or from your sales rep. [Click here](#) to activate your evaluation period

Enter Activation Code

Cancel

- 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. Dans la zone (2) Saisir le code d'activation, cliquez sur le lien vers le Portail libre-service.

OT Security vous redirige vers la page My Account (Mon compte) du portail [Tenable Account Management](#).



Remarque : si vous êtes en période d'évaluation, cliquez sur le [deuxième lien](#). Voir [Mettre à jour votre licence en mode hors ligne](#).

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

- a. Dans le volet de navigation de gauche, cliquez sur Products (Produits).

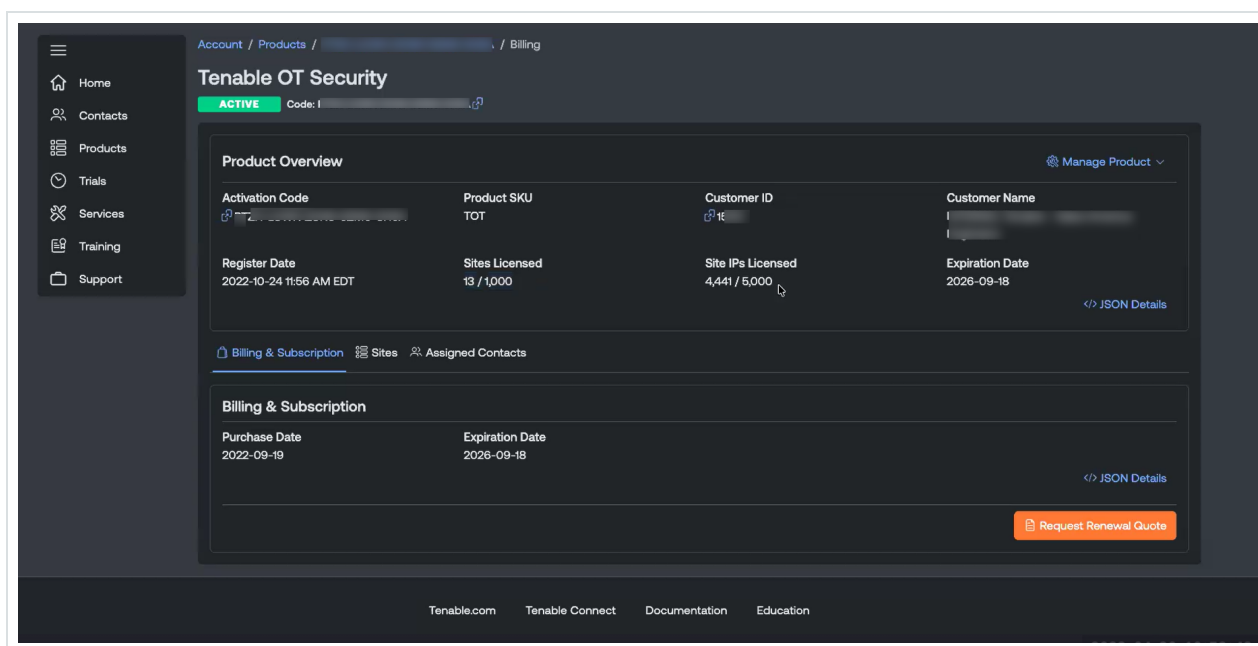
La page My Products (Mes produits) apparaît.

- b. Recherchez votre produit à l'aide du code de licence à 20 chiffres de OT Security.

Le produit OT Security apparaît avec le code de licence spécifique.

- c. Cliquez sur le code de licence pour afficher les détails du produit.

La page Tenable OT Security apparaît et présente des détails tels que Product Overview (Vue d'ensemble du produit), Billing & Subscription (Facturation et abonnement) et Sites.



- d. Cliquez sur l'onglet Sites.

La section Sites apparaît.

Account / Products / [redacted] / Sites

Tenable OT Security

ACTIVE Code: [redacted]

Product Overview

[Manage Product](#)

Activation Code [redacted]	Product SKU TOT	Customer ID [redacted]	Customer Name [redacted]
Register Date 2022-10-24 11:56 AM EDT	Sites Licensed 12 / 1,000	Site IPs Licensed 4,241 / 5,000	Expiration Date 2026-09-18 JSON Details

[Billing & Subscription](#) [Sites](#) [Assigned Contacts](#)

Sites (12)

[Manage Sites](#)

Start typing to search...

Columns 1 to 12 of 12 Page 1 of 1

Status	Label	Site ID	Size	Created Date	Expiration Date
Active	SE30 - HQ ICS .33	[redacted]	150	2024-10-10	58685-09-28
Active	HQ Lenovo SE30	[redacted]	165	2024-10-10	58685-09-28
Active	HQ ICS .57	[redacted]	150	2024-10-10	58685-09-28

e. Sur la ligne du site que vous souhaitez modifier, cliquez sur le bouton **...**.

Un menu apparaît.

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

La page Edit Site Details (Modifier les détails du site) apparaît.

Edit Site Details

1 Update Details

2 Review Seat

After modifying the site size, you will need to re-enter the new activation code into your Tenable OT Security instance. This will be a one-time generated code.

Label
Optional label for the site

Warehouse .30

Size
Number of IPs allocated to the site

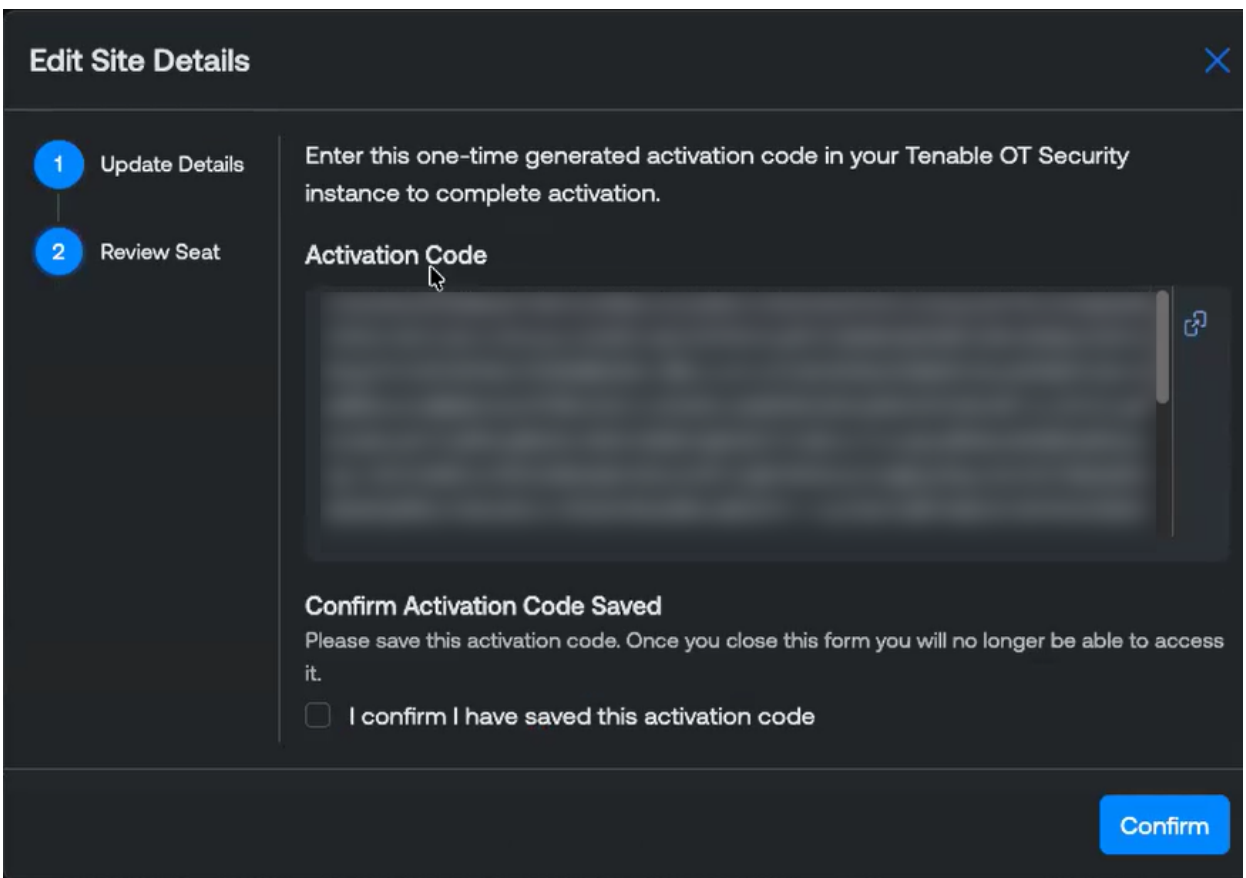
150

License Certificate
Enter your Tenable OT Security license certificate

Cancel Updating...

- g. Modifiez les détails selon les besoins.
- h. 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.
- i. 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.



Edit Site Details ✕

1 Update Details

2 Review Seat

Enter this one-time generated activation code in your Tenable OT Security instance to complete activation.

Activation Code

Confirm Activation Code Saved
Please save this activation code. Once you close this form you will no longer be able to access it.

☐ I confirm I have saved this activation code

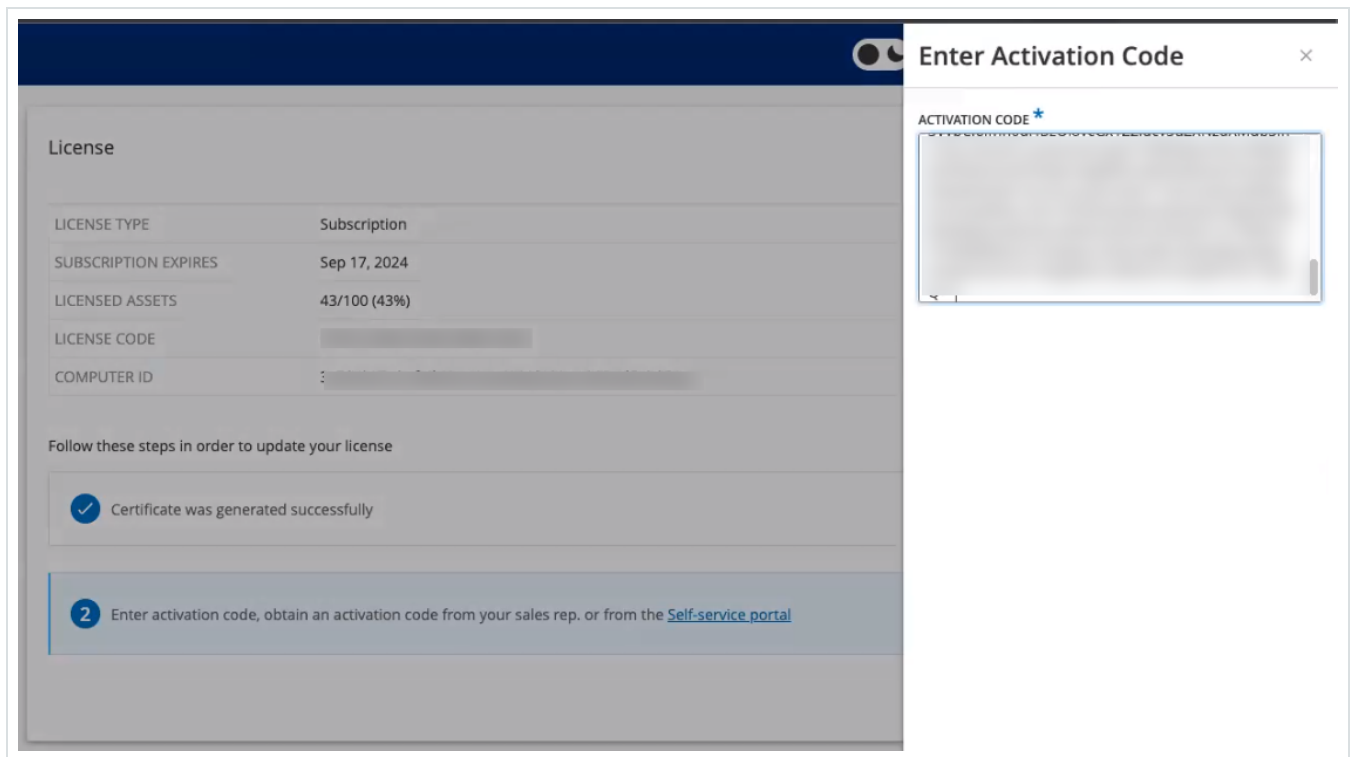
Confirm

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

7. Revenez à l'instance OT Security.

8. Dans la zone (2) Saisir le code d'activation, cliquez sur Saisir le code d'activation.

9. 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).



10. 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 1 à 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.



License

LICENSE TYPE	Perpetual
MAINTENANCE EXPIRES	Dec 29, 2993
LICENSED ASSETS	Unlimited
LICENSE CODE	
COMPUTER ID	

Follow these steps in order to update your license



Certificate was generated successfully

[Generate certificate](#)

2

Enter activation code, obtain an activation code from Tenable [Self-service portal](#) or from your sales rep. [Click here](#) to activate your evaluation period

[Enter Activation Code](#)

[Cancel](#)

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

documentation page.' There are two input fields: 'Activation Code' and 'Activation Certificate', both with the placeholder text 'Enter your Tenable OT Security activation code.' Below these is the 'Accept License Agreement' section, which says 'Please review and accept the [Tenable Software License Agreement](#).' and has a checkbox labeled 'I have read and understand the Tenable Software License Agreement'. A blue 'Submit' button is at the bottom right." data-bbox="117 68 936 467"/>

Tenable | Account

Tenable OT Security Offline Activation

Activate your Tenable OT Security instance offline. For detailed instructions on offline activation, visit the [documentation](#) page.

Activation Code
Enter your Tenable OT Security activation code.

Activation Certificate
Enter your Tenable OT Security activation code.

Accept License Agreement
Please review and accept the [Tenable Software License Agreement](#).

☐ I have read and understand the Tenable Software License Agreement

Submit

Remarque : vous pouvez accéder à l'écran Activer 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).

Tenable OT Security Offline Activation

Activate your Tenable OT Security instance offline. For detailed instructions on offline activation, visit the [documentation](#) page.

Activation Code
Enter your Tenable OT Security activation code.

Activation Certificate
Enter your Tenable OT Security activation code.

Accept License Agreement
Please review and accept the [Tenable Software License Agreement](#).

☒ I have read and understand the Tenable Software License Agreement

Submit

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

6. Cliquez sur Envoyer.

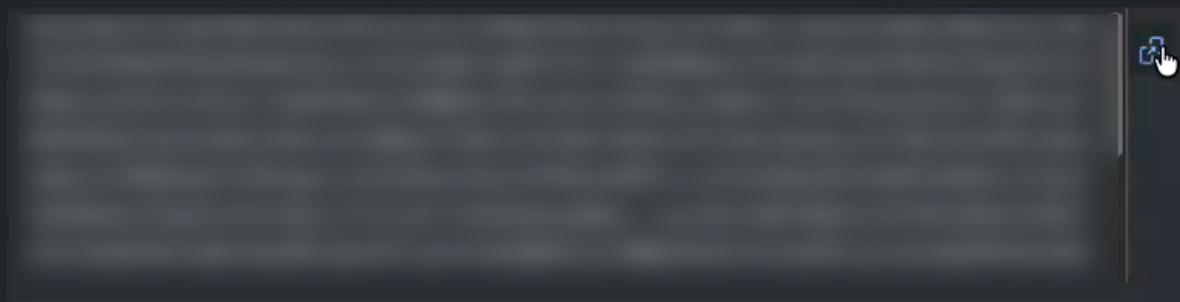
OT Security génère le code d'activation.



Tenable OT Security Offline Activation

Enter this one-time generated activation code in your Tenable OT Security instance to complete activation. For detailed instructions on offline activation, visit the [documentation](#) page.

Activation Code



Please save this activation code. Once you exit this page you will no longer be able to access it.

[View My Account](#)

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.



License

LICENSE TYPE	Perpetual
MAINTENANCE EXPIRES	Dec 29, 2993
LICENSED ASSETS	Unlimited
LICENSE CODE	
COMPUTER ID	

Follow these steps in order to update your license

Certificate was generated successfully

Generate certificate

2

Enter activation code, obtain an activation code from Tenable [Self-service portal](#) or from your sales rep. [Click here](#) to activate your evaluation period

Enter Activation Code

Cancel

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.

Remarque : une licence d'évaluation ou temporaire a toujours un code de licence unique.

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 locaux > Configuration système > Licence.

License

Actions ▾

LICENSE TYPE	Subscription
SUBSCRIPTION EXPIRES	Sep 17, 2024
LICENSED ASSETS	43/100 (43%)
LICENSE CODE	
COMPUTER ID	

2. Dans le menu Actions, sélectionnez Réinitialiser la licence.

Une fenêtre de confirmation apparaît.

3. Cliquez sur Réinitialiser.

i

Reinitialize License

×

Are you sure?

Once you complete the three-step process to reinitialize your license, the current license will be replaced by the new one. Until the process is completed, your current license will remain in effect.

Cancel

Reinitialize



La fenêtre Licence apparaît avec les trois étapes de réinitialisation.

License

LICENSE TYPE	Perpetual
MAINTENANCE EXPIRES	Dec 29, 2993
LICENSED ASSETS	Unlimited
LICENSE CODE	
COMPUTER ID	

Follow these steps in order to reinitialize your license

1

Enter license code

Enter license code

2

Generate activation certificate

Generate Certificate

3

Enter activation code, obtain an activation code from Tenable [Self-service portal](#) or from your sales rep. [Click here](#) to activate your evaluation period

Enter Activation Code

Cancel

4. Suivez les étapes de démarrage du système (Étape 1 à 17) pour activer votre licence dans la section 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 et les serveurs d'authentification pour commencer à utiliser OT Security.

Activer le système OT Security

Rôle utilisateur OT Security requis : Administrateur

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.

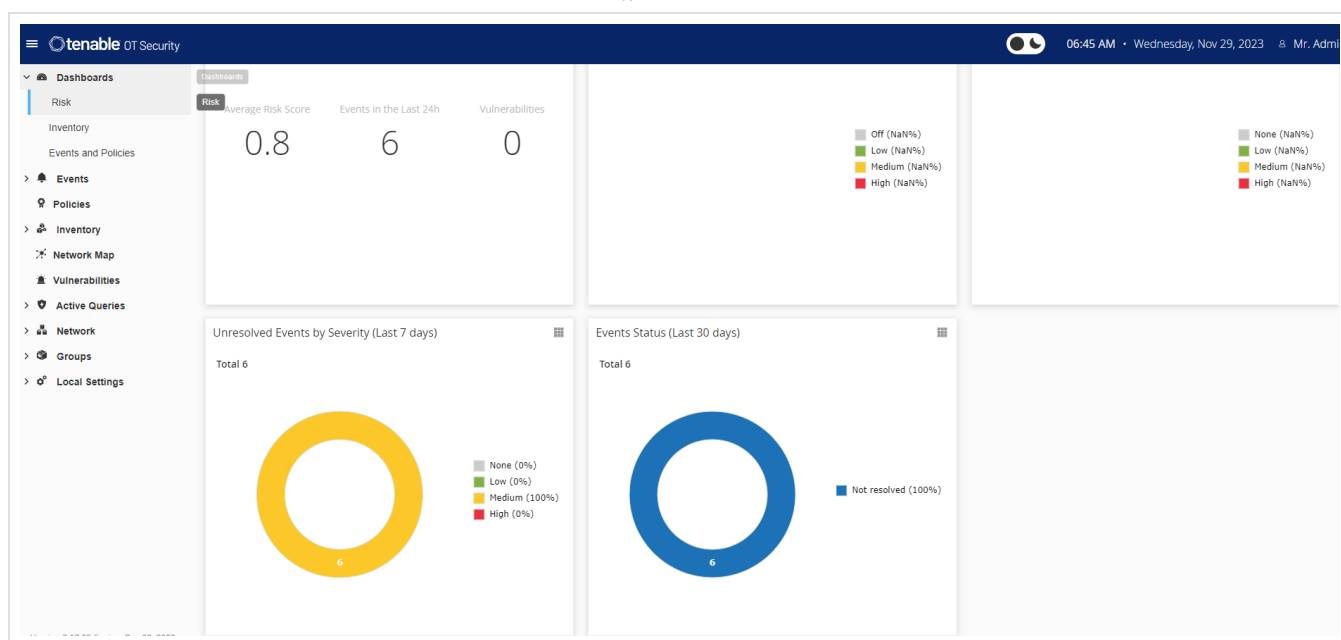
Vous pouvez configurer et activer des fonctions supplémentaires telles que Requêtes actives dans la fenêtre Paramètres de la console de gestion (interface utilisateur). Pour plus d'informations, voir [Requêtes actives](#).

Important : à partir de la version 4.4, la surveillance passive est désactivée par défaut lorsque vous activez OT Security pour réduire la surcharge liée aux alertes. Pour activer la surveillance passive, accédez à la page Paramètres > Définitions de réseau et cliquez pour activer le curseur Surveillance passive. L'icône de surveillance passive  dans l'en-tête indique si la surveillance passive est activée ou désactivée.

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 [Paramètres de l'environnement](#).

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](#)).

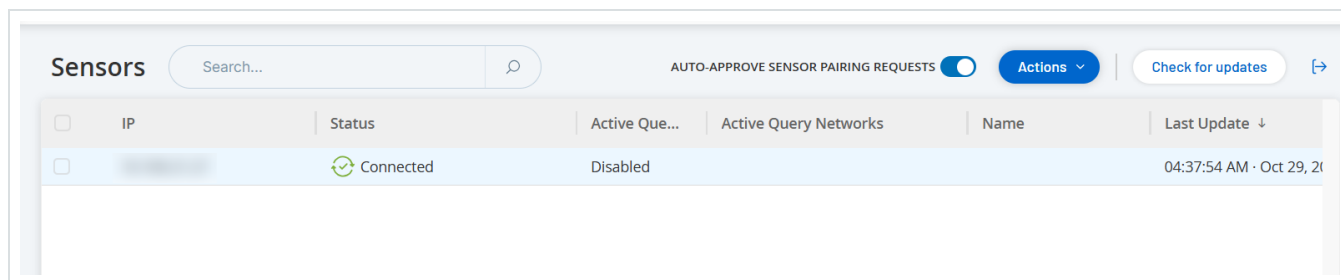
Remarque : Tenable recommande de créer un utilisateur ICP dédié avec un rôle d'administrateur pour le processus d'appairage des capteurs, afin d'éviter les interruptions de la connectivité (voir [Ajout d'utilisateurs locaux](#)). Vous pouvez ajouter un nouvel administrateur pour appairer plusieurs capteurs.

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 locaux > Capteurs.

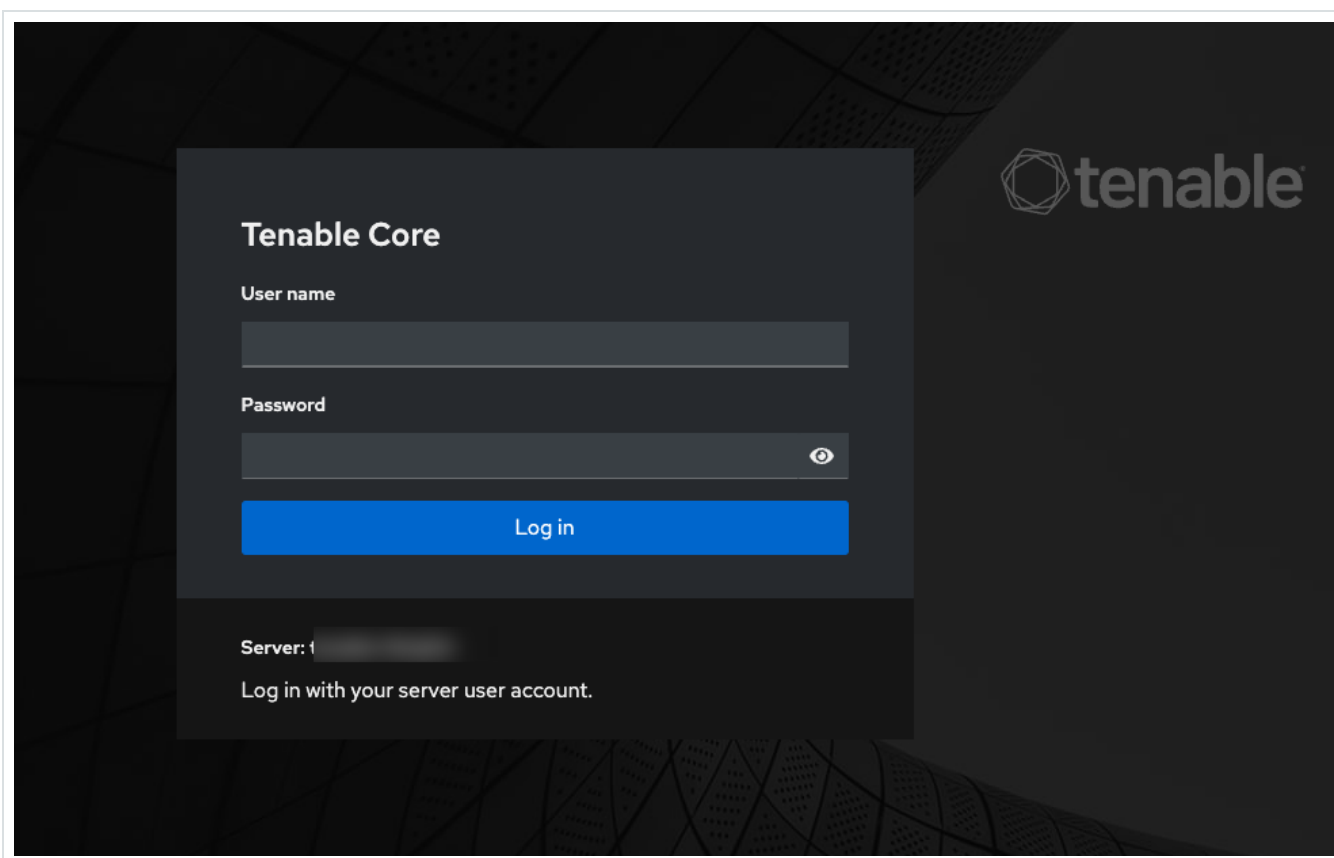




2. Pour activer l'approbation automatique de l'appairage de capteurs, vous devez activer l'option Approuver automatiquement les demandes d'appairage des capteurs en cliquant sur le curseur qui se trouve en haut de la page. Si vous ne le faites pas, vous devrez approuver manuellement toutes les demandes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

TENABLE.OT SENSOR PAIR

This Tenable.ot Sensor is not currently paired with a Tenable.ot ICP.
Enter the following information to pair it:

* ICP IP Address:

ICP User:

ICP Password:

ICP API Key:

Unauthenticated Pairing ☐

* - Field is required to continue. Username and password OR api key is required to continue.

✖ Error: Either API Key or username and password must be provided.

Pair Sensor Close

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.



TENABLE.OT ICP CERTIFICATE:

Certificate Subject:	Tenable.ot
Certificate Issuer:	Tenable.ot
Certificate Fingerprint:	
Not Valid Before:	Sun Jul 25 2021 16:46:57 GMT+0300
Not Valid After:	Tue Jul 25 2023 16:46:57 GMT+0300
Approval Status:	Pending user approval Approve Delete
Upload Approved Certificate	Choose File certificate (1).pem

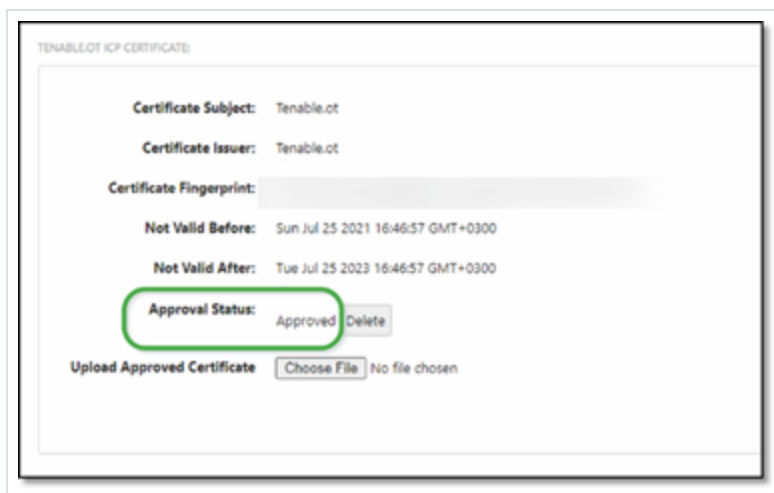
- b. Cliquez sur Approuver pour approuver le certificat.
- c. Dans la fenêtre Confirm Accept **Tenable OT Security** Server Certificate (Confirmer l'acceptation du certificat du serveur Tenable OT Security), cliquez sur Accept This Certificate (Accepter ce certificat).

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.

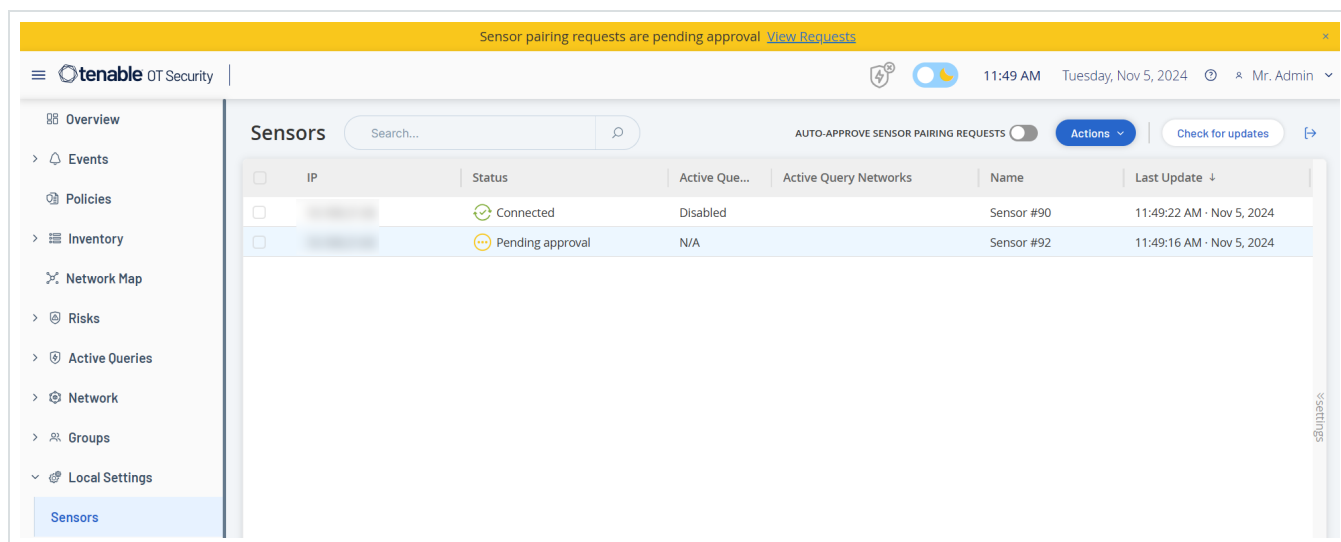


Une fois qu'un certificat valide est chargé, son statut d'approbation (Approval Status) dans le tableau OT Security ICP Certificate (Certificat ICP Tenable OT Security) apparaît comme Approved (Approuvé).

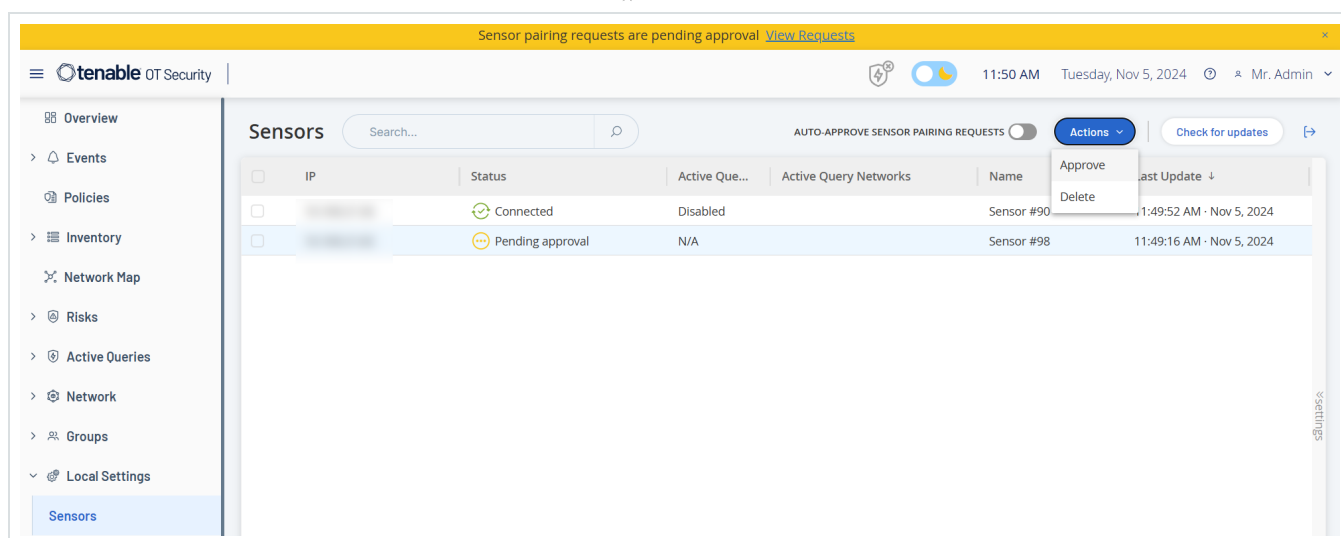


11. Dans l'interface utilisateur ICP, accédez à Paramètres locaux > Capteurs.

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 [Gérer les 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



Vous pouvez installer le capteur du modèle configurable sur un rail DIN ou le monter sur un rack 19 pouces standard (à l'aide du kit d'adaptation « oreilles de montage »).

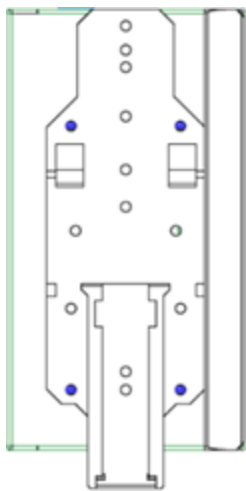
Configurer un capteur configurable

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 »).

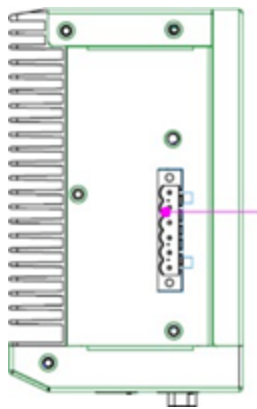
Montage sur rail DIN

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)

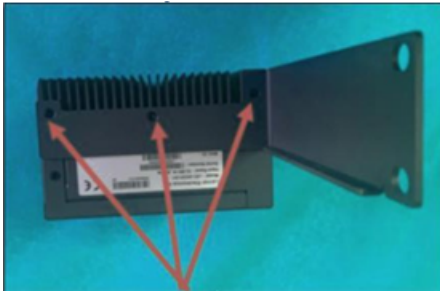
Un capteur configurable peut être fixé à un rack de montage à l'aide des « oreilles de montage » fournies.

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.

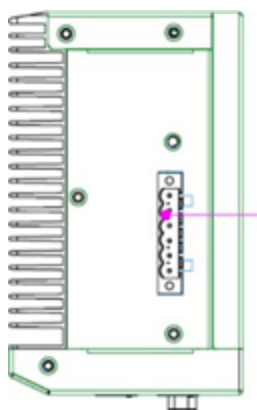
Remarque :

- 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 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

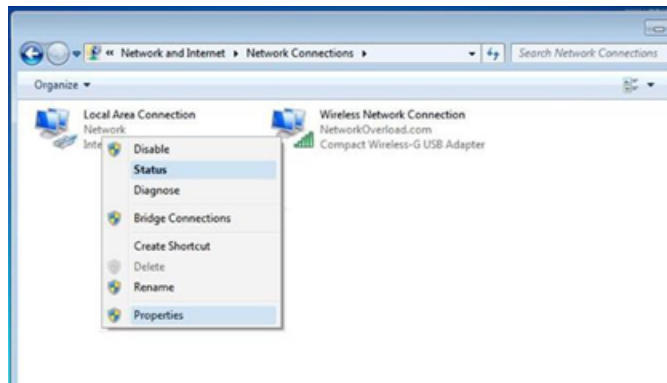
Pour se connecter à la console de gestion :

1. Effectuez l'une des actions suivantes :
 - Connectez le poste de travail de la console de gestion (PC ou ordinateur portable) directement au port 1 de 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.

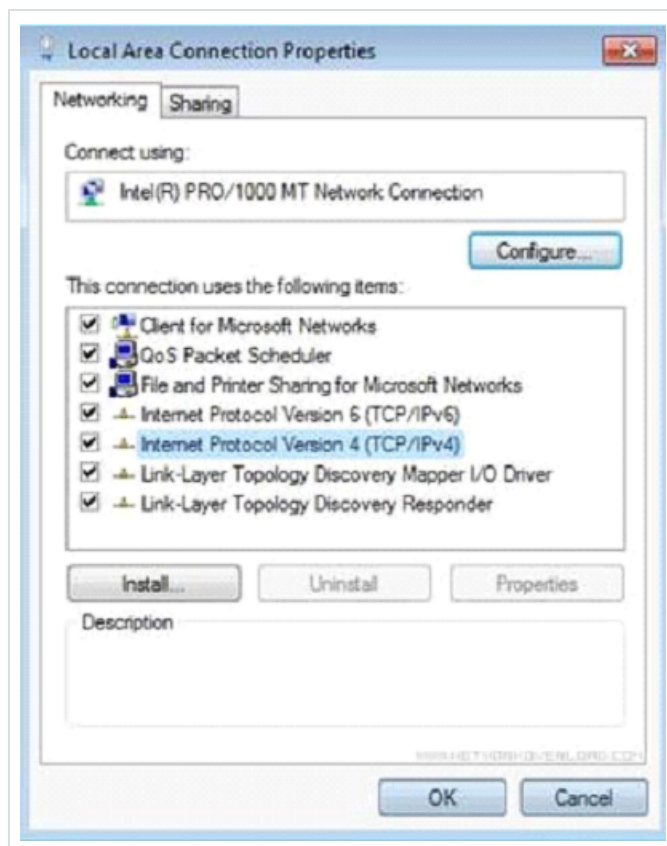


La fenêtre Connexions réseau apparaît.



- 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.



Établissement de la connexion à la console et de la configuration initiale

Cette rubrique décrit comment connecter une console série locale à vos appliances OT Security (ICP et capteurs). Utilisez cette méthode de connexion pour la configuration IP initiale, la résolution des problèmes réseau et la restauration de l'accès lorsque l'adresse IP de gestion est inaccessible.

Avant de commencer

Vous devez disposer du matériel et des logiciels suivants :

Logiciels

- Émulateur de terminal : utilitaire tel que PuTTY, Tenable Term, Série ou Minicom.
- Pilotes : assurez-vous d'installer les pilotes conçus pour votre câble ou votre adaptateur USB spécifique (par exemple, FTDI ou PL2303).

Options de matériel et de câble

Identifiez votre type d'appliance pour sélectionner la méthode de câble correcte :

- **Tenable OT Security** ou console ICP (plateforme Core industrielle) **Tenable**
 - Type de port : console RJ-45.
 - Câble recommandé : câble de console USB vers RJ45.

Remarque : un câble de console bleu clair de type Cisco est généralement inclus dans la boîte de l'appliance. Il s'agit d'un câble standard (environ 10 \$), couramment utilisé pour les commutateurs réseau.

- **Capteurs Tenable** : les capteurs existent en deux versions matérielles. Vérifiez les ports physique sur votre appareil :



- Port console RJ-45 : utilisez un câble console USB vers RJ45.
- Port DB9 (série) : utilisez un câble série USB-DB9.

Conseil : Tenable recommande d'utiliser des câbles de connexion directe USB vers DB9 (monobloc) plutôt que des adaptateurs en plusieurs parties pour minimiser les problèmes de connectivité.

Méthode alternative (adaptateurs antérieurs)

Si vous utilisez un adaptateur série-USB standard au lieu d'un câble direct USB-console , vous devez ajouter un adaptateur ou un connecteur modem nul dans la chaîne.

Conseil : de nombreux échecs de connexion se produisent parce que les adaptateurs série standard ne croisent pas correctement les broches de transmission ou de réception sans boîtier modem nul.

Connexion physique

1. Connectez l'extrémité USB de votre câble à votre poste de travail.
2. Connectez l'autre extrémité (RJ-45 ou DB9) à l'appliance.
 - Ports étiquetés : localisez le port ayant l'étiquette console, une icône de moniteur ou le symbole IOIOI.
 - Ports non étiquetés : si les ports n'ont pas d'étiquette, connectez-vous au port RJ-45 unique situé à gauche des ports USB.
3. Assurez-vous que le câble est correctement enfoncé.

Identifier le port COM (Windows)

Vous devez identifier le port de communication (COM) que Windows a attribué à votre câble.



1. Sur votre ordinateur Windows, effectuez un clic droit sur Démarrer et sélectionnez Gestionnaire de périphériques.

La fenêtre Gestionnaire de périphériques apparaît.

2. Dépliez l'entrée Ports (COM et LPT).
3. Localisez votre appareil (p. ex., port série USB) et notez le numéro (p. ex., COM3).

Configurer un terminal (PuTTY)

Lancez votre émulateur de terminal (PuTTY ou autre) et configurez la session avec les paramètres TTY Tenable suivants.

Dans PuTTY, accédez à Connexion > Série et configurez les paramètres suivants :

Paramètre	Valeur
Type de connexion	Numéro de série
Ligne série :	Votre port COM (p. ex., COM3)
Débit (Bauds)	115200
Bits de données	8
Bits d'arrêt	1
Parité	Aucun(e)
Contrôle de flux	Aucun(e) Remarque : vérifiez que le contrôle de flux n'est pas défini sur XON/XOFF.

Conseil : sur la page Sessions, enregistrez ces paramètres sous l'intitulé « Console Tenable OT » pour les réutiliser.



Établir une connexion

1. Cliquez sur Ouvrir pour démarrer la session.
2. Lorsque la fenêtre du terminal apparaît, appuyez deux fois sur Entrée pour activer la console.
3. Vérifiez que l'invite suivante apparaît :

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

4. Connectez-vous à l'invite.

Configuration réseau initiale

L'interface de gestion nécessite une adresse IP statique. Le protocole DHCP n'est pas pris en charge.

1. Exécutez l'outil de gestionnaire de réseau :

```
sudo nmtui
```

2. Sélectionnez Edit a connection (Modifier une connexion).
3. Sélectionnez l'interface de gestion (généralement la première interface, p. ex. nic0 ou eth0).

Attention : ne configurez pas la deuxième interface (généralement nic1). Il s'agit du port SPAN ou miroir dédié à la surveillance passive ; il ne nécessite pas d'adresse IP.

4. Réglez la configuration IPv4 sur <Manual> (manuelle).
5. Sélectionnez <Show> (Afficher) et saisissez les éléments suivants :



- Adresses (Adresses) : votre adresse IP statique ou votre CIDR (p. ex., 192.168.1.50/24)
- Gateway (Passerelle) : adresse IP de votre passerelle.
- DNS Serveurs (Serveurs DNS) : les adresses IP de vos DNS.

6. Descendez au bas de l'écran et sélectionnez <OK> pour enregistrer.

7. Sélectionnez <Quit> (Quitter).

Accéder à l'interface utilisateur

Après avoir configuré l'adresse IP, effectuez les opérations suivantes :

1. Connectez un câble réseau du port de gestion à votre commutateur réseau.
2. Ouvrez un navigateur et accédez à l'adresse IP via le port 8000 : `https://<VOTRE_IP_STATIQUE>:8000`

La page de connexion OT Security apparaît. Vous pouvez maintenant suivre l'assistant de configuration. Voir [Configurer les paramètres OT Security à l'aide de l'assistant de configuration](#).

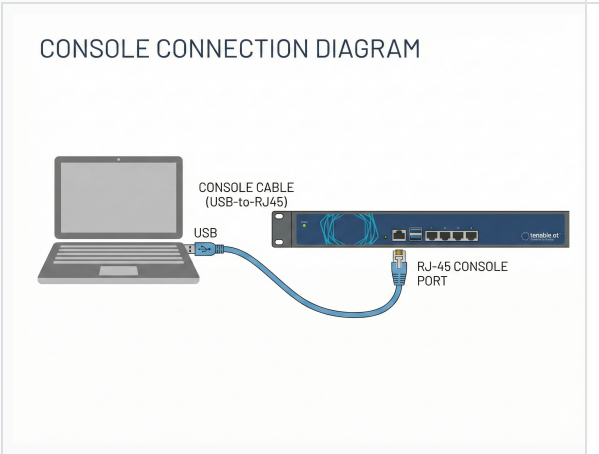
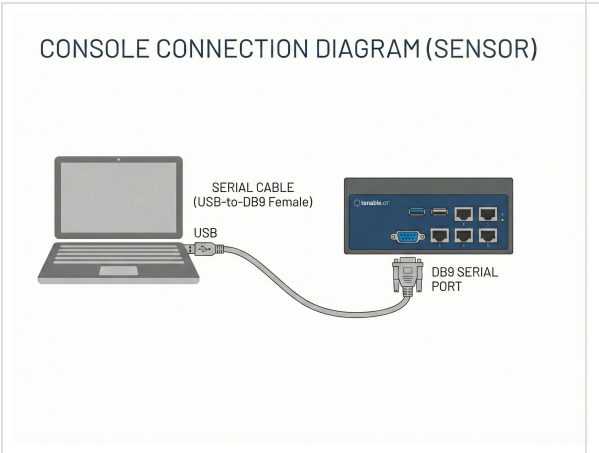
Voir aussi

[Câbles console à connecter au Capteur OT Security](#)

Câbles console à connecter au Capteur OT Security

Vous pouvez utiliser les câbles suivants pour connecter votre ordinateur portable au Capteur OT Security :



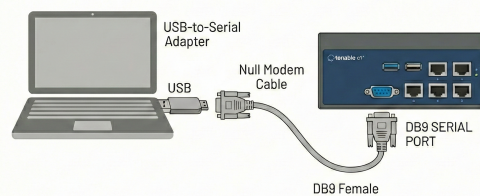
Câble	Image	Schéma de connexion à la console
Câble console (USB vers RJ45)		CONSOLE CONNECTION DIAGRAM  CONSOLE CABLE (USB-to-RJ45) USB RJ-45 CONSOLE PORT
Câble série (USB-to-DB9)		CONSOLE CONNECTION DIAGRAM (SENSOR)  SERIAL CABLE (USB-to-DB9 Female) USB DB9 SERIAL PORT



Câble
modem
nul



CONSOLE CONNECTION DIAGRAM (SENSOR - ADAPTER METHOD)



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.

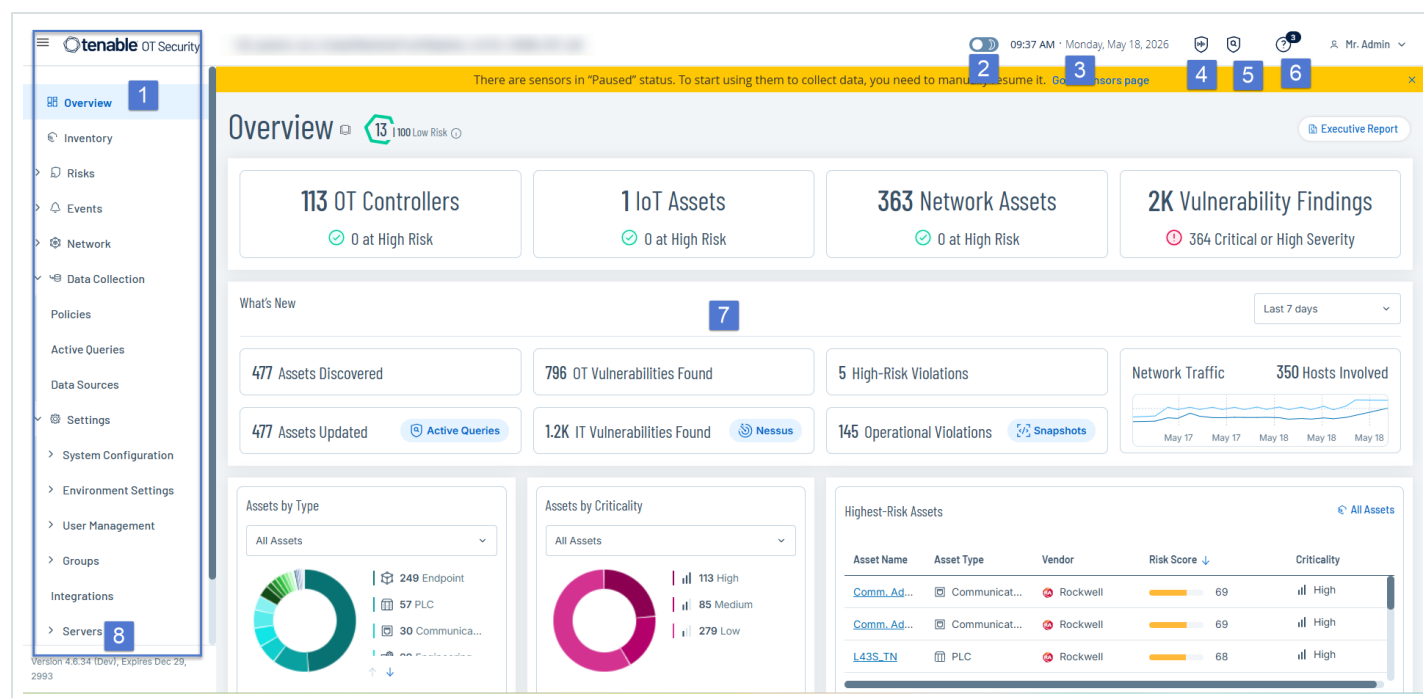
OT Security est restauré et vous pouvez accéder à l'application. Pour vérifier que OT Security est en cours d'exécution, utilisez votre navigateur pour vous connecter à l'interface utilisateur OT Security via le port 443 (HTTPS).



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.

N° de série	Élément de l'interface utilisateur	Description
1	Navigation principale	Menu de navigation principal. Cliquez sur l'icône 



		pour afficher/masquer le menu de navigation principal.
2	Mode sombre/Mode clair	Permet de basculer la palette de couleurs en mode sombre ou en mode clair.
3	Date et heure en cours	Affiche la date et l'heure actuelles enregistrées dans le système.
4	Surveillance passive	Indique si la surveillance passive est activée ou non.
4	Requêtes actives	Indique si les requêtes actives sont activées ou désactivées.
5	Centre de ressources	Centre de ressources OT Security. Cliquez pour accéder aux ressources d'aide, découvrir les mises à jour de fonctionnalités et faire part de vos commentaires.
6	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.
7	Informations sur la licence	Affiche la version du logiciel OT Security et la date d'expiration de la licence.
8	Écran principal	Affiche l'écran que vous avez sélectionné dans la navigation principale.



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

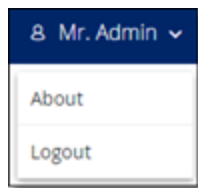
Vous pouvez vérifier la version du logiciel en utilisant l'icône de profil utilisateur dans le coin supérieur droit de la barre d'en-tête.

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.



Accéder au Centre de ressources

Le Centre de ressources affiche une liste de sources d'informations : des annonces de produits, des articles de blog Tenable et de la documentation à l'intention des utilisateurs.

Remarque : l'accès au Centre de ressources nécessite une connexion Internet. Le Centre de ressources  est désactivé par défaut. Pour activer le Centre de ressources, accédez à Paramètres > Configuration système > Appareil, puis cliquez pour activer le curseur Activer les statistiques



Enable Usage Statistics

Enable this option to turn on telemetry and to access the OT Security Resource Center. After enabling or disabling, refresh your browser for the change to take effect.

Note: When enabled, Tenable collects anonymous telemetry data from your account. This information cannot be attributed to a specific individual; it does not include Personal Data. We analyze this data in-house and also send it to third-party partners for analytics and optimization. We use this data to identify ways of improving the user experience in future Tenable OT Security releases. We may also use the data for other reasonable business purposes in accordance with the Tenable Master Agreement. You can disable this option at any time, in order to stop sharing usage statistics with Tenable.

l'utilisation.

Pour accéder au Centre de ressources :

1. Dans le coin supérieur droit, cliquez sur le bouton .

Le menu Centre de ressources apparaît.

2. Cliquez sur le lien d'une ressource pour y accéder. Vous trouverez les ressources suivantes :
 - Recherche dans la base de connaissances OT Security
 - Mises à jour de fonctionnalités

Naviguer dans OT Security

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

- Vue d'ensemble - Affiche des widgets qui donnent une vue générale de l'inventaire et de la sécurité de votre réseau. Cette section fournit un instantané localisé de l'empreinte totale des assets de votre réseau, des principales vulnérabilités et des alertes de sécurité critiques. Voir [Vue d'ensemble de OT Security](#).



- 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](#).
- Risques – 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](#).
- 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](#).
- Collecte de données - Cette section comprend les pages de configuration suivantes :
 - Politiques - Plan de contrôle administratif pour les règles relatives aux menaces. Affichez, modifiez et activez les politiques dans le système. Voir [Politiques](#).
 - Requêtes actives - Vous permet de configurer et d'activer des requêtes actives. Voir [Gérer les requêtes actives](#).
 - Sources de données - Configurez les capteurs, les agents et les connecteurs IoT. Chargez manuellement des assets, des fichiers SCD, des fichiers de projet Rockwell et des fichiers PCAP. Voir [Sources de données](#).
- Requêtes actives - Vous permet de configurer et d'activer des requêtes actives. Voir [Gérer les requêtes actives](#).
- 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.
- Cartographie du réseau - Affiche une représentation visuelle des assets du réseau et de leurs connexions. Voir [Cartographie du réseau](#).
- Paramètres - Affichez et configurez les paramètres système. Voir [Paramètres](#).
- Groupes - Affichez, créez et modifiez les groupes utilisés dans Configuration de la politique. Voir [Groupes](#).

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.

Important : dans la version 4.0, OT Security introduit plusieurs modifications de l'interface utilisateur, mais les pages de l'application ne sont pas toutes mises à jour. Dans cette version, seules les pages sous Inventaire et Vulnérabilités détectées utilisent la méthode améliorée pour personnaliser, filtrer, trier et rechercher. Ces étapes sont documentées dans des sections dont les en-têtes sont marqués spécifiquement pour la version 4.0. Par exemple : Personnaliser l'affichage des colonnes dans OT Security 4.0 et versions ultérieures.

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. Pour OT Security 4.0 et versions ultérieures, cliquez sur Colonnes affichées > Rétablir l'affichage par défaut.

Personnaliser l'affichage des colonnes (version 3.19 et antérieures)



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.

The screenshot shows the Tenable OT Security interface. On the left is a navigation sidebar with categories like Dashboards, Risk, Inventory, Events, Policies, Inventory, Network Map, Vulnerabilities, Active Queries, Network, Groups, and Local Settings. The main area displays the 'All Events' table. The table has columns: S..., Log ID, Time, Event Type, Severity, and Policy Name. The 'Table Settings' panel is open on the right, showing a list of columns with checkboxes to select or deselect them. The selected columns are: Status, Log ID, Time, Event Type, Severity, Policy Name, Source Asset, Source Address, Destination Asset, Destination Address, Protocol, Event Category, Resolved By, Resolved On, and Comment. A 'Reset table to default' button is at the bottom of the panel.

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 :

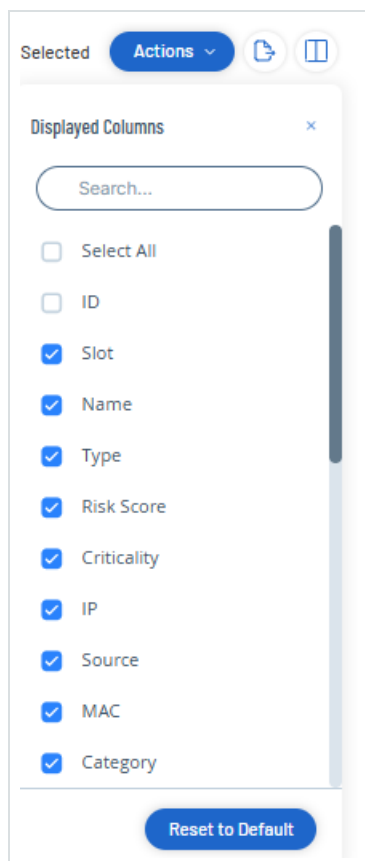
1. Cliquez sur un en-tête de colonne et faites-le glisser vers la position souhaitée.

Personnaliser l'affichage des colonnes (version 4.0 et ultérieures)



1. Dans la barre d'en-tête, cliquez sur le bouton .

Le panneau Colonnes affichées apparaît.



2. Cochez les cases à côté des colonnes que vous souhaitez afficher.

Remarque : décochez la case à côté des colonnes que vous souhaitez masquer.

Conseil : utilisez la zone de recherche pour rechercher des colonnes spécifiques.

3. Cliquez sur le bouton  pour fermer le panneau Colonnes affichées.

OT Security affiche uniquement les colonnes sélectionnées.

Regrouper des listes par catégories (version 3.19 et antérieures)



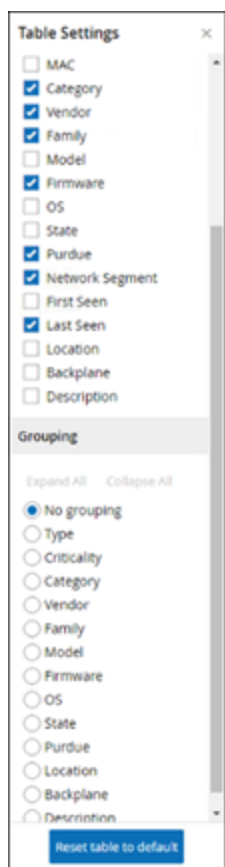
Pour les pages Inventaire, vous pouvez regrouper les listes selon divers paramètres pertinents pour cet écran particulier.

Pour regrouper les listes :

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

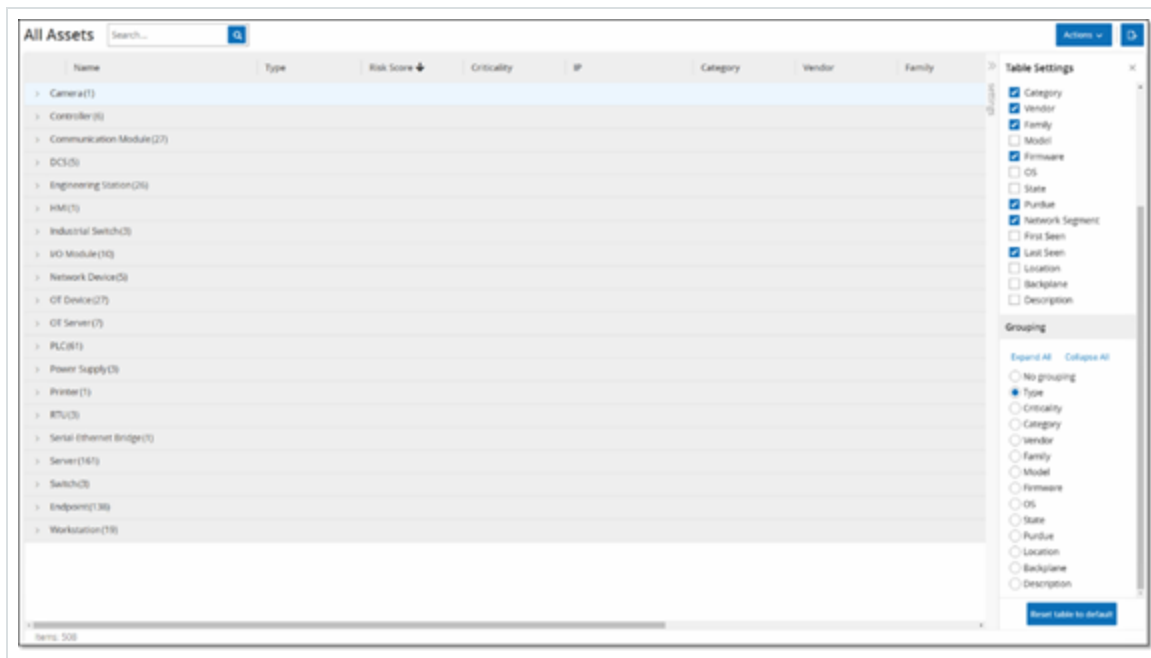
Le panneau Paramètres du tableau apparaît sur le côté droit, en affichant les sections Colonnes et Regroupements.

2. Faites défiler jusqu'à la section Regroupements.



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

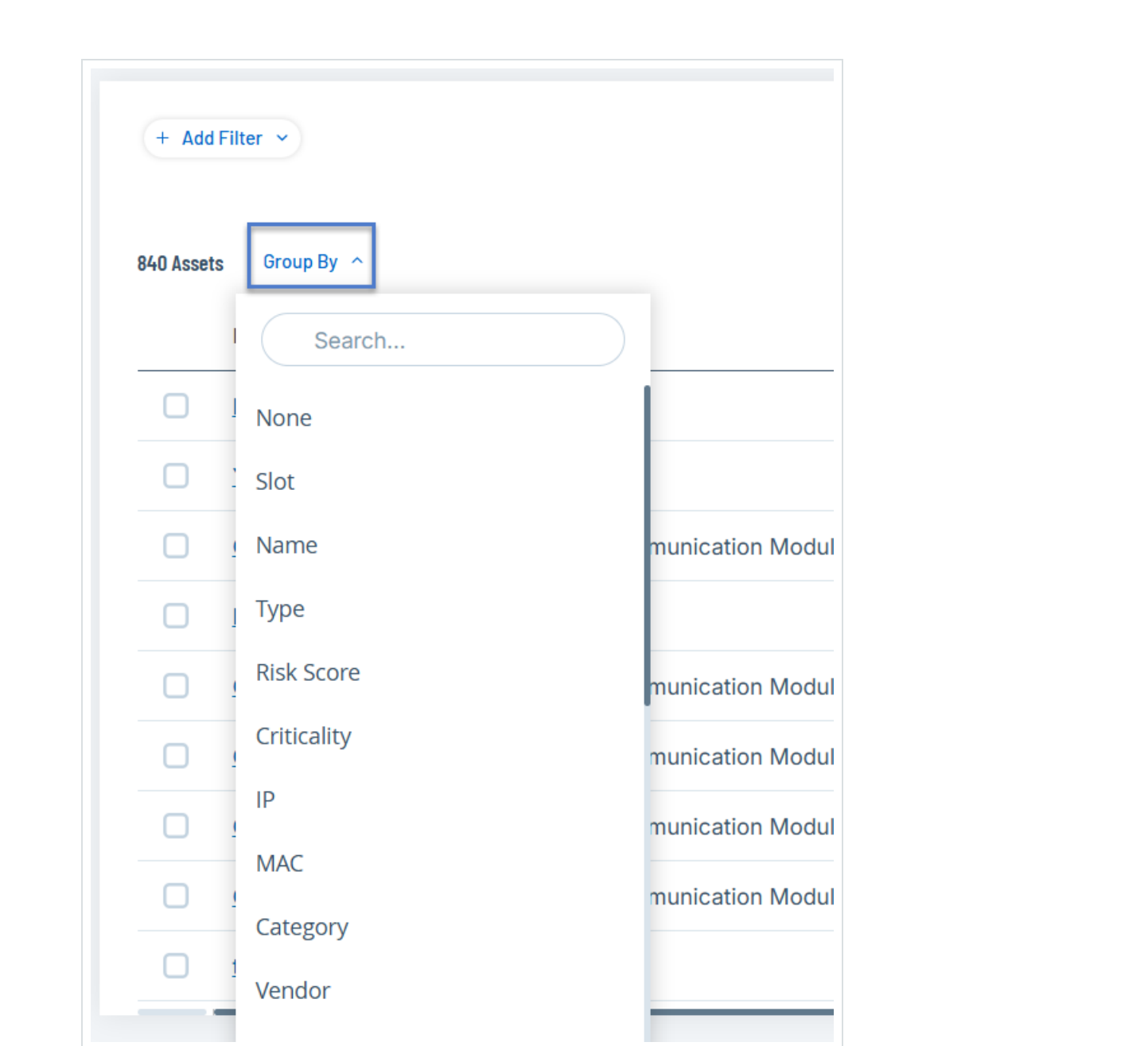
OT Security affiche les catégories regroupées.



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.

Name	Type	Risk Score	Criticality	IP	Category	Vendor	Family
> Camera(1)							
> Controller(6)							
> Communication Module(27)							
☐ Comm_Adapter #56	Communication M...	25	High	10.100.101.151 10.100...	Controllers	Rockwell	
☐ Comm_Adapter #64	Communication M...	25	High	10.100.101.151 10.100...	Controllers	Rockwell	
☐ Comm_Adapter #82	Communication M...	25	High	10.100.101.151 10.100...	Controllers	Rockwell	
☐ Comm_Adapter #52	Communication M...	25	High	10.100.101.151 10.100...	Controllers	Rockwell	
☐ Comm_Adapter #220	Communication M...	25	High	10.100.105.24	Controllers	Schneider	
☐ Comm_Adapter #53	Communication M...	25	High	10.100.101.151 10.100...	Controllers	Rockwell	
☐ BMX_NOC601	Communication M...	16	High	10.100.105.40	Controllers	Schneider	
☐ CM 3342-1-1	Communication M...	16	High	10.100.102.70 10.100.1...	Controllers	Siemens	
☐ 00300622830C	Communication M...	3	High	10.100.111.5	Controllers	Wago Corporation	
☐ Comm_Adapter #253	Communication M...	16	High		Controllers	Rockwell	

Regrouper des listes par catégories (version 4.0 et ultérieures)



Conseil : utilisez la zone de recherche pour rechercher un paramètre spécifique.



Remarque : utilisez les boutons Tout développer ou Tout réduire pour développer ou réduire la liste.

Trier des colonnes

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).

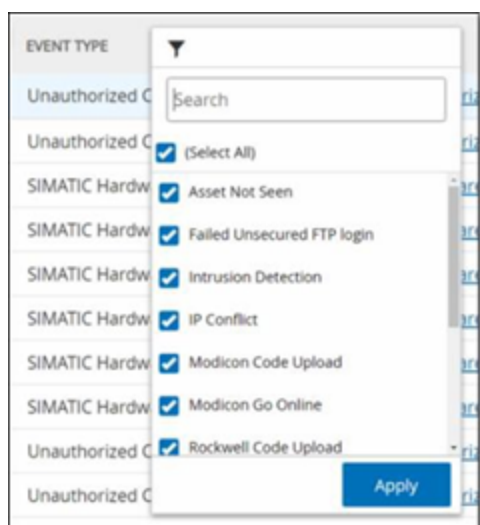
Filtrer les colonnes (version 3.19 et antérieures)

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 page propose une sélection de filtres pertinents. Par exemple, dans la fenêtre Inventaire des contrôleurs, vous pouvez filtrer par nom, adresses, type, fond de panier et fournisseur.

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 :

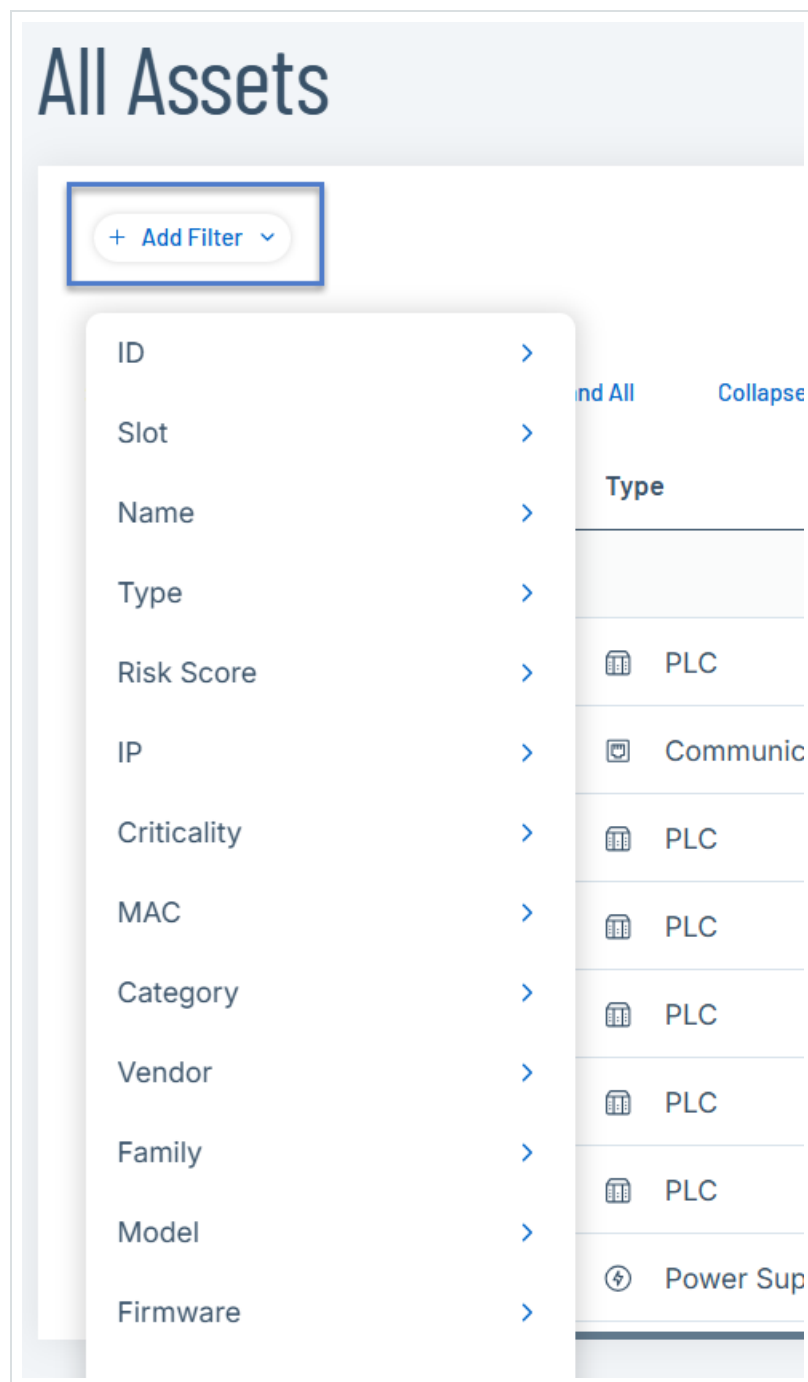
1. Cliquez sur le bouton de filtre ▼.
2. Cliquez sur la case Tout sélectionner pour effacer toutes les sélections.
3. Cliquez à nouveau sur la case Tout sélectionner pour sélectionner tous les éléments.
4. Cliquez sur Appliquer.

Filtrer les colonnes (version 4.0 et ultérieures)



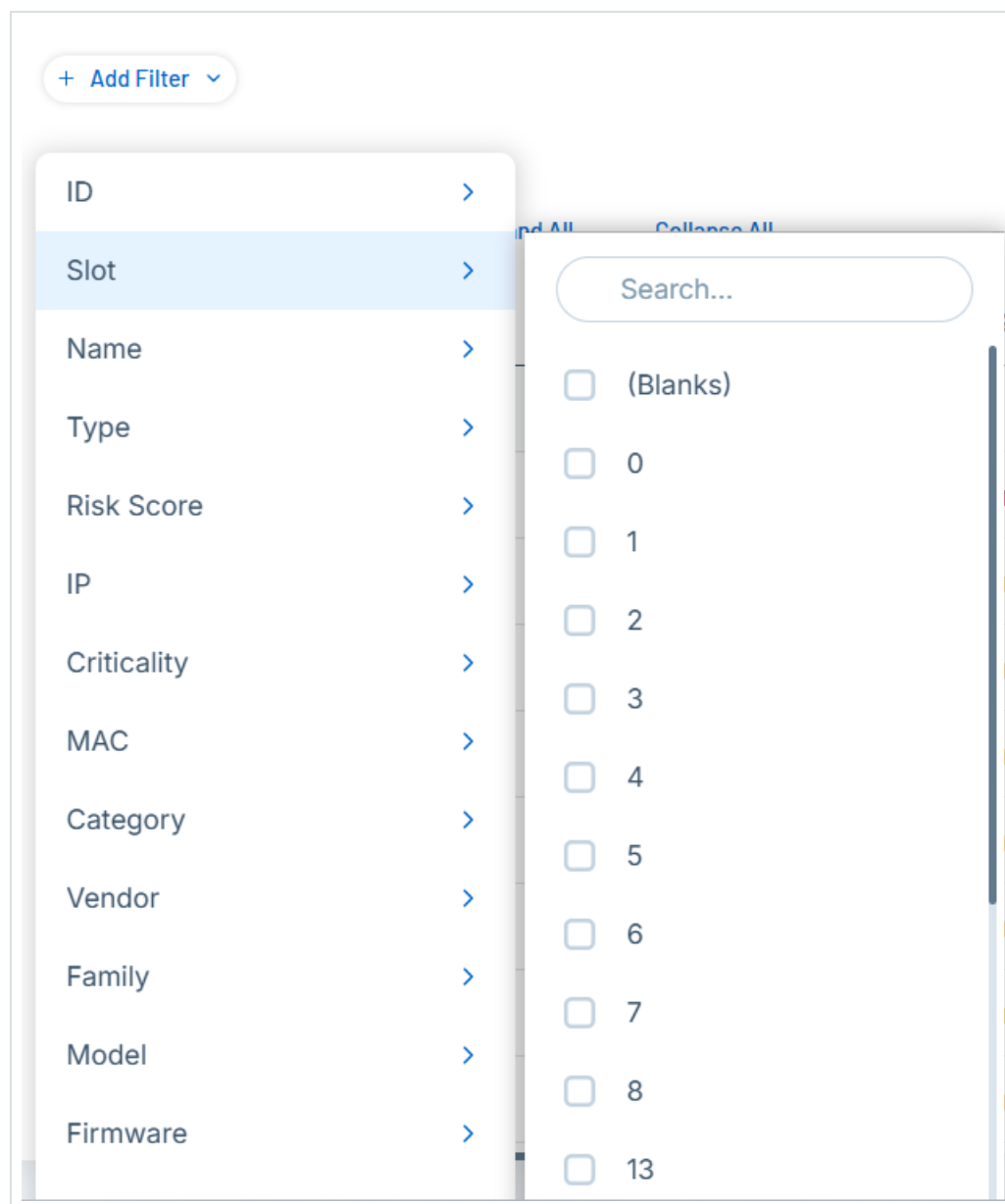
1. Dans l'en-tête du tableau, cliquez sur la liste déroulante Ajouter un filtre  .

Un menu déroulant apparaît avec les éléments de filtrage disponibles.



2. Sélectionnez l'élément selon lequel vous souhaitez filtrer.

Une liste d'options de filtrage apparaît.



3. Cochez les cases à côté des options que vous souhaitez filtrer.

Conseil : utilisez la zone de recherche pour rechercher des options de filtrage spécifiques.

Enregistrer un filtre



Vous pouvez enregistrer les filtres que vous utilisez fréquemment et y accéder à partir de la fonctionnalité Filtres enregistrés selon les besoins. Vous pouvez ainsi enregistrer des vues filtrées spécifiques pour y revenir rapidement.

The screenshot shows the 'Inventory' dashboard with tabs for 'All Assets', 'Controllers & Modules', 'Network Assets', and 'IoT Assets'. The 'All Assets' tab is selected. A search bar and a '+ Add Filter' button are visible. The dropdown menu for '+ Add Filter' is open, showing a list of saved filters: 'Filter_1_type', 'New_saved filter', 'saved_filter_1', 'IP saved filters', 'Copy of Filter_1_type', and 'backplane filter'. Below the dropdown, a table displays asset information with columns for 'Type', 'Risk Score', and 'Criticality'.

Type	Risk Score	Criticality
PLC	76	High
Communication Mo...	75	High
PLC	71	High

Remarque : la fonctionnalité Filtres enregistrés est disponible sur les pages Inventaire, Détections > Vulnérabilités et Détections > Violations de politique.

Pour enregistrer un filtre fréquemment utilisé :

1. Dans l'en-tête du tableau, cliquez sur la liste déroulante Ajouter un filtre .

Un menu déroulant apparaît avec les éléments de filtrage disponibles.

2. Sélectionnez les éléments de filtrage souhaités.
3. Cliquez sur Appliquer le filtre.

OT Security affiche les résultats filtrés.



4. Pour enregistrer le filtre, cliquez sur Enregistrer le filtre.

Le panneau Enregistrer le filtre apparaît.

5. Dans la zone Nom, saisissez le nom du filtre.

6. Cliquez sur Enregistrer.

OT Security enregistre le filtre.

7. Pour accéder aux filtres enregistrés, cliquez sur le bouton .

La liste des filtres enregistrés apparaît.

8. Cliquez sur le filtre souhaité et affichez les résultats filtrés.

Modifier les filtres enregistrés

Vous pouvez modifier les filtres enregistrés.

Pour modifier les filtres enregistrés :

1. Dans l'en-tête du tableau, cliquez sur le bouton .

La liste des filtres enregistrés apparaît.

2. Cliquez sur un filtre enregistré que vous souhaitez modifier.
3. Ajoutez ou supprimez des éléments de filtrage selon les besoins.
4. Cliquez sur Enregistrer le filtre et sélectionnez Enregistrer les modifications.

OT Security enregistre les modifications apportées au filtre.

Créer une copie du filtre enregistré

Vous pouvez dupliquer le filtre enregistré et l'enregistrer comme un nouveau filtre.

Pour dupliquer un filtre enregistré et l'enregistrer sous un nouveau nom :



1. Dans l'en-tête du tableau, cliquez sur le bouton

La liste des filtres enregistrés apparaît.

2. Cliquez sur un filtre enregistré que vous souhaitez copier.
3. Cliquez sur Enregistrer le filtre et sélectionnez Enregistrer comme copie.

Le panneau Enregistrer le filtre apparaît.

4. Dans la zone Nom, modifiez le nom du filtre.
5. Cliquez sur Enregistrer.

OT Security enregistre le filtre.

Supprimer tous les filtres

Pour supprimer tous les filtres appliqués et remettre le tableau à son état d'origine, c'est-à-dire sans filtre :

- Dans l'en-tête du tableau, cliquez sur Supprimer tous les filtres.

Voir les filtres enregistrés

Vous pouvez afficher vos filtres enregistrés en procédant de deux manières :

- Sur n'importe quelle page où les filtres enregistrés sont activés, sélectionnez l'icône Filtres enregistrés. Voir [Enregistrer un filtre](#).

Remarque : les filtres enregistrés ne sont actuellement activés que sur les pages Inventaire, Détections de vulnérabilités et Violations de politique.

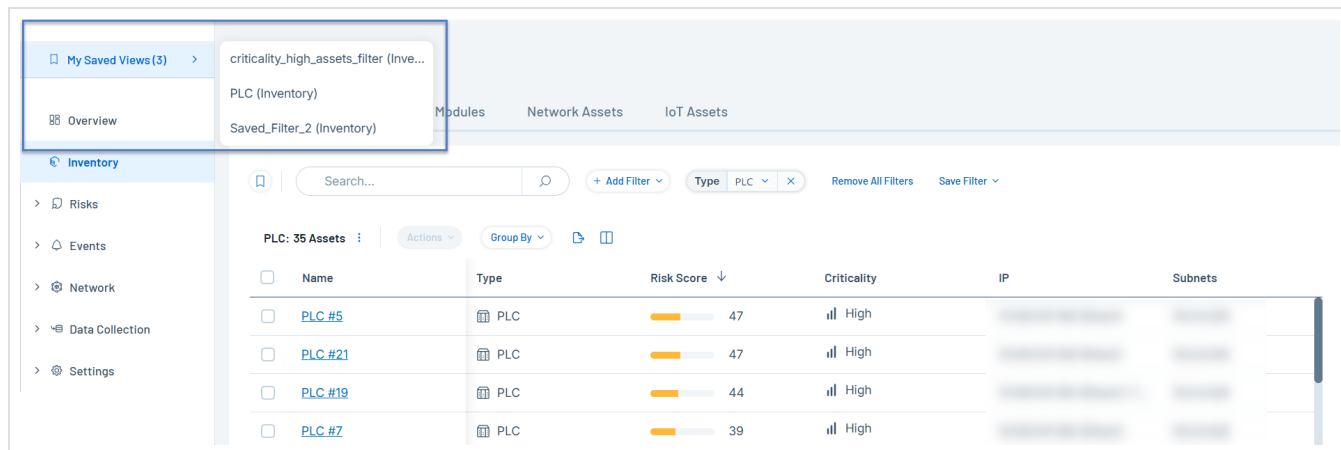
- Sur n'importe quelle page, sélectionnez Mes vues enregistrées dans le menu de navigation de gauche.

Pour afficher tous vos filtres enregistrés à partir de n'importe quelle page :



1. Dans le menu de navigation de gauche, cliquez sur Mes vues enregistrées ou sélectionnez l'icône Filtres enregistrés sur la page Inventaire.

Une liste des filtres enregistrés apparaît.



2. Cliquez sur un nom de filtre.

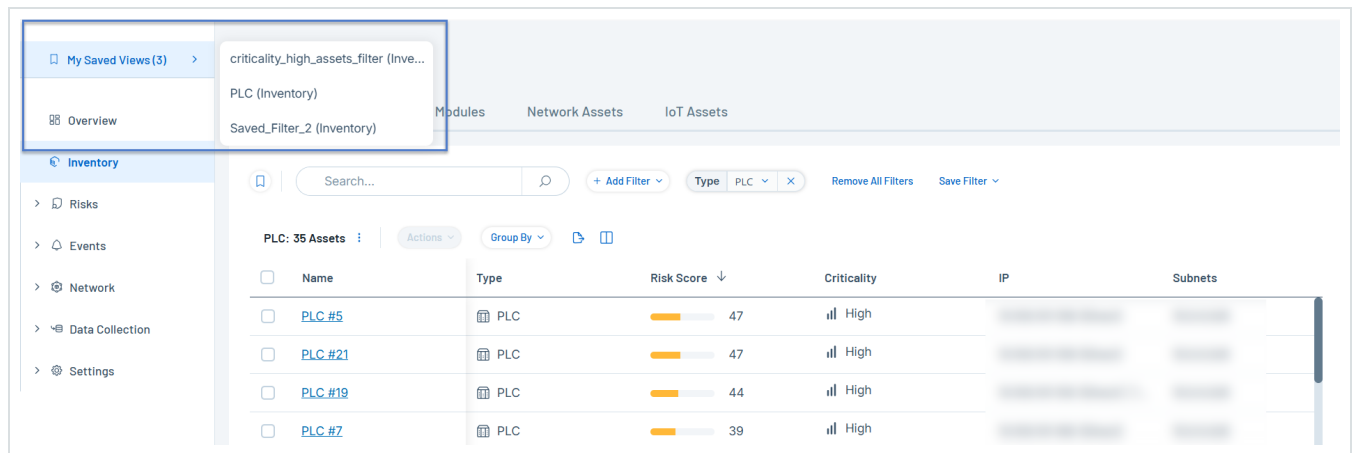
OT Security affiche la page Inventaire avec la vue filtrée des assets.

Modifier le nom du filtre enregistré

Pour modifier le nom du filtre :

1. Dans le menu de navigation de gauche, cliquez sur Mes vues enregistrées ou sélectionnez l'icône Filtres enregistrés sur la page Inventaire.

Une liste des filtres enregistrés apparaît.

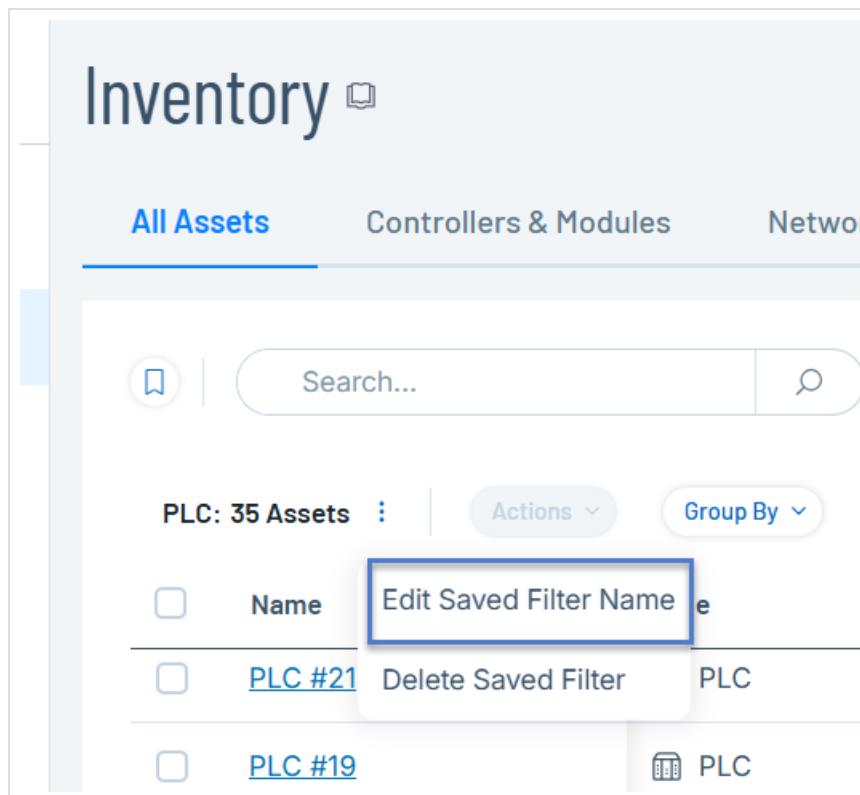


2. Cliquez sur le nom du filtre que vous souhaitez modifier.

OT Security affiche la page Inventaire avec la vue filtrée des assets.

3. Cliquez sur le bouton d'options Plus : à côté du nom du filtre.

Un menu apparaît.





4. Sélectionnez Modifier le nom du filtre enregistré.

Le volet Modifier le filtre enregistré apparaît.

5. Modifiez le nom comme souhaité.
6. Cliquez sur Enregistrer.

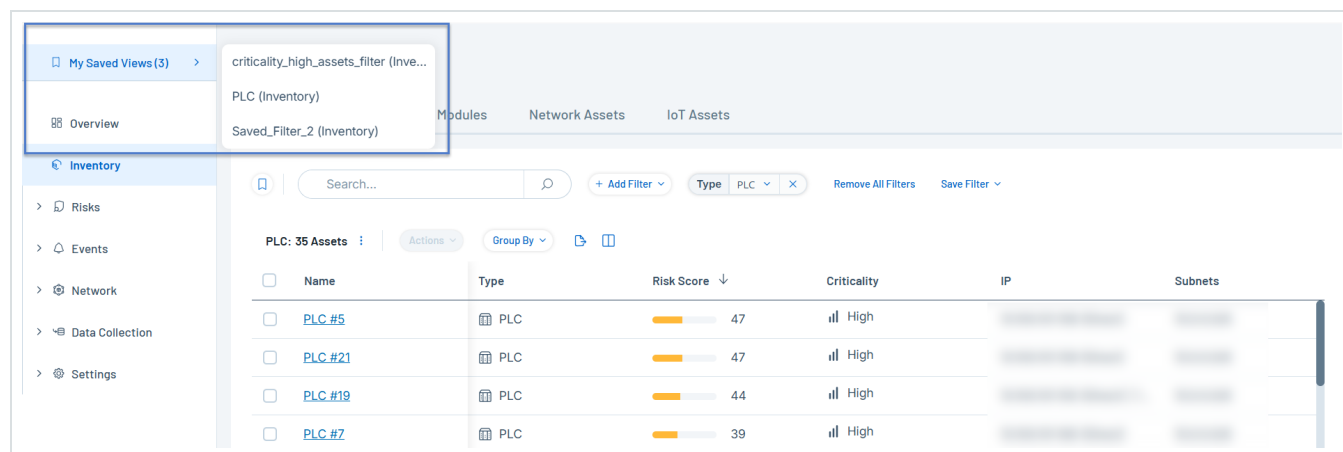
OT Security enregistre le nom de filtre modifié. Pour modifier les détails d'un filtre, afin d'ajouter ou de retirer des filtres, par exemple, voir [Modifier les filtres enregistrés](#).

Supprimer un filtre enregistré

Pour supprimer des filtres :

1. Dans le menu de navigation de gauche, cliquez sur Mes vues enregistrées ou sélectionnez l'icône Filtres enregistrés sur la page Inventaire.

Une liste des filtres enregistrés apparaît.

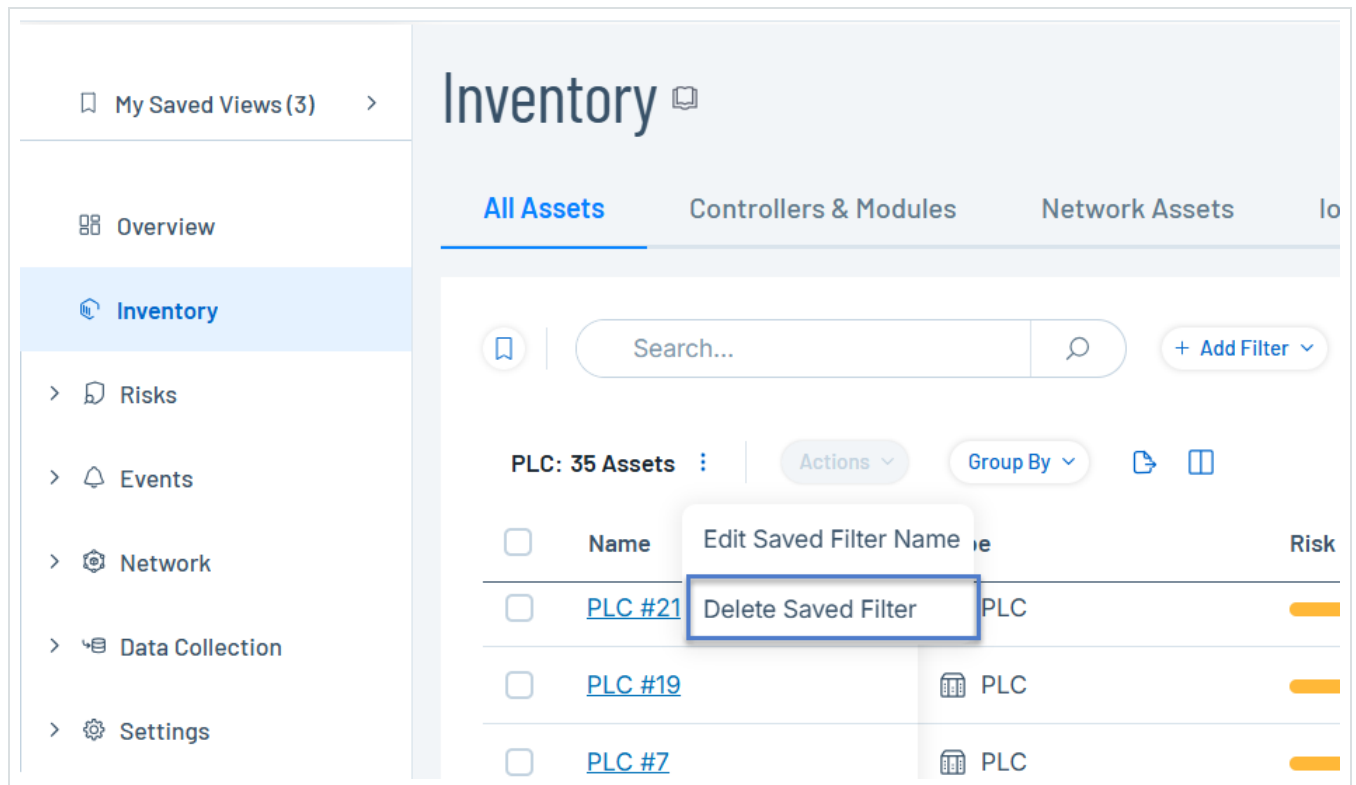


2. Cliquez sur le filtre que vous souhaitez supprimer.

OT Security affiche la page Inventaire avec la vue filtrée des assets.

3. Cliquez sur le bouton d'options Plus  à côté du nom du filtre.

Un menu apparaît.



4. Sélectionnez Supprimer le filtre enregistré.

OT Security supprime le filtre.

Effectuer une recherche (version 3.19 et antérieures)

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 ».

Effectuer une recherche (version 4.0 et ultérieures)



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 .

Exporter des données

Vous pouvez exporter des données de n'importe quelle liste affichée dans l'interface utilisateur de OT Security (p. ex. : événements et inventaire) 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 le bouton .

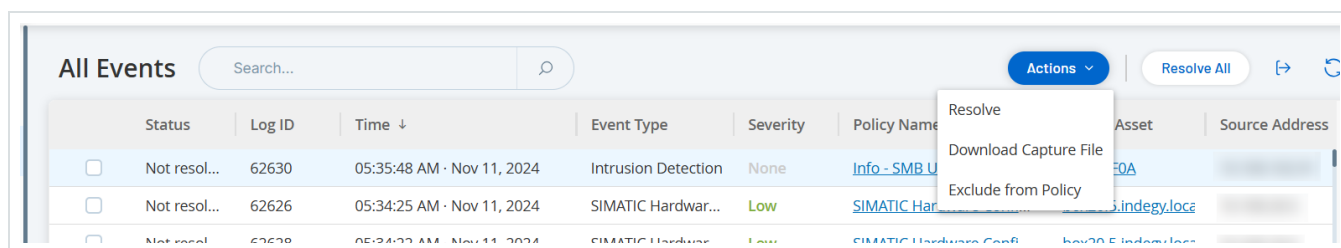
OT Security télécharge les données au format CSV.

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** un événement ou **télécharger le fichier de capture** correspondant.

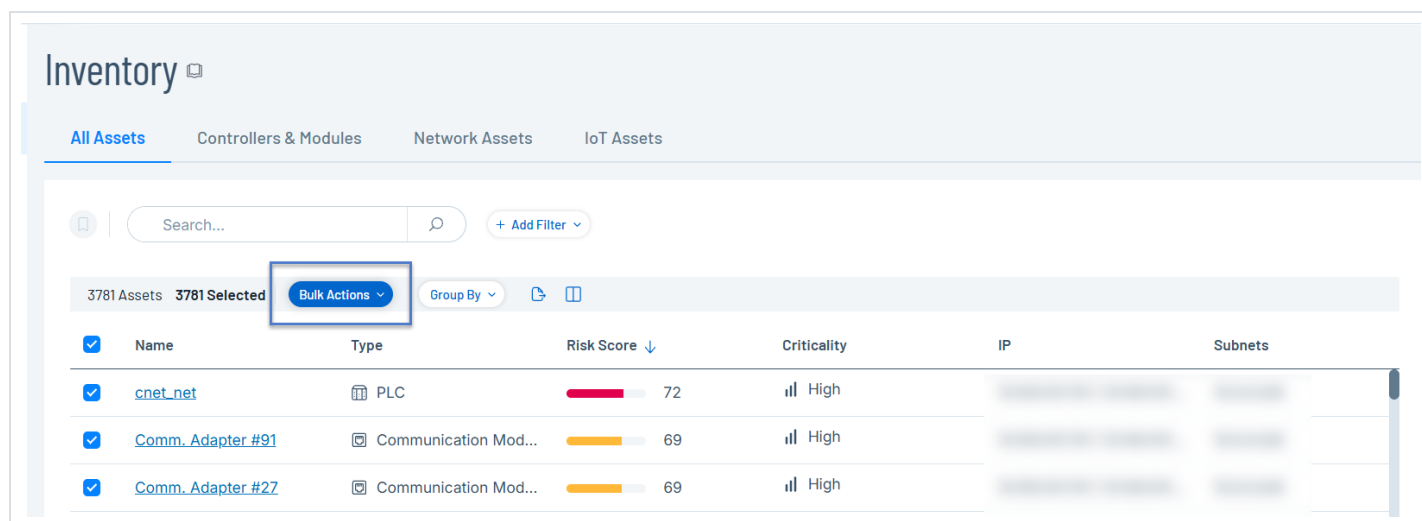
Pour accéder au menu Actions :

- Sélectionnez un élément, puis cliquez sur Actions dans la barre d'en-tête,



Actions en bloc

Lorsque vous sélectionnez plusieurs éléments sur une page, OT Security active l'option Actions en bloc dans l'en-tête.





Vue d'ensemble de OT Security

Utilisez la page Vue d'ensemble pour afficher les informations clés de votre environnement OT via des widgets interactifs. Les widgets de cette page fournissent des informations en temps réel sur votre environnement, et notamment :

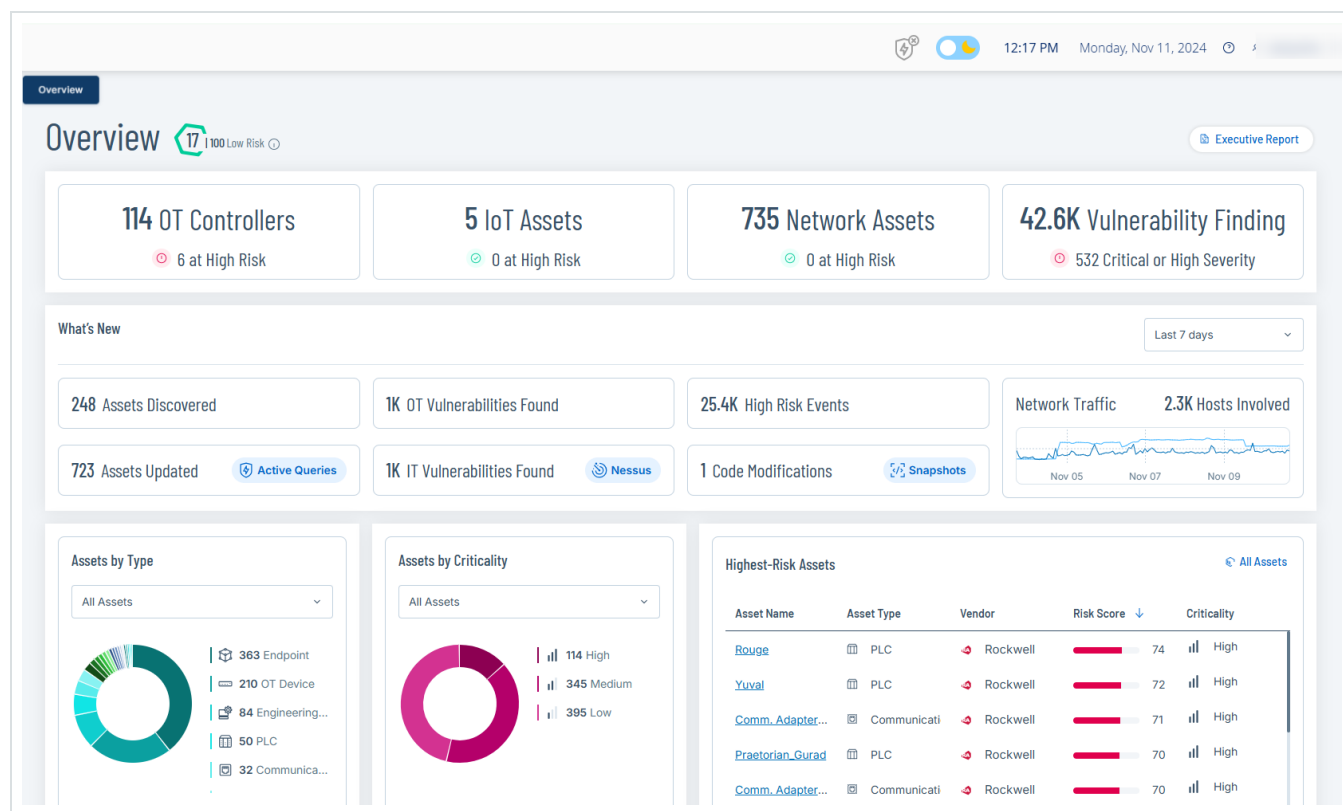
- Des informations sur la posture de sécurité de votre environnement.
- Un résumé des changements récents depuis votre dernière connexion.
- Une répartition des différents types d'assets de votre inventaire.
- L'état actuel des assets et des vulnérabilités.
- Les assets qui présentent le plus de risque.
- L'horodatage de votre dernière révision de code.

Pour accéder à la page Vue d'ensemble :



1. Dans la barre de navigation de gauche, cliquez sur Vue d'ensemble.

La page Vue d'ensemble apparaît.



La page Vue d'ensemble comprend les widgets suivants :

Widget	Description
Score de risque	Le score de risque moyen est la moyenne de tous les scores d'assets de votre environnement. Pour afficher une répartition du score, survolez la valeur. Le score de risque moyen utilise les codes couleur suivants pour indiquer la sévérité du risque : - Faible (vert) : 0-29 - Moyenne (jaune) : 30-69



	• Élevée (rouge) : 70-100 OT Security calcule les scores des assets en fonction des facteurs suivants, qui évoluent au fil du temps (obsolescence des événements, firmware et changements d'état) : • Criticité - En fonction du type d'asset et du niveau Purdue. Par exemple, un PLC contrôle la production. Il est donc considéré comme critique, tandis qu'une caméra sera généralement considérée comme moins critique. • Vulnérabilités - En fonction du classement VPR (Vulnerability Priority Rating) associé à l'asset. • Événements - En fonction des événements associés à l'asset. Les politiques déclenchent des événements et chacune d'elle définit une sévérité. La sévérité est calculée en fonction du nombre d'événements, de leur sévérité et de la durée de leur présence. Les événements plus anciens ont moins d'influence sur le score que les événements récents. • Fond de panier - Un asset qui réside sur un fond de panier influence le score des assets voisins. Par exemple, si un module est vulnérable, l'ensemble du fond de panier l'est également.
Assets et vulnérabilités	État actuel des assets et des vulnérabilités de votre environnement. Inclut des widgets distincts pour chaque type d'asset (contrôleurs OT, assets réseau, assets IoT) qui affichent le nombre d'assets dans cette catégorie et le nombre d'assets à haut risque. Remarque : les assets avec un score de risque de 70 et plus sont considérés à haut risque.



Nouveautés	Résumé des changements depuis votre dernière connexion, tels que les assets, vulnérabilités et événements à haut risque qui sont apparus. Accédez à la page des assets, événements ou vulnérabilités respectifs pour afficher les assets, les vulnérabilités ou les événements filtrés. Résumé des changements depuis votre dernière connexion, tels que les assets, vulnérabilités, violations à haut risque et exceptions opérationnelles qui sont apparus. Accédez à la page des assets, détections ou vulnérabilités correspondante pour afficher les assets, les vulnérabilités ou les événements filtrés. Utilisez le menu déroulant des filtres pour filtrer les résultats à l'aide des options Dernier jour, 7 derniers jours (par défaut) ou 30 derniers jours.
Assets par type	Nombre d'assets par type, par exemple : endpoint, PLC et appareil OT.
Assets par criticité	Nombre d'assets par criticité : élevée, moyenne ou faible.
Assets présentant le plus de risque	Répertorie tous les assets à haut risque avec des détails tels que le nom de l'asset, le type, le fournisseur, le score du risque et la criticité. Pour accéder à la page Tous les assets : dans le coin supérieur droit, cliquez sur le lien Tous les assets.
Rapport exécutif	Génère un rapport d'évaluation des risques de votre environnement OT. Pour plus d'informations, voir Générer un rapport exécutif .

Générer un rapport exécutif

Vous pouvez générer un rapport d'évaluation des risques de votre environnement sur la base des données des 30 derniers jours. OT Security utilise des widgets clés des dashboards Risques, Inventaire et Événements et politiques pour créer un aperçu graphique de haut niveau mettant en



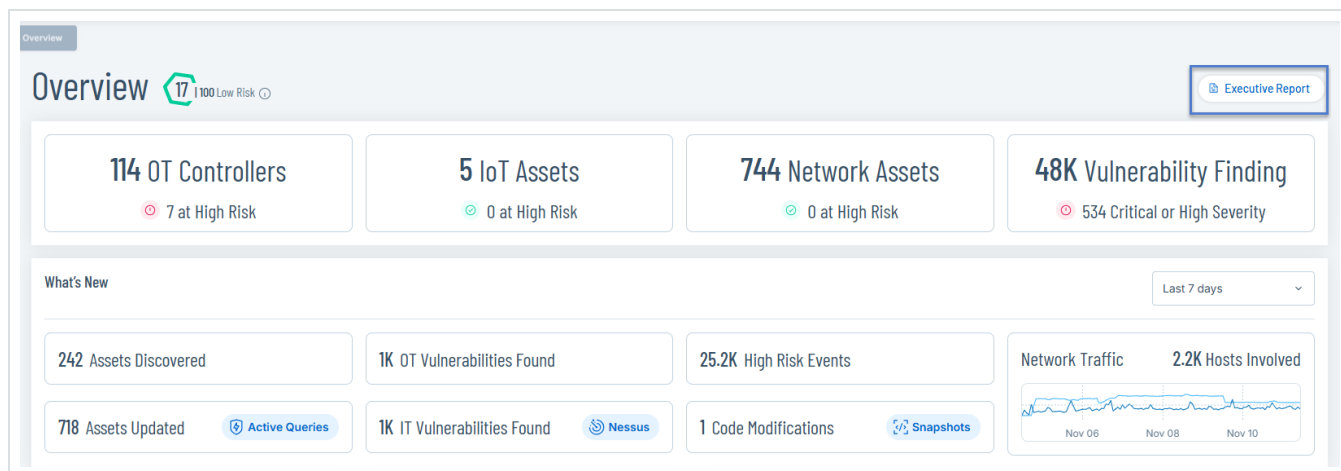
évidence les assets à haut risque, les vulnérabilités critiques et courantes, les familles de plug-ins courantes et les assets récemment découverts.

Utilisez les graphiques du rapport (vulnérabilités par sévérité, assets par score de risque et assets par criticité, etc.) pour identifier les assets critiques et les vulnérabilités les plus graves de votre environnement au cours des 30 derniers jours.

Pour générer un rapport mensuel :

1. Dans la barre de navigation de gauche, accédez à Vue d'ensemble.

La page Vue d'ensemble apparaît.



2. Dans le coin supérieur droit, cliquez sur Rapport exécutif.

OT Security ouvre le rapport sur votre navigateur.

3. Pour télécharger le rapport au format PDF, cliquez sur Enregistrer au format PDF en haut de la page.

La boîte de dialogue Imprimer apparaît.

4. Dans la zone déroulante Cible, sélectionnez Enregistrer au format PDF.
5. Accédez à l'emplacement où vous souhaitez enregistrer le rapport.



6. Cliquez sur Enregistrer.

OT Security enregistre le rapport au format PDF.

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

Inventory

All Assets Controllers & Modules Network Assets IoT Assets

Search...

+ Add Filter

969 Assets Actions Group By

	Name	Type	Risk Score	Criticality	IP	Subnets	Source	Tags
☐	Comm. Adapter #12	Communication Mo...	70	High			nic1 (Local) nic0 (Local)	
☐	testigy	PLC	67	High			nic1 (Local) nic0 (Local)	
☐	PLC #63	PLC	66	High			nic1 (Local) nic0 (Local)	
☐	Comm. Adapter #20	Communication Mo...	66	High			nic1 (Local) nic0 (Local)	
☐	Comm. Adapter #23	Communication Mo...	66	High			nic1 (Local) nic0 (Local)	
☐	A10_L81E	PLC	62	High			nic1 (Local) nic0 (Local)	
☐	BMX.NOC0401	Communication Mo...	61	High			nic1 (Local) nic0 (Local)	
☐	ML1100	PLC	60	High			nic1 (Local) nic0 (Local)	
☐	Praetorian_Gurad	PLC	60	High			nic1 (Local) nic0 (Local)	
☐	RTU #1	RTU	59	High			nic1 (Local) nic0 (Local)	
☐	CPU_412-2 PN/DP	PLC	59	High			nic1 (Local) nic0 (Local)	

Inventory

All Assets Controllers & Modules Network Assets IoT Assets

Search...

+ Add Filter

2291 Assets Actions Group By



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.



Paramètre	Description
	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.
Sous-réseaux	Les sous-réseaux découverts en interrogeant les appareils réseau via SNMP.
Source	Nom de la source. Par exemple, nic 1 ou nic 2 pour une source locale, ou le nom du capteur si la source est un capteur.
MAC	L'adresse MAC de l'asset.
Tags	Les tags que vous créez pour l'asset sur la page Groupes d'assets et tags .
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 .



Paramètre	Description
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



Paramètre	Description
	son type. Vous pouvez ajuster manuellement la valeur.
Niveau Purdue	Le niveau Purdue de l'asset (0=Processus physique, 1=Appareils intelligents, 2=Systemes de contrôle, 3=Systemes d'exploitation de fabrication, 4=Systemes 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	 Contrôleur



Catégorie	Niveau de criticité/Niveau Purdue par défaut	Description	Sous-types	
		l'état des appareils de sortie. Cette catégorie comprend tous les types de contrôleurs et leurs composants associés.		



Catégorie	Niveau de criticité/Niveau Purdue par défaut	Description	Sous-types	
				PLC



Catégorie	Niveau de criticité/Niveau Purdue par défaut	Description	Sous-types	
				DCS
				IED
				RTU
				Contrôleur BMS
				Robot
				Module de communication
				Module E/S
				CNC
				Alimentation
				Module de fond de panier



Catégorie	Niveau de criticité/Niveau Purdue par défaut	Description	Sous-types	
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



Catégorie	Niveau de criticité/Niveau Purdue par défaut	Description	Sous-types	
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		Serveur OT



Catégorie	Niveau de criticité/Niveau Purdue par défaut	Description	Sous-types	
		serveurs OT et leurs composants associés.		
				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



Catégorie	Niveau de criticité/Niveau Purdue par défaut	Description	Sous-types	
				Commutateur
				Pont Série-Ethernet
				Passerelle
				Hub
				Point d'accès sans fil
				Pare-feu
				Convertisseur
				Répétiteur



Catégorie	Niveau de criticité/Niveau Purdue par défaut	Description	Sous-types	
				
				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



Catégorie	Niveau de criticité/Niveau Purdue par défaut	Description	Sous-types	
Serveurs	Low / 3 (Faible / 3)	Cette catégorie comprend divers types de serveurs informatiques.		Serveur
				Serveur de fichiers
				Serveur web
				Serveur virtuel
				Appliance de sécurité
				TenableICP
				TenableEM



Catégorie	Niveau de criticité/Niveau Purdue par défaut	Description	Sous-types	
				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



Catégorie	Niveau de criticité/Niveau Purdue par défaut	Description	Sous-types
			 Imprimante 3D
			 Imprimante
			 UPS
			 Téléphone IP
			 Capteur intelligent
			 Lecteur de code-barres
			 Système de contrôle d'accès
			Contrôle



Catégorie	Niveau de criticité/Niveau Purdue par défaut	Description	Sous-types	
				d'éclairage



Catégorie	Niveau de criticité/Niveau Purdue par défaut	Description	Sous-types	
Terminaux	Low / 3 (Faible /	Une adresse IP non		Module HVAC
				SmartHub
				SmartTV
				Appareil médical
				Tablette
				Appareil mobile
				Périphérique de stockage
Terminaux	Low / 3 (Faible /	Une adresse IP non		Terminal



Catégorie	Niveau de criticité/Niveau Purdue par défaut	Description	Sous-types
	3)	identifiée sur le réseau.	

Afficher les détails d'un asset

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité, Analyste sécurité, Opérateur de site, Lecture seule

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.

Rouge
PLC

74 Actions Resync

IP MAC Vendor Model Last Seen State Family
Firmware 20.055 Rockwell 1756-L61/B LOGIX5561 Nov 27, 2024 06:52:31 AM Unknown ControlLogix 5560

Details

Code Revision

IP Trail

Attack Vectors

Open Ports

Vulnerabilities

Active (3)

Fixed (0)

Events

Network Map

Related Assets

Sources

Overview

NAME Rouge

PURDUE LEVEL Level 1

STATE Unknown

ADDITIONAL IPS

ADDITIONAL MACS

FAMILY ControlLogix 5560

VENDOR Rockwell

MODEL NAME 1756-L61/B LOGIX5561

LAST SEEN 06:52:31 AM · Nov 27, 2024

FIRST SEEN 09:53:34 AM · Oct 30, 2024

LAST UPDATE 06:51:44 AM · Nov 27, 2024

SOURCES nic1 (Local), nic0 (Local)

NETWORK SEGMENTS Controller / Controller /

CRITICALITY High

RISK SCORE 74

General

PLC NAME Rouge

SERIAL D7D63D

Backplane View

Backplane #4

0 1 2 3 4 5 6 7 8 9

Comm. Adapter #44 Comm. Adapter #48 Comm. Adapter #45 Yuval A10 Rouge Comm. Adapter #47 Comm. Adapter #43 Comm. Adapter #46

No card selected...



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.
- Assets associés - Affiche la liste de tous les assets imbriqués.
- Sources – Affiche toutes les informations liées à la source de l'asset, telles que l'emplacement, le type, les adresses IP et Mac de l'asset, ainsi que la première et la dernière date/heure de signalement.

Volet d'en-tête

Le volet d'en-tête affiche un aperçu de l'état actuel de l'asset.

Rouge

PLC

74

Actions

Resync

IP	MAC	Vendor	Model	Last Seen	State	Family
Firmware 20.055		Rockwell	1756-L61/B LOGIX5561	Nov 27, 2024 06:52:31 AM	Unknown	ControlLogix 5560

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.

Unresolved Events 3544	Vulnerabilities 3	Criticality High	74
---------------------------	----------------------	---------------------	----

- 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.



Section	Description
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.
Tags	Les tags associés à l'asset. Voir Groupes d'assets et tags .

Vue du fond de panier

Rouge

PLC

74

Actions

Resync

IP

MAC

Vendor

Model

Last Seen

State

Family

Firmware

20.055

Rockwell

1756-L61/B LOGIX5561

Nov 27, 2024 06:52:31 AM

Unknown

ControlLogix 5560

Details

Code Revision

IP Trail

Attack Vectors

Open Ports

Vulnerabilities

Active (3)

Fixed (0)

Events

Network Map

Related Assets

Sources

Overview

NAME

Rouge

PURDUE LEVEL

Level 1

STATE

Unknown

ADDITIONAL IPS

ADDITIONAL MACS

FAMILY

ControlLogix 5560

VENDOR

Rockwell

MODEL NAME

1756-L61/B LOGIX5561

LAST SEEN

06:52:31 AM · Nov 27, 2024

FIRST SEEN

09:53:34 AM · Oct 30, 2024

LAST UPDATE

06:51:44 AM · Nov 27, 2024

SOURCES

nic1 (Local),nic0 (Local)

NETWORK SEGMENTS

Controller / 10.100.101.X | Controller / 10.101.101.X

CRITICALITY

High

RISK SCORE

74

General

PLC NAME

Rouge

SERIAL

D7D63D

Backplane View

Backplane #4

0

1

2

3

4

5

6

7

8

9

Comm. Adapter #44

Comm. Adapter #48

Comm. Adapter #45

Yuvel

A10

Rouge

Comm. Adapter #47

Comm. Adapter #43

Comm. Adapter #46

No card selected...

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.

Informations sur le scan Nessus

Les informations sur le scan Nessus vous aident à :

- Identifier les assets évalués et non évalués.
- Comprendre si vos assets sont ciblés par des scans authentifiés ou non authentifiés.
- Suivre les meilleures pratiques en matière de scan et de gestion des vulnérabilités. Par exemple, vous pouvez effectuer des scans d'évaluation de vulnérabilités sur des assets de type informatique exécutant Windows ou Linux. Les scans, avec ou sans informations



d'authentification, permettent d'évaluer la part de la surface d'attaque de votre organisation qui est exposée à la fois en interne et en externe.

Pour plus d'informations sur les scans Nessus, voir [Créer des scans des plug-ins Nessus](#).

La section Informations sur le scan Nessus sur la page Détails fournit les informations suivantes :

- Dernier scan réussi
- Dernier scan authentifié
- Durée du dernier scan

The screenshot shows the Tenable OT Security interface. The sidebar on the left contains navigation options: Inventory (All Assets, Controllers and Modules, Network Assets, IoT, Network Map), Risks, Active Queries (Queries Management, Credentials), Network, Groups, Local Settings (Sensors, System Configuration, Environment Configur..., User Management), Integrations, and IoT Connectors.

The main content area displays the details of a Tenable ICP #25 scan. The top section shows the scan name and a table of assets. Below this, there is a table of vulnerabilities with columns for Details, IP Trail, Attack Vectors, Open Ports, Vulnerabilities (Active (73), Fixed (0)), Events, Network Map, Related Assets, and Sources.

The Nessus Scan Information section is highlighted with a red box and contains the following data:

Nessus Scan Information	
LAST SUCCESSFUL SCAN	04:19:24 PM · Jan 6, 2025
LAST SCAN DURATION	21 minutes (12:20:05 PM · Apr 21, 1984)



CEI 61850

La section « CEI 61850 » sur la page Détails affiche la configuration suivante pour l'asset IED spécifique.

- Fournisseur
- Modèle
- Révision

The screenshot displays the 'IED #3' details page. The left sidebar contains a navigation menu with the following items: Details, IP Trail, Attack Vectors, Open Ports, Vulnerabilities (expanded), Events, Network Map, Related Assets, IEC 61850, and Sources. The 'Details' tab is selected, showing a table of attributes for the IED. The table has columns for Name, Vendor, Last Seen, State, and Risk Score. The 'Vulnerabilities' section is expanded, showing a list of vulnerabilities with columns for Name, Vendor, Last Seen, First Seen, Last Update, Sources, Network Segments, Criticality, and Risk Score. The 'IEC 61850' section is highlighted with a red box, showing the following configuration:

Attribute	Value
NAME	IED #3
PURDUE LEVEL	Level 1
STATE	Unknown
DIRECT IP	
DIRECT MAC	
VENDOR	ABB
LAST SEEN	10:08:18 AM - Jan 27, 2025
FIRST SEEN	03:59:22 PM - Jan 20, 2025
LAST UPDATE	05:36:18 AM - Jan 27, 2025
SOURCES	nic1 (Local)
NETWORK SEGMENTS	Controller
CRITICALITY	High
RISK SCORE	15
IEC-61850	
VENDOR	ABB
MODEL	IEC61850 8-1 SVR
REVISION	ISS V5.30.00.24

Pour plus d'informations sur les fichiers SCD, voir les sections suivantes :

- Fichiers SCD
- CEI 61850

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.

74

Actions

Resync

Finished taking snapshot successfully

IP

MAC

Vendor

Model

Last Seen

State

Family

Firmware

Nov 11, 2024 06:53:52 AM

Unknown

ControlLogix 5560

20.055

Rockwell

1756-L61/B LOGIX5561

Details

Code Revision

IP Trail

Attack Vectors

Open Ports

Vulnerabilities

Active (3)

Fixed (0)

Events

Network Map

Version 1

Baseline

06:55:07 AM · Nov 11, 2024

Version 1

Search...

☐ Compare to

Previous Version

Set Version as Baseline

Take Snapshot

Name	Size	Compiled on
Rouge (39)		
Tags (9)		
(Unknown) 0:I	0	Nov 11, 2024 06:55:09 AM
(Unknown) 0:O	0	Nov 11, 2024 06:55:09 AM
(Unknown) 0:S	0	Nov 11, 2024 06:55:09 AM
(Unknown) 7:I	0	Nov 11, 2024 06:55:09 AM
(Bool) False_Ala	0	Nov 11, 2024 06:55:09 AM
(DInt) RougeTag	0	Nov 11, 2024 06:55:09 AM

Version {{ordinal}}

Snapshots List

User-Initiated Snapshot

06:55:07 AM · Nov 11, 2024

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).

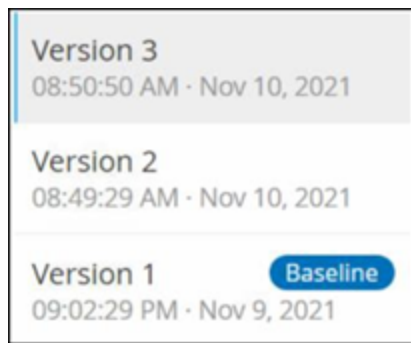


- Lancé par l'utilisateur - L'utilisateur peut déclencher manuellement un instantané en cliquant sur le bouton Prendre un instantané pour un asset spécifique.

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



Name	Size	Compiled on
[-] Rouge (30)		
[-] Tags (2)		
(Dir) RougeTag1	0	Nov 9, 2021 09:02:29 PM
(Bool) VAZTEXT1	0	Nov 9, 2021 09:02:29 PM
[-] Tasks (26)		
[-] MainTask (23)		
[-] Programs (22)		
[-] MainProgram (21)		
[-] Routines (2)		
(Ladder) Main_Routine	16	Nov 10, 2021 08:49:30 AM
(SFC) SFC1	432	Nov 9, 2021 09:02:29 PM
[-] Tags (17)		
(Bool) MyBit	0	Nov 10, 2021 08:49:30 AM
(VStep) Step_000	0	Nov 9, 2021 09:02:29 PM
(VStep) Step_001	0	Nov 9, 2021 09:02:29 PM
(Bool) Tran_000	0	Nov 9, 2021 09:02:29 PM
(Bool) Tran_001	0	Nov 9, 2021 09:02:29 PM
(Dir) ...SL7162	0	Nov 9, 2021 09:02:29 PM

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

Version 1 Snapshots List	
User Initiated Snapshot	08:02:10 AM · Nov 10, 2021
Routine Snapshot	09:02:29 PM · Nov 9, 2021

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.

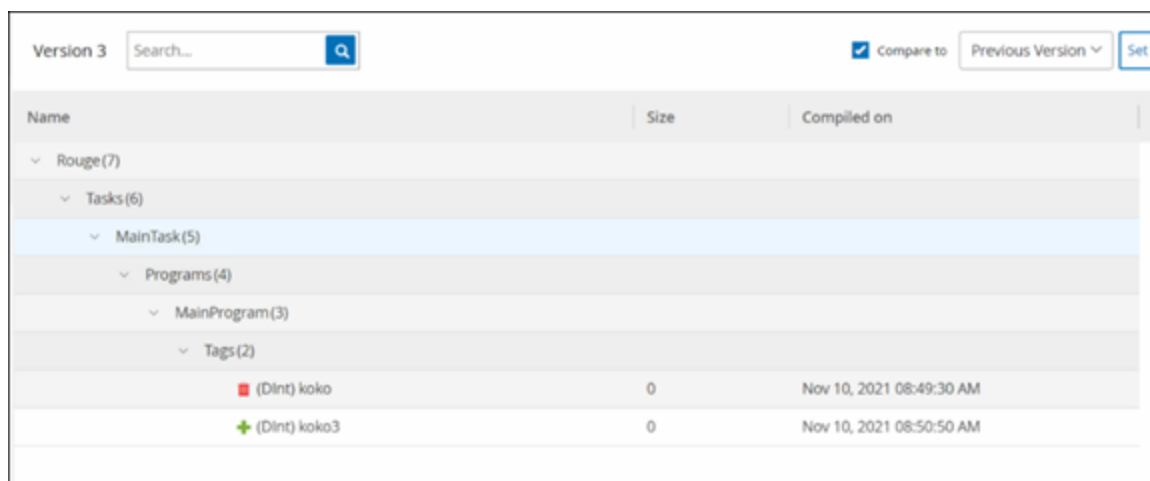
Pour comparer une version d'instantané à la version précédente :

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.
7. Dans le champ à côté de cette case, sélectionnez Version de référence dans le menu déroulant.

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

Vous pouvez lancer manuellement un instantané. Tenable recommande 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.

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.

Rouge PLC		74 Actions Resync				
IP	MAC	Vendor	Model	Last Seen	State	Family
20.055		Rockwell	1756-L61/B LOGIX5561	Nov 27, 2024 08:41:46 AM	Unknown	ControlLogix 5560
Details Code Revision IP Trail Attack Vectors Open Ports Vulnerabilities Active (3) Fixed (0) Events Network Map Related Assets Sources						
Search...						
IP	Start Date	End Date				
1756-EN2T/D Slot 1 (1)						
	Oct 30, 2024 09:53:07 AM	Active				
1756-EN2TR/C Slot 6 (1)						
	Oct 30, 2024 09:53:48 AM	Active				
1756-ENBT/A Slot 8 (1)						
	Oct 30, 2024 09:53:58 AM	Active				
1756-L81E/B Slot 3 (1)						
	Oct 30, 2024 09:53:07 AM	Active				

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

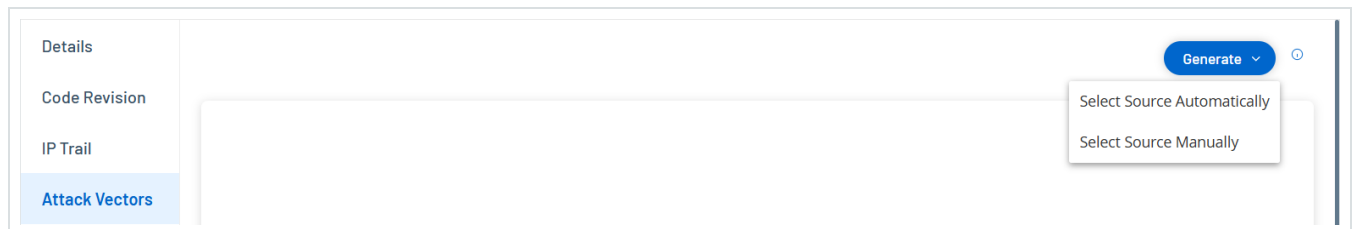
Les vecteurs d'attaque doivent être générés manuellement pour chaque asset cible pertinent. Cela se fait dans l'onglet Vecteurs d'attaque pour l'asset cible souhaité. Il existe deux méthodes pour générer des vecteurs d'attaque :



- 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



1757 Assets

Name	Risk Score	Type
Endpoint #1721	0	Endpoint
Endpoint #1526	0	Endpoint
Endpoint #875	0	Endpoint
Endpoint #286	0	Endpoint
Endpoint #258	0	Endpoint
Endpoint #1458	0	Endpoint
Endpoint #1711	0	Endpoint
Endpoint #95	0	Endpoint
Endpoint #1543	0	Endpoint
Endpoint #1204	0	Endpoint
Endpoint #910	0	Endpoint

Cancel

Generate



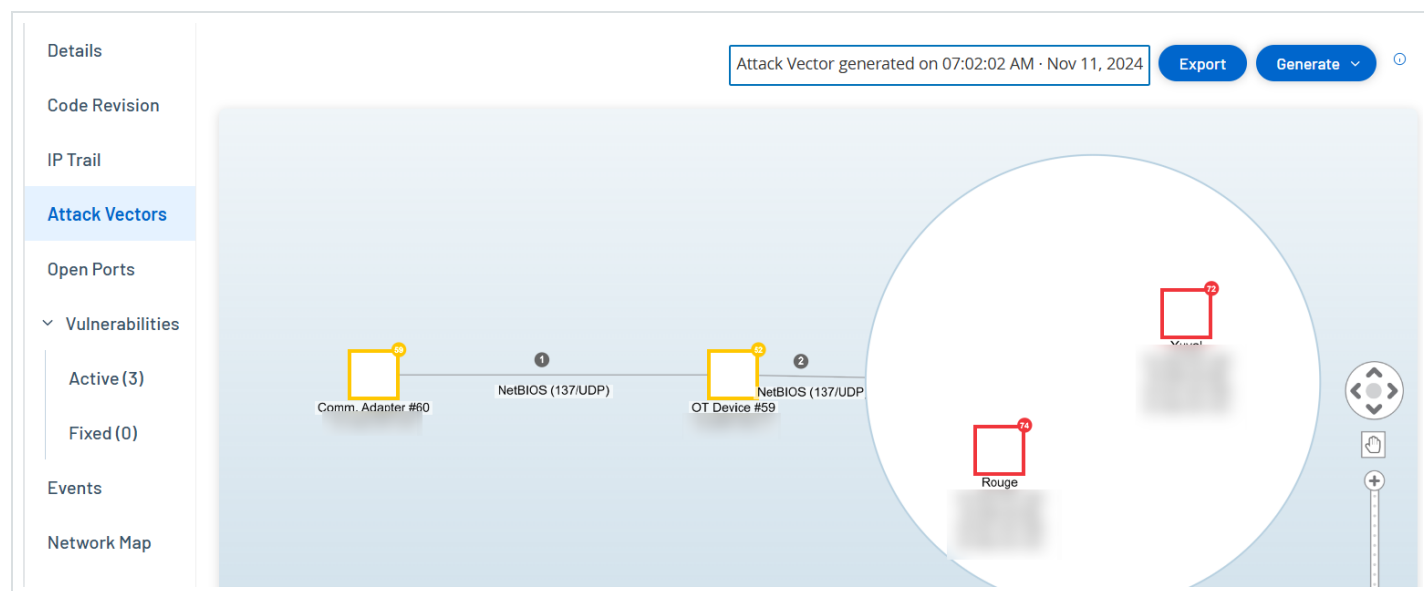
Remarque : par défaut, les assets sources sont triés par score de risque. Vous pouvez régler les paramètres d'affichage ou rechercher l'asset souhaité.

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.

The screenshot shows the Tenable Security Center interface. At the top, there's a header for the asset 'Rouge PLC' with a red status indicator (74) and buttons for 'Actions' and 'Resync'. Below the header, there's a table with columns: IP, MAC, Vendor, Model, Last Seen, State, and Family. The first row shows 'Hrmware 20.055', 'Rockwell', '1756-L61/B LOGIX5561', 'Nov 27, 2024 08:46:41 AM', 'Unknown', and 'ControlLogix 5560'.

On the left sidebar, there's a menu with options: Details, Code Revision, IP Trail, Attack Vectors, Open Ports, Vulnerabilities (Active (3), Fixed (0)), Events, Network Map, Related Assets, and Sources. The 'Open Ports' option is selected.

The main content area shows a search bar and a button 'Update Open Ports'. Below that, there's a message: 'Port mapping is turned off' with a 'Configure Queries' link. The main table displays a list of open ports for the asset. The table has columns: Port, Protocol, Source, Description, and Last update. The data is grouped by IP address, with expandable sections for each IP.

Port	Protocol	Source	Description	Last update
1756-L81E/B Slot 3 (2)				
80	HTTP (80/TCP)	Conversations	Hypertext Transfer Protocol	Nov 27, 2024 08:42:58 AM
44818	Ethernet/IP (44818/TCP)	Conversations	Ethernet/IP	Nov 27, 2024 08:46:23 AM
1756-EN2T/D Slot 1 (2)				
80	HTTP (80/TCP)	Conversations	Hypertext Transfer Protocol	Nov 27, 2024 08:42:58 AM
44818	Ethernet/IP (44818/TCP)	Conversations	Ethernet/IP	Nov 27, 2024 08:46:46 AM
1756-ENBT/A Slot 8 (2)				
80	HTTP (80/TCP)	Conversations	Hypertext Transfer Protocol	Nov 16, 2024 04:13:17 PM
44818	Ethernet/IP (44818/TCP)	Conversations	Ethernet/IP	Nov 16, 2024 04:17:50 PM
1756-EN2TR/C Slot 6 (1)				
44818	Ethernet/IP (44818/TCP)	Conversations	Ethernet/IP	Nov 27, 2024 08:43:37 AM

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.

Mettre à jour les ports ouverts

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité, Analyste sécurité, Opérateur de site

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.

Exécuter un scan

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.

Afficher le portail de l'asset

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 Risques > Vulnérabilités, mais seules les vulnérabilités pertinentes pour l'asset spécifié sont affichées. Pour une explication des informations sur les vulnérabilités, voir [Vulnérabilités](#).

The screenshot shows the Tenable Nessus interface for an asset named 'Rouge PLC'. The 'Vulnerabilities' tab is selected, showing a list of active vulnerabilities. The table has columns for Name, Severity, VPR, Plugin family, Plugin ID, Source, Owner, and Comment. Two vulnerabilities are listed, both with a severity of 'Critical'.

Name	Severity	VPR	Plugin family	Plugin ID	Source	Owner	Comment
Rockwell Automation Logix5000 Programmable Automation Controller Buffer Overflow (CVE-2016-9343)	Critical	6.5	Tenable.ot	500092	Tot		
Rockwell Automation Logix5000 Programmable Automation Controller Buffer Overflow (CVE-2016-9343)	Critical	5.9	Tenable.ot	500451	Tot		

Items: 3

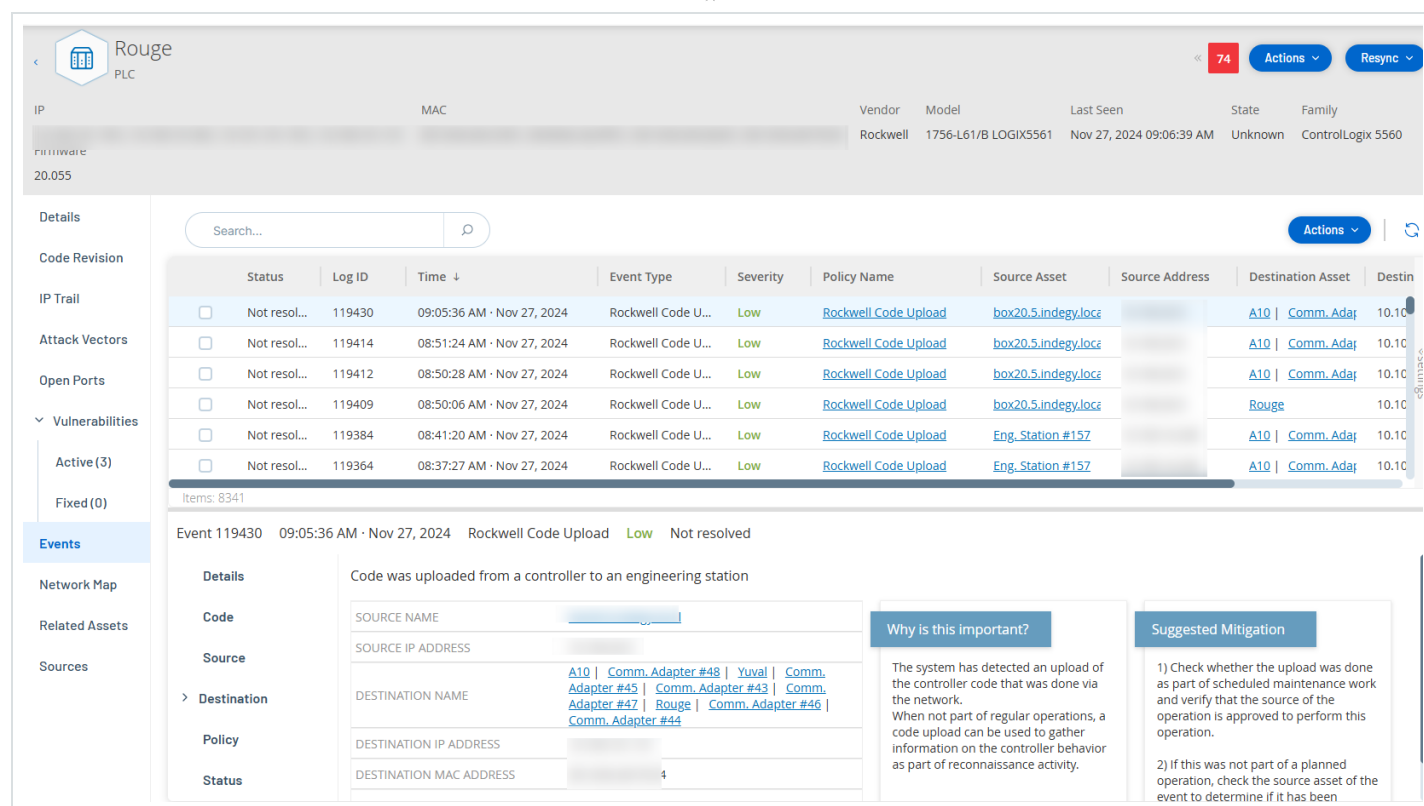
Plugin Output

Port: 0 / tcp Source: Tot Last Hit date: 11:20:26 AM · Nov 25, 2024

Vendor : Rockwell
Family : ControlLogix 5560
Model : 1756-L61/B LOGIX5561
Version : 20.055

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](#).



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.



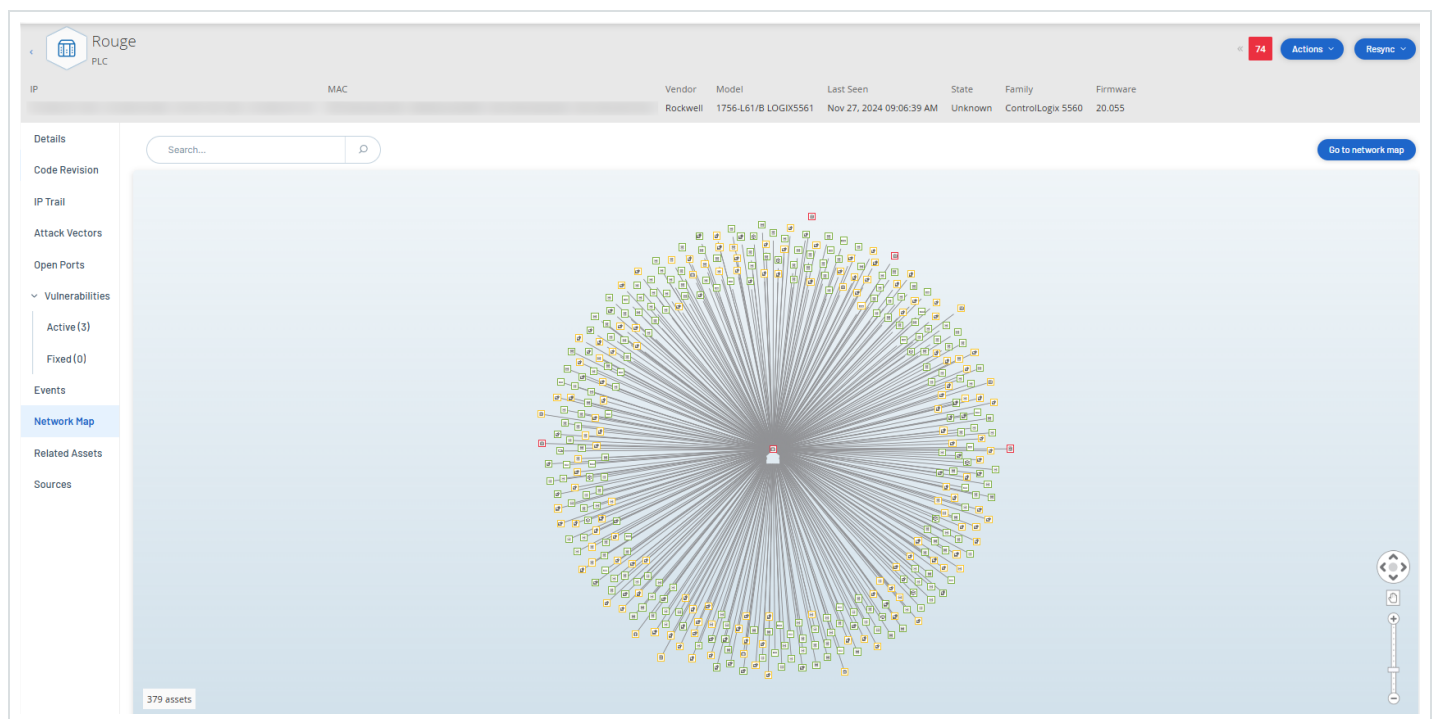
Paramètre	Description
Asset cible	Le nom de l'asset qui a été affecté par l'événement. Ce champ est un lien vers les listes d'assets.
Adresse cible	L'adresse IP ou MAC de l'asset qui a été affecté par l'événement.
Protocole	Lorsque c'est pertinent, montre le protocole utilisé pour la communication qui 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.



Paramètre	Description
	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.

Assets associés

La page Assets associés d'un asset affiche la liste de tous ses assets imbriqués.

Pour accéder à la page Assets associés :

1. Dans le tableau Inventaire > Tous les assets, cliquez sur un asset pour ouvrir la page de ses détails.
2. Dans le volet de navigation de gauche, cliquez sur Assets associés.

La page Assets associés apparaît.

La page Assets associés présente les détails suivants :

Colonne	Description
Asset partenaire	Le nom de l'asset associé.
Type de relation	Le type de relation avec l'asset associé : imbrication.
Direction d'accès	La direction de l'accès entre l'asset et son partenaire.
Détails	Les détails du type d'asset. Par exemple : ControlNet ou IP.
Première détection	La date à laquelle OT Security a découvert cet asset pour la première fois.
Dernière détection	La date à laquelle OT Security a détecté cet asset pour la dernière fois.

Détails de l'asset imbriqué



Les appareils imbriqués sont des contrôleurs logiques programmables (PLC) ou des modules de système de contrôle industriel (ICS) connectés derrière un fond de panier ou un appareil de PLC. On peut les comparer à un variateur de fréquence connecté directement à un adaptateur de communications. Pour afficher les détails d'un asset imbriqué, cliquez sur le lien de l'asset imbriqué sur la page Assets associés. OT Security signale les appareils imbriqués à l'aide de l'icône

Comm. Adapter #89
Communication Module

38 Actions Resync

IP	MAC	Vendor	Model	Last Seen	State	Family	Firmware
		Rockwell	1756-CNB/E 11.004	Nov 11, 2024 07:19:08 AM	Unknown	ControlLogix	11.004

Details

IP Trail

Attack Vectors

Open Ports

Vulnerabilities

Active (0)

Fixed (0)

Events

Network Map

Related Assets

Sources

Overview

NAME	Comm. Adapter #89
PURDUE LEVEL	Level 1
STATE	Unknown
ADDITIONAL IP	
ADDITIONAL MAC	
FAMILY	ControlLogix
VENDOR	Rockwell
MODEL NAME	1756-CNB/E 11.004
LAST SEEN	07:19:08 AM · Nov 11, 2024
FIRST SEEN	09:54:34 AM · Oct 30, 2024
LAST UPDATE	06:38:10 AM · Nov 11, 2024
SOURCES	nic1 (Local)
NETWORK SEGMENTS	Controller /

Backplane View

Backplane #187

0

1

2

3

Comm. Adapt...

Yuval_L71_A4

Sith

Comm. Adapt...

Communication Module Details

Nested Devices (9)

Communication Module Details

NAME	Comm. Adapter #89
RISK SCORE	38
TYPE	Communication Module

La page des détails de l'asset imbriqué présente les détails suivants :

Section	Description
Vue d'ensemble	Inclut des détails de l'asset tels que son nom, son niveau Purdue, son état et son adresse IP supplémentaire.
Général	Contient des détails tels que le numéro de série, la version du firmware, le type d'appareil, le numéro de fond de panier et le numéro d'emplacement.



Vue du fond de panier	Inclut une vue graphique du fond de panier. Cliquez sur le nom de l'appareil dans la vue du fond de panier pour afficher les onglets Détails du module de communication et Appareils imbriqués.
-----------------------	---

CEI 61850

En fonction du fichier SCD (Substation Configuration Description) que vous chargez, OT Security génère la liste des rapports MMS (Manufacturing Message Specification) qui décrivent la communication entre les assets de la sous-station. OT Security affiche un message d'erreur lorsqu'il détecte un accès non autorisé dans la configuration du fichier SCD. Pour plus d'informations sur le chargement de fichiers SCD, voir [Fichiers SCD](#).

Pour accéder à la page « CEI 61850 » :

1. Accédez à Inventaire > Tous les assets.

La page Tous les assets apparaît.

2. Recherchez et sélectionnez l'asset ou la sous-station dont vous souhaitez afficher la configuration CEI 61850.

La page des détails de l'asset apparaît.

3. Dans la barre de navigation de gauche, sélectionnez CEI 61850.



La page CEI 61850 apparaît avec les détails suivants.

EN100_E+ IED_Indegy
IED

39 Actions Resync

IP	MAC	Vendor	Last Seen	State
		SIEMENS PTD PA	Jan 27, 2025 09:44:33 AM	Unknown

Details

Code Revision

IP Trail

Attack Vectors

Open Ports

Vulnerabilities

Active (13)

Fixed (0)

Events

Network Map

Related Assets

IEC 61850

Sources

106 MMS reports have no clients assigned, exposing unauthorized access. Assign authorized clients or remove redundant configurations from the SCD file. [Download Details](#)

+ Add Filter

Search...

108 MMS Reports Group By

Report ID	Report Name	Dataset Name	Client Name	Substation	Project
IED_Indegy2PROT/LLN0\$RP\$urcbZ01	urcbA	TEST	HMLM	Substation	Station Indegy
IED_Indegy2PROT/LLN0\$RP\$urcbC01	urcbC	TEST	Client	Substation	Station Indegy
IED_Indegy2MEAS/LLN0\$RP\$urcbJ01	urcbJ		Not defined	Substation	Station Indegy
IED_Indegy2PROT/PDIF2\$RP\$urcbB01	urcbB		Not defined	Substation	Station Indegy
IED_Indegy2CTRL/LLN0\$RP\$urcbB01	urcbB		Not defined	Substation	Station Indegy
IED_Indegy2CTRL/LLN0\$RP\$urcbA01	urcbA		Not defined	Substation	Station Indegy
IED_Indegy2MEAS/M3_MSQI\$RP\$urcbB01	urcbB		Not defined	Substation	Station Indegy
IED_Indegy2CTRL/QOCSWI\$RP\$urcbB01	urcbB		Not defined	Substation	Station Indegy

Colonne	Description
ID du rapport	L'ID du rapport MMS servant d'identifiant unique pour le rapport.
Nom du rapport	L'ID du rapport MMS servant d'identifiant unique pour le rapport.
Nom du jeu de données	Le nom du jeu de données lié au rapport MMS définissant le groupe de points de données inclus dans le rapport.
Nom du client	Le nom de l'application cliente ou du système qui s'abonne au rapport et le reçoit.
Sous-station	La sous-station où se trouve l'IED (appareil électronique intelligent) générant le rapport MMS.
Projet	Le projet CEI 61850 global ou la configuration système à laquelle le



rapport et les composants associés appartiennent.

4. Pour afficher les détails des détections détectées par OT Security : dans le message d'erreur en haut de la page, cliquez sur Télécharger les détails.

OT Security télécharge les détails au format CSV.

Remarque : le nombre de rapports MMS dans le message d'erreur s'applique à l'asset spécifique, tandis que le fichier CSV téléchargé contient des détails sur tous les assets.



90 MMS reports have no clients assigned, exposing unauthorized access. Assign authorized clients or remove redundant configurations from the SCD file.

[Download Details](#)

Sources

La page Sources d'un asset fournit toutes les informations liées à la source de l'asset, telles que l'emplacement, le type, ainsi que la première et la dernière date/heure de signalement. Vous pouvez également afficher la source de l'asset dans la colonne Sources sur la page Inventaire > Tous les assets.

Pour accéder à la page Sources :

1. Dans le tableau Inventaire > Tous les assets, cliquez sur un asset pour ouvrir la page de ses détails.

La page des détails de l'asset apparaît.

2. Dans le volet de navigation de gauche, cliquez sur Sources.



La page Sources apparaît.

The screenshot shows the 'Sources' page for a device named 'Rouge PLC'. The page displays a table of sources with columns: Name, Type, Reported IPs, Reported MACs, Last Reported, and First Reported. Two sources are listed: 'nic1' and 'nic0', both of type 'Local'. The left sidebar shows navigation options like Details, Code Revision, IP Trail, Attack Vectors, Open Ports, Vulnerabilities, Events, Network Map, Related Assets, and Sources (selected). The top right shows a red status indicator with '74' and buttons for 'Actions' and 'Resync'.

La page Sources apparaît avec les détails suivants :

Colonne	Description
Nom	Nom de la source, par exemple nic 1 ou nic 2 pour une source locale, ou le nom du capteur si la source est un capteur.
Type	Type de source : ICP locale ou capteur.
IP signalées	Adresses IP provenant de l'asset source.
MAC signalées	Adresses MAC provenant de l'asset source. OT Security signale une adresse MAC si le capteur est suffisamment proche pour observer l'asset. Si le capteur est loin de l'asset, mais observe une communication entre eux, OT Security signale uniquement les adresses IP observées.
Dernier signalement	Date/heure à laquelle l'asset source a été signalé pour la dernière fois.



Premier signalement	Date/heure à laquelle l'asset source a été signalé pour la première fois.
---------------------	---

Modifier les détails de l'asset

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Opérateur de site

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.
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.



Controllers and Modules

+ Add Filter

Search...

114 Assets Grouped By: Backplane Expand All Collapse All 1 Selected Actions [→] [□]

Name	Type	Risk Score	Criticality	IP	Vendor
Backplane #101					
☒ 140-NOE-771-01 Module	Communication Module	57	High	10.100.105.27 (Direct)	Schneider
☐ PLC #44	PLC	45	High	10.100.105.27	Schneider
Backplane #103					
Backplane #104					
Backplane #106					
Backplane #112					
Backplane #115					
Backplane #137					

Un fichier CSV de l'inventaire est téléchargé.

3. Accédez au fichier qui vient d'être téléchargé et ouvrez-le.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	ID	Slot	Name	Type	Risk	Criticality	Addresses	Vendor	Family	Model	Firmware	State	Purdue	Last Seen	Location	Backplane	Description		
2	Q1N2XQ6A1TA2MDE		DESKTOP-PLC		47	High	Critici 33.180.38	Beckhoff	C-Series		2.11.2305	Unknown	Level1	*****					
3	Q1N2XQ6A1TU5WV		SIMATIC H-PLC		32	High	Critici 33.180.38	Siemens	S7-400	CPU 412-5	6.0.6	Fault	Level1	*****			Siemens, SIMATIC S7		
4	Q1N2XQ6A1UHTN		C Yairdeg	Communic	20	High	Critici 33.180.38	Helmholtz	Netlink	NETLink PI	2.7	Unknown	Level1	*****			700-884-MPI21		
5	Q1N2XQ6A1U3Y4		J4aaa	Controller	20	High	Critici 33.180.38	Texas Instruments				Unknown	Level1	*****					
6	Q1N2XQ6A1U3Y4		J4aaa	Controller	20	High	Critici 33.180.38	Texas Instruments				Unknown	Level1	*****					
7	Q1N2XQ6A1U3Y4		J4aaa	Controller	20	High	Critici 33.180.38	Texas Instruments				Unknown	Level1	*****					
8	Q1N2XQ6A1U3Y4		J4aaa	Controller	20	High	Critici 33.180.38	Texas Instruments				Unknown	Level1	*****					
9	Q1N2XQ6A1U3Y4		J4aaa	Controller	20	High	Critici 33.180.38	Texas Instruments				Unknown	Level1	*****					
10	Q1N2XQ6A1U3Y4		J4aaa	Controller	20	High	Critici 33.180.38	Texas Instruments				Unknown	Level1	*****					
11	Q1N2XQ6A1U3Y4		J4aaa	Controller	20	High	Critici 33.180.38	Texas Instruments				Unknown	Level1	*****					
12	Q1N2XQ6A1U3Y4		J4aaa	Controller	20	High	Critici 33.180.38	Texas Instruments				Unknown	Level1	*****					

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 locaux, accédez à Paramètres de l'environnement > Définitions de réseau.

La page Définition de réseau apparaît.

The screenshot shows the 'Network Definitions' page. At the top, there's a header 'Network Definitions' with a sub-header 'Monitored Network' and an 'Edit' button. Below this, a text block explains that the Assets Network is an aggregation of IP ranges. A table lists 'DEFAULT IP RANGES' with three entries: '192.168.0.0/16', '172.16.0.0/12', and '169.254.0.0/...'. A 'Show More' link is present. Below the table is a section for 'ADDITIONAL IP RANGES'. Further down, there's a 'Passive Monitoring' section with a toggle switch and a description. At the bottom, a blue information icon is followed by a list of steps to follow before enabling passive monitoring.

Network Definitions

Monitored Network [Edit](#)

The Assets Network is an aggregation of IP ranges in which assets are located. Use these settings in order to configure these IP ranges. Please note that in addition to these settings, any host within Tenable OT Security sensors' subnets or any activity-performing device will be classified as an asset.

DEFAULT IP RANGES	192.168.0.0/16 172.16.0.0/12 169.254.0.0/... Show More
ADDITIONAL IP RANGES	

☒ **Passive Monitoring**

Passive Monitoring captures network traffic to fingerprint assets and detect activities or threats on the network.

Before enabling Passive Monitoring, it's recommended to follow these steps:

1. Set Monitored Network (Above this section)
2. Enable Active Queries and run Initial asset enrichment queries
3. Tune your Policies

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 > **Paramètres** 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 > de l'environnement Paramètres > Assets masqués.



6. Cliquez sur Masquer.

OT Security masque les assets sur les pages Inventaire et Groupes.

Exporter les diagnostics

Vous pouvez exporter et télécharger le rapport de diagnostic d'un asset ou d'un groupe d'assets qui présente des faux positifs ou un autre type de problème. Vous pouvez partager ce rapport avec l'Assistance Tenable pour une analyse détaillée. Selon vos besoins, vous pouvez extraire des diagnostics directement de l'inventaire des assets ou passer par l'interface de gestion Tenable Core.

Exporter un rapport de diagnostic d'asset

Pour exporter le rapport de diagnostic :

1. Dans la barre de navigation de gauche, accédez à Inventaire > Tous les assets.

La page Tous les assets apparaît.

2. Dans le tableau Tous les assets, sélectionnez un ou plusieurs assets à exporter dans le rapport de diagnostic.

3. Effectuez l'une des actions suivantes :

- Pour un seul asset : dans le coin supérieur droit, cliquez sur Actions > Exporter les diagnostics.
- Pour plusieurs assets : dans le coin supérieur droit, cliquez sur Actions en bloc > Exporter les diagnostics.



OT Security télécharge le rapport de diagnostic pour le ou les assets sélectionnés. Le rapport de diagnostic est un fichier tar.gz et les détails de l'asset sont inclus dans un fichier .json.

Le nom du rapport de diagnostic inclut le nom de l'asset, l'horodatage et la version de OT Security. Exemples :

Pour un seul asset : TOTS_Rouge_3.19.15_2024-06-03T07_05_27.tar.gz

Pour plusieurs assets : TOTS_AssetsReport_3.19.15_2024-06-03T07_17_54.tar.gz

4. Extrayez le rapport de diagnostic et envoyez-le à l'Assistance Tenable pour une analyse plus approfondie.

Exporter le rapport de diagnostic Tenable OT Security (Tenable Core)

Vous pouvez générer et exporter un rapport de diagnostic spécifique à Tenable OT Security à partir de Tenable Core à des fins de dépannage.

Avant de commencer

- Assurez-vous de disposer d'un accès administrateur.

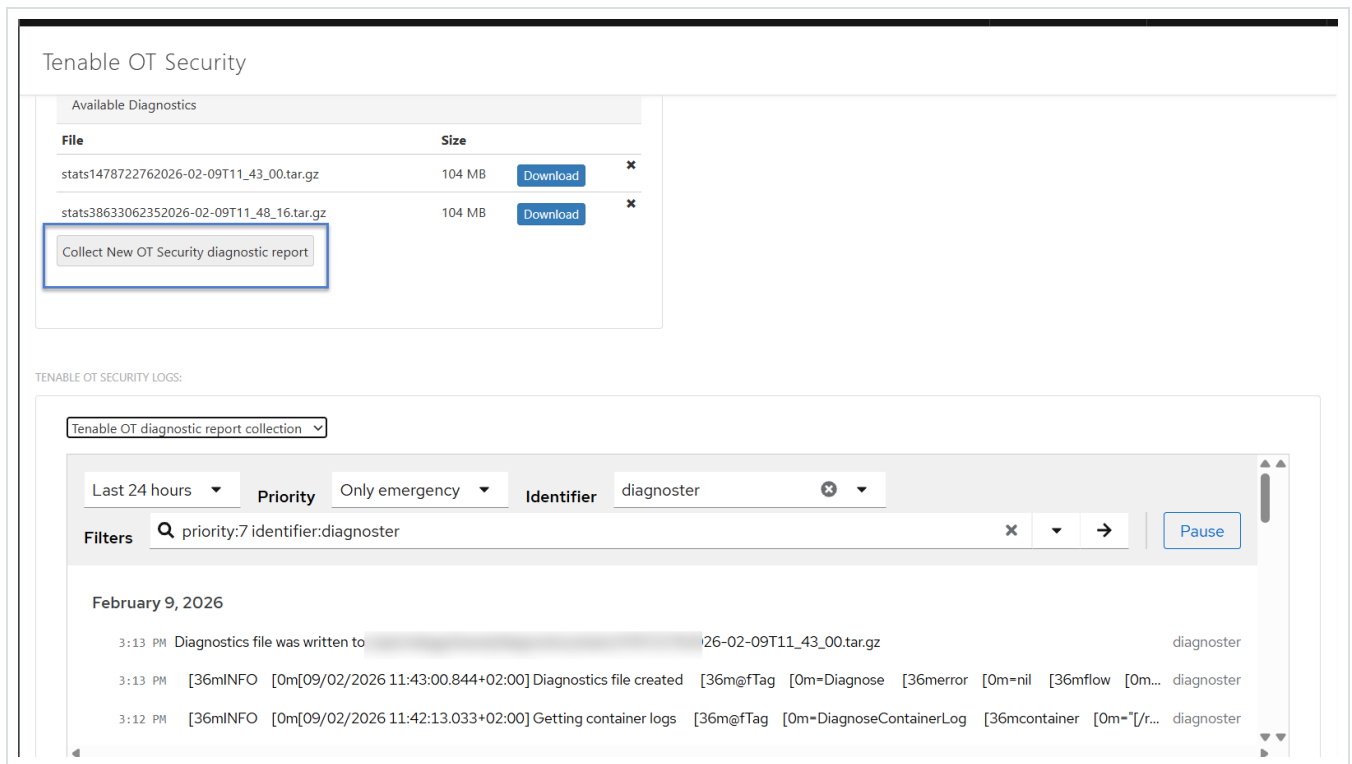
Pour générer le rapport de diagnostic :

1. Connectez-vous à Tenable Core.
2. Dans la barre de navigation de gauche, cliquez sur **Tenable OT Security**.

La page **Tenable OT Security** apparaît.

3. Dans la section OT Diagnostics (Diagnostic OT), cliquez sur Collect New OT Security Diagnostic Report (Collecter le nouveau rapport de diagnostic OT Security).

Le système génère le rapport de diagnostic.



4. Cliquez sur Download (Télécharger) devant le rapport que vous souhaitez télécharger.

Tenable Core télécharge le rapport sur votre système. Une fois que Tenable Core génère les journaux, il faut parfois compter plusieurs minutes avant que les données n'apparaissent dans les journaux de débogage.

Fusionner des assets

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Opérateur de site

Les appareils de votre réseau peuvent apparaître comme deux assets distincts ou plus dans OT Security en raison de l'observation passive du trafic, des configurations de routage ou d'informations insuffisantes sur les détails de l'asset qui empêchent la fusion automatique des assets en interne.

Par exemple, les appareils en multi-homing tels que les stations de travail, les serveurs ou les contrôleurs disposent généralement de plusieurs adresses IP qui leur permettent de communiquer



sur divers réseaux. Pensez également aux interfaces réseau virtuelles sur un commutateur, un routeur ou un pare-feu. Même s'il s'agit d'extensions virtuelles d'un seul appareil réseau physique, chacun d'entre elles peut être enregistrée en tant qu'asset distinct.

Dans ce cas, vous pouvez utiliser l'option Fusion d'assets pour fusionner deux assets et supprimer les doublons. Vous pouvez accéder à cette option soit à partir de la page Inventaire, soit à partir de la page des détails de l'asset.

Attention : cette action est irréversible.

Pour fusionner des assets :

1. Dans le menu de navigation de gauche, accédez à Inventaire > Tous les assets.

La page Tous les assets apparaît.

2. Dans le tableau « Tous les assets », effectuez l'une des opérations suivantes :

- Sélectionnez l'asset cible à fusionner.
- Cliquez sur le lien de l'asset pour ouvrir la page des détails de l'asset.

OT Security active Actions.

3. Cliquez sur Actions > Fusionner avec un autre.

Inventory

All Assets

Controllers & Modules

Network Assets

IoT Assets

Search...

+ Add Filter

880 Assets

Actions

Group By

	Name	Type	Risk Score	Criticality	IP	Subnets
☐	testigy	PLC	62	High		
☐	PLC #29	PLC	60	High		
☐	RTU #1	RTU	59	High		
☐	CPU 412	PLC	59	High		

testigy

PLC

62

Actions

Resync

IP	MAC	Vendor	Model	Last Seen	State	Family	Firmware
		Schneider	BMX P34 2020	Aug 28, 2025 09:28:24 AM	Unknown	Modicon M340	3.51

Details

Code Revision

IP Trail

Attack Vectors

Open Ports

Vulnerabilities

Events

Network Map

Related Assets

Overview

NAME

DESCRIPTION

PURDUE LEVEL

STATE

ADDITIONAL IP

ADDITIONAL MAC

FAMILY

VENDOR

MODEL NAME

LAST SEEN

FIRST SEEN

Backplane View

Backplane #7

0

1

2

testigy

Comm. Adapte...

I/O #1

BMX NOC0401

No card selected...

Le panneau Fusionner l'asset | Sélectionner l'asset apparaît.

Merge Asset | Select Source Asset



Target Asset: OT Server #11



Note: the source asset that is selected here will be deleted from the inventory, after its attributes and findings are merged into the target asset **OT Server #11**. Any case of conflict will be resolved by the system to keep the merged asset's data as full, accurate, and up to date as possible, based on the data of both assets. **This action is irreversible.**

[Read more about asset merging in our user guide](#)

☐ Force merge even if attributes conflict

Search...



+ Add Filter

199 Assets

Group By



Name	Type	Risk Score
OT Device #25	OT Device	0
Endpoint #135	Endpoint	0
Endpoint #111	Endpoint	0
Endpoint #112	Endpoint	0
Endpoint #123	Endpoint	0

Cancel

Merge and Delete

4. Filtrez ou recherchez l'asset source.



5. Sélectionnez l'asset source à fusionner avec l'asset cible.
6. (Facultatif) Cochez la case Forcer la fusion même en cas de conflit d'attributs pour contourner les conflits.
7. Cliquez sur Fusionner et supprimer.

OT Security supprime l'asset source et fusionne ses attributs et détections avec l'asset cible.

Processus de fusion d'assets

Le processus de fusion d'assets combine deux assets en une seule entité tout en maintenant l'intégrité des données dans le système.

Cette opération implique les étapes clés suivantes :

- Consolidation des propriétés des assets : lorsque les assets sont fusionnés, leurs propriétés sont fusionnées dans l'asset cible. Si les deux assets ont une valeur différente pour la même propriété, le système utilise un mécanisme de priorité pour choisir la valeur à conserver. Grâce à ce processus, l'asset fusionné conserve les informations les plus précises ou les plus récentes.
- Préservation des connexions : les connexions réseau pointant auparavant vers l'un ou l'autre des assets renvoient désormais à l'asset fusionné. Cela inclut :
 - Connexions directes à d'autres appareils
 - Connexions basées sur les emplacements au sein des fonds de panier
 - Mappages d'interfaces réseau, y compris les adresses IP et MAC. Le système s'assure que toutes les informations d'adresse historiques sont conservées et les entrées dupliquées sont supprimées.
- Consolidation des détections : le système regroupe l'ensemble des détections, vulnérabilités



et événements de sécurité sous le nouveau asset, préservant ainsi son historique de sécurité complet.

Conflits de fusion et fusion forcée

Les assets suivants ne peuvent pas être fusionnés :

- Assets spéciaux tels que l'ICP, le capteur ou les assets de diffusion.
- Assets de différents fonds de panier (un seul d'entre eux est autorisé à avoir un fond de panier).
- Assets ayant des emplacements différents (si les deux assets ont des emplacements, il doit s'agir du même emplacement).
- Assets ayant des numéros de série différents.

Forcer la fusion : l'option Forcer la fusion permet de contourner les vérifications du système concernant les conflits liés au fond de panier, à l'emplacement et au numéro de série. Bien que cette option ne garantisse pas la réussite de la fusion et que le moteur de fusion puisse toujours bloquer les opérations non valides, le système exécute la fusion avant qu'elle ne puisse être bloquée.

Comment corriger une fusion accidentelle

Si une fusion d'assets a été effectuée par erreur ou que vous devez rétablir les deux assets dans leur état non fusionné, supprimez l'asset que vous souhaitez fusionner. Le système pourra ainsi redécouvrir l'asset tel qu'il était avant la fusion. Pour plus d'informations sur la suppression d'un asset ou d'un groupe d'assets de OT Security, voir cet [article de la base de connaissances](#).

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

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité, Analyste sécurité, Opérateur de site

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.

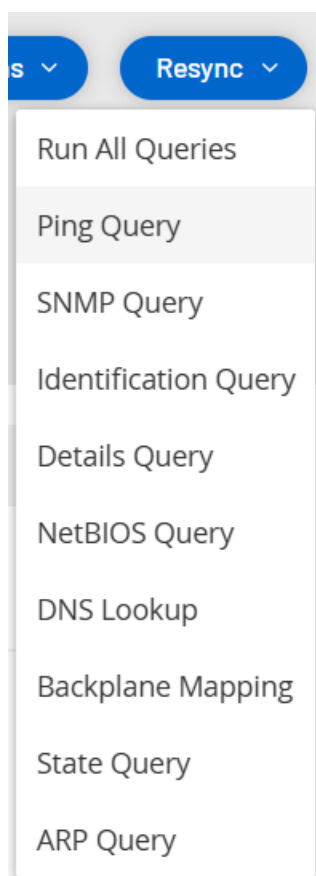
Le bouton Resynchroniser peut être désactivé dans des conditions spécifiques. Les raisons possibles incluent :

- L'appareil est inaccessible ou ne dispose pas de requêtes disponibles.
- L'autorisation configurée sur la page Requetes 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 Requetes 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.

✓	Ping Query completed successfully	×
×	The query failed due to a network error. This may be due to temporary network issues or firewall restrictions. Please check your network connectivity and retry the query. Protocol: NBNS; Operation: NtstatQueryType; Ip: [redacted]	×
	State	Family
✓	SNMP Query completed successfully	×
✓	DNS Lookup completed successfully	×
ION	Rockwell Automation 1756-L81E/B	
✓	State Query completed successfully	×
	Stopped	
✓	Details Query completed successfully	×

Pour chaque requête terminée, les données système de cet asset sont mises à jour par OT Security en fonction des nouvelles données.

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 et ports ouverts vulnérables).

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 [Paramètres de l'environnement](#).

Afficher les vulnérabilités

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité, Analyste sécurité, Opérateur de site, Lecture seule

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](#).

(Pour la version 3.19 uniquement) Les options Vulnérabilités actives et Vulnérabilités corrigées disponibles dans la barre de navigation de gauche vous permettent d'afficher respectivement les vulnérabilités ouvertes et corrigées.

Remarque : OT Security conserve les vulnérabilités corrigées pendant un an avant qu'elles n'expirent.

tenable OT Security

06:22 AM

Monday, Nov 11, 2024

Overview

Events

Policies

Inventory

Network Map

Risks

Vulnerabilities

Findings

Compliance

Active Queries

Network

Groups

Local Settings

Vulnerabilities

Search...

Plugin set 202410280920

Actions

Update plugins

License outdated—Nessus plugin set cloud updates are not available. [Update license](#)

Name	Severity ↓	VPR	Active Ass...	Fixed Asse...	Plugin family	Plugin ID	Sou
Schneider Electric Modicon Improper Au...	Critical	6.7	1	0	Tenable.ot	500033	Tot
Schneider Electric Modicon Quantum Im...	Critical	5.2	1	0	Tenable.ot	500069	Tot
Schneider Electric Modicon Missing Auth...	Critical	6.7	1	0	Tenable.ot	500071	Tot
Rockwell Micrologix Privilege escalation ...	Critical	5.2	2	0	Tenable.ot	500076	Tot
Rockwell Automation Allen-Bradley Micr...	Critical	5.9	1	0	Tenable.ot	500084	Tot
Rockwell Automation Logix5000 Progra...	Critical	6.5	2	0	Tenable.ot	500092	Tot
Rockwell Automation Allen-Bradley Micr...	Critical	5.9	1	0	Tenable.ot	500110	Tot
Schneider Electric Modicon Authenticati...	Critical	6.7	1	0	Tenable.ot	500122	Tot
Schneider Electric Modicon Exposure of ...	Critical	6.7	1	0	Tenable.ot	500125	Tot
Rockwell MicroLogix Improper Restrictio...	Critical	5.9	1	0	Tenable.ot	500134	Tot
Rockwell MicroLogix Improper Restrictio...	Critical	5.9	1	0	Tenable.ot	500167	Tot
Schneider Electric Modicon Weak Passw...	Critical	6.7	3	0	Tenable.ot	500170	Tot
Rockwell Automation CompactLogix 537...	Critical	5.9	3	0	Tenable.ot	500201	Tot

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 actifs	Nombre d'assets de votre réseau actuellement affectés par cette vulnérabilité.
Assets corrigés	Nombre d'assets de votre réseau affectés par cette vulnérabilité et corrigés récemment, sur une période définie (par défaut, un an). Contactez Assistance Tenable pour personnaliser cette période.
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



Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité, Analyste sécurité

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.

Afficher une sortie de plug-in à partir de la page Vulnérabilités

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.

Afficher une sortie de plug-in à partir de la page Inventaire

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



<

MS10-031: Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution (978213)

Actions

Vulnerability

Severity: Critical, VPR: 8.9, Affected Assets: 1, Plugin Family Name: Windows : Microsoft Bulletins, Plugin ID: 46313

Details

Affected Assets

Name	Last Hit Date	Type	Risk Score	Criticality	IP	MAC	Category	Vendor
WIN-18OFIPB12HM	Jul 10, 2023 09:52:26 PM	Engineering S...	47	Medium	(Direct)		Network Assets	Rockwell

Items: 1

WIN-18OFIPB12HM (Direct) Engineering Station 47 Jul 18, 2023 02:50:54 PM

Plugin Output

Port: 445 / tcp / cifs Source: Nessus Hit date: 09:52:26 PM - Jul 10, 2023 Copy to clipboard

- C:\Program Files (x86)\Common Files\Microsoft Shared\VBA\VBA6\Vbe6.dll has not been patched.
Remote version : 6.0.87.14
Should be : 6.5.10.53

Exemple de sortie d'un plug-in OT Security

<

Rockwell Automation ControlLogix Communications Modules Remote Code Execution (CVE-2023-3595)

Actions

Vulnerability

Severity: Critical, VPR: 6.7, Affected Assets: 3, Plugin Family Name: Tenable.ot, Plugin ID: 501226

Details

Affected Assets

Name	Last Hit Date	Type	Risk Score	Criticality	IP	MAC	Category	Vendor
Comm. Adapter #50	Jul 18, 2023 07:05:36 PM	Communicati...	61	High			Controllers	Rockwell
Comm. Adapter #35	Jul 18, 2023 07:05:36 PM	Communicati...	67	High	1		Controllers	Rockwell
Comm. Adapter #53	Jul 18, 2023 07:05:35 PM	Communicati...	68	High			Controllers	Rockwell

Items: 3

Comm. Adapter #50 10.100.101.152 (Direct) Communication Module 61 Jul 18, 2023 07:10:14 PM

Plugin Output

Port: 0 / tcp Source: Tot Hit date: 07:05:36 PM - Jul 18, 2023 Copy to clipboard

Vendor : Rockwell
Family : ControlLogix
Model : 1756-EN2T/D
Version : 10.007



Détections

Utilisez la page Détections pour passer en revue la liste des instances individuelles de vulnérabilité qui affectent votre environnement, par asset. La page Détections vous permet d'effectuer les opérations suivantes :

- Afficher des preuves détaillées pour chaque « correspondance » spécifique d'une vulnérabilité dans votre environnement.
- Filtrer la liste des vulnérabilités selon les propriétés du plug-in, de l'asset affecté et de l'instance spécifique, par exemple Statut, Dernière correspondance ou une combinaison de propriétés.
- Exporter la liste filtrée des détections en vue de leur remédiation.

Pour accéder à la page Détections :

1. Dans le menu de navigation de gauche, accédez à Risques > Détections.

La page Détections apparaît avec les vulnérabilités sous forme de tableau.

Findings 

 You can enable automatic cloud updates for the Nessus Plugin Set [Configure Settings](#) ×

[Vulnerabilities](#)  Policy Violations


Status Active, Resurfaced ▾ ×
Severity Low, Medium, High +1 ▾ ×
+ Add Filter ▾
[Remove All Filters](#)

1090 Vulnerability Findings Group By ▾  

Affected Asset	IP	Severity 1 ▾	Plugin Name	Protocol	Port
RTU #1		● Critical	Siemens SCALANCE, RUGGEDCOM, SI...	TCP	0
CP-420FA6		● Critical	Beckhoff ADS protocol Authentication...	TCP	0
testigy		● Critical	Schneider Electric Modicon Weak Pass...	TCP	0
ML1100		● Critical	Rockwell Automation Micrologix Impropr...	TCP	0
testigy		● Critical	Schneider Electric Modicon Weak Pass...	TCP	0
Comm. Adapter #30		● Critical	Rockwell Automation Select Communic...	TCP	0
Comm. Adapter #30		● Critical	Rockwell Automation products using G...	TCP	0

Findings 

 You can enable automatic cloud updates for the Nessus Plugin Set [Configure Settings](#) ×

[Vulnerabilities](#)  Policy Violations


Status Active, Resurfaced ▾ ×
Severity Low, Medium, High +1 ▾ ×
+ Add Filter ▾
[Remove All Filters](#)
[Save Filter](#)

40989 Vulnerability Findings Group By ▾  

Affected Asset	IP	Severity 1 ▾	Plugin Name	Protocol	Port
		● Critical		TCP	0
		● Critical		TCP	0
		● Critical		TCP	0
		● Critical		TCP	0
RTU #2		● Critical		TCP	0
RTU #1		● Critical		TCP	0

Le tableau Détections contient les détails suivants :



Colonne	Description
Asset affecté	Asset dans lequel la vulnérabilité est détectée.
IP	Adresse IP de l'asset.
Sévérité	Sévérité de la vulnérabilité : critique, moyenne, faible ou info.
Nom du plug-in	Plug-in ayant détecté la vulnérabilité.
ID de plug-in	ID du plug-in.
Port	Port sur lequel la vulnérabilité est détectée.
Protocole	Protocole utilisé pour communiquer avec l'asset.
VPR	Classement VPR (Vulnerability Priority Rating) de la vulnérabilité.
Statut	Statut de la vulnérabilité. Les valeurs possibles sont : Active – Indique que la vulnérabilité est présente de façon continue depuis sa détection initiale. Corrigée – Indique que la vulnérabilité est initialement apparue, a disparu et n'a pas réapparu. Réapparue – Indique que la vulnérabilité est apparue et a disparu, puis a réapparu.
Source du plug-in	Source du plug-in.
Première correspondance	Date/heure à laquelle la vulnérabilité a été détectée pour la première fois.
Dernière correspondance	Date/heure à laquelle la vulnérabilité a été détectée pour la dernière fois.



Colonne	Description
Tags d'assets	Les tags associés à l'asset. Voir Groupes d'assets et tags .
Corrigée à	Date/heure à laquelle la vulnérabilité a été corrigée.
Famille du plug-in	Famille du plug-in.
Type d'asset	Type d'asset, p. ex. PLC et appareil OT.
Score de risque de l'asset	Score de risque de l'asset.
Catégorie d'asset	Catégorie à laquelle l'asset appartient, p. ex. Contrôleur, Assets réseau.
Fournisseur de l'asset	Nom du fournisseur de l'asset.
Criticité de l'asset	Criticité de l'asset en fonction de la sévérité de la vulnérabilité : criticité élevée, criticité moyenne ou faible criticité.
Famille d'assets	Famille de l'asset.
Modèle d'asset	Modèle de l'asset.
Firmware	Firmware de l'asset.
OS	Système d'exploitation sur lequel l'asset s'exécute.
État de l'asset	État actuel de l'asset.
Niveau Purdue	Niveau Purdue de l'asset.
Segment réseau	Segment réseau auquel l'asset appartient.



Colonne	Description
Emplacement	Emplacement de l'asset.
Nom du fond de panier	Nom du fond de panier où la vulnérabilité a été détectée.

Afficher les détails des détections

Les détails des détections comprennent les éléments suivants :

- Sortie du plug-in
- Détails de la vulnérabilité
- Détails des assets affectés

Pour afficher les détails des détections :

1. Sur la page Détections, cliquez sur le lien dans la colonne Assets affectés ou Nom du plug-in.

Le panneau Détails de la vulnérabilité apparaît.

The screenshot shows the Nessus Findings interface. On the left, a list of 13 Vulnerability Findings is displayed, filtered by 'Active, Resurfaced' status and 'Medium' severity. The right panel shows the details for a specific vulnerability: 'Recursive DNS Server Detection' (Plugin ID 3703, Severity Medium, Active). The details include the plugin source (NNM), plugin ID (3703), last hit time (02:42:57 PM, Jun 10, 2025), and a table of affected assets (1 asset). The 'Vulnerability Details' section includes an overview table and a plugin details table.

Findings

You can enable automatic cloud updates for the Nessus Plugin Set

Search... Status: Active, Resurfaced

Severity: Low, Medium, High +1

13 Vulnerability Findings Group By

Affected Asset	IP	Severity
...	...	Medium
...	...	Medium
...	...	Medium
...	...	Medium
...	...	Medium
...	...	Medium
...	...	Medium
...	...	Medium

Vulnerability Details

Recursive DNS Server Detection

Port 53/UDP

Plugin Source NNM Plugin ID 3703 Last Hit 02:42:57 PM · Jun 10, 2025

Plugin Output

02:42:57 PM · Jun 10, 2025

Vulnerability Details

Overview

SEVERITY	Medium
AFFECTED ASSETS	1

Plugin details

PLUGIN SOURCE	NNM
PLUGIN ID	0

Vous pouvez afficher les détails suivants :

- Sévérité
- Assets affectés
- Source du plug-in
- ID de plug-in
- Détails de l'asset affecté : Nom, Type, Criticité, Score de risque, Adresse IP, Niveau Purdue.
- Pour développer le panneau des détails de la vulnérabilité, cliquez sur le bouton  dans le coin supérieur droit.
- Pour fermer le panneau, cliquez sur le bouton  dans le coin supérieur droit.
- Pour afficher tous les détails de l'asset, dans la section Asset affecté, cliquez sur Afficher tous les détails de l'asset .



- OT Security ouvre la page Inventaire contenant les détails de l'asset dans un nouvel onglet de navigateur.

Violations de politique

Utilisez la page Violations de politique pour afficher tous les événements associés à la même politique, source et cible. Chaque détection figurant sur la page est une agrégation de plusieurs événements résultant de correspondances avec la même politique et partageant la même source et la même cible.

Pour accéder à la page Violations de politique :

1. Dans le menu de navigation de gauche, cliquez sur Risques > Détections.

La page Détections apparaît.

2. Cliquez sur l'onglet Violations de politique.

La page Violations de politique apparaît avec la liste des événements.

Findings

You can enable automatic cloud updates for the Nessus Plugin Set

Configure Settings

Vulnerabilities

Policy Violations

Full Event Log

Search...

Status Active, Resurfaced

+ Add Filter

Remove All Filters

58 Policy Violation Findings

Actions

Group By

	Status	Sev... 1	Violation Type	Source Asset	Source IP	Destination Asset	Destination IP
☐	Active	Medium	Unauthorized Conversati...	Eng_Station #1			
☐	Active	Medium	Intrusion Detection	Endpoint #73			
☐	Active	Medium	ARP Scan	Endpoint #5			
☐	Active	Medium	Intrusion Detection	Endpoint #73			
☐	Active	Medium	Intrusion Detection	Endpoint #73			
☐	Active	Medium	Intrusion Detection	Endpoint #101			
☐	Active	Medium	Unauthorized Conversati...	Eng_Station #1			

Findings

You can enable automatic cloud updates for the Nessus Plugin Set

Configure Settings

Vulnerabilities

Policy Violations

Full Event Log

Search...

Status Active, Resurfaced

+ Add Filter

Remove All Filters

Save Filter

4029 Policy Violation Findings

Actions

Group By

	Status	Sev... 1	Violation Type	Source Asset	Source IP	Destination Asset	Destination IP
☐	Active	High	Change in Firmware Ver...				
☐	Active	High	Rockwell PLC Stop				
☐	Active	High	Rockwell PLC Stop				
☐	Active	High	Change in Firmware Ver...				
☐	Active	High	Intrusion Detection				
☐	Active	High	Change in Firmware Ver...				
☐	Active	Medium	Failed Unsecured FTP Io...				

L'onglet Violations de politique contient les détails suivants :



Colonne	Description
ID	ID de la violation.
Statut	Statut de la violation : active, réapparue ou résolue.
Sévérité	Sévérité de la violation : élevée, moyenne ou faible.
Type de violation	Type de violation. Par exemple, Unauthorized Conversation (Communication non autorisée) et Intrusion Detection (Détection d'intrusion).
Catégorie de violation	Catégorie à laquelle appartient le type de violation.
Politique	Politique à l'origine de la violation.
Nom du plug-in	Plug-ins associés à la violation.
Tactiques Mitre ICS	Raison ou motif d'une technique d'attaque Mitre spécifique visant les systèmes de contrôle industriels (ICS).
Techniques Mitre ICS	Méthode utilisée par un attaquant pour atteindre un but tactique.
Asset source	Asset au niveau duquel la violation est apparue.
IP source	Adresse IP de l'asset source.
Asset cible	Asset au niveau duquel la violation a pris fin.
IP cible	Adresse IP de l'asset cible.
Protocole	Protocole associé à la violation.



Colonne	Description
Première correspondance	Date/heure à laquelle la violation a été détectée pour la première fois.
Dernière correspondance	Date/heure à laquelle la violation a été détectée pour la dernière fois.
Correspondances actives	Nombre d'événements entraînant la violation.
Type d'asset	Type d'asset dans lequel la violation a été détectée.
Criticité de l'asset	Criticité de l'asset.
Fournisseur de l'asset	Fournisseur associé à l'asset.
Famille d'assets	Famille à laquelle l'asset appartient.
Tags d'assets	Tags associés à l'asset.
Niveau Purdue	Niveau Purdue de l'asset.
Emplacement de l'asset	Région où l'asset est situé.
Résolue le	Date à laquelle la violation a été résolue.
Résolue par	Utilisateur ayant résolu la violation.
Commentaire	Commentaires ajoutés par l'utilisateur lors de la résolution de la violation.

3. (Facultatif) Vous pouvez effectuer les opérations suivantes sur la page Violations :



- Personnaliser les colonnes comme décrit dans [Personnaliser les tableaux](#).
- Filtrer le tableau des détections. Voir [Filtrer les tableaux](#).
- [Exporter](#) les données au format CSV.

Menu Actions

Résoudre une détection

- Pour résoudre une détection :
 - a. Sélectionnez la ligne de la détection et cliquez sur Actions > Résoudre.

Le panneau Résoudre apparaît.
 - b. Saisissez un commentaire pour résoudre la détection.
 - c. Cliquez sur Enregistrer.

OT Security résout la détection et le panneau Détails du plug-in affiche le statut Résolu.

Remarque : si l'événement se reproduit, OT Security rouvre la détection et son statut devient Réapparue.

Exclure de la politique

- Pour exclure la détection d'une politique :
 - a. Sélectionnez la ligne de la détection et cliquez sur Actions > Exclure de la politique.

Le panneau Exclure de la politique apparaît.
 - b. Sélectionnez les conditions d'exclusion.

Remarque : les conditions d'exclusion sont basées sur le dernier et le plus récent événement.



- c. Renseignez le champ Description de l'exclusion.
- d. Cliquez sur Enregistrer.

OT Security exclut l'événement le plus récent de la politique.

Télécharger le dernier fichier de capture

- Pour télécharger le dernier fichier de capture :
 - a. Sélectionnez la ligne de la détection et cliquez sur Actions > Télécharger le dernier fichier de capture.

OT Security télécharge le fichier de capture de l'événement le plus récent.

Détails du plug-in

Pour afficher les détails du plug-in de la détection :

1. Dans l'onglet Violations de politique, cliquez sur la ligne de la détection pour afficher les détails de son plug-in.

Le panneau des détails du plug-in apparaît avec les détails de la violation tirés de la [page des plug-ins OT Security](#).

Le panneau affiche les détails de la violation dans quatre onglets distincts : Détails, Source, Cibles et Politique.

Rechercher des événements

Pour rechercher des événements spécifiques à l'origine de la violation :

- a. Pour trouver les événements d'une détection spécifique, cliquez sur  Copier l'ID de détection.
- b. Pour accéder à la page Événements, cliquez sur le lien Journal complet des événements .



La page Tous les événements apparaît.

- c. Dans la zone de recherche, collez l'ID de détection que vous avez copié précédemment.

OT Security répertorie les événements de la détection spécifique.

Dashboard Conformité

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité, Analyste sécurité, Opérateur de site, Lecture seule

La conformité aux cadres de sécurité tels que la directive NIS 2 et les contrôles ISO 27001 est désormais obligatoire dans la plupart des entreprises d'infrastructures critiques pour réussir les contrôles d'audit.

Le respect des cadres de conformité peut être un processus complexe et nécessite des connaissances spécialisées. Utilisez le dashboard Conformité pour avoir une vision d'ensemble des assets, vulnérabilités et événements susceptibles d'affecter les opérations métier critiques de votre organisation, mais aussi pour répondre à ces questions d'audit essentielles :

- Quelles politiques de sécurité avez-vous mises en place pour détecter les activités suspectes ?
- Combien de temps vous faut-il pour traiter un incident ?
- Les alertes sont-elles intégrées à votre SOC/SIEM dans le cadre de votre plan de réponse aux incidents (IR) ?
- Combien d'événements de sécurité avez-vous constatés sur vos assets critiques au cours de la semaine ou du mois dernier ?

Le dashboard Conformité vous permet d'aligner les mesures de sécurité clés sur les exigences réglementaires, de suivre vos progrès et vos améliorations au fil du temps, et de renforcer votre posture de sécurité.



À l'aide des données du dashboard, vous pouvez identifier les domaines dans lesquels l'organisation est conforme et améliorer les domaines qui affectent l'entreprise du point de vue du risque.

Compliance

[Security Framework Preferences](#)

General Info

TOTAL ASSETS IN SCOPE	841
FRAMEWORKS IN SCOPE	Not Defined (Default)

Incident Handling

Assets with abnormal unresolved events

Event Category	Asset Criticality: High	Asset Criticality: Medium	Asset Criticality: Low
Network Events	93	16	9
Network Threats	91	38	19

[Show Asset List](#)

Vulnerability Handling

Active vulnerabilities by asset type category

Pour afficher le dashboard Conformité :

1. Dans la barre de navigation de gauche, cliquez sur Dashboards > Conformité.

Le dashboard Conformité apparaît.

2. Dans la barre de navigation de gauche, cliquez sur Risques > Conformité.

Le dashboard Conformité apparaît.

Remarque : pour configurer les préférences du cadre de sécurité, accédez à Paramètres locaux > Configuration système > Conformité. Pour plus d'informations, voir [Définir les préférences du dashboard Conformité](#).

Le dashboard comprend les widgets suivants.



Conseil : survolez l'icône  en regard des sections du widget pour obtenir plus d'informations sur les mesures du cadre traitées par chaque widget.

Widget	Description
Gestion des incidents	Donne un aperçu des assets à risque selon leur criticité : élevée, moyenne ou faible. Vous pouvez utiliser ces données pour répondre aux incidents de sécurité à haut risque. En fonction de la résolution d'événements hautement critiques au cours des 30 derniers jours, OT Security enregistre le temps moyen de réponse (MTTR) aux événements. Cette valeur aide à comprendre le délai moyen nécessaire pour répondre à chaque événement critique. Le MTTR est un indicateur clé de performance critique : une valeur de MTTR basse est le signe d'un processus de résolution des incidents efficace. Remarque : pour afficher tous les assets à haut risque avec des événements ouverts suspects, cliquez sur le lien Afficher la liste des assets. Pour refermer la liste des assets, cliquez sur Masquer la liste des assets.
Gestion des vulnérabilités	Donne un aperçu de toutes les vulnérabilités par sévérité et type d'assets affectés. Ce widget vous permet d'identifier, d'évaluer, de signaler et de corriger les vulnérabilités OT, réseau et IoT de manière continue. En fonction des vulnérabilités corrigées au cours des 90 derniers jours, OT Security enregistre le temps moyen de réponse (MTTR). Les paramètres MTTR et Accord de niveau de service (SLA) permettent de comprendre le délai moyen nécessaire pour répondre à chaque vulnérabilité critique et de suivre les progrès de l'équipe dans l'atténuation des vulnérabilités, par rapport aux SLA définis. Une valeur



Widget	Description
	de MTTR basse est le signe d'un processus de résolution des incidents efficace. Remarque : pour afficher tous les assets à haut risque avec des vulnérabilités critiques actives, cliquez sur Afficher la liste des assets. Pour refermer la liste des assets, cliquez sur Masquer la liste des assets.
Gestion de la configuration et des modifications	Donne un aperçu de tous les assets avec des événements de configuration non résolus (modifications apportées après la définition d'une base de référence, par exemple) et des activités critiques liées au statut du contrôleur, telles que l'arrêt de l'appareil. Les données de ce widget aident à détecter les modifications non autorisées et les événements critiques, afin de garantir la continuité des opérations et une reprise rapide en cas d'interruption de service. Remarque : pour afficher les assets à haut risque avec des événements de changement de configuration, cliquez sur le lien Afficher la liste des assets. Pour refermer la liste des assets, cliquez sur Masquer la liste des assets.
Risque d'exposition externe	Donne un aperçu des connexions externes aux réseaux de systèmes de contrôle industriels (ICS). Vous pouvez utiliser les données de ce widget pour identifier les communications externes inattendues sur les assets OT, réseau et IoT, les évaluer et atténuer les risques correspondants. Ces données garantissent également la conformité aux mesures de sécurité de la chaîne d'approvisionnement lorsque les fournisseurs et constructeurs d'équipements et de machines ICS utilisent des modèles hybrides et déplacent leur portail et leurs stations d'ingénierie vers le cloud, où il existe un risque d'exposition externe.
Cryptographie non	Donne un aperçu des événements cryptographiques non sécurisés, tels



Widget	Description
sécurisée	que les connexions non sécurisées et les informations d'identification non chiffrées. Ces données peuvent aider à surveiller et détecter les événements cryptographiques non sécurisés, pour éviter que des informations sensibles ne soient compromises et que le service ne soit interrompu. Remarque : pour afficher tous les assets à haut risque avec des événements d'authentification non sécurisée, cliquez sur le lien Afficher la liste des assets. Pour refermer la liste des assets, cliquez sur Masquer la liste des assets.
Surveillance des communications non sécurisées	Donne un aperçu des assets à haut risque avec des événements de communication non sécurisée et des accès non autorisés. Ces données peuvent aider à empêcher toute communication non sécurisée et tout accès non authentifié suspect pouvant rendre des informations sensibles ou des assets critiques vulnérables aux attaquants. Remarque : pour afficher tous les assets à haut risque avec des événements d'authentification non sécurisée, cliquez sur le lien Afficher la liste des assets. Pour refermer la liste des assets, cliquez sur Masquer la liste des assets.
Évaluation des risques	Donne un aperçu des assets à risque selon leur criticité. Ces données aident à évaluer et à gérer les risques associés aux assets OT, réseau et IoT, ainsi qu'à identifier et atténuer les menaces potentielles de manière proactive. Remarque : pour afficher tous les assets à haut risque, cliquez sur le lien Afficher la liste des assets. Pour refermer la liste des assets, cliquez sur Masquer la liste des assets.



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

tenable OT Security

Overview

Events

All Events

Configuration Events

SCADA Events

Network Threats

Network Events

Policies

Inventory

All Assets

Controllers and Modules

Network Assets

IoT

Network Map

Risks

All Events

Search...

Actions

Resolve All

Status	Log ID	Time	Event Type	Severity	Policy Name	Source Asset	Source Address
☐	Not resol...	63026	08:22:08 AM · Nov 11, 2024	Rockwell Code U...	Low	Rockwell Code Upload	
☐	Not resol...	63025	08:21:50 AM · Nov 11, 2024	Rockwell Code U...	Low	Rockwell Code Upload	
☐	Not resol...	63024	08:21:50 AM · Nov 11, 2024	Rockwell Code U...	Low	Rockwell Code Upload	
☐	Not resol...	63021	08:20:41 AM · Nov 11, 2024	Rockwell Code U...	Low	Rockwell Code Upload	
☐	Not resol...	63020	08:20:41 AM · Nov 11, 2024	Rockwell Code U...	Low	Rockwell Code Upload	
☐	Not resol...	63019	08:20:29 AM · Nov 11, 2024	Modicon Code U...	Low	Modicon Code Upload	

Items: 63026

Event 63026

08:22:08 AM · Nov 11, 2024

Rockwell Code Upload

Low

Not resolved

Details

Code was uploaded from a controller to an engineering station

Code

Source

Destination

Policy

Status

SOURCE NAME

SOURCE IP ADDRESS

DESTINATION NAME

DESTINATION IP ADDRESS

DESTINATION MAC ADDRESS

PROTOCOL

CIP (TCP)

Why is this important?

The system has detected an upload of the controller code that was done via the network. When not part of regular operations, a code upload can be used to gather information on the controller behavior as part of reconnaissance activity.

Suggested Mitigation

1) Check whether the upload was done as part of scheduled maintenance work and verify that the source of the operation is approved to perform this operation.
2) If this was not part of a



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 et du nom de la politique. 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



Paramètre	Description
	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.



Paramètre	Description
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



Paramètre	Description
	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.



Paramètre	Description
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.



All Events

Search...

Actions ▼ | Resolve All ↗ ↺

	Status	Log ID	Time ↓	Event Type	Severity	Policy Name	Source Asset	Source Address
☐	Not resol...	62947	07:48:59 AM · Nov 11, 2024	SIMATIC Hardwar...	Low	SIMATIC Hardware Confi...		
☒	Not resol...	62952	07:48:59 AM · Nov 11, 2024	ARP Scan	Medium	ARP Scan Detection		
☐	Not resol...	62944	07:48:57 AM · Nov 11, 2024	SIMATIC Hardwar...	Low	SIMATIC Hardware Confi...		
☐	Not resol...	62949	07:48:55 AM · Nov 11, 2024	SIMATIC Hardwar...	Low	SIMATIC Hardware Confi...		
☐	Not resol...	62943	07:48:53 AM · Nov 11, 2024	Modicon Code U...	Low	Modicon Code Upload	BOA2024-11-11-07:48:53	10.100.20.3
☐	Not resol...	62948	07:48:52 AM · Nov 11, 2024	SIMATIC Hardwar...	Low	SIMATIC Hardware Confi...	BOA2024-11-11-07:48:52	10.100.20.3
☐	Not resol...	62942	07:48:51 AM · Nov 11, 2024	Rockwell Code U...	Low	Rockwell Code Upload		
☐	Not resol...	62941	07:48:37 AM · Nov 11, 2024	Rockwell Code U...	Low	Rockwell Code Upload		

Items: 63027 | Selected Items: 1 | [Deselect all](#)

Event 62952 | 07:48:59 AM · Nov 11, 2024 | ARP Scan | Medium | Not resolved

Details

Affected Assets

Policy

Scanned Addresses

Status

ARP scans are used to map devices in a local network

SOURCE NAME

SOURCE MAC ADDRESS

PROTOCOL

OT Server #5

ARP

Why is this important?

ARP scans can be used for network mapping. It is important to know what assets are mapping the network and to verify that such mapping is

Suggested Mitigation

Check the source asset to determine whether it is expected to be generating ARP scans for monitoring purposes. If not, contact the source asset

Créer des exclusions de politique

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité

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 ».

Exclude From Policy

Future events that meet this condition will not affect asset risk score and will not appear in the events list. You will be able to delete this condition from the exclusions tab in the policy page.

Policy Name
Snapshot Mismatch

Exclude Conditions *
☒ Source asset is Rouge

Exclusion Description

Cancel Exclude

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



Catégorie de politique	Type d'événement	Conditions d'exclusion
		• 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



Catégorie de politique	Type d'événement	Conditions d'exclusion
		• 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



Catégorie de politique	Type d'événement	Conditions d'exclusion
		• 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



Catégorie de politique	Type d'événement	Conditions d'exclusion
		• 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)	• Asset source • IP source



Catégorie de politique	Type d'événement	Conditions d'exclusion
	CEI60870-5-104)	• 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

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité, Analyste sécurité

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). 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

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité

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.

Create Policy on FortiGate ×

SOURCE ADDRESS:
[Greyed out]

DESTINATION ADDRESS:
[Greyed out]

FORTIGATE SERVER: *

[Dropdown menu with options: FortiGate1, fortigateSTAS]

Cancel Create

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.

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 et les ressources impliquées. Voir [Communications](#)

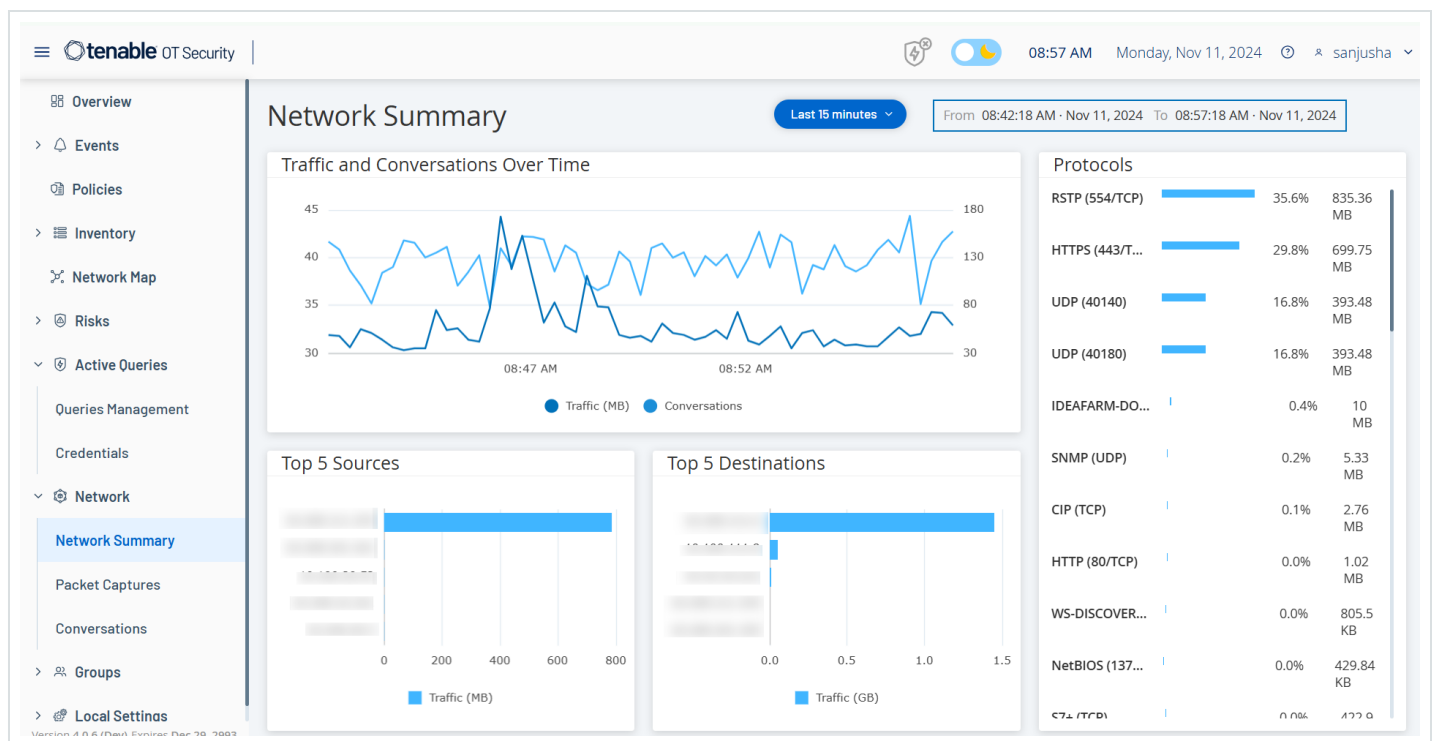
Pour accéder à la page Réseau :

1. Dans le volet de navigation de gauche, sélectionnez Réseau.

La page Récapitulatif réseau apparaît.

Récapitulatif réseau

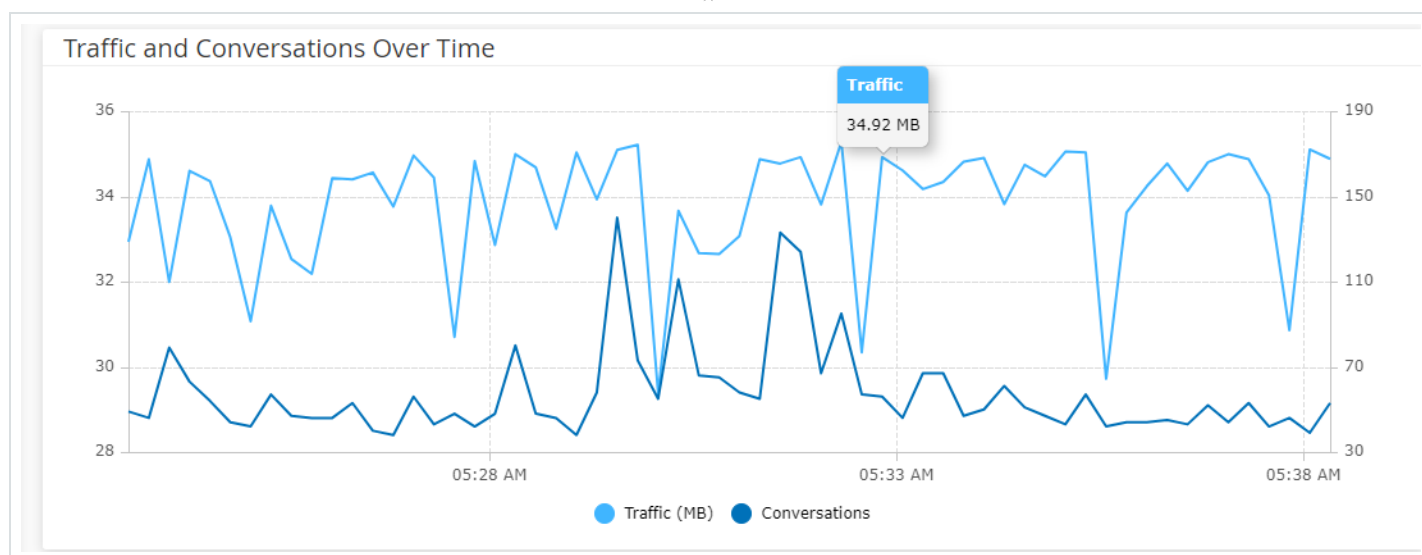
La page Récapitulatif réseau affiche des graphes visuels qui résument l'activité du réseau. Vous pouvez afficher les données associées à une période spécifique.



Interagissez avec les widgets suivants pour afficher des détails supplémentaires.

Traffic et communications au fil du temps

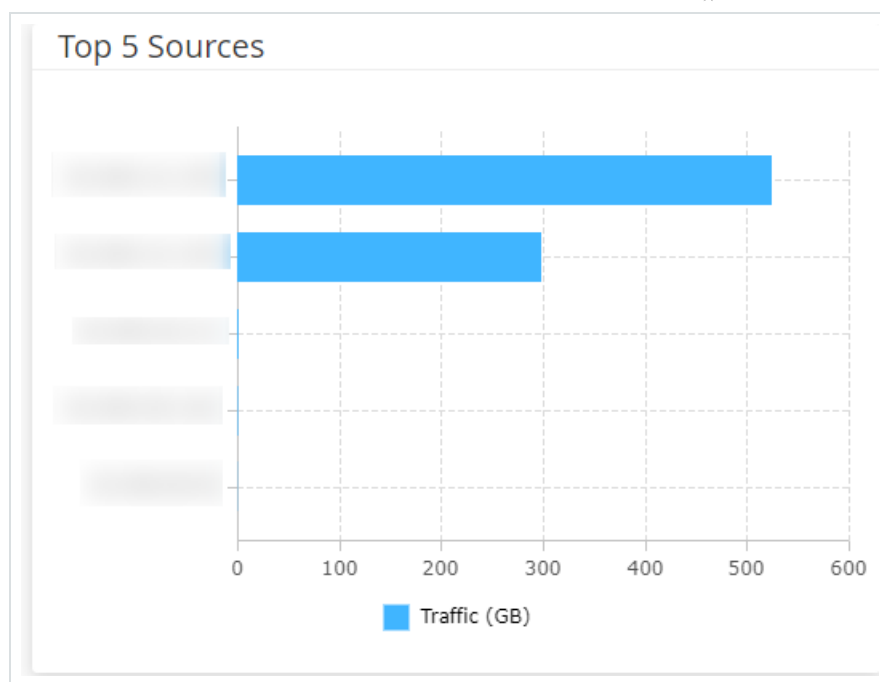
Un graphique en courbe affiche le volume de trafic (exprimé en Ko/Mo/Go) et le nombre de communications survenues sur le réseau au fil du temps. La légende apparaît en haut du graphe. Survolez un point du graphe avec la souris pour afficher des données spécifiques sur le trafic et les communications 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.

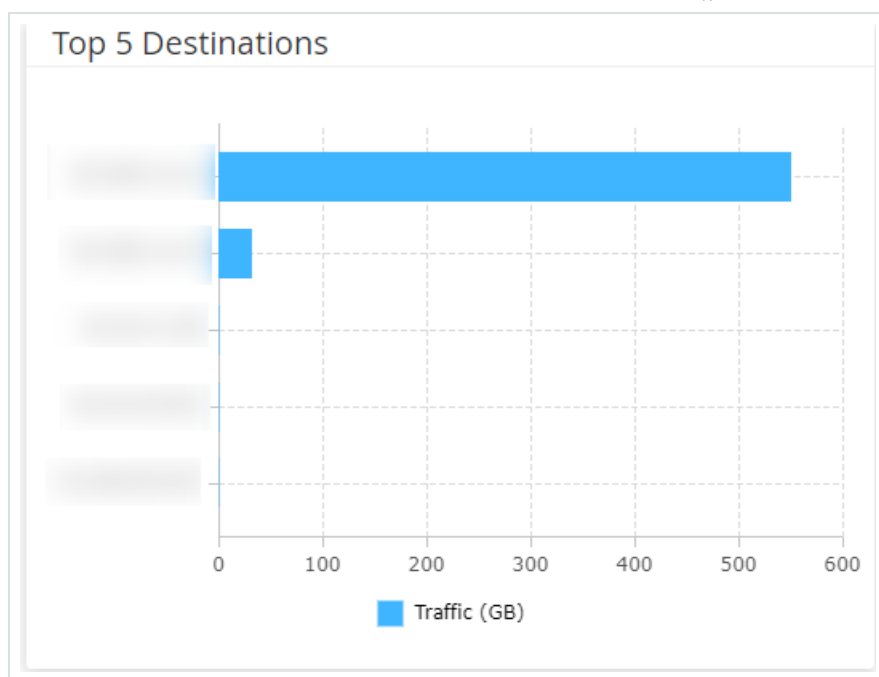
Top 5 sources

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.



Protocols			
HTTPS (443/TCP)		34.0%	483.18 GB
UDP (6970)		21.0%	298.51 GB
UDP (58940)		18.5%	262.23 GB
UDP (56570)		16.6%	235.59 GB
RSTP (554/TCP)		7.3%	103.19 GB
UDP (49910)		1.9%	26.63 GB
HTTP (80/TCP)		0.3%	4.06 GB
SNMP (UDP)		0.1%	1.25 GB
NetBIOS (137/UDP)		0.1%	910.19 MB
CIP (TCP)		0.1%	763.85 MB
SSH (22/TCP)		0.0%	530.26 MB
WS-DISCOVERY (370...		0.0%	525.29 MB
HTTPS (8443/TCP)		0.0%	399.99 MB

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

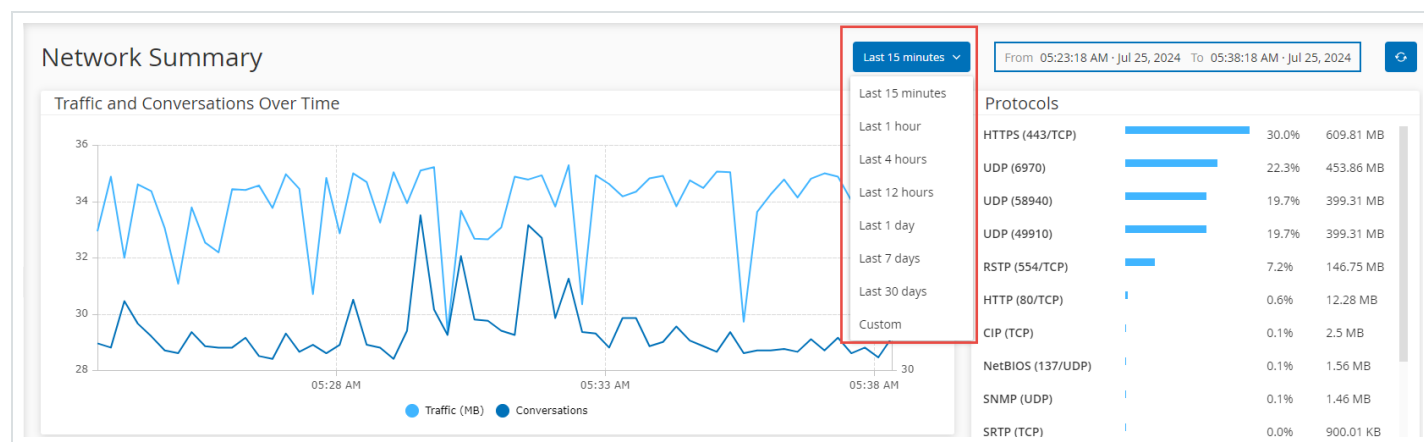


période par défaut correspond aux 15 dernières minutes. La barre d'en-tête indique également les dates/heures de début et de fin de la période.

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.

Remarque : les rôles Lecture seule et Opérateur de site ne sont pas autorisés à arrêter les captures en cours ni à télécharger les captures de paquets enregistrées.

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

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité, Analyste sécurité

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.



Conversations							
Search...							
Start Time ↓	End Time	Duration	Bytes	Packets	Source Address	Destination Ad...	Protocol
Completed (10000)							
Nov 11, 2024 09:02:58 AM	Nov 11, 2024 09:02:58 AM	1 second	587	10			HTTP (80/TCP)
Nov 11, 2024 09:02:57 AM	Nov 11, 2024 09:02:57 AM	1 second	202	2			HTTP (80/TCP)
Nov 11, 2024 09:02:57 AM	Nov 11, 2024 09:02:57 AM	1 second	200	3			HTTP (80/TCP)
Nov 11, 2024 09:02:55 AM	Nov 11, 2024 09:02:57 AM	2 seconds	32487	688			SNMP (161/UDP)
Nov 11, 2024 09:02:53 AM	Nov 11, 2024 09:02:53 AM	1 second	82	1			SNMP (161/UDP)
Nov 11, 2024 09:02:53 AM	Nov 11, 2024 09:02:53 AM	1 second	82	1			SNMP (161/UDP)
Nov 11, 2024 09:02:53 AM	Nov 11, 2024 09:02:53 AM	1 second	82	1			SNMP (161/UDP)
Nov 11, 2024 09:02:47 AM	Nov 11, 2024 09:02:47 AM	1 second	54	1			3COM-NSD (1742...
Nov 11, 2024 09:02:47 AM	Nov 11, 2024 09:02:47 AM	1 second	54	1			CISCO-NET-MGM...
Nov 11, 2024 09:02:47 AM	Nov 11, 2024 09:02:47 AM	1 second	54	1			ENCORE (1740/U...
Nov 11, 2024 09:02:47 AM	Nov 11, 2024 09:02:47 AM	1 second	54	1			CINEGRFX-LM (17...

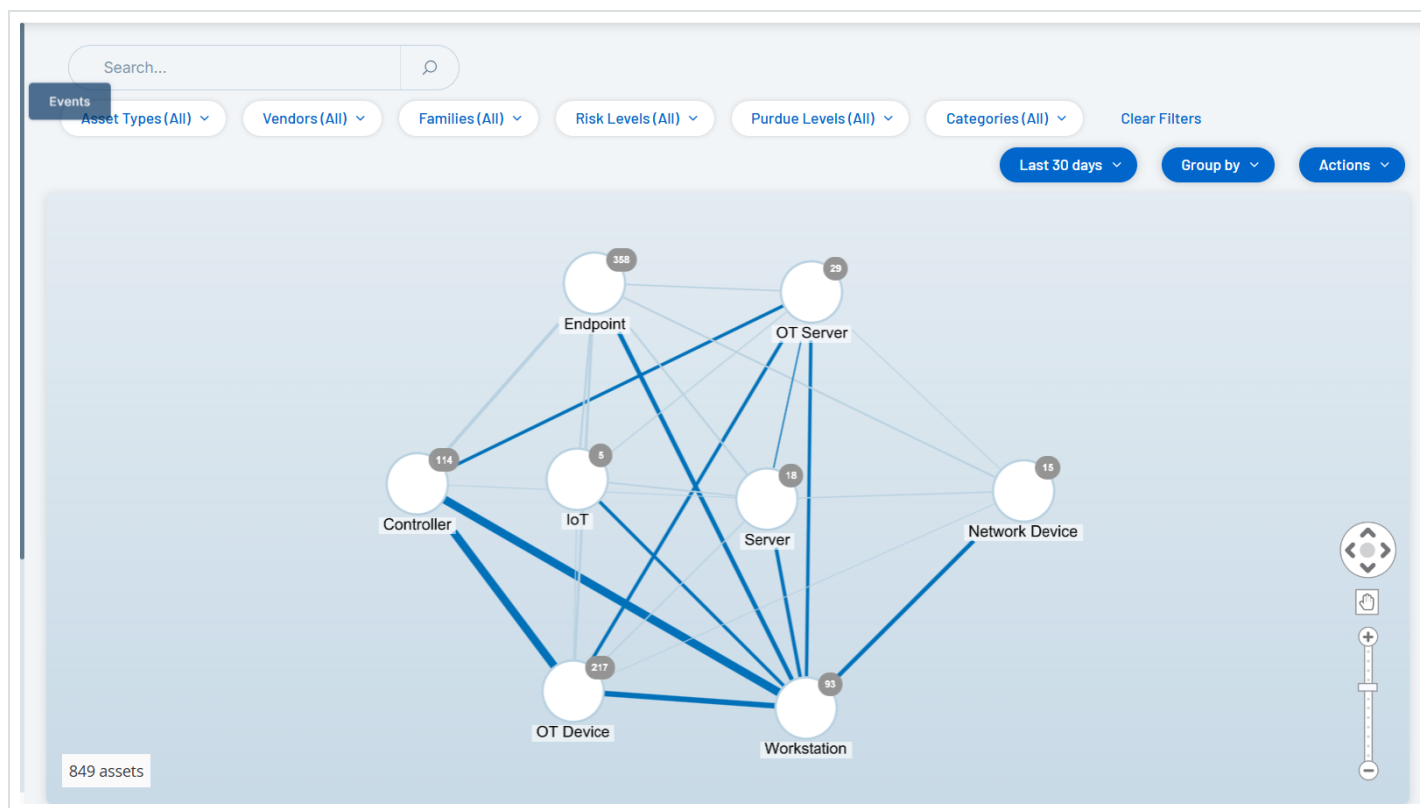
La page Communications affiche les détails suivants :

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.

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.

La cartographie du réseau utilise des codes couleur pour différencier les protocoles IT et OT.

- Une ligne grise indique les protocoles IT uniquement (par exemple, DNS, HTTP et FTP).
- Une ligne bleue indique la présence de protocoles OT (par exemple, HTTP, MODBUS, CIP et FTP).
- 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

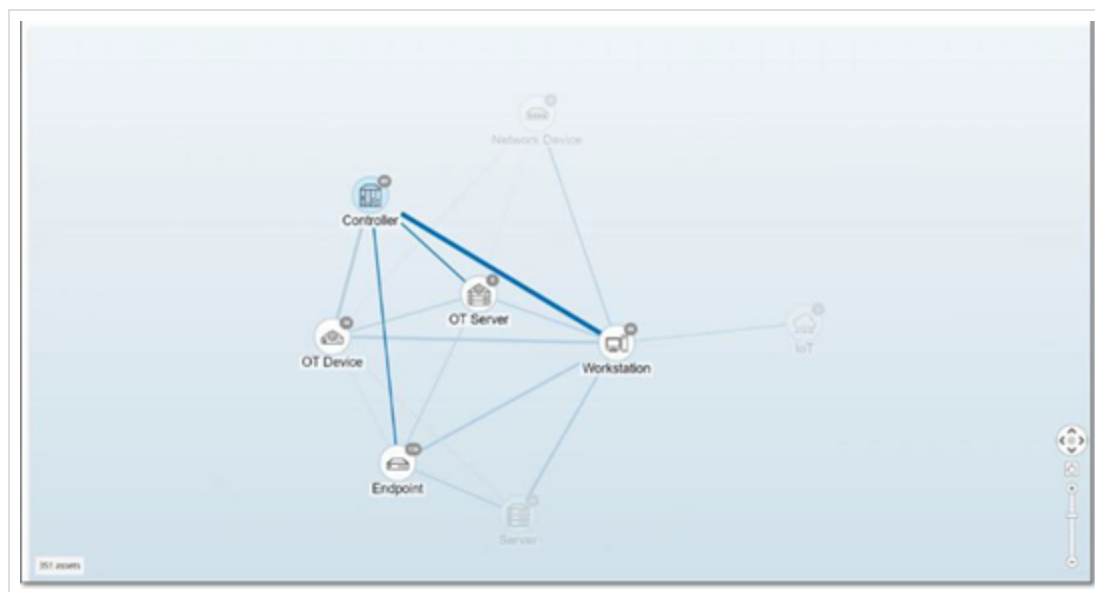


suivante : Niveau Purdue/Niveau de risque > Type d'asset > Fournisseur > Famille > Asset individuel. Chaque niveau est représenté par un cercle entourant les groupes/assets inclus.

L'exemple suivant montre comment vous pouvez détailler l'affichage :

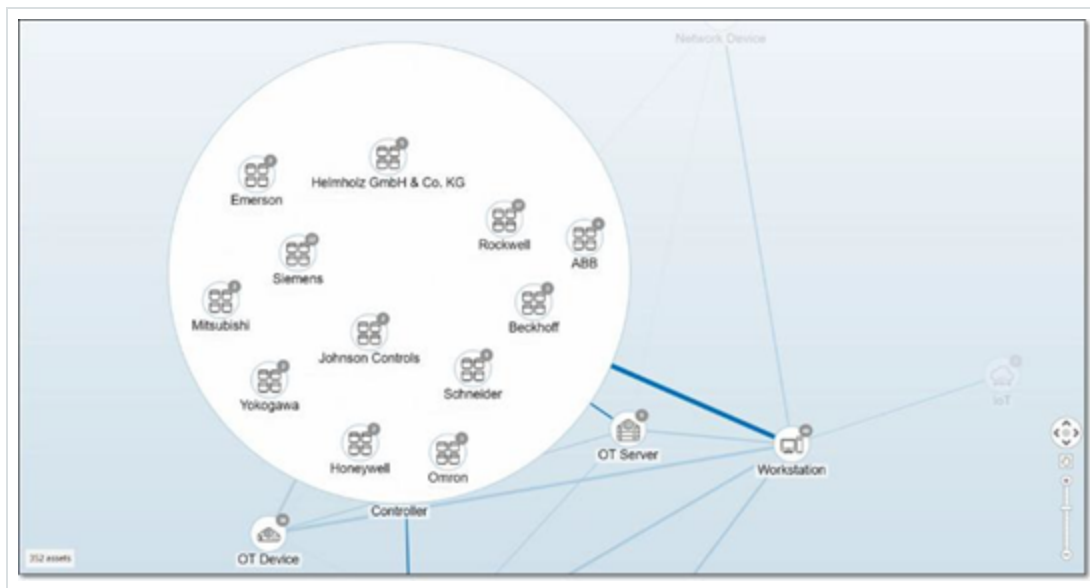
Pour détailler un groupe de types d'assets :

1. Par défaut, lorsque vous ouvrez l'écran Cartographie du réseau, il regroupe les assets par type.

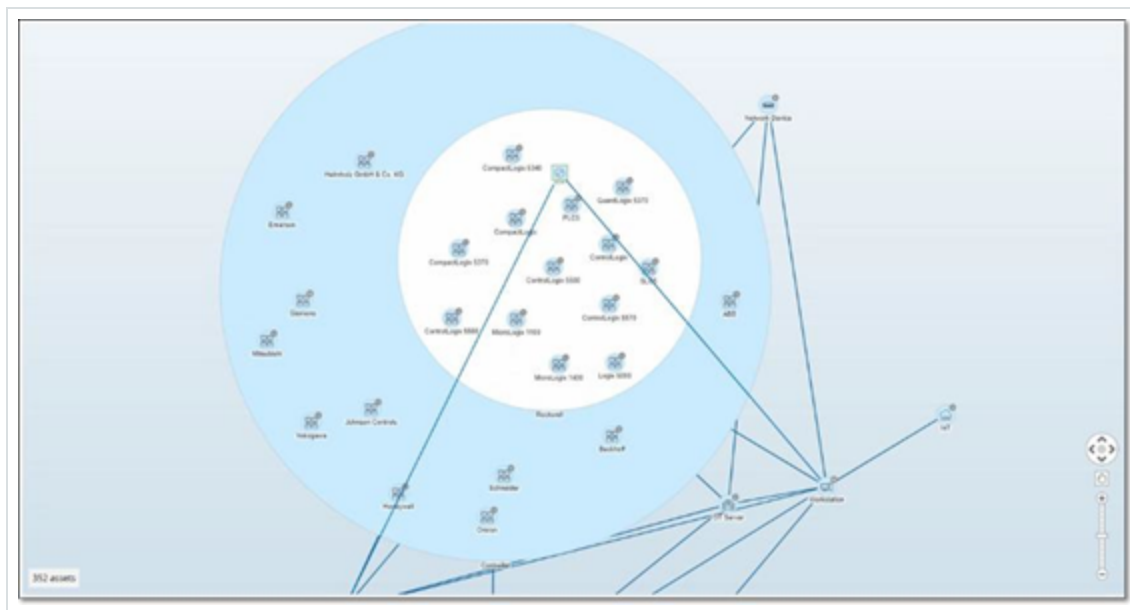


2. Double-cliquez sur l'icône du groupe que vous souhaitez détailler (par exemple Contrôleur).

Le groupe est développé, affichant les groupes de fournisseurs qu'il contient.

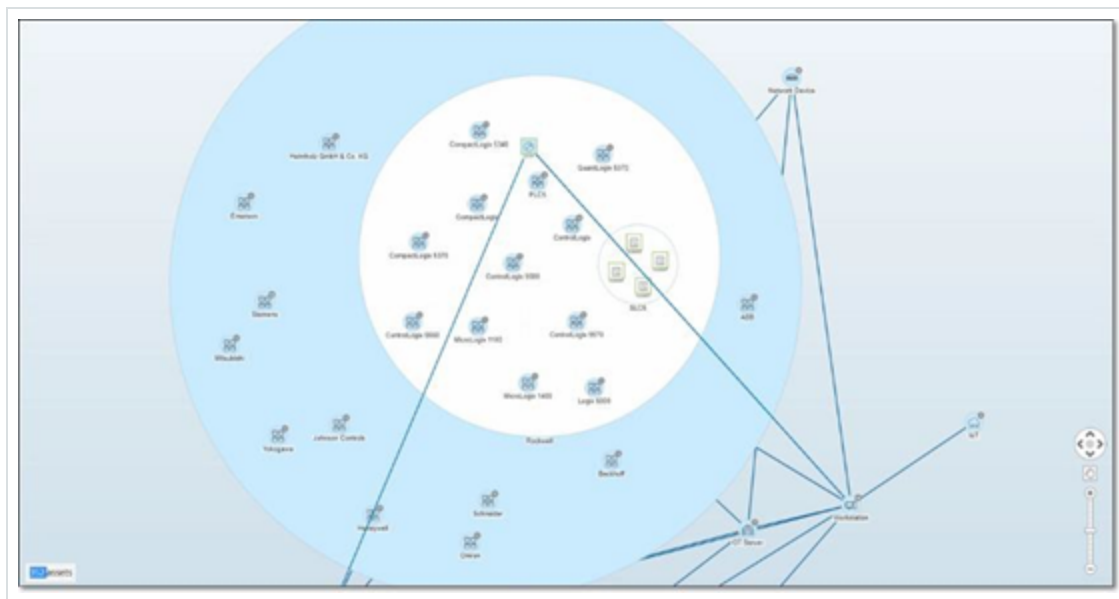


3. Pour aller plus loin, cliquez sur un groupe de fournisseurs (par exemple Rockwell).



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.

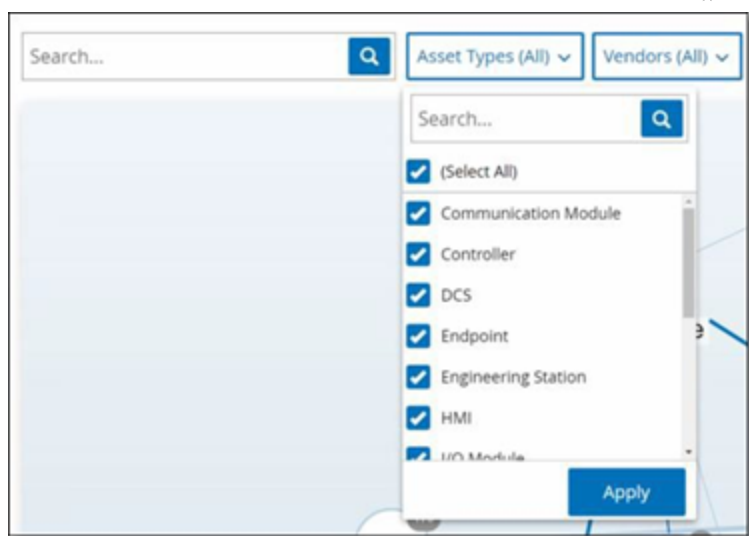
Pour supprimer tous les regroupements :

1. Cliquez sur le bouton Grouper par.
2. Sélectionnez Pas de regroupement.

La carte affiche tous les assets uniques sans les regrouper.

Appliquer des 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.

Afficher les 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.



Collecte de données

La section Collecte de données dans OT Security comprend les pages de configuration suivantes :

- [Politiques](#)
- [Gérer les requêtes actives](#)
- [Sources de données](#)

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 et la criticité
- 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 et par service.



- 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) ou par fabricant (par exemple, Protocoles autorisés par Rockwell).
- 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 et du week-end.
- 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 et session en ligne Modicon.

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 et test.
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 <u>Définition d'une base de référence réseau</u> . 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 sensibilité, Planification	Détecte les pics anormaux dans le volume du trafic 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.
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)	Source, Cible, Planification	Une connexion RDP (connexion bureau à distance) a été établie sur le réseau à l'aide des identifiants



(Connexion RDP (authentifiée))		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 sécurisée réussie)	Source, Cible, Planification	OT Security considère FTP comme un protocole non sécurisé. Cette politique détecte les connexions réussies à l'aide du protocole FTP.
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	Source, Cible, Planification	OT Security considère Telnet comme un protocole non sécurisé. Cette politique détecte les connexions réussies à l'aide du protocole Telnet.



login (Connexion Telnet non sécurisée réussie)		
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



		(attaques ICS, déni de service et malware) et sous-catégories (attaques ICS - Stuxnet et attaques ICS - Black Energy). 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, Asset cible, Planification	Détecte le code d'erreur « 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	Détecte les écritures non



	tags, Valeur du tag, Planification	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	Asset source, Asset cible, Planification	Détecte les commandes spécifiques envoyées aux unités principales ou subordonnées CEI-104 considérées comme risquées.



Command with Time Tag (commande de test avec marqueur temporel)		
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) et Warm/Cold Restart (Redémarrage à chaud/à froid). 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

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité

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.

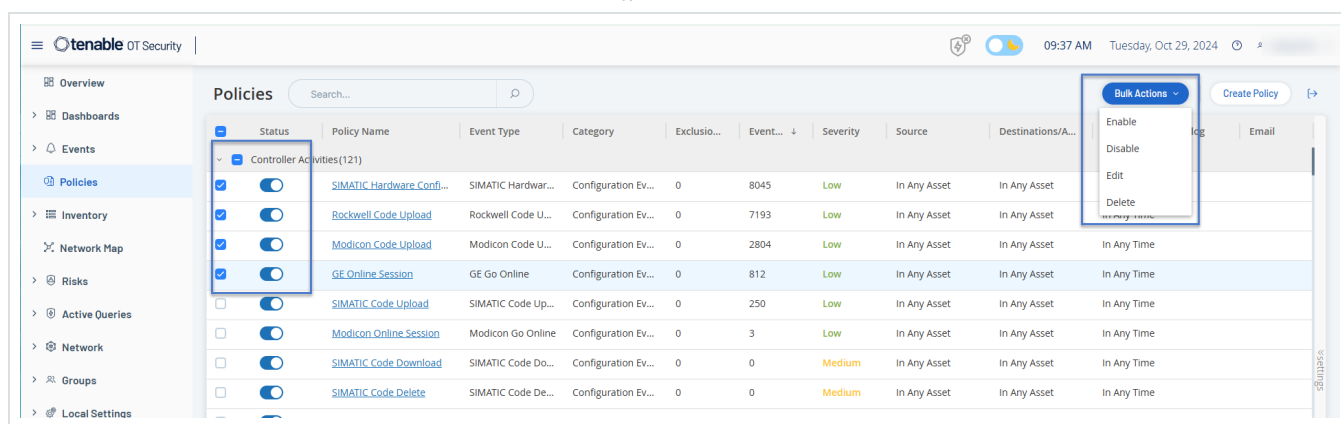
☐	Status	Policy Name	Event Type	Category	Exclusio...	Event...	Severity	Source	Destinations/A...	Schedule	Syslog	Email
Controller Activities (121)												
☐	☒	SIMATIC Hardware Conf...	SIMATIC Hardwar...	Configuration Ev...	0	7681	Low	In Any Asset	In Any Asset	In Any Time		
☐	☒	Rockwell Code Upload	Rockwell Code U...	Configuration Ev...	0	6791	Low	In Any Asset	In Any Asset	In Any Time		
☐	☒	Modicon Code Upload	Modicon Code U...	Configuration Ev...	0	2663	Low	In Any Asset	In Any Asset	In Any Time		
☐	☒	GE Online Session	GE Go Online	Configuration Ev...	0	809	Low	In Any Asset	In Any Asset	In Any Time		
☐	☒	SIMATIC Code Upload	SIMATIC Code Up...	Configuration Ev...	0	233	Low	In Any Asset	In Any Asset	In Any Time		
☐	☒	Modicon Online Session	Modicon Go Online	Configuration Ev...	0	3	Low	In Any Asset	In Any Asset	In Any Time		
☐	☒	SIMATIC Code Download	SIMATIC Code Do...	Configuration Ev...	0	0	Medium	In Any Asset	In Any Asset	In Any Time		
☐	☒	SIMATIC Code Delete	SIMATIC Code De...	Configuration Ev...	0	0	Medium	In Any Asset	In Any Asset	In Any Time		
☐	☒	SIMATIC Hardware Conf...	SIMATIC Hardwar...	Configuration Ev...	0	0	Medium	In Any Asset	In Any Asset	In Any Time		
☐	☒	SIMATIC Firmware Downl...	SIMATIC Firmwar...	Configuration Ev...	0	0	High	In Any Asset	In Any Asset	In Any Time		
☐	☒	SIMATIC Firmware Upload	SIMATIC Firmwar...	Configuration Ev...	0	0	Medium	In Any Asset	In Any Asset	In Any Time		
☐	☒	SIMATIC PLC Stop	SIMATIC PLC Stop	Configuration Ev...	0	0	High	In Any Asset	In Any Asset	In Any Time		
☐	☒	SIMATIC PLC Start	SIMATIC PLC Start	Configuration Ev...	0	0	Low	In Any Asset	In Any Asset	In Any Time		
☐	☒	SIMATIC Enable IO Forcing	SIMATIC IO Forcin...	Configuration Ev...	0	0	Medium	In Any Asset	In Any Asset	In Any Time		
☐	☒	SIMATIC Disable IO Forcing	SIMATIC IO Forcin...	Configuration Ev...	0	0	Medium	In Any Asset	In Any Asset	In Any Time		

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

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité, Analyste sécurité, Opérateur de site, Lecture seule

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 générerait 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, P1 pour les activités de contrôleur et P2 pour les événements réseau.
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 .

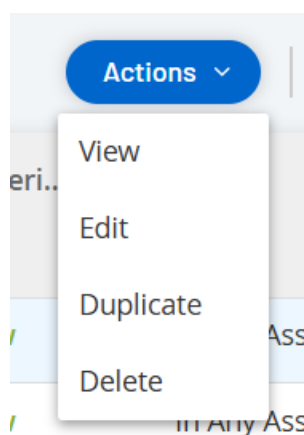
Afficher les détails d'une politique

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.

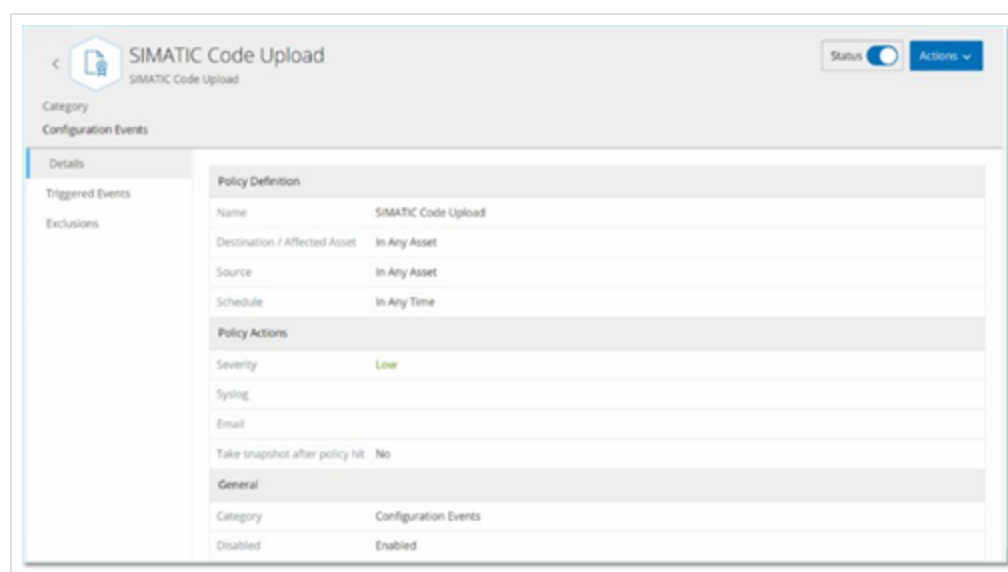
Pour ouvrir l'écran des détails de la politique pour une politique donnée :



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



Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité

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.



Create Policy



> Configuration Events (130)

> Network Events (17)

> Network Threats (3)

> SCADA Events (38)

Items: 188

Cancel

Next >



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.

Create Policy ×

●

●

●

Event Type

Policy Definition

Policy Actions

🔍

▼ Configuration Events (130)

▶ Controller Activities (124)

▼ Controller Validation (6)

Change in Key Switch
The state of the write lock key on the controller has changed

Change in State
A change in the asset running state has been detected

3. Sélectionnez un type de politique.



Create Policy

Event Type Policy Definition Policy Actions

Change in Firmware Version

POLICY NAME *

AFFECTED ASSETS *

In ▾

Select ▾

Or

And

SCHEDULE *

In ▾

Select ▾

< Back

Cancel

Next >



4. 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 :

Attention : 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.

Remarque : la sélection disponible inclut tous les groupes d'assets, à l'exception des groupes d'assets dynamiques dont l'ensemble de règles contient l'une des propriétés d'asset suivantes :

- Score de risque
- Nom du fond de panier
- Sources
- Tags
- État du matériel
- Statut du cycle de vie
- Produit de remplacement



Create Policy



Event Type Policy Definition Policy Actions

Change in Firmware Version

POLICY NAME *

AFFECTED ASSETS *

In ▾

And

SCHEDULE *

In ▾

Select ▾

Or

Search...

- Private IP ranges
- OT Servers
- Tablets
- Medical Devices
- Domain Controllers
- Security Appliances

< Back

Cancel

Next >



- 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.



Create Policy



● — ● — ●

Event Type Policy Definition Policy Actions

Change in Firmware Version

SEVERITY *

High

Medium

Low

None

SYSLOG

Syslog servers are not configured

EMAIL

SMTP servers are not configured

< Back

Cancel

Create



8. 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

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité

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.

Gérer les requêtes actives

La page Gestion des requêtes actives vous permet de configurer et d'activer des requêtes actives. 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.



Active Queries Management

ACTIVE QUERIES ENGINE ENABLED ☒ [Add Restrictions](#)

[OT Queries](#) [IT Queries](#) [Discovery](#) [Initial Enrichment](#) [Credentials](#) [Nessus Scans](#)

OT Queries

Identification Query FUNDAMENTAL

Identification Query is a set of unicast queries that will fingerprint the asset based on network protocols, services, and banners.

ENABLE MANUAL RUN ☒

Custom Variations Actions [Create Query Variation](#)

Name	Status	Assets	Recurrence	Next execution	Last execution
Identification query	Created	Any Asset	☒ Every day at 12:00 P		

Items: 1

Backplane Mapping FUNDAMENTAL

En plus des requêtes automatiques qui sont exécutées périodiquement, vous pouvez lancer des requêtes à la demande en activant le curseur Activer l'exécution manuelle dans la fiche de la requête. Si vous désactivez l'option Activer l'exécution manuelle, OT Security vous invite à contourner ce réglage lorsque vous sélectionnez [Exécuter une resynchronisation](#) sur la page Détails de l'asset (Inventaire > Tous les assets).

Pour plus d'informations sur la technologie de requête, voir [Technologies OT Security](#).

Remarque : il se peut que OT Security ne parvienne pas à identifier les assets lorsque vous désactivez des requêtes. OT Security assure le suivi des appareils par le biais d'une surveillance passive et de requêtes actives.

Conseil : pour permettre aux requêtes actives de fonctionner, cliquez sur la curseur Moteur de requêtes actives activé. Après avoir activé les requêtes actives, OT Security affiche l'icône  sur l'en-tête pour indiquer que le moteur de requête est en cours d'exécution. Pour exécuter des requêtes actives, vous devez toujours activer chaque requête séparément.

La page Gestion des requêtes actives répartit les requêtes en différentes catégories. Chaque type de requête possède son propre onglet qui affiche la liste de requêtes correspondantes.



- Requêtes 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 effectue des requêtes en lecture seule pour collecter des informations sur les appareils, et notamment connaître l'état de fonctionnement du PLC et d'autres modules connectés au fond de panier. Les appareils qui écoutent les protocoles propriétaires pris en charge par OT Security sont interrogés. Les types de requêtes sont Requête d'identification, Mappage de fond de panier, Requête de détails, Requête d'état et Instantanés de code.
- Requêtes IT – Il s'agit des requêtes qui récupèrent des points de données supplémentaires à partir d'assets de type IT surveillés que OT Security observe. 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 pour solliciter l'infrastructure réseau ou les appareils en réseau qui prennent en charge le protocole SNMP, afin d'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.

OT Security fournit également les options suivantes pour tirer parti de votre requête SNMP :

- État des ports SNMP : activez le curseur État des ports SNMP pour obtenir le statut du port réseau des assets et activez le curseur Récupérer les éléments voisins.
- Récupérer les éléments voisins : lorsque vous activez cette option, OT Security collecte les adresses MAC et IP des appareils à proximité via SNMP. Pour ajouter



ces assets à votre inventaire, activez Paramètres > Configuration de l'environnement > Définitions de réseau > Découvrir de nouveaux assets via SNMP.

- La requête de détails WMI récupère divers points de données importants à partir des systèmes Windows. Le système interrogé par OT Security 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.
- Le scan Nessus de base récupère des détails du système tels que l'adresse IP, le nom de domaine complet (FQDN), les systèmes d'exploitation et les ports ouverts.
- La requête ARP (protocole de résolution d'adresse) récupère l'adresse matérielle de l'interface réseau ou l'adresse MAC des appareils connectés par IP dans le même domaine de diffusion.
- Découverte – Ces requêtes détectent les assets en direct sur le réseau que OT Security surveille.
 - Découverte des assets – Utilise le protocole ICMP (Internet Control Message Protocol) ou ping pour détecter les adresses IP actives et qui répondent.
 - Découverte automatique des sous-réseaux – Détecte les sous-réseaux en interrogeant les appareils réseau via SNMP. Sur la page Inventaire, la colonne Sous-réseaux indique les sous-réseaux auxquels les adresses IP des assets appartiennent. Vous pouvez également filtrer les assets au sein d'un sous-réseau spécifique.



- Suivi des assets actifs – Tente régulièrement d'interroger un asset connu et surveillé pour déterminer s'il est toujours opérationnel et disponible.
- 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.
- Requête ping – Envoie des pings ICMP (Internet Control Message Protocol) pour vérifier si un asset est joignable.
- Recherche DNS – Récupère les détails du serveur DNS.
- Mappage de port – Récupère des détails à propos des ports ouverts sur les assets surveillés.
- Enrichissement initial – Requêtes OT Security automatiques reposant sur certains critères ou certaines conditions. 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.
- Scans OTD - Jeu d'instructions techniques créé via l'assistant de scan OT Discovery. Il définit les modalités : informations d'authentification, planification et restrictions.
- Scan Nessus – Le scan de plug-in Tenable 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. Pour plus d'informations, voir [Créer des scans des plug-ins Nessus](#).

Créer des requêtes personnalisées

Rôle utilisateur OT Security requis : Administrateur, Superviseur



Chaque type de requête a une variante système par défaut que vous pouvez exécuter périodiquement ou à la demande. Vous pouvez également créer des variantes supplémentaires de chaque requête, avec leur propre configuration, pour différents projets et fonctions.

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 variante de requête :

1. Accédez à Collecte de données > Requêtes actives.

La page Gestion des requêtes actives apparaît.

2. Cliquez sur l'onglet de type de requête concerné.

OT Security affiche le type de requête avec la liste des requêtes disponibles.

3. Dans la section du type de requête requis, cliquez sur Créer une variante de requête.

Le panneau Créer une variante de requête apparaît.

4. Dans la zone Nom, saisissez le nom de la requête.

5. Dans la zone déroulante Assets, sélectionnez un groupe d'assets.

Remarque : vous pouvez également utiliser la zone de recherche pour rechercher un groupe particulier.

6. Pour répéter la requête, cliquez sur la curseur Exécution récurrente.

OT Security active la section Répéter chaque.



7. 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.
8. 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.
9. (Uniquement pour la découverte des assets) Dans la zone Plages d'adresses IP, saisissez les adresses IP des assets.
10. (Uniquement pour les requêtes de découverte) Dans la zone déroulante Nombre d'assets à interroger simultanément, sélectionnez le nombre d'assets (10, 20 ou 30).
11. (Uniquement pour les requêtes de découverte) Dans la zone déroulante Temps entre les requêtes de découverte, sélectionnez l'intervalle entre les requêtes de découverte (1 à 3 secondes).
12. (Uniquement pour les réseaux dupliqués) Dans la zone Capteurs concernés, sélectionnez les capteurs associés.
13. Cliquez sur Enregistrer.

OT Security ajoute la requête au tableau Variantes personnalisées.

Voir [Exécuter une variante de requête](#).

Ajouter des restrictions

Rôle utilisateur OT Security requis : Administrateur, Superviseur

Vous pouvez empêcher les requêtes de s'exécuter sur certains groupes d'assets, tels que des plages d'adresses IP, des serveurs OT, des tablettes, des dispositifs médicaux et des contrôleurs de domaine. Vous pouvez également appliquer des restrictions à des protocoles spécifiques (clients).



Remarque : les restrictions ne s'appliquent pas aux requêtes de découverte (ICMP) et de vérification des ports ouverts (dans les requêtes d'enrichissement d'asset).

Pour ajouter des restrictions :

1. Accédez à Collecte de données > Requêtes actives.

La page Gestion des requêtes actives apparaît.

2. Dans le coin supérieur droit, cliquez sur Ajouter des restrictions.

Le panneau Ajouter des restrictions s'affiche.

3. Dans la zone déroulante Assets bloqués, sélectionnez les groupes d'assets à bloquer.

Remarque : vous pouvez utiliser la zone de recherche pour rechercher des groupes d'assets spécifiques.

4. Dans la zone déroulante Clients restreints, sélectionnez les clients requis.

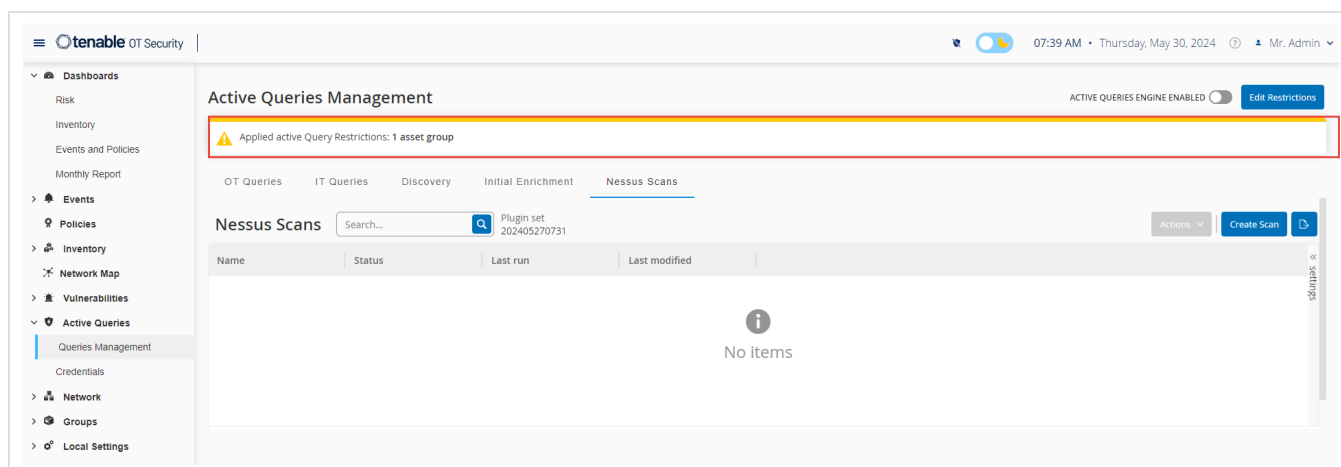
5. Dans la zone déroulante Période d'indisponibilité, sélectionnez la durée de blocage des requêtes actives. Les options disponibles dépendent des groupes de planification. Les options par défaut sont : Aucune, Heures ouvrées.

6. Cliquez sur Enregistrer.

OT Security applique les restrictions aux clients et aux groupes d'assets. En haut de chaque



onglet, une bannière indique que des restrictions sont en place.



Modifier la variante de requête

Rôle utilisateur OT Security requis : Administrateur, Superviseur

Pour modifier les détails d'une requête :

1. Accédez à Collecte de données > Requêtes actives.

La fenêtre Gestion des requêtes actives apparaît.

2. Dans la liste des requêtes, sélectionnez celle qui doit être modifiée et effectuez l'une des opérations suivantes :

- Effectuez un clic droit sur la requête et sélectionnez Modifier.
- Sélectionnez la requête, puis cliquez sur Actions > Modifier.

Le panneau Modifier la requête apparaît.

3. Modifiez la requête selon les besoins.



4. Cliquez sur Enregistrer.

OT Security enregistre les modifications apportées à la variante de requête.

Dupliquer une variante de requête

Rôle utilisateur OT Security requis : Administrateur, Superviseur

1. Accédez à Collecte de données > Requêtes actives.

La page Gestion des requêtes actives apparaît.

2. Dans la liste des requêtes, sélectionnez celle à dupliquer et effectuez l'une des opérations suivantes :

- Effectuez un clic droit sur la requête et sélectionnez Dupliquer.
- Sélectionnez la requête, puis cliquez sur Actions > Dupliquer.

Le panneau Dupliquer la requête apparaît avec les détails de la requête.

3. Renommez la requête et modifiez les détails selon les besoins.
4. Cliquez sur Enregistrer.

OT Security enregistre la requête, qui apparaît ensuite dans le tableau Requêtes.

Exécuter une variante de requête

Rôle utilisateur OT Security requis : Administrateur, Superviseur

Vous pouvez exécuter des requêtes actives en cas de besoin.

Pour exécuter une requête :



1. Accédez à Collecte de données > Requêtes actives.

La page Gestion des requêtes actives apparaît.

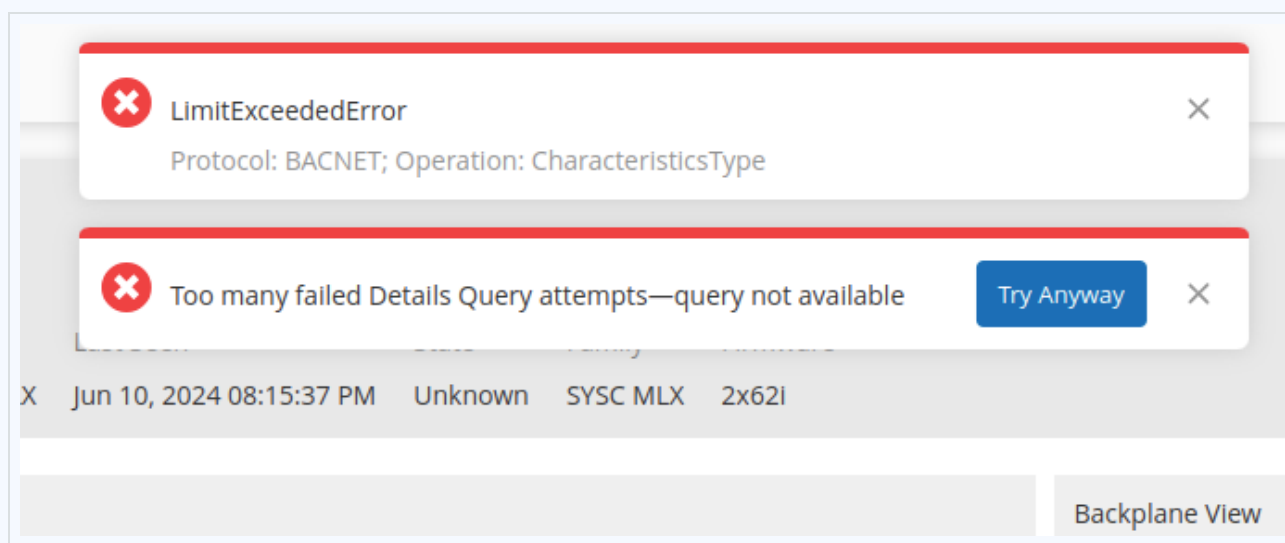
2. Dans la liste des requêtes, sélectionnez celle que vous souhaitez exécuter et exécutez l'une des actions suivantes :
 - Effectuez un clic droit sur la requête et sélectionnez Exécuter maintenant.
 - Dans le menu Actions, cliquez sur Exécuter maintenant.

Un message demande de confirmer l'exécution de la requête.

3. Cliquez sur OK.

OT Security exécute la requête sélectionnée.

Remarque : vous pouvez utiliser l'option Essayer quand même pour exécuter des requêtes actives sur les appareils ou le réseau en dépassant la limite du nombre de tentatives de requêtes actives.



Télécharger le journal de requête

Rôle utilisateur OT Security requis : Administrateur, Superviseur



Vous pouvez télécharger le journal de la dernière exécution d'une variante de requête. Vous pouvez utiliser le journal pour résoudre les problèmes affectant n'importe lequel des assets ou des protocoles inclus dans la requête active.

Pour télécharger le dernier journal de requête :

1. Accédez à Collecte de données > Requêtes actives.

La fenêtre Gestion des requêtes actives apparaît.

2. Dans la liste des requêtes, sélectionnez celle dont vous voulez télécharger le journal et exécutez l'une des actions suivantes :

- Effectuez un clic droit sur la requête et sélectionnez Télécharger le dernier journal d'exécution.
- Dans le menu Actions, cliquez sur Télécharger le dernier journal d'exécution.

OT Security télécharge le journal de la dernière requête active.

Types de requêtes de découverte

OT Security utilise plusieurs requêtes de découverte des assets pour collecter des données sur différents types de réseaux et d'appareils.

Type de requête	Description
SnmpType (requête SNMP)	Normalise la collecte des données système à partir des appareils réseau gérés tels que les commutateurs et les routeurs. Cette requête récupère les détails du matériel, le statut des interfaces et les configurations système de base à l'aide du protocole SNMP (gestion de réseau simple).



ArpType (diffusion ARP de la couche 2)	Utilise les diffusions du protocole ARP (résolution d'adresse) de la couche 2 pour découvrir les appareils actifs sur le segment de réseau local. C'est essentiel pour identifier les assets à proximité qui ne communiquent pas sur les passerelles.
IdentificationType (requête d'identification)	Agit comme outil d'empreinte numérique principal en interrogeant l'appareil pour connaître son identité Core. Cette requête récupère le fabricant, le modèle et la version du firmware afin d'établir le profil de référence de l'asset.
CharacteristicsType (requête de détails)	Utilise des protocoles industriels propriétaires pour extraire des métadonnées approfondies. Cette requête fournit des informations matérielles et logicielles détaillées auxquelles les requêtes d'identification standard ne peuvent pas accéder.
BpScanType (scan du fond de panier)	Énumère l'ensemble des modules, cartes et sous-composants reposant sur un châssis physique pour le matériel modulaire. Cette requête fournit l'architecture interne complète d'un contrôleur logique programmable (PLC) ou d'un contrôleur.
RunStatusType (requête sur l'état du contrôleur)	Surveille le mode opérationnel des PLC, des IED et des contrôleurs. Les modes sont notamment RUN (exécution), STOP (arrêt), or FAULT (défaut). Cette requête est essentielle pour déterminer si un processus est actif ou si un appareil a basculé dans un état de programmation vulnérable.
NbstatQueryType (découverte NetBIOS)	Interroge le service de nom NetBIOS pour identifier les systèmes basés sur Windows et d'autres appareils compatibles. Utilisez cette requête pour résoudre les noms d'hôte et les informations de groupe de travail des assets du sous-réseau local.
WmiType (requête	Utilise l'instrumentation WMI (Windows Management



avancée WMI)	Instrumentation) authentifiée pour effectuer des audits approfondis des terminaux Windows. Utilisez cette requête pour collecter des données précises sur les logiciels installés, les correctifs d'OS, les utilisateurs actifs et les correctifs système.
WmiUsbType (requête WMI USB ou HID)	Requête WMI spécialisée permettant d'auditer les périphériques physique connectés. Cette requête détecte et consigne les supports amovibles, comme les stockages USB et les interfaces humains-machine (HID). Ces appareils sont couramment employés comme vecteurs pour introduire des logiciels malveillants dans les environnements hermétiques.
DnsType (recherche DNS)	Utilise les serveurs DNS configurés pour déduire le nom de domaine complet (FQDN) d'une adresse IP. Les assets apparaissent ainsi dans la console de gestion sous leur nom réseau lisible.

Informations d'authentification

Rôle utilisateur OT Security requis : Administrateur, Superviseur

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.



Active Queries Management

ACTIVE QUERIES ENGINE ENABLED ☐ [Add Restrictions](#)

[OT Queries](#) [IT Queries](#) [Discovery](#) [Initial Enrichment](#) [Nessus Scans](#) [Credentials](#)

Credentials

 [Actions](#) [Add Credentials](#)

Name	Type ↑	Description	Last modified by	Last modified on
IT Credentials(1)				
SNMP V1+V2	SNMP v1+v2	Commonly used SNMP credentia...	system	01:45:09 PM · Aug 26, 2025

Ajouter des informations d'authentification

Pour ajouter des informations d'authentification :

1. Accédez à Collecte de données > Requêtes actives.

La page Gestion des requêtes actives apparaît.

2. Cliquez sur l'onglet Informations d'identification.

La page Informations d'authentification apparaît.

3. Dans le coin supérieur droit, cliquez sur Ajouter des informations d'authentification.



Le panneau Ajouter des informations d'authentification apparaît.

Add Credentials

×

✓

Credentials TypeCredentials Details

WMI

NAME *

WMI Local User

DESCRIPTION

Authentication for workstations.

USERNAME *

localuser

PASSWORD *

.....

TEST IP ADDRESS

[Test Credentials](#)

< Back

Cancel

Save



4. 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

5. Cliquez sur Suivant.

Le panneau Détails des informations d'authentification apparaît.

6. 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.



7. Cliquez sur Tester les informations d'authentification pour vérifier si OT Security peut accéder à l'appareil à l'aide des informations d'authentification.
8. (Pour les réseaux dupliqués) Dans la zone Doublon (capteur), sélectionnez les capteurs associés.
9. 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 Collecte de données > Requêtes actives.

La page Gestion des requêtes actives apparaît.

2. Cliquez sur l'onglet Informations d'identification.

La page Informations d'authentification apparaît.

3. 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.

4. Modifiez les détails selon les besoins.
5. 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 Collecte de données > Requêtes actives.

La page Gestion des requêtes actives apparaît.

2. Cliquez sur l'onglet Informations d'identification.

La page Informations d'authentification apparaît.

3. 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



Rôle utilisateur OT Security requis : Administrateur, Superviseur

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.

À partir de OT Security 4.1, vous pouvez créer de nouveaux scans avec les options suivantes :

- Effectuer des tests approfondis – Cette option permet à Nessus d'effectuer un scan détaillé comprenant des plug-ins qui peuvent augmenter la durée du scan, mais permet de découvrir des détails approfondis tels que les fichiers JAR ou les bibliothèques Python installées.
- Traitement à verbosité élevée – Cette option permet au scan de fournir des détails supplémentaires sur la vulnérabilité que vous pouvez utiliser pour dépanner une détection du scan. Cette option permet également à Attack Path Analysis de tirer parti des données de connexions de scan Nessus.
- Délai d'attente du réseau (en secondes) – Délai maximal pendant lequel Nessus doit attendre une réponse de l'hôte. Si vous scannez sur un hôte lent, vous pouvez augmenter le nombre de secondes. La valeur par défaut est de 15 secondes.
- Nombre maximal de vérifications simultanées par hôte – Nombre maximal de vérifications que Nessus doit réaliser sur l'hôte. Le nombre de vérifications par défaut est de 2.
- Nombre maximal d'hôtes simultanés par scan – Nombre maximal d'hôtes que Nessus peut scanner simultanément. Le nombre d'hôtes par défaut est de 10.

Les informations sur le scan Nessus comprennent les détails suivants pour un scan authentifié :



- Dernier scan réussi
- Durée du dernier scan
- Dernier scan authentifié réussi

tenable OT Security | 03:57 PM · Wednesday, Feb 5, 2025 · Mr. Admin

WIN-UEUPT5DGA0H
OT Server

38 Actions Resync

IP	MAC	Vendor	Model	Last Seen	State	Family	Firmware	OS
(Direct)	(Direct)	Rockwell	RSLink Server	Feb 5, 2025 03:53:39 PM	Unknown	RSLink Server	1.001	Windows Server 2012 R2

Details

Overview

NAME	WIN-UEUPT5DGA0H
PURDUE LEVEL	Level 2
STATE	Unknown
DIRECT IP	
DIRECT MAC	
FAMILY	RSLink Server
VENDOR	Rockwell
MODEL NAME	RSLink Server
OS	Windows Server 2012 R2
LAST SEEN	03:53:39 PM · Feb 5, 2025
FIRST SEEN	11:48:54 PM · Jan 30, 2025
LAST UPDATE	02:01:15 AM · Feb 5, 2025
SOURCES	nic1 (Local),Nessus (Nessus),nic0 (Local)
NETWORK SEGMENTS	OT Server / 1 .X
CRITICALITY	Medium
RISK SCORE	38

General

FIRMWARE VERSION	1.001
DEVICE TYPE	Generic Device
COMMAND	1
SERVER TYPE	36871

Nessus Scan Information

LAST SUCCESSFUL SCAN	03:19:41 PM · Feb 4, 2025
LAST SCAN DURATION	15 minutes
LAST SUCCESSFUL AUTHENTICATED SCAN	04:41:25 PM · Feb 3, 2025

Les informations sur le scan Nessus vous aident à :

- Identifier les assets évalués et non évalués.
- Comprendre si vos assets sont ciblés par des scans authentifiés ou non authentifiés.



- Suivre les meilleures pratiques en matière de scan et de gestion des vulnérabilités. Par exemple, vous en effectuant des scans d'évaluation de vulnérabilités sur des assets de type informatique exécutant Windows ou Linux. Les scans, avec ou sans informations d'authentification, permettent d'évaluer la part de la surface d'attaque de votre organisation qui est exposée à la fois en interne et en externe.

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.

Créer un scan de plug-in Nessus

Pour créer un scan de plug-in Nessus :

1. Accédez à Requêtes actives > Gestion des requêtes.

La page Gestion des requêtes actives apparaît.

2. Accédez à Collecte de données > Requêtes actives.

La page Gestion des requêtes actives apparaît.



3. Cliquez sur l'onglet Scans Nessus.

La page Scans Nessus apparaît.

4. Dans le coin supérieur droit, cliquez sur Créer un scan.

Le panneau Créer un scan de la liste des plug-ins Nessus apparaît.



Create Nessus Plugin List Scan



IP Ranges Plugins



Nessus plugin list scan runs a user-defined list of plugins only on network assets within the specified IP ranges (CIDRs).

NAME *

IP RANGES *

CREDENTIALS

Note: if many credentials are defined in this site, the first option isn't recommended, as it might prolong the scan or cause other issues

- ☒ Try All Available Credentials
- ☐ Do Not Use Credentials
- ☐ Use Only Specific Credentials

☒ PERFORM THOROUGH TESTS ⓘ

☒ HIGH VERBOSITY PROCESSING ⓘ

NETWORK TIMEOUT (IN SECONDS) * ⓘ

MAX SIMULTANEOUS CHECKS PER HOST * ⓘ

MAX SIMULTANEOUS HOSTS PER SCAN * ⓘ

Cancel

Next >



Remarque : l'image affiche les valeurs par défaut pour la création d'un nouveau scan Nessus. Si vous choisissez d'exécuter le scan avec les valeurs par défaut, le scan s'exécute avec la même configuration que les scans précédents.

5. Dans la zone Nom, saisissez le nom du scan Nessus.
6. Dans la zone Plages d'adresses IP, saisissez une plage d'adresses IP ou de CIDR.
7. Sélectionnez l'une des options d'attribution d'informations d'authentification pour le scan Nessus :
 - Ne pas utiliser d'informations d'authentification - Sélectionnez cette option pour exécuter un scan non authentifié.

Conseil : si vous avez plusieurs informations d'authentification configurées, ignorez cette option car elle peut prolonger le scan.

- Essayer toutes les informations d'authentification disponibles – Sélectionnez cette option si vous souhaitez que le scan essaie toutes les informations d'authentification disponibles.
 - Utiliser uniquement des informations d'authentification spécifiques
 - a. Si vous sélectionnez Utiliser uniquement des informations d'authentification spécifiques, choisissez les informations d'authentification requises dans la liste des informations d'authentification définies dans l'ICP.
8. (Facultatif) Cliquez sur le curseur Tests approfondis pour activer un scan détaillé.

Remarque : l'option Tests approfondis comprend des plug-ins qui peuvent augmenter la durée du scan. Cependant, lorsqu'elle est activée, cette option aide le scan Nessus à découvrir des détails approfondis tels que les fichiers JAR ou les bibliothèques Python installées.

9. (Facultatif) Cliquez sur le curseur Verbose supérieure pour permettre au scan de fournir des détails supplémentaires sur la vulnérabilité.



Remarque : l'activation de l'option Verbose supérieure permet au scan de fournir des détails supplémentaires sur la vulnérabilité ou de faciliter la résolution de problèmes liés à une détection du scan. Cette option permet également à Attack Path Analysis de tirer parti des données de connexions de scan Nessus.

10. Dans la zone Délai d'attente du réseau (en secondes), saisissez le délai maximal pendant lequel Nessus doit attendre une réponse de l'hôte. Si vous scannez sur un hôte lent, vous pouvez augmenter le nombre de secondes. Le délai d'attente par défaut est de 15 secondes.
11. Dans la zone Nombre maximal de vérifications simultanées par hôte, saisissez le nombre maximal de vérifications que Nessus doit réaliser sur l'hôte. Le nombre de vérifications par défaut est de 2.
12. Dans la zone Nombre maximal d'hôtes simultanés par scan, saisissez le nombre maximal d'hôtes que Nessus peut scanner simultanément. Le nombre d'hôtes par défaut est de 10.
13. 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](#).

14. 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>.

15. 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.

Créer des scans OTD

Rôle utilisateur OT Security requis : Administrateur



Vous pouvez utiliser l'assistant de scan OT Discovery (OTD) afin de définir un ensemble d'instructions pour effectuer des scans hors ligne. La configuration du scan OTD définit ses modalités d'exécution : les informations d'authentification, les planifications et les restrictions.

Pour plus d'informations sur l'utilisation de la configuration des scans OTD dans les scans d'agents d'état portables, voir la documentation [Effectuer un scan à l'aide d'agents OT portables](#).

Pour créer un scan OTD à l'aide de l'assistant de configuration :

1. Accédez à Collecte de données > Requêtes actives.

La page Gestion des requêtes actives apparaît.

2. Cliquez sur l'onglet Scans d'agent.

La page Scans OTD apparaît.

3. Cliquez sur Créer un scan OTD.

Le panneau Créer une scan OTD apparaît.

Create OTD Scan

NAME

scan2_floor2

DESCRIPTION

Floor 2 scan

Credentials

SNMP V1+V2

Monitored Networks

192.168.0.0/16

* Network Areas

Sensor #1 (Sensor)

floor3

OTAgent #1 (Agent)

☒ ENABLE SCHEDULE

REPEATS EVERY *

4

Weeks

Cancel

Save

4. Dans la zone Nom, saisissez le nom du scan.
5. Dans la zone Description, saisissez le contexte ou les détails du scan.
6. Dans la zone déroulante Informations d'authentification, sélectionnez les informations d'authentification requises.



7. (Facultatif) Dans le coin supérieur droit, cliquez sur Ajouter des restrictions pour appliquer des restrictions au scan. Pour plus d'informations, voir [Ajouter des restrictions](#).
8. Dans la zone déroulante Réseaux surveillés, sélectionnez un ou plusieurs sous-réseaux à scanner ou saisissez une plage de CIDR.

Remarque : vous pouvez préremplir les sous-réseaux sur la page Réseaux surveillés ou les créer directement dans ce champ en saisissant la plage de CIDR.

9. Dans la zone déroulante Zones de réseaux, sélectionnez une ou plusieurs zones de réseaux.

Remarque : vous pouvez préremplir les zones de réseaux sur la page Zones de réseau ou les créer directement dans ce champ en saisissant un nouveau nom pour la zone de réseaux.

10. Pour les agents statiques, définissez une planification.
 - a. Cliquez sur le curseur Activer la planification.
 - b. Dans la zone déroulante Répéter chaque, spécifiez la fréquence en minutes, heures, jours ou semaines.
 - c. Dans la section Le, sélectionnez les jours de la semaine où vous souhaitez exécuter le scan.
 - d. Dans la zone déroulante À, sélectionnez l'heure de la journée à laquelle vous souhaitez exécuter le scan.

11. Cliquez sur Enregistrer.

OT Security enregistre la configuration du scan OTD.

Que faire ensuite

[Effectuer un scan à l'aide d'agents OT portables](#)

Sources de données



La section Source de données dans OT Security comprend les pages de configuration suivantes :

- 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](#).
- Agents - Créez des agents OT pour scanner les machines Windows distantes sur lesquelles il n'est pas possible d'installer des capteurs. Voir [Agents OT](#).
- Connecteurs IoT - Associe tous les appareils IoT (Internet des objets) gérés à leur serveur d'application respectif. Voir [Gérer les connecteurs IoT](#).
- 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](#).
- Chargements manuels :
 - 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. Voir [Mettre à jour les détails d'un asset à l'aide d'un fichier 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](#).
 - Fichiers SCD – Chargez un fichier SCD (Substation Configuration Description) sur OT Security et gagnez en visibilité sur vos assets et la configuration CEI 61850, tout en bénéficiant d'informations sur la sécurité de votre environnement. Voir [Fichiers SCD](#).
 - Fichiers de projet Rockwell – Chargez des fichiers Rockwell .L5X pour créer des assets, affiner les détails des assets et établir des relations entre les assets dans des environnements isolés ou à visibilité limitée. Voir [Fichiers de projet Rockwell](#).

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.

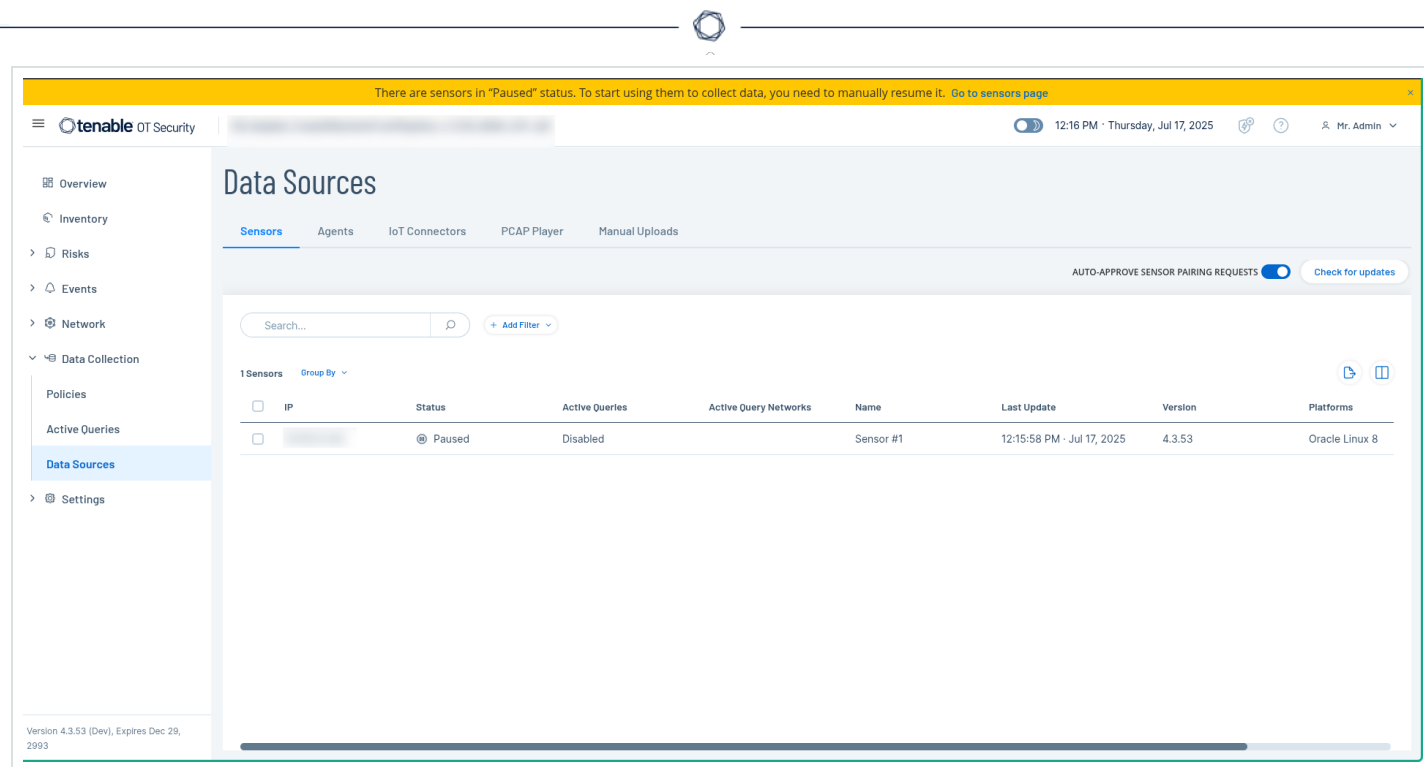
Remarque : les modèles de capteurs antérieurs à la version 2.214 n'apparaissent pas sur la page Capteurs ICP. Cependant, ils peuvent toujours être utilisés en mode non authentifié.

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

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité, Analyste sécurité, Opérateur de site, Lecture seule

Le tableau Capteurs affiche une liste de tous les capteurs de la version 2.214 et des versions ultérieures sur le système. Pour plus d'informations sur la personnalisation des tableaux, voir [Éléments de l'interface utilisateur de la console de gestion](#).



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

Rôle utilisateur OT Security requis : Administrateur

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.

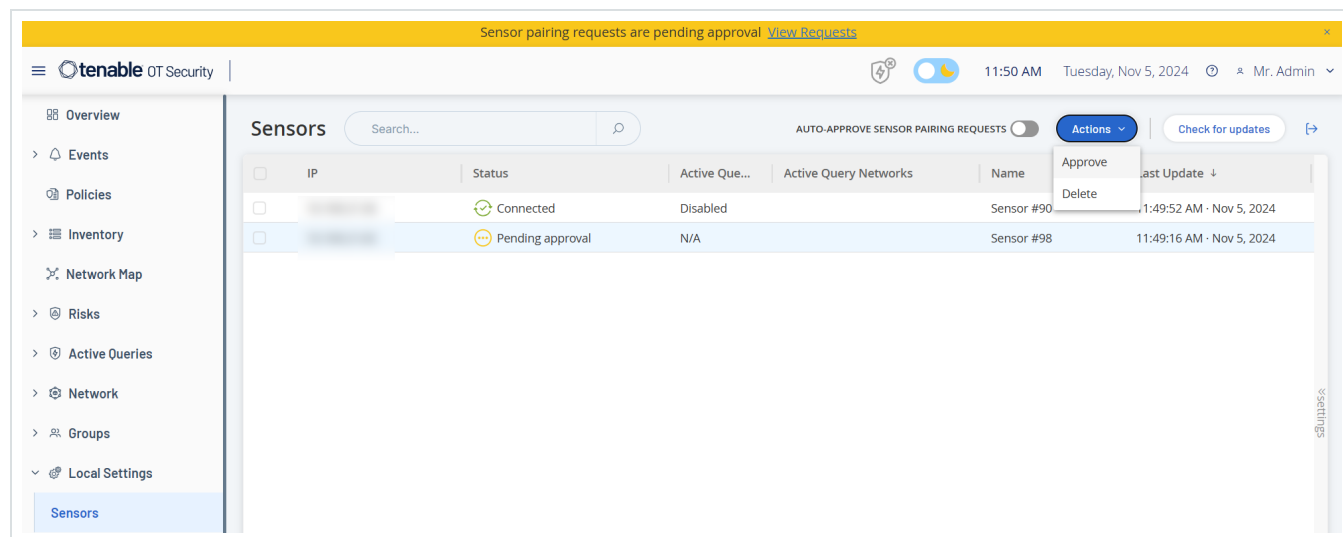
Pour approuver manuellement une demande entrante d'appairage des capteurs :

1. Sur la page Collecte de données > Sources de données, cliquez sur l'onglet Capteurs.

La page Capteurs apparaît.



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

Rôle utilisateur OT Security requis : Administrateur

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. Sur la page Collecte de données > Sources de données, cliquez sur l'onglet Capteurs.

La page Capteurs apparaît.

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.

Edit Sensor ×

NAME
Test3

Active Query Networks
ONE CIDR PER LINE

☒ Sensor active queries

Cancel Save

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.

Remarque : si le capteur fait partie d'un réseau dupliqué, l'adresse IP du réseau dupliqué apparaît dans la zone Réseaux de requêtes actives et ne peut être modifiée.

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

Rôle utilisateur OT Security requis : Administrateur

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.

Remarque : (pour les utilisateurs OT Security EM uniquement) 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 via un EM, placez le fichier ISO hors ligne de l'EM sous `/srv/tenablecore/offlineiso/tenable-offline-updates.iso` sur l'EM.

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 [Appairer le capteur](#).

Pour mettre à jour le capteur authentifié version 3.16 ou ultérieure avec l'ICP :

1. Sur la page Collecte de données > Sources de données, cliquez sur l'onglet 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.

Agents OT



Les agents OT sont des composants logiciels que vous pouvez installer sur des machines Windows distantes pour interroger et découvrir activement des assets OT Security dans des environnements où l'installation de capteurs n'est pas possible ni faisable. Les agents OT utilisent des requêtes actives pour scanner les réseaux dupliqués et les réseaux de requêtes actives répertoriés sous Réseaux surveillés. Cela permet à l'agent, qui s'exécute sur une passerelle Windows, une station de travail ingénieur ou une interface homme-machine (IHM), d'identifier les dispositifs OT/IoT critiques et les appareils intégrés sur le réseau.

Chaque asset OT découvert par l'agent OT est associé à cet agent spécifique en tant que source de découverte. Cela assure la traçabilité de l'identification des assets au sein de votre réseau.

Pour scanner les réseaux, installez et configurez d'abord l'agent OT. Les sections suivantes décrivent comment installer, configurer et exécuter des scans à l'aide de l'agent OT.

1. Télécharger l'agent OT
2. Installer l'agent OT
3. Configurer l'agent OT
4. Exécuter des scans

Afficher les agents OT

La page Agents OT sert de plateforme centrale pour superviser et configurer les agents que vous déployez pour surveiller votre réseau.

Pour accéder à la page Agents OT :

1. Dans le menu de navigation de gauche, cliquez sur Collecte de données > Sources de données.

La page Sources de données apparaît.

2. Cliquez sur l'onglet Agents.



La page Agents apparaît et affiche une liste de vos agents OT déployés.

Data Sources ⓘ

Sensors **Agents** IoT Connectors PCAP Player Manual Uploads

Search... ⓘ + Add Filter ▾

3 Agents Actions ▾ Group By ▾ ⓘ ⓘ

AUTO-APPROVE AGENT PAIRING REQUESTS ☒ AUTO-UPDATES ☐ Generate Pairing key

☐	IP/Host	Status	Last Scan Result	Active Query Networks	Agent Name	Host Asset	Scan Schedule	Last Scan
☐	██████████	Connected	Completed	192.168.0.0/16	OTAgent #1	AgentHost	Every 2 days at 01:09 PM	Feb 16, 202
☐	██████████	Scanning	Completed	10.0.0.0/8	OTAgent #2		Every 2 days at 01:09 PM	Feb 13, 202
☐	██████████	Scanning	Completed	10.0.0.0/8	OTAgent #3		Every 2 days at 01:09 PM	Jan 1, 2001

La page Agents contient les détails suivants :

Paramètre	Description
IP/Hôte	Adresse IPv4 de la machine sur laquelle l'agent OT est installé.
Statut	Le statut de l'agent : • Connecté • En suspens • Déconnecté • Configuration en attente • Approbation en attente • Préparation de la connexion • En attente de connexion • Mise à jour en cours • Scan en cours



Résultat du dernier scan	Le statut du dernier scan : Terminé ou Échec.
Réseaux de requêtes actives	Les segments réseau spécifiques ciblés par les agents OT dans le scan en cours.
Nom de l'agent	Nom unique attribué à l'agent OT.
Asset de l'hôte	Un lien direct vers la page des détails de l'asset hôte.
Planification du scan	La fréquence configurée pour le scan. La colonne affiche Désactivé s'il n'y a pas de planification.
Dernier scan	La date et l'heure auxquelles le dernier scan a été lancé.
Durée du dernier scan	Le temps nécessaire pour terminer le dernier scan.
Informations d'authentification	Les identifiants utilisés par les agents pour scanner les appareils.
Assets signalés	Le nombre d'assets détectés dans le scan.
Version de l'agent	La version de l'agent OT.
Version d'OTD	La version du moteur OT Discovery.
Système d'exploitation de l'hôte	Le système d'exploitation de la machine hôte.

Installer l'agent OT

Rôle utilisateur OT Security requis : Administrateur

Installez l'agent OT sur une machine Windows pour scanner les environnements OT.



Avant de commencer

- Téléchargez l'agent OT à partir du [portail des téléchargements Tenable](#).
- Assurez-vous de disposer des autorisations d'administrateur sur la machine Windows.

Remarque : les ports par défaut pour l'appairage et la connexion sont respectivement 443 et 28306. Pour plus d'informations sur les ports, voir [Considérations sur le pare-feu](#).

Pour installer l'agent OT :

1. Transférez le fichier d'installation (Tenable-OT-Agent-version.msi) sur la machine Windows.
2. Cliquez sur le fichier d'installation .msi pour ouvrir l'assistant d'installation.
3. Dans la fenêtre OT-Agent Setup Wizard (Assistant de configuration de l'agent OT), cliquez sur Next (Suivant).

La fenêtre Enter ICP Details (Saisir les détails de l'ICP) apparaît.

4. Sélectionnez l'une des options suivantes :

- **Utiliser une clé d'appairage**

Il s'agit de l'option par défaut. Si vous avez sélectionné cette option, effectuez les étapes suivantes :

1. Dans OT Security, accédez à Collecte de données > Sources de données.

La page Sources de données apparaît.

2. Cliquez sur l'onglet Agents.

La page Agents apparaît.



3. Dans le coin supérieur droit, cliquez sur Générer une clé d'appairage.

Le panneau Générer une clé d'appairage d'agents apparaît.

Data Sources

Sensors **Agents** IoT Connectors PCAP Player Manual Uploads

Search... + Add Filter

1 Agents Group By

☐	IP/Host	Status	Active Query Networks	Agent Name	Host Asset	Scan Schedule
☐		Connected		OTAgent #1		Disabled

Generate Agent Pairing key

Generate Key Get Key

A pairing key is a secure file that combines an API key, a certificate and the IP address of the ICP into a single object. It's used to quickly and securely register OT Agents to the ICP.

ICP IP/HOST

EXPIRATION PERIOD * 90 DAYS

DESCRIPTION *

Cancel Next

4. Dans la zone IP/Hôte de l'ICP, saisissez l'adresse IP ou le nom d'hôte de l'ICP.
5. Dans la zone déroulante Période d'expiration, conservez la valeur par défaut de 90 jours ou indiquez le nombre de jours après lequel la clé doit expirer.
6. Dans la zone Description, donnez une description de la clé.
7. Cliquez sur Suivant.

OT Security génère la clé d'appairage.

8. Cliquez sur le bouton  pour copier la clé d'appairage.
9. Cliquez sur Terminé.

OT Security referme le panneau.



10. Revenez à la machine hôte Windows.
11. Dans la zone Pairing Key (Clé d'appairage), collez la clé d'appairage que vous avez copiée à partir de l'ICP.



ICP Pairing Configuration



- ☒ Pair Using Pairing Key
- ☐ Pair Using Username And Password
- ☐ Pair Using API Secret

PAIRING KEY

The pairing key can be generated in the ICP under Data Collection
> Data Sources > Agents

Cancel

Submit



- Appairer à l'aide du nom d'utilisateur et du mot de passe

Si vous sélectionnez cette option, les champs pertinents apparaissent pour vous permettre de fournir les détails demandés pour l'ICP.

1. Dans la zone Nom d'hôte/adresse IP de l'ICP, saisissez le nom d'hôte ou l'adresse IP de l'ICP.
2. Dans la zone Nom d'utilisateur, indiquez votre nom d'utilisateur ICP.
3. Dans la zone Mot de passe, indiquez votre mot de passe ICP. Pour conserver un mot de passe enregistré, laissez ce champ vide.
4. Dans la zone Certificate Fingerprint (Empreinte du certificat), indiquez l'empreinte générée à partir de l'ICP.

L'empreinte se trouve dans l'ICP sous Paramètres > Configuration système > Certificats. Voir [Certificats](#).

5. Cliquez sur Envoyer.

- Appairer à l'aide du secret API

Si vous sélectionnez cette option, les champs pertinents apparaissent pour vous permettre de fournir les détails demandés pour l'ICP.

1. Dans la zone Nom d'hôte/adresse IP de l'ICP, saisissez le nom d'hôte ou l'adresse IP de l'ICP.
2. Dans la zone Clé secrète de l'API, indiquez la clé API générée à partir de l'ICP. Pour conserver une clé API existante, laissez ce champ vide.

Vous pouvez générer la clé API dans l'ICP sous Paramètres > Configuration



système > Clés API. Voir [Générer des clés API](#).

3. Cliquez sur Envoyer.

Remarque : la clé et les certificats d'appairage ne sont requis que pour le processus d'appairage. Une fois l'appairage terminé, vous pouvez supprimer la clé et le certificat d'appairage, si nécessaire.

5. Cliquez sur Next (Suivant).

La fenêtre Destination Folder (Dossier de destination) apparaît.

6. Dans la zone Install OT-Agent to: (Installer l'agent OT sur :), conservez la destination par défaut ou indiquez le chemin d'installation de l'agent OT et cliquez sur Next (Suivant).

7. Cliquez sur Install (Installer).

Le programme d'installation installe l'agent OT et le répertorie dans l'onglet Agents dans OT Security avec le statut Configuration en attente.

8. Cliquez sur Finish (Terminé) pour fermer le programme d'installation.

Remarque : en cas de problème d'appairage, vous pouvez utiliser l'option Repair (Réparer) dans l'assistant d'installation de l'agent OT pour ressaisir les détails de l'appairage.

9. Pour approuver automatiquement la demande d'appairage, cliquez pour activer l'option Approuver automatiquement les demandes d'appairage des agents.

Si cette option n'est pas activée, procédez comme suit :

- Faites un clic droit sur l'agent OT nouvellement ajouté.

Un menu apparaît.

- Cochez la case à côté de l'agent OT.

OT Security active le menu Actions > Approuver.

10. Cliquez sur Approuver.



OT Security approuve l'appairage de l'agent et fait passer le statut à Configuration en attente.

Data Sources 

Sensors **Agents** IoT Connectors PCAP Player Manual Uploads

Search...  [+ Add Filter](#)

2 Agents [Actions](#) [Group By](#)  

AUTO-APPROVE AGENT PAIRING REQUESTS ☒ AUTO-UPDATES ☒ [Generate Pairing key](#)

☐	IP/Host	Status	Last Scan Result	Active Query Networks	Agent Name	Host Asset
☐		Connected			OTAgent #2	
☐		Scanning	Completed		OTAgent #1	AgentHost

Remarque : avant d'exécuter l'agent OT, assurez-vous que sa configuration est complète, même si l'option Approuver automatiquement les demandes d'appairage des agents est activée.

Que faire ensuite

Configurer l'agent OT

Configurer l'agent OT

Rôle utilisateur OT Security requis : Administrateur

Après avoir installé l'agent OT, configurez-le pour définir son nom, spécifier les réseaux qu'il scanne et définir une planification pour les requêtes actives.

Avant de commencer

- Installez l'agent OT.

Pour configurer l'agent OT :



1. Dans l'onglet Agents, effectuez l'une des actions suivantes :

- Faites un clic droit sur l'agent OT nouvellement ajouté.

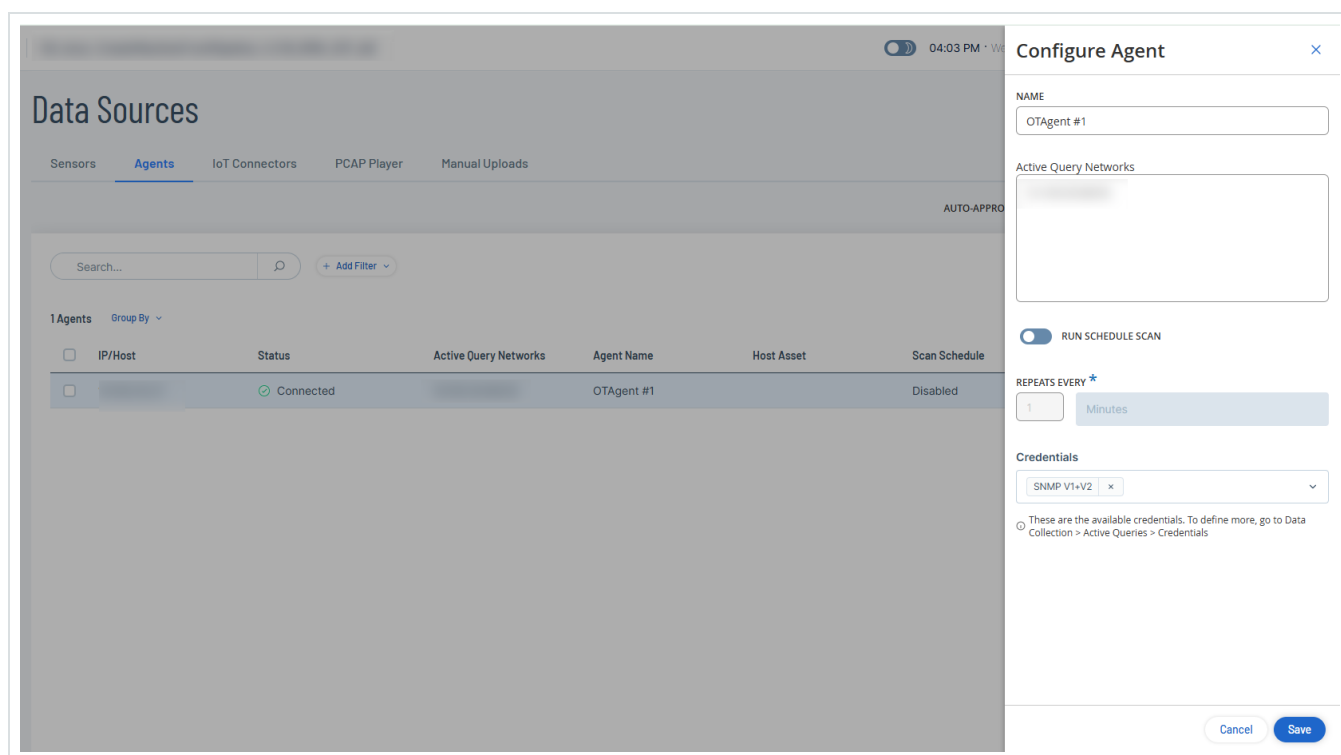
Un menu apparaît.

- Cochez la case à côté de l'agent OT.

OT Security active le menu Actions > Configurer.

2. Cliquez sur Configurer.

Le panneau Configurer l'agent apparaît.



3. Dans la zone Nom, saisissez le nom de l'agent.

4. Dans la zone Requête active, indiquez les adresses IP des réseaux à scanner.



Remarque : l'agent OT scanne uniquement les adresses IP des réseaux de requêtes actives qui font partie des réseaux surveillés (Configuration de l'environnement > Définitions de réseau > Réseaux surveillés).

5. (Facultatif) Pour activer les scans planifiés, cliquez sur le curseur Exécuter un scan planifié.

OT Security active la zone déroulante Répéter chaque.

6. (Facultatif) Indiquez les minutes, les heures, les jours ou les semaines selon les besoins.
7. Dans le menu déroulant Informations d'authentification, sélectionnez les informations d'authentification requises.

Remarque : seules les informations d'authentification que vous créez dans Requêtes actives > Informations d'authentification apparaissent dans cette liste. Pour plus d'informations, voir [Informations d'authentification](#).

8. Cliquez sur Enregistrer.

OT Security met à jour le statut de l'agent OT pour qu'il passe à Connecté.

Que faire ensuite

Exécuter des scans

Exécuter des scans à l'aide d'un agent OT

Rôle utilisateur OT Security requis : Administrateur

Lorsque vous lancez un scan d'agent, il déclenche les requêtes actives suivantes :

- Découverte : détecte les assets en direct sur le réseau surveillé.
- Vérification des ports ouverts : scanne les ports les plus fréquemment utilisés des clients de requête actives.



- Enrichissement initial : identifie les assets nouvellement découverts avec le moteur de prise d'empreinte numérique dynamique (DFE).
- Requêtes OT : collecte des informations sur les appareils, notamment l'état de fonctionnement du PLC et d'autres modules connectés au fond de panier.
- Requêtes IT : obtient les données des appareils informatiques surveillés par OT Security.

Pour plus d'informations, voir [Gérer les requêtes actives](#).

Pour exécuter un scan avec agent :

1. Dans l'onglet Sources de données > Agents, effectuez l'une des actions suivantes :

- Faites un clic droit sur l'agent OT nouvellement ajouté.

Un menu apparaît.

- Cochez la case à côté de l'agent OT.

OT Security active le bouton Actions dans l'en-tête.

Remarque : pour lancer des scans pour plusieurs agents, sélectionnez plus d'un agent OT, puis cliquez sur Actions en bloc > Scanner maintenant.

2. Cliquez sur Actions > Scanner maintenant.

Le statut de l'agent passe à Scan et le scan des réseaux spécifiés commence. Une fois le scan terminé, cliquez sur le lien dans la colonne Assets signalés du tableau des agents pour afficher les résultats filtrés sur la page Inventaire.

Abandonner un scan

Rôle utilisateur OT Security requis : Administrateur

Si vous devez arrêter un scan en cours :



1. Dans l'onglet Sources de données > Agents, effectuez l'une des actions suivantes :

- Effectuez un clic droit sur l'agent et sélectionnez Abandonner le scan.
- Cochez la case à côté de l'agent, puis cliquez sur Actions > Abandonner le scan.

OT Security interrompt le scan et la colonne Résultat du dernier scan affiche Échec.

Mettre à jour l'agent OT

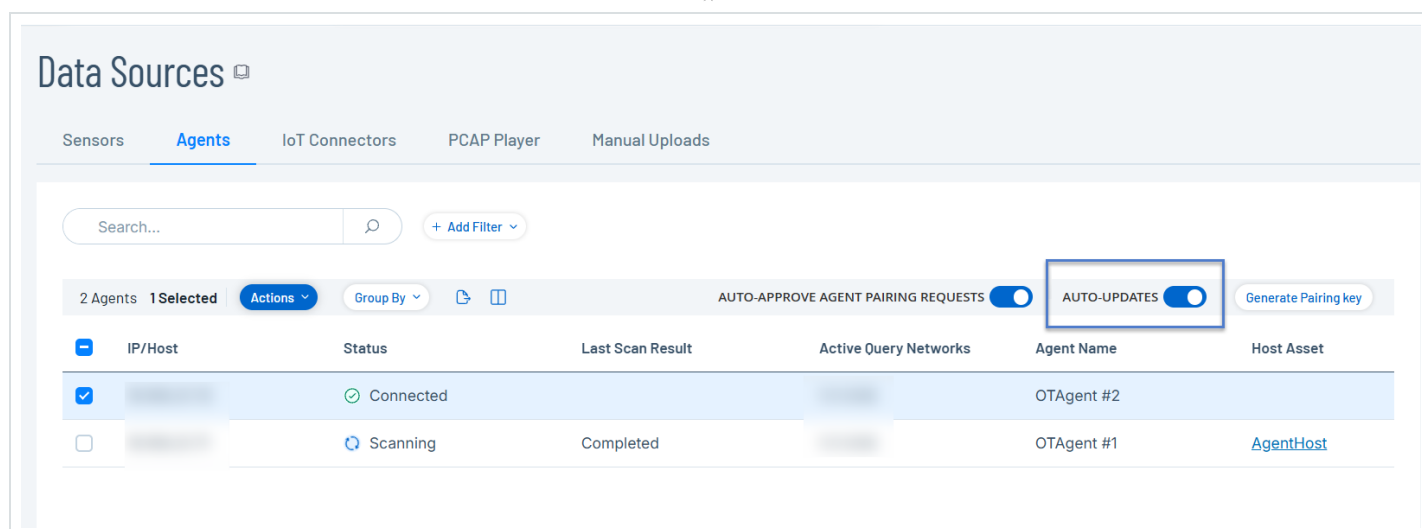
Rôle utilisateur OT Security requis : Administrateur

Rôle utilisateur **OT Security** requis pour charger le fichier : Administrateur, Superviseur et Analyste sécurité

Les agents OT utilisent le moteur OT Discovery (OTD) pour scanner activement votre environnement. Vous pouvez mettre à jour les versions du moteur OT Discovery manuellement ou automatiquement à partir de la page Agents.

Mises à jour automatiques

Pour mettre à jour automatiquement les versions OTD lorsqu'une mise à jour de l'ICP est disponible, activez le curseur Mises à jour automatiques. Le curseur est désactivé par défaut. Lorsque vous activez les mises à jour automatiques, OT Security envoie automatiquement la dernière version du moteur OTD aux agents connectés chaque fois qu'une nouvelle version est disponible.



Mises à jour manuelles

Utilisez les mises à jour manuelles lorsque vous devez mettre à jour le moteur OTD entre deux versions officielles ou appliquer une mise à jour à plusieurs agents simultanément.

Avant de commencer

- Chargez le fichier OTD dans la section Configuration système > Mises à jour > Mise à jour du moteur OT Discovery (OTD) comme mentionné dans [Mise à jour du moteur OT Discovery \(OTD\)](#).
- Vérifiez que l'agent OT est en ligne et que le statut est Connecté.

Pour mettre à jour manuellement le moteur OTD :

1. Dans la barre de navigation de gauche, cliquez sur Sources de données > Agents.

L'onglet Agents apparaît.

2. Pour mettre à jour les agents, utilisez l'une des méthodes ci-dessous :

- Effectuez un clic droit sur l'agent que vous souhaitez mettre à jour.

Un menu apparaît.



- Cochez la case en regard de l'agent que vous souhaitez mettre à jour.

OT Security active le menu Actions.

Remarque : pour mettre à jour plusieurs moteurs OTD simultanément, sélectionnez plusieurs agents, puis cliquez sur Actions en bloc > Mettre à jour.

3. Cliquez sur Actions > Mettre à jour.

La boîte de dialogue Mettre à jour la version d'OTD apparaît.

4. Cliquez sur Mettre à jour pour confirmer.

OT Security met à jour les moteurs OT Discovery vers la dernière version.

Supprimer un agent OT

Rôle utilisateur OT Security requis : Administrateur

La désinstallation de l'agent OT de la machine Windows fait passer le statut de l'agent à Déconnecté dans OT Security.

Pour supprimer un agent OT :

1. Sur la machine Windows, ouvrez le programme d'installation et cliquez sur Supprimer.
2. Suivez les étapes de l'assistant pour désinstaller l'agent.

L'agent OT est désinstallé de la machine Windows.

3. Accédez à l'onglet Sources de données > Agents dans OT Security.

OT Security met à jour le statut de l'agent pour qu'il passe à l'état Déconnecté.

4. Effectuez l'une des actions suivantes :



- Faites un clic droit sur l'agent OT nouvellement ajouté.

Un menu apparaît.

- Cochez la case à côté de l'agent OT.

OT Security active le menu Actions > Supprimer.

Remarque : pour supprimer plusieurs agents OT simultanément, sélectionnez-les, puis cliquez sur Actions en bloc > Supprimer.

5. Cliquez sur Supprimer.

OT Security supprime l'agent OT.

Remarque : si des réseaux dupliqués sont associés à l'agent, vous devez d'abord les supprimer avant de supprimer l'agent.

Installer des agents OT à l'aide de la CLI

Rôle utilisateur OT Security requis : Administrateur

Utilisez les commandes de la CLI pour installer l'agent OT avec la clé d'appairage, les informations d'authentification de l'ICP ou la clé API. Vous pouvez également désinstaller l'agent OT via la CLI.

Avant de commencer

- Téléchargez le programme d'installation de l'agent OT à partir du portail des téléchargements Tenable.

Pour installer l'agent OT à l'aide d'une clé d'appairage, exécutez la commande suivante :

```
msiexec.exe /i "<OtAgentInstaller.msi>" /qn PAIRING_KEY="<PairingKey>"
```

Où :



- `OtAgentInstaller.msi` est le fichier d'installation.
- `IpAddress` est l'adresse IP de l'ICP.
- `APIKey` est la clé API générée à partir de l'ICP.
- `CertFingerprint` est le certificat généré à partir de l'ICP.
- `FullDirPath` est le chemin d'accès du répertoire d'installation.

```
msiexec.exe /i "OtAgentInstaller.msi" /qn ICP_ADDRESS="XX.XXX.XX.XX" ICP_APIKEY="xxxxxxxxxxxxxxxxxxxxx_
xxxxxxxxxx=" ICP_FINGERPRINT="XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX
```

[illegible]

```
msiexec.exe /x "<OtAgentInstaller.msi>" /qn
```

- `OtAgentInstaller.msi` est le fichier d'installation.

Activez ou désactivez simultanément des scans planifiés pour plusieurs agents OT à l'aide de l'option Actions en bloc.



Avant de commencer

- Assurez-vous que les agents OT sont en ligne et que la mention Connecté s'affiche bien dans la colonne Statut.

Pour effectuer des actions en bloc sur les scans d'agent planifiés :

- Dans le tableau Agents, sélectionnez plusieurs agents OT pour votre scan.

OT Security active le bouton Actions en bloc dans l'en-tête.

- Sélectionnez l'une des options suivantes :

Option d'action en bloc	Description
Activer un scan planifié	Sélectionnez cette option pour activer les scans d'agent planifiés. Le scan planifié s'exécute toutes les minutes par défaut.
Désactiver un scan planifié	Sélectionnez cette option pour désactiver les scans d'agent planifiés.
Définir un scan planifié	- Pour configurer un scan planifié, cliquez sur Actions en bloc > Définir un scan planifié. Le panneau Définir la planification apparaît. - Dans la zone Répéter chaque, sélectionnez la fréquence à laquelle vous souhaitez répéter le scan. - Indiquez les minutes, les heures, les jours ou les semaines selon les besoins. Remarque : la planification que vous spécifiez ici remplace toutes



les planifications existantes pour les agents.

d. Cliquez sur Enregistrer.

Comparaison de l'agent OT et du capteur

Capacité	Agent OT	Capteur
Cas d'utilisation cible	Pour les évaluations, les PoV et les environnements OT flexibles basés sur Windows.	Pour les déploiements complets où l'inspection et le contrôle du trafic sont requis.
Type de déploiement	Installé sur des machines Windows (IHM, poste de travail, jumpbox)	Installé sur du matériel ou une VM, basé sur le système d'exploitation Tenable Core.
Dépendance ICP	Nécessite l'appairage avec l'ICP, mais peut fonctionner indépendamment pour collecter des données (nécessite une assistance + des scripts)	Entièrement dépendant de l'ICP
Complexité de l'installation	Léger et flexible ; peut être déployé en bloc	Nécessite un déploiement physique ou virtuel ainsi qu'une configuration
Flux de données vers l'ICP	Résultats envoyés après la fin du scan	Flux de données continu (actif + passif)
Type d'exécution	Scans actifs uniquement	Scans actifs et passifs



Interface utilisateur de gestion des scans	Géré à partir de la page Agents uniquement	Requêtes déclenchées à partir des pages Requête active et Inventaire.
Intégration Nessus	Non prise en charge	Les requêtes Nessus peuvent être acheminées via les capteurs.
Mise en correspondance des vulnérabilités	Utilise Nessus intégré à l'ICP pour la mise en correspondance.	Utilise Nessus intégré à l'ICP pour la mise en correspondance et les scans actifs.
Planification des scans	Prise en charge (ponctuelle ou récurrente).	Prise en charge (ponctuelle ou récurrente).
Visibilité des assets	Assets affichés dans l'inventaire mais non interrogeables à partir de l'inventaire.	Assets entièrement interrogeables à partir de l'inventaire.
Portée des informations d'authentification	Utilise des informations d'authentification dédiées configurés par agent.	Utilise les informations d'authentification globales de l'ICP.
Prise en charge des réseaux dupliqués	Pris en charge	Pris en charge
Respect des restrictions globales	Non pris en charge dans la version 4.3	Pris en charge



Méthode d'appairage	Clé d'appairage (clé API + certificat + adresse IP de l'ICP dans un seul blob).	Nécessite une clé API, un certificat ou une adresse IP configurée manuellement.
Matériel	Aucun - s'exécute sur les machines Windows existantes.	Matériel dédié ou VM requise.
Capture de trafic passive	Non prise en charge	Entièrement prise en charge

Interface de l'agent OT Tenable

Rôle utilisateur OT Security requis : Administrateur

Les agents OT Tenable sont des composants logiciels que vous pouvez installer sur des machines Windows distantes pour interroger et découvrir activement des assets OT Security dans des environnements où l'installation de capteurs n'est pas possible ni faisable.

Les agents OT utilisent des requêtes actives pour scanner les réseaux dupliqués et les réseaux de requêtes actives répertoriés sous Réseaux surveillés. Cela permet à l'agent, qui s'exécute sur une passerelle Windows, une station de travail ingénieur ou une interface homme-machine (IHM), d'identifier les dispositifs OT/IoT critiques et les appareils intégrés sur le réseau.

Pour télécharger et installer l'agent OT Tenable, suivez les étapes de la documentation sur les agents OT.

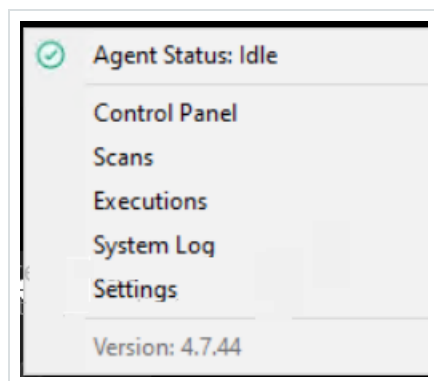
Accéder à l'agent depuis la barre d'état système

L'agent OT Tenable s'exécute en arrière-plan et reste accessible depuis la barre d'état système de Windows.



1. Dans la barre des tâches de Windows, cliquez sur l'icône de la barre d'état système (coin inférieur droit de l'écran).
2. Cliquez sur l'icône Agent OT Tenable.

Le menu contextuel qui apparaît indique le statut actuel de l'agent et les options suivantes :



- Statut de l'agent : affiche l'état actuel de l'agent (par exemple, « Inactif » ou « Actif »).
 - **Panneau de contrôle** : ouvre le dashboard Panneau de contrôle.
 - **Scans** : ouvre la page Scans.
 - **Exécutions** : ouvre la page Exécutions.
 - **Journal système** : ouvre la page Journal système.
 - **Paramètres** : ouvre la page Paramètres.
 - Version : affiche la version installée de l'agent.
3. Cliquez sur n'importe quel élément du menu pour accéder directement à la section correspondante de l'interface de l'agent.

Panneau de contrôle

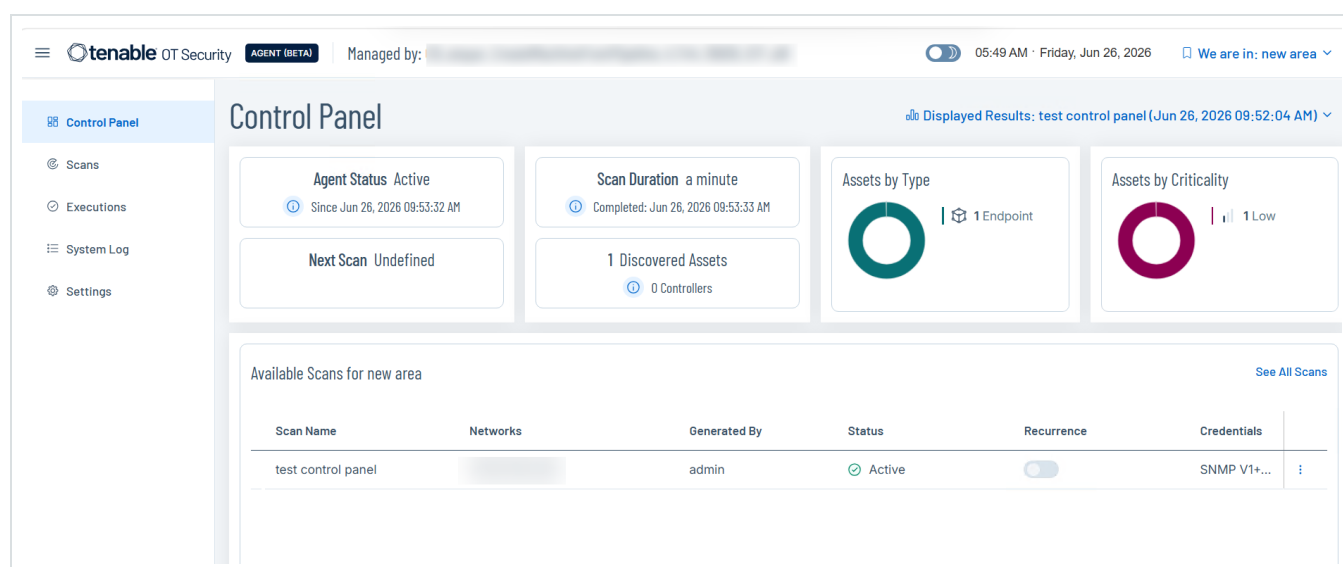


Le panneau de contrôle est le dashboard principal de l'agent OT Tenable. Il donne un résumé en temps réel du statut de l'agent, de l'activité de scan récente et des assets découverts dans la zone actuellement sélectionnée.

Pour accéder au Panneau de contrôle :

- Dans le volet de navigation de gauche, cliquez sur Panneau de contrôle.

La page Panneau de contrôle apparaît.



Le dashboard charge les résultats du scan le plus récent dans la zone active. La zone actuelle et l'horodatage de l'instantané apparaissent dans le coin supérieur droit.

En l'absence de scans, la page Panneau de contrôle affiche des options permettant de télécharger des fichiers de scan ou d'appairer une ICP.



Control Panel



Welcome to Tenable OT Agent!

How would you like to proceed?

Is it a portable agent for covering remote network areas?

[Upload Scan Files](#)

OR

Is this agent stationed in a network for online use?

[Online Pair with ICP](#)

Dashboard

La ligne supérieure de la page Panneau de contrôle affiche les widgets suivants :

- « Statut de l'agent » indique si l'agent OT Security est actif ou inactif, ainsi que l'horodatage de son dernier changement de statut. Un statut actif signifie que l'agent est en cours d'exécution et que vous pouvez l'utiliser pour effectuer des scans.
- « Durée du scan » indique la durée du scan le plus récent et l'heure à laquelle il s'est terminé. Cela vous permet d'évaluer les performances des scans au fil du temps.
- « Assets par type » affiche un graphique en anneau des assets découverts, triés par catégorie (par exemple, endpoints, contrôleurs). Chaque segment est accompagné du nombre d'assets.
- « Assets par criticité » affiche un graphique en anneau des assets découverts, triés par leur niveau de criticité (par exemple, faible, moyen, élevé, critique).
- « Assets découverts » affiche le nombre total d'assets détectés lors du dernier scan.



- « Prochain scan » indique quand le prochain scan planifié doit s'exécuter selon sa configuration. Si aucune récurrence n'est configurée, la mention « Non défini(e) » s'affiche.

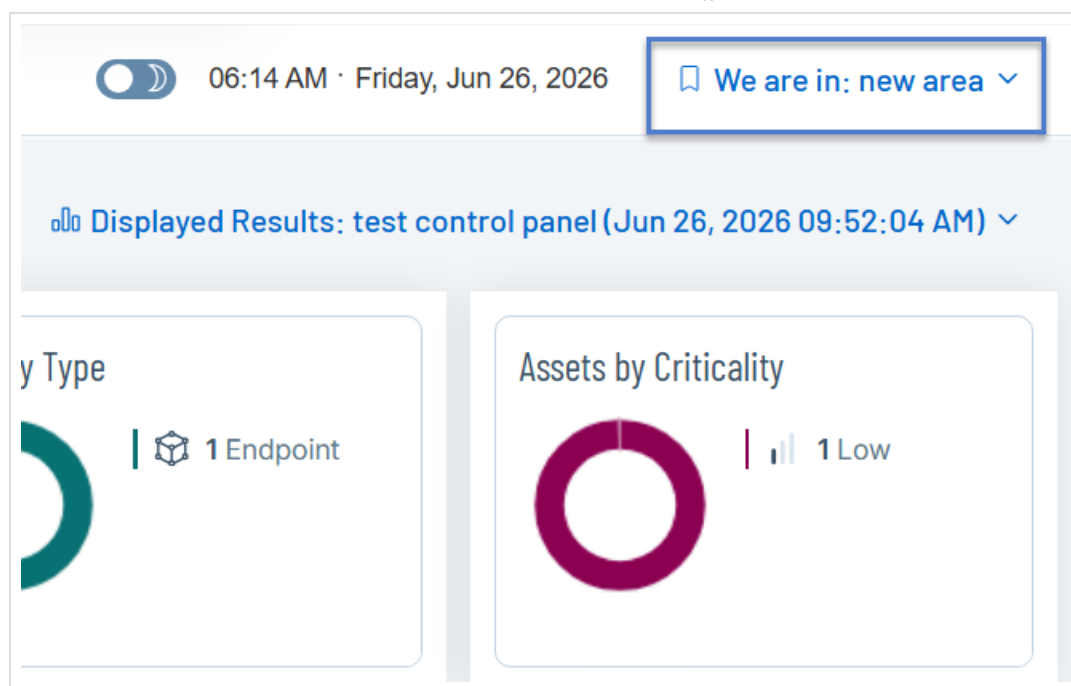
Scans disponibles

Le tableau Scans disponibles répertorie tous les scans configurés pour la zone actuelle et contient les détails suivants :

Colonne	Description
Nom du scan	Nom attribué au scan.
Réseaux	Plage d'adresses IP ou sous-réseau ciblés par le scan.
Généré par	Utilisateur ayant créé le scan.
Statut	Le statut du scan, actif ou inactif.
Récurrence	Curseur indiquant si le scan s'exécute selon une planification définie.
Informations d'authentification	Profil d'informations d'authentification utilisé pour le scan (par exemple, SNMP V1).
Voir tous les scans	Pour afficher tous les scans dans toutes les zones, cliquez sur Voir tous les scans dans le coin supérieur droit du tableau.
⋮	Pour accéder aux options d'un scan spécifique (Exécuter maintenant ou Abandonner), cliquez sur le bouton ⋮ .

Changer de zone réseau

En haut à droite de l'en-tête, le sélecteur de zone (« Nous sommes dans : zone ») contrôle les données de la zone affichée. Cliquez dessus pour passer à une autre zone. Le panneau de contrôle, la liste des scans et les résumés d'assets s'actualisent en fonction de la zone sélectionnée.



Scans

La page Scans répertorie tous les scans configurés pour la zone actuellement sélectionnée. Vous pouvez utiliser la page Scans pour charger des fichiers de scan à partir de l'ICP. Affichez, exécutez et regroupez les scans à partir de cette page.

Pour accéder à la page Scans :

- Dans le volet de navigation de gauche, cliquez sur Scans.

La page Scans apparaît.

tenable OT Security AGENT (BETA) Managed by: 06:16 AM · Friday, Jun 26, 2026 We are in: new area

Control Panel

Scans

Scans

Search... + Add Filter

1 Scans Actions Group By

Upload Scan File(s)

Scan Name	Networks	Generated By	Status	Recurrence	Credentials
test control panel		admin	Active		SNMP V1+V2 (Sn...



La page « Scans » contient les détails suivants :

Colonne	Description
Rechercher et filtrer	Utilisez la barre de recherche pour rechercher des scans par nom. Cliquez sur + Ajouter un filtre et sélectionnez des critères de filtrage dans la liste déroulante.
Grouper par	Cliquez sur Grouper par pour organiser la liste des scans selon un attribut spécifique, comme le statut ou le réseau.
Nom du scan	Nom attribué au scan.
Réseaux	Plage d'adresses IP ou sous-réseau ciblés par le scan.
Généré par	Utilisateur ayant créé le scan.
Statut	Le statut du scan, actif ou inactif.
Récurrence	Curseur indiquant si le scan s'exécute selon une planification définie.
Informations d'authentification	Profil d'informations d'authentification utilisé pour le scan (par exemple, SNMP V1).
Exporter	Cliquez sur le bouton  pour exporter les données des scans au format CSV.
Colonnes affichées	Cliquez sur le bouton  pour inclure ou exclure des colonnes du tableau des scans.

Charger les fichiers de scan

Pour importer la configuration de scan ou le fichier de scan OTD à partir de l'ICP, cliquez sur Charger le(s) fichier(s) de scan dans le coin supérieur droit et sélectionnez le fichier à charger.



Pour créer des scans OTD, voir [Définir le scan OT Discovery](#). Le fichier de scan OTD possède l'extension .otds.

Exécuter des scans

Pour exécuter des scans :

1. Dans le tableau « Scans », effectuez l'une des opérations suivantes :

- Sélectionnez le scan que vous souhaitez exécuter.

L'agent Tenable OT active le menu Actions.

2. Cliquez sur Exécuter maintenant.

L'agent Tenable OT exécute le scan. Le statut devient « En cours d'exécution ».

Remarque : pour arrêter un scan, effectuez un clic droit dessus et cliquez sur Abandonner.

Exécutions

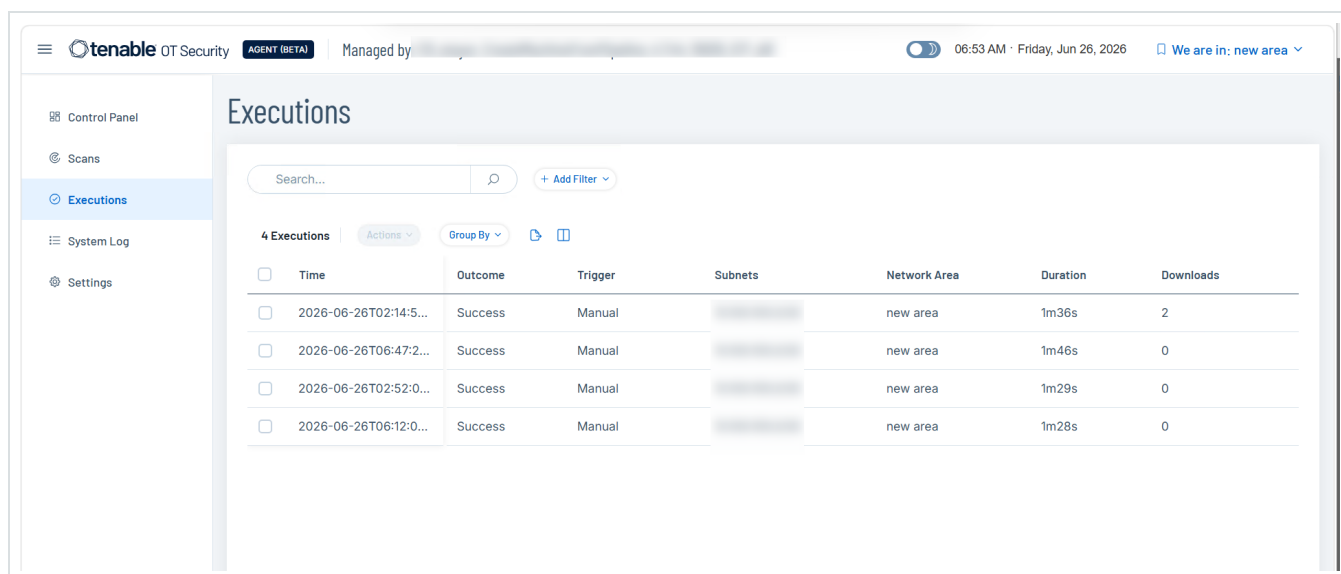
La page Exécutions affiche un journal de toutes les exécutions de scan pour la zone réseau actuellement sélectionnée. Utilisez-la pour consulter les résultats des scans passés et la durée des scans, et pour télécharger les résultats.

Pour accéder à la page Exécutions :



- Dans le volet de navigation de gauche, cliquez sur Exécutions.

La page Exécutions apparaît.



Le tableau « Exécutions » comprend les informations suivantes :

Colonne	Description
Rechercher et filtrer	Utilisez la barre de recherche pour retrouver des exécutions par mot-clé. Cliquez sur + Ajouter un filtre et sélectionnez des critères de filtrage dans la liste déroulante.
Grouper par	Cliquez sur Grouper par pour organiser les exécutions selon un attribut spécifique, comme le résultat ou la zone de réseaux.
Date/Heure	La date et l'heure auxquelles l'exécution a commencé.
Résultat	Le résultat de l'exécution. Par exemple, Réussite ou Échec.
Déclencheur	Mode de lancement du scan : manuel ou planifié.
Sous-réseaux	La plage d'adresses IP scannée au cours de cette exécution.



Zone de réseaux	La zone de réseaux spécifiée dans le fichier de configuration du scan.
Durée	Le temps nécessaire pour terminer le scan.
Téléchargements	Le nombre de fois que le fichier de résultats a été téléchargé.

Télécharger les résultats du scan

Téléchargez les résultats du scan pour les charger sur l'ICP à des fins d'analyse.

Pour télécharger les résultats du scan :

1. Dans le tableau « Exécutions », effectuez l'une des opérations suivantes :

- Sélectionnez le résultat de scan dont vous souhaitez télécharger le fichier de résultats.

L'agent OT Tenable active le menu Actions, qui propose l'option Télécharger le fichier de résultats.

- Effectuez un clic droit sur le résultat de scan dont vous souhaitez télécharger le fichier de résultats.

2. Cliquez sur Télécharger le fichier de résultats.

L'agent OT Tenable télécharge le fichier de résultats. Chargez ce fichier sur l'ICP pour procéder à une analyse plus approfondie. Le fichier de résultats possède l'extension .otdr.

Voir [Charger les résultats](#).

Journal système

La page Journal système contient un enregistrement chronologique de l'activité de l'agent OT Tenable. Il capture les événements générés par le système (démarrages et achèvements de scans, téléchargements de fichiers et changements de zone) pour vous informer sur l'ensemble des actions réalisées dans le produit.

Pour accéder à la page Journal système :



- Dans le volet de navigation de gauche, cliquez sur Journal système.

La page Journal système apparaît.

Time	Event	Entry ID
02:10:24 PM · Jun 26, 20...	Scan results downloaded — 1 execution(s), file: otd_scan_result_CB_a...	System
01:49:09 PM · Jun 26, 20...	Scan 'test control panel' completed (1m46s)	System
01:47:23 PM · Jun 26, 20...	Manual scan 'test control panel' started — networks: [redacted]	System
01:13:36 PM · Jun 26, 20...	Scan 'test control panel' completed (1m28s)	System
01:12:09 PM · Jun 26, 20...	Manual scan 'test control panel' started — networks: [redacted]	System
12:49:41 PM · Jun 26, 20...	Network area switched from 'Global' to 'new area' — 1 scan(s) in scope	System

Le tableau « Journal système » contient les détails suivants :

Colonne	Description
Rechercher et filtrer	Utilisez la barre de recherche pour retrouver des entrées par mot-clé. Cliquez sur + Ajouter un filtre et sélectionnez des critères de filtrage dans la liste déroulante.
Grouper par	Cliquez sur Grouper par pour organiser les entrées de journal selon un attribut spécifique, tel que l’ID d’entrée ou le type d’événement.
Événement	Description de l'activité. Par exemple, un scan terminé, un démarrage manuel de scan, le téléchargement de résultats de scan ou une modification de la zone réseau.
ID d'entrée	Source de l’événement.
Exporter	Cliquez sur le bouton  pour exporter les données des scans au format CSV.
Colonnes affichées	Cliquez sur le bouton  pour inclure ou exclure des colonnes du tableau des scans.



Paramètres

Utilisez la page Paramètres pour configurer le site de gestion, la connexion ICP et les préférences de localisation de l'agent OT Tenable.

Gérer le site

Affiche le site auquel l'agent est actuellement associé. Les fichiers de scan, les actions et les données d'exécution sont ceux du site actuellement sélectionné. Si vous utilisez cet agent comme scanner portable, sélectionnez le site sur lequel vous travaillez actuellement avant d'exécuter des scans.

Cliquez sur **Changer de site de gestion** pour modifier le site actif. Vous pouvez changer de site de gestion à tout moment à l'aide de ce paramètre.

Appairage en ligne de l'ICP

Établissez une connexion en ligne entre l'agent OT Tenable et l'ICP. Lorsqu'elle est appairée en ligne, l'ICP gère l'activité de l'agent.

Cliquez sur **Appairer l'ICP** pour lancer le processus d'appairage en ligne. Pour utiliser l'agent hors ligne après l'appairage, vous devez d'abord le déconnecter de l'ICP.

Settings

Managing Site:

Switch Managing Site

If you are using this agent as a portable scanner, select the site you're currently working under. All scan files, actions and execution data apply only to the currently selected site. You can switch the managing site at any time from here.

ICP Online Pairing

Pair ICP

Set up an online connection with the ICP. When an agent is paired online, its activity is managed by the ICP. To regain control over it and use it offline, it is required to disconnect it.

Localization

Edit

Language

English (English)



Pour procéder à l'appairage à l'aide d'une clé d'appairage :

1. Cliquez sur Appairer l'ICP.

La boîte de dialogue Configuration de l'appairage ICP apparaît.

2. Sélectionnez Appairer à l'aide de la clé d'appairage.



ICP Pairing Configuration

☒ Pair Using Pairing Key

☐ Pair Using Username And Password

☐ Pair Using API Secret

PAIRING KEY

The pairing key can be generated in the ICP under Data Collection
> Data Sources > Agents

Cancel

Submit

3. Dans l'ICP, accédez à Collecte de données > Sources de données > Agents et générez une clé d'appairage.
4. Collez la clé d'appairage dans la zone Clé d'appairage.



5. Cliquez sur Envoyer.

Pour procéder à l'appariage à l'aide du nom d'utilisateur et du mot de passe :

1. Cliquez sur Appairer l'ICP.

La boîte de dialogue Configuration de l'appariage ICP apparaît.

2. Sélectionnez Appairer à l'aide du nom d'utilisateur et du mot de passe.



ICP Pairing Configuration

☐ Pair Using Pairing Key

☒ Pair Using Username And Password

☐ Pair Using API Secret

HOSTNAME/IP OF THE ICP *

USERNAME *

PASSWORD *

Leave empty to keep existing password 

ICP CERTIFICATE FINGERPRINT

The fingerprint can be found in the ICP under Settings > System Configuration > Certificates

Cancel

Submit

3. Dans la zone Nom d'hôte/adresse IP de l'ICP, saisissez le nom d'hôte ou l'adresse IP de l'ICP.
4. Dans la zone Nom d'utilisateur, indiquez votre nom d'utilisateur ICP.



5. Dans la zone Mot de passe, indiquez votre mot de passe ICP. Pour conserver un mot de passe enregistré, laissez ce champ vide.

6. Dans la zone Empreinte du certificat de l'ICP, indiquez l'empreinte du certificat de l'ICP.

L'empreinte se trouve dans l'ICP sous Paramètres > Configuration système > Certificats. Pour plus d'informations, voir [Certificats](#).

7. Cliquez sur Envoyer.

Pour procéder à l'appairage à l'aide d'un secret API :

1. Cliquez sur Appairer l'ICP.

La boîte de dialogue Configuration de l'appairage ICP apparaît.

2. Sélectionnez Appairer à l'aide du secret API.



ICP Pairing Configuration

☐ Pair Using Pairing Key

☐ Pair Using Username And Password

☒ Pair Using API Secret

HOSTNAME/IP OF THE ICP *

API SECRET *

The API key can be generated in the ICP under Settings > System Configuration > API Keys

Leave empty to keep existing API key 

ICP CERTIFICATE FINGERPRINT

The fingerprint can be found in the ICP under Settings > System Configuration > Certificates

Cancel

Submit

3. Dans la zone Nom d'hôte/adresse IP de l'ICP, saisissez le nom d'hôte ou l'adresse IP de l'ICP.



4. Dans la zone Clé secrète de l'API, saisissez la clé API. Pour conserver une clé API existante, laissez ce champ vide.

Vous pouvez générer la clé API dans l'ICP sous Paramètres > Configuration système > Clés API. Pour plus d'informations, voir [Générer des clés API](#).

5. Dans la zone Empreinte du certificat de l'ICP, saisissez l'empreinte du certificat de l'ICP.

L'empreinte se trouve dans l'ICP sous Paramètres > Configuration système > Certificats. Pour plus d'informations, voir [Certificats](#).

6. Cliquez sur Envoyer.

Localisation

Affiche le paramètre de langue actuel de l'interface. La valeur par défaut est « Anglais (anglais) ».

Pour modifier la langue d'affichage :

1. Dans la section Localisation, cliquez sur Modifier.
2. Sélectionnez la langue de votre choix.
3. Cliquez sur Enregistrer.

Gérer les connecteurs IoT

Rôle utilisateur OT Security requis : Administrateur, Superviseur

OT Security vous permet de mapper tous les appareils IoT (Internet des objets) gérés avec leur serveur d'application correspondant en configurant le moteur de connecteurs IoT et en synchronisant les assets à partir du serveur d'application spécifique.

Dans l'exemple d'une caméra IP, vous pouvez voir le serveur du système de gestion vidéo (VMS) qui la gère. Sur la page Inventaire OT Security, accéder au serveur de l'application VMS affiche toutes les caméras qu'il gère sur la page Inventaire > Assets associés.



Remarque : par défaut, lors de l'importation d'assets à partir d'un connecteur IoT, OT Security importe l'adresse IP avec l'adresse MAC des appareils. Pour importer uniquement l'adresse MAC, accédez à Paramètres > Configuration de l'environnement > Paramètres des assets et désactivez l'option Récupérer une adresse IP pour les assets IoT.

Configuration requise pour l'IoT Connector Agent

Catégorie d'exigence	Exigence minimale
Système d'exploitation	- Windows XP, 7, 10 ou 11 ; Windows Server 2003, 2008, 2012, 2016, 2019 ou 2022 - Ubuntu 20.x ou 22.x
Mémoire	1 Go
Espace disque	1 Go
Processeur	Tout matériel avec un minimum de 10 % de capacité de processeur dédié.

Moteur de connecteurs IoT

OT Security inclut un moteur de connecteur IoT que vous pouvez intégrer à vos serveurs IoT/VMS.

Ce moteur prend en charge deux méthodes de connexion : authentification à l'aide d'un service d'API d'application distante ou connexion via un agent. Après l'intégration de vos serveurs d'applications avec le moteur, OT Security importe tous les appareils gérés, tels que les caméras, les systèmes d'accès par badge et les panneaux de commande d'alarme incendie.

Vous pouvez effectuer les tâches suivantes pour les connecteurs IoT :

Ajouter des connecteurs IoT



1. Sur la page Collecte de données > Sources de données, cliquez sur l'onglet Connecteurs IoT.

La page Connecteurs IoT apparaît.

2. Dans le coin supérieur droit, cliquez sur Ajouter un connecteur IoT.

Un menu déroulant apparaît.

3. Sélectionnez l'une des options suivantes :

- **Via un agent**

1. Dans la zone Nom du connecteur, saisissez le nom du connecteur.
2. Dans la zone Adresse IP du serveur, saisissez l'adresse IP du connecteur à ajouter.
3. Pour vous connecter au VMS hébergé dans la base de données, cliquez pour activer le curseur Informations d'authentification VMS.

OT Security active les champs pertinents requis pour les informations d'authentification VMS.
4. Dans la zone Adresse IP de la base de données, ajoutez l'adresse IP de la base de données hébergeant le VMS.
5. Dans la zone Port de la base de données, ajoutez le numéro de port pour vous connecter au serveur.
6. Dans la zone Nom d'utilisateur, saisissez le nom d'utilisateur de la base de données.
7. Dans la zone Mot de passe, saisissez le mot de passe de la base de données.
8. Cliquez sur Enregistrer.



Remarque : si le OT Security IoT Connector Agent n'est pas installé sur votre serveur d'application, la connexion échoue et OT Security affiche un message d'erreur.

- Via une API distante

1. Dans la section Type de connecteur, sélectionnez le connecteur IoT à ajouter.
2. Cliquez sur Suivant.

La section Détails du connecteur apparaît.

3. Dans la zone Nom du connecteur, saisissez le nom du connecteur.
4. Dans la zone IP, saisissez l'adresse IP du connecteur.
5. Dans la zone Port, saisissez le numéro de port via lequel OT Security peut se connecter. Le numéro de port par défaut est 22609.
6. Dans la zone Nom d'utilisateur, saisissez le nom d'utilisateur utilisé pour la connexion au connecteur.
7. Dans la zone Mot de passe, saisissez le mot de passe du connecteur.
8. Cliquez sur Enregistrer.

OT Security enregistre le connecteur, qui apparaît ensuite sur la page Connecteurs IoT.

Name	IP	Connection Method	Connector Type	Status	Assets
Lab Milestone		Via Remote API	Milestone	Connected	3
Sallent Agent		Via Agent	Agent	Disconnected	1
Lab Exacq		Via Remote API	Exacq Edge	Connected	1

Afficher les assets liés au connecteur IoT

Une fois connecté au serveur d'application, vous pouvez afficher les assets ou les services associés gérés par le serveur d'application.



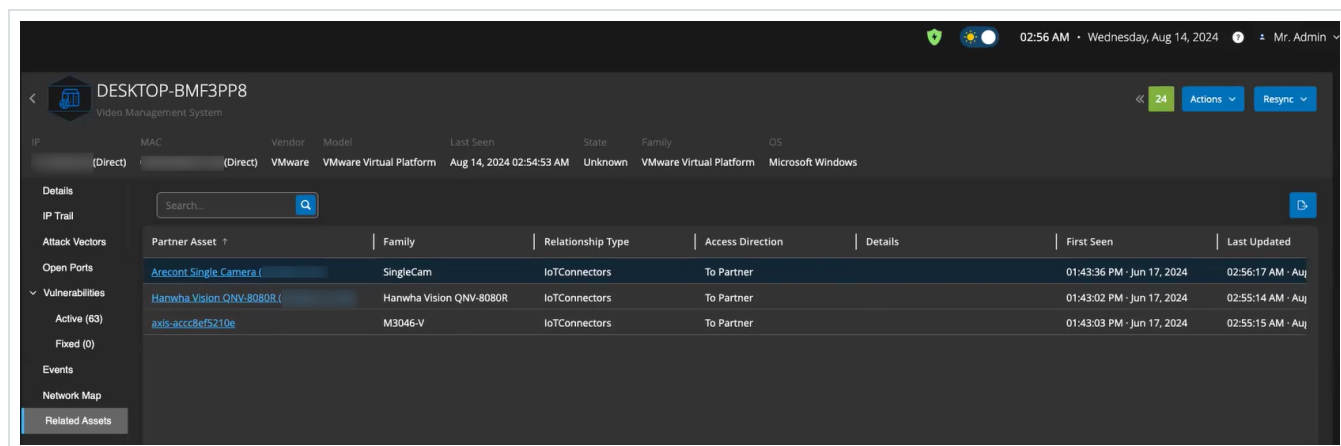
Pour afficher tous les appareils gérés par le serveur :

1. Accédez à Inventaire > Tous les assets.

La page Tous les assets apparaît.

2. Utilisez la zone de recherche pour rechercher le serveur d'application.

La page du serveur d'application sélectionné apparaît avec la liste des appareils qu'il gère.



Tester la connexion IoT

Après avoir ajouté un connecteur IoT, vous pouvez vérifier si OT Security peut l'atteindre.

1. Dans le tableau Connecteurs IoT, effectuez l'une des opérations suivantes :
 - Sur la ligne du connecteur IoT que vous souhaitez tester, effectuez un clic droit et sélectionnez Tester la connexion.
 - Sélectionnez le connecteur IoT que vous souhaitez tester, puis cliquez sur Actions > Tester la connexion.

OT Security exécute le test pour vérifier s'il peut atteindre le connecteur.

Modifier un connecteur IoT



1. Dans le tableau Connecteurs IoT, effectuez l'une des opérations suivantes :

- Sur la ligne du connecteur IoT que vous souhaitez modifier, effectuez un clic droit et sélectionnez Modifier.
- Sélectionnez le connecteur IoT que vous souhaitez modifier, puis cliquez sur Actions > Modifier.

Le panneau Modifier le connecteur IoT via l'agent ou l'API distante apparaît.

2. Modifiez les détails selon les besoins.

3. Cliquez sur Enregistrer.

OT Security enregistre les modifications apportées au connecteur IoT.

Supprimer un connecteur IoT

1. Dans le tableau Connecteurs IoT, effectuez l'une des opérations suivantes :

- Sur la ligne du connecteur IoT que vous souhaitez supprimer, effectuez un clic droit et sélectionnez Supprimer.
- Sélectionnez le connecteur IoT que vous souhaitez supprimer, puis cliquez sur Actions > Supprimer.

OT Security supprime le connecteur IoT.

Remarque : lorsque vous supprimez un connecteur IoT, OT Security désinstalle l'IoT Connector Agent du serveur d'application. Si vous souhaitez vous connecter au même serveur d'application via un agent, vous devez réinstaller le [OT Security IoT Connector Agent](#).

Installer l'IoT Connector Agent sous Windows

Rôle requis : Administrateur



OT Security vous permet de mapper tous les appareils IoT (Internet des objets) gérés avec leur serveur d'application correspondant en configurant le moteur de connecteurs IoT et en synchronisant les assets à partir du serveur d'application spécifique. Pour connecter votre serveur d'application via un agent, vous devez installer le OT Security IoT Connector Agent.

Pour installer le OT Security IoT Connector Agent :

1. Connectez-vous à la page [Téléchargements Tenable](#).
2. Accédez à la page **OT Security**.
3. Dans la section Visibilité avancée des IoT, téléchargez le pack Windows IoT Connector Agent.

Advanced IoT Visibility			
 Windows IoT Connector Agent	Tenable IoT Connector Agent for Windows Server 2012, Server 2016, Server 2019, Server 2022, 7, 8, 10, and 11 (64-bit)(v341)	190 MB	Checksum
 Ubuntu IoT Connector Agent	Tenable IoT Connector Agent for Ubuntu 20.x, 22.x, 24.x (amd64)(v341)	212 MB	Checksum

4. Copiez le pack Windows IoT Connector Agent téléchargé sur le serveur d'application où vous souhaitez l'installer.
5. Exécutez l'assistant Tenable IoT Connector Agent.

Un message indique que l'assistant de l'agent de connecteur est en cours d'initialisation et la fenêtre Welcome to the Tenable IoT Connector Agent Setup Wizard (Bienvenue dans l'assistant de configuration de l'IoT Connector Agent Tenable) apparaît.

6. Cliquez sur Suivant.

La fenêtre License Agreement (Contrat de licence) apparaît.

7. Sélectionnez I accept the agreement (I accept the agreement) et cliquez sur Next (Suivant).

La fenêtre Select Destination Directory (Sélectionner le répertoire de destination) apparaît.



8. Spécifiez le répertoire d'installation de l'IoT Connector Agent (ou utilisez le répertoire par défaut) et cliquez sur Next (Suivant).

L'installation du Tenable IoT Connector Agent commence.

9. Une fois l'installation terminée, vérifiez que le service « Tenable IoT Connector Agent » est en cours d'exécution.

- a. Dans la fenêtre Exécuter une commande, saisissez `services.msc`.

La fenêtre Services apparaît.

- b. Confirmez que **OT Security IoT Connector Agent** apparaît dans la liste des services en cours d'exécution.

Une fois l'installation terminée, vous pouvez connecter votre serveur d'application à OT Security. Pour plus d'informations sur la connexion au serveur d'application via un agent distant, voir [Ajouter des connecteurs IoT via un agent](#).

Lecteur PCAP

Rôle utilisateur OT Security requis : Administrateur, Superviseur

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.

PCAP Player					
Search...		Actions ▾ Upload PCAP File Export			
File Name	File Size	Uploaded At	Uploaded By	Last Played ▾	Last Played By
tag-write.pcap	15.57 MB	Sep 29, 2020 07:19:04 AM	admin	Never	Never
full-download-nochange.pcap	16.48 MB	Sep 29, 2020 07:19:43 AM	admin	Never	Never



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. Sur la page Collecte de données > Sources de données, cliquez sur l'onglet Lecteur PCAP.

La page Lecteur PCAP apparaît.

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 PCAP :

1. Sur la page Collecte de données > Sources de données, cliquez sur l'onglet Lecteur PCAP.

La page Lecteur PCAP apparaît.

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.

Chargements manuels

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Opérateur de site

L'onglet Chargements manuels contient les éléments suivants :

- Mettre à jour les détails des assets à l'aide d'un fichier CSV
- Ajouter des assets manuellement
- Fichiers SCD
- Fichiers de projet Rockwell

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. Sur la page Collecte de données > Sources de données, cliquez sur l'onglet Chargements manuels.
2. Dans la section Mettre à jour les détails de l'asset à l'aide d'un fichier CSV, cliquez sur Charger.
3. Accédez à l'emplacement où se trouve le fichier CSV et chargez-le.

Ajouter des assets manuellement

Pour suivre votre inventaire, vous souhaitez 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. Accédez à Collecte de données > Sources de données.

La page Sources de données apparaît.

2. Dans l'onglet Chargements manuels, accédez à la section Ajouter des assets manuellement.
3. Dans le menus Actions, sélectionnez Télécharger le modèle CSV.

OT Security télécharge le modèle de document tot_Assets.

4. Ouvrez le document modèle tot_Assets.
5. Modifiez le modèle tot_Assets en suivant précisément les instructions trouvées dans le fichier, en ne laissant que les en-têtes de colonne tels que Nom et Type, et les valeurs que vous fournissez.
6. Enregistrez le fichier modifié.
7. Revenez à la page Paramètres des assets.
8. Depuis le menu Actions, sélectionnez Charger un fichier CSV, accédez au fichier CSV souhaité et ouvrez-le pour le charger.
9. 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	Descriptio	Result	Error
2	AAA	Plc	HighCritic	10.100.20.aa	bbcccd	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:bbcd:	Catalyst	C2960	12.3		Level3			Success	
5	DDD	Unknown	None	Criticality					Linux	Level4	Israel		Success	

Fichiers SCD

Le fichier SCD (Substation Configuration Description) contient tous les détails liés aux communications d'une sous-station. Vous pouvez désormais charger un fichier SCD sur OT



Security et gagner en visibilité sur vos assets et la configuration CEI 61850, tout en bénéficiant d'informations sur la sécurité de votre environnement.

En fonction des informations contenues dans le fichier SCD, OT Security signale les détections liées à une mauvaise configuration de la sous-station, notamment :

- Accès aux rapports MMS (Manufacturing Message Specification) par des clients non autorisés.
- Tentative d'abonnement aux rapports MMS par des clients non autorisés non mentionnés dans le fichier SCD.

Remarque : OT Security ne prend en charge que les formats suivants pour les fichiers SCD :

- Versions 1.0 et 2.0 de SCL (Substation Configuration Language).
- Fichiers SCD avec une seule sous-station.

Pour charger un fichier SCD :

1. Accédez à Collecte de données > Sources de données.

La page Sources de données apparaît.

2. Dans l'onglet Chargements manuels, accédez à la section Fichiers SCD.
3. Dans la section Fichiers SCD, cliquez sur Charger.

SCD Files

Upload

1285 MMS reports have no clients assigned, exposing unauthorized access. Assign authorized clients or remove redundant configurations from the SCD file. [Download Details](#)

Upload SCD files to import each of your substations' configuration and define IED device communication settings according to the IEC 61850 Standard.

Note: only one SCD file is allowed per substation. The most recently uploaded file containing the same substation name will override previous ones.

Project	SCD File Name	Substation	Last Updated
Station Indegy	Station Indegy (t1).scd	Substation	03:59:12 PM · Jan 20
huh	SBUSServer.scd		02:16:48 PM · Jan 26
S/S 8860	SBUSServer.scd	S/S 8610	02:50:54 PM · Jan 26
NIC STATION	NIC STATION.scd		03:08:44 PM · Jan 26



Remarque : vous ne pouvez charger qu'un seul fichier SCD par sous-station. Le dernier fichier chargé contenant le même nom de sous-station remplace le précédent.

4. Recherchez et sélectionnez le fichier à charger.

OT Security charge le fichier SCD. Vous pouvez afficher les détails de l'asset dans les onglets Inventaire > Détails et CEI 61850. Toute mauvaise configuration du fichier SCD déclenche un événement et un message d'erreur d'accès non autorisé apparaît en haut des pages [Détails](#) et [CEI 61850](#).

5. (Facultatif) Pour télécharger les détails des détections, dans le message d'erreur, cliquez sur Télécharger les détails.

OT Security télécharge les détails au format CSV.

Fichiers de projet Rockwell

Vous pouvez charger des fichiers Rockwell .L5X pour créer des assets, affiner les détails des assets et établir des relations entre les assets dans des environnements isolés ou à visibilité limitée. La taille maximale du fichier de projet est de 50 Mio.

Important : par défaut, le paramètre `ProjectFilePopulatePrimaryLayerAssetIPs` est défini sur `Vrai` et le paramètre `ProjectFilePopulateNonPrimaryLayerAssetIPs` est défini sur `Faux`. Lors du chargement de plusieurs fichiers de projet contenant des assets avec des adresses IP identiques, le fait de définir le paramètre de configuration `ProjectFilePopulateNonPrimaryLayerAssetIPs` sur `Vrai` résout les assets dupliqués. Ainsi, le système peut afficher les adresses IP des assets de la couche non principale, ce qui vous permet de résoudre les assets avec la même adresse IP qu'un asset unique et de les placer correctement sur le même fond de panier. Pour modifier la configuration, contactez l'assistance Tenable.

Pour charger un fichier Rockwell :

1. Accédez à Collecte de données > Sources de données.

La page Sources de données apparaît.



2. Dans l'onglet Chargements manuels, accédez à la section Fichiers de projet Rockwell.

Rockwell Project Files

Upload a single project file (.LSX) to extract controller configuration and enrich your asset inventory with details like controller type, IP address, and backplane structure.

Upload

3. Cliquez sur Charger.
4. Recherchez et sélectionnez le fichier à charger.

OT Security charge le fichier de projet Rockwell. Vous pouvez afficher les détails de l'asset dans l'onglet Inventaire > Détails.



Paramètres

La section Paramètres dans OT Security comprend la plupart des pages de configuration pour OT Security :

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](#).

Paramètres de l'environnement

- **Définitions de réseau**

- Surveillance passive – Activez la surveillance passive pour permettre à OT Security de découvrir les assets. Voir [Surveillance passive](#).
- 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. Voir [Mettre à jour les détails d'un asset à l'aide d'un fichier 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 de 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.

- Réseau surveillé - Affichez et modifiez l'agrégation des plages d'adresses IP dans lesquelles le système classe les assets. Voir [Réseaux surveillés](#).
- 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 :
 - Réinitialiser aux paramètres d'usine - Rétablit tous les paramètres d'usine par défaut. Seul un administrateur ou un responsable sécurité peut effectuer une réinitialisation aux paramètres d'usine.

Attention : cette opération est irréversible et toutes les données du système sont perdues.

Les options suivantes sont désormais disponibles dans Tenable Core :

- 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.
- Journal système - Affiche le journal de tous les événements système qui se sont produits dans le système. Par exemple, Politique activée, Politique modifiée et Événement résolu. Vous pouvez exporter le journal dans un fichier CSV ou l'envoyer à un serveur Syslog. Voir [Journal système](#).

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

Rôle utilisateur OT Security requis : Administrateur, Superviseur



La page Appareil affiche des informations détaillées sur votre configuration OT Security. Vous pouvez afficher et modifier la configuration sur cette page.



Device

Site Name

[Edit](#)

The name of the site where the Tenable OT Security ICP device is installed

Site Name

Device URLs

[Edit](#)

Device URLs allows you to set multiple URLs from which the system can be accessed (FQDN/IP) in addition to the locally configured IP addresses. (Change requires restart).

Maximum Log-in Session Time-out

[Edit](#)

Determines the session period after which logged in users will be logged out automatically and required to log in again. (Requires log-out)

Log out After

2 Weeks

Maximum Inactivity Time-out

[Edit](#)

Determines the inactivity period after which logged-in users will be logged out automatically and required to log in again. (Requires log-out)

Log out After

1 Hour

Open Ports Age-out Period

[Edit](#)

Discovered open ports will disappear from the list after a certain period of time.

Period

2 weeks



Packet Capture

Turning on the full packet capture capability will cause Tenable OT Security to record all traffic from all its sensors in a continuous process to files, as well as to delete older files upon reaching maximum storage capacity limit.



Auto-Approve Sensor Pairing Requests



Nom du site

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. Veuillez à vérifier la résolution avant de continuer.

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, 1 heure, 4 heures, 12 heures, 1 jour, 1 semaine 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](#).

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

À partir de la version 4.1, vous pouvez passer en revue et configurer l'interface Tenable Core des ports divisés sur le port 8000.

Définir les préférences du dashboard Conformité

Rôle utilisateur OT Security requis : Administrateur, Superviseur

Vous pouvez spécifier les cadres de sécurité auxquelles le dashboard Conformité se réfère pour générer les données.

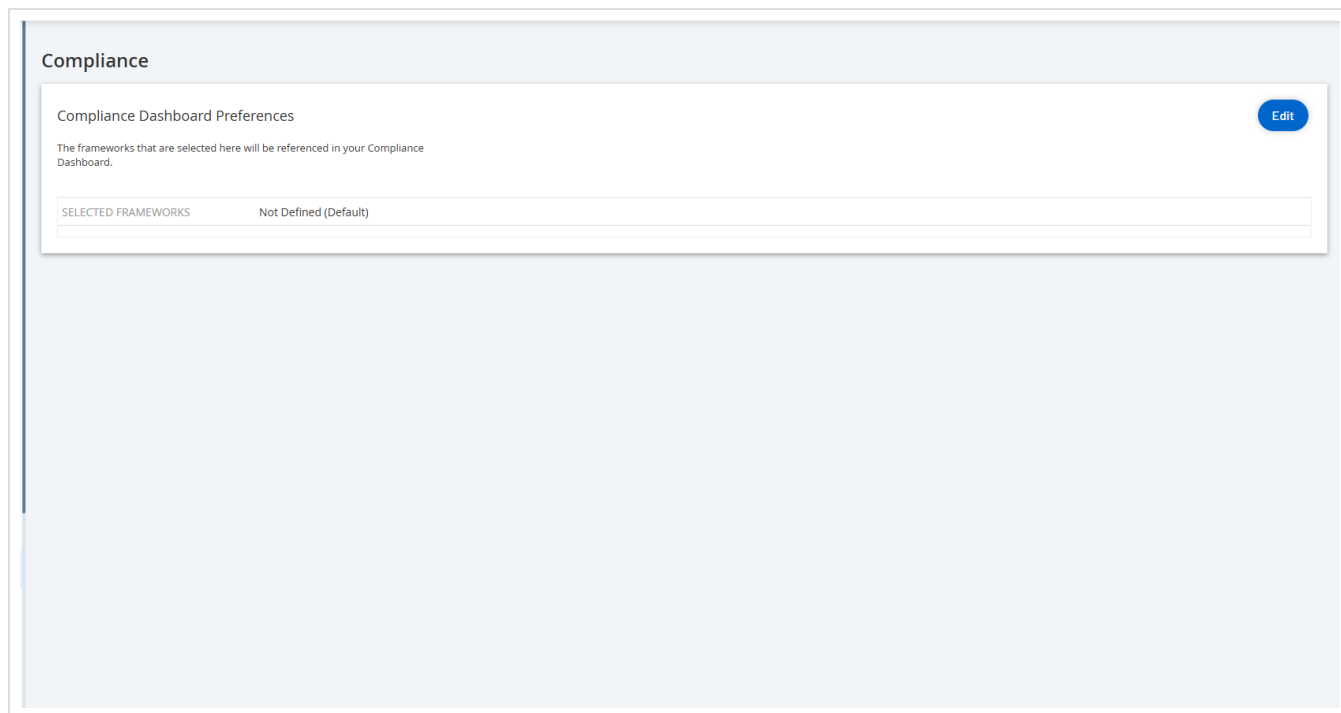
Pour définir les préférences du dashboard Conformité :



1. Effectuez l'une des actions suivantes :

- Accédez à Paramètres > Configuration système > Conformité.
- Sur la page du dashboard Conformité, cliquez sur le lien Préférences du cadre de sécurité.

La page Conformité apparaît.



2. Dans la section Préférences du dashboard Conformité, cliquez sur Modifier.

Le volet Modifier les cadres de conformité référencés apparaît.

3. Sélectionnez les cadres de conformité requis. Vous pouvez faire votre choix parmi les options suivantes :

- Contrôles ISO 27001
- Principes du CAF



- Sous-domaines OTCC
- Directive NIS2 (Article 21)
- Exigences NERC-CIP
- Exigences CEI 62443-3-3

4. Cliquez sur Enregistrer.

OT Security enregistre les préférences du cadre de conformité et vérifie la conformité de votre organisation par rapport aux préférences spécifiées. OT Security affiche les résultats des vérifications de conformité sur le [dashboard Conformité](#).

Mises à jour

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité

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. OT Security offre la possibilité de mettre à jour la classification, la famille et la couverture via les mises à jour cloud du moteur de prise d'empreinte numérique dynamique (DFE). 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.



Updates

☐ Nessus Plugin Set Cloud Updates

Update from FileEdit FrequencyUpdate Now

FREQUENCY	Every day at 02:00 AM
LAST UPDATED	
PLUGIN SET	202411070852

☐ IDS Engine Ruleset Cloud Updates

Update from FileEdit FrequencyUpdate Now

FREQUENCY	Every week on Monday and Thursday at 02:00 AM
LAST UPDATED	
RULE SET	202411062338

☐ Dynamic Fingerprinting Engine (DFE) Cloud Update

Update From FileEdit FrequencyUpdate From File

FREQUENCY	Every week on Monday and Thursday at 02:00 AM
LAST UPDATED	
VERSION	202410230822

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

Pour activer les mises à jour automatiques des plug-ins :

1. Accédez à 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

1. Accédez à 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.

Edit Frequency

REPEATS EVERY ^{*}

1 Days

AT ^{*}

02:00:00

Repeats every day at 02:00 AM
Next run at 02:00:00 AM - Jan 21, 2023

Cancel Save

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 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 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.



Update from File



 [Download the latest Nessus plugin file](#)
(Requires Internet connection)

UPLOAD PLUGIN SET FILE

DROP FILE HERE

Browse

Cancel - 498 - Update



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

Pour activer les mises à jour automatiques de l'ensemble de règles du moteur IDS :

1. Accédez à 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

1. Accédez à 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.

Edit Frequency [X]

REPEATS EVERY *
1 Days

AT *
02:00:00 [Clock Icon]

Repeats every day at 02:00 AM
Next run at 02:00:00 AM - Jan 21, 2023

Cancel Save

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 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 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.

Update from File

Download the latest IDS Engine ruleset file

(Requires Internet connection)

UPLOAD IDS ENGINE RULESET FILE

DROP FILE HERE

Browse

Cancel

Update

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.

- 502 -



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.

Mises à jour cloud du DFE

Vous pouvez utiliser la section Mises à jour du moteur de prise d'empreinte numérique dynamique (DFE) pour mettre à jour des modifications ou ajouter une nouvelle classification à votre système OT Security.

Configurer des mises à jour cloud automatiques du DFE

Pour activer les mises à jour automatiques du DFE :

1. Accédez à locaux > Configuration système > Mises à jour.

La page Mises à jour apparaît. La section Mises à jour cloud du DFE affiche la fréquence définie pour les mises à jour automatiques, la date de la dernière mise à jour et la version actuelle de la mise à jour.

2. Pour activer les mises à jour automatiques, cliquez sur le curseur Mises à jour cloud du DFE.

Modifier la fréquence des mises à jour du DFE

1. Accédez à locaux > Configuration système > Mises à jour.

La page Mises à jour apparaît. La section Mises à jour cloud du DFE affiche la fréquence définie pour les mises à jour automatiques, la date de la dernière mise à jour et la version actuelle de la 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 pour la mise à jour du DFE en saisissant un nombre et en sélectionnant une unité de temps (jours ou semaines) dans la zone déroulante.

Si vous sélectionnez Semaines, sélectionnez aussi les jours de la semaine pour la mise à jour hebdomadaire du DFE.

4. Dans la section À, définissez l'heure de la mise à jour du DFE (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 le DFE via le cloud

Pour mettre à jour manuellement le DFE :

1. Accédez à locaux > Configuration système > Mises à jour.

La page Mises à jour apparaît. La section Mises à jour cloud du DFE affiche la fréquence définie pour les mises à jour automatiques, la date de la dernière mise à jour et la version actuelle de la 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 Version affiche la version actuelle du DFE.

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 le DFE en téléchargeant la dernière version du DFE depuis le portail client de Tenable puis en chargeant le fichier.



Pour effectuer une mise à jour hors ligne du DFE :

1. Accédez à locaux > Configuration système > Mises à jour.

La fenêtre Mises à jour apparaît. La section Mises à jour cloud du DFE affiche la fréquence définie pour les mises à jour automatiques, la date de la dernière mise à jour et la version actuelle de la mise à jour.

2. Cliquez sur Mettre à jour à partir du fichier.

La fenêtre Mettre à jour à partir du fichier apparaît.

Update From File

Download the latest DFE file

(Requires internet connection)

UPLOAD DFE FILE

DROP FILE HERE

Browse

Cancel

Update

3. Si vous ne l'avez pas encore fait, cliquez sur le lien pour télécharger le dernier fichier de signatures d'appareils.

- 506 -



Remarque : le téléchargement du dernier fichier de signatures d'appareils à partir du lien est possible uniquement via une connexion Internet, par exemple avec un PC connecté à Internet.

4. Cliquez sur Parcourir et accédez au fichier de signatures d'appareils que vous avez téléchargé à partir du portail client de OT Security.
5. Cliquez sur Mettre à jour.

Mises à jour du moteur OT Discovery (OTD)

Rôle utilisateur OT Security requis : Administrateur, Superviseur et Analyste sécurité

Les agents OT utilisent le moteur OT Security (OTD) pour scanner votre environnement. Vous pouvez mettre à jour les moteurs OTD manuellement ou automatiquement à partir de la page Sources de données > Agents. Avant de mettre à jour le moteur OTD, vous devez d'abord charger le dernier fichier OTD sur OT Security.

Avant de commencer

- Téléchargez le fichier du moteur OT Discovery (OTD) à partir du portail des [téléchargements](#).

Pour charger le fichier du moteur OTD :

1. Accédez à Paramètres > Configuration système > Mises à jour.

La page Mises à jour apparaît.

2. Dans la section Mise à jour du moteur OT Discovery (OTD), cliquez sur Charger.

Le panneau Charger un fichier apparaît.

3. Cliquez sur Parcourir et accédez au fichier de moteur OTD que vous avez téléchargé à partir du portail de téléchargements de Tenable.
4. Cliquez sur Charger.
5. Pour mettre à jour le moteur OTD, suivez les étapes de la section [Mettre à jour l'agent OT](#).



Certificats

Rôle utilisateur OT Security requis : Administrateur

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 > Configuration système > Certificats.

La fenêtre Certificats apparaît.

2. Dans le menu Actions, sélectionnez Générer un certificat auto-signé.

Certificates

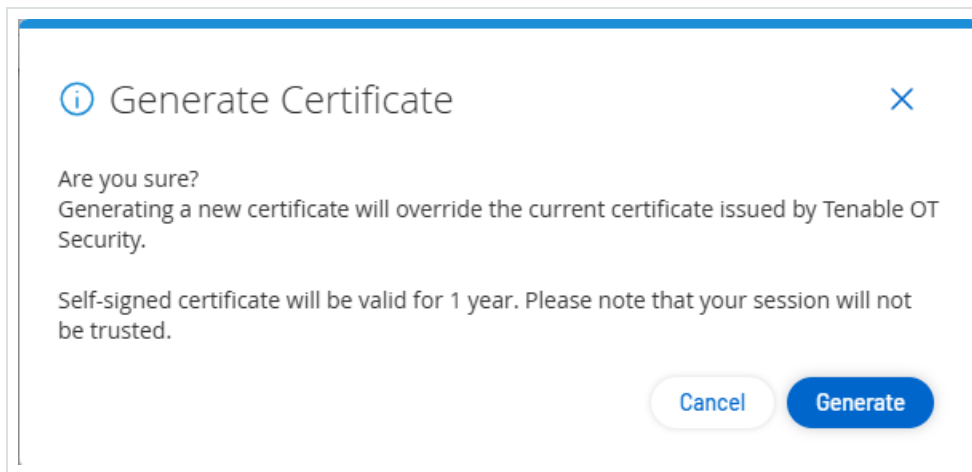
The certificate is used to secure the HTTPS connection. Use this section to generate a self-signed certificate or to upload an externally signed one.

ISSUED TO	Tenable OT Security
ISSUED BY	Tenable OT Security
ISSUED ON	Oct 31, 2023
EXPIRES ON	Oct 30, 2025
CERTIFICATE FINGERPRINT	[REDACTED]

Actions

- Generate Self-Signed Certificate
- Upload Certificate
- Download Certificate

La fenêtre de confirmation de génération du certificat apparaît.



3. Cliquez sur Générer.

OT Security génère le certificat auto-signé qui peut être consulté sur la page Certificats.

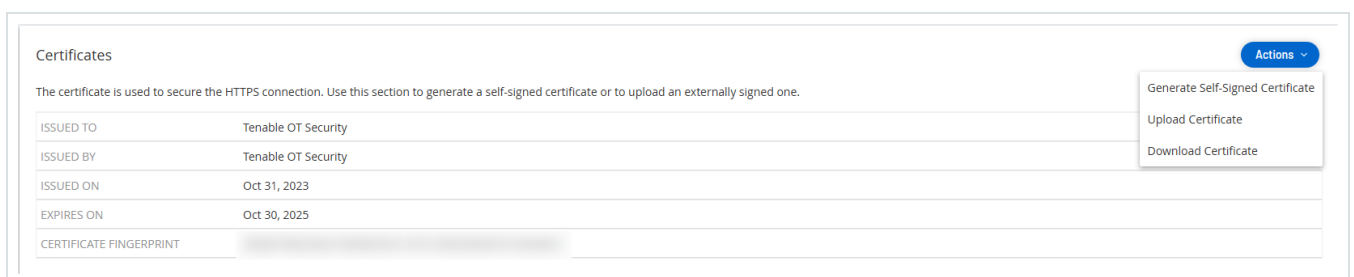
Charger un certificat HTTPS

Pour charger un certificat HTTPS :

1. Accédez à Paramètres > Configuration système > Certificats.

La fenêtre Certificats apparaît.

2. Dans le menu Actions, sélectionnez Charger le 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

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité, Analyste sécurité, Opérateur de site, Lecture seule

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 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

Rôle utilisateur OT Security requis : Administrateur, Superviseur

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.

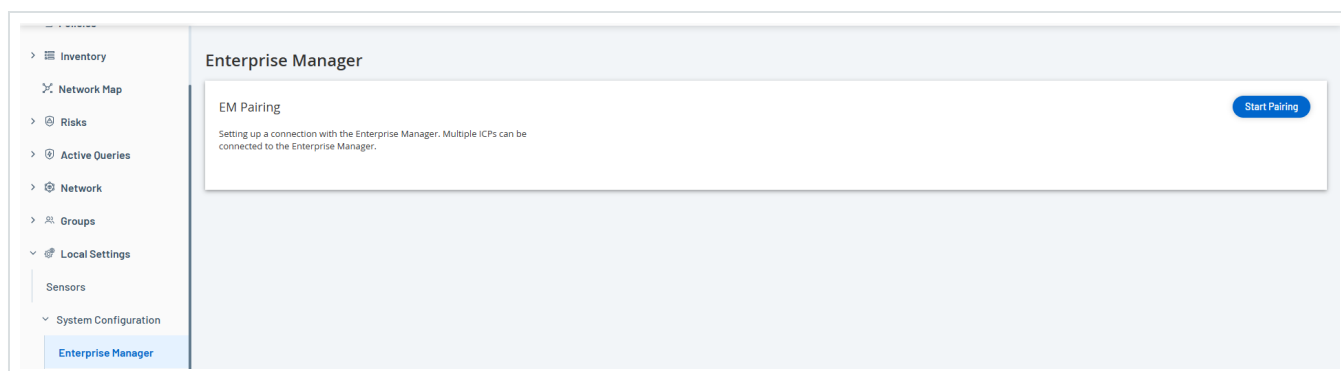
Remarque : cela n'est nécessaire que lorsque l'appairage se fait à l'aide de l'option de la clé API.

Pour appairer l'ICP avec OT Security EM :



1. Dans OT Security, accédez à 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

Rôle utilisateur OT Security requis : Administrateur, Superviseur

Vous pouvez déconnecter l'appairage ICP d'EM ou de l'ICP lorsque l'appairage n'est plus nécessaire.

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.



Déconnecter un appairage ICP de OT Security

1. Dans OT Security, accédez à 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.

Paramètres de l'environnement

Définitions de réseau

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Opérateur de site

La page Définitions de réseau comprend les sections suivantes :



- Surveillance passive
- Réseaux internes dupliqués
- Découvrir de nouveaux assets via SNMP
- Récupérer une adresse IP pour les assets IoT

Surveillance passive

La surveillance passive est désactivée lors de la configuration initiale de OT Security. Tenable vous recommande de terminer la configuration de vos réseaux surveillés avant d'activer la surveillance passive. Cela permet de réduire la surcharge liée à un trop grand nombre d'alertes initiales et d'événements de sécurité.

Réseaux internes dupliqués

Rôle utilisateur OT Security requis : Administrateur, Superviseur

Un chevauchement de plages d'adresses IP se produit lorsqu'une même adresse IP est attribuée à plusieurs appareils. Il est fréquent que des plages d'adresses IP se chevauchent dans les environnements de fabrication, ce qui complique l'identification et le suivi précis des assets. Cela a pour effet de dégrader la visibilité et d'introduire des erreurs dans l'association des assets. Vous pouvez définir des chevauchements de réseaux pour OT Security afin de suivre les assets avec précision, même lorsque les adresses IP sont réutilisées sur différents segments.

Remarque : si un asset d'un réseau dupliqué est détecté à la fois par un capteur et une autre source (telle qu'un autre capteur ou l'ICP en local), l'interface OT Security le fusionne en un seul asset. Cependant, la licence le considère comme deux assets distincts. Pour éviter cela, Tenable recommande d'ajuster la plage de réseau dupliquée pour exclure les assets de ce type.

Ajouter un réseau dupliqué

Avant de commencer



- Assurez-vous d'avoir appairé des capteurs authentifiés.

Remarque : OT Security ne prend pas en charge les réseaux dupliqués sur des capteurs non authentifiés.

Pour définir les réseaux dupliqués dans votre environnement :

1. Accédez à Paramètres > Configuration de l'environnement > Définitions de réseau.

La page Définition de réseau apparaît.

2. Dans la section Réseaux internes dupliqués, cliquez sur Ajouter un réseau.

Le panneau Ajouter un réseau dupliqué apparaît avec les détails du réseau.

Remarque : OT Security utilise la plage d'adresses IP 240.0.0.0/4 comme groupe de réserve interne pour le mappage d'adresses IP pour l'allocation d'adresses IP NAT. Pour modifier cette plage de groupe de réserve, contactez l'assistance Tenable.

Add Duplicated Network

IP Reserve Pool: 240.0.0.0/4

This pool will be used internally within OT Security for the purposes of background reservation of IP address mapping for NAT IP allocation.
If you wish to change the designated segment, contact Tenable OT Security Support.

DUPLICATED IP RANGE *

If the range is not in the monitored network, it will be added to it

192.168.0.0/16

* Duplicates (Sensors)

Sensor #1 x

^

☒ Sensor #1

Cancel

Next >

3. Dans la zone Plage d'adresses IP dupliquée, saisissez la plage d'adresses IP au format CIDR, par exemple 192.168.0.0/24.



4. Dans la zone déroulante Doublons (capteurs), sélectionnez les capteurs associés à la plage d'adresses IP dupliquée.
5. Cliquez sur Suivant.

Le panneau Confirmation apparaît.

Add Duplicated Network

Network Details

Confirmation

Please Confirm Asset Deletion
In order to separate these 33 assets into their own networks, the system will need to delete them automatically, allowing them to be rediscovered again after startup.
If you wish not to delete these 33 assets, they will remain in their current IP range and this may cause data inconsistencies or unexpected behavior. Best practices suggest deleting the affected overlapping assets.
[View Assets in New Tab](#)

☒ Delete Assets

< Back

Cancel

Save

6. (Facultatif) Cochez la case Supprimer les assets.



Conseil : pour séparer tous les assets sélectionnés en leurs propres réseaux, Tenable vous recommande d'autoriser OT Security à supprimer les assets et à les redécouvrir après le démarrage. Si vous ne cochez pas la case Supprimer les assets, les assets resteront dans la plage d'adresses IP actuelle, ce qui pourrait provoquer des incohérences ou un comportement inattendu.

7. Cliquez sur Enregistrer.

OT Security enregistre la plage d'adresses IP dupliquée qui apparaît alors dans le tableau « Réseaux internes dupliqués ».

Duplicated Internal Networks

Add Network

IP Reserve Pool: 240.0.0.0/4

This pool will be used internally within OT Security for the purposes of background reservation of IP address mapping for NAT IP allocation. If you wish to change the designated segment, contact Tenable OT Security Support.

1 Duplicated Networks

Actions

CIDR	Sensors	In Use - Discovery Queries	In Use - Nessus Scans
192.168.0.0/16	Sensor #1		

Important : une fois la configuration des réseaux dupliqués terminée, Tenable vous recommande de redémarrer OT Security avant d'activer les capteurs.

8. Redémarrez OT Security.

9. Pour activer les capteurs, accédez à Paramètres > Capteurs :

Remarque : les plages d'adresses IP (CIDR) pour la requête active sont celles que vous avez configurées dans les paramètres des réseaux internes dupliqués.

1. Effectuez l'une des actions suivantes :

- Pour un seul capteur : effectuez un clic droit sur le capteur et cliquez sur Modifier. Dans le panneau Modifier le capteur, cliquez sur le curseur Requête active du capteur pour activer les requêtes actives.



- Pour plusieurs capteurs : sélectionnez tous les capteurs requis. Dans l'en-tête, sélectionnez Actions en bloc > Activer les requêtes actives.

2. Effectuez un clic droit sur les capteurs et activez-les en faisant passer l'état de En pause à Connecté.

Étapes suivantes

Après avoir configuré les réseaux dupliqués et redémarré OT Security, les assets apparaissent avec leurs adresses IP réelles dans le tableau Tous les assets. De plus, lorsque vous saisissez une adresse IP attribuée à un réseau dupliqué, vous devez sélectionner le capteur correspondant. Par exemple : dans Requête active > Découverte/Scan Nessus > Créer un scan ou dans Informations d'authentification > Tester les informations d'authentification :

- Dans Inventaire > Tous les assets, affichez les adresses IP réelles et la source des assets dans le tableau « Tous les assets ». Il pourra s'agir, par exemple, de deux assets qui partagent la même adresse IP mais sont associés à des capteurs différents.
- Dans Requêtes actives > Gestion des requêtes > Découverte ou Scans Nessus > Créer un scan, lors de la configuration d'une requête active impliquant des réseaux dupliqués, sélectionnez les capteurs concernés pour cette plage d'adresses IP. Cela vous permet d'exécuter la requête pour les assets associés à un capteur spécifique tout en excluant les autres capteurs.

Remarque : OT Security active la case Capteurs concernés uniquement pour les plages d'adresses IP dans les réseaux dupliqués. Elle reste désactivée pour toutes les autres plages d'adresses IP.

- Dans Requêtes actives > Informations d'authentification > Tester les informations d'authentification, lors de la configuration des informations d'authentification, si vous saisissez une plage d'adresses IP dans un réseau dupliqué, vous devez également sélectionner les capteurs associés dans la zone Doublon (capteur).
- Pour créer des groupes d'assets pour les assets faisant partie de réseaux dupliqués, utilisez



l'option Sélection d'assets et identifiez l'adresse IP spécifique en fonction de la colonne Source du tableau « Assets ».

Tableau « Réseaux internes dupliqués »

Le tableau « Réseaux internes dupliqués » affiche les détails suivants :

Colonne	Description
CIDR	La plage d'adresses IP du réseau dupliqué.
Capteurs	Les capteurs associés à la plage d'adresses IP du réseau dupliqué.
En cours d'utilisation - Requêtes de découverte	Indique si les CIDR sont utilisés dans au moins une découverte d'assets (requête active). Si c'est le cas, retirez le CIDR de la découverte active avant de supprimer le réseau dupliqué qui contient ce CIDR.
En cours d'utilisation - Scans Nessus	Indique si les CIDR sont utilisés dans au moins un scan Nessus. Si c'est le cas, retirez le CIDR du scan Nessus avant de supprimer le réseau dupliqué qui contient ce CIDR.

Actions sur les réseaux internes dupliqués

Modifier un réseau dupliqué

Vous pouvez modifier la configuration du réseau dupliqué selon vos besoins.

Pour modifier un réseau dupliqué :

1. Dans la section Réseaux internes dupliqués, sélectionnez le réseau dupliqué à modifier.
2. Effectuez l'une des actions suivantes :



- Effectuez un clic droit sur le réseau dupliqué et sélectionnez Modifier.
- Dans le coin supérieur droit de la section, sélectionnez Actions > Modifier.

Le panneau Modifier le réseau dupliqué apparaît avec les détails du réseau sélectionné.

3. Modifiez les valeurs selon les besoins.
4. Cliquez sur Suivant.
5. Dans le panneau Confirmation, cliquez sur Enregistrer.

OT Security enregistre les modifications apportées au réseau dupliqué.

Supprimer un réseau dupliqué

Vous pouvez supprimer les réseaux dupliqués dont vous n'avez plus besoin.

Pour supprimer un réseau dupliqué :

1. Dans la section Réseaux internes dupliqués, sélectionnez le réseau dupliqué à supprimer.
2. Effectuez l'une des actions suivantes :
 - Effectuez un clic droit sur le réseau dupliqué et sélectionnez Supprimer.
 - Dans le coin supérieur droit de la section, sélectionnez Actions > Supprimer.

OT Security supprime le réseau dupliqué.

Supprimer un capteur utilisé dans un réseau dupliqué

Pour supprimer un capteur utilisé dans un réseau dupliqué :

1. Supprimez les CIDR du scan Nessus/de la découverte active.
2. Supprimez le capteur de la configuration des paramètres du réseau dupliqué.



3. En cas de remplacement, utilisez l'API pour définir le nouvel identifiant de capteur et remplacer l'ancien capteur.
4. Sur la page Capteurs, supprimez l'ancien capteur.

Découvrir de nouveaux assets via SNMP

Lorsque vous activez l'option Découverte de nouveaux assets via SNMP, OT Security ajoute les assets découverts par les requêtes SNMP à l'inventaire des assets.

Récupérer une adresse IP pour les assets IoT

Par défaut, lors de l'importation d'assets à partir d'un connecteur IoT, OT Security importe l'adresse IP avec l'adresse MAC des appareils. Pour importer uniquement l'adresse MAC, désactivez l'option Récupérer une adresse IP pour les assets IoT. Pour plus d'informations, voir [Gérer les connecteurs IoT](#).

Groupes d'événements

Rôle utilisateur OT Security requis : Administrateur, Superviseur

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.

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 > 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.

Réseaux surveillés

Rôle utilisateur OT Security requis : Administrateur, Superviseur

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).



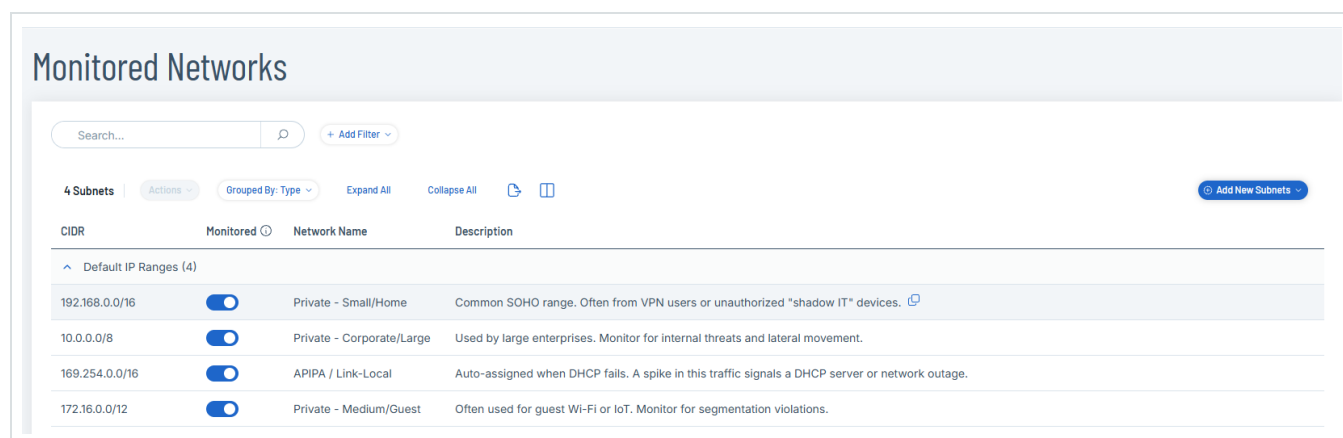
Attention : si vous configurez plus de 5 000 sous-réseaux surveillés uniques, OT Security tronque la liste après les 5 000 premières entrées. Le système ne donne aucune indication de l'invisibilité d'une partie de la liste.

Pour les composants Nessus Network Monitor (NNM), OT Security traite uniquement les 128 premières entrées.

Pour désactiver l'une des plages par défaut ou pour ajouter des plages appropriées à votre réseau :

1. Accédez à Paramètres > Configuration de l'environnement > Réseaux surveillés.

La page Réseaux surveillés apparaît.



2. Accédez à Paramètres > Configuration de l'environnement > Gestion des réseaux.

La page Gestion du réseau apparaît et affiche l'onglet Réseaux surveillés par défaut.

3. Personnalisez les tableaux selon vos besoins. Voir [Personnaliser les tableaux](#).

4. Le tableau Réseaux surveillés contient les détails suivants :

Colonne	Description
Plages d'adresses IP par défaut et plages d'adresses IP	La section Plages d'adresses IP par défaut affiche les plages d'adresses IP par défaut configurées dans OT



personnalisées	Security. La section Plages d'adresses IP personnalisées affiche toutes les plages d'adresses IP que vous créez.
CIDR	La colonne CIDR affiche les adresses IP à surveiller.
Surveillé	Cliquez pour activer ou désactiver la surveillance des adresses IP configurées.
Nom du réseau	Le nom du réseau.
Description	La description des plages d'adresses IP.
	Survolez une valeur pour afficher le bouton Copier  . Vous pouvez l'utiliser pour copier la valeur du paramètre.

Ajouter des sous-réseaux

Vous pouvez ajouter un sous-réseau ou une liste de sous-réseaux à surveiller.

Pour ajouter un sous-réseau :

1. Dans le menu de navigation de gauche, accédez à Paramètres > Configuration de l'environnement > Réseaux surveillés.

La page Réseaux surveillés apparaît.

2. Dans le coin supérieur droit, cliquez sur Ajouter de nouveaux sous-réseaux.

Un menu apparaît.

3. Sélectionnez l'une des options suivantes :



- Ajouter un sous-réseau - Sélectionnez cette option pour ajouter un seul sous-réseau.
- Ajouter une liste de sous-réseaux - Sélectionnez cette option pour ajouter une liste de sous-réseaux.

Le panneau Ajouter un sous-réseau apparaît.

4. Si vous avez sélectionné Ajouter un sous-réseau :

- a. Dans la zone CIDR, saisissez la plage d'adresses IP. Par exemple, 192.168.1.0/24.
- b. Cliquez sur le curseur Surveillé pour autoriser OT Security à capturer le trafic et à exécuter des requêtes actives au sein de la plage d'adresses IP.

Remarque : le curseur Surveillé est activé par défaut. Pour désactiver la surveillance, cliquez sur le curseur Surveillé.

- c. (Facultatif) Dans le champ Nom du réseau, saisissez le nom du réseau.
- d. (Facultatif) Dans la zone Description, saisissez la description des sous-réseaux.
- e. Cliquez sur Enregistrer.

5. Si vous avez sélectionné Ajouter une liste de sous-réseaux, procédez comme suit dans le panneau Ajouter des sous-réseaux :

- a. Dans la zone CIDR, indiquez la liste des CIDR en saisissant un CIDR par ligne.
- b. Cliquez sur le curseur Surveillés (tous les sous-réseaux ajoutés) pour autoriser OT Security à capturer le trafic et à exécuter des requêtes actives dans tous les sous-réseaux répertoriés.

Remarque : le curseur Surveillé est activé par défaut. Pour désactiver la surveillance, cliquez sur le curseur Surveillés (tous les sous-réseaux ajoutés).

- c. Cliquez sur Enregistrer.

OT Security enregistre les sous-réseaux. Ils apparaissent sur la page Réseaux surveillés.



Modifier un sous-réseau

Vous pouvez apporter des modifications à un sous-réseau.

1. Pour modifier un sous-réseau, effectuez l'une des actions suivantes :

- Dans le tableau Réseaux surveillés, survolez avec la souris la ligne de la plage d'adresses IP que vous souhaitez modifier.

OT Security active le menu Actions.

- Dans le tableau Réseaux surveillés, effectuez un clic droit sur la ligne de la plage d'adresses IP que vous souhaitez modifier.

Un menu apparaît.

2. Sélectionnez Modifier un sous-réseau.

Le panneau Modifier un sous-réseau apparaît.

3. Apportez les modifications nécessaires.

4. Cliquez sur Enregistrer.

OT Security enregistre les modifications apportées aux sous-réseaux.

Effectuer un scan à l'aide d'agents OT portables

Rôle utilisateur OT Security requis : Administrateur

Un agent OT à l'état portable peut découvrir des assets dans des environnements OT complexes, hermétiques et isolés, puis renvoyer les résultats à OT Security pour analyse.

Les fonctionnalités interconnectées suivantes permettent aux agents d'effectuer des analyses dans des environnements complexes hermétiques :



- Zones de réseaux, permettant de rattacher les assets à des sites logiques ou physiques. Pour plus d'informations, voir [Zones de réseaux](#).
- Un agent dans un état portable déconnecté collecte et regroupe les données de découverte, puis les transfère en toute sécurité vers l'ICP sans nécessiter de connexion active.
- Interface native permettant aux techniciens de terrain de charger des profils de scan, de suivre la progression des scans, d'exécuter des scans hors ligne et de télécharger les résultats. L'interface sert également à l'appairage et au journal système.

Concepts clés

La coordination des entités suivantes permet de mener des activités portables de découverte OT.

- Zones de réseaux - Conteneurs logiques ou physiques (par exemple, bâtiment B) qui rattachent les assets à un emplacement. OT Security traite les adresses IP identiques appartenant à des zones de réseaux (réseaux dupliqués) différentes comme des assets distincts et uniques.
- Scan OT Discovery (scan OTD) - Jeu d'instructions techniques que vous créez via l'assistant de scan OT Discovery. Le jeu d'instructions définit les informations d'authentification et les planifications.
- Sous-réseau (réseau surveillé) - Plage réseau en notation CIDR (par exemple, 192.168.0.0/24) qui définit le périmètre de l'activité de découverte. OT Security ne crée pas d'assets en dehors des sous-réseaux configurés.
- Source - Toute entité qui signale des données d'assets : capteurs, agents, ICP locale, chargements CSV ou lecteur PCAP (capture de paquets).

États de l'agent

L'état d'un agent est déterminé par sa dernière connexion à OT Security :



- Statique - L'agent est activement connecté à OT Security et reçoit les configurations de scan en temps réel.
- Portable - La dernière connexion de l'agent avait pour but de charger des résultats, sans établir de connexion active. L'agent fonctionne de façon autonome dans les environnements hermétiques et mène des activités de découverte OT sans chemin réseau vers OT Security.

Workflow de scan d'agent à l'état portable

Conditions préalables

- Vérifiez que vous disposez des autorisations d'administrateur.
- Définissez votre zone de réseaux et vos sous-réseaux sur la page [Zones de réseaux](#).

Remarque : la zone de réseaux et le sous-réseau doivent tous deux exister dans OT Security pour que l'agent renvoie des résultats. Si un chargement de résultat fait référence à une zone de réseaux ou à un sous-réseau qui n'existent pas, OT Security vous avertit et conserve les résultats. OT Security publie les résultats une fois que vous les avez liés à une zone de réseaux existante ou que vous en avez créé une nouvelle.

- [Installer l'agent OT](#).

Étape 1 : Définir le scan OT Discovery

Vous devez d'abord créer un scan OTD à l'aide de l'assistant de configuration OTD :

1. Accédez à Collecte de données > Requêtes actives.

La page Gestion des requêtes actives apparaît.

2. Cliquez sur l'onglet Scans OTD.

La page Scans OTD apparaît.

3. Cliquez sur Créer un scan OTD.

Le panneau Créer une scan OTD apparaît.

Create OTD Scan

×

NAME

scan2_floor2

DESCRIPTION

Floor 2 scan

Credentials

SNMP V1+V2

×

▼

Monitored Networks

192.168.0.0/16

×

▼

* Network Areas

Sensor #1 (Sensor)

×

floor3

×

OTAgent #1 (Agent)

×

▼

☒ ENABLE SCHEDULE

REPEATS EVERY *

4

Weeks

▼

Cancel

Save

4. Dans la zone Nom, saisissez le nom du scan.
5. Dans la zone Description, saisissez le contexte ou les détails du scan.
6. Dans la zone déroulante Informations d'authentification, sélectionnez les informations d'authentification requises.

Étape 2 : Lier le sous-réseau et la zone de réseaux



Dans l'assistant de scan OTD, vous devez lier le sous-réseau et la zone de réseaux.

1. Dans la zone déroulante Réseaux surveillés, sélectionnez un ou plusieurs sous-réseaux à scanner ou saisissez une plage de CIDR.

Remarque : vous pouvez préremplir les sous-réseaux sur la page Réseaux surveillés ou les créer directement dans ce champ en saisisant la plage de CIDR.

2. Dans la zone déroulante Zones de réseaux, sélectionnez une ou plusieurs zones de réseaux.

Remarque : vous pouvez préremplir les zones de réseaux sur la page Zones de réseau ou les créer directement dans ce champ en saisisant un nouveau nom.

3. Définissez un calendrier.

- a. Cliquez sur le curseur Activer la planification.

La zone déroulante Répéter chaque devient active.

- b. (Facultatif) Indiquez l'intervalle en minutes, en heures, en jours ou en semaines comme requis.
- c. Dans la section Le, sélectionnez les jours auxquels vous souhaitez exécuter le scan.
- d. Dans la zone déroulante À, sélectionnez l'heure à laquelle vous souhaitez exécuter le scan.

4. Cliquez sur Enregistrer.

OT Security enregistre le scan OTD.

Étape 3 : Synchroniser la configuration avec l'agent

1. Accédez à l'interface de votre agent OT local sur Windows.

Remarque : l'agent synchronise automatiquement les configurations de scan disponibles chaque fois qu'il se connecte à OT Security.



2. Sélectionnez le fichier à charger pour l'exécuter ou procédez à un appairage avec l'ICP (statique ou en ligne).
3. Sélectionnez la zone de réseaux dans laquelle vous voulez exécuter le scan.

Étape 4 : Exécuter le scan

1. Exécutez le scan à partir de l'interface de l'agent local. À l'état portable, l'agent mène des activités de découverte OT sur le réseau sélectionné sans connexion active à Tenable OT Security.
2. Affichez la progression du scan dans le journal d'exécution et téléchargez les résultats.

Étape 5 : Charger les résultats

Chargez les résultats via Chargements manuels dans OT Security.

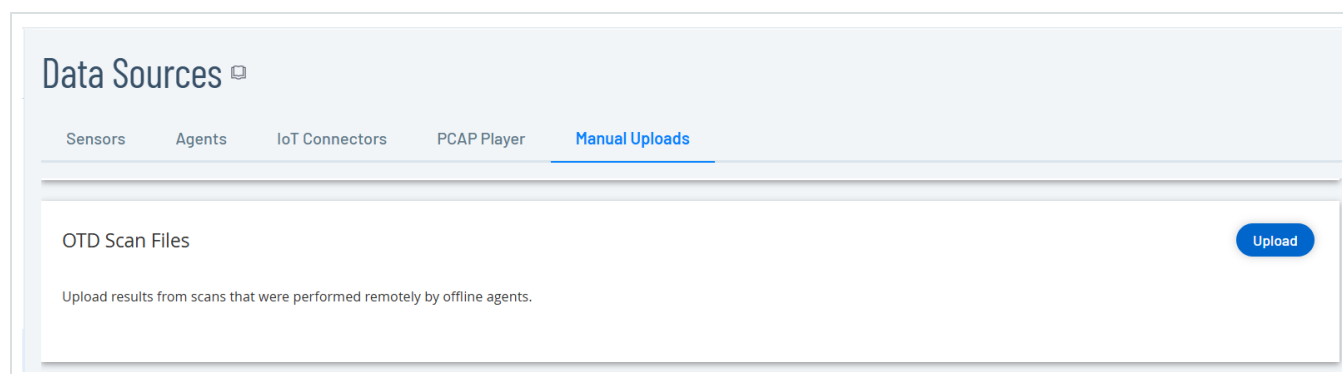
1. Accédez à Collecte de données > Sources de données.

La page Sources de données apparaît.

2. Cliquez sur l'onglet Chargements manuels.

La page Chargements manuels apparaît.

3. Accédez à la section Fichiers de scan OTD et cliquez sur Charger.



4. Accédez à votre fichier local de résultats de scan OTD et sélectionnez-le pour l'importer.



Remarque : si vous ne définissez pas la zone de réseaux ou le sous-réseau avant de procéder au chargement, OT Security vous avertit. Vous devez lier les résultats à une zone de réseaux existante ou en créer une nouvelle portant un nom identique aux résultats pour que le système puisse remplir votre inventaire d'assets.

5. Affichez les résultats des données d'assets importés sur la page Inventaire.

Réseaux surveillés

Rôle utilisateur OT Security requis : Administrateur, Superviseur

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).

Attention : si vous configurez plus de 5 000 sous-réseaux surveillés uniques, OT Security tronque la liste après les 5 000 premières entrées. Le système ne donne aucune indication de l'invisibilité d'une partie de la liste.

Pour les composants Nessus Network Monitor (NNM), OT Security traite uniquement les 128 premières entrées.

Pour désactiver l'une des plages par défaut ou pour ajouter des plages appropriées à votre réseau :

1. Accédez à Paramètres > Configuration de l'environnement > Réseaux surveillés.

La page Réseaux surveillés apparaît.



Monitored Networks			
Search... + Add Filter			
4 Subnets Actions Grouped By: Type Expand All Collapse All + Add New Subnets			
CIDR	Monitored	Network Name	Description
Default IP Ranges (4)			
192.168.0.0/16	☒	Private - Small/Home	Common SOHO range. Often from VPN users or unauthorized "shadow IT" devices.
10.0.0.0/8	☒	Private - Corporate/Large	Used by large enterprises. Monitor for internal threats and lateral movement.
169.254.0.0/16	☒	APIPA / Link-Local	Auto-assigned when DHCP fails. A spike in this traffic signals a DHCP server or network outage.
172.16.0.0/12	☒	Private - Medium/Guest	Often used for guest Wi-Fi or IoT. Monitor for segmentation violations.

2. Accédez à Paramètres > Configuration de l'environnement > Gestion des réseaux.

La page Gestion du réseau apparaît et affiche l'onglet Réseaux surveillés par défaut.

3. Personnalisez les tableaux selon vos besoins. Voir [Personnaliser les tableaux](#).

4. Le tableau Réseaux surveillés contient les détails suivants :

Colonne	Description
Plages d'adresses IP par défaut et plages d'adresses IP personnalisées	La section Plages d'adresses IP par défaut affiche les plages d'adresses IP par défaut configurées dans OT Security. La section Plages d'adresses IP personnalisées affiche toutes les plages d'adresses IP que vous créez.
CIDR	La colonne CIDR affiche les adresses IP à surveiller.
Surveillé	Cliquez pour activer ou désactiver la surveillance des adresses IP configurées.
Nom du réseau	Le nom du réseau.



Description	La description des plages d'adresses IP.
	Survolez une valeur pour afficher le bouton Copier  . Vous pouvez l'utiliser pour copier la valeur du paramètre.

Ajouter des sous-réseaux

Vous pouvez ajouter un sous-réseau ou une liste de sous-réseaux à surveiller.

Pour ajouter un sous-réseau :

1. Dans le menu de navigation de gauche, accédez à Paramètres > Configuration de l'environnement > Réseaux surveillés.

La page Réseaux surveillés apparaît.

2. Dans le coin supérieur droit, cliquez sur Ajouter de nouveaux sous-réseaux.

Un menu apparaît.

3. Sélectionnez l'une des options suivantes :

- Ajouter un sous-réseau - Sélectionnez cette option pour ajouter un seul sous-réseau.
- Ajouter une liste de sous-réseaux - Sélectionnez cette option pour ajouter une liste de sous-réseaux.

Le panneau Ajouter un sous-réseau apparaît.

4. Si vous avez sélectionné Ajouter un sous-réseau :



- a. Dans la zone CIDR, saisissez la plage d'adresses IP. Par exemple, 192.168.1.0/24.
- b. Cliquez sur le curseur Surveillé pour autoriser OT Security à capturer le trafic et à exécuter des requêtes actives au sein de la plage d'adresses IP.

Remarque : le curseur Surveillé est activé par défaut. Pour désactiver la surveillance, cliquez sur le curseur Surveillé.

- c. (Facultatif) Dans le champ Nom du réseau, saisissez le nom du réseau.
 - d. (Facultatif) Dans la zone Description, saisissez la description des sous-réseaux.
 - e. Cliquez sur Enregistrer.
5. Si vous avez sélectionné Ajouter une liste de sous-réseaux, procédez comme suit dans le panneau Ajouter des sous-réseaux :

- a. Dans la zone CIDR, indiquez la liste des CIDR en saisissant un CIDR par ligne.
- b. Cliquez sur le curseur Surveillés (tous les sous-réseaux ajoutés) pour autoriser OT Security à capturer le trafic et à exécuter des requêtes actives dans tous les sous-réseaux répertoriés.

Remarque : le curseur Surveillé est activé par défaut. Pour désactiver la surveillance, cliquez sur le curseur Surveillés (tous les sous-réseaux ajoutés).

- c. Cliquez sur Enregistrer.

OT Security enregistre les sous-réseaux. Ils apparaissent sur la page Réseaux surveillés.

Modifier un sous-réseau

Vous pouvez apporter des modifications à un sous-réseau.



1. Pour modifier un sous-réseau, effectuez l'une des actions suivantes :

- Dans le tableau Réseaux surveillés, survolez avec la souris la ligne de la plage d'adresses IP que vous souhaitez modifier.

OT Security active le menu Actions.

- Dans le tableau Réseaux surveillés, effectuez un clic droit sur la ligne de la plage d'adresses IP que vous souhaitez modifier.

Un menu apparaît.

2. Sélectionnez Modifier un sous-réseau.

Le panneau Modifier un sous-réseau apparaît.

3. Apportez les modifications nécessaires.

4. Cliquez sur Enregistrer.

OT Security enregistre les modifications apportées aux sous-réseaux.

Zones de réseaux

Rôle utilisateur OT Security requis : Administrateur

Les zones de réseaux associent vos sous-réseaux à leur emplacement physique. Ce mappage permet de différencier les données de scan provenant de plages d'adresses IP qui se chevauchent sur différents emplacements physiques.

La page Zones de réseaux affiche toutes les zones de réseaux configurées dans votre système. Les zones de réseaux se divisent en deux catégories distinctes :



- Automatiques : créées par le système lorsque vous enregistrez un capteur ou un agent statique.
- Manuelles : créées par un administrateur à titre d'espace réservé pour un scan d'agent portable.

Utilisez la page Zones de réseaux pour créer des catégories de regroupement pour vos sous-réseaux.

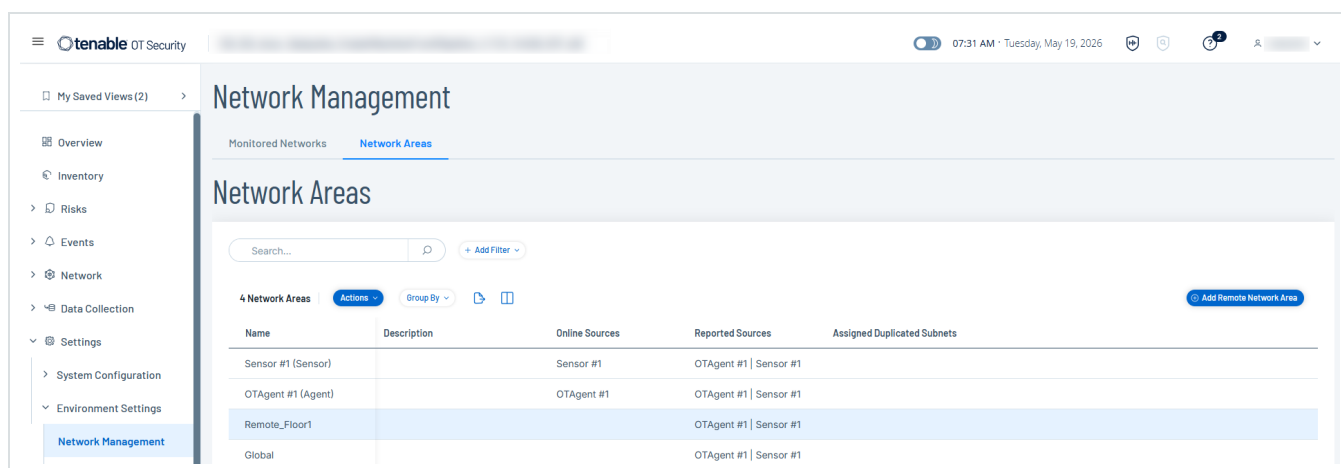
Afficher les zones de réseaux

1. Accédez à Paramètres > Configuration de l'environnement > Gestion des réseaux.

La page Gestion des réseaux apparaît. L'onglet ouvert par défaut est Réseaux surveillés.

2. Cliquez sur l'onglet Zones de réseaux.

La page Zones de réseaux apparaît et répertorie l'ensemble des capteurs et agents configurés dans votre ICP.



Le tableau Réseaux surveillés contient les détails suivants :

Colonne	Description
Nom	Identifiant unique de la zone de réseaux.



Description	Description courte de la zone de réseaux.
Sources en ligne	Toutes les entités en ligne associées à cette zone de réseaux.
Sources signalées	Toutes les entités associées à cette zone de réseaux qui émettent des signalements.
Sous-réseaux dupliqués attribués	Affiche la plage de CIDR et un compteur indiquant la position de la zone de réseaux parmi toutes celles qui partagent ce sous-réseau. Par exemple, si cinq zones réseau partagent un même sous-réseau, la colonne affiche 1/5, 2/5, 3/5, 4/5, 5/5 pour chaque sous-réseau.
En cours d'utilisation	Indique si cette zone réseau est activement utilisée dans des scans Nessus ou OT Discovery (OTD). Une zone de réseaux marquée En cours d'utilisation ne peut pas être supprimée tant qu'elle n'a pas été retirée de tous les scans associés.

Ajouter des zones de réseaux distante

1. Accédez à Paramètres > Configuration de l'environnement > Gestion des réseaux.

La page Gestion des réseaux apparaît.

2. Cliquez sur l'onglet Zones de réseaux.

La page Zones de réseaux apparaît.

3. Dans le coin supérieur droit, cliquez sur Ajouter une zone de réseaux distante.

Le panneau Ajouter une zone de réseaux distante apparaît.



Add Remote Network Area ×

NAME

Floor 2

DESCRIPTION

Network area for floor 2

Cancel

Save

4. Dans la zone Nom, saisissez le nom de la zone distante.
5. Dans la zone Description, saisissez la description de la zone distante.
6. Cliquez sur Enregistrer.

OT Security enregistre la zone de réseaux distante.

Déplacer des sources vers une zone de réseaux

Vous pouvez regrouper plusieurs sources dans une même zone de réseaux. Par exemple, si un étage ou un bâtiment spécifique est surveillé par trois capteurs différents, vous pouvez les



regrouper sous une même zone de réseaux. Si vous avez deux bâtiments contenant respectivement quatre capteurs, vous n'avez besoin de configurer que deux zones de réseaux (une par bâtiment) au lieu de huit zones distinctes.

Pour combiner plusieurs sources de signal en une même zone de réseaux :

1. Dans le tableau Zones de réseaux, effectuez l'une des opérations suivantes :

- Sélectionnez la zone de réseaux à partir de laquelle vous souhaitez déplacer les sources.

OT Security active le bouton Actions dans l'en-tête.

- Effectuez un clic droit sur la zone de réseaux à partir de laquelle vous souhaitez déplacer les sources.

Un menu apparaît.

2. Sélectionnez Déplacer les sources.

Le volet Déplacer les sources apparaît.



Move Sources ×

Sources to Move

Sensor #1 × ▼

Move to Network Area

Remote_Floor1 ▼

Cancel

Save

3. Dans la zone déroulante Sources à déplacer, sélectionnez une ou plusieurs sources à déplacer.
4. Dans la zone déroulante Déplacer vers la zone de réseaux, sélectionnez la zone de réseaux cible dans la liste.
5. Cliquez sur Enregistrer.

OT Security déplace les sources sélectionnées vers la zone de réseaux spécifiée.

Modifier une zone de réseaux distante

Vous pouvez modifier le nom et la description d'une zone de réseaux distante existante.



1. Dans le tableau Zones de réseaux, effectuez l'une des opérations suivantes :

- Sélectionnez la zone de réseaux que vous souhaitez modifier.

OT Security active le bouton Actions dans l'en-tête.

- Effectuez un clic droit sur la zone de réseaux que vous souhaitez modifier.

Un menu apparaît.

2. Sélectionnez Modifier les détails.

Le panneau Modifier les détails apparaît.

3. Modifiez les détails selon les besoins.

4. Cliquez sur Enregistrer.

OT Security enregistre vos modifications et le tableau Zones de réseaux affiche les détails mis à jour.

Supprimer une zone de réseaux distante

Vous pouvez supprimer les zones de réseaux dont vous n'avez plus besoin.

Remarque : vous ne pouvez pas supprimer une zone de réseaux désignée comme En cours d'utilisation. Pour supprimer une zone de réseaux, vous devez supprimer toutes les sources qui lui sont associées et veiller à la retirer de tous les scans Nessus et OT Discovery actifs.

Pour supprimer une zone de réseaux :

1. Dans le tableau Zones de réseaux, effectuez l'une des opérations suivantes :

- Sélectionnez la zone de réseaux que vous souhaitez supprimer.

OT Security active le bouton Actions dans l'en-tête.



- Effectuez un clic droit sur la zone de réseaux que vous souhaitez supprimer.

Un menu apparaît.

2. Sélectionnez Supprimer.

OT Security supprime la zone de réseaux sélectionnée.

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), et Site Operators (Groupe d'utilisateurs > rôle Site Operator). 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

Rôle utilisateur OT Security requis : Administrateur

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.

Local Users		
Search...		
Actions Add User		
Full Name ↑	Username	User Groups
Mr. Admin	admin	Administrators
		Supervisors Site Operators Security Managers Security Analysts Read...

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 > 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), et Site Operators (Groupe d'utilisateur > rôle Site Operator). 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 locaux > Gestion des utilisateurs > Utilisateurs locaux.

La page Utilisateurs locaux apparaît.

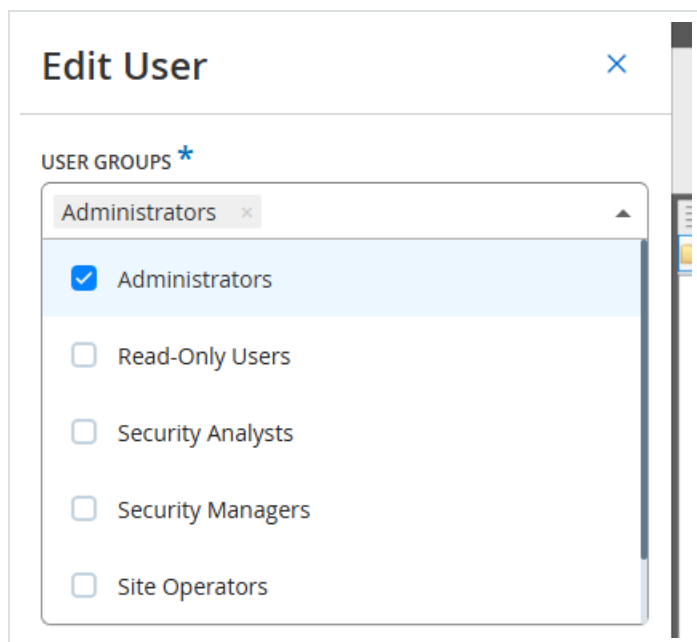
2. Effectuez un clic droit sur l'utilisateur et sélectionnez Modifier l'utilisateur.

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 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 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



Rôle utilisateur OT Security requis : Administrateur

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), et Site Operators (Groupe d'utilisateurs > rôle Site Operator). 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.

User Groups			
Search...		Actions ▼ Create User Group ℹ	
Name ↑	Members	Role	Authentication Servers
Administrators	Mr. Admin sanjusha	Administrator	
Read-Only Users		Read Only	
Security Analysts		Security Analyst	
Security Managers		Security Manager	
Site Operators		Site Operator	
Supervisors		Supervisor	

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'utilisateur .

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 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.



Create User Group



NAME *

ROLE *

LOCAL MEMBERS

ZONES

AUTHENTICATION SERVERS

Cancel

Create

Create User Group



NAME *

* Role



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 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.

The screenshot shows a dialog box titled "Edit User Group". It contains three main sections: "NAME" with a text input field containing "Security Analysts"; "ROLE" with a dropdown menu showing "Security Analyst"; and "USERS" with a list of users "Bob Smith" and "Mr. Admin", each with a small 'x' icon to remove it. There is also a plus icon and a dropdown arrow to add more users.

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 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 (local)	Administrateur (externe/AD)	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	✓	✓	✓	✓	✓	✗	✗



Autorisation	Administrateur (local)	Administrateur (externe/AD)	Superviseur	Responsable sécurité	Analyste sécurité	Opérateur de site	Lecture seule
Exporter	✓	✓	✓	✓	✓	✓	✓
Créer une politique sur FortiGate	✓	✓	✓	✓	✗	✗	✗
Actualiser	✓	✓	✓	✓	✓	✓	✓
Politiques							
Afficher les politiques	✓	✓	✓	✓	✓	✓	✓
Activer/Désactiver	✓	✓	✓	✓	✗	✗	✗
Afficher l'action	✓	✓	✓	✓	✓	✓	✓
Modifier	✓	✓	✓	✓	✗	✗	✗
Dupliquer	✓	✓	✓	✓	✗	✗	✗
Supprimer	✓	✓	✓	✓	✗	✗	✗
Créer une politique	✓	✓	✓	✓	✗	✗	✗



Autorisation	Administrateur (local)	Administrateur (externe/AD)	Superviseur	Responsable sécurité	Analyste sécurité	Opérateur de site	Lecture seule
Exporter	✓	✓	✓	✓	✓	✓	✓
Assets							
Afficher les assets	✓	✓	✓	✓	✓	✓	✓
Afficher l'action	✓	✓	✓	✓	✓	✓	✓
Modifier	✓	✓	✓	✗	✗	✓	✗
Supprimer	✓	✓	✓	✗	✗	✓	✗
Importer (charger de nouveaux assets via csv)	✓	✓	✓	✗	✗	✓	✗
Masquer	✓	✓	✓	✗	✗	✓	✗
Exporter	✓	✓	✓	✓	✓	✓	✓
Resynchroniser	✓	✓	✓	✓	✓	✓	✗
Scan Nessus	✓	✓	✓	✓	✓	✓	✗



Autorisation	Administrateur (local)	Administrateur (externe/AD)	Superviseur	Responsable sécurité	Analyste sécurité	Opérateur de site	Lecture seule
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	✓	✓	✓	✓	✓	✓	✓



Autorisation	Administrateur (local)	Administrateur (externe/AD)	Superviseur	Responsable sécurité	Analyste sécurité	Opérateur de site	Lecture seule
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	✓	✓	✓	✓	×	×	×



Autorisation	Administrateur (local)	Administrateur (externe/AD)	Superviseur	Responsable sécurité	Analyste sécurité	Opérateur de site	Lecture seule
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	✓	✓	✓	✓	✓	✓	✓



Autorisation	Administrateur (local)	Administrateur (externe/AD)	Superviseur	Responsable sécurité	Analyste sécurité	Opérateur de site	Lecture seule
une cartographie							
Actualiser la cartographie	✓	✓	✓	✓	✓	✓	✓
Groupes							
Afficher les groupes	✓	✓	✓	✓	✓	✓	✓
Afficher l'action	✓	✓	✓	✓	✓	✓	✓
Modifier	✓	✓	✓	✓	✗	✗	✗
Dupliquer	✓	✓	✓	✓	✗	✗	✗
Supprimer	✓	✓	✓	✓	✗	✗	✗
Créer un groupe	✓	✓	✓	✓	✗	✗	✗
Exporter	✓	✓	✓	✓	✓	✓	✓



Autorisation	Administrateur (local)	Administrateur (externe/AD)	Superviseur	Responsable sécurité	Analyste sécurité	Opérateur de site	Lecture seule
Rapport							
Afficher les rapports	✓	✓	✓	✓	✓	✓	✓
Générer	✓	✓	✓	✓	✓	✓	✓
Télécharger	✓	✓	✓	✓	✓	✓	✓
Exporter	✓	✓	✓	✓	✓	✓	✓
Segments réseau							
Afficher les segments réseau	✓	✓	✓	✓	✓	✓	✓
Modifier	✓	✓	✓	✓	✗	✗	✗
Supprimer	✓	✓	✓	✓	✗	✗	✗
Créer	✓	✓	✓	✓	✗	✗	✗
Exporter	✓	✓	✓	✓	✓	✓	✓
En savoir plus	✓	✓	✓	✓	✓	✓	✓



Autorisation	Administrateur (local)	Administrateur (externe/AD)	Superviseur	Responsable sécurité	Analyste sécurité	Opérateur de site	Lecture seule
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	✓	✓	×	×	×	×	×



Autorisation	Administrateur (local)	Administrateur (externe/AD)	Superviseur	Responsable sécurité	Analyste sécurité	Opérateur de site	Lecture seule
on système - Certificat (HTTPS)							
Configuration système - Clés API	✓	✗	✓ (Utilisateurs locaux uniquement)	✓ (Utilisateurs locaux uniquement)	✓ (Utilisateurs locaux uniquement)	✓ (Utilisateurs locaux uniquement)	✓ (Utilisateurs locaux uniquement)
Configuration système - Licence	✓	✓	✗	✗	✗	✗	✗
Configuration de l'environnement - Paramètres de l'asset	✓	✓	✓	✗	✗	✗	✗
Configuration de l'environnement - Assets	✓	✓	✓	✓ - pas de restauration	✓ - pas de restauration	✓	✓ - pas de restauration



Autorisation	Administrateur (local)	Administrateur (externe/AD)	Superviseur	Responsable sécurité	Analyste sécurité	Opérateur de site	Lecture seule
masqués							
Configuration de l'environnement - Champs personnalisés	✓	✓	✓	×	×	×	×
Configuration de l'environnement - Clusters d'événements	✓	✓	✓	×	×	×	×
Configuration de l'environnement - Lecteur PCAP	✓	✓	✓	×	×	×	×
Utilisateurs et rôles -	✓	✓	✓	×	×	×	×



Autorisation	Administrateur (local)	Administrateur (externe/AD)	Superviseur	Responsable sécurité	Analyste sécurité	Opérateur de site	Lecture seule
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)



Autorisation	Administrateur (local)	Administrateur (externe/AD)	Superviseur	Responsable sécurité	Analyste sécurité	Opérateur de site	Lecture seule
Actions système	✓	✓ sans réinitialisation des paramètres d'usine	✓ sauvegarde et diagnostics uniquement	✓ diagnostics uniquement	✗	✗	✗
Journal système	✓	✓	✓	✓	✓	✓	✓ pas de journal syslog
Activer (lors de la configuration et après la désactivation)	✓	✓	✗	✗	✗	✗	✗
Supprimer les assets	✓	✓	✓	✗	✗	✗	✗

Autorisation	Administrateur (local)	Administrateur (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	Responsabl e 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	×	×	×	×	×



ystème - Certificat (HTTPS)					
Configuration système - Clés API	✓ (Utilisateurs locaux uniquemen t)	✓ (Utilisateurs locaux uniquement)	✓ (Utilisateurs locaux uniquemen t)	✓ (Utilisateurs locaux uniquemen t)	✓ (Utilisateurs locaux uniquemen t)
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

Rôle utilisateur OT Security requis : Administrateur

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 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 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 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 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 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

Rôle utilisateur OT Security requis : Administrateur

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 livré avec un ensemble de groupes d'utilisateurs pré-définis, correspondant à chacun des rôles disponibles, à savoir Administrators (Groupe d'utilisateurs > rôle Administrator), et Site Operators (Groupe d'utilisateur > rôle Site Operator). 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 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.



Active directory changes are pending a restart

Restart

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 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 adsrv1.tenable.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 adsrv1.tenable.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 adsrv1.tenable.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

Rôle utilisateur OT Security requis : Administrateur

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 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.

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

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité, Analyste sécurité, Opérateur de site, Lecture seule

Pour afficher les groupes :

1. Accédez à Paramètres > 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 et tags - Les assets sont des entités matérielles du réseau. Les groupes d'assets sont utilisés comme condition pour un grand nombre de types de politiques.
- 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 de contrôleur - 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 et tags

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.

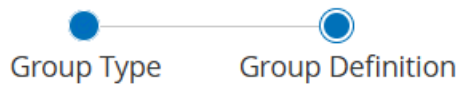
Tags

Les tags permettent de regrouper les assets en fonction de critères spécifiques vous permettant de simplifier et de prioriser divers workflows. Lorsque vous créez des groupes, OT Security les convertit en tags sur vos assets.

Pour afficher les tags sur les assets, cochez la case Afficher un tag sur les assets membres lorsque vous créez des groupes d'assets.



Create Asset Group



NAME *

AssetGroup1

☒ Display tag on member assets

Search...



1737 Assets Group By ▾



☐ Name Type IP

☐ [Endpoint #1526](#) Endpoint

☐ [Endpoint #875](#) Endpoint

☐ [Endpoint #286](#) Endpoint

☐ [Endpoint #258](#) Endpoint

☐ [Endpoint #1458](#) Endpoint

☐ [Endpoint #1711](#) Endpoint

☐ [Endpoint #105](#) Endpoint

< Back

Cancel

Create



Pour activer ou désactiver l'affichage des tags pour plusieurs assets, sélectionnez plusieurs assets. Dans le menu Actions en bloc, choisissez Activer l'affichage des tags ou Désactiver l'affichage des tags, selon les besoins. Vous pouvez également activer ou désactiver le curseur dans la colonne Afficher un tag pour chaque asset.

N...	Type	Display Tag	Members	Used in Policies	Used in Queries
User-defined asset groups (1)					
☒ Asse...	Asset Selection	☒	Endpoint #1721 Endpoint #1526 Endpoint #875 Endpoint #286		
Predefined asset groups (121)					
☒ 3D P...	Function Group	☒			
☒ ABB...	Function Group	☒		Use of Unauthorized Protocols in ABB 800X ...	☒
☒ ABB...	Function Group	☒			
☐ ABB...	Function Group	☐			
☐ ABB...	Function Group	☐			
☐ Acce...	Function Group	☐			
☐ Actu...	Function Group	☐			
☐ Any ...	Function Group	☐		SIMATIC Code Download SIMATIC Code Upload ...	Active Asset T Nessus Basic
☐ Apo...	Function Group	☐		Use of Unauthorized Protocols in Apogee ...	
☐ Bac...	Function Group	☐		Use of Unauthorized Protocols in Bachmann ...	

Ces groupes d'assets apparaissent dans la colonne Tags sur la page Inventaire > Tous les assets.



Inventory						
All Assets Controllers & Modules Network Assets IoT Assets						
Search... + Add Filter						
702 Assets Group By						
Actions						
Criticality	IP	Source	Tags	Category	Vendor	
☐ Low		nic0 (Local) OTAgent #...		Network Assets	Fortinet	
☐ Low		nic0 (Local) OTAgent #...		Network Assets	Tenable	
☐ Low		nic0 (Local) OTAgent #...		Network Assets	Tenable	
☐ Low		nic0 (Local) OTAgent #...	groupwithtags1	Network Assets	Tenable	
☐ Low		nic0 (Local)		Network Assets	VMware	
☐ Low		nic0 (Local)		Network Assets	VMware	
☐ Low		nic0 (Local)		Network Assets	Tenable	
☐ Low		nic0 (Local) OTAgent #...		Network Assets	Tenable	
☐ Low		nic0 (Local) OTAgent #...		Network Assets	Tenable	

Afficher les groupes d'assets et les tags

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 générerait un trop grand nombre d'événements, une icône d'avertissement apparaît. Activez ou désactivez une politique à l'aide du curseur de statut.



ID	L'ID attribué au groupe d'assets.
Nom	Le nom de la politique.
Afficher un tag	Le curseur permettant d'activer l'affichage des tags sur la page Inventaire > Tous les assets.
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.
Origine	L'origine du groupe d'assets : Défini par l'utilisateur ou Défini par le système.
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 : • Fonction (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.
Type	Le type de groupe. Les options sont Statique ou Dynamique.
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.
Utilisé dans les zones	Affiche le nom de la zone 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

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité

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.

Remarque : pour les réseaux dupliqués, utilisez l'option Sélection d'assets pour créer un groupe d'assets.

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 Paramètres > 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.

Name	Type	Addresses	Location
☐ Power Supply #1	Power Supply	10.100.105.27	
☐ Endpoint #77	Endpoint	10.100.101.200	
☐ Endpoint #71	Endpoint	10.100.110.152	
☐ Endpoint #55	Endpoint	10.100.30.47	
☐ HRP	OT Device	10.100.103.22	
☐ H50854	HMI	192.168.136.193	
☐ Gurad	PLC	10.100.101.154	

5. Pour afficher les tags sur les assets, cochez la case Afficher un tag sur les assets membres.

Remarque : si cette option est sélectionnée, OT Security affiche les tags dans la colonne Tags sur la page Inventaire > Tous les assets.

6. Dans la zone Nom, saisissez le nom du groupe.

Choisissez un nom qui décrit un élément commun catégorisant les assets inclus dans le groupe.

7. Cochez la case à côté de chaque asset à inclure dans le groupe.
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 Plage IP :

1. Accédez à Paramètres > 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 Paramètres > 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.

Créer des groupes et des tags d'assets

Vous pouvez créer des groupes d'assets personnalisés pour les utiliser lors de la configuration de politiques. Le regroupement d'assets similaires vous permet de créer des politiques qui s'appliquent à tous les assets du groupe. Vous pouvez créer des groupes soit en sélectionnant les assets requis, soit en définissant une règle de filtre pour regrouper les assets dans une catégorie spécifique. Le regroupement dynamique d'assets en fonction de critères sélectionnés permet de fluidifier et d'étendre les processus, tels que la priorisation et les rapports.

Pour créer un groupe d'assets :

1. Accédez à Groupes > Groupes et tags d'assets.

La page Groupes et tags d'assets apparaît.

2. Pour créer un groupe d'assets, cliquez sur Créer un groupe d'assets.

La fenêtre Créer un groupe d'assets apparaît.

3. Dans la section Type de groupe, sélectionnez l'une des options suivantes :

- Statique (sélection manuelle) - Les groupes d'assets statiques sont définis en sélectionnant manuellement les assets et en les ajoutant au groupe. Une fois que vous avez défini le groupe, ses membres ne changent pas, à moins que vous ne les modifiez.



- Dynamique (basé sur des règles) - Les groupes d'assets dynamiques utilisent des règles pour filtrer votre inventaire d'assets. Au fil de la découverte et de l'enrichissement d'assets, les membres sont automatiquement ajoutés ou supprimés du groupe, afin de le maintenir à jour.

4. Cliquez sur Suivant.

Le panneau Définition de groupe apparaît.

5. Dans la zone Nom, saisissez le nom du groupe d'assets. Choisissez un nom qui décrit un élément commun catégorisant les assets inclus dans le groupe.
6. Si vous avez sélectionné Statique, procédez comme suit :
- a. Cochez les cases à côté des assets à ajouter au groupe.
7. Si vous avez sélectionné Dynamique, cliquez sur Ajouter un filtre pour activer une règle pour la création d'un groupe. Voir [Filtrer les assets](#).

Remarque : vous devez ajouter au moins un filtre pour permettre la création d'un groupe.

8. Pour afficher les tags de chaque asset, cochez la case Afficher un tag sur les assets membres. Cette option est sélectionnée par défaut.
9. Cliquez sur Créer.

OT Security crée le groupe d'assets et l'affiche sur la page Groupes et tags d'assets. Vous pouvez désormais utiliser ce groupe lors de la configuration des politiques.

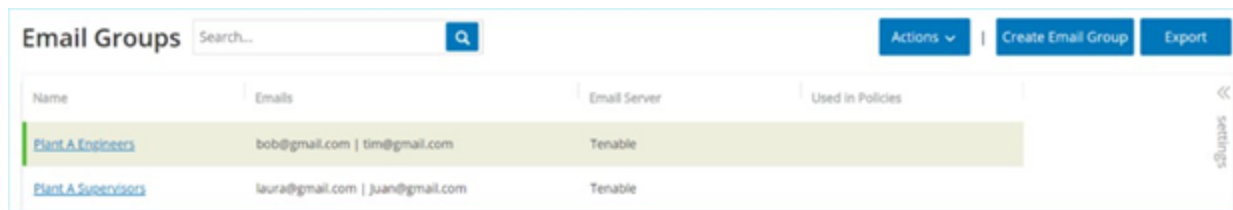
Groupes de messagerie

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 et



par service 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

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité

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 Paramètres > 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	Affiche le nom de chaque politique qui utilise ce groupe de ports dans sa



les politiques	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

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité

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 Paramètres > 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, par exemple Modbus, PROFINET et CIP. 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

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité

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 Paramètres > 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 (Récurent) - 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

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité

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 (Récurent) - 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 Récurent :

1. Accédez à Paramètres > 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 Récurent.

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 Paramètres > 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 de contrôleur

Les tags sont des paramètres dans les contrôleurs qui contiennent des données opérationnelles spécifiques. Les groupes de tags de contrôleur sont utilisés comme condition dans 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 de contrôleur



La page Groupes de tags de contrôleur affiche tous les groupes de tags actuellement configurés dans le système.

Le tableau Groupes de tags de contrôleur 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 de contrôleur

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité



Vous pouvez créer des groupes de tags de contrôleur 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 de contrôleur.

Pour créer un groupe de tags :

1. Accédez à Paramètres > Groupes > Groupes de tags de contrôleur.
2. Cliquez sur Créer un groupe de tags de contrôleur.

Le panneau Créer un groupe de tags de contrôleur 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 de contrôleur. 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	Affiche l'identifiant de chaque politique qui utilise ce groupe de règles dans sa



les politiques	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

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité

Pour créer un groupe de règles :

1. Accédez à Paramètres > 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

Rôle utilisateur OT Security requis : Administrateur, Superviseur, Responsable sécurité



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.

La page correspondant au type de groupe sélectionné apparaît.



2. Sélectionnez le groupe que vous souhaitez afficher.

OT Security active le bouton Actions.

3. Effectuez l'une des actions suivantes :

- Cliquez sur Actions et sélectionnez Afficher.
- Effectuez un clic droit sur le groupe et sélectionnez Afficher.

4. Sélectionnez Afficher.

La page des détails du groupe apparaît.

Modifier un groupe

Vous pouvez modifier les détails d'un groupe existant.

Pour modifier les détails d'un groupe :

1. Dans Groupes, sélectionnez le type de groupe souhaité.

La page correspondant au type de groupe sélectionné apparaît.

2. Sur la page Groupes, sélectionnez le groupe que vous souhaitez modifier.

OT Security active le bouton Actions.

3. Effectuez l'une des actions suivantes :

- Cliquez sur Actions et sélectionnez Modifier.
- Effectuez un clic droit sur le groupe et sélectionnez Modifier.

4. Sélectionnez Modifier.

5. La fenêtre Modifier le groupe apparaît et affiche les paramètres pertinents pour le type de groupe spécifié.

6. Modifiez le groupe selon les besoins.



7. 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. Dans Groupes, sélectionnez le type de groupe souhaité.

La page correspondant au type de groupe sélectionné apparaît.

2. Sélectionnez le groupe que vous souhaitez dupliquer.

OT Security active le bouton Actions.

3. Effectuez l'une des actions suivantes :

- Cliquez sur Actions et sélectionnez Dupliquer.
- Effectuez un clic droit sur le groupe et sélectionnez Dupliquer.

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. Dans Groupes, sélectionnez le type de groupe souhaité.

La page correspondant au type de groupe sélectionné apparaît.

2. Sélectionnez le groupe que vous souhaitez supprimer.

OT Security active le bouton Actions.

3. Effectuez l'une des actions suivantes :

- Cliquez sur Actions et sélectionnez Supprimer.
- Effectuez un clic droit sur le groupe et sélectionnez Supprimer.

4. Sélectionnez Supprimer.

Une fenêtre de confirmation apparaît.

5. Cliquez sur Supprimer.

OT Security supprime définitivement le groupe du système.

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

Rôle utilisateur OT Security requis : Administrateur

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. Dans l'interface Tenable OT Security, accédez à Paramètres > 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

Rôle utilisateur OT Security requis : Administrateur

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



ne clé secrète que vous saisissez dans la console OT Security lors de la configuration de intégration.

Pour effectuer l'intégration à Tenable Vulnerability Management :

1. Dans l'interface Tenable OT Security, accédez à Paramètres > 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

Rôle utilisateur OT Security requis : Administrateur

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)

Rôle utilisateur OT Security requis : Administrateur



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. Dans l'interface Tenable OT Security, accédez à Paramètres > 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

Rôle utilisateur OT Security requis : Administrateur

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. Dans l'interface Tenable OT Security, accédez à Paramètres > 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 afficher des assets et des données de scores de risque dans Tenable Exposure 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.

Après l'intégration, OT Security envoie les données suivantes à Tenable One :

- OT Security synchronise tous les assets et attributs d'assets avec la page Gestion de l'exposition > Inventaire. Ces attributs incluent le fournisseur, la marque, le modèle, l'état, le firmware et le numéro de série. La synchronisation couvre les champs suivants :
 - OT_BACKPLANE_ID
 - OT_BACKPLANE_NAME
 - OT_CATEGORY
 - OT_CRITICALITY
 - OT_DESCRIPTION
 - OT_FAMILY
 - OT_FIRMWARE
 - OT_ID
 - OT_LOCATION
 - OT_MODEL
 - OT_SERIAL_NUMBER
 - OT_SLOT
 - OT_STATE
 - OT_VENDOR
 - OT_SENSOR_NAME



- OT_DIRECT_IP_ADDRESSES
- OT_RISK
- Toutes les détections de vulnérabilités associées aux assets, y compris les ID des plug-ins, leur nom et leur sortie. Tenable One utilise ces données pour déterminer si le statut de vulnérabilité de chaque asset est Active ou Corrigée.
- (Version 4.4 et ultérieures) Toutes les détections de violations de politique associées à chaque asset. Ces données incluent le type d'événement de politique, la sortie de plug-in détaillée décrivant l'événement et les assets impliqués. Elles précisent également les tactiques, techniques et procédures (TTP) MITRE ATT&CK correspondant à l'activité observée.
- (Version 4.5 et ultérieures) Tous les tags dynamiques associés aux assets. Ils apparaissent dans Tenable One en tant que tags externes.

Remarque : les détections OT Security n'apparaissent pas dans Tenable Vulnerability Management ; pour qu'elles y soient visibles, vous devez intégrer Tenable Vulnerability Management à OT Security ou utiliser le moteur OT Discovery dans vos scans.

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. Dans l'interface Tenable OT Security, accédez à Paramètres > 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.

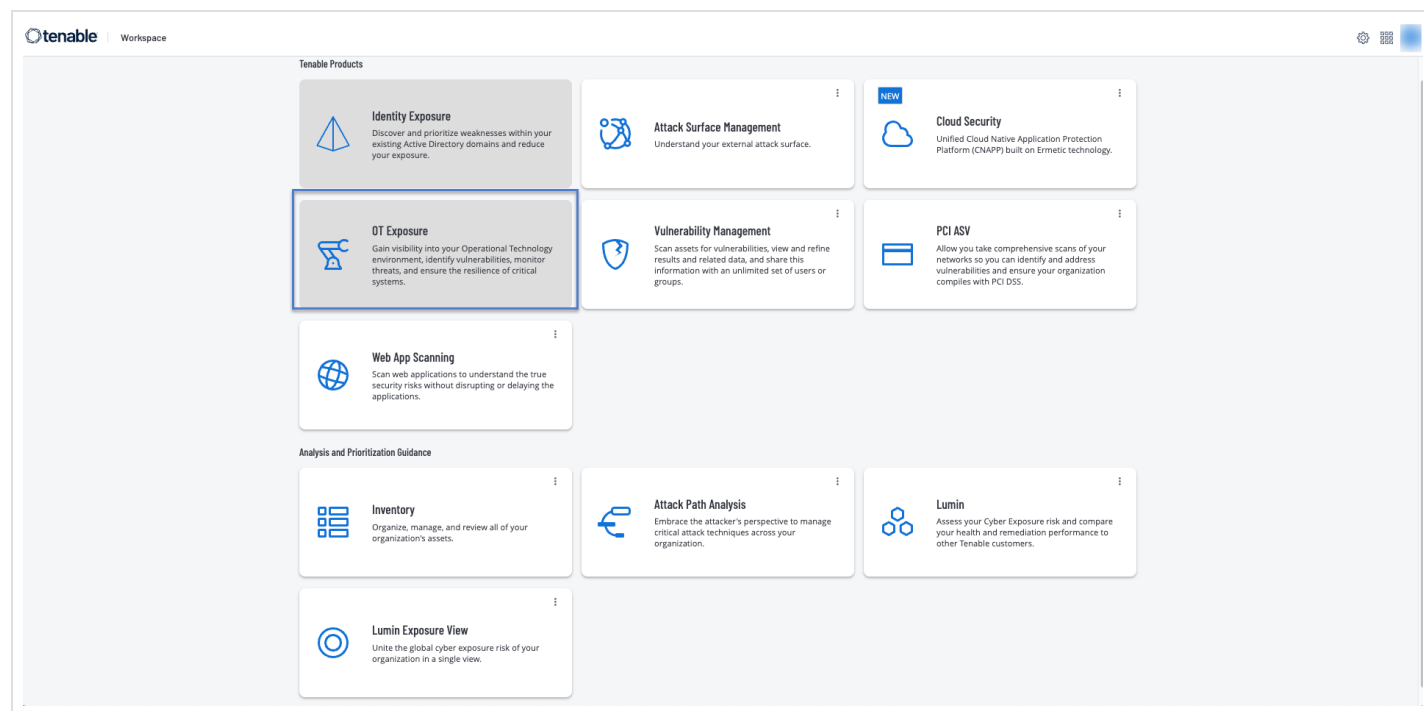
Pour plus d'informations sur la procédure complète de déploiement et gestion des licences de Tenable OT Security pour Tenable One, voir le [Guide de déploiement de Tenable One](#).

Configurer l'intégration SAML pour Tenable One

Configurez SAML sur votre instance Tenable One pour accéder à OT Security via SSO.



La tuile OT Exposure sur la page Tenable One Espace de travail est désactivée par défaut. Pour activer la tuile OT Exposure, vous devez d'abord configurer SAML pour Tenable One.



Avant de commencer

- Vous devez disposer d'une licence Tenable One et OT Security valide.

Pour configurer SAML pour Tenable OT Security :

1. Récupérez les détails du fournisseur d'identité (IDP) SAML et les ID d'objets de groupe à partir de Tenable One :

- a. Dans un navigateur pris en charge, connectez-vous à <https://cloud.tenable.com> pour accéder à la page Espace de travail.
- b. Dans le coin supérieur droit, cliquez sur le bouton .

La page Paramètres apparaît.

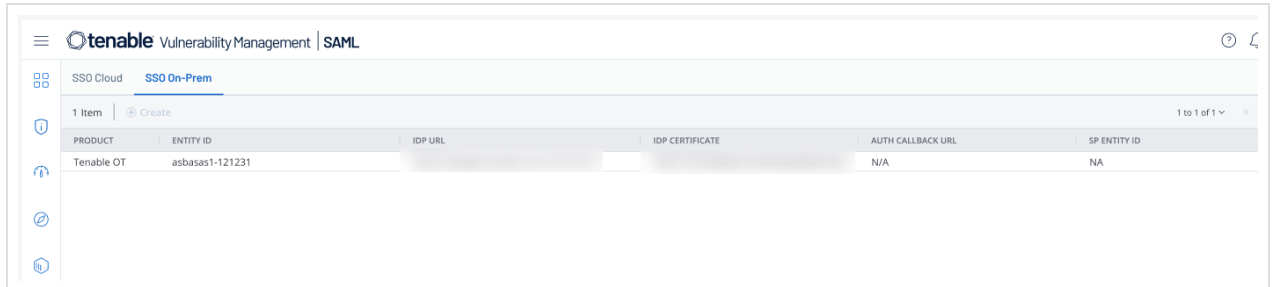
- c. Cliquez sur la tuile SAML.



La page SAML apparaît.

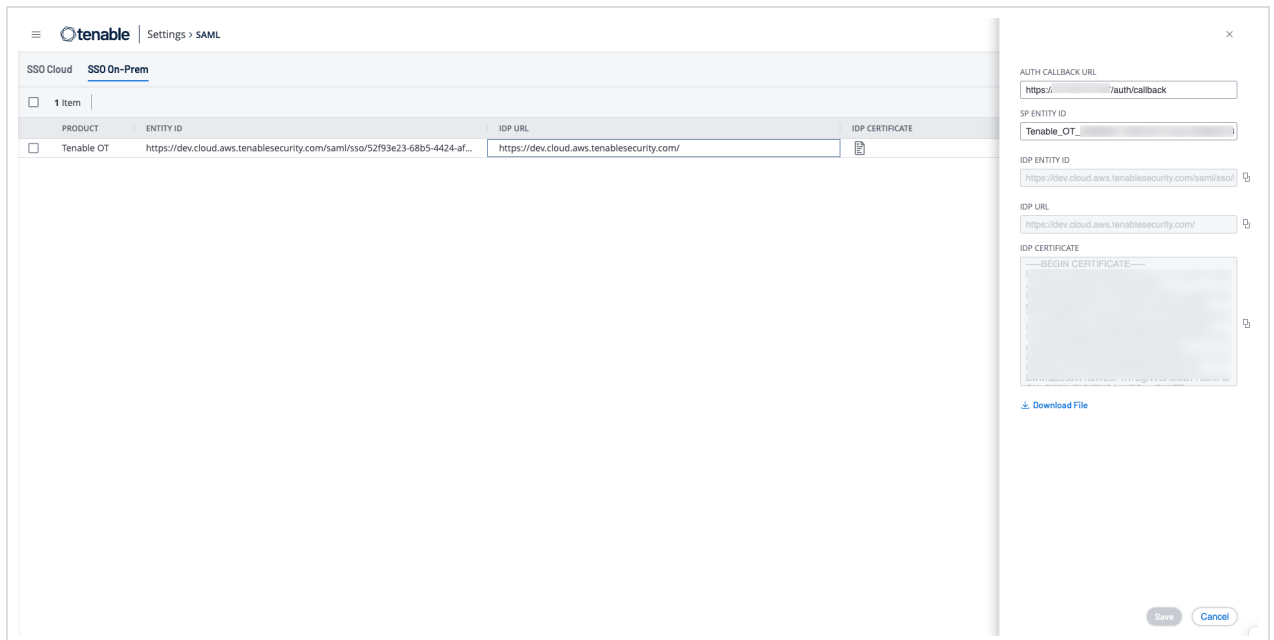
- d. Cliquez sur l'onglet SSO sur site.

La page SSO sur site apparaît avec la configuration SSO pour Tenable OT Security.



- e. Survolez la ligne Tenable OT Security et cliquez dessus.

Le panneau des détails de l'IDP apparaît sur la droite.



- f. Utilisez le bouton  pour copier ces détails.



- ID de l'entité IDP
- URL IDP
- Certificat de l'IDP

- g. Cliquez sur [↓ Télécharger le fichier](#) pour télécharger le certificat sur votre système local.
- h. Récupérez les données de mappage des groupes. Pour trouver les informations sur l'ID d'objet de groupe, accédez à Paramètres > Contrôle d'accès > Groupes et recherchez ou ajoutez les groupes concernés.

Par exemple, dans Tenable One, créez deux groupes : Administrateurs OT et OT en lecture seule. Pour les mapper aux rôles d'utilisateur dans OT Security, ajoutez les noms de groupe aux champs respectifs ID d'objet du groupe Administrateurs et ID d'objet du groupe Utilisateurs en lecture seule sur la page OT Security SAML.



tenable | Settings > Access Control > Groups > Edit User Group

OT Read-Only

General

USER GROUP NAME

OT Read-Only

☐ Managed by SAML ⓘ

USERS

Select Users

OT E2E SSO Access

tenable | Settings > Access Control > Groups > Edit User Group

OT Administrators

General

USER GROUP NAME

OT Administrators

☐ Managed by SAML ⓘ

USERS

Select Users

OT E2E SSO Access - Site Supervisor

Permissions

Search

0 Items | [+ Add Permissions](#)

NAME	USERS
------	-------



2. Configurer SAML dans OT Security :

- a. Connectez-vous à OT Security.
- b. Accédez à locaux > Gestion des utilisateurs > SAML.

La page SAML apparaît.

- c. Cliquez sur Configurer ou Modifier si vous modifiez une configuration existante.

Le panneau Configurer SAML apparaît.

- d. Fournissez les informations suivantes que vous avez copiées à partir de la page Tenable One SAML > SSO sur site :

- a. Dans la zone ID de l'IDP, collez l'ID de l'entité IDP copiée à partir de la page Tenable One SAML.
- b. Dans la zone URL de l'IDP, collez l'URL de l'IDP copiée à partir de la page Tenable One SAML.
- c. Dans la zone Données de certificat, accédez à l'emplacement où vous avez téléchargé le fichier de certificat et chargez-le.
- d. Dans la zone Attribut de nom d'utilisateur, saisissez :

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

- e. Dans la zone Attribut de groupe, saisissez **groupes** (le mot doit être en minuscules, pas Groupes).
- f. Fournissez les informations sur l'ID d'objet de groupe que vous avez récupérées auprès de Tenable One.



Par exemple, à l'étape h, vous avez créé deux groupes dans Tenable One :
Administrateurs et OT en lecture seule. Ajoutez ces noms de groupe aux champs
correspondants ID d'objet du groupe Administrateurs et ID d'objet du groupe
Utilisateurs en lecture seule sur la page Configurer SAML.



Configure SAML



IDP ID *

https://dev.cloud.aws.tenablesecurity.com/saml/sso/d:

IDP URL *

https://dev.cloud.aws.tenablesecurity.com/

CERTIFICATE DATA *

PEM format only

[Replace Current Certificate](#)

USERNAME ATTRIBUTE *

http://schemas.xmlsoap.org/ws/2005/05/identity/claim

GROUPS ATTRIBUTE *

groups

DESCRIPTION

ADMINISTRATORS GROUP OBJECT ID

OT Administrators

READ-ONLY USERS GROUP OBJECT ID

OT Read-Only

SECURITY ANALYSTS GROUP OBJECT ID

Cancel

Save



g. Cliquez sur Enregistrer.

OT Security enregistre la configuration et affiche les informations suivantes :

SAML

☒ SAML single sign-on log-in [Edit](#)

Populate SAML account with the following

ENTITY ID	Tenable_OT_
URL	https://.../auth/callback

Configuration details

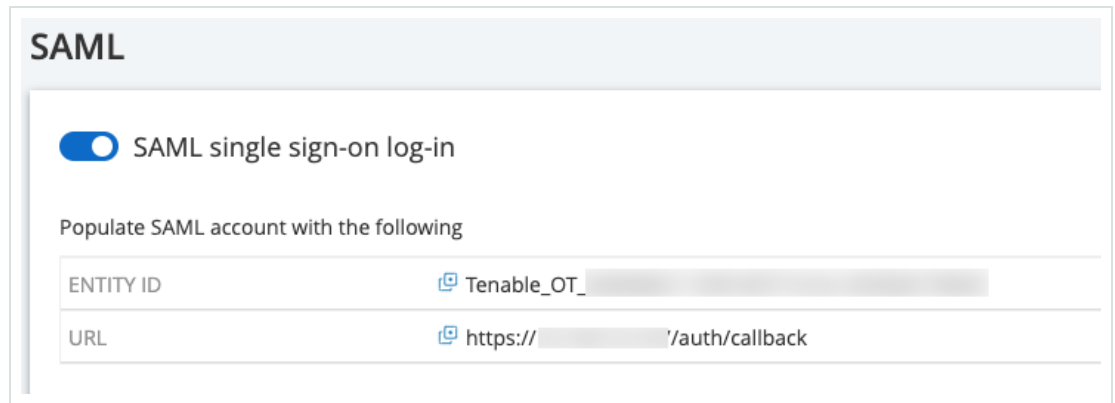
IDP ID	https://dev.cloud.aws.tenablesecurity.com/saml/so/...
IDP URL	https://dev.cloud.aws.tenablesecurity.com/
CERTIFICATE DATA	-----BEGIN CERTIFICATE----- [Redacted] -----END CERTIFICATE----- Read More

USERNAME ATTRIBUTE	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
GROUPS ATTRIBUTE	groups
ADMINISTRATORS GROUP OBJECT ID	OT Administrators
READ-ONLY USERS GROUP OBJECT ID	OT Read-Only

Important : ne redémarrez pas après avoir enregistré la configuration. Ne redémarrez qu'après avoir terminé les étapes de configuration sur OT Security et Tenable One.

h. Sur la page SAML, copiez les valeurs suivantes. Vous avez besoin de ces valeurs pour la configuration finale sur Tenable One.

- ID de l'entité
- URL



SAML

☒ SAML single sign-on log-in

Populate SAML account with the following

ENTITY ID	 Tenable_OT_ [redacted]
URL	 https:// [redacted] /auth/callback

3. Terminez la configuration finale sur Tenable One :

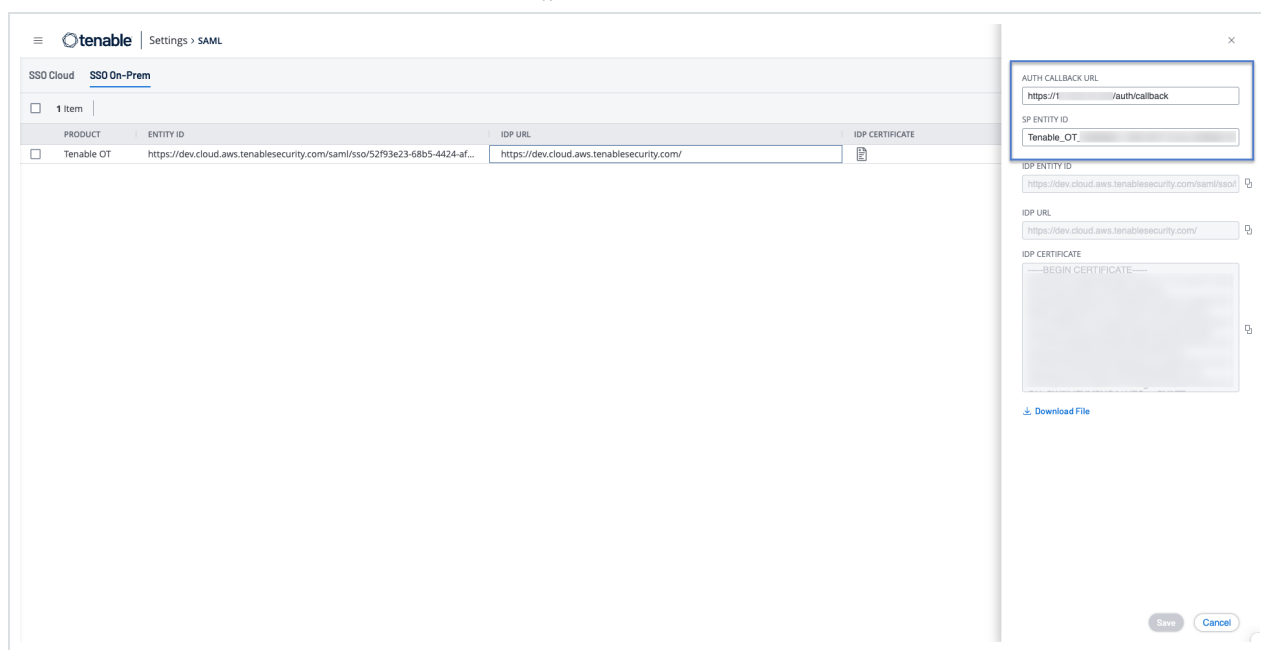
- a. Dans Tenable One, accédez à la page Paramètres > SAML > SSO sur site.

La page SSO sur site apparaît avec la configuration SSO pour Tenable OT Security.

- b. Cliquez sur la ligne OT Security.

Le panneau des détails de la configuration OT Security apparaît.

- c. Fournissez l'URL de rappel d'authentification et les détails de l'ID de l'entité SP copiés à partir de la page SAML de OT Security.



d. Cliquez sur Enregistrer.

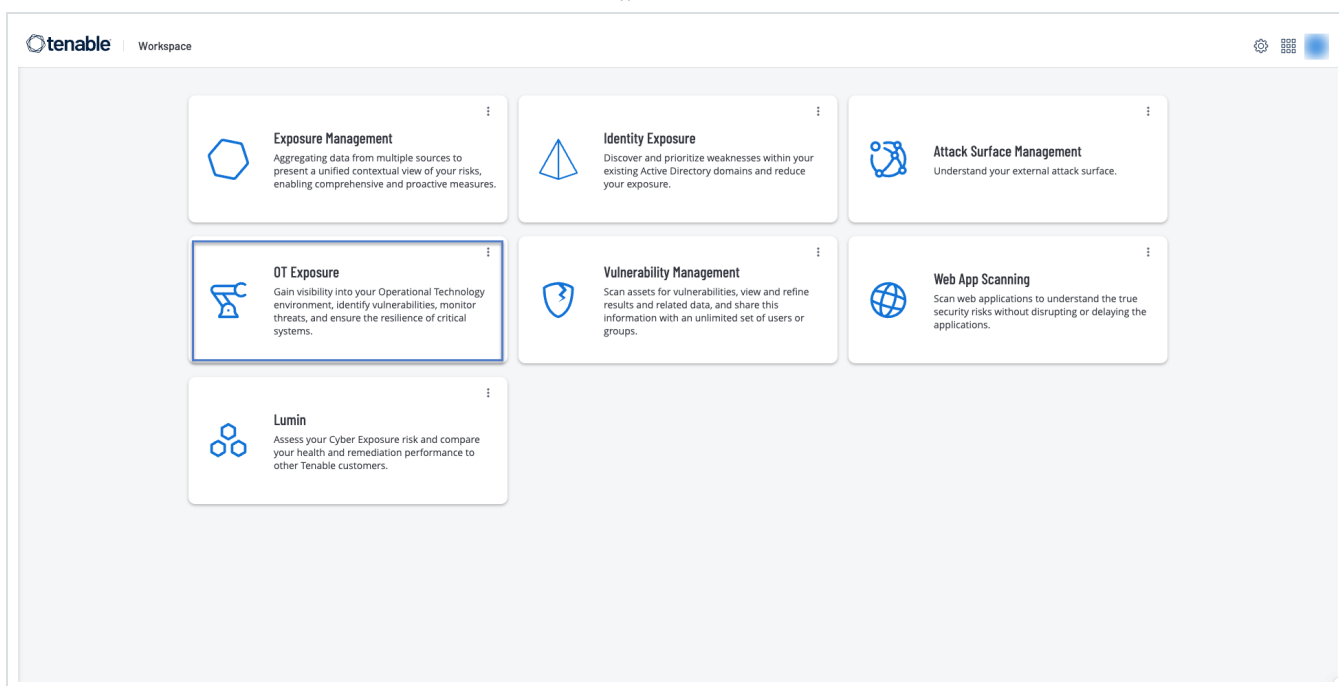
OT Security enregistre la configuration SAML.

4. Cliquez sur le curseur Connexion unique SAML pour activer SAML.

OT Security vous invite à redémarrer.

5. Redémarrez OT Security.

Tenable active la tuile OT Exposure sur la page Espace de travail. Cliquez sur la tuile OT Exposure et accédez à OT Security.



Serveurs

Rôle utilisateur OT Security requis : Administrateur, Superviseur

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



généérés. 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 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 locaux > Serveurs > Serveurs Syslog.
2. Cliquez sur + Ajouter un serveur Syslog. La fenêtre de configuration Serveurs SMTP apparaît.



Syslog Servers

SERVER NAME *

HOSTNAME / IP *

PORT *

TRANSPORT *

☐ Send keep alive message every 10m0s

☒ Allow syslog message caching

Cancel

Create

Send Test Message

Add Syslog Server

Syslog Servers

SERVER NAME *

HOSTNAME / IP *

PORT *

* Transport -



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. Pour chiffrer la transmission syslog à l'aide du chiffrement TLS, cochez la case TLS.

Remarque : lorsque TLS est sélectionné, le port standard 6514 (RFC 5425) est automatiquement suggéré.

11. 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 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 :

Access Control	Permissions	Set All
Security Fabric	☒ None ☐ Read ☐ Read/Write	
FortiView	☒ None ☐ Read ☐ Read/Write	
User & Device	☒ None ☐ Read ☐ Read/Write	
Firewall	☐ None ☐ Read ☒ Read/Write ☐ Custom	
Log & Report	☒ None ☐ Read ☐ Read/Write ☐ Custom	
Network	☐ None ☒ Read ☐ Read/Write ☐ Custom	
System	☒ None ☐ Read ☐ Read/Write ☐ Custom	
Security Profile	☒ None ☐ Read ☐ Read/Write ☐ Custom	
VPN	☒ None ☐ Read ☐ Read/Write	
WAN Opt & Cache	☒ None ☐ Read ☐ Read/Write	
WiFi & Switch	☒ None ☐ Read ☐ Read/Write	

Journal système

Rôle utilisateur OT Security requis : Administrateur

La page Journal système affiche le journal de tous les événements système (par exemple, politique activée, politique modifiée et événement résolu) 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. Pour plus d'informations sur la personnalisation des tableaux, voir [Éléments de l'interface utilisateur de la console de gestion](#).

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.

Envoyer le 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 > 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.

TENB OT RESEARCH AND DEVEL...

Create your own application

 Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

What are you looking to do with your application?

- ☐ Configure Application Proxy for secure remote access to an on-premises application
- ☐ Register an application to integrate with Microsoft Entra ID (App you're developing)
- ☒ Integrate any other application you don't find in the gallery (Non-gallery)

Create

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.

Microsoft Azure

Home > TENB OT Research and Development | Overview > Browse Microsoft Entra Gallery > Tenable_OT

Tenable_OT | SAML-based Sign-on

Enterprise Application

Upload metadata file Change single sign-on mode Test this application Got feedback?

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating Tenable_OT.

- #### Basic SAML Configuration

Identifier (Entity ID) **Required**
 Reply URL (Assertion Consumer Service URL) **Required**
 Sign on URL *Optional*
 Relay State (Optional) *Optional*
 Logout Url (Optional) *Optional*

Edit
- #### Attributes & Claims

Fill out required fields in Step 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- #### SAML Certificates

Token signing certificate

Status: Active

Thumbprint: [Redacted]

Expiration: 11/27/2029, 11:04:39 AM

Notification Email: [Redacted]

App Federation Metadata Url: [Redacted]

Certificate (Base64): [Redacted]

Certificate (Raw): [Redacted]

Federation Metadata XML: [Redacted]

Edit

Download Download Download

2. Dans la section 1 - Configuration SAML de base, cliquez sur Modifier .

Le panneau latéral Configuration SAML de base apparaît.

Copilot

2

TENB OT RESEARCH AND DEVEL...

Basic SAML Configuration

Save

Got feedback?

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Add identifier

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Add reply URL

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Enter a sign on URL

Relay State (Optional)

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Enter a relay state

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.

Enter a logout url

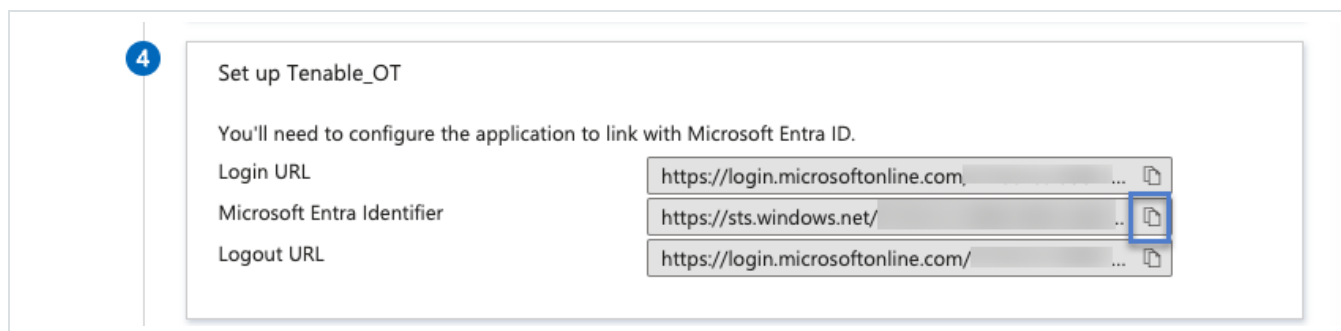
- Dans la zone Identificateur (ID de l'entité), saisissez un identifiant temporaire pour l'application Tenable (par exemple : tenable_ot).



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.



4

Set up Tenable_OT

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	https://login.microsoftonline.com	...	
Microsoft Entra Identifier	https://sts.windows.net/	...	
Logout URL	https://login.microsoftonline.com/	...	

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.



Configure SAML

IDP ID *

IDP URL *

CERTIFICATE DATA *
PEM format only

DROP FILE HERE

Browse

USERNAME ATTRIBUTE *

GROUPS ATTRIBUTE *

DESCRIPTION

ADMINISTRATORS GROUP OBJECT ID

Cancel

Save

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.

[Home](#) > [TENB OT Research and Development | Overview](#) > [Browse Microsoft Entra Gallery](#) > [Tenable_OT | SAML-based Sign-on](#) > [SAML-based Sign-on](#) >

Attributes & Claims

[+ Add new claim](#) [+ Add a group claim](#) [Columns](#) | [Got feedback?](#)

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname [...]

Advanced settings

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.

Microsoft Azure

Home > TENB OT Research and Development | Overview > Browse Microsoft Entra Gallery > Tenable_OT | SAML-based Sign-on > SAML-based Sign-on >

Attributes & Claims

+ Add new claim + Add a group claim Columns Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname [...]

Advanced settings

Group Claims

Manage the group claims used by Microsoft Entra ID to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

☒ All groups

☐ None

☐ Security groups

☐ Directory roles

☐ Groups assigned to the application

Source attribute *

Group ID

☐ Emit group name for cloud-only groups

Advanced options

Save

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].



[Home](#) > [TENB OT Research and Development | Overview](#) > [Browse Microsoft Entra Gallery](#) > [Tenable_OT | SAML-based Sign-on](#) > [SAML-based Sign-on](#) >

Attributes & Claims

[+ Add new claim](#) [+ Add a group claim](#) [Columns](#) | [Got feedback?](#)

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname [...]

Advanced settings

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.

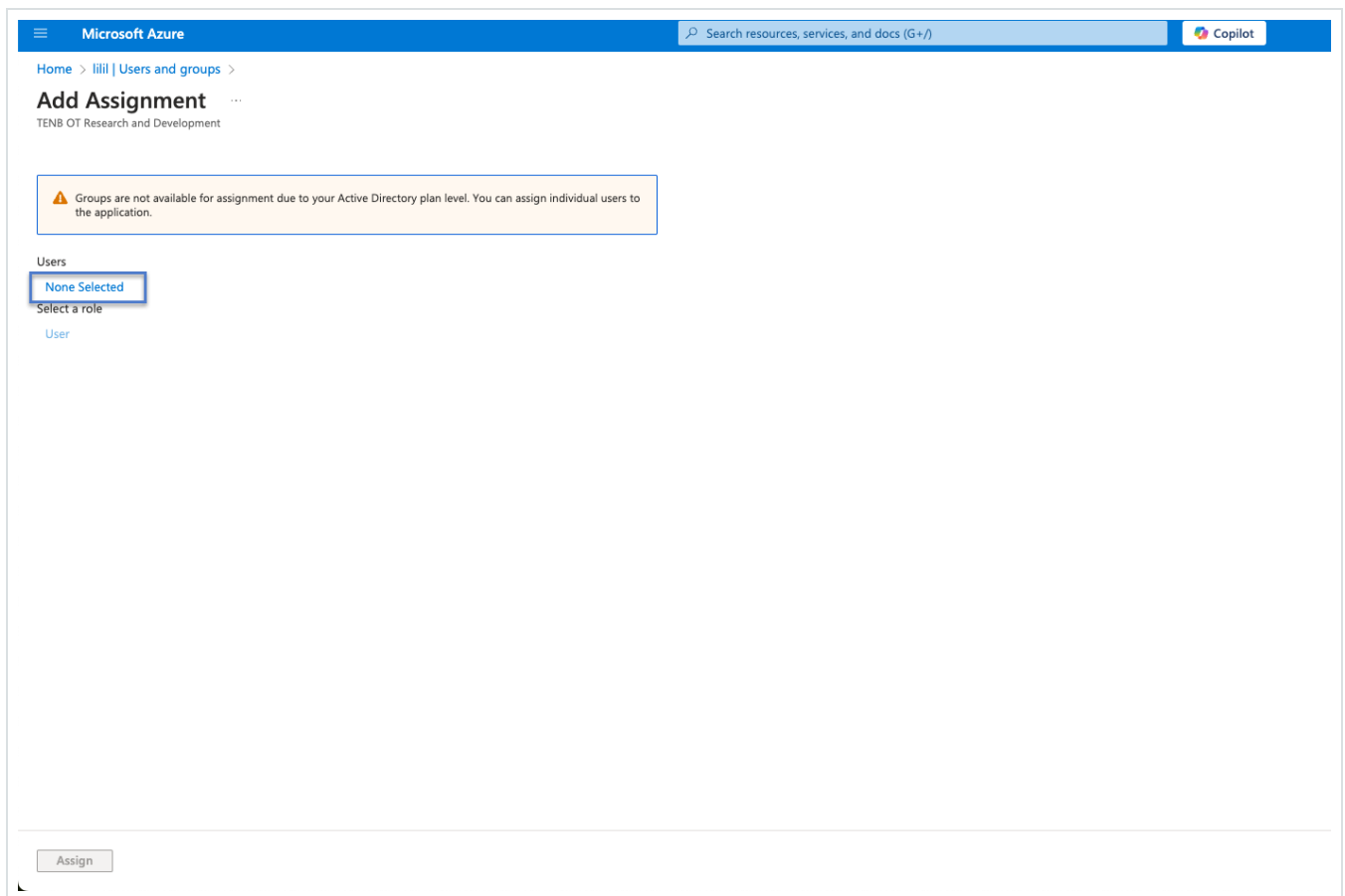


Remarque : les administrateurs connectés via SAML sont considérés comme des administrateurs (externes) et ne bénéficient pas de tous les privilèges des administrateurs locaux. Les utilisateurs affectés à plusieurs groupes d'utilisateurs reçoivent les autorisations les plus élevées possibles parmi leurs groupes.

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.

Users

Try changing or adding filters if you don't see what you're looking for.

Search

25 results found

All Users

	Name	Type	Details
☐	 [Name]	User	[Details]
☐	 [Name]	User	[Details]
☐	 [Name]	User	[Details]
☐	 [Name]	User	[Details]
☐	 [Name]	User	[Details]
☐	 [Name]	User	[Details]
☐	 [Name]	User	[Details]
☐	 [Name]	User	[Details]
☐	 [Name]	User	[Details]
☐	 [Name]	User	[Details]

Select

Selected (0)

Reset

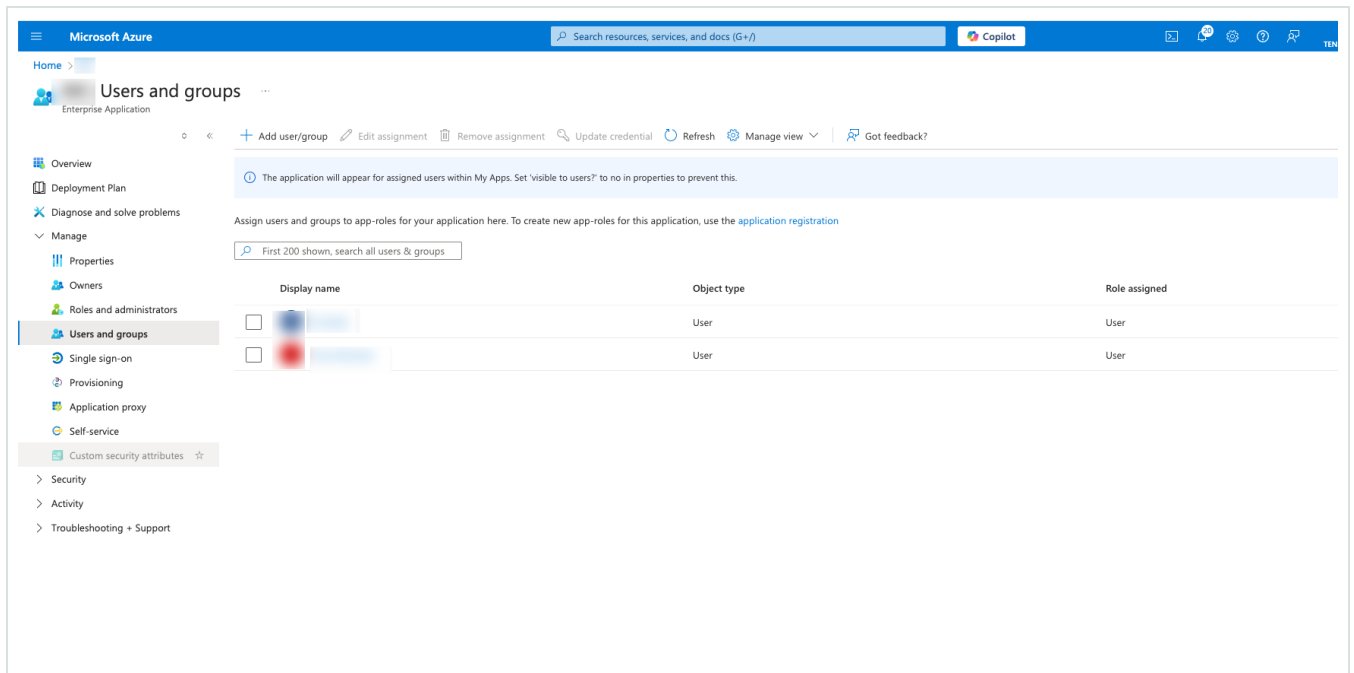
No items selected

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.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Users and groups >

User

Search

Edit properties Delete Refresh Reset password Revoke sessions Manage view Got feedback?

Overview

Audit logs
Sign-in logs
Diagnose and solve problems
Custom security attributes
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods
New support request

Overview Monitoring Properties

Basic info

User principal name
Object ID
Created date time
User type
Identities

Group memberships
Applications
Assigned roles
Assigned licenses

My Feed

Account status
Enabled
Edit

B2B invitation
Invitation state: Accepted
Reset redemption status

Quick actions

Edit properties

7. Dans la colonne ID d'objet, sélectionnez et copiez la valeur du groupe qui sera mappé à Tenable.

Home > Groups

User

Search

Add memberships Remove memberships Refresh Columns Got feedback?

Search groups Add filters

Name	Object id	Group Type	Membership Type	Email	Source
☐ OT_test		Security	Assigned		Cloud



- 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.

Configure SAML ×

GROUPS ATTRIBUTE ✱

fsf

DESCRIPTION

ADMINISTRATORS GROUP OBJECT ID

READ-ONLY USERS GROUP OBJECT ID

SECURITY ANALYSTS GROUP OBJECT ID

SECURITY MANAGERS GROUP OBJECT ID

SITE OPERATORS GROUP OBJECT ID

SUPERVISORS GROUP OBJECT ID

Cancel

Save



9. Répétez les étapes 1 à 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.

SAML

☒ SAML single sign-on log-in Edit

Populate SAML account with the following

ENTITY ID	Tenable_OT_
URL	https://

Configuration details

IDP ID	fsfsf
IDP URL	fsfsf
CERTIFICATE DATA	-----BEGIN CERTIFICATE----- Read More
USERNAME ATTRIBUTE	fsf
GROUPS ATTRIBUTE	fsf
ADMINISTRATORS GROUP OBJECT ID	7D7D

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.

SAML

☒ SAML single sign-on log-in Edit

Populate SAML account with the following

ENTITY ID	 Tenable_OT_
URL	 https://.

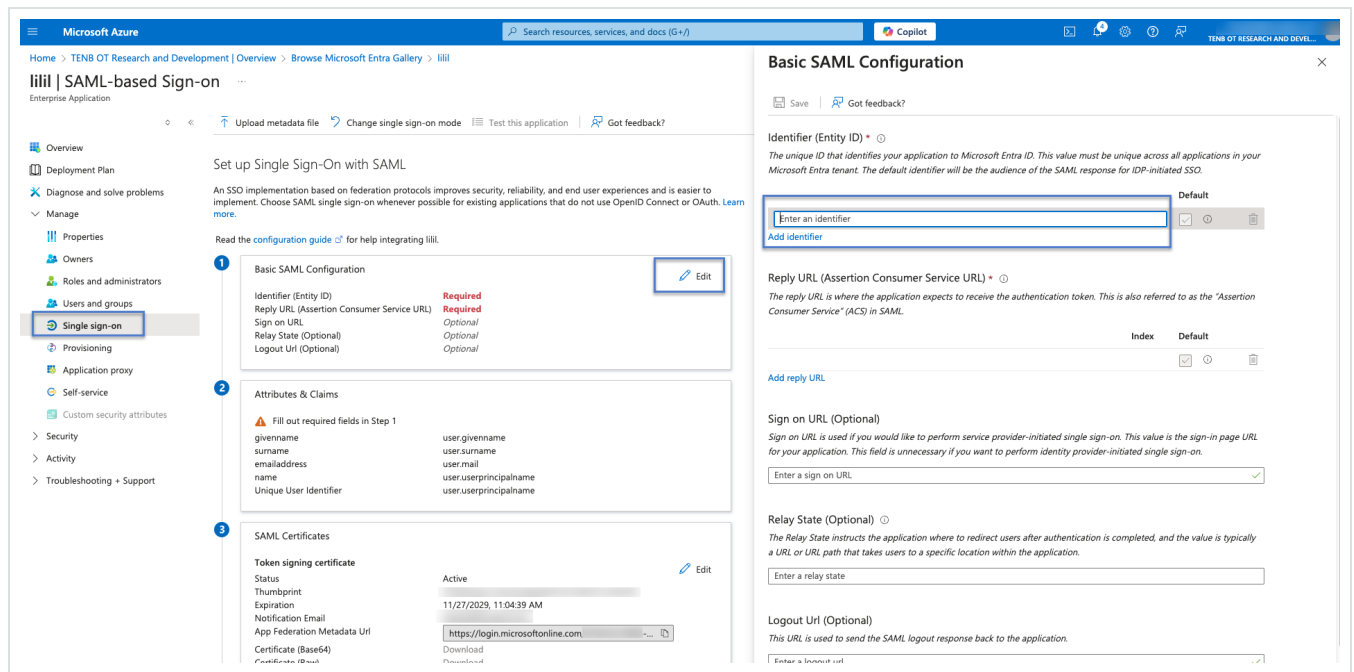
Configuration details

IDP ID	fsfsf
IDP URL	fsfsf
CERTIFICATE DATA	-----BEGIN CERTIFICATE-----  Read More
USERNAME ATTRIBUTE	fsf
GROUPS ATTRIBUTE	fsf
ADMINISTRATORS GROUP OBJECT ID	דגדג

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

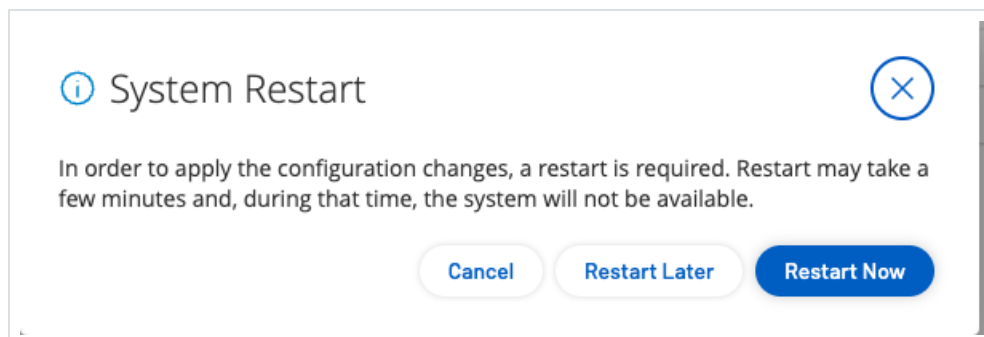
Pour activer l'intégration SAML, vous devez redémarrer OT Security. Vous pouvez redémarrer le système immédiatement ou choisir de le redémarrer plus tard.

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 :

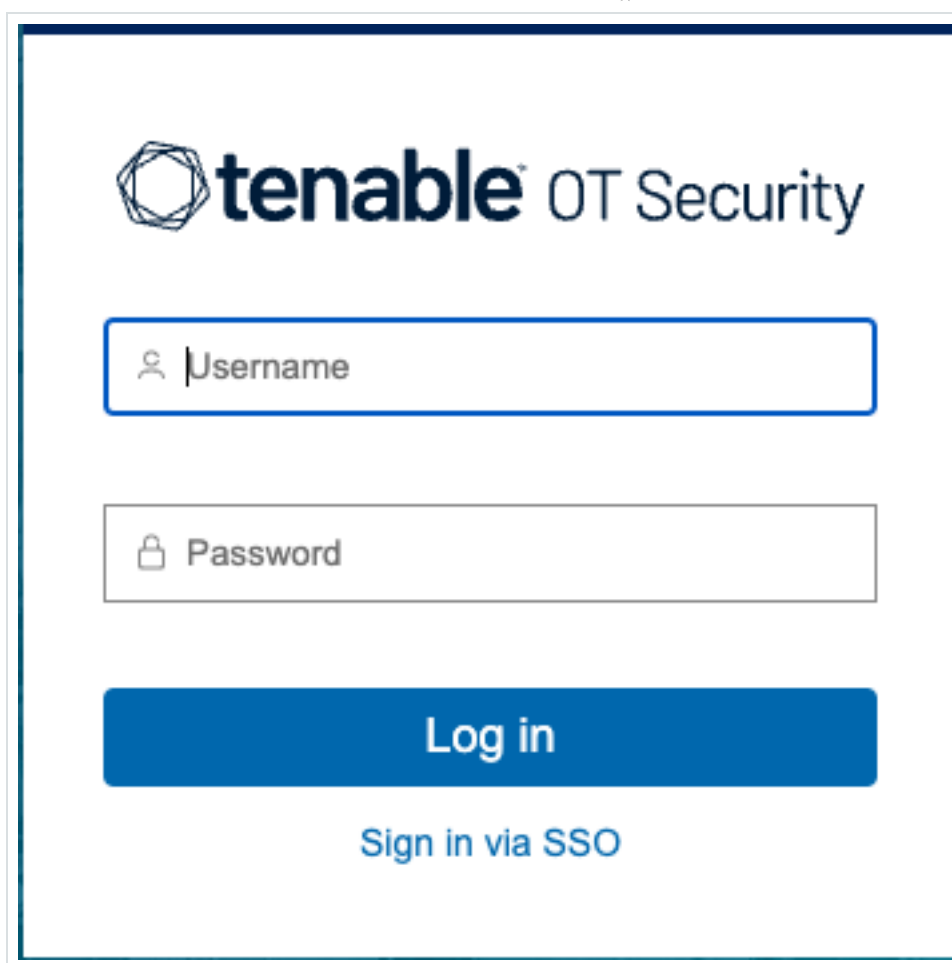


Se connecter via SSO

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).



The image shows the login interface for Tenable OT Security. At the top, there is a logo consisting of a hexagon with internal lines forming a cube-like structure, followed by the text "tenable" in a bold, sans-serif font, and "OT Security" in a regular, sans-serif font. Below the logo, there are two input fields. The first field is labeled "Username" and contains a small icon of a person. The second field is labeled "Password" and contains a small icon of a padlock. Below these fields is a large blue button with the text "Log in" in white. Below the button is a link that says "Sign in via SSO" in blue text.

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.