# TENABLE.OT

## GUIDE DE L'UTILISATEUR

## VERSION 3.15

# HISTORIQUE DES RÉVISIONS

Version du produit : Tenable.ot 3.15

Historique des révisions du document :

| Révision du document | Date | Description |
|---|---|---|
| **1.0** | 8 octobre 2018 | Création de la première version du guide de l'utilisateur pour la version 2.5 |
| **1.1** | 28 janvier 2019 | Mise à jour pour la version 2.7 |
| **1.2** | 20 août 2019 | Mise à jour pour la version 3.1 |
| **1.3** | 10 octobre 2019 | Révision pour les fonctionnalités actuellement prises en charge |
| **1.4** | 12 janvier 2019 | Mise à jour pour la version 3.3 |
| **1.5** | 24 mars 2020 | Mise à jour pour la version 3.4 |
| **1.6** | 6 avril 2020 | Mise à jour pour la version 3.5 |
| **1.7** | 27 avril 2020 | Ajout de documentation sur les capteurs |
| **1.8** | 3 juin 2020 | Mise à jour pour la version 3.6 |
| **1.9** | 8 août 2020 | Mise à jour pour la version 3.7 |
| **2.0** | 11 octobre 2020 | Mise à jour pour la version 3.8 |
| **2.1** | 2 décembre 2020 | Mise à jour pour la version 3.9 |
| **2.2** | 6 avril 2021 | Mise à jour pour la version 3.10 |
| **2.3** | 30 juin 2021 | Mise à jour pour la version 3.11 |
| **2.4** | 12 décembre 2021 | Mise à jour pour la version 3.12 |
| **2.5** | 25 mars 2022 | Mise à jour pour la version 3.13 |
| **2.6** | 22 août 2022 | Mise à jour pour la version 3.14 |
| **2.7** | 25 septembre 2022 | Ajout de l'intégration SAML (SP1) |
| **2.8** | 31 janvier 2023 | Mise à jour pour la version 3.15 |

# Table des matières

**Table des matières** ..... **3**

**Introduction** ..... **9**
- Technologies Tenable.ot ..... 10
- Architecture de la solution ..... 11
  - Composants de la plateforme Tenable.ot ..... 11
  - Composants réseau ..... 11
- Éléments système ..... 12
  - Assets ..... 12
  - Politiques et événements ..... 12

**Composants matériels Tenable.ot** ..... **15**
- Appliance Tenable.ot ..... 15
  - Panneau avant ..... 15
  - Panneau arrière ..... 15
  - Contenu du pack ..... 16
- Capteur Tenable.ot ..... 17
  - Capteur pour montage en rack ..... 17
  - Capteur configurable ..... 19

**Considérations relatives au pare-feu** ..... **21**
- Plateforme Tenable.ot Core ..... 21
- **Capteurs Tenable.ot** ..... 21
- **Requête active** ..... 22
- Intégrations Tenable.ot ..... 22

**Installation de l'appliance Tenable.ot** ..... **23**
- Étape 1 – Configuration de l'appliance Tenable.ot ..... 23
  - Montage en rack ..... 23
  - Surface plane ..... 23
- Étape 2 – Connexion de Tenable.ot au réseau ..... 24
- Étape 3 – Connexion à la console de gestion ..... 24
- Étape 4 – Assistant de configuration ..... 27
  - Écran 1 – Informations utilisateur ..... 27
  - Écran 2 – Appareil ..... 28
  - Écran 3 – Heure système ..... 30
- Étape 5 – Gestion de licence ..... 32
  - Conditions préalables ..... 32
  - Activation de votre licence ..... 32
- Étape 6 – Activation du système ..... 37

Étape 7 – Connexion du port de gestion séparé (pour l'option de séparation des ports) ..... 38

**Installation d'un capteur Tenable.ot ..... 39**

Appairage des capteurs avec l'ICP ..... 39

Conditions préalables ..... 39

Appairage du capteur ..... 39

**Éléments de l'interface utilisateur de la console de gestion ..... 43**

Principaux éléments de l'interface utilisateur ..... 43

Activer/désactiver le mode sombre ..... 44

Vérification de la version actuelle du logiciel ..... 44

Écrans principaux ..... 45

Utilisation des listes ..... 46

Personnalisation de l'affichage des colonnes ..... 46

Regroupements ..... 47

Tri ..... 48

Filtres ..... 49

Recherche ..... 49

Exportation des données ..... 50

Menus Actions ..... 50

**Dashboards ..... 51**

Dashboard Risque ..... 52

Dashboard Inventaire ..... 53

Dashboard Événements et politiques ..... 53

Interagir avec les dashboards ..... 54

Mode graphique ..... 54

Mode tableau ..... 56

Modification du dashboard par défaut ..... 57

Exportation de dashboard ..... 57

**Politiques ..... 58**

Configuration des politiques ..... 58

Groupes ..... 58

Niveaux de sévérité ..... 59

Notifications d'événement ..... 59

Catégories et sous-catégories de politiques ..... 60

Types de politiques ..... 60

Activer et désactiver les politiques ..... 65

Affichage des politiques ..... 67

Affichage des détails d'une politique ..... 68

Création de politiques ..... 70

Création de politiques d'écriture non autorisée ..... 75
Autres actions sur les politiques ..... 76
Modification de politiques ..... 76
Duplication de politiques ..... 78
Suppression de politiques ..... 80
Suppression d'exclusions de politique ..... 81
Groupes ..... 82
Groupes d'assets ..... 83
Segments réseau ..... 87
Groupes de messagerie ..... 90
Groupes de ports ..... 92
Groupes de protocoles ..... 95
Groupe de planification ..... 97
Groupes de tags ..... 101
Groupes de règles ..... 104
Actions sur les groupes ..... 106

**Inventaire ..... 111**
Affichage des assets ..... 111
Types d'assets ..... 113
Affichage des détails d'un asset ..... 118
Volet d'en-tête ..... 119
Onglet Détails ..... 120
Révisions de code ..... 120
Itinéraire IP ..... 124
Vecteurs d'attaque ..... 124
Ports ouverts ..... 127
Vulnérabilités ..... 129
Événements ..... 129
Cartographie du réseau ..... 131
Ports du périphérique ..... 132
Modification des détails d'un asset ..... 133
Modification des détails d'un asset via l'interface utilisateur ..... 133
Modification des détails d'un asset en téléchargeant un fichier CSV ..... 135
Masquer des assets ..... 137
Exécution d'un scan Nessus spécifique à un asset ..... 137
Exécution d'une resynchronisation ..... 138

**Événements ..... 140**
Affichage des événements ..... 140
Affichage des détails d'un événement ..... 143

Affichage des clusters d'événements ..... 144
Résolution d'événements ..... 144
Résolution d'événements individuels ..... 144
Résolution de tous les événements ..... 146
Création d'exclusions de politique ..... 147
Téléchargement de fichiers de capture individuels ..... 151
Téléchargement d'un fichier PCAP ..... 151
Création de politiques FortiGate ..... 151

**Réseau ..... 153**
Récapitulatif réseau ..... 153
Définition d'une période d'activité ..... 154
Trafic et communications au fil du temps ..... 155
Top 5 sources ..... 155
Top 5 cibles ..... 156
Protocoles ..... 156
Captures de paquets ..... 157
Filtrage de l'affichage de la capture de paquets ..... 158
Activation/désactivation des captures de paquets ..... 158
Téléchargement de fichiers ..... 159
Communications ..... 160

**Cartographie du réseau ..... 161**
Regroupements d'assets ..... 162
Application de filtres à l'affichage de la cartographie ..... 165
Affichage des détails d'un asset ..... 166
Définition d'une base de référence réseau ..... 166

**Vulnérabilités ..... 167**
Écran Vulnérabilités ..... 167
Détails du plug-in ..... 168
Modification des détails d'une vulnérabilité ..... 169

**Paramètres locaux ..... 170**
Requêtes ..... 172
Toutes les requêtes de contrôleur ..... 172
Toutes les requêtes réseau ..... 173
Découverte des assets ..... 175
Scans de plug-in Nessus ..... 177
Configuration système ..... 181
Appareil ..... 181
Requêtes ping ..... 182

Captures de paquets ..... 182
Approuver automatiquement les demandes d'appairage des capteurs ..... 183
Activer les statistiques d'utilisation ..... 183
Capteurs ..... 183
Configuration des ports ..... 186
Mises à jour ..... 186
Certificat ..... 193
Licence ..... 195
Configuration de l'environnement ..... 201
Paramètres d'un asset ..... 201
Clusters d'événements ..... 202
Lecteur PCAP ..... 203
Utilisateurs et rôles ..... 204
Utilisateurs locaux ..... 204
Affichage des utilisateurs locaux ..... 204
Ajout d'utilisateurs locaux ..... 205
Actions supplémentaires sur les comptes utilisateur ..... 206
Groupes d'utilisateurs ..... 208
Serveurs d'authentification ..... 217
SAML ..... 224
Intégrations ..... 226
Produits Tenable ..... 226
Palo Alto Networks – Pare-feu de nouvelle génération (NGFW) ..... 226
Aruba – Gestionnaire de politiques ClearPass ..... 226
Serveurs ..... 227
Serveurs SMTP ..... 227
Serveurs Syslog ..... 228
Pare-feu FortiGate ..... 229
Journal système ..... 231
Envoi du journal système à un serveur Syslog ..... 231

**Annexe 1 – Installation d'un capteur (Versions 3.13 et antérieures) ..... 232**
Étape 1 - Configuration du capteur ..... 232
Configuration d'un capteur pour montage en rack ..... 232
Configuration d'un capteur configurable ..... 234
Étape 2 – Connexion du capteur au réseau ..... 236
Étape 3 – Accès à l'assistant de configuration du capteur ..... 237
Étape 4 – Assistant de configuration du capteur ..... 239

**Annexe 2 – Intégration SAML pour Azure Active Directory ..... 241**
Configuration de l'intégration ..... 241

Étape 1 – Création de l'application Tenable dans Azure ..... 241
Étape 2 – Configuration initiale ..... 242
Étape 3 – Mappage des utilisateurs Azure aux groupes Tenable ..... 246
Étape 4 – Finalisation de la configuration dans Azure ..... 250
Étape 5 – Activation de l'intégration ..... 251
Connexion à l'aide d'une authentification unique (SSO) ..... 252

# Introduction

**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 Tenable permettent de maximiser la visibilité, la sécurité et le contrôle de vos environnements opérationnels.

**Tenable.ot** fournit des outils et des rapports de sécurité complets pour le personnel de sécurité IT et les ingénieurs OT. La solution offre une visibilité inégalée sur les segments IT et OT convergés et sur l'activité ICS, et elle vous fournit un état des lieux clair et détaillé de tous les sites et de leurs assets OT respectifs, des serveurs Windows aux fonds de panier de contrôleur PLC, le tout au travers d'une vue centralisée.

**Tenable.ot** 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. Tenable.ot s'intègre également de manière native aux principaux 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 nouvelle génération et les systèmes de tickets. Tous ces éléments combinés forment un écosystème de confiance où tous vos produits de sécurité fonctionnent de façon coordonnée pour assurer la sécurité de votre environnement.
- **Détection et atténuation des menaces** – Tenable.ot 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 révolutionnaire, Tenable.ot offre une visibilité inégalée sur votre infrastructure, non seulement au niveau du réseau, mais jusqu'à l'appareil lui-même. Tenable.ot utilise des protocoles de communication natifs pour interroger activement 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, Tenable.ot génère des niveaux de vulnérabilité et de risque via Predictive Prioritization (priorisation prédictive) pour chaque asset de votre réseau ICS. Ces rapports incluent une évaluation des scores de risque, des informations exploitables détaillées, ainsi que des suggestions d'atténuation.
- **Contrôle des configurations** – Tenable.ot 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.

# Technologies Tenable.ot

La solution complète Tenable.ot comprend deux technologies de collecte principales :

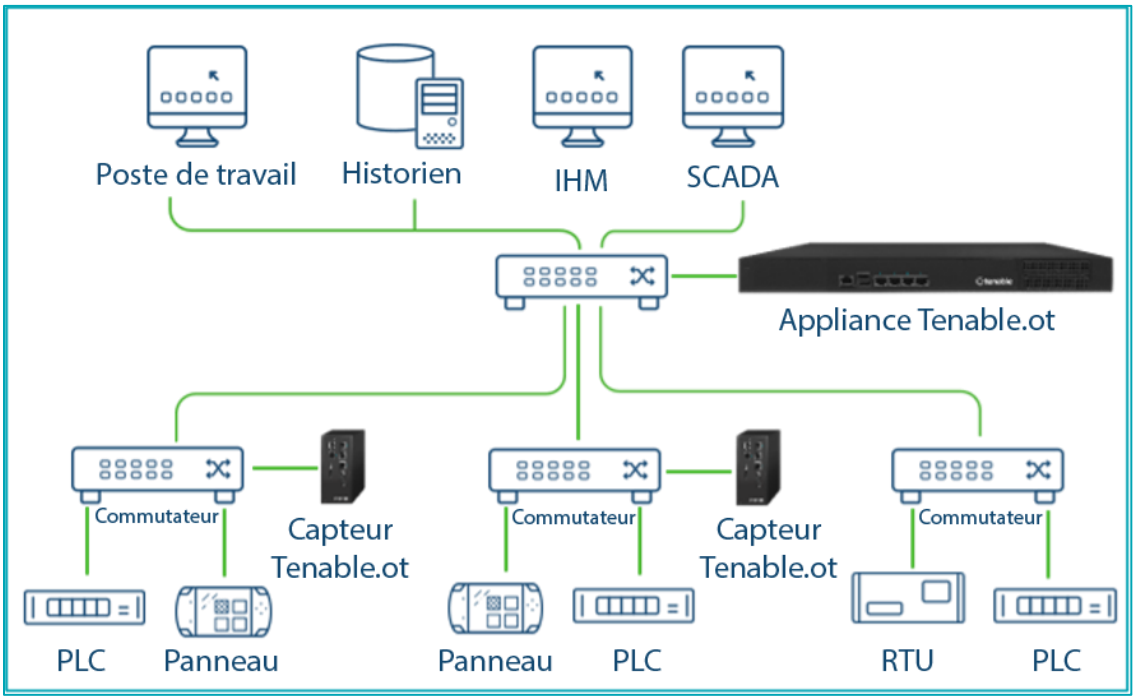
- **Détection réseau** – La technologie de détection de réseau de Tenable.ot est un moteur passif d'inspection approfondie des paquets, spécialement conçu pour répondre aux caractéristiques et aux exigences uniques des systèmes de contrôle industriels. La détection réseau offre une visibilité approfondie 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 autorisée et/ou liste bloquée 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 Tenable.ot 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 Tenable.ot 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 permet d'être totalement 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 Tenable.ot

La solution Tenable.ot est constituée de deux composants :

- **Appliance Tenable.ot** – 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 des capteurs Tenable.ot. L'appliance Tenable.ot exécute à la fois les fonctions de détection réseau et de requête active.
- **Capteurs Tenable.ot** – Désigne 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 sont disponibles en 2 formats : montage en rack compact ou montage sur rail DIN. Les capteurs Tenable.ot offrent une visibilité totale sur ces segments de réseau : ils capturent l'ensemble du trafic, l'analysent, puis communiquent les informations à l'appliance Tenable.ot. Les capteurs versions 3.14 et supérieures peuvent également être configurés pour envoyer des requêtes actives aux segments de réseau sur lesquels ils sont déployés.




Déploiement réseau de l'appliance Tenable.ot et des capteurs

## Composants réseau

Tenable.ot prend en charge l'interaction avec les composants réseau suivants :

- **Utilisateur Tenable.ot (gestion)** – Des comptes d'utilisateurs sont créés pour contrôler l'accès à la console de gestion Tenable.ot. La console de gestion est accessible sur un navigateur web (Google Chrome) via une authentification HTTPS en SSL (Secure Socket Layer).

L'interface utilisateur n'est accessible qu'à partir d'un navigateur Chrome. Vous devez également utiliser la dernière version de Chrome.

- **Serveur Active Directory** – Les informations d'identification 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.
- **SIEM** – Les journaux d'événements Tenable.ot peuvent être envoyés à un SIEM à l'aide du protocole Syslog.
- **Serveur SMTP** – Les notifications d'événements Tenable.ot 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 Tenable.ot pour aider à résoudre les noms d'assets.
- **Applications tierces** – Les applications externes peuvent interagir avec Tenable.ot à l'aide de son API REST, ou accéder aux données à l'aide d'autres intégrations spécifiques[1].

# Éléments système

## Assets

Les assets représentent les composants matériels de votre réseau, tels que les contrôleurs, les stations d'ingénierie, les serveurs, etc. Les fonctions automatisées de découverte, de classification et de gestion des assets de Tenable.ot 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

Tenable.ot 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).

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

- **Vulnérabilités** – Désigne les CVE qui affectent les assets de votre réseau, ainsi que d'autres menaces identifiées sur le réseau (par exemple, systèmes d'exploitation obsolètes, utilisation de protocoles vulnérables, ports ouverts vulnérables, etc.). Tenable.ot 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.

> 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 sont utilisées pour définir 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 d'une *Définition de politique* pour une politique donnée, un événement est généré dans le système. L'événement est consigné dans le système et des notifications sont envoyées conformément aux *Actions de politique* configurées pour la politique.

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

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)** – Par exemple, 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** – Par exemple, 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** – Par exemple, 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** – Par exemple, 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. L'utilisateur peut 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'événement 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 de Tenable.ot. 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 matériels Tenable.ot

## Appliance Tenable.ot

### Panneau avant


| Composant | Description |
|---|---|
| **Voyant d'alimentation** | Indique si l'appliance Tenable.ot est allumée (vert) ou éteinte. |
| **Port console** | Non utilisé |
| **Ports USB** | Non utilisés |
| **Ports Ethernet** | Quatre ports GbE sont utilisés pour se connecter aux réseaux de gestion et opérationnels comme suit :<br>Port 1 – Par défaut, ce port est utilisé à la fois pour la gestion (interface utilisateur) et comme port de requête active (qui communique avec les assets du réseau). Cette configuration de port peut être modifiée (au moment de la configuration ou plus tard dans la page Paramètres) pour inclure uniquement les requêtes. L'idée est de séparer l'interface de gestion du réseau des contrôleurs.<br>Port 2 – Port miroir : utilisé comme destination de la session de mise en miroir (SPAN). Ce port reçoit une copie du trafic réseau. Ce port ne dispose pas d'adresse IP.<br>Port 3 – Si l'option de séparation des ports est activée, ce port est utilisé uniquement pour la gestion (IU) et peut être connecté à un réseau qui ne fait pas partie du réseau du contrôleur.<br>Port 4 – Port réservé, utilisé par les services de conseil de Tenable.ot pour l'assistance locale ou à distance. |

### Panneau arrière

| Composant | Description |
|---|---|
| **Ventilateurs de refroidissement** | Deux ventilateurs de refroidissement. Assurez-vous que les ventilateurs ne sont pas obstrués. |
| **Interrupteur d'alimentation** | Interrupteur ON/OFF. Maintenez enfoncé pendant quelques secondes pour éteindre. |
| **Port d'alimentation** | Connecteur d'alimentation CA ; 100–240 V CA |

### Contenu du pack

| Composant | Description |
|---|---|
| **Deux câbles Ethernet** | Deux câbles Ethernet RJ45 standard. Utilisez ces câbles pour connecter l'appliance Tenable.ot au commutateur réseau. |
| **Port d'alimentation** | Connecteur d'alimentation CA ; 100–240 V CA. |
| **Supports de montage** | 2 supports de montage en rack 1U. |

# Capteur Tenable.ot

## Capteur pour montage en rack

> Le capteur pour montage en rack n'est plus disponible. Au lieu de cela, nous proposons désormais un kit d'adaptateur qui vous permet de fixer le modèle de capteur configurable à un montage en rack.


### Panneau avant

| Composant | Description |
|---|---|
| **Port console** | Non utilisé |
| **Ports USB** | Non utilisés |
| **Ports Ethernet** | Quatre ports 1GbE sont utilisés pour se connecter aux réseaux de gestion et opérationnels comme suit :<br>Port 1 – Port de gestion : utilisé pour gérer l'appareil.<br>Port 2 – Port miroir : utilisé comme destination de la session de mise en miroir (SPAN). Ce port reçoit une copie du trafic réseau. Ce port ne dispose pas d'adresse IP.<br>Port 3 – Non utilisé.<br>Port 4 – Non utilisé. |

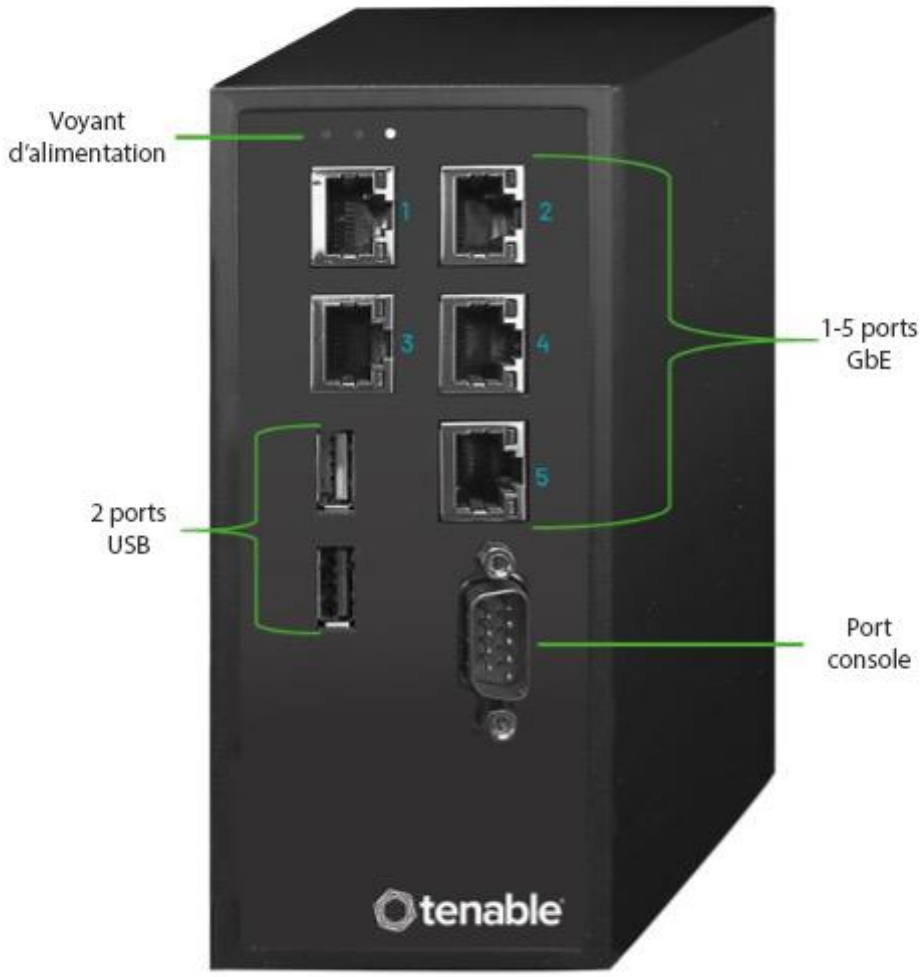
## Panneau arrière

| Composant | Description |
|---|---|
| **Bouton d'alimentation** | Mode veille (en rouge) ; Mode sous tension (en vert). |
| **Bouton de réinitialisation** | Redémarre le système sans couper l'alimentation. |
| **Interrupteur d'alimentation** | Interrupteur ON/OFF. Maintenez enfoncé pendant quelques secondes pour éteindre. |
| **Port d'alimentation** | Connecteur d'alimentation CA ; 100–240 V CA |

## Contenu du pack

| Composant | Description |
|---|---|
| **Câble Ethernet** | Câble Ethernet RJ45 standard. Utilisez ce câble pour connecter le capteur au commutateur réseau. |
| **Câble d'alimentation** | Câble d'alimentation secteur local standard. |
| **Alimentation** | Adaptateur d'alimentation CA 60 W ; 100–240 V CA. |
| **Supports de montage** | 2 supports de montage en rack 1U en L. |
| **Paquet de vis** | |

### Capteur configurable




Ce modèle peut être monté soit sur un rail DIN, soit sur un rack de montage (à l'aide du kit d'adaptateur). Par le passé, ce modèle était appelé Capteur pour rail DIN.

#### Panneau avant

| Composant | Description |
|---|---|
| **Voyant d'alimentation** | Indique si le capteur est allumé (vert) ou éteint. |
| **Port console** | Non utilisé |
| **Ports USB** | Non utilisé |

| Composant | Description |
|---|---|
| **Ports Ethernet** | Cinq ports GbE sont utilisés pour se connecter aux réseaux de gestion et opérationnels comme suit :<br>Port 1 – Port de gestion : utilisé pour gérer l'appareil.<br>Port 2 – Non utilisé.<br>Port 3 – Port miroir : utilisé comme destination de la session de mise en miroir (SPAN). Ce port reçoit une copie du trafic réseau. Ce port ne dispose pas d'adresse IP.<br>Port 4 – Non utilisé.<br>Port 5 – Non utilisé. |

## Contenu du pack

| Composant | Description |
|---|---|
| **Câble d'alimentation** | Câble d'alimentation secteur local standard. |
| **Alimentation** | Adaptateur d'alimentation CA 60 W ; 100–240 V CA. |
| **Câble Ethernet** | Câble Ethernet RJ45 standard. Utilisez ce câble pour connecter le capteur au commutateur réseau. |
| **Oreilles de montage** | 2 supports de montage en rack 1U en L (« oreilles »). |
| **Paquet de vis** | |

# Considérations relatives au pare-feu

Lors de la configuration de votre système Tenable.ot, il est important de déterminer quels ports doivent rester ouverts pour que le système Tenable puisse fonctionner correctement. Les tableaux suivants indiquent quels ports doivent être laissés ouverts pour utiliser la plateforme Tenable.ot Core et les capteurs Tenable.ot. D'autres tableaux indiquent également les ports requis pour exécuter des requêtes actives, ainsi que pour l'intégration avec Tenable.io et Tenable.sc.

## Plateforme Tenable.ot Core

Les ports suivants doivent rester ouverts pour assurer la communication avec la plateforme Tenable.ot Core.

| Sens du flux | Port | Communique avec | Usage |
|---|---|---|---|
| Entrant | TCP 443 | Interface web pour Tenable.ot | Accès par navigateur à Tenable.ot |
| Entrant | TCP 8000 | Interface web pour Tenable Core | Accès par navigateur à Tenable Core |
| Entrant | TCP 22 | Capteurs | Communication du capteur |
| Entrant | TCP 22 | Appliance pour l'accès SSH | Accès par ligne de commande au système d'exploitation ou à l'appliance |
| Sortant* | TCP 443 | Tenable.sc | Envoie les données pour intégration |
| Sortant* | TCP | cloud.tenable.com | Envoie les données pour intégration |
| Sortant* | Divers protocoles industriels | PLC/contrôleurs | Requête active |
| Sortant* | TCP 25 | Serveur de messagerie pour les alertes | SMTP (e-mails d'alerte, rapports) |
| Sortant* | UDP 514 | Serveur Syslog | Serveur Syslog |
| Sortant* | UDP 53 | Serveur DNS | Résolution de nom |
| Sortant* | UDP 123 | Serveur NTP | Service de temps |
| Sortant* | TCP 636 | Serveur AD | Authentification AD LDAP |
| Sortant* | TCP 443 | Fournisseur SAML | Authentification unique |
| Sortant* | UDP 161 | Serveur SNMP | Surveillance SNMP vers Tenable Core |
| Sortant* | TCP\443 | *.tenable.com | Mises à jour automatiques des plug-ins, des applications et du système d'exploitation** |

* services optionnels

** procédure hors ligne disponible

## Capteurs Tenable.ot

Les ports suivants doivent rester ouverts pour la communication avec les capteurs Tenable.ot.

| Sens du flux | Port | Communique avec | Usage |
|---|---|---|---|
| Entrant | TCP 8000 | Interface web | Accès du navigateur à l'IGU |
| Sortant | TCP 22 | Appliance Tenable.ot | Communication du capteur |
| Entrant | TCP 22 | Appliance pour l'accès SSH | Accès par ligne de commande au système d'exploitation ou à l'appliance |
| Sortant* | TCP 25 | Serveur de messagerie pour les alertes | SMTP (e-mails d'alerte, rapports) |

| Sens du flux | Port | Communique avec | Usage |
|---|---|---|---|
| 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 |

* services optionnels

## Requête active

Les ports suivants doivent rester ouverts afin d'utiliser la fonction d'active querying Requête active.

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

* utilisé exclusivement pour le fournisseur

** selon la marque et le modèle des appareils, d'autres ports et protocoles peuvent être nécessaires

# Intégrations Tenable.ot

Les ports suivants doivent rester ouverts pour communiquer avec les intégrations Tenable.io et Tenable.sc.

| Sens du flux | Port | Communique avec | Usage |
|---|---|---|---|
| Sortant | TCP 443 | cloud.tenable.com | Intégration Tenable.io |
| Sortant | TCP 443 | Tenable.sc | Intégration Tenable.sc |

# Installation de l'appliance Tenable.ot

## Étape 1 – Configuration de l'appliance Tenable.ot

L'appliance Tenable.ot peut être soit montée en rack, soit simplement posée sur une surface plane (telle qu'un bureau).

### Montage en rack

➡ **Pour monter l'appliance Tenable.ot sur un rack standard (19 pouces) :**

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

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

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

### Surface plane

➡ **Pour installer l'appliance Tenable.ot sur une surface plane :**

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

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

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

# Étape 2 – Connexion de Tenable.ot au réseau

Tenable.ot est utilisé à la fois pour les fonctions Requête active et Surveillance réseau.

- **Pour assurer la surveillance du réseau**, vous devrez connecter l'unité à un port de mise en miroir sur le commutateur réseau, qui est connecté aux contrôleurs/PLC pertinents.
- **Pour effectuer une requête active**, vous devrez connecter l'unité à un port standard possédant une adresse IP sur le commutateur réseau, qui est connecté aux contrôleurs/PLC pertinents.

Par défaut, la fonction Requête active et la console de gestion sont configurées pour utiliser le même port sur l'unité (Port 1). Après la configuration initiale, il est cependant possible de séparer le port de gestion du port de requête active, en configurant la gestion sur le port 3. Après cette configuration, vous devez connecter le port 3 de l'unité à un port standard du commutateur pour effectuer la gestion comme décrit à l'**Étape 7 – Connexion du port de gestion séparé (pour l'option de séparation des ports)**.

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

### ➡ Pour connecter l'appliance Tenable.ot au commutateur réseau :

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

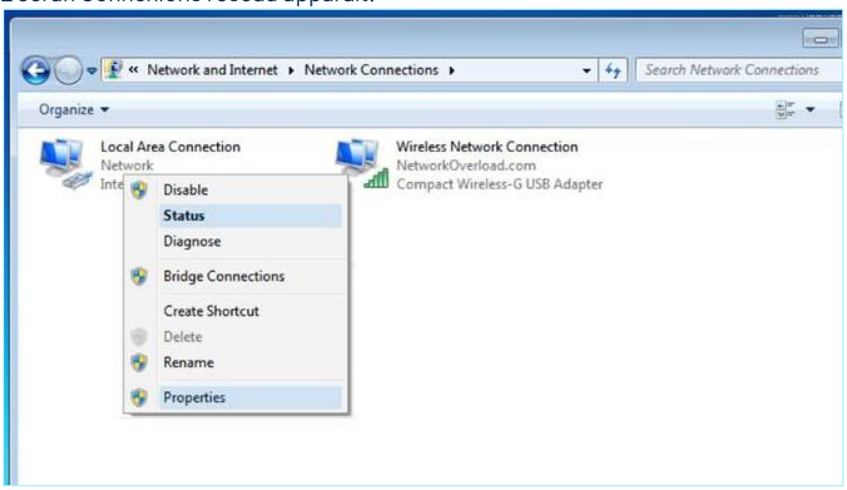
# Étape 3 – Connexion à la console de gestion

### ➡ Pour se connecter à la console de gestion :

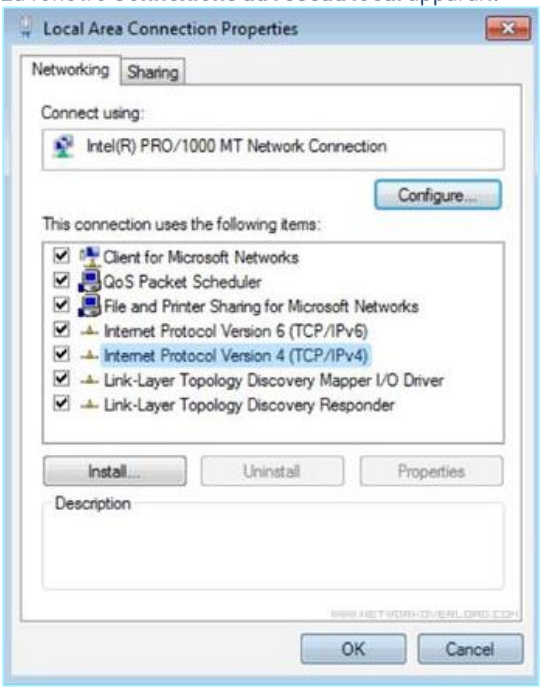
1. Effectuez l'une des actions suivantes :
   - Connectez le poste de travail de la console de gestion (PC, ordinateur portable, etc.) directement au port 1 de l'appliance Tenable.ot à l'aide du câble Ethernet, OU
   - Connectez le poste de travail de la console de gestion au commutateur réseau.
2. Assurez-vous que le poste de travail de la console de gestion fait partie du même sous-réseau que l'appliance Tenable.ot (qui est 192.168. 1.0/24) 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 à l'appliance Tenable.ot) :
   a. Accédez à **Réseau et Internet** > **Centre Réseau et partage** > **Modifier les paramètres de la carte**.

La navigation peut varier légèrement selon la version de Windows.

b. L'écran Connexions réseau apparaît.




c. Effectuez un clic droit sur **Connexions au réseau local** et sélectionnez **Propriétés**. La fenêtre **Connexions au réseau local** apparaît.



d. Sélectionnez **Protocole Internet version 4 (TCP/IPv4)** et cliquez sur **Propriétés**.
La fenêtre Propriétés d'Internet Protocol Version 4 (TCP/IPv4) apparaît.


e. Sélectionnez **Utiliser l'adresse IP suivante**.
f. Dans le champ Adresse IP, saisissez ***192.168.1.10***
g. Dans le champ Masque de sous-réseau, saisissez ***255.255.255.0***.
h. Cliquez sur **OK**.
Les nouveaux paramètres sont appliqués.

4. À partir de votre navigateur web Chrome, accédez à https://192.168.1.5.
L'écran de bienvenue de l'assistant de configuration apparaît.


L'interface utilisateur n'est accessible qu'à partir d'un navigateur Chrome. Vous devez également utiliser la dernière version de Chrome.

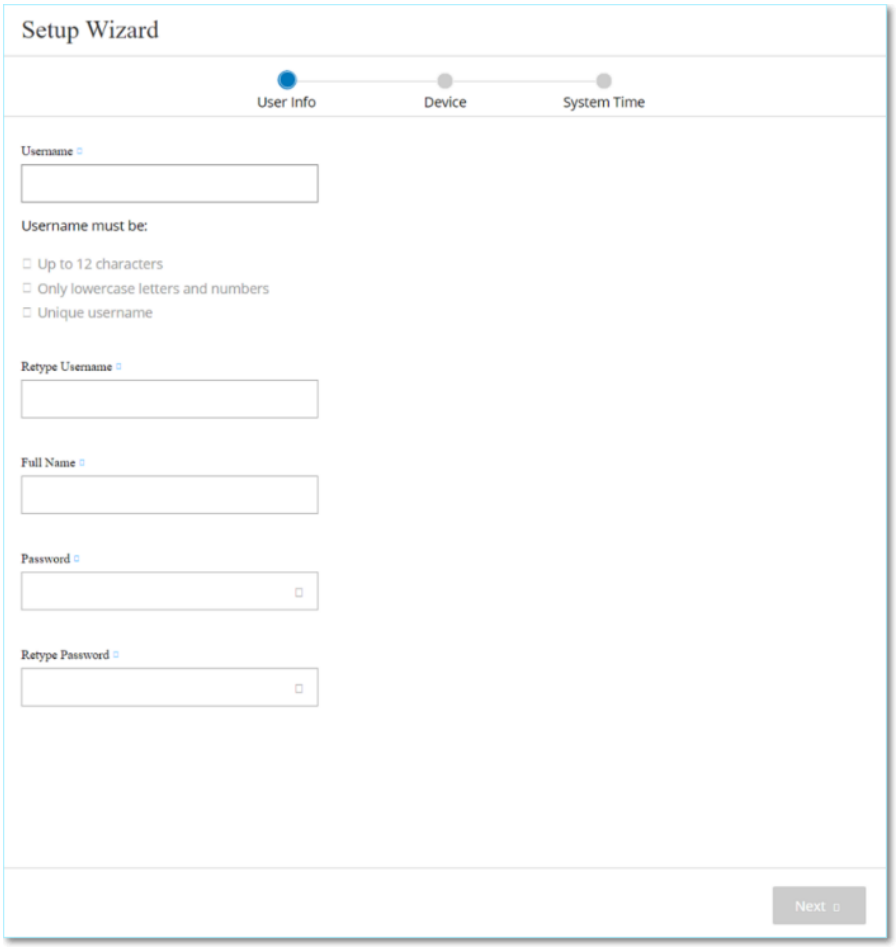
5. Cliquez sur **Démarrer l'assistant de configuration**.
L'assistant de configuration apparaît et affiche la page **Informations utilisateur**.

# Étape 4 – Assistant de configuration

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

Si vous souhaitez modifier la configuration ultérieurement, vous pourrez le faire dans l'écran **Paramètres** de la console de gestion (IU).

### Écran 1 – Informations utilisateur




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

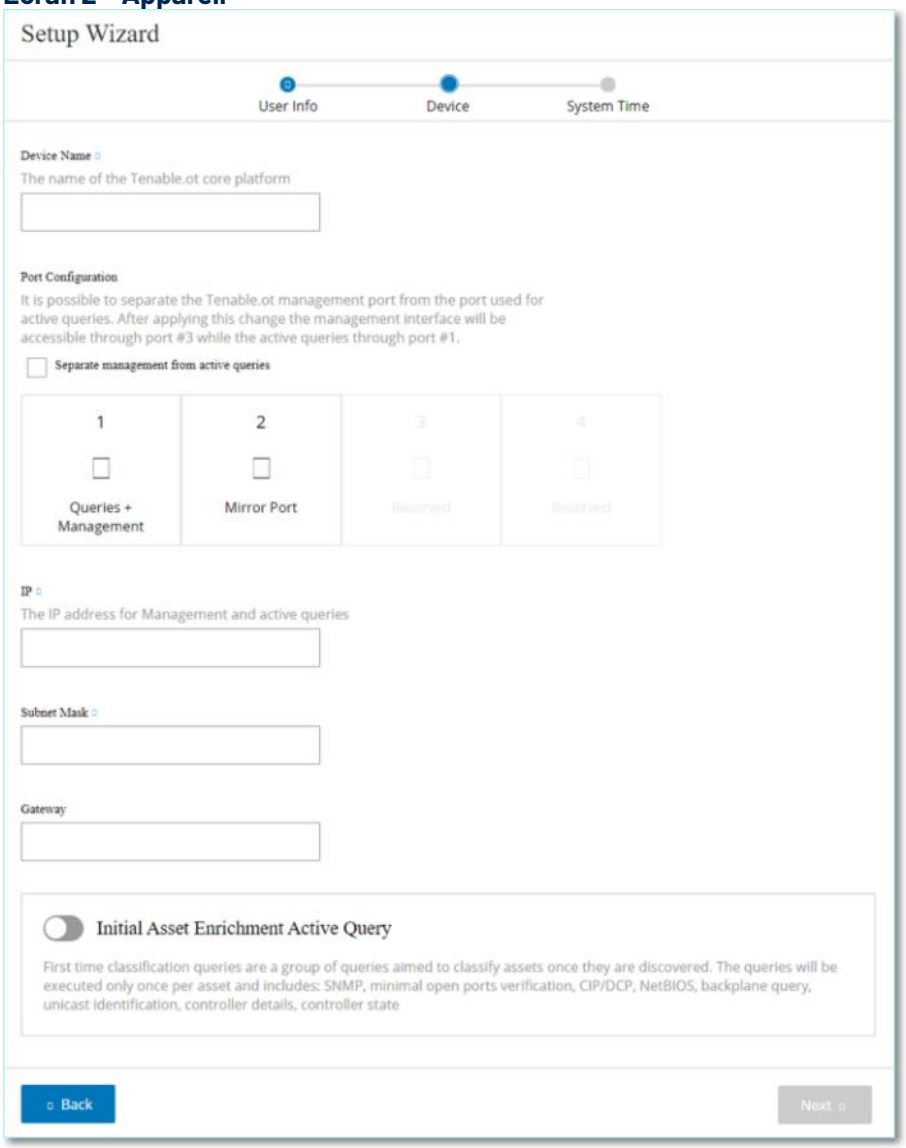
Dans l'assistant de configuration, vous allez configurer les informations d'identification pour un compte administrateur. Après vous être connecté à l'interface utilisateur, vous pourrez créer des comptes utilisateur supplémentaires. Pour plus d'informations sur les comptes utilisateur, voir **Utilisateurs et rôles**.

1. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur pour vous connecter 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 le champ **Confirmer le nom d'utilisateur**, saisissez à nouveau le même nom d'utilisateur.
3. Dans la section **Nom complet**, saisissez vos **prénom et nom de famille**.

C'est le nom qui apparaîtra dans la barre d'en-tête et sur les journaux de votre activité dans le système.

4. Dans le champ **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 le champ **Confirmer le mot de passe**, ressaisissez le même mot de passe.
6. Cliquez sur **Suivant**.
   La page **Appareil** de l'assistant de configuration apparaît.

### Écran 2 – Appareil



### ➡ Sur la page Appareil, renseignez les informations de la plateforme Tenable.ot comme suit :

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

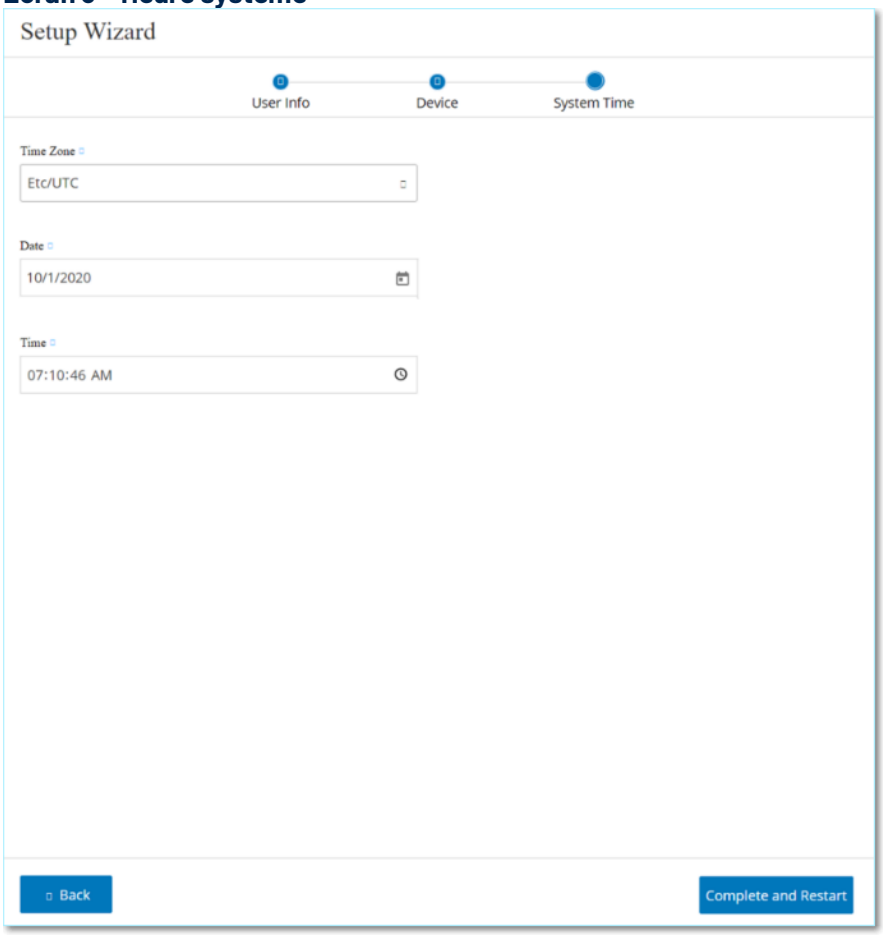
Sur certains systèmes, l'option de **séparation des ports** peut ne pas être disponible. Contactez votre agent d'assistance pour obtenir de l'aide.

   - **Aucune séparation** – Pour maintenir les requêtes et la gestion sur le même port, ne sélectionnez pas **Gestion séparée des requêtes actives**. Dans ce cas, vous pouvez ignorer les étapes 3 à 5 de cette procédure et passer à l'**étape 6.**
3. Si vous avez sélectionné l'option de **séparation des ports**, dans le champ **IP des requêtes actives**, saisissez l'adresse IP du *port de requêtes* de l'unité. Ce port sera connecté à un port standard du commutateur réseau, qui peut communiquer avec (c'est-à-dire être routé vers) les contrôleurs. De plus, étant donné que Tenable.ot se connectera activement aux contrôleurs, il aura besoin d'une adresse IP dans le sous-réseau du réseau.
4. Si vous avez sélectionné l'option de **séparation des ports**, dans le champ **Masque de sous-réseau des requêtes actives**, saisissez le masque de sous-réseau du *port de requêtes*.
5. Si vous avez sélectionné l'option de **séparation des ports**, dans le champ optionnel **Passerelle des requêtes actives** , saisissez l'adresse IP de la passerelle dans le réseau opérationnel.
6. Dans le champ **IP de gestion**, saisissez l'adresse IP (dans le sous-réseau du réseau) à appliquer à la plateforme Tenable.ot. Elle devient l'adresse IP de gestion de Tenable.ot. Il s'agit également de l'adresse des *requêtes* s'il n'y a pas de séparation entre les ports.
7. Dans le champ **Masque de sous-réseau de gestion**, saisissez le masque de sous-réseau du réseau.
8. Pour configurer une passerelle (facultatif), saisissez l'adresse IP de la passerelle du réseau dans le champ **Passerelle de gestion**.

Si vous ne renseignez pas ce champ, Tenable.ot ne pourra pas communiquer avec des composants externes en dehors du sous-réseau (par exemple, serveurs de messagerie, serveurs syslog, etc.).

9. *Requête active pour l'enrichissement initial de l'asset* est une série de requêtes exécutées sur chaque asset découvert dans le système. Elle aide Tenable.ot à classifier les assets. Pour exécuter ces requêtes sur chaque nouvel asset découvert, **activez** l'option associée dans la zone inférieure de la fenêtre.
10. Cliquez sur **Suivant**.
    La page **Heure système** de l'assistant de configuration apparaît.

### Écran 3 – Heure système



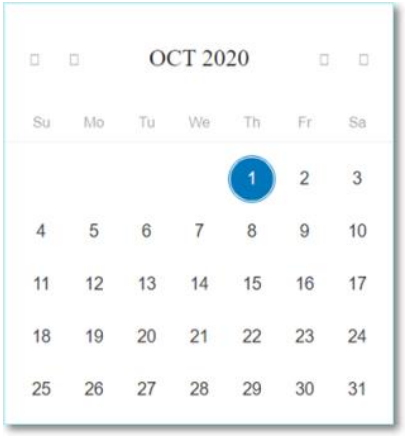

Sur la page **Heure système**, l'heure et la date correctes sont généralement définies automatiquement.

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

**➡ Si la date et l'heure ne sont pas correctement définies, remplissez les informations comme suit.**

1. Dans le champ **Fuseau horaire**, sélectionnez dans la liste déroulante le fuseau horaire local correspondant à l'emplacement du site.

2. Dans le champ **Date**, cliquez sur l'icône du calendrier .
   Un calendrier apparaît dans une fenêtre pop-up.




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

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

5. Pour finaliser la procédure de configuration, cliquez sur **Terminer et redémarrer**.
   Une fois le redémarrage terminé, vous êtes redirigé vers l'écran de gestion de la licence.

# Étape 5 – Gestion de licence

Avant de pouvoir activer le système, vous devez enregistrer votre licence Tenable.ot.

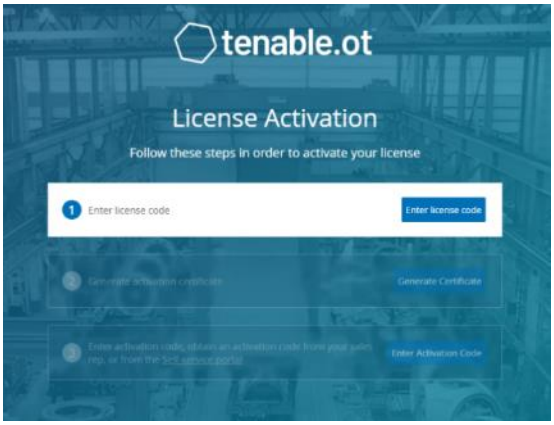
### Conditions préalables

- Le code de licence (20 caractères, lettres et chiffres) que vous avez reçu de Tenable lorsque vous avez commandé votre appareil.
- Vous devez avoir accès à Internet. Si votre appareil Tenable.ot n'est pas connecté à Internet, vous pouvez enregistrer la licence depuis n'importe quel PC.

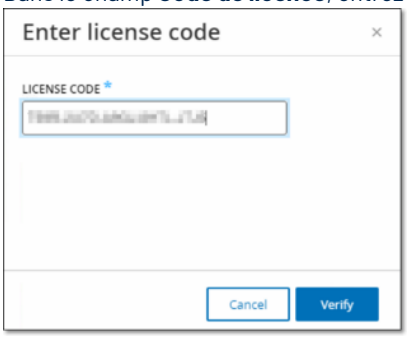
### Activation de votre licence

➡ **Pour activer votre licence :**

1. Sur l'écran d'**activation de la licence**, à l'étape 1, dans le champ **Saisissez le code de licence**, cliquez sur le bouton **Saisir le code de licence**.

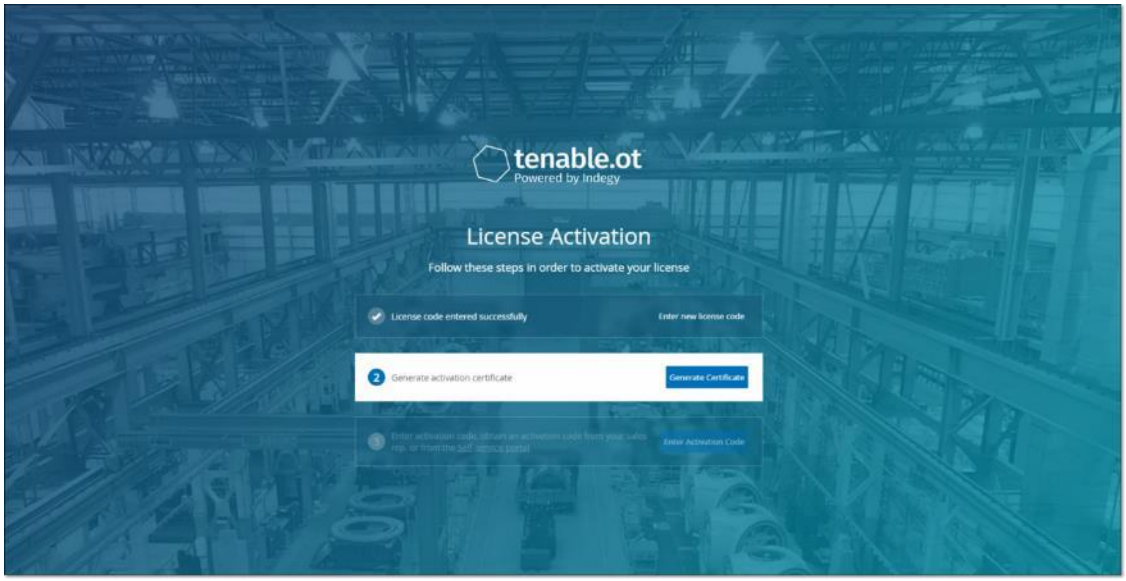



   Le panneau latéral **Saisissez le code de licence** apparaît alors sur le côté droit.
2. Dans le champ **Code de licence**, entrez votre code de licence et cliquez sur **Vérifier**.



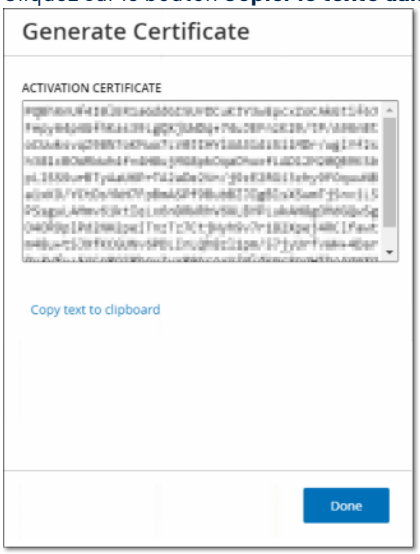

   Le panneau latéral se referme.

3. À l'étape 2, dans le champ **Generate activation certificate** (Générer un certificat d'activation), cliquez sur **Generate Certificate** (Générer un certificat).



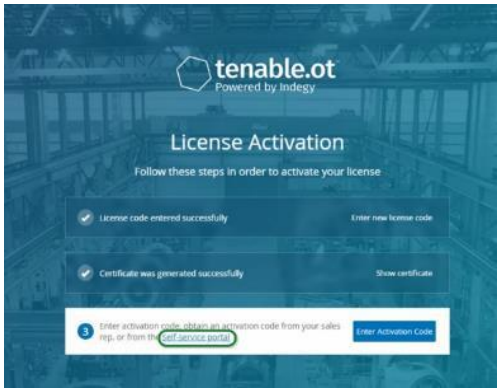

Le panneau latéral **Generate Certificate** (Générer un certificat) apparaît avec le certificat d'activation.

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

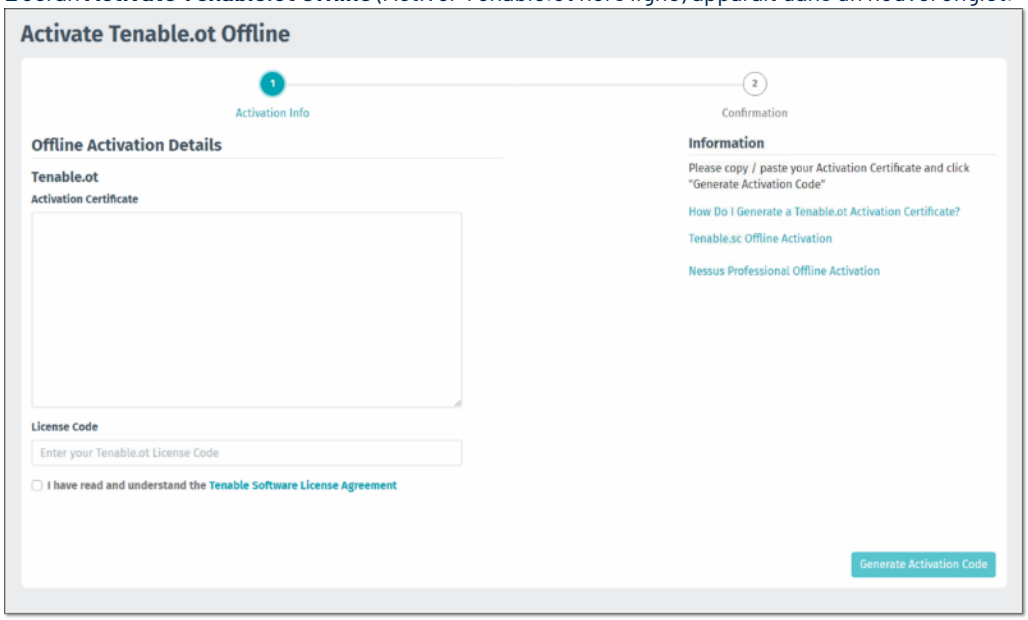



Le panneau latéral se referme.

5. À l'étape 3, dans le champ **Enter activation code** (Saisissez le code d'activation), cliquez sur le lien **Portail libre-service**.




L'écran **Activate Tenable.ot Offline** (Activer Tenable.ot hors ligne) apparaît dans un nouvel onglet.



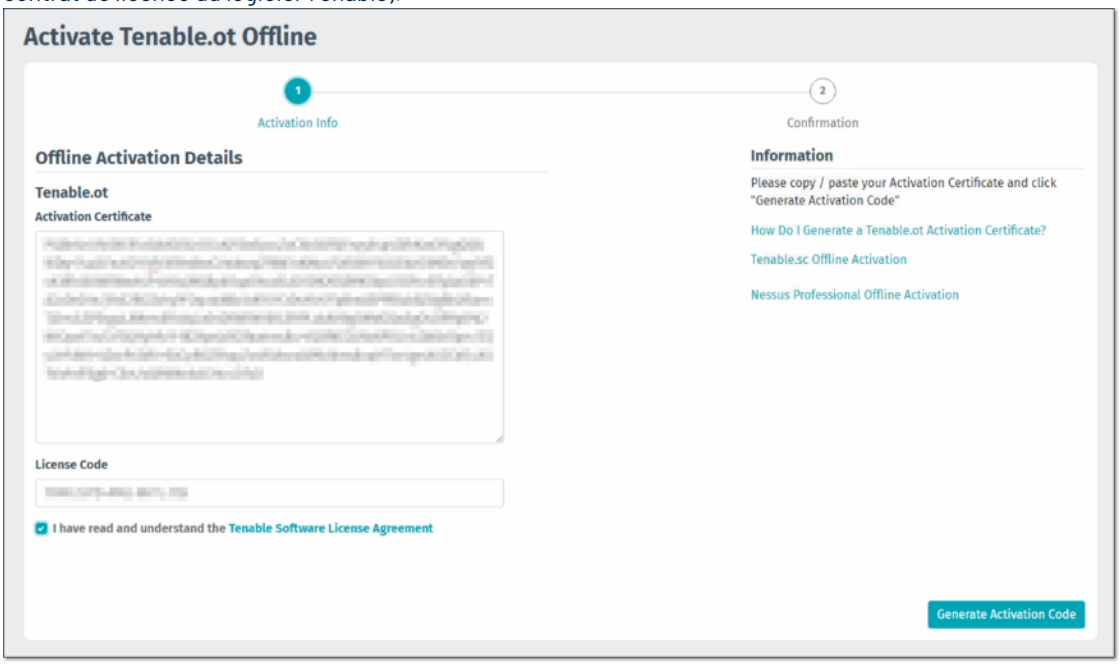

Si votre appareil Tenable.ot n'est pas connecté à Internet, vous devrez accéder à l'écran Activate Tenable.ot Offline à partir d'un appareil connecté à Internet via l'URL suivante : https://provisioning.tenable.com/activate/offline/tenable-ot.

Si vous n'êtes pas connecté à tenable.com actuellement, vous devez vous connecter à l'aide de votre adresse e-mail et de votre mot de passe. Vous devez utiliser le compte de messagerie sur lequel vous avez reçu votre code de licence.

Si vous n'avez pas d'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.

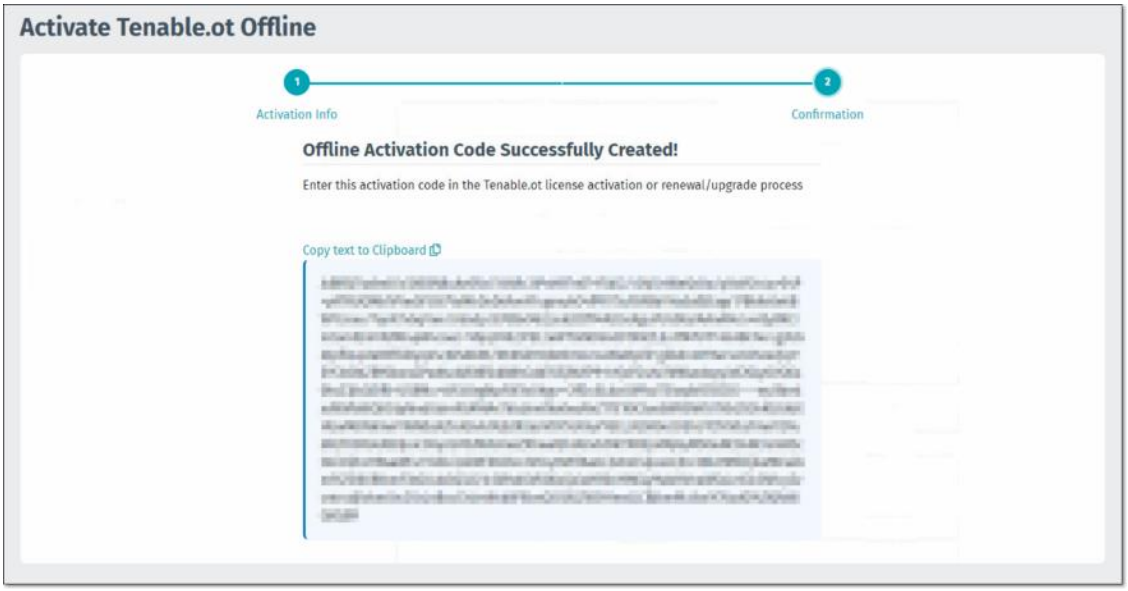
6. Dans le champ Activation Certificate (Certificat d'activation), saisissez le certificat d'activation.
7. Dans le champ **License Code** (Code de licence), saisissez le **code de licence** à 20 caractères que vous avez saisi à l'étape 2 de cette procédure.

8. 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).



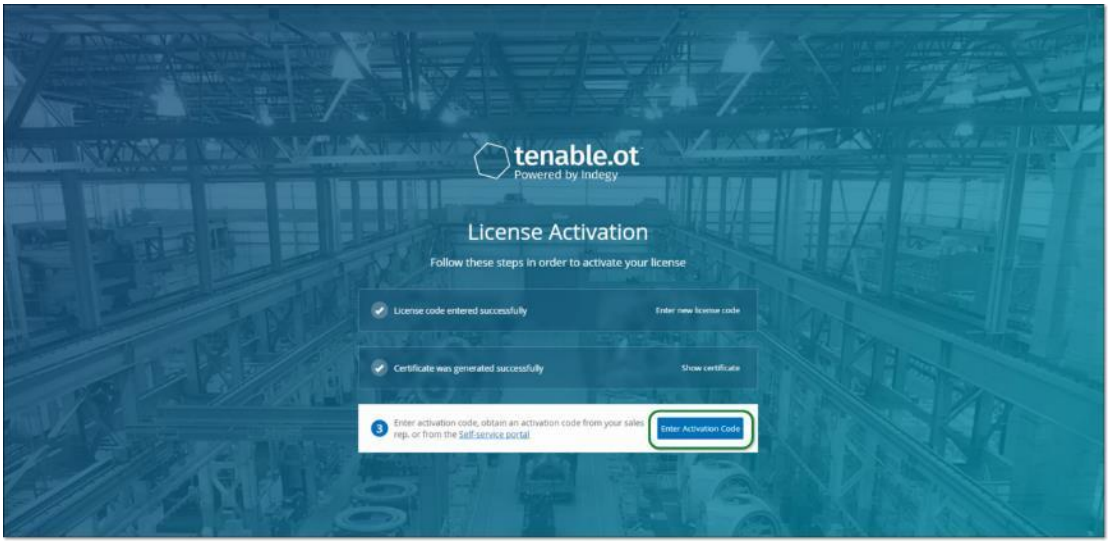

Pour afficher le contrat de licence, cliquez sur le lien **Tenable Software License Agreement** (Contrat de licence du logiciel Tenable).

9. Cliquez sur le bouton **Generate Activation Code** (Générer un code d'activation).
Le message « **Offline Activation Code Successfully Created!** » (Code d'activation hors ligne créé) apparaît à l'écran.



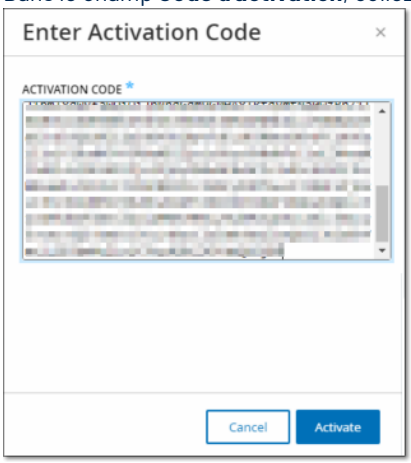

10. Cliquez sur **Copier le texte dans le presse-papiers**.

11. Revenez à l'écran **Activation de licence** sur votre appareil Tenable.ot et cliquez sur le bouton **Saisir le code d'activation**.




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

12. Dans le champ **Code d'activation**, collez votre code d'activation et cliquez sur le bouton **Activer**.




Le panneau latéral se referme et l'écran d'accueil Tenable.ot apparaît. Le bouton Activer apparaît.

Pour plus d'informations sur la mise à jour de votre licence, voir **Mise à jour de la licence**.

# Étape 6 – Activation du système

Une fois l'activation de la licence terminée, le bouton *Activer* apparaît.


Pour activer la fonctionnalité principale du système, vous devez préalablement activer le système.

Une fois le système activé, les fonctionnalités suivantes sont également activées :

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

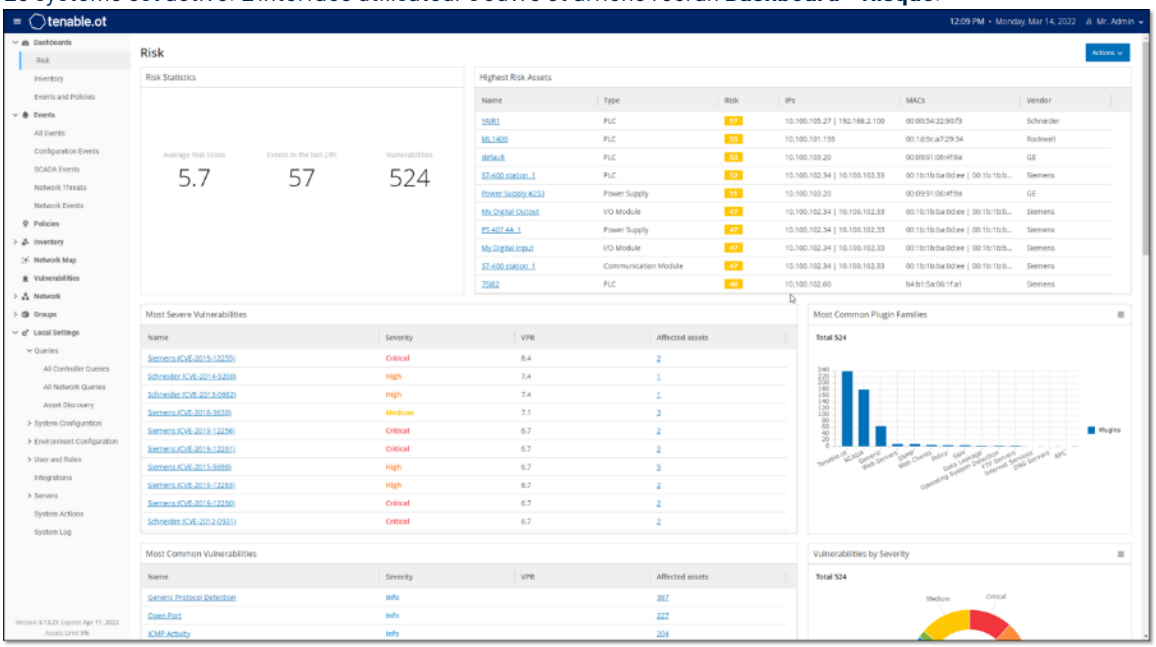
Toutes les données et analyses compilées à partir des fonctionnalités ci-dessus peuvent être visualisées dans la console de gestion (IU).

Ce sont des processus continus qui se poursuivent au fil du temps. Il faudra donc un certain temps pour que les résultats affichés dans l'interface utilisateur soient entièrement à jour.

Des fonctions supplémentaires telles que Requêtes actives peuvent être configurées et activées sur l'écran **Paramètres locaux** de la console de gestion (IU), voir **Requêtes**.

### Pour activer le système :

1. Cliquez sur le bouton **Activer**.
   Le système est activé. L'interface utilisateur s'ouvre et affiche l'écran **Dashboard** > **Risque**.




> Il faudra quelques minutes au système pour identifier vos assets. Vous devrez peut-être actualiser la page pour commencer à afficher les données.

## Étape 7 – Connexion du port de gestion séparé (pour l'option de séparation des ports)

Si vous avez sélectionné l'option de séparation des ports (pour séparer les **requêtes** de la gestion), vous devez connecter le port 3 de l'appliance Tenable.ot, qui est désormais le port de gestion, à l'un des ports d'un commutateur réseau. Il peut s'agir d'un commutateur réseau différent, tel qu'un commutateur réseau du réseau IT.

### Pour connecter le port de gestion :

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

# Installation d'un capteur Tenable.ot

## Appairage des capteurs avec l'ICP

La section suivante décrit la procédure de configuration d'un capteur versions 3.14 et supérieures. Pour configurer un capteur de modèle antérieur, utilisez la procédure décrite dans l'**Annexe 1 – Installation d'un capteur (Versions 3.13 et antérieures).**

L'appairage des capteurs avec l'ICP s'effectue à l'aide de la console de gestion ICP et de l'interface utilisateur Tenable Core du capteur.

Vous pouvez choisir d'autoriser ou non l'approbation automatique des demandes d'appairage entrantes, afin d'exiger ou non une approbation manuelle pour chaque nouvelle demande d'appairage de capteur.

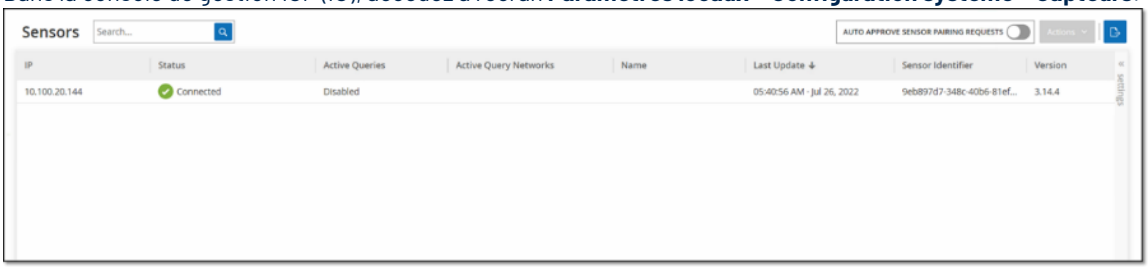
### Conditions préalables

- Le matériel du capteur est correctement installé (voir **Étape 1 - Configuration du capteur**).
- Le capteur est connecté à votre commutateur réseau (voir **Étape 2 – Connexion du capteur au réseau**).
- Le capteur possède sa propre adresse IPv4 statique (voir **Étape 3 – Accès 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 principale. Pour plus d'informations sur l'utilisation de l'interface utilisateur Tenable Core, voir https://docs.tenable.com/tenablecore/Tenableot/Content/TenableCore/Introduction_OT.htm.
- Vérifiez que vous disposez d'un certificat valide dans la console ICP (voir **Certificat**).
- Il est recommandé 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**). Un même nouvel utilisateur administrateur peut être créé pour appairer plusieurs capteurs.

### Appairage du capteur

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

1. Dans la console de gestion ICP (IU), accédez à l'écran **Paramètres locaux** > **Configuration système** > **Capteurs**.



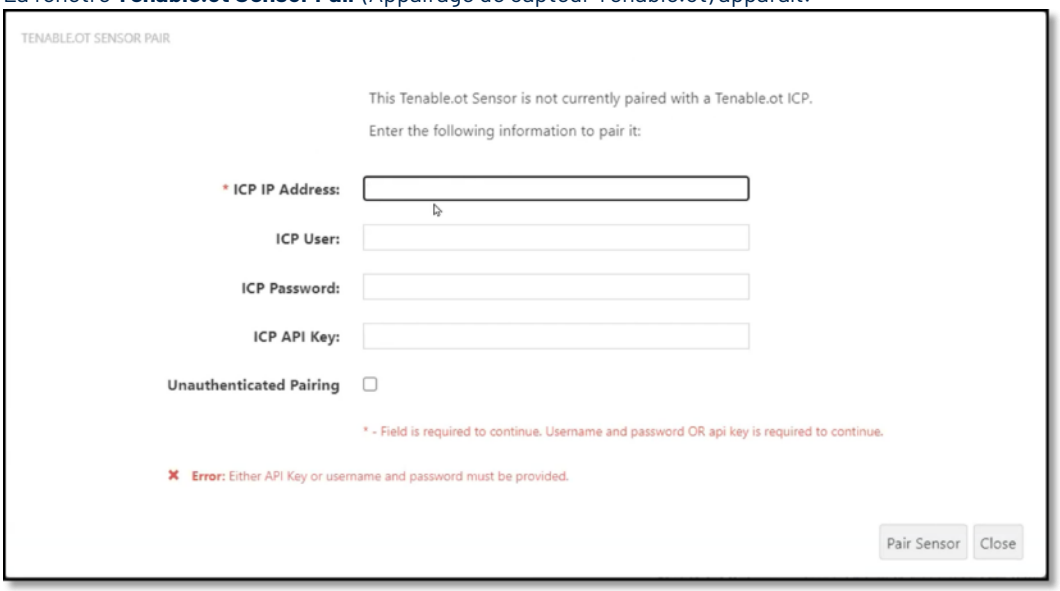

2. Si vous souhaitez autoriser l'approbation automatique de l'appairage de capteurs, assurez-vous d'**activer** l'option **Approuver automatiquement les demandes d'appairage des capteurs**. Si cette option n'est pas sélectionnée, toutes les demandes d'appairage devront être approuvées manuellement.
3. Ouvrez un nouvel onglet, en laissant l'onglet ICP ouvert, et accédez à l'interface utilisateur Tenable Core du capteur en saisissant **<Sensor IP>:8000**.

L'interface utilisateur n'est accessible qu'à partir d'un navigateur Chrome. Vous devez également utiliser 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).


Si la case **Reuse my password for privileged tasks** (Réutiliser mon mot de passe pour les tâches privilégiées) n'est pas cochée lors de la connexion, l'utilisateur ne pourra pas redémarrer le service des capteurs.

5. Dans la barre de menu Navigation, cliquez sur **Tenable.ot Sensor** (Capteur Tenable.ot).
La fenêtre **Tenable.ot Sensor Pair** (Appairage de capteur Tenable.ot) apparaît.




La fenêtre **Tenable.ot Sensor Pair** (Appairage de capteur Tenable.ot) 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 le champ **ICP IP Address** (Adresse IP de l'ICP), saisissez l'adresse IPv4 de l'ICP avec lequel vous souhaitez appairer ce capteur.

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

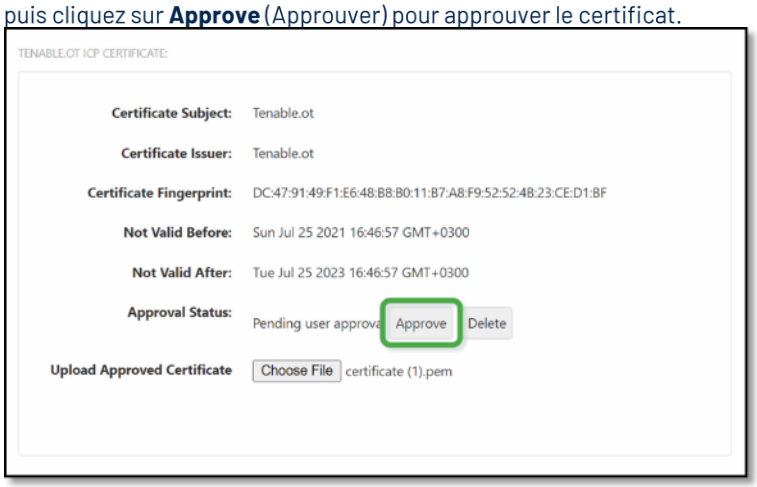
> Les capteurs qui utilisent l'appairage non authentifié ne peuvent que scanner passivement leurs segments de réseau et ne peuvent pas être gérés par l'ICP afin d'envoyer des requêtes actives.

8. Pour authentifier l'appairage, effectuez l'une des opérations suivantes :
   - Saisissez le nom d'utilisateur ICP dans le champ **ICP User** (Utilisateur ICP) et le mot de passe ICP dans le champ **ICP Password** (Mot de passe ICP), OU
   - Saisissez une clé API pour l'ICP dans le champ **ICP API Key** (Clé API ICP).

> Il est recommandé 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**).

> L'avantage de la méthode d'authentification via nom d'utilisateur et mot de passe est que les informations d'identification 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 la console **Tenable Core**, dans la section **Tenable ICP Certificate** (Certificat ICP Tenable), sous **Approval Status** (Statut d'approbation), attendez que les informations du certificat soient chargées, puis cliquez sur **Approve** (Approuver) pour approuver le certificat.

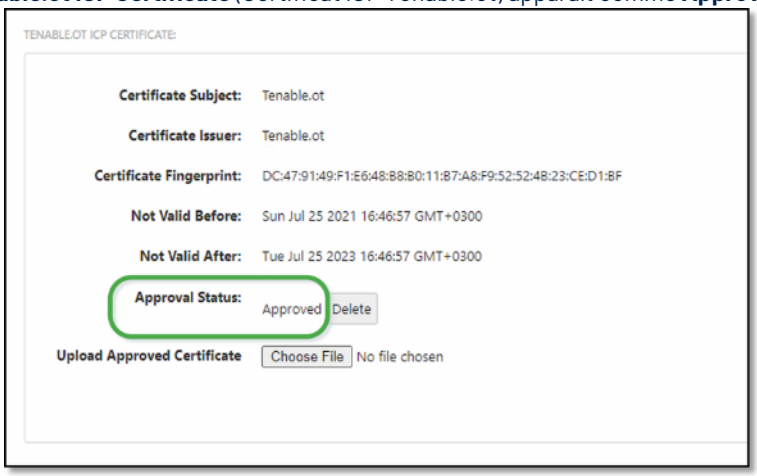



    b. Dans la fenêtre pop-up **Confirm Accept Tenable.ot Server Certificate** (Confirmer l'acceptation du certificat du serveur Tenable.ot), cliquez sur **Accept This Certificate** (Accepter ce certificat).

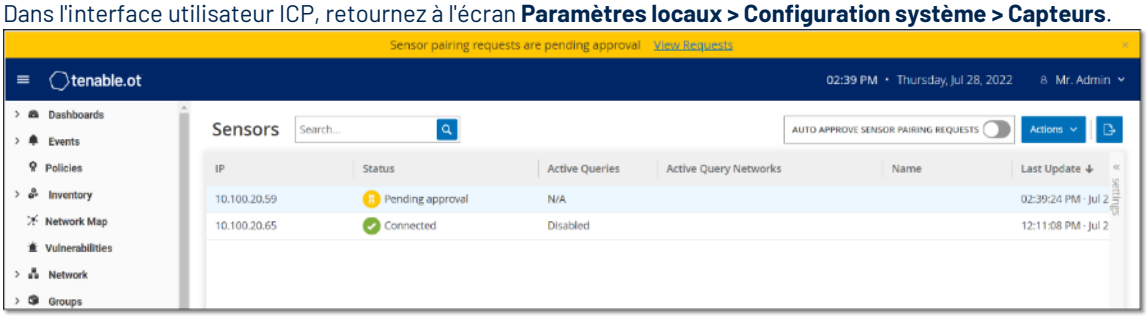
Si vous préférez importer manuellement un certificat :

    a. Dans la console **Tenable ICP**, suivez la procédure décrite dans la section **Génération d'un certificat HTTPS.**
    b. Dans la console **Tenable Core**, dans la section **Tenable ICP Certificate** (Certificat ICP Tenable), sous **Upload Approved Certificate** (Importer 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 accepté, son **statut d'approbation (Approval Status)** dans le tableau **Tenable.ot ICP Certificate** (Certificat ICP Tenable.ot) apparaît comme **Approved** (Approuvé).

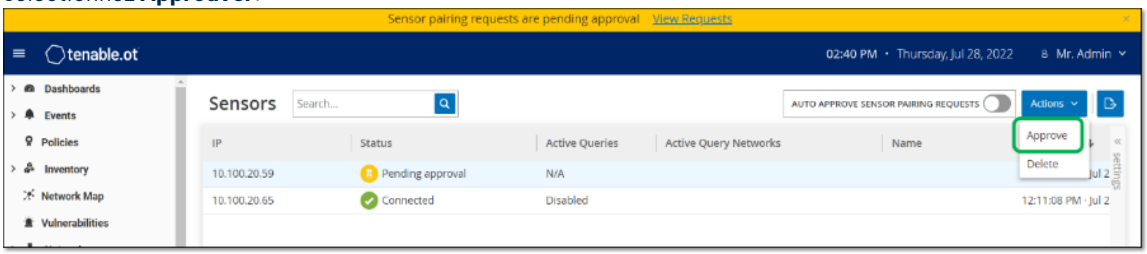



11. Dans l'interface utilisateur ICP, retournez à l'écran **Paramètres locaux > Configuration système > Capteurs**.




Le nouveau capteur est affiché dans le tableau. Le statut doit être *En attente d'approbation*.

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



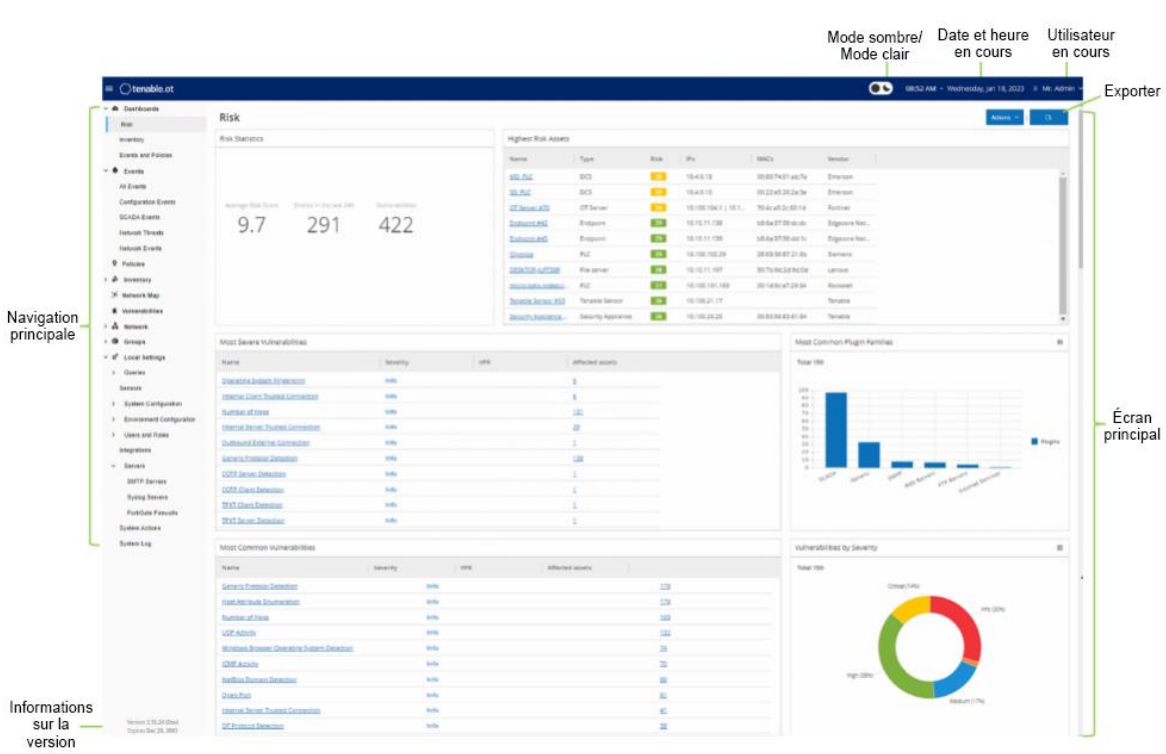

13. L'état doit passer à *Connecté*, indiquant que l'appairage a réussi. Les autres statuts possibles sont :
    - *Connecté (Non authentifié)* – Le capteur est connecté en mode non authentifié. Le capteur ne peut exécuter qu'une détection de réseau passive.
    - *En pause* – Le capteur est correctement 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 (erreur de tunnel ou problème d'API, par exemple).
14. Une fois l'appairage terminé pour un capteur authentifié, vous pouvez configurer les requêtes actives pour qu'elles s'exécutent sur ce capteur. Voir **Configuration des requêtes actives**.

Une fois l'appairage terminé, il est recommandé d'utiliser uniquement la page ICP pour gérer le capteur, et non l'interface utilisateur Tenable Core.

# 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 Tenable.ot 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 Tenable.ot en fonction de vos besoins. Ce chapitre donne un bref aperçu des éléments de l'interface utilisateur. Des détails sur les fonctionnalités spécifiques de l'interface utilisateur sont fournis dans les chapitres suivants.

## Principaux éléments de l'interface utilisateur




Le tableau suivant décrit les principaux éléments de l'interface utilisateur qui sont toujours affichés.

| Élément de l'IU | Description |
|---|---|
| **Navigation principale** | Menu de navigation principal. Cliquez sur l'icône pour afficher/masquer le menu de navigation. |
| **Date et heure en cours** | Affiche la date et l'heure actuelles enregistrées dans le système. |
| **Nom d'utilisateur en cours** | Affiche le nom de l'utilisateur actuellement connecté au système. Cliquez sur la flèche du bas pour afficher un menu de sélection. Les options de menu sont À propos ou Déconnexion. |
| **Informations sur la licence** | Affiche la version du logiciel Tenable.ot et la date d'expiration de la licence. |

| Élément de l'IU | Description |
|---|---|
| **Écran principal** | Affiche l'écran qui a été sélectionné dans la navigation principale. |
| **Mode sombre/Mode clair** | Permet de basculer la palette de couleurs en mode sombre ou en mode clair. |
| **Exporter** | Télécharge un PDF du dashboard. |

### Activer/désactiver le mode sombre

L'utilisateur peut utiliser la palette de couleurs du mode sombre sur tous les écrans en activant le mode sombre.

#### Pour activer/désactiver le mode sombre :

1. Cliquez sur le bouton **Mode sombre**  en haut de l'écran.

   Le réglage est appliqué à tous les écrans et le bouton **Mode clair**  apparaît.
2. Pour restaurer le paramètre Mode clair, cliquez sur le bouton **Mode clair**.

### Vérification de la version actuelle du logiciel

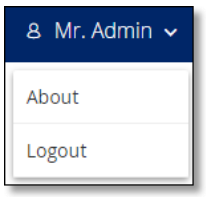
L'utilisateur peut vérifier la version de son logiciel en utilisant le bouton de nom d'utilisateur dans le coin supérieur droit de la barre d'en-tête.

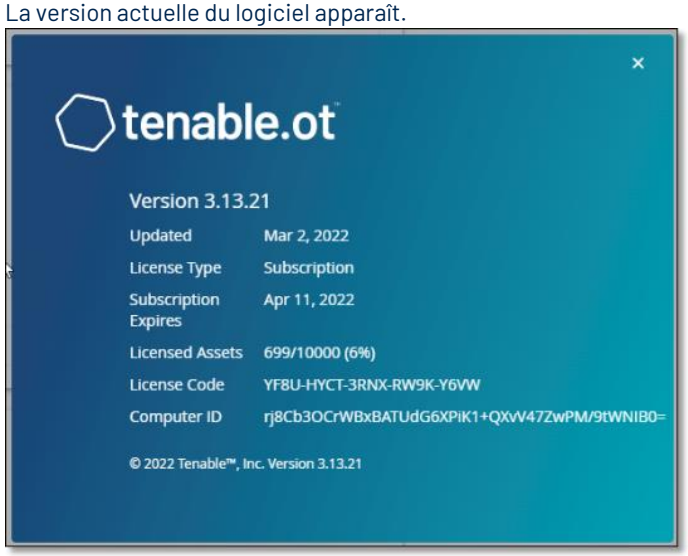
#### Pour afficher la version actuelle du logiciel :

1. Dans la barre d'en-tête principale, cliquez sur le bouton du nom d'utilisateur dans le coin supérieur droit pour ouvrir le menu.

   Le menu utilisateur apparaît.

   
   
2. Dans le menu, cliquez sur **À propos**.
   La version actuelle du logiciel apparaît.

# Écrans principaux

L'interface utilisateur comporte plusieurs écrans principaux accessibles à partir de la **Navigation principale**. Voici une brève description des différents écrans. Chacun d'entre eux sera expliqué plus en détail dans les chapitres suivants.

- **Dashboards** – Affichez des widgets contenant des graphiques et des tableaux qui donnent une vue d'ensemble de l'inventaire et de la sécurité de votre réseau. Il existe trois dashboards distincts pour les *risques*, l'*inventaire* ainsi que les *événements et politiques*. Voir le chapitre **Dashboards**.
- **Événements** – Affiche tous les événements qui se sont produits à la suite d'événements de correspondance avec une politique dans le système. Un écran permet d'afficher *tous les événements*. Des écrans séparés affichent les événements de chaque type spécifique (événements de configuration, événements SCADA, événements de menaces réseau ou événements réseau). Voir le chapitre **Événements**.
- **Politiques** – Affichez, modifiez et activez les politiques dans le système. Voir le chapitre **Politiques**.
- **Inventaire** – Affiche un inventaire de tous les assets découverts, permettant une gestion complète des assets, la surveillance de l'état de chaque asset et la visualisation de leurs événements associés. Un écran permet d'afficher *tous* les assets. Des écrans séparés affichent les assets de types spécifiques (*contrôleurs et modules*, *assets réseau* et *IoT*). Voir le chapitre **Inventaire**.
- **Cartographie du réseau** – Affiche une représentation visuelle des assets du réseau et de leurs connexions.
- **Vulnérabilités** – Affiche une liste détaillée de toutes les menaces du réseau détectées par les plug-ins Tenable.ot et fournit les étapes de remédiation recommandées. Cette section comprend les CVE ainsi que les autres menaces pesant sur les assets de votre réseau (par exemple, systèmes d'exploitation obsolètes, utilisation de protocoles vulnérables, ports ouverts vulnérables, etc.).
- **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 le chapitre **Réseau**.
  Les informations sont affichées sur trois écrans distincts :
  - **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 communications détectées sur le réseau, avec des détails sur la date/heure à laquelle elles se sont produites, les ressources impliquées, etc.
- **Groupes** – Affichez, créez et modifiez les groupes utilisés dans Configuration de la politique. Voir le chapitre **Groupes**.
- **Paramètres locaux** – Affichez et configurez les paramètres système. Voir le chapitre **Paramètres locaux**.

# Utilisation des listes

Les différents écrans Tenable.ot affichent des données pertinentes sous forme de tableau avec une liste pour chaque élément. Ces tableaux ont des fonctionnalités de personnalisation standardisées, permettant à l'utilisateur d'accéder facilement aux informations pertinentes. Les sections suivantes décrivent les fonctions de personnalisation.

Des exemples sont présentés pour les écrans Tous les événements et Tous les assets, mais une fonctionnalité similaire est disponible pour la plupart des écrans de l'interface utilisateur.

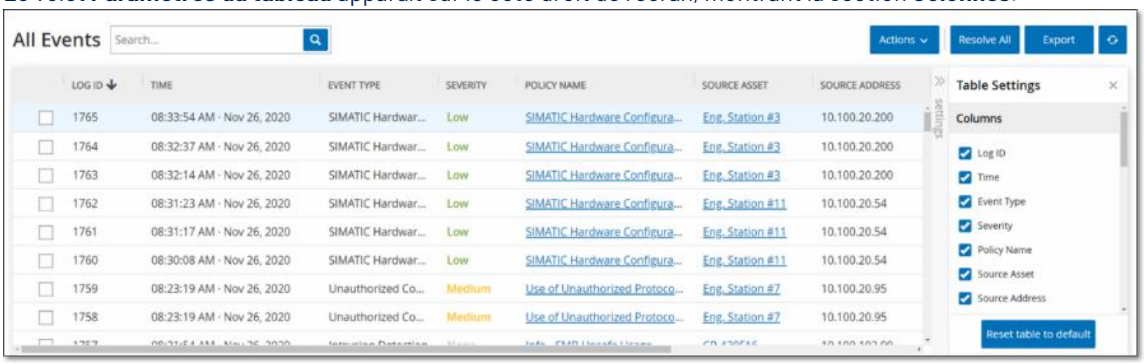
Vous pouvez rétablir les paramètres d'affichage par défaut à tout moment en cliquant sur **Paramètres** > **Réinitialiser le tableau aux valeurs par défaut**.

## Personnalisation de l'affichage des colonnes

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

### Pour sélectionner les colonnes à afficher :

1. Cliquez sur l'onglet **Paramètres** le long du bord droit du tableau.
   Le volet **Paramètres du tableau** apparaît sur le côté droit de l'écran, montrant la section **Colonnes**.




2. Dans la section **Colonnes**, cochez la case à côté de chaque colonne que vous souhaitez afficher.
3. Décochez la case devant chaque colonne que vous souhaitez masquer.
   Seules les colonnes sélectionnées sont affichées.
4. Cliquez sur le signe « **x** » (ou sur l'onglet **Paramètres**) pour refermer la fenêtre *Paramètres du tableau*.

### Pour ajuster l'ordre d'affichage des colonnes :

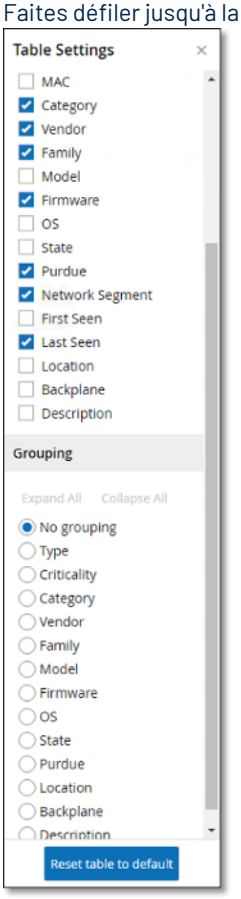
1. Cliquez sur une colonne et faites-la glisser vers la position souhaitée.

### Regroupements

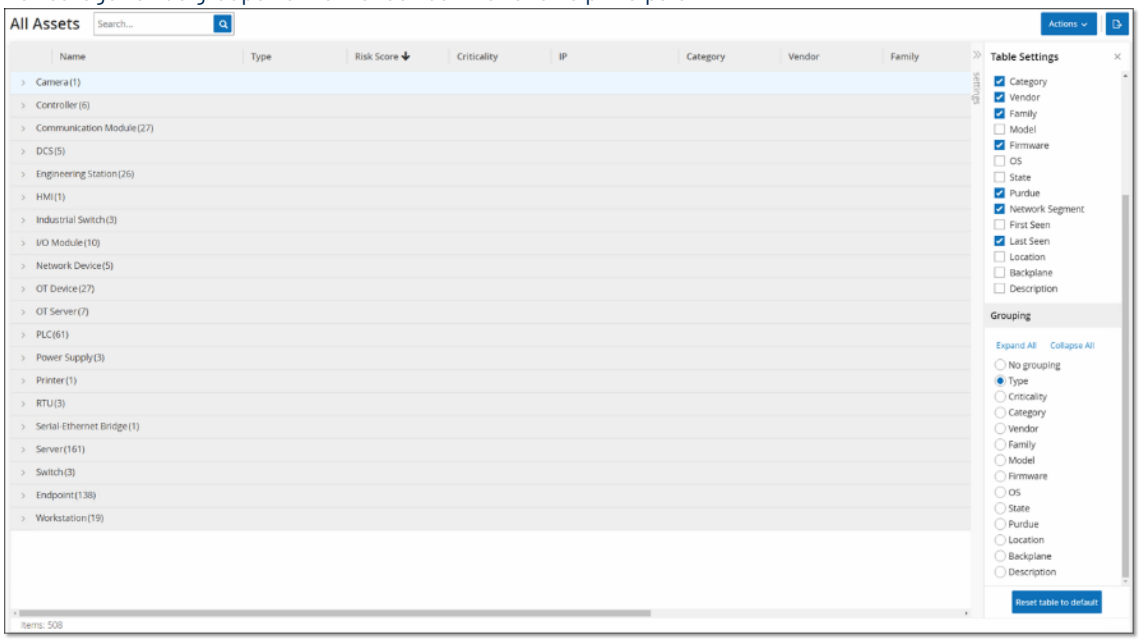
Pour chacun des écrans d'inventaire, vous pouvez regrouper les listes selon divers paramètres pertinents pour cet écran particulier.

### Pour regrouper les listes :

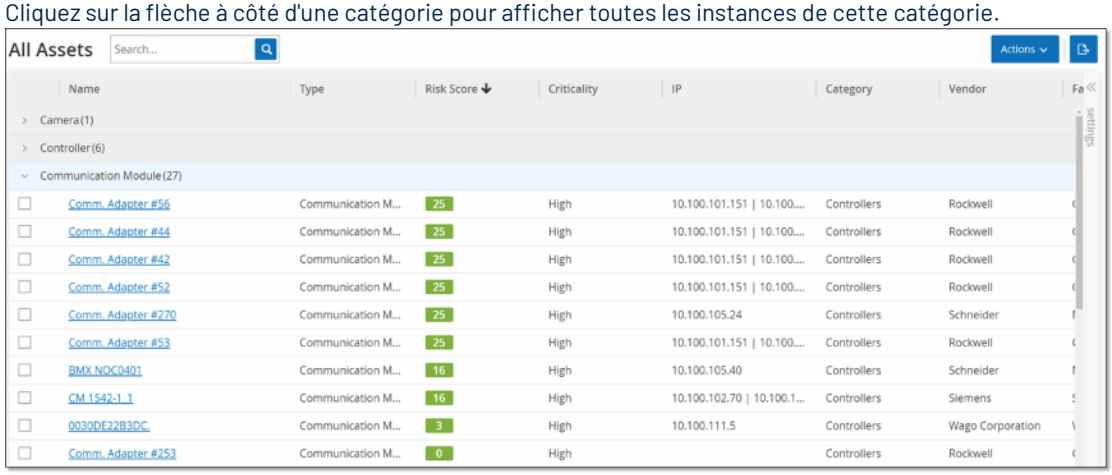
1. Cliquez sur l'onglet **Paramètres** le long du bord droit du tableau.
   Le volet **Paramètres du tableau** apparaît sur le côté droit de l'écran, affichant les sections **Colonnes** et **Regroupements**.
2. Faites défiler jusqu'à la section **Regroupements**.



3. Sélectionnez le bouton radio à côté du paramètre selon lequel vous souhaitez regrouper les listes (par exemple Type).
   Les catégories de groupe sont affichées dans la fenêtre principale.




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.




## Tri

### Pour trier les listes :

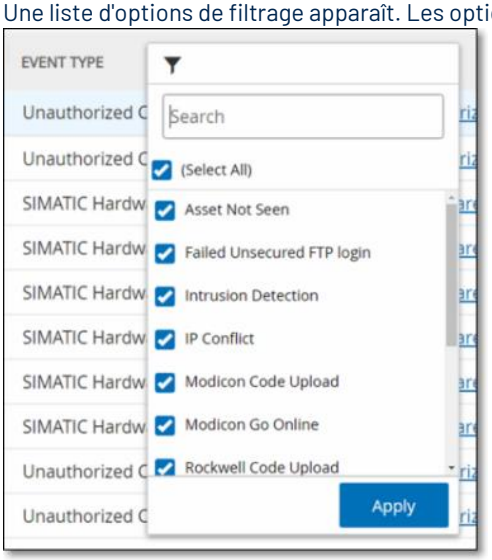
1. Cliquez sur un en-tête de colonne pour trier les assets selon ce paramètre (par exemple, cliquez sur l'en-tête **Nom** pour afficher les assets par ordre alphabétique de nom).
2. Cliquez une deuxième fois sur l'en-tête de la colonne pour inverser l'ordre d'affichage (passer de A→Z à Z→A).

## Filtres

Vous pouvez définir des filtres pour un ou plusieurs en-têtes de colonne. Les filtres peuvent être cumulés afin que seules les listes qui répondent à tous les critères soient affichées. Les options de filtrage sont spécifiques à chaque en-tête de colonne. Chaque écran propose une sélection de filtres pertinents. Par exemple, sur l'écran de l'inventaire des contrôleurs, vous pouvez filtrer par *nom*, *adresses*, *type*, *fond de panier*, *fournisseur*, etc.

### Pour filtrer les listes :

1. Survolez avec la souris un en-tête de colonne pour afficher l'icône de filtre .
2. Cliquez sur l'icône de filtre .
   Une liste d'options de filtrage apparaît. Les options sont spécifiques à chaque paramètre.




3. Sélectionnez les éléments que vous souhaitez afficher et désélectionnez ceux que vous souhaitez masquer.

> Vous pouvez commencer par décocher la case **Tout sélectionner**, puis sélectionner ce que vous souhaitez afficher.

4. Vous pouvez rechercher dans la liste les filtres que vous souhaitez sélectionner ou non.
5. Cliquez sur **Appliquer**.
   Les listes sont ainsi filtrées selon vos critères.
6. L'icône 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 l'icône de filtre .
2. Cliquez sur la case *Tout sélectionner* pour effacer toutes les sélections.
3. Cliquez **à nouveau** sur la case *Tout sélectionner* pour sélectionner tous les éléments.
4. Cliquez sur **Appliquer**.

## Recherche

Sur chaque écran, vous pouvez rechercher des enregistrements spécifiques.

### Pour rechercher dans les listes :

1. Saisissez votre recherche dans la barre dédiée.
2. Cliquez sur l'icône .
3. Pour effacer le texte de la recherche, cliquez sur le signe « **x** ».

# Exportation des données

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

> 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 :**

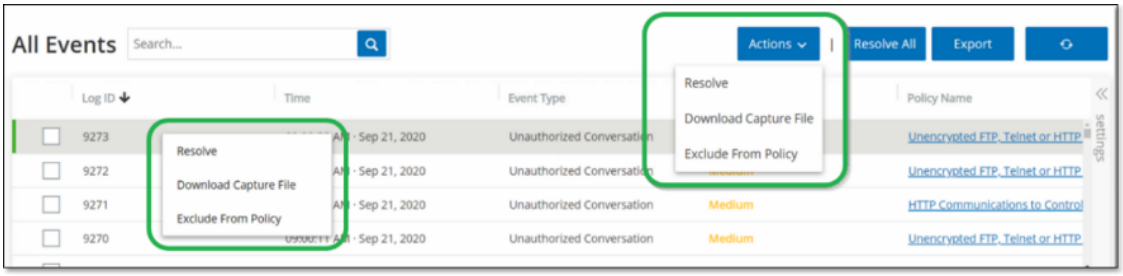
1. Accédez à l'écran dont vous souhaitez exporter les données.
2. Dans la barre d'en-tête, cliquez sur **Exporter**.

# Menus Actions

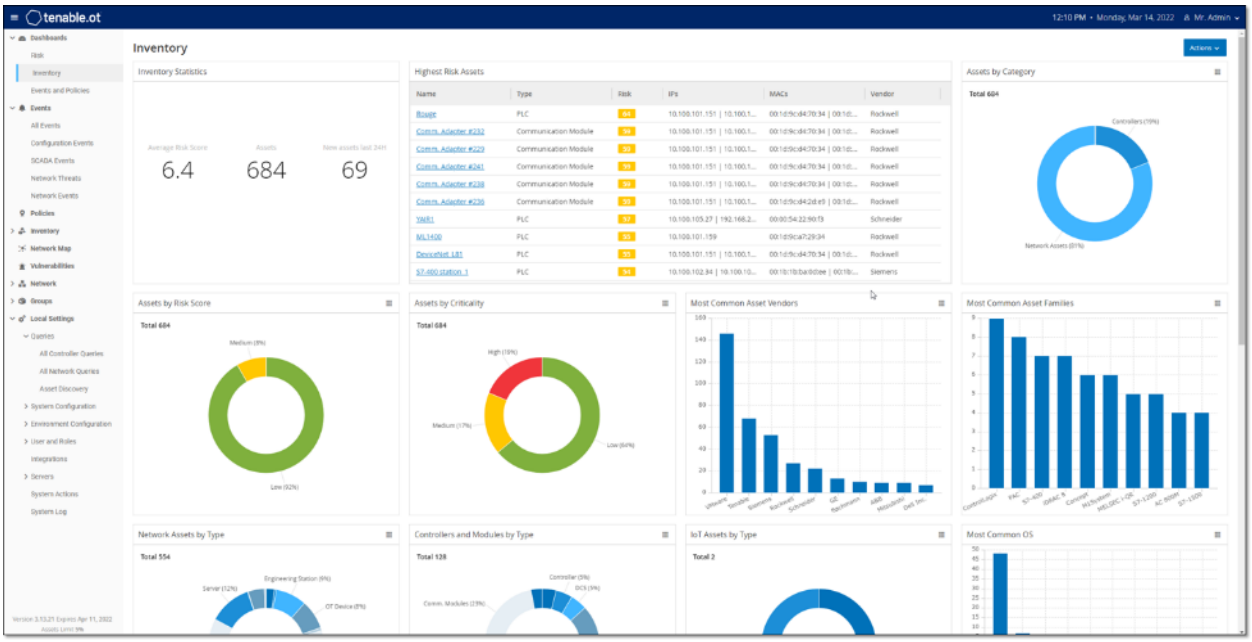
Chaque écran dispose d'un ensemble d'actions spécifiques aux éléments qui y sont affichés. Par exemple, sur l'écran Politiques, vous pouvez *afficher*, *modifier*, *dupliquer* ou *supprimer* une politique. Sur l'écran Événements, vous pouvez *résoudre* ou *télécharger le fichier de capture* pour un événement,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

Il existe deux manières d'accéder au menu Actions :

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



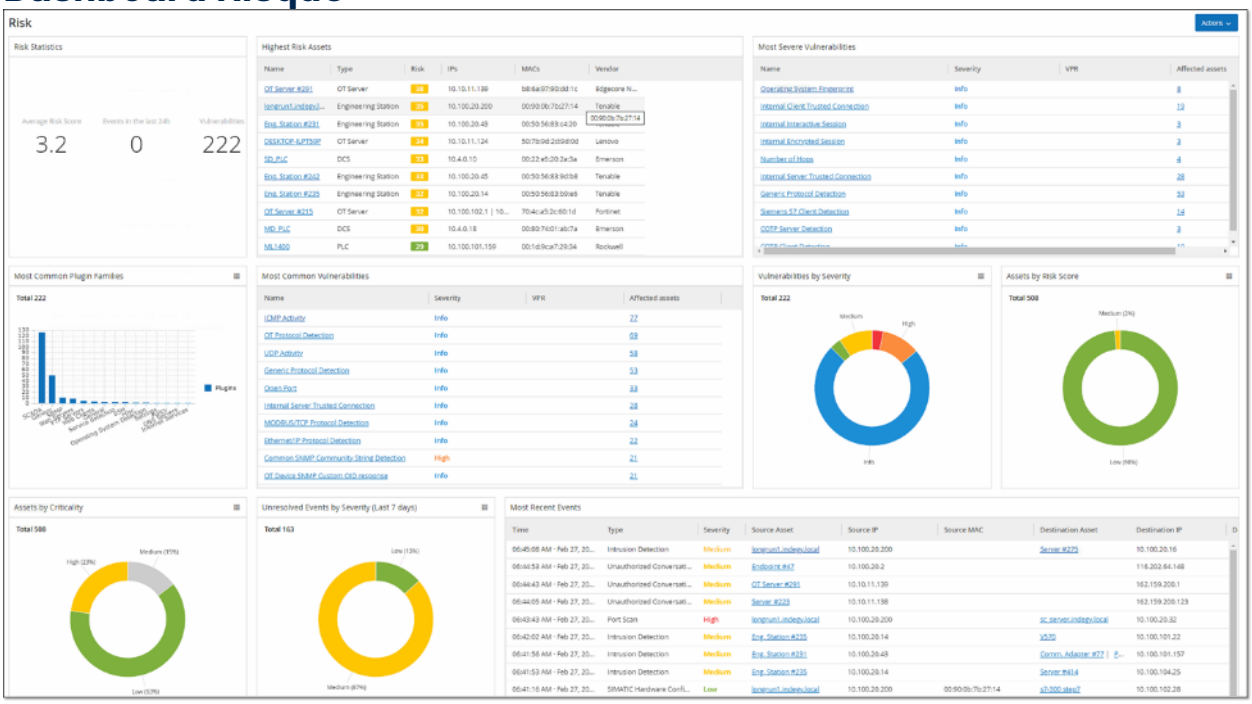
# Dashboards




Il existe trois dashboards distincts pour les *risques*, l'*inventaire* ainsi que les *événements et politiques*. Ces trois dashboards contiennent des widgets qui donnent une vue d'ensemble de l'inventaire et de la sécurité de votre réseau. Vous pouvez choisir un dashboard depuis la navigation principale. Vous pouvez également en sélectionner un dans le menu qui apparaît en cliquant sur le bouton **Dashboards** dans le coin supérieur droit. Le dashboard *Risque* est la vue par défaut initiale. Cependant, vous pouvez assigner un autre dashboard à la vue par défaut.

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

# Dashboard Risque

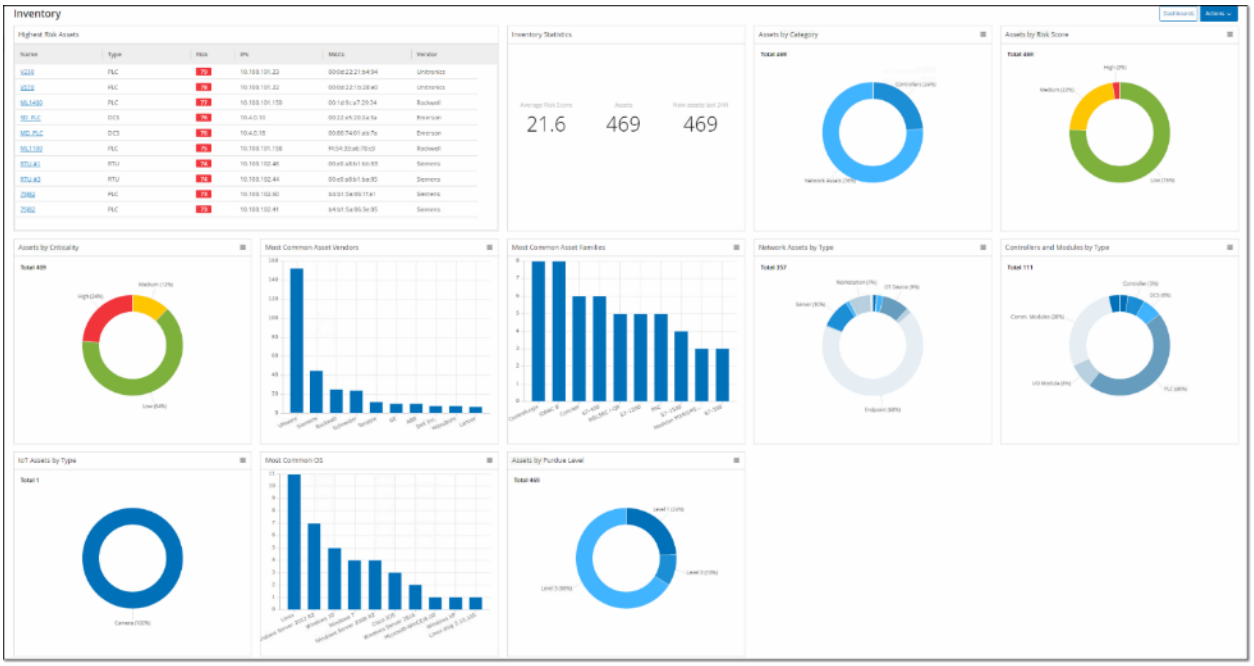



Le dashboard **Risque** fournit des informations sur la cyber-exposition du réseau en se basant sur deux métriques : le score de risque des assets et la gestion des vulnérabilités.

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

En cliquant sur le lien d'un asset ou d'une vulnérabilité, vous accédez à l'élément correspondant sur l'écran d'inventaire ou l'écran des vulnérabilités.

# Dashboard Inventaire

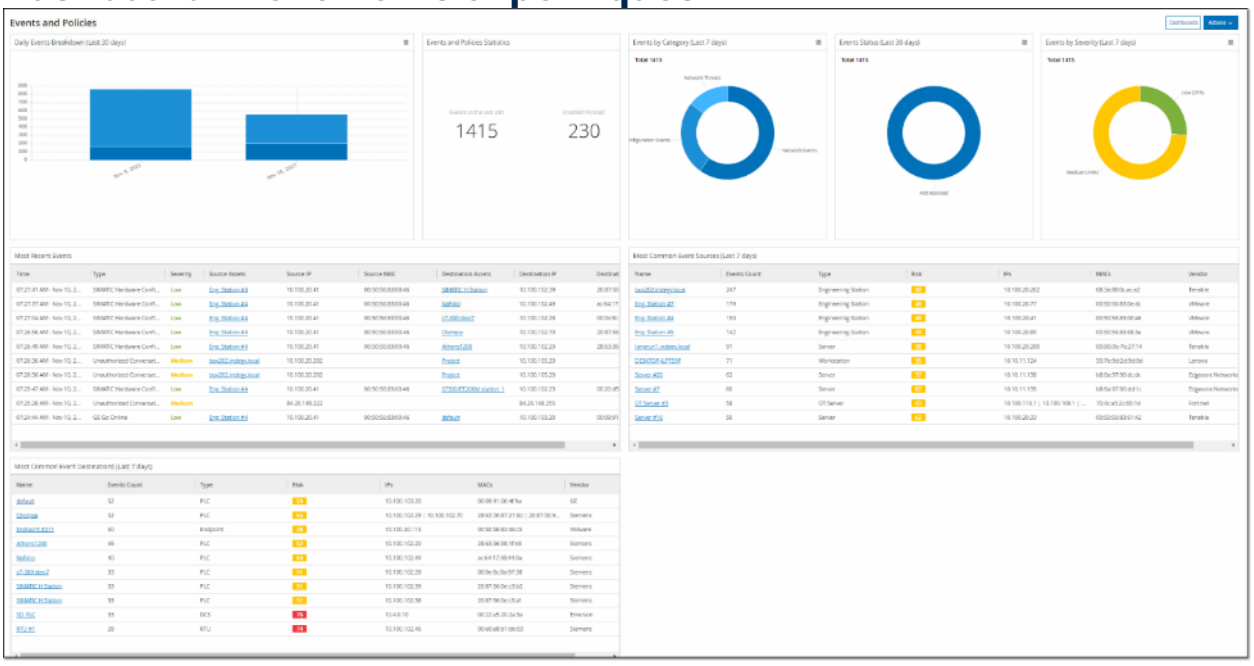



Le dashboard **Inventaire** offre une visibilité sur l'inventaire des assets, facilitant ainsi leur gestion et leur suivi.

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

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

# Dashboard Événements et politiques



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

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

En cliquant sur le lien d'un asset ou d'un événement, vous accédez à l'élément correspondant sur l'écran d'inventaire ou des événements.

# Interagir avec les dashboards

Vous pouvez modifier l'affichage d'un dashboard en interagissant avec les widgets. Vous pouvez afficher les données des dashboards sous forme de graphique ou de tableau. Certains widgets ont un mode d'affichage fixe, d'autres peuvent être affichés sous différentes formes. Les widgets affichant un symbole dans le coin supérieur droit peuvent être visualisés en mode graphique ou en mode tableau. Cliquez sur le symbole tableau/graphique pour passer d'un mode à l'autre.

Les filtres ne peuvent être définis qu'en mode tableau. Une fois qu'un filtre est défini, il est également appliqué en mode graphique.

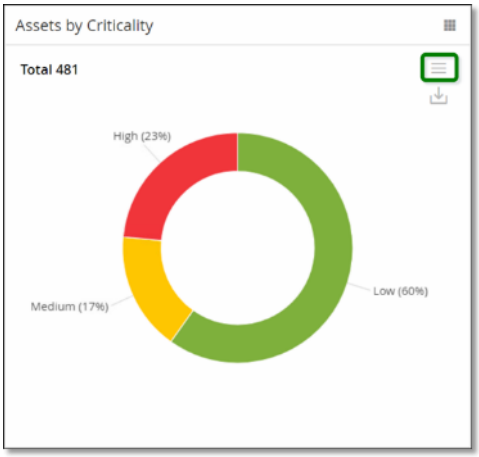
## Mode graphique

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

Vous pouvez interagir avec les widgets des manières suivantes :

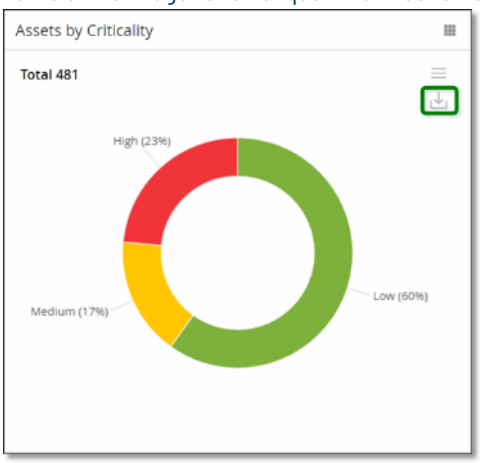
- En survolant un point du graphique avec la souris, vous pouvez afficher une fenêtre contextuelle avec des données spécifiques à ce segment du graphique.


Vous pouvez modifier le type de graphique affiché en cliquant sur le bouton **Paramètres** dans le coin supérieur droit.



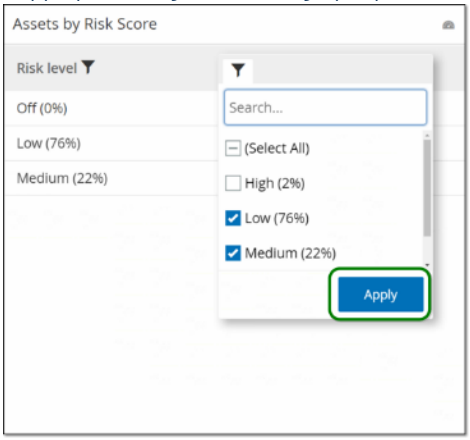

Vous pouvez ensuite sélectionner l'un des autres types de graphiques dans le menu **Paramètres**.

- Lorsque vous affichez un widget en mode graphique, vous pouvez télécharger une image du graphique en survolant le widget et en cliquant sur l'icône **Télécharger**.




## Mode tableau


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

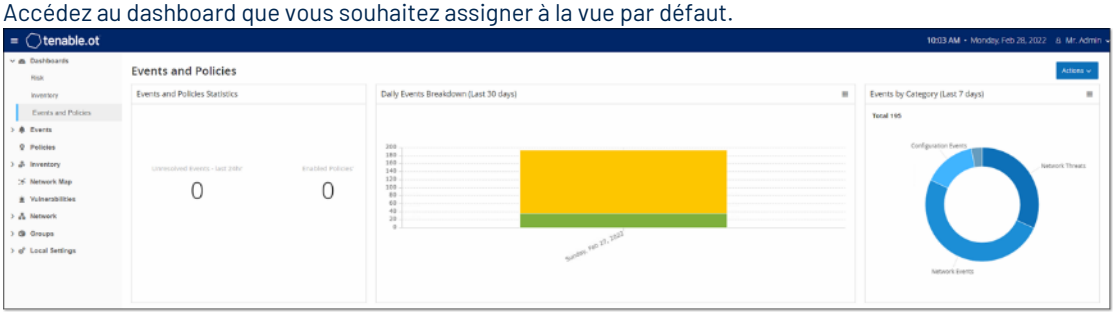


## Modification du dashboard par défaut

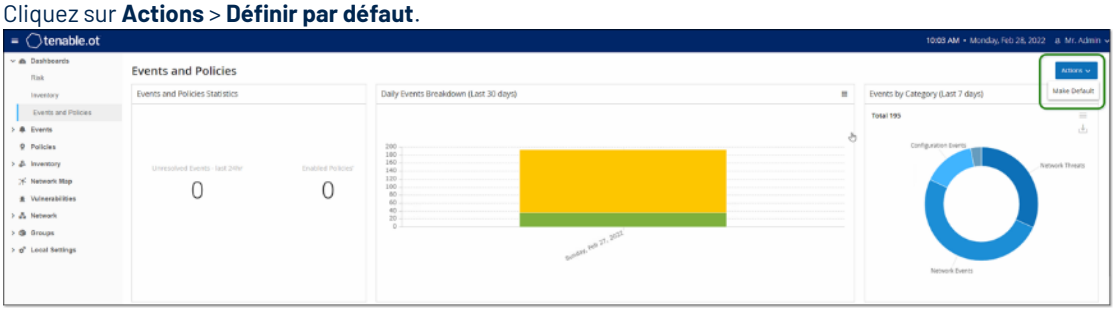
Le dashboard Risque est la vue par défaut initiale de la console de gestion. Vous pouvez assigner un autre dashboard à la vue par défaut.

### Pour modifier le dashboard affiché par défaut :

1. Accédez au dashboard que vous souhaitez assigner à la vue par défaut.




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



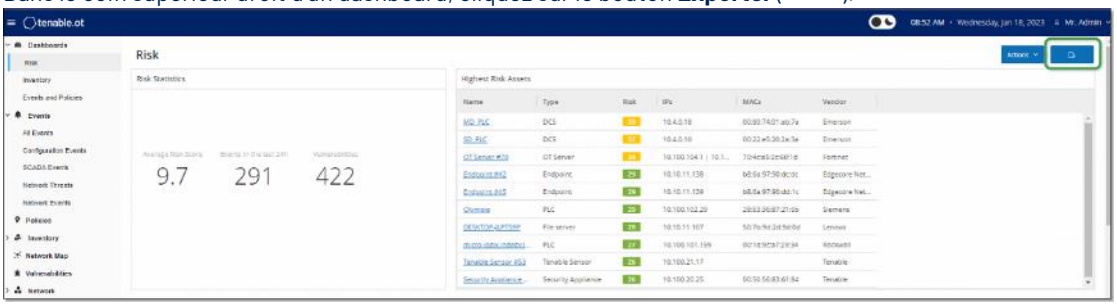

Le dashboard par défaut est mis à jour. La prochaine fois que vous accéderez à la console de gestion, ce dashboard apparaîtra.

## Exportation de dashboard

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

### Pour exporter le dashboard :

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




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

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

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

# Politiques

Les politiques sont utilisées pour définir 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 d'une *Définition de politique* pour une politique donnée, un événement est généré dans le système. L'événement est consigné dans le système et des notifications sont envoyées conformément aux *Actions de politique* configurées pour la politique.

Il existe deux types d'événements liés aux politiques :

- **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 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.

Par défaut, *la plupart* des politiques sont activées. Pour activer/désactiver des politiques, voir **Activer et desactiver les 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 sera 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 aspect essentiel de la définition des politiques de Tenable.ot. 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. 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 de travail), 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*.

Les types de groupes suivants sont utilisés dans le cadre de la configuration des politiques :

- **Groupes d'assets** – Le système est livré avec des groupes d'assets prédéfinis basés sur le type d'asset. Vous pouvez ajouter des groupes personnalisés en fonction d'autres facteurs tels que l'emplacement, le service, la criticité, etc.
- **Segments réseau** – Le système génère automatiquement des segments réseau en fonction du type d'asset et de la plage d'adresses IP. Vous pouvez créer des segments réseau personnalisés pour définir tous les groupes d'assets dont les modèles de communication doivent être similaires.
- **Groupes de messagerie** – Vous pouvez regrouper plusieurs comptes de messagerie qui recevront des notifications par e-mail pour des événements spécifiques. Par exemple, vous pouvez regrouper par rôle, par service, etc.
- **Groupes de ports** – Les ports utilisés de manière similaire peuvent être regroupés. Il pourra s'agir par exemple des ports qui sont généralement ouverts sur les contrôleurs Rockwell.

- **Groupes de protocoles** – Les protocoles de communication peuvent être regroupés par type de protocole (par exemple, Modbus), par fabricant (par exemple, Protocoles autorisés par Rockwell), etc.
- **Groupes de planification** – Plusieurs plages temporelles peuvent être regroupées en un groupe de planification autour d'une caractéristique commune. Il pourra s'agir par exemple des heures de travail, du weekend, etc.
- **Groupes de tags** – Vous pouvez regrouper les tags qui ont des données opérationnelles similaires au sein de plusieurs contrôleurs. Il pourra s'agir par exemple des tags qui contrôlent la température du four.
- **Groupes de règles** – Les groupes de règles sont constitués d'un ensemble de règles associées, reconnues par leurs identifiants de signature Suricata (SID). Ces groupes sont utilisés comme conditions de politiques pour définir des politiques de détection d'intrusion.

Les politiques ne peuvent être définies qu'à l'aide de groupes qui ont été configurés dans votre système. Le système est livré avec un ensemble de groupes prédéfinis. Vous pouvez modifier ces groupes et ajouter les vôtres, voir le chapitre **Groupes**.

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. La signification des différents niveaux d'événement est décrite dans le tableau suivant.

| Sévérité | Description |
|---|---|
| **Aucune** | L'événement n'est pas préoccupant. |
| **Faible** | Aucune raison de s'inquiéter dans l'immédiat. À vérifier au moment opportun. |
| **Moyenne** | 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. Tous les événements sont affichés dans les Événements. Chaque événement est également répertorié sous la politique qui l'a déclenché sur l'écran Politiques, ainsi que sous l'asset affecté par l'événement sur l'écran Inventaire. De plus, les politiques peuvent être configurées pour envoyer des notifications d'événement 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 (qui sont configurées pour être utilisées avec Tenable.ot). Pour une explication sur la façon d'interpréter les notifications Syslog, voir le **Tenable.ot Syslog Integration Guide** (Guide d'intégration Syslog de Tenable.ot).
- **Notifications par e-mail** – Les e-mails contiennent des détails sur l'événement qui a généré la notification, ainsi que des suggestions de mesures à prendre pour atténuer la menace.

### Catégories et sous-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 de listes de blocage (ou listes rouges) et de listes d'autorisations (listes vertes) pour les assets, les activités et les calendriers est prise en charge.
- **Politiques d'événement 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 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.

### Types de politiques

Chaque catégorie et sous-catégorie contient différents types de politiques. Le système est livré avec 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 du contrôleur* sont les activités qui se produisent sur le réseau (c'est-à-dire les « commandes » mises en œuvre entre les assets du réseau). Il existe de nombreux types d'événements liés aux activités du contrôleur. Ils sont définis par le type de contrôleur sur lequel l'activité est exécutée, ainsi que l'activité spécifique identifiée (par exemple, l'arrêt du PLC Rockwell, le téléchargement du code SIMATIC, la session en ligne Modicon, etc.).

Les paramètres 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.

> Les conditions de politique relatives aux assets, sources ou cibles affectés 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. (Actuellement pris en charge uniquement pour les contrôleurs Rockwell.) |
| **Change in state (Changement d'état)** | Asset affecté, Planification | Le contrôleur est passé d'un état opérationnel (par exemple, en cours d'exécution, arrêté, test, etc.) à un autre. |
| **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.

Les conditions de politique relatives aux assets, sources ou cibles affectés 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. |
| **Change in USB configuration (Changement dans la configuration USB)** | Asset affecté, 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 au cours de la plage temporelle spécifiée. |

| Type d'événement | Conditions de politique | Description |
|---|---|---|
| **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, suivez les procédures décrites dans la section **Définition d'une base de référence réseau**. La politique s'applique à la communication provenant d'un asset du groupe Asset source vers un asset du groupe Asset cible, à l'aide d'un protocole provenant du groupe Protocole, au cours de la plage temporelle spécifiée. |
| **New asset discovered (Nouvel asset découvert)** | Asset affecté, Planification | Détecte les nouveaux assets du type spécifié dans le groupe Asset *source* qui apparaissent sur votre réseau au cours de la plage temporelle spécifiée. |
| **Open Port (Port ouvert)** | Asset affecté, Port | Détecte les nouveaux ports ouverts sur votre réseau. Les ports ouverts non utilisés peuvent présenter un risque pour la sécurité. La politique s'applique aux assets du groupe Asset affecté, et aux ports du groupe Port. |
| **Spike in network traffic (Pic de trafic réseau)** | Fenêtre temporelle, Niveau de 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) (Connexion RDP (authentifiée))** | Source, Cible, Planification | Une connexion RDP (connexion bureau à distance) a été établie sur le réseau à l'aide des identifiants d'authentification. La politique s'applique à un asset du groupe Asset *source* se connectant à un asset du groupe Asset *cible*, au cours de la plage temporelle spécifiée. |
| **RDP connection (not authenticated) (Connexion RDP (non authentifiée))** | Source, Cible, Planification | Une connexion RDP (connexion bureau à distance) a été établie sur le réseau sans utiliser d'identifiants d'authentification. La politique s'applique à un asset du groupe Asset *source* se connectant à un asset du groupe Asset *cible*, au cours de la plage temporelle spécifiée. |
| **Unauthorized conversation (Communication non autorisée)** | Source, Cible, Protocole, Planification | Détecte les communications envoyées entre assets du réseau. La politique s'applique à la communication provenant d'un asset du groupe Asset *source* vers un asset du groupe Asset *cible*, à l'aide d'un *protocole* provenant du groupe Protocole, au cours de la plage temporelle spécifiée. |

| Type d'événement | Conditions de politique | Description |
|---|---|---|
| **Successful unsecured FTP login (Connexion FTP non sécurisée réussie)** | Source, Cible, Planification | FTP est considéré 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 | FTP est considéré comme un protocole non sécurisé. Cette politique détecte les tentatives de connexion infructueuses à l'aide du protocole FTP. |
| **Successful unsecured Telnet login (Connexion Telnet non sécurisée réussie)** | Source, Cible, Planification | Telnet est considéré comme un protocole non sécurisé. Cette politique détecte les connexions réussies à l'aide du protocole Telnet. |
| **Failed unsecured Telnet login (Échec de la connexion Telnet non sécurisée)** | Source, Cible, Planification | Telnet est considéré 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 | Telnet est considéré comme un protocole non sécurisé. Cette politique détecte les tentatives de connexion à l'aide de Telnet (pour lesquelles le statut du résultat n'a pas été détecté). |

## Types d'événements liés aux menaces réseau

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

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

| Type d'événement | Conditions de politique | Description |
|---|---|---|
| **Intrusion Detection (Détection d'intrusion)** | Source, Asset affecté, Groupe de règles, Planification | Les politiques de détection d'intrusion détectent les menaces OT et IT basées sur les signatures, afin d'identifier le trafic réseau indiquant des menaces d'intrusion. La détection est basée sur des règles cataloguées dans le moteur de détection de menaces Suricata. Les règles sont regroupées en catégories (par exemple, attaques ICS, déni de service, malware, etc.) et sous-catégories (par exemple, attaques ICS – Stuxnet, attaques ICS – Black Energy, etc.). Le système est livré avec un ensemble de groupes prédéfinis de règles associées. Vous pouvez également configurer vos propres regroupements de règles. |

| Type d'événement | Conditions de politique | Description |
|---|---|---|
| **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.

Les conditions de politique relatives aux assets, sources ou cibles affectés 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. |

| Type d'événement | Conditions de politique | Description |
|---|---|---|
| **Unauthorized write (Écriture non autorisée)** | Asset source, Groupe de tags, Valeur du tag, Planification | Détecte les écritures non autorisées pour un ou plusieurs tags spécifiés sur un contrôleur (actuellement pris en charge pour les contrôleurs Rockwell et ST) dans le groupe Asset source spécifié. La politique peut être configurée pour détecter toute nouvelle écriture, un changement par rapport à une valeur spécifiée ou une valeur en dehors d'une plage spécifiée. La politique s'applique uniquement au cours de la plage temporelle spécifiée. |
| **ABB - Unauthorized write (ABB - Écriture non autorisée)** | Asset source, Asset cible, Planification | Détecte les commandes d'écriture envoyées via MMS aux contrôleurs ABB 800xA étant hors de la plage autorisée. |
| **Commandes CEI 60870-5-104 : Start/Stop Data Transfer (démarrage/arrêt du transfert de données), Interrogation Command (commande d'interrogation), Counter Interrogation Command (commande d'interrogation de compteur), Clock Synchronization Command (commande de synchronisation d'horloge), Reset Process Command (commande de processus de réinitialisation), Test Command with Time Tag (commande de test avec marqueur temporel)** | Asset source, Asset cible, Planification | Détecte les commandes spécifiques envoyées aux unités principales ou subordonnées CEI-104 considérées comme risquées. |
| **DNP3 Commands (Commandes DNP3)** | Asset source, Asset cible, Planification | Détecte toutes les commandes principales envoyées à l'aide du protocole DNP3, par exemple Select (Sélection), Operate (Exécution), Warm/Cold Restart (Redémarrage à chaud/à froid), etc. Détecte également les erreurs provenant d'indicateurs internes tels que les codes de fonction non pris en charge et les erreurs de paramètre. |

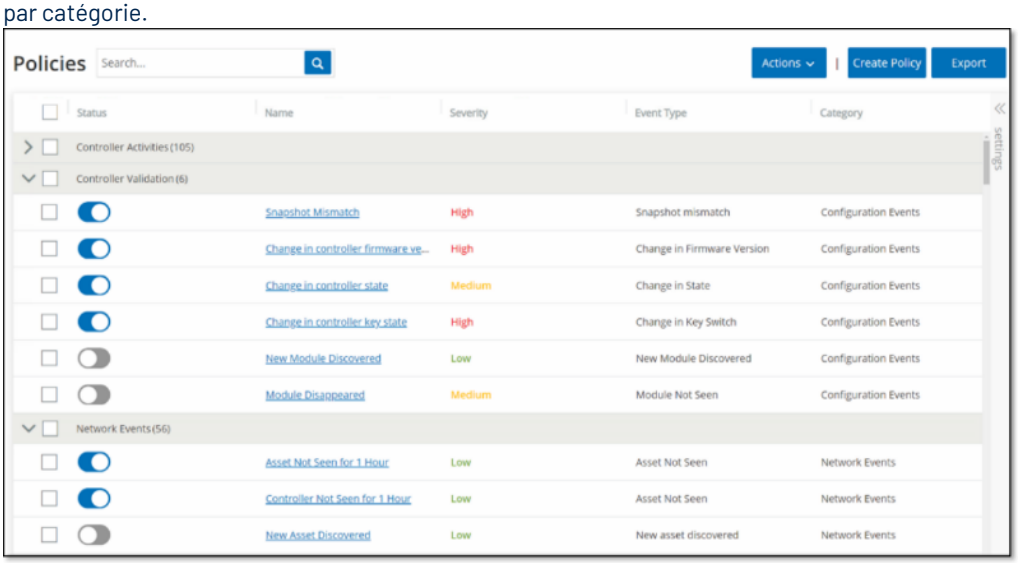
## Activer et désactiver les politiques

Toute politique déjà configurée dans votre système (à la fois pré-configurée et définie par l'utilisateur) peut facilement être activée ou désactivée. Vous pouvez activer et désactiver les politiques individuellement ou en bloc après en avoir sélectionné plusieurs.

De nombreuses 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 fonctionneront pas correctement. Les requêtes peuvent être activées en allant dans **Paramètres locaux** > **Requêtes**, voir **Requêtes**.

### Pour activer/désactiver une politique :

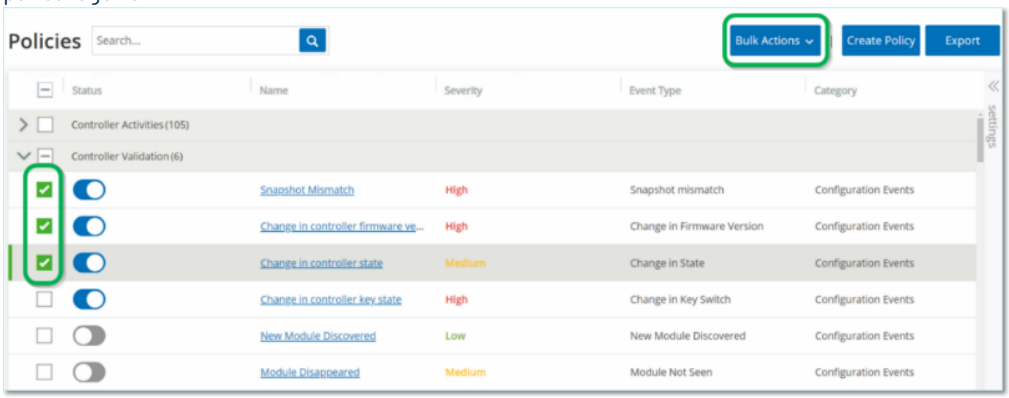
1. Accédez à l'écran **Politiques.**
   Une liste apparaît pour chaque politique configurée dans le système. Les listes de politiques sont regroupées par catégorie.




2. **Activez ou désactivez** le **statut** situé en regard de la politique souhaitée.

### Pour activer/désactiver plusieurs politiques :

1. Accédez à l'écran **Politiques.**
   Une liste apparaît pour chaque politique configurée dans le système. Les listes de politiques sont regroupées par catégorie.




2. Cochez la case à côté de chacune des politiques que vous souhaitez activer/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. Cliquez sur le bouton **Actions en bloc** dans la barre d'en-tête.
4. Sélectionnez l'action souhaitée (**Activer** ou **Désactiver**) dans la liste déroulante.
   Toutes les politiques sélectionnées sont activées/désactivées.

# Affichage des politiques

L'écran **Politiques** affiche la liste de toutes les politiques configurées dans votre système. Les listes sont regroupées par onglets distincts pour chaque catégorie de politique. Les politiques pré-configurées et les politiques définies par l'utilisateur sont répertoriées sur cet écran. Chaque élément de liste s'accompagne d'un curseur montrant le statut actuel de la politique, ainsi que 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 une explication des fonctionnalités de personnalisation, voir **Utilisation des listes**.

Les paramètres de politique sont décrits dans le tableau suivant.

| Paramètre | Description |
|---|---|
| **Statut** | Indique si la politique est activée ou désactivée. Si la politique a été automatiquement désactivée par le système car elle générait trop d'événements, une icône d'avertissement apparaît.<br>Activez ou désactivez la politique à l'aide du curseur. |
| **ID de la politique** | Un identifiant unique pour la politique dans le système. Les ID de politiques sont regroupés par catégorie, avec un préfixe différent pour chaque catégorie (par exemple, P1 pour les activités de contrôleur, P2 pour les événements réseau, etc.). |
| **Nom** | Le nom de la politique. |
| **Sévérité** | Le degré de sévérité de l'événement. Les valeurs possibles sont : Aucune, Faible, Moyenne ou Élevée. Voir la section **Niveaux de sévérité** pour une description des niveaux de sévérité. |
| **Type d'événement** | Le type spécifique d'événement qui déclenche cette politique d'événement. |
| **Catégorie** | La catégorie générale du type d'événement qui déclenche cette politique d'événement. Les valeurs possibles sont : Configuration, SCADA, Menaces réseau ou Événements réseau. Pour une explication des différentes catégories, voir **Catégories et sous-catégories de politiques**. |
| **Source** | Une condition de politique. Le groupe d'assets Source/Segment réseau (c'est-à-dire, l'asset qui a lancé l'activité) auquel la politique s'applique. |
| **Cible/ Assets affectés** | Une condition de politique. Le groupe d'assets cible/segment réseau (l'asset qui reçoit l'activité) auquel la politique s'applique. Pour les politiques impliquant un seul asset (pas de source ni de cible), ce paramètre affiche l'asset qui a été affecté par l'événement. |
| **Planification** | Une condition de politique. La plage temporelle pour laquelle la politique s'applique. |
| **Syslog** | Le serveur Syslog (SIEM) où les événements de cette politique sont enregistrés. |
| **E-mail** | Le groupe de messagerie auquel les notifications d'événement pour cette politique sont envoyées. |

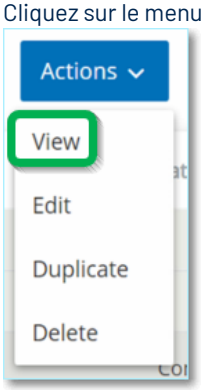
| Paramètre | Description |
|---|---|
| **Sous-catégorie** | La classification de la sous-catégorie de l'événement. La catégorie *Événements de configuration* est composée des sous-catégories *Activités du contrôleur* et *Validation du contrôleur*. Pour une explication des différentes sous-catégories, voir **Catégories et sous-catégories de politiques**. |
| **Nombre d'événements par politique** | Répertorie le nombre d'événements générés par chaque politique. En cliquant sur la colonne, il est possible de trier la liste afin de se concentrer sur les politiques ayant connu le plus de violations/d'événements. |
| **Exclusions** | Répertorie le nombre d'exclusions ajoutées à chaque politique. Pour plus d'informations, voir **Création d'exclusions de politique**. |

## Affichage des détails d'une politique

Vous pouvez ouvrir l'écran Détails de la politique pour afficher des détails supplémentaires sur une politique. Cet écran affiche une liste complète de toutes les conditions de la politique. Il affiche également une liste de tous les événements déclenchés par la politique sélectionnée.

### Pour ouvrir l'écran Détails de la politique pour une politique donnée :

1. Sur l'écran **Politiques**, sélectionnez la politique souhaitée.
2. Cliquez sur le menu **Actions** et sélectionnez **Afficher** dans la liste déroulante.




Vous pouvez également accéder au menu Actions en faisant un clic droit sur la politique pertinente.

L'écran Détails de la politique apparaît pour la politique sélectionnée.


L'écran Détails de la politique contient les éléments suivants :

- **Barre d'en-tête** – Affiche le nom, le type et la catégorie de la politique. Un curseur permet également d'activer/de désactiver la politique, et une liste déroulante propose les actions disponibles (Modifier, Dupliquer et Supprimer).
- **Onglet Détails** – Affiche des détails sur la configuration de la politique dans trois sections :
    - **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. Pour chaque événement, des informations sont affichées à propos du ou des assets impliqués et de la nature de l'événement. Les informations affichées dans cet onglet sont **identiques aux informations affichées sur l'écran Événements**, mais seuls les événements pour la politique spécifiée sont affichés ici. Pour une explication des informations sur les événements, voir **Affichage des événements**. **Onglet Exclusions** – Si vous constatez qu'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). Cela s'effectue sur l'écran Événements. Voir **Création d'exclusions de politique**. L'onglet Exclusions affiche toutes les exclusions appliquées à cette politique. Pour chaque exclusion, le détail des conditions exclues est affiché. À partir de cet onglet, vous pouvez supprimer une exclusion (permettant ainsi au système de reprendre la génération d'événements pour les conditions spécifiées).

# Création de politiques

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

Les politiques sont définies à l'aide de groupes qui ont été 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 **In** (Inclure) pour ajouter le groupe spécifié à la liste d'autorisation (c'est-à-dire l'inclure dans la politique), OU
- sélectionnez **Not In** (Ne pas inclure) pour ajouter le groupe spécifié à la liste de blocage (c'est-à-dire l'exclure de la politique).

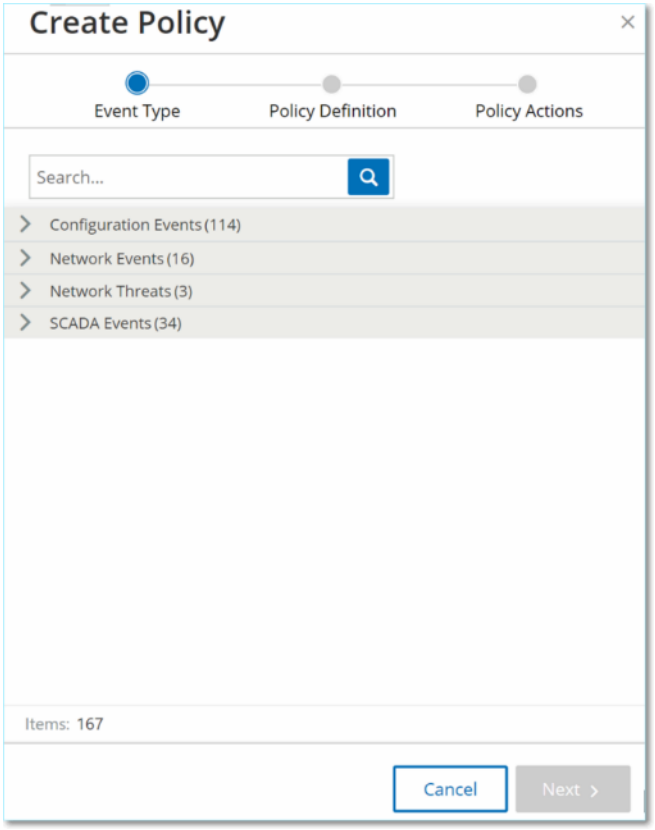
Pour les paramètres des groupe d'assets et Segment réseau (c'est-à-dire les assets *sources, cibles* et *affectés*), vous pouvez utiliser des opérateurs logiques (et/ou) pour appliquer la politique à diverses combinaisons ou sous-ensembles de vos groupes prédéfinis. Par exemple, si vous souhaitez qu'une 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 **Duplication de politiques**.

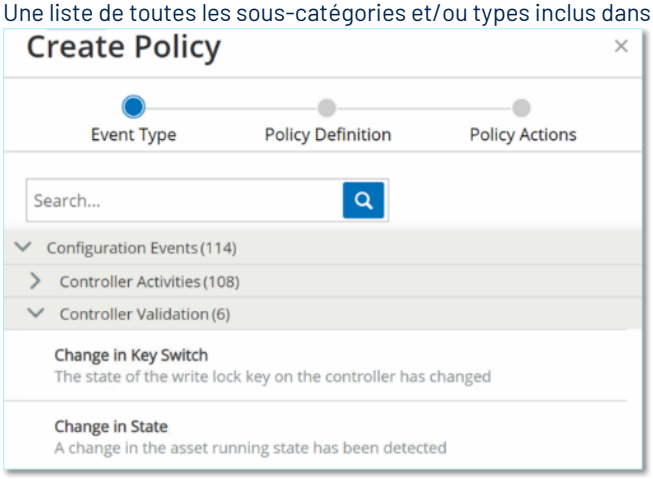
Si, après avoir créé une politique, vous constatez qu'elle génère des événements pour des situations qui ne nécessitent pas d'attention, vous pouvez exclure certaines conditions spécifiques de la politique. Voir **Création d'exclusions de politique**.

### Pour créer une politique :

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

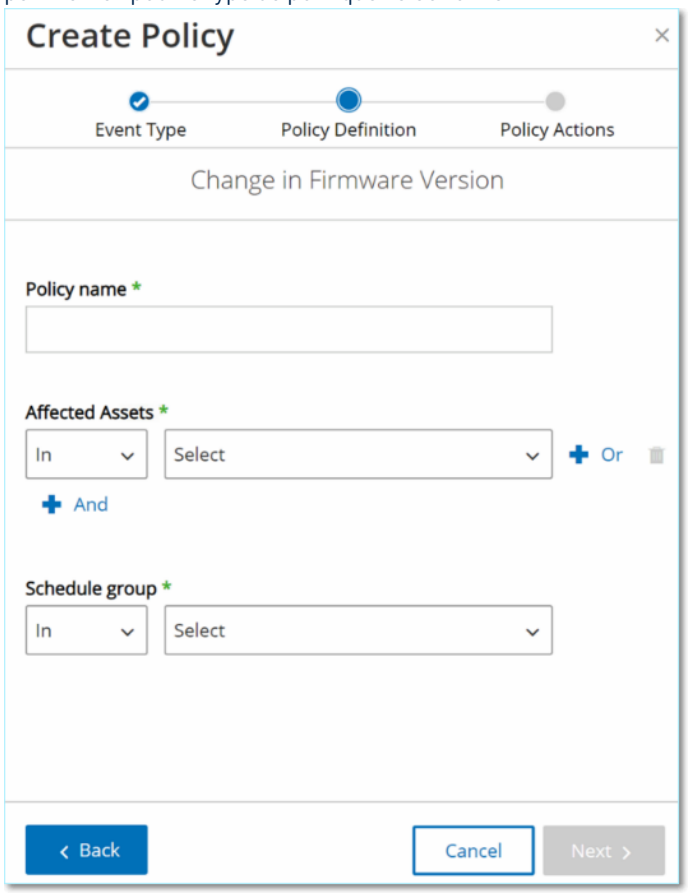



2. Cliquez sur une **catégorie de politique** pour afficher les sous-catégories et/ou les types de politiques.
   Une liste de toutes les sous-catégories et/ou types inclus dans cette catégorie apparaît.




3. Sélectionnez un type de politique.

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

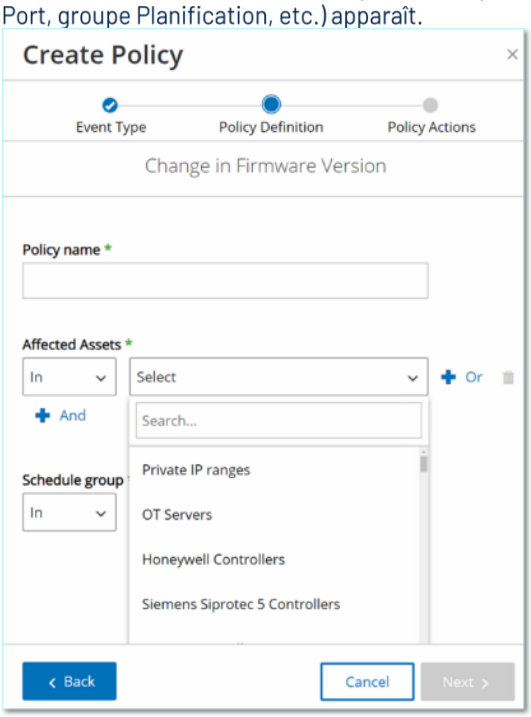



5. Dans le champ **Nom de la politique**, saisissez un nom pour cette politique.

> Choisissez un nom décrivant la nature spécifique du type d'événement que la politique est censée détecter.

6. Pour chaque paramètre affiché :
   a. Lorsque c'est pertinent, sélectionnez **In** (Inclure), option par défaut, pour ajouter l'élément sélectionné à la liste d'autorisations ou **Not In** (Exclure) pour le placer sur la liste de blocage.

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



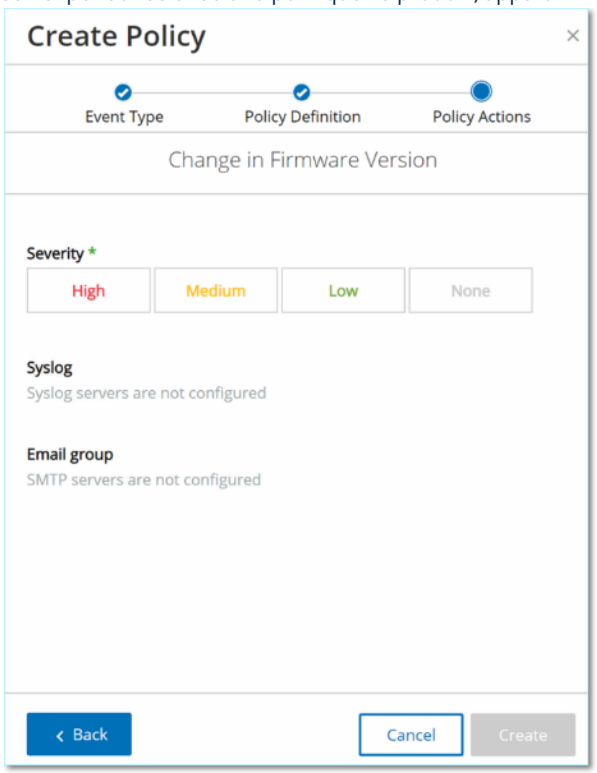

c. Sélectionnez l'élément souhaité.

> 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 *Source*, *Cible* et *Assets affectés*), si vous souhaitez ajouter un groupe d'assets/segment réseau supplémentaire avec une condition « Ou », cliquez sur le bouton « **+ Ou** » bleu à côté du champ et sélectionnez un autre groupe d'assets/segment réseau.

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

7. Une fois tous les champs remplis, cliquez sur **Suivant**.
   Une série de paramètres d'action de politique (c'est-à-dire les actions entreprises par le système lorsqu'une correspondance avec une politique se produit) apparaît.




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

> 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.

> Pour ajouter un serveur SMTP, voir **Serveurs SMTP**.

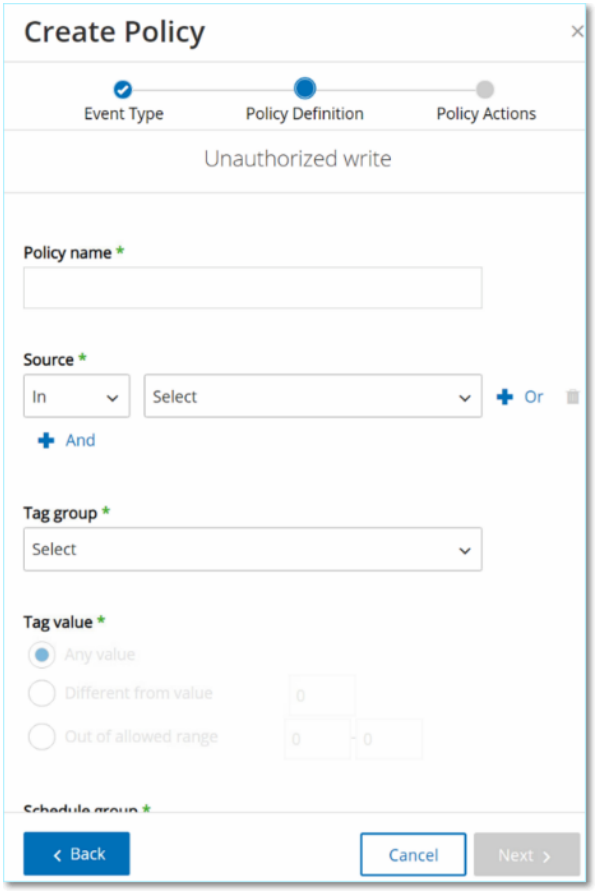
11. Dans la section **Actions supplémentaires**, lorsque l'action spécifiée est pertinente :
    - Pour désactiver la politique après la première correspondance, cochez la case **Désactiver la politique après la première correspondance**. (Cette action est pertinente pour certains types de politiques 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. Une fois tous les champs remplis, cliquez sur **Créer**.
    La nouvelle politique est créée et automatiquement activée. La politique apparaît maintenant dans les listes 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 **Création de 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.

> 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 ou les chaînes personnalisés.

4. Effectuez les procédures de création de politique décrites dans **Création de politiques**.

# Autres actions sur les politiques

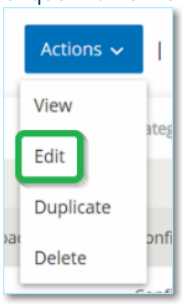
## Modification de politiques

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 de définition (conditions de la politique) et les paramètres d'action de la politique. Pour les politiques de détection d'intrusion, vous pouvez uniquement ajuster les paramètres d'action.

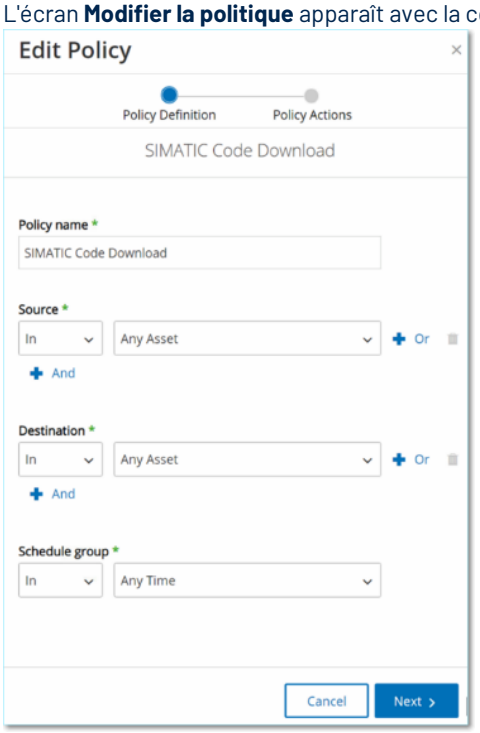
Vous pouvez également modifier les paramètres d'action de plusieurs politiques à la fois.

### Pour modifier une politique :

1. Sur l'écran **Politiques**, cochez la case à côté de la politique souhaitée.
2. Cliquez sur le menu **Actions** et sélectionnez **Modifier** dans la liste déroulante.



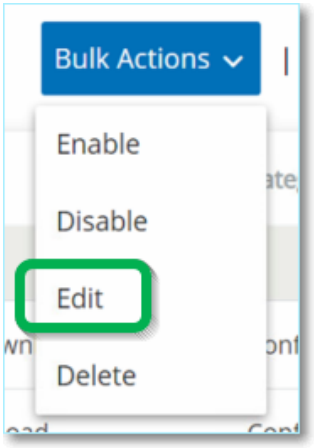

L'écran **Modifier la politique** apparaît avec la configuration actuelle.



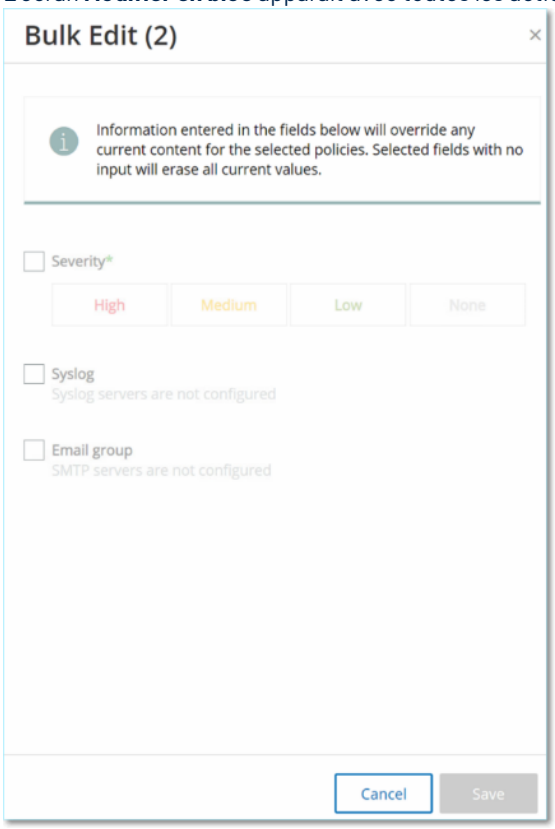

3. Ajustez les paramètres de *définition de la politique* selon vos besoins.
4. Cliquez sur **Suivant**.
5. Ajustez les paramètres *d'action de la politique* selon vos besoins.
6. Cliquez sur **Enregistrer**.
   La politique est enregistrée avec la nouvelle configuration.

### Pour modifier plusieurs politiques (action en bloc) :

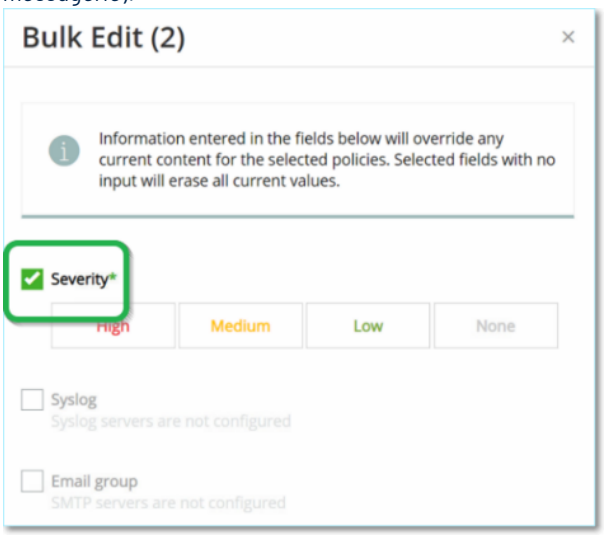
1. Sur l'écran **Politiques**, cochez les cases pour deux politiques ou plus.
2. Cliquez sur le menu **Actions en bloc** et sélectionnez **Modifier** dans la liste déroulante.




L'écran **Modifier en bloc** apparaît avec toutes les actions de politique disponibles pour la modification en bloc.



3. Cochez la case à côté de chacun des paramètres que vous souhaitez modifier (*Sévérité*, *Syslog*, *Groupe de messagerie*).




4. Réglez chaque paramètre selon vos besoins.

> Les informations saisies dans les champs de modification 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 de ce paramètre seront effacées.

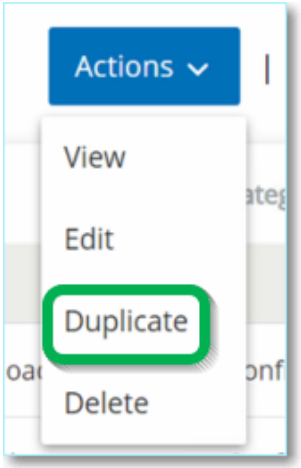
5. Cliquez sur **Enregistrer**.
   Les politiques sont enregistrées avec la nouvelle configuration.

## Duplication de politiques

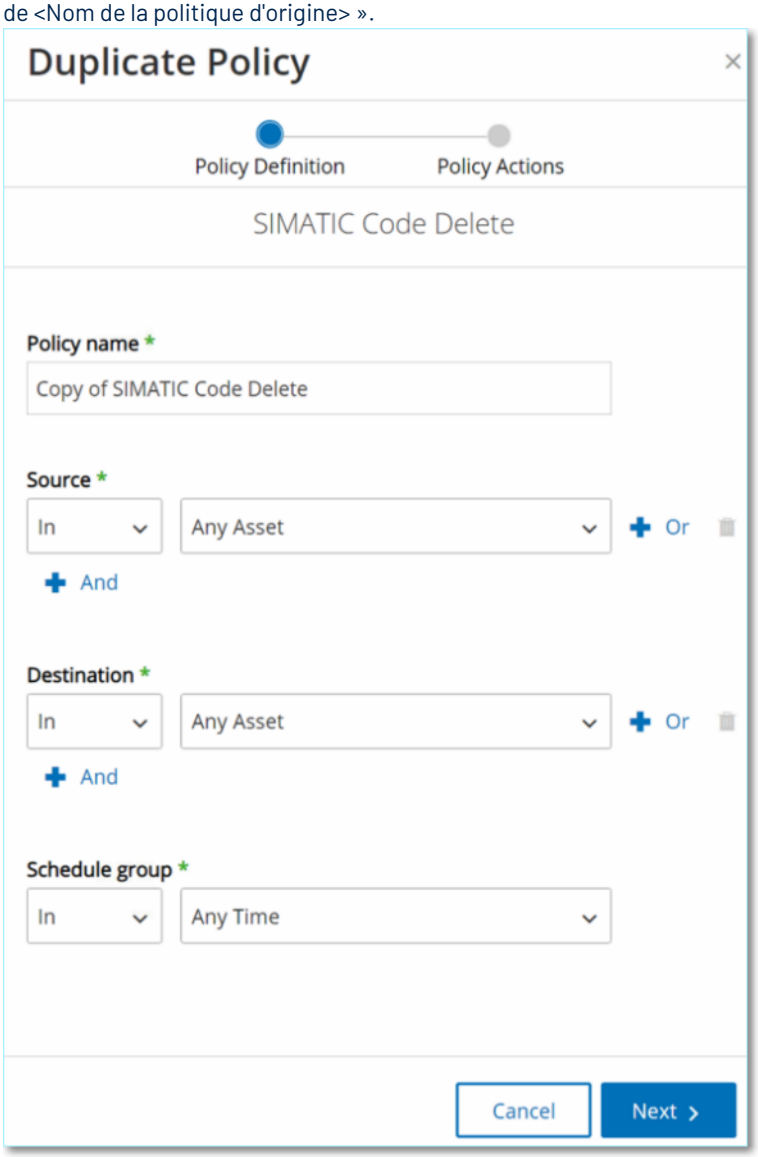
Vous pouvez créer une nouvelle politique similaire à une politique existante en *dupliquant* la politique d'origine et en effectuant les ajustements souhaités. Vous pouvez dupliquer les politiques prédéfinies et définies par l'utilisateur (à l'exception des politiques de détection d'intrusion).

### Pour dupliquer une politique :

1. Sur l'écran **Politiques**, cochez la case à côté de la politique souhaitée.
2. Cliquez sur le menu **Actions** et sélectionnez **Dupliquer** dans la liste déroulante.



L'écran **Dupliquer la politique** apparaît avec la configuration actuelle et le nom défini par défaut comme « Copie de <Nom de la politique d'origine> ».




3. Ajustez les paramètres de *définition de la politique* selon vos besoins.
4. Cliquez sur **Suivant**.
5. Ajustez les paramètres *d'action de la politique* selon vos besoins.
6. Cliquez sur **Enregistrer**.
   La politique est enregistrée avec la nouvelle configuration.

### Suppression de politiques

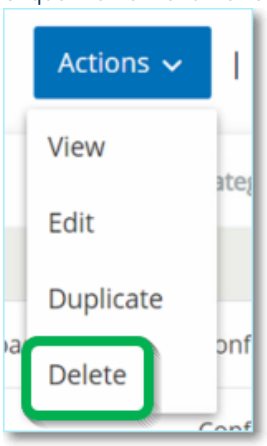
Vous pouvez supprimer une politique du système. Vous pouvez supprimer les politiques prédéfinies et définies par l'utilisateur (à l'exception des politiques de détection d'intrusion qui ne peuvent pas être supprimées).

Vous pouvez également supprimer plusieurs politiques à la fois.

> 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. Sur l'écran **Politiques**, cochez la case à côté de la politique souhaitée.
2. Cliquez sur le menu **Actions** et sélectionnez **Supprimer** dans la liste déroulante.

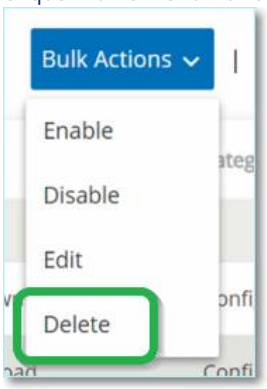



Une fenêtre de confirmation apparaît.

3. Cliquez sur **Supprimer**.
La politique est supprimée du système.

#### Pour supprimer plusieurs politiques (action en bloc) :

1. Sur l'écran **Politiques**, cochez les cases pour chaque politique souhaitée.
2. Cliquez sur le menu **Actions en bloc** et sélectionnez **Supprimer** dans la liste déroulante.




Une fenêtre de confirmation apparaît.

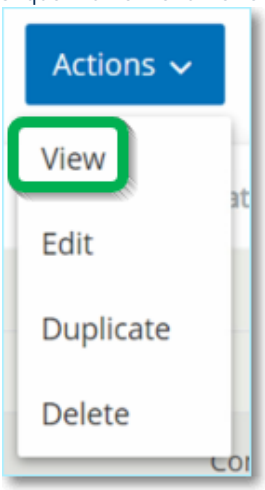
3. Cliquez sur **Supprimer**.
Les politiques sont supprimées du système.

## Suppression d'exclusions de politique

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

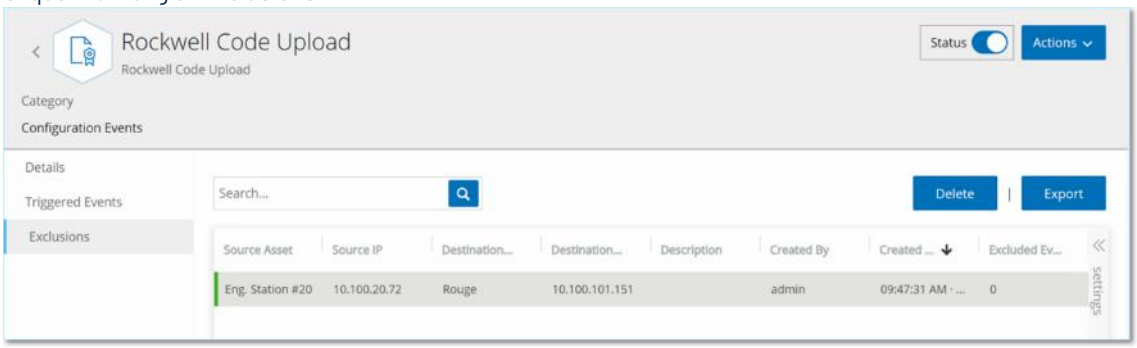
### Pour supprimer une exclusion de politique :

1. Sur l'écran **Politiques**, sélectionnez la politique souhaitée.
2. Cliquez sur le menu **Actions** et sélectionnez **Afficher** dans la liste déroulante.




> Vous pouvez également accéder au menu Actions en faisant 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**.
   L'exclusion est supprimée du système.

# Groupes

Les groupes sont des éléments indispensables dans l'élaboration des politiques. Lors de la configuration d'une politique, chaque condition s'applique à un groupe et non à des entités spécifiques. Le système est livré avec quelques groupes prédéfinis. Vous pouvez également définir vos propres groupes. Par conséquent, il est recommandé de configurer à l'avance les groupes dont vous aurez besoin pour fluidifier le processus de modification et de création de politiques.

Les paramètres de politique ne peuvent être définis qu'à l'aide des groupes. Pour qu'une politique s'applique à une entité particulière, vous devez configurer un groupe comprenant uniquement cette entité.

Sous **Groupes**, vous pouvez afficher tous les groupes qui ont été configurés dans votre système. Les groupes sont divisés en deux catégories :

- **Groupes prédéfinis** – Pré-configurés dans le système, ils ne peuvent pas être modifiés.
- **Groupes définis par l'utilisateur** – Créés par l'utilisateur final, ils peuvent être modifiés.

Il existe plusieurs types de groupes, chacun étant utilisé pour la configuration de plusieurs types de politiques. Chaque type de groupe est affiché sur un écran séparé sous Groupes. Les types de groupes sont :

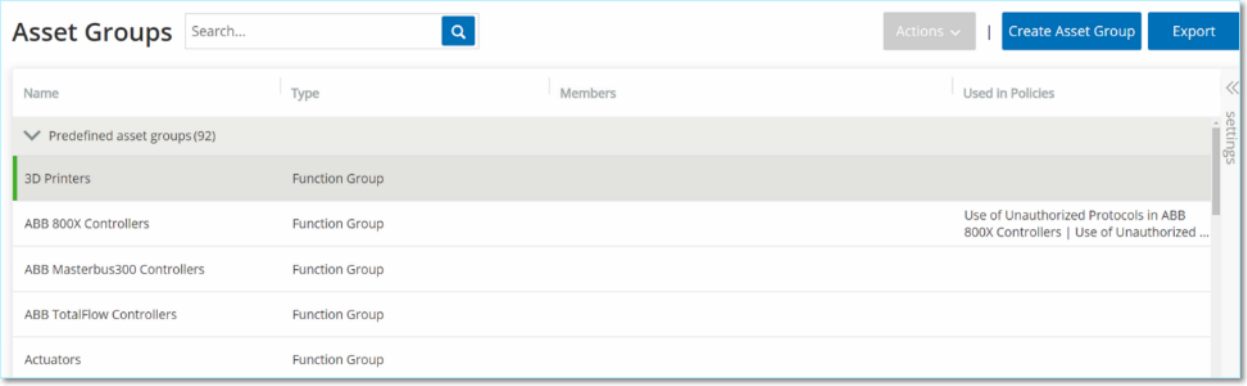
- **Groupes d'assets** – Les assets sont des entités matérielles du réseau. Les groupes d'assets sont utilisés comme condition pour un grand nombre de types de politiques.
- **Segments réseau** – La segmentation du réseau est une méthode de création de groupes d'assets réseau associés, qui permet d'isoler logiquement un groupe d'assets d'un autre.
- **Groupes de messagerie** – Groupes d'e-mails qui sont notifiés lorsqu'un événement lié à une politique se produit. Utilisés pour tous les types de politiques.
- **Groupes de ports** – Groupes de ports utilisés par les assets du réseau. Utilisés pour les politiques qui identifient les ports ouverts.
- **Groupes de protocoles** – Groupes de protocoles par lesquels les communications sont menées entre les assets du réseau. Utilisés comme condition de politique pour les événements réseau.
- **Groupes de planification** – Les groupes de planification sont des plages temporelles utilisées pour configurer la date et l'heure auxquelles l'événement spécifié doit se produire pour remplir les conditions de la politique.
- **Groupes de tags** – Les tags sont des paramètres dans les contrôleurs qui contiennent des données opérationnelles spécifiques. Les groupes de tags sont utilisés comme condition de politique pour les événements SCADA.
- **Groupes de règles** – Les groupes de règles sont constitués d'un ensemble de règles associées, reconnues par leurs identifiants de signature Suricata (SID). Ces groupes sont utilisés comme conditions de politiques pour définir des politiques de détection d'intrusion.

La procédure de création de chaque type de groupe est décrite dans les sections suivantes. De plus, vous pouvez afficher, modifier, dupliquer ou supprimer un groupe existant. Voir **Actions sur les groupes**.

## Groupes d'assets

Les assets sont des entités matérielles du réseau. Le regroupement d'assets similaires vous permet de créer des politiques qui s'appliquent à tous les assets du groupe. Par exemple, vous pouvez utiliser un groupe d'assets nommé *Contrôleurs* 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.

### Affichage des groupes d'assets




L'écran **Groupes d'assets** affiche tous les groupes d'assets actuellement configurés dans le système. L'onglet *Prédéfinis* affiche les groupes intégrés au système qui ne peuvent pas être modifiés, dupliqués ou supprimés. L'onglet *Définis par l'utilisateur* affiche les groupes personnalisés qui ont été créés par l'utilisateur. Ces groupes peuvent être modifiés, dupliqués ou supprimés.

Les informations affichées sur cet écran sont décrites dans le tableau suivant.

| Paramètre | Description |
|---|---|
| **Statut** | Indique si la politique est activée ou désactivée. Si la politique a été automatiquement désactivée par le système car elle générait trop d'événements, une icône d'avertissement apparaît.<br>Activez ou désactivez la politique à l'aide du curseur. |
| **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 : Configuration, SCADA, Menaces réseau ou Événements réseau. Pour une explication des différentes catégories, voir **Catégories et sous-catégories de politiques**. |
| **Source** | Une condition de politique. Le groupe d'assets Source (c'est-à-dire l'asset qui a lancé l'activité) auquel la politique s'applique. |
| **Nom** | Nom utilisé pour identifier le groupe. |

| Paramètre | Description |
|---|---|
| **Type** | Affiche le type de groupe. Les options sont :<br>• Function (Fonction) – Un groupe d'assets prédéfini qui a été créé pour remplir une fonction spécifique.<br>• Sélection des assets – Des assets spécifiés sont inclus dans le groupe.<br>• Liste d'IP – Assets avec l'adresse IP spécifiée.<br>• Plage IP – Assets au sein de la plage d'adresses IP spécifiée. |
| **Membres** | Affiche la liste des assets inclus dans ce groupe. Aucune valeur n'est affichée pour les groupes de type Function Groups (Groupes de fonction).<br>**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.<br>**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**. |

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**.

## Création de groupes d'assets

Vous pouvez créer des groupes d'assets personnalisés à utiliser dans la configuration des 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 :

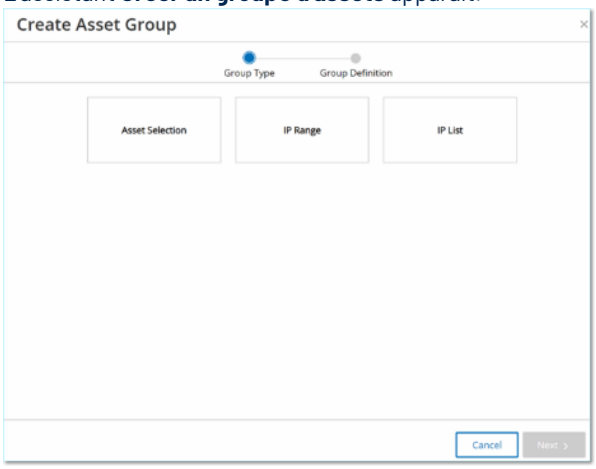
- **Sélection des assets** – Indique les assets spécifiques inclus dans le groupe.
- **Liste d'IP** – Indique les adresses IP des assets inclus dans le groupe.
- **Plage IP** – Indique les plages d'adresses IP des assets inclus dans le groupe.

Il existe différentes procédures pour créer chaque type de groupe d'assets.

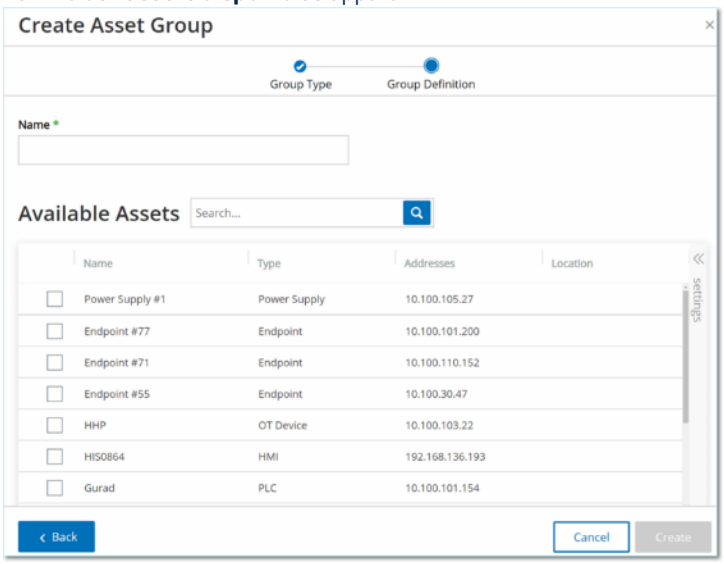
### ➡ Pour créer un groupe d'assets de type Sélection des assets :

1. Sous Groupes, sélectionnez Groupes d'assets.
2. Cliquez sur Créer un groupe d'assets.

L'assistant **Créer un groupe d'assets** apparaît.




3. Cliquez sur Sélection des assets.
4. Cliquez sur **Suivant**.
   La liste des **assets disponibles** apparaît.



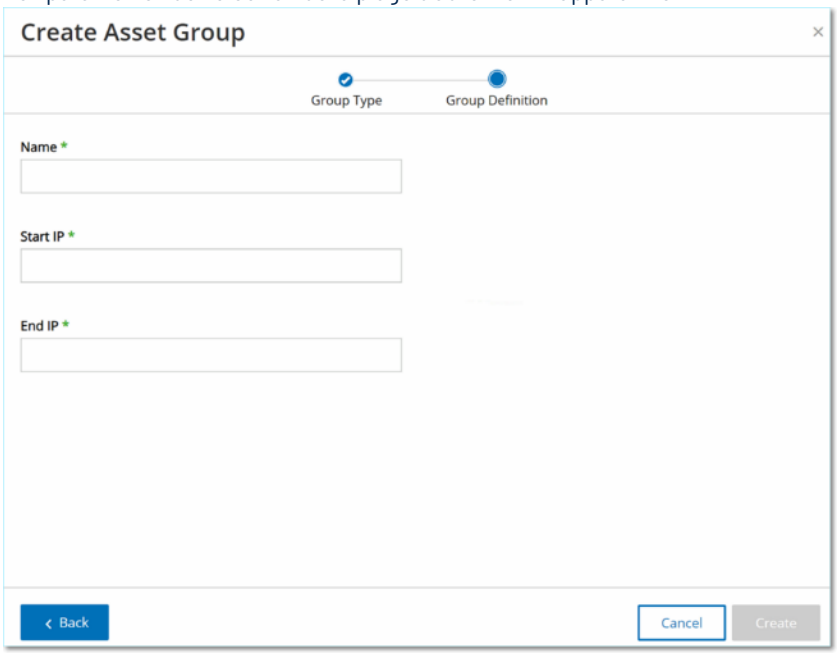

5. Dans le champ **Nom**, saisissez un nom pour ce groupe.
   Choisissez un nom qui décrit un élément commun catégorisant les assets inclus dans le groupe.
6. Cochez la case à côté de chaque asset que vous souhaitez inclure dans le groupe.
7. Une fois vos sélections terminées, cliquez sur **Créer**.
   Le nouveau groupe d'assets est créé et apparaît 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. Sous Groupes, sélectionnez Groupes d'assets.

2. Cliquez sur Créer un groupe d'assets.
   L'assistant Créer un groupe d'assets apparaît.


3. Cliquez sur **Plage IP**.
4. Cliquez sur **Suivant**.
   Les paramètres de sélection de la plage d'adresses IP apparaissent.



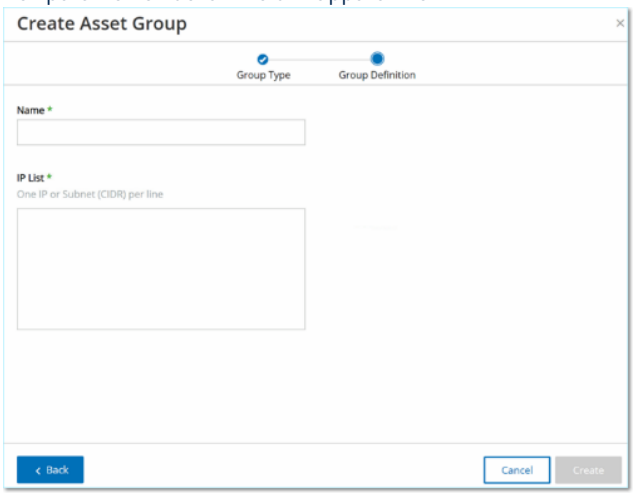

5. Dans le champ **Nom**, saisissez un nom pour ce groupe.
   Choisissez un nom qui décrit un élément commun catégorisant les assets inclus dans le groupe.
6. Dans le champ **Adresse IP de début**, saisissez l'adresse IP débutant la plage à inclure.
7. Dans le champ **Adresse IP de fin**, saisissez l'adresse IP finissant la plage à inclure.
8. Cliquez sur **Créer**.
   Le nouveau groupe d'assets est créé et apparaît 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. Sous Groupes, sélectionnez Groupes d'assets.

2. Cliquez sur Créer un groupe d'assets.
   L'assistant Créer un groupe d'assets apparaît.


3. Cliquez sur **Liste d'IP**.
4. Cliquez sur **Suivant**.
   Les paramètres de la liste d'IP apparaissent.



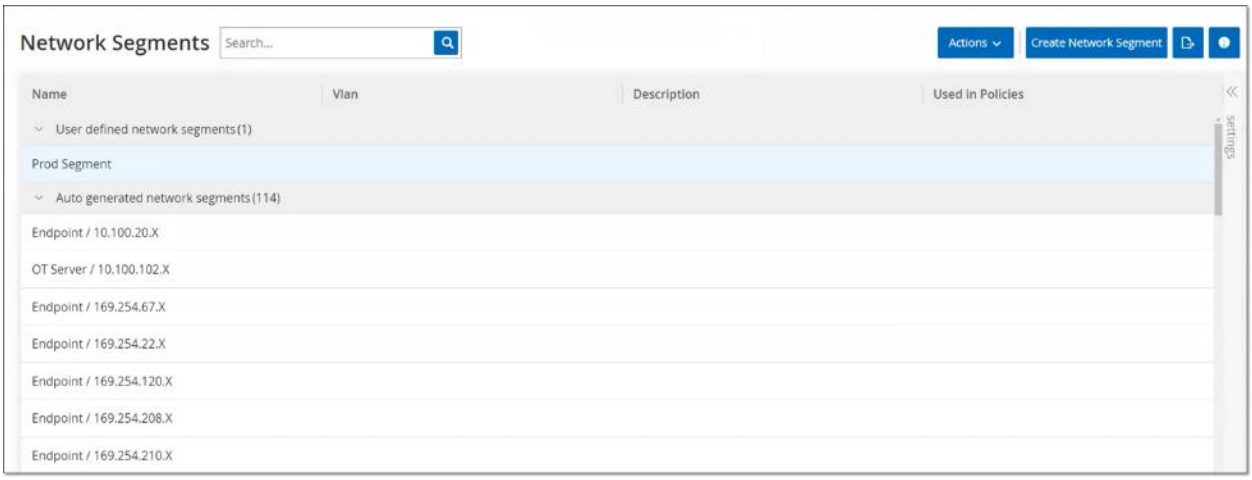

5. Dans le champ **Nom**, saisissez un nom pour ce groupe.
   Choisissez un nom qui décrit un élément commun catégorisant les assets inclus dans le groupe.
6. Dans la zone **Liste d'IP**, saisissez une adresse IP ou un sous-réseau à inclure dans le groupe.
7. Pour ajouter d'autres assets au groupe, saisissez chaque adresse IP ou sous-réseau supplémentaire sur une ligne distincte.
8. Cliquez sur **Créer**.
   Le nouveau groupe d'assets est créé et apparaît sur l'écran Groupes d'assets. Vous pouvez désormais utiliser ce groupe lors de la configuration des politiques.

## Segments réseau

La segmentation du réseau est une méthode de création de groupes d'assets réseau associés, qui permet d'isoler logiquement un groupe d'assets d'un autre. Tenable.ot attribue automatiquement à un segment réseau chaque adresse IP associée à un asset de votre réseau. Pour les assets avec plus d'une adresse IP, chaque adresse IP est associée à un segment réseau. Chaque segment généré automatiquement inclut tous les assets d'une catégorie spécifique (contrôleur, serveurs OT, appareils réseau, etc.) qui ont des adresses IP avec la même adresse réseau de classe C (les IP ont les mêmes premiers 24 bits).

Vous pouvez créer des segments réseau définis par l'utilisateur et préciser les assets affectés à ce segment. Sur les écrans d'inventaire, une colonne indique le segment réseau pour chaque asset, facilitant ainsi le tri et le filtrage de vos assets par segment réseau.

## Affichage des segments réseau




L'écran Segments réseau affiche tous les segments réseau actuellement configurés dans le système. L'onglet *Segments réseau générés automatiquement* contient les segments réseau générés automatiquement par le système. L'onglet *Segments réseau définis par l'utilisateur* contient les segments réseau personnalisés qui ont été créés par l'utilisateur.

Les informations affichées sur cet écran sont décrites dans le tableau suivant :

| Paramètre | Description |
|---|---|
| **Nom** | Le nom utilisé pour identifier le segment réseau. |
| **VLAN** | Le numéro de VLAN du segment réseau. (Facultatif) |
| **Description** | Une description du segment réseau. (Facultatif) |
| **Utilisé dans les politiques** | Affiche les noms des politiques qui s'appliquent à ce segment réseau. **Remarque :** pour afficher plus de détails sur les politiques dans lesquelles le segment réseau est utilisé, cliquez sur le menu **Actions du tableau > Afficher > onglet Utilisé dans les politiques**. |

La procédure de création d'un segment réseau est décrite dans la section suivante. De plus, vous pouvez afficher, modifier, dupliquer ou supprimer un segment réseau existant. Voir **Actions sur les groupes**.

## Création de segments réseau

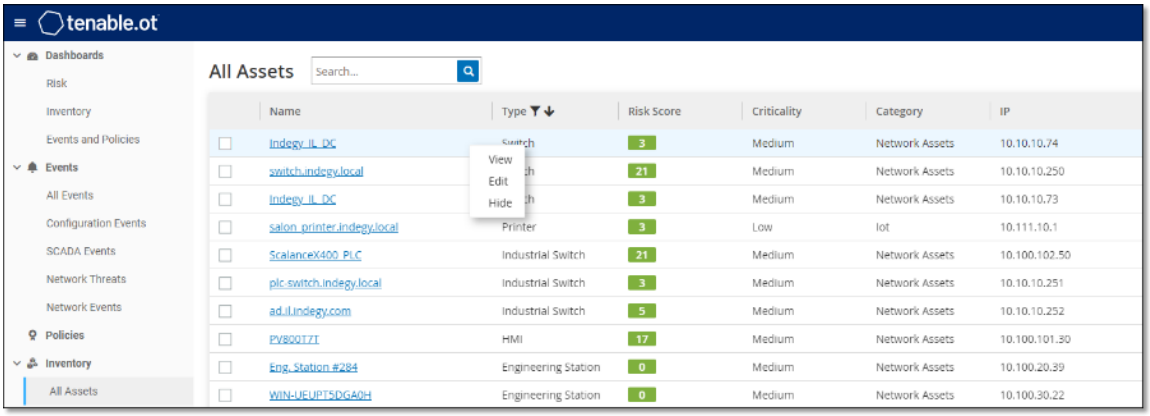
Vous pouvez créer des segments réseau à utiliser dans la configuration des politiques. Le regroupement de segments réseau similaires vous permet de créer des politiques qui définissent le trafic réseau acceptable pour les assets de ce segment.

### Pour créer un segment réseau :

1. Sous **Groupes**, sélectionnez **Segments réseau**.
2. Cliquez sur **Créer un segment réseau**.

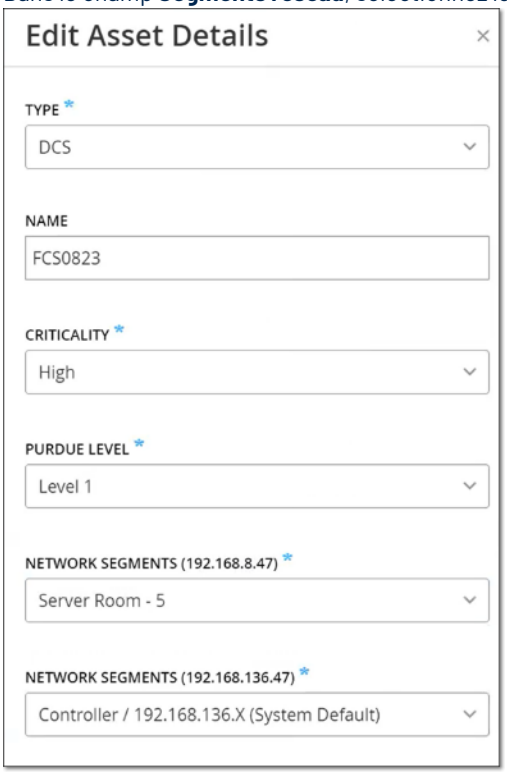
L'assistant **Créer un segment réseau** apparaît.


3. Dans le champ **Nom**, saisissez un nom pour ce segment réseau.
4. Dans le champ **VLAN**, saisissez un numéro de VLAN pour ce segment réseau. (Facultatif)
5. Dans le champ **Description** , saisissez une description du segment réseau. (Facultatif)
6. Cliquez sur **Créer**.
   Le nouveau segment réseau est créé et apparaît dans la liste des segments réseau.
7. Sous **Inventaire**, sélectionnez **Tous les assets**.
8. Effectuez un clic droit sur l'asset que vous souhaitez assigner au segment réseau nouvellement créé et sélectionnez **Modifier**.




La fenêtre **Modifier les détails de l'asset** apparaît.

9. Dans le champ **Segments réseau**, sélectionnez le segment réseau approprié dans la liste déroulante.



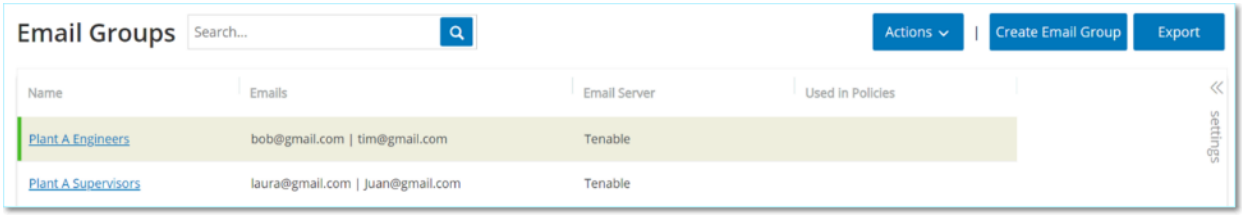

Certains assets ont plusieurs adresses IP associées. Vous pouvez sélectionner le segment réseau approprié pour chacun.

Le segment réseau est appliqué à l'asset et apparaît dans la colonne Segment réseau. Vous pouvez désormais utiliser ce segment réseau lors de la configuration des politiques.

## Groupes de messagerie

Les groupes de messagerie sont des groupes contenant les adresses e-mail de parties concernées. Les groupes de messagerie sont utilisés pour préciser les destinataires des notifications d'événement déclenchées par des politiques spécifiques. Par exemple, le regroupement par rôle ou par service (entre autres) vous permet d'envoyer aux parties concernées les notifications liées à des politiques d'événements spécifiques.

### Affichage des groupes de messagerie




L'écran Groupes de messagerie affiche tous les groupes de messagerie actuellement configurés dans le système.

Les informations affichées sur cet écran sont décrites dans le tableau suivant :

Vous pouvez afficher des détails supplémentaires sur un groupe spécifique en sélectionnant le groupe et en cliquant sur le menu **Actions du tableau** > **Afficher**.

| Paramètre | Description |
|---|---|
| **Nom** | Nom utilisé pour identifier le groupe. |
| **E-mails** | La liste des adresses e-mails incluses dans le groupe.<br>**Remarque :** s'il n'y a pas assez de place pour afficher tous les membres de ce groupe, cliquez sur le menu **Actions du tableau > Afficher > onglet Membres**. |
| **Serveur de messagerie** | Nom attribué au serveur SMTP utilisé pour envoyer les e-mails à ce groupe. |
| **Utilisé dans les politiques** | Affiche les noms des politiques pour lesquelles des notifications sont envoyées à ce groupe.<br>**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**. |

La procédure de création d'un groupe de messagerie est décrite dans la section suivante. De plus, vous pouvez afficher, modifier, dupliquer ou supprimer un groupe existant. Voir **Actions sur les groupes**.

### Création de groupes de messagerie

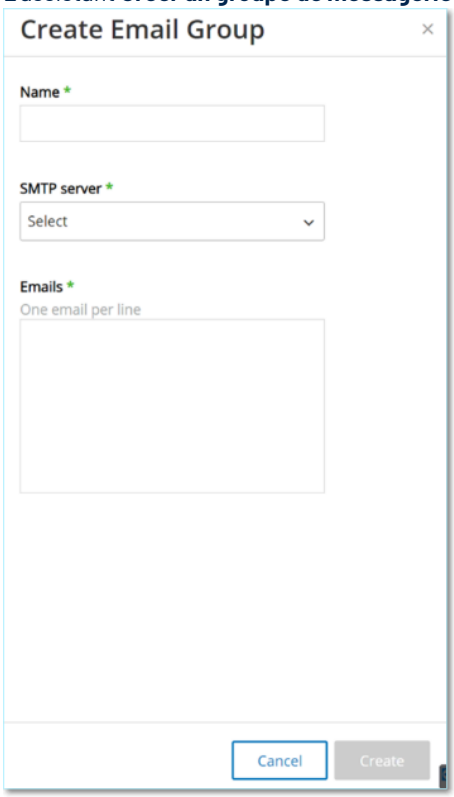
Vous pouvez créer des groupes de messagerie personnalisés à utiliser dans la configuration des politiques. En regroupant les adresses e-mails associées, vous pouvez configurer les notifications d'événement de politique à envoyer à tout le personnel concerné.

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. Sous **Groupes**, sélectionnez **Groupes de messagerie**.
2. Cliquez sur **Créer un groupe de messagerie**.

L'assistant **Créer un groupe de messagerie** apparaît.




3. Dans le champ **Nom**, saisissez un nom pour ce groupe.
4. Dans le champ **Serveur SMTP**, sélectionnez dans la liste déroulante le serveur utilisé pour envoyer les notifications par e-mail.

> 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 le champ **E-mails** , saisissez l'adresse e-mail de chaque membre du groupe sur une ligne distincte.
6. Cliquez sur **Créer**.
   Le nouveau groupe de messagerie est créé et apparaît sur l'écran Groupes de messagerie. Vous pouvez désormais utiliser ce groupe lors de la configuration des politiques.

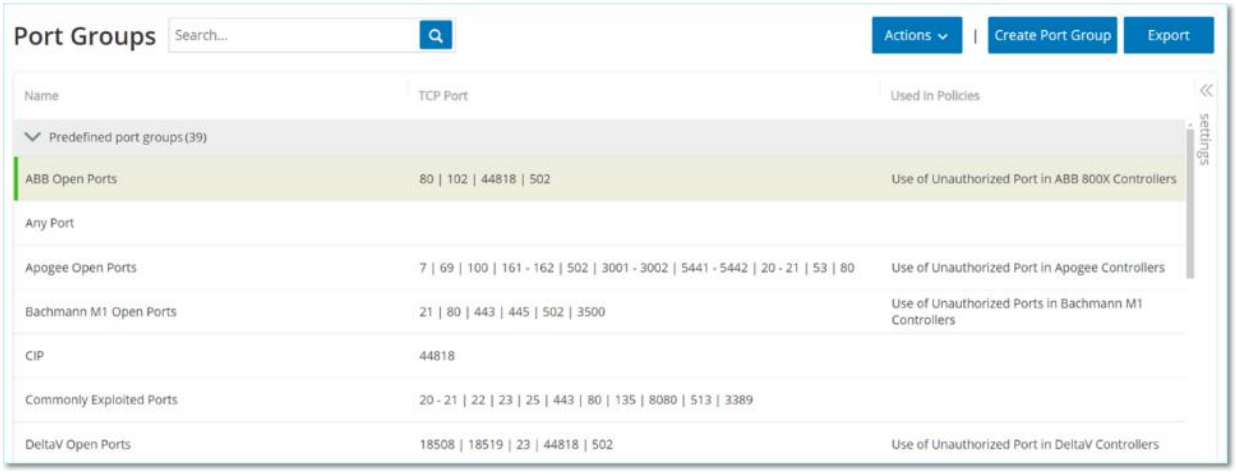
## Groupes de ports

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 des 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 des groupes personnalisés créés par l'utilisateur. Ces groupes peuvent être modifiés, dupliqués ou supprimés.

## Affichage des groupes de ports




Les informations affichées sur cet écran sont décrites dans le tableau suivant :

| Paramètre | Description |
|---|---|
| **Nom** | Nom utilisé pour identifier le groupe. |
| **Ports TCP** | La liste des ports et/ou des plages de ports inclus dans le groupe.<br>**Remarque :** s'il n'y a pas assez de place pour afficher tous les membres de ce groupe, cliquez sur le menu **Actions du tableau > Afficher > onglet Membres**. |
| **Utilisé dans les politiques** | Affiche le nom de chaque politique qui utilise ce groupe de ports dans sa configuration. **Remarque :** pour afficher plus d'informations sur les politiques dans lesquelles ce groupe est utilisé, cliquez sur l'onglet **Actions du tableau > Afficher > onglet Utilisé dans les politiques**. |

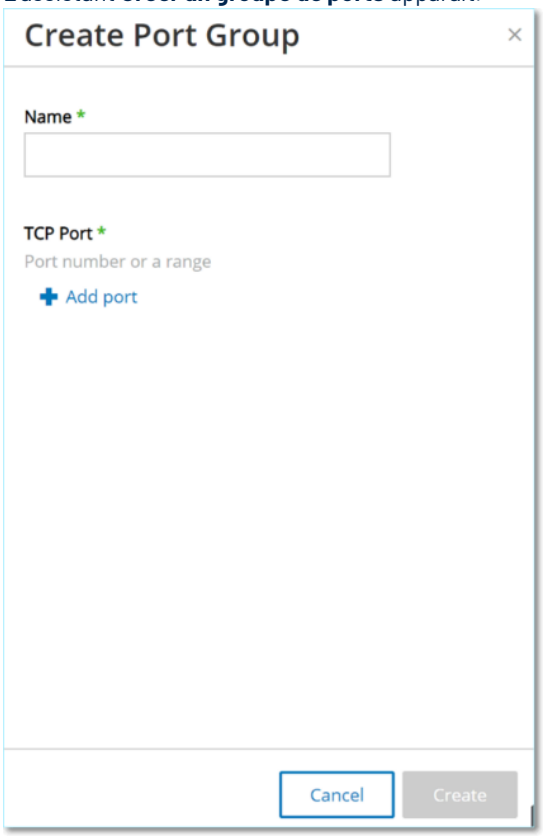
## Création de groupes de ports

Vous pouvez créer des groupes de ports personnalisés à 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. Sous **Groupes**, sélectionnez **Groupes de ports**.
2. Cliquez sur **Créer un groupe de ports**.

L'assistant **Créer un groupe de ports** apparaît.



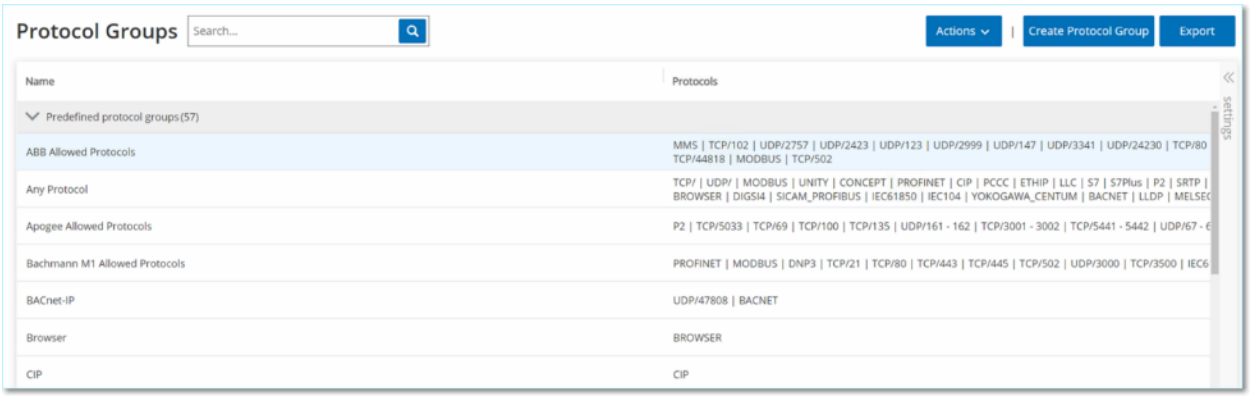

3. Dans le champ **Nom**, saisissez un nom pour ce groupe.
4. Dans le champ **Port TCP**, saisissez un port unique ou une plage de ports à inclure dans le groupe.
5. Pour ajouter des ports supplémentaires au groupe, utilisez la procédure suivante pour chaque port supplémentaire.
    a. Cliquez sur **+ Ajouter un port**.
    Un nouveau champ de sélection de port apparaît.
    b. Dans le nouveau champ **Numéro de port**, saisissez un port unique ou une plage de ports à inclure dans le groupe.
6. Cliquez sur **Créer**.
Le nouveau groupe de ports est créé et apparaît 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 de groupes de protocoles par lesquels les communications sont menées entre les assets du réseau. Les groupes de protocoles sont utilisés comme condition pour les politiques réseau, définissant quels protocoles utilisés entre des assets donnés déclenchent une politique.

Tenable.ot 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. Ces groupes ne peuvent pas être modifiés ni supprimés. 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 également être regroupés par type de protocole (Modbus, PROFINET, CIP, etc.). Vous pouvez également créer vos propres groupes de protocole.

### Affichage des 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. Ces groupes ne peuvent pas être modifiés, dupliqués ni supprimés. L'onglet *Définis par l'utilisateur* affiche des groupes personnalisés qui ont été créés par l'utilisateur. Ces groupes peuvent être modifiés, dupliqués ou supprimés.

Les informations affichées sur cet écran sont décrites dans le tableau suivant.

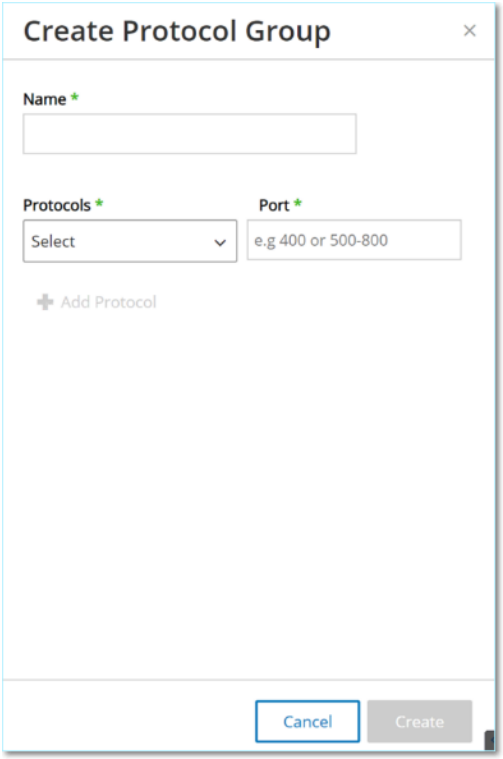
| Paramètre | Description |
|---|---|
| **Nom** | Nom utilisé pour identifier le groupe. |
| **Protocoles** | La liste des protocoles inclus dans le groupe.<br>**Remarque :** s'il n'y a pas assez de place pour afficher tous les membres de ce groupe, cliquez sur le menu **Actions du tableau > Afficher > onglet Membres**. |
| **Utilisé dans les politiques** | Affiche le nom de chaque politique qui utilise ce groupe de protocoles dans sa configuration.<br>**Remarque :** pour afficher plus de détails sur les politiques dans lesquelles ce groupe est utilisé, cliquez sur le menu **Actions du tableau > Afficher > onglet Utilisé dans les politiques**. |

## Création de groupes de protocoles

Vous pouvez créer des groupes de protocoles personnalisés à utiliser dans la configuration des politiques. Le regroupement de protocoles similaires permet de créer des politiques qui définissent les protocoles suspects.

### Pour créer un groupe de protocoles :

1. Sous **Groupes**, sélectionnez **Groupes de protocoles**.
2. Cliquez sur **Créer un groupe de protocoles**.
   L'assistant **Créer un groupe de protocoles** apparaît.

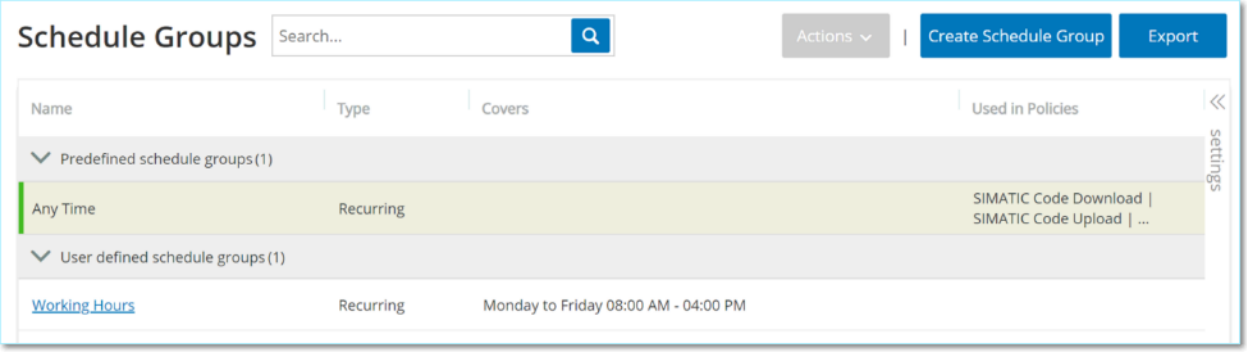



3. Dans le champ **Nom**, saisissez un nom pour ce groupe.
4. Dans le champ **Protocoles**, sélectionnez un type de protocole dans le menu déroulant.
5. Si le protocole sélectionné est *TCP* ou *UDP*, saisissez un numéro de port ou une plage de ports dans le champ **Port**. Pour les autres types de protocoles, aucune valeur n'est saisie dans le champ **Port**.
6. Chaque fois que vous souhaitez ajouter un ou plusieurs protocoles supplémentaires au groupe, utilisez la procédure suivante.
   a. Cliquez sur **+ Ajouter un protocole**.
      Un nouveau champ de **sélection de protocole** apparaît.
   b. Sélectionnez un nouveau protocole comme décrit aux étapes 4 et 5.
7. Cliquez sur **Créer**.
   Le nouveau groupe de protocoles est créé et apparaît 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 de travail, tandis que d'autres activités sont censées avoir lieu pendant les temps d'arrêt.

#### Affichage des groupes de planification




L'écran **Groupes** de **planification** affiche tous les groupes de planification actuellement configurés dans le système. L'onglet *Prédéfinis* affiche les groupes prédéfinis dans le système. Ces groupes ne peuvent pas être modifiés, dupliqués ni supprimés. L'onglet *Définis par l'utilisateur* contient des groupes personnalisés créés par l'utilisateur. Ces groupes peuvent être modifiés, dupliqués ou supprimés.

Les informations affichées sur cet écran sont décrites dans le tableau suivant.

| Paramètre | Description |
|---|---|
| **Nom** | Nom utilisé pour identifier le groupe. |
| **Type** | Affiche le type de groupe. Les options sont :<br>• Function (Fonction) – Un groupe de planification prédéfini qui a été créé pour remplir une fonction donnée.<br>• Recurring (Récurrent) – Pour une planification quotidienne ou hebdomadaire. Par exemple, une planification « Heures de travail » peut être définie du lundi au vendredi de 9h00 à 17h00.<br>• 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.<br>**Remarque :** s'il n'y a pas assez de place pour afficher tous les membres de ce groupe, cliquez sur le menu **Actions du tableau > Afficher > onglet Membres**. |
| **Utilisé dans les politiques** | Affiche l'identifiant de chaque politique qui utilise ce groupe de planification dans sa configuration.<br>**Remarque :** pour afficher plus de détails sur les politiques dans lesquelles ce groupe est utilisé, cliquez sur le menu **Actions du tableau > Afficher > onglet Utilisé dans les politiques**. |

## Création de groupes de planification

Vous pouvez créer des groupes de planification personnalisés à utiliser dans la configuration des politiques. Définissez une ou plusieurs plages temporelles dont les caractéristiques communes rendent les activités qui se produisent pendant cette période dignes d'intérêt.

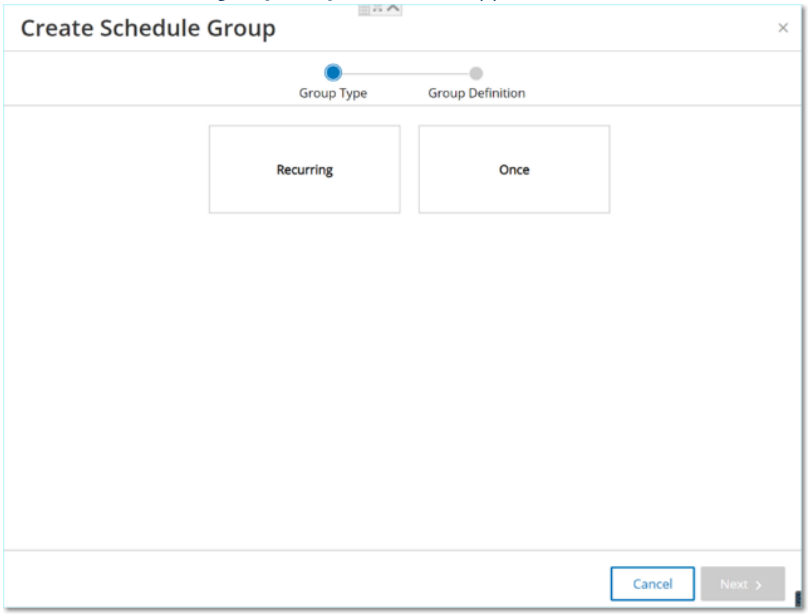
Il existe deux types de groupes de planification :

- **Recurring (Récurrent)** – Pour une planification hebdomadaire. Par exemple, une planification « Heures de travail » peut être définie du lundi au vendredi de 9h00 à 17h00.
- **Once (Ponctuel)** – 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. Il existe différentes procédures pour créer chaque type de groupe de planification.

Il existe différentes procédures pour créer chaque type de groupe de planification.

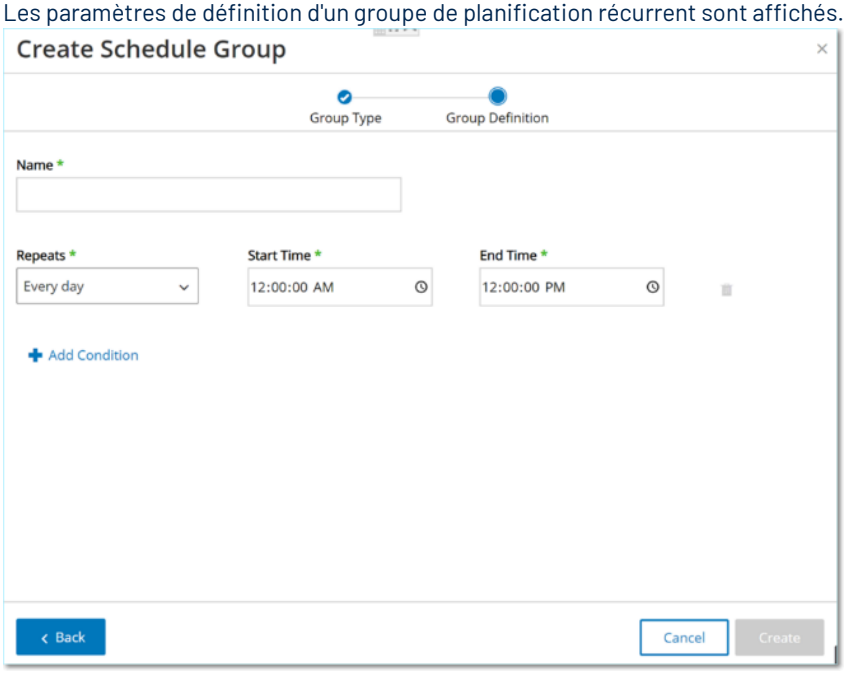
### Pour créer un groupe de planification de type Récurrent :

1. Sous **Groupes**, sélectionnez **Groupes de planification**.
2. Cliquez sur **Créer un groupe de planification**.
3. Sur l'écran **Groupes de planification**, cliquez sur **Créer un groupe de planification**.
   L'assistant **Créer un groupe de planification** apparaît.




4. Sélectionnez **Récurrent**.

5. Cliquez sur **Suivant**.
   Les paramètres de définition d'un groupe de planification récurrent sont affichés.




6. Dans le champ **Nom**, saisissez un nom pour ce groupe.
7. Dans le champ **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.

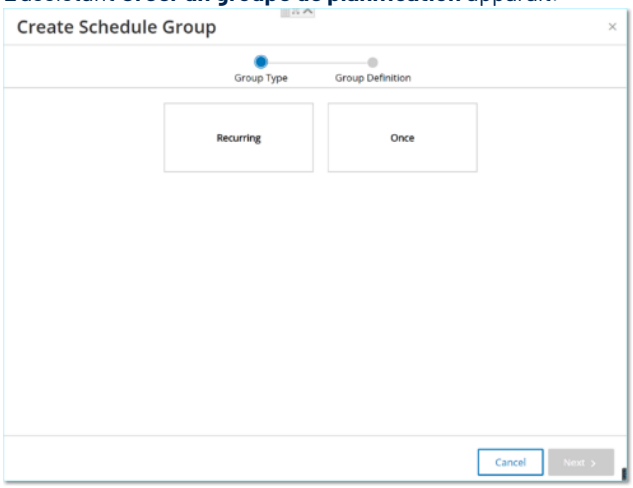
> Pour inclure des jours spécifiques de la semaine, par exemple le lundi et le mercredi, vous devez ajouter une condition distincte pour chaque jour.

8. Dans le champ **Heure de début**, saisissez le début de la plage temporelle (sous la forme heure, minutes, secondes) incluse dans le groupe de planification.
9. Dans le champ **Heure de fin**, saisissez la fin de la plage temporelle (sous la forme heures, minutes, secondes) incluse dans le groupe de planification.
10. Pour ajouter des conditions supplémentaires (ici, des plages temporelles) au groupe de planification, suivez la procédure suivante.
    a. Cliquez sur **+ Ajouter une condition**.
       Une nouvelle ligne de champs de sélection de planification apparaît.
    b. Remplissez les champs comme décrit ci-dessus aux étapes 5 à 7.
11. Cliquez sur **Créer**.
    Le nouveau groupe de planification est créé et apparaît dans la liste des groupes de planification. Vous pouvez désormais utiliser ce groupe lors de la configuration des politiques.

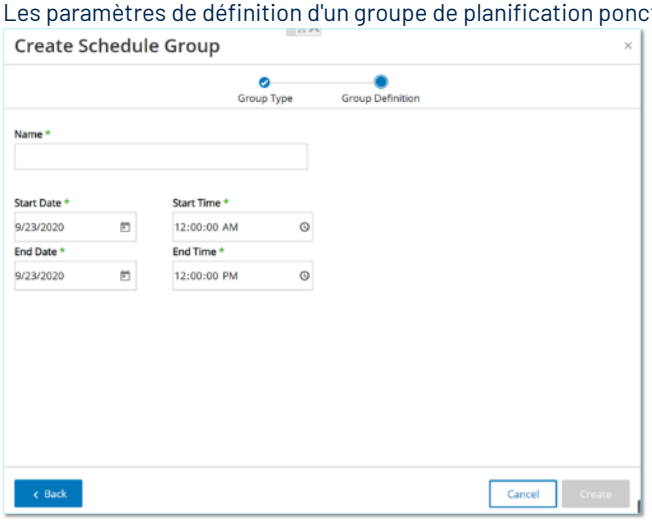
### Pour créer un groupe de planification ponctuel :

1. Sous **Groupes**, sélectionnez **Groupes de planification**.
2. Cliquez sur **Créer un groupe de planification**.

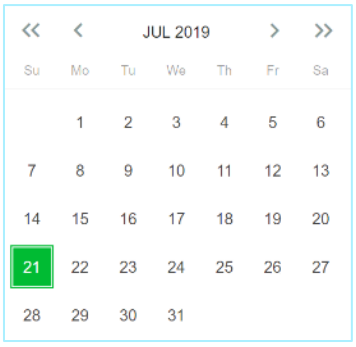
L'assistant **Créer un groupe de planification** apparaît.




3. Sélectionnez **Once** (Ponctuel).
4. Cliquez sur **Suivant**.
   Les paramètres de définition d'un groupe de planification ponctuel sont affichés.




5. Dans le champ **Nom**, saisissez un nom pour ce groupe.
6. Dans le champ **Date de début**, cliquez sur l'icône du calendrier .
   Une fenêtre de calendrier apparaît.



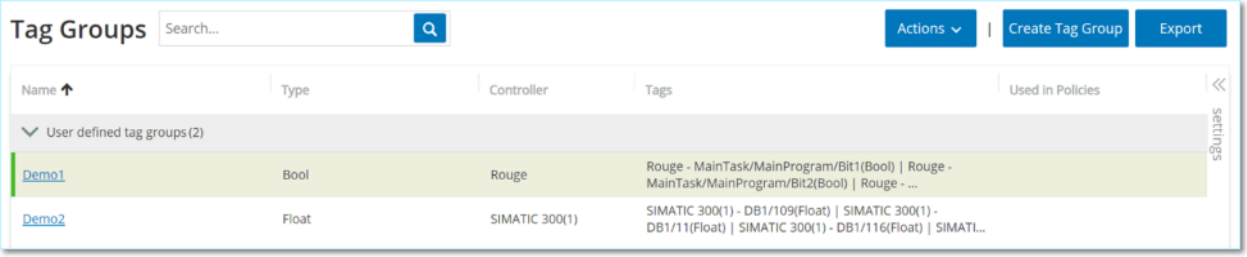

7. Sélectionnez la date à laquelle le groupe de planification commence (par défaut : la date actuelle).
8. Dans le champ **Heure de début**, saisissez le début de la plage temporelle (sous la forme heure, minutes, secondes) incluse dans le groupe de planification.

9. Dans le champ **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 le champ **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**.
    Le nouveau groupe de planification est créé et apparaît dans la liste des groupes de planification. Vous pouvez désormais utiliser ce groupe lors de la configuration des politiques.

## Groupes de tags

Les tags sont des paramètres dans les contrôleurs qui contiennent des données opérationnelles spécifiques.
Les groupes de tags sont utilisés comme condition pour les **politiques d'événements SCADA**. Le regroupement de tags aux rôles similaires permet de créer des politiques qui détectent les modifications suspectes du paramètre spécifié. Par exemple, en regroupant des tags qui contrôlent la température des fours, vous pouvez créer une politique qui détecte les changements de température qui pourraient être nocifs pour les fours.

### Affichage des groupes de tags




L'écran Groupes de tags affiche tous les groupes de tags actuellement configurés dans le système.

Les informations affichées sur cet écran sont décrites dans le tableau suivant.

| 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 Tenable.ot 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.<br>**Remarque :** s'il n'y a pas assez de place pour afficher tous les tags de cette ligne, cliquez sur le menu **Actions du tableau > Afficher > onglet Membres**. |
| **Utilisé dans les politiques** | Affiche l'identifiant de chaque politique qui utilise ce groupe de planification dans sa configuration.<br>**Remarque :** pour afficher plus de détails sur les politiques dans lesquelles ce groupe est utilisé, cliquez sur le menu **Actions du tableau > Afficher > onglet Utilisé dans les politiques**. |

La procédure de création d'un groupe de ports est décrite dans la section suivante. De plus, vous pouvez afficher, modifier, dupliquer ou supprimer un groupe existant. Voir **Actions sur les groupes**.

## Création de groupes de tags

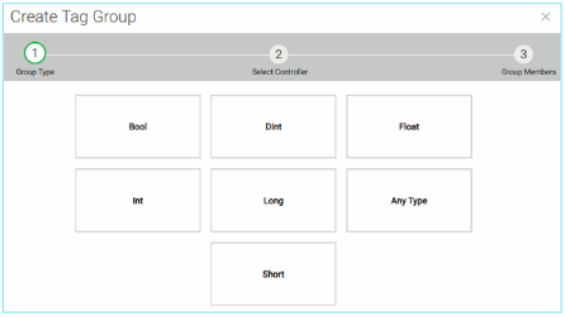
Vous pouvez créer des groupes de tags personnalisés à utiliser dans la configuration des politiques. Le regroupement de tags similaires vous permet de créer des politiques qui s'appliquent à tous les tags du groupe. Sélectionnez les tags de type similaire et nommez-les de manière à représenter l'élément 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.

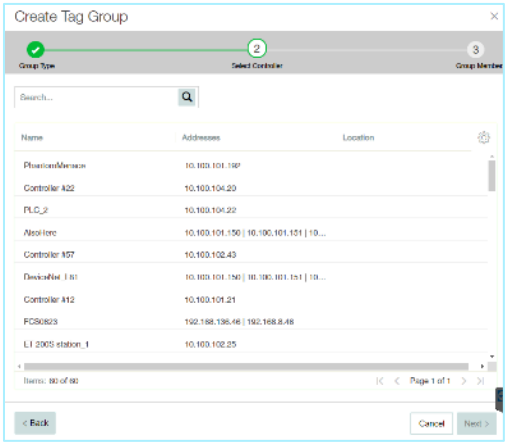
Les groupes de tags peuvent être modifiés, dupliqués ou supprimés.

### Pour créer un groupe de tags :

1. Sous **Groupes**, sélectionnez **Groupes de tags**.
2. Cliquez sur **Créer un groupe de tags**.
   L'assistant **Créer un groupe de tags** apparaît.

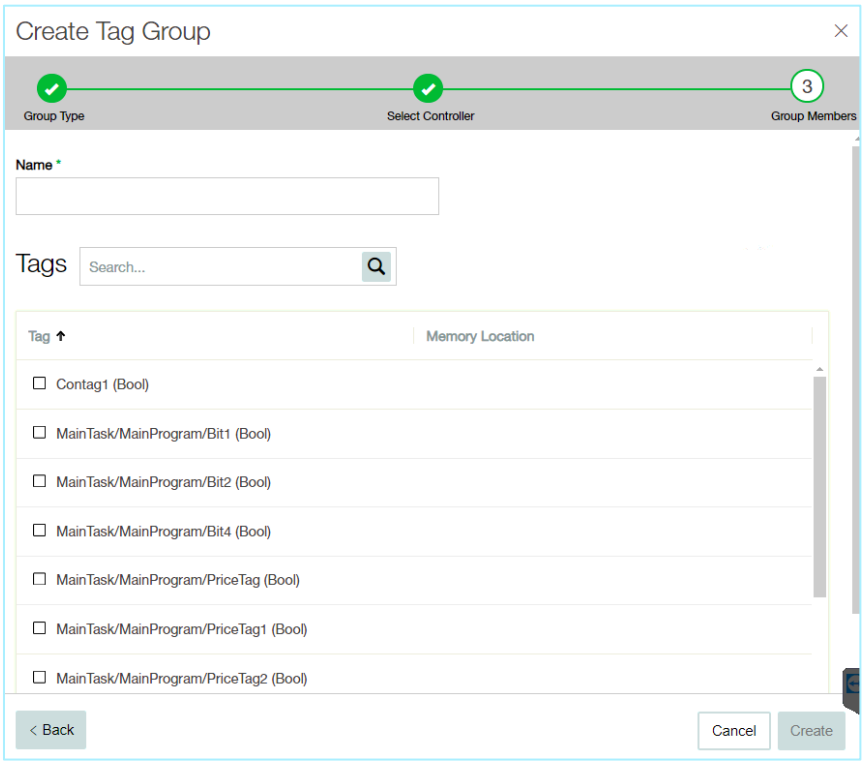



3. Sélectionnez un type de tag. Les options sont : *Bool*, *Dint*, *Float*, *Int*, *Long*, *Short* ou *Any Type* (qui peut inclure des tags de différents types).
4. Cliquez sur **Suivant**.
   Une liste des contrôleurs de votre réseau apparaît.




5. Sélectionnez un contrôleur pour lequel vous souhaitez inclure des tags dans le groupe.
6. Cliquez sur **Suivant**.

Une liste de tags du type spécifié sur le contrôleur spécifié apparaît.




7. Dans le champ **Nom**, saisissez un nom pour ce groupe.
8. Cochez la case à côté des tags que vous souhaitez inclure dans le groupe.
9. Cliquez sur **Créer**.

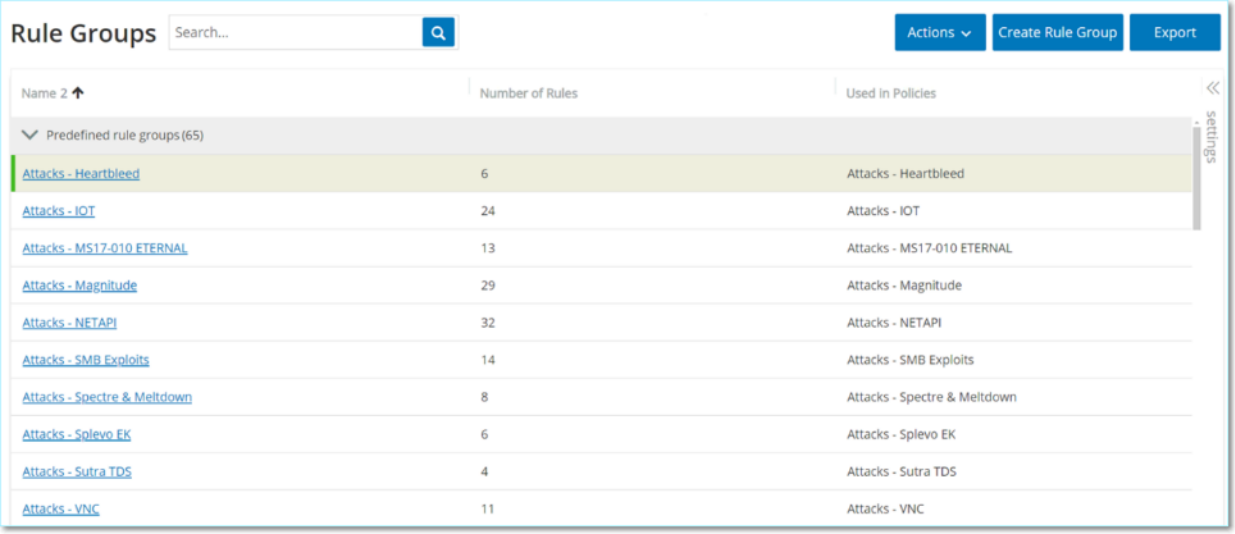
   Le nouveau groupe de tags est créé et apparaît dans la liste des groupes de tags. Vous pouvez désormais utiliser ce groupe lors de la configuration des politiques d'événement SCADA.

## Groupes de règles

Les groupes de règles sont constitués d'un ensemble de règles associées, reconnues par leurs identifiants de signature Suricata (SID). Ces groupes sont utilisés comme conditions pour définir des politiques de détection d'intrusion.

Tenable.ot 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.

### Affichage des 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. Ces groupes ne peuvent pas être modifiés, dupliqués ni supprimés. L'onglet *Définis par l'utilisateur* contient des groupes personnalisés créés par l'utilisateur. Ces groupes peuvent être modifiés, dupliqués ou supprimés.

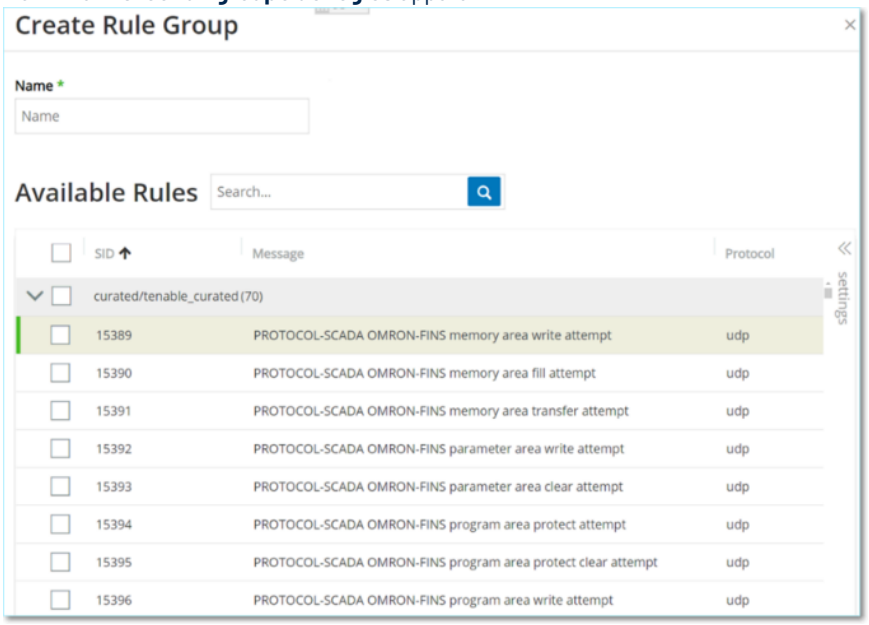
Les informations affichées sur cet écran sont décrites dans le tableau suivant.

| Paramètre | Description |
|---|---|
| **Nom** | Nom utilisé pour identifier le groupe. |
| **Nombre de règles** | Le nombre de règles (SID) qui composent ce groupe de règles. |
| **Utilisé dans les politiques** | Affiche l'identifiant de chaque politique qui utilise ce groupe de règles dans sa configuration.<br>**Remarque :** pour afficher plus de détails sur les politiques dans lesquelles ce groupe est utilisé, cliquez sur le menu **Actions du tableau** > **Afficher** > **onglet Utilisé dans les politiques**. |

## Création de groupes de règles

### Pour créer un groupe de règles :

1. Sous **Groupes**, sélectionnez **Groupes de règles**.
2. Cliquez sur **Créer un groupe de règles**.
   L'assistant **Créer un groupe de règles** apparaît.




3. Dans le champ **Nom**, saisissez un nom pour ce groupe.
4. Dans la section **Règles disponibles**, cochez la case à côté des règles que vous souhaitez inclure dans le groupe.

> Utilisez la zone de recherche pour trouver les règles souhaitées.

5. Cliquez sur **Créer**.
   Le nouveau groupe de règles est créé et apparaît dans la liste des groupes de règles. Vous pouvez désormais utiliser ce groupe lors de la configuration des politiques de détection d'intrusion.

### Actions sur les groupes

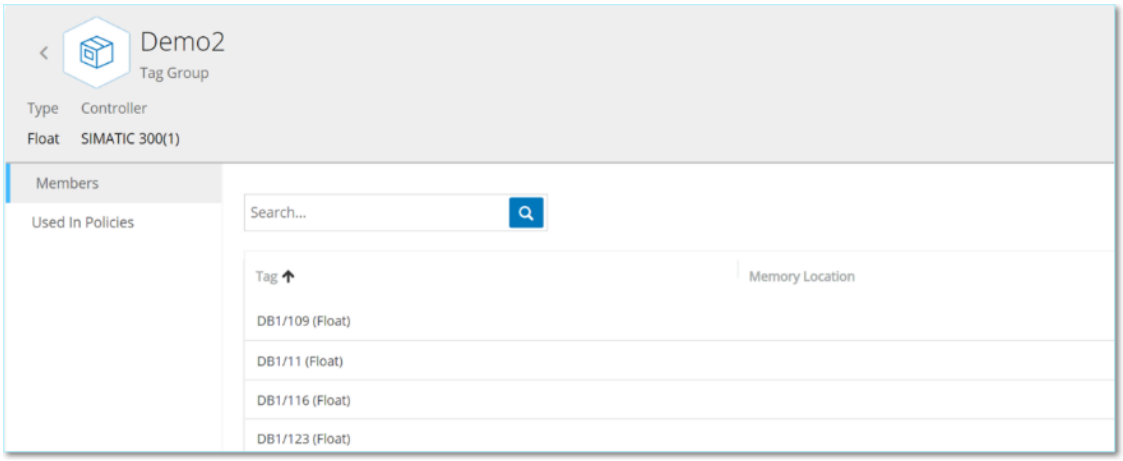
Lorsque vous sélectionnez un groupe (s'applique à tous les écrans de groupe), le menu Actions en haut de l'écran vous permet d'effectuer les actions suivantes :

- **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.
- **Modifier** – Modifie les détails du groupe.
- **Dupliquer** – Crée un groupe avec une configuration similaire au groupe spécifié.
- **Supprimer** – Supprime le groupe du système.

> Les groupes prédéfinis ne peuvent pas être modifiés ni supprimés. Certains groupes prédéfinis ne peuvent pas non plus être dupliqués.
>
> Le menu Actions est également accessible en effectuant un clic droit sur un groupe.

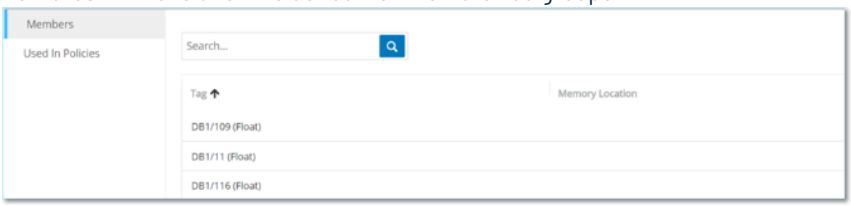
#### Affichage des détails d'un groupe

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 également deux onglets :

- **Membres** – Affiche une liste de tous les membres du groupe.

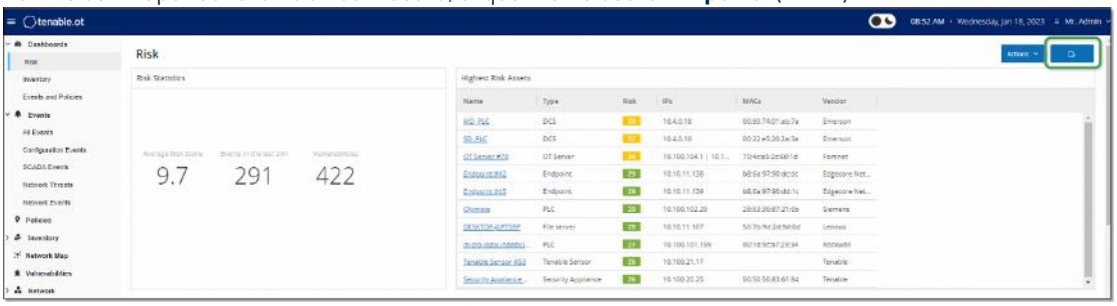



- **Utilisé dans les politiques** – Affiche une liste pour chaque politique pour laquelle le groupe spécifié est utilisé comme condition. Un curseur permet d'activer/désactiver la politique dans les différentes listes. Les informations affichées dans les listes de politiques sont expliquées dans le chapitre **Exportation de dashboard**.

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

### Pour exporter le dashboard :

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

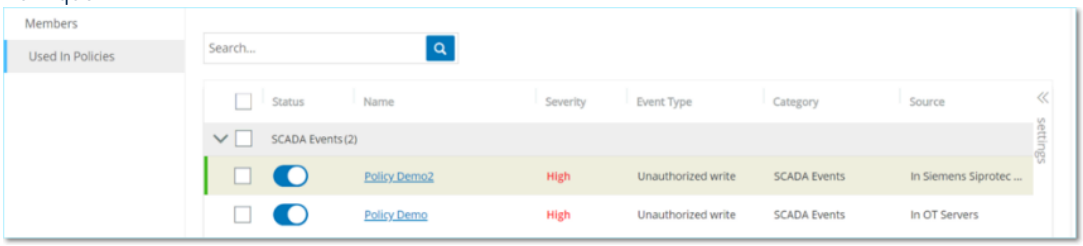



Le PDF se télécharge automatiquement dans le dossier de téléchargement par défaut.

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

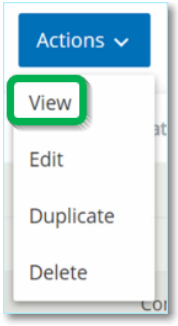
2. Une fois le fichier téléchargé, ouvrez-le pour l'afficher ou le partager.

- Politiques.




### Pour afficher les détails d'un groupe :

1. Sous **Groupes**, sélectionnez le type de groupe souhaité.
2. Sélectionnez le groupe souhaité.
3. Cliquez sur **Actions** (ou effectuez un clic droit sur le groupe).
4. Dans le menu déroulant, sélectionnez **Afficher**.



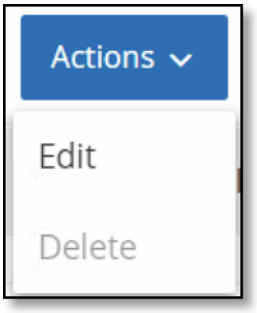

L'écran Détails du groupe apparaît.

## Modification d'un groupe

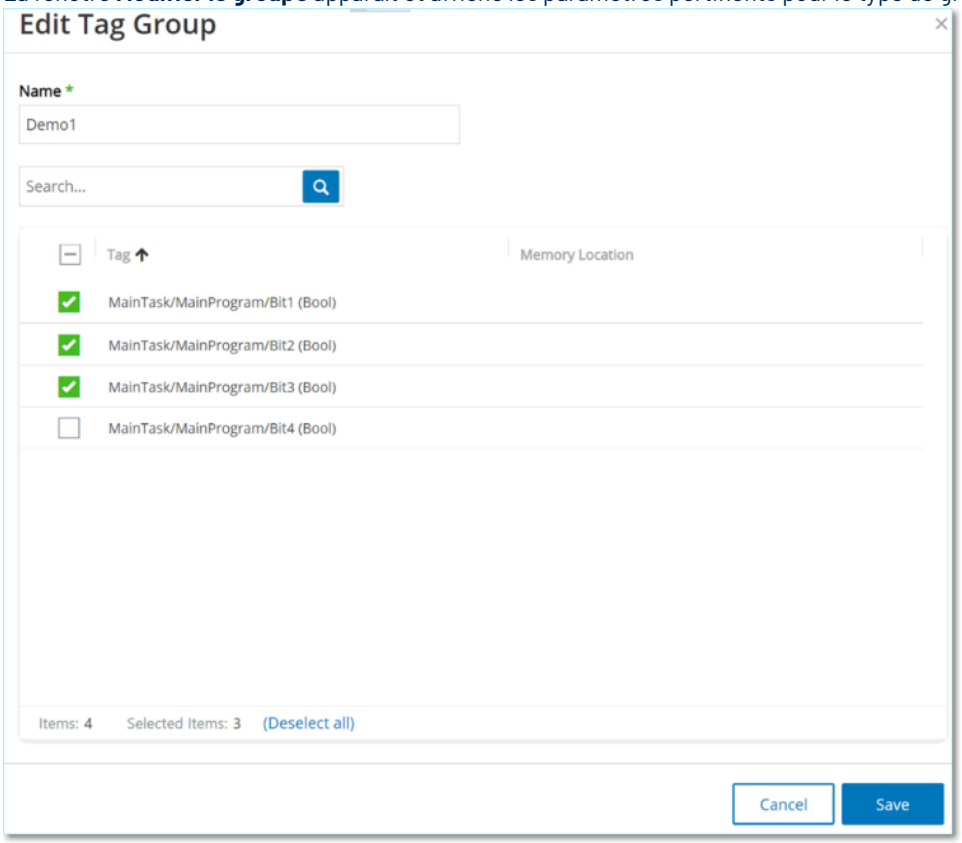
Vous pouvez modifier les détails d'un groupe existant.

### Pour afficher les détails d'un groupe :

1. Sous **Groupes**, sélectionnez le type de groupe souhaité.
2. Sélectionnez le groupe souhaité.
3. Cliquez sur **Actions** (ou effectuez un clic droit sur le groupe).
4. Dans le menu déroulant, sélectionnez **Modifier**.




5. La fenêtre **Modifier le groupe** apparaît et affiche les paramètres pertinents pour le type de groupe spécifié.



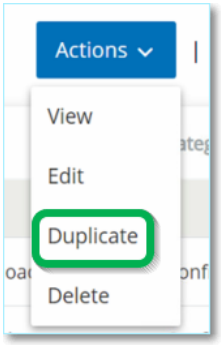

6. Effectuez les modifications souhaitées.
7. Cliquez sur **Enregistrer**.
   Le groupe est enregistré avec les nouveaux paramètres.

## Duplication d'un groupe

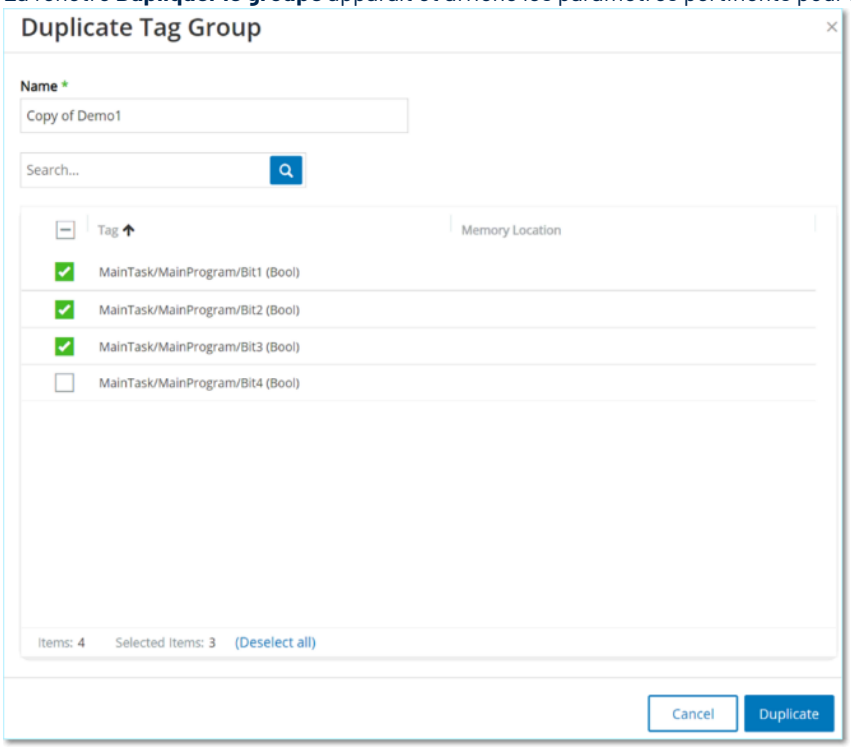
Pour créer un groupe avec des paramètres similaires à un groupe existant, vous pouvez « dupliquer » le groupe existant. Lorsque vous dupliquez un groupe, le nouveau groupe est enregistré sous un nouveau nom, en plus du groupe d'origine.

### Pour dupliquer un groupe :

1. Sous **Groupes**, sélectionnez le type de groupe souhaité.
2. Sélectionnez le groupe existant sur lequel vous souhaitez baser le nouveau groupe.
3. Cliquez sur **Actions** (ou effectuez un clic droit sur le groupe).
4. Dans le menu déroulant, sélectionnez **Dupliquer**.




5. La fenêtre **Dupliquer le groupe** apparaît et affiche les paramètres pertinents pour le type de groupe spécifié.



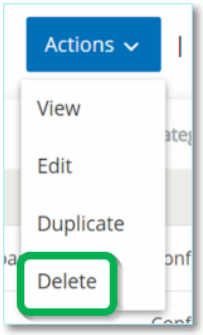

6. Dans le champ **Nom**, saisissez un nom pour ce groupe. Par défaut, le nouveau groupe est nommé « Copie de » suivi du nom du groupe d'origine.
7. Apportez les modifications souhaitées aux paramètres du groupe.
8. Cliquez sur **Dupliquer**.
   Le nouveau groupe est enregistré avec les nouveaux paramètres, en plus du groupe existant.

## Suppression d'un groupe

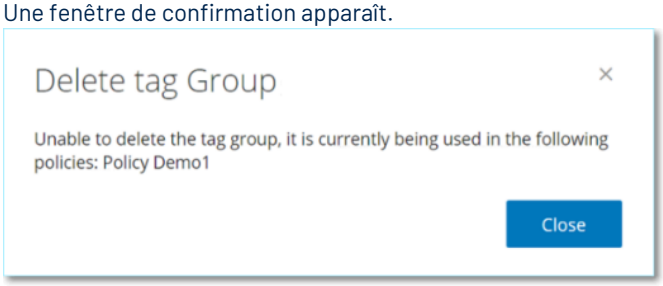
Vous pouvez supprimer des groupes définis par l'utilisateur, mais pas des groupes prédéfinis. De plus, si un groupe défini par l'utilisateur est utilisé comme condition pour une ou plusieurs politiques, il ne peut pas être supprimé.

### Pour supprimer un groupe :

1. Sous **Groupes**, sélectionnez le type de groupe souhaité.
2. Sélectionnez le groupe que vous souhaitez supprimer.
3. Cliquez sur **Actions** (ou effectuez un clic droit sur le groupe).
4. Dans le menu déroulant, sélectionnez **Supprimer**.




5. Une fenêtre de confirmation apparaît.

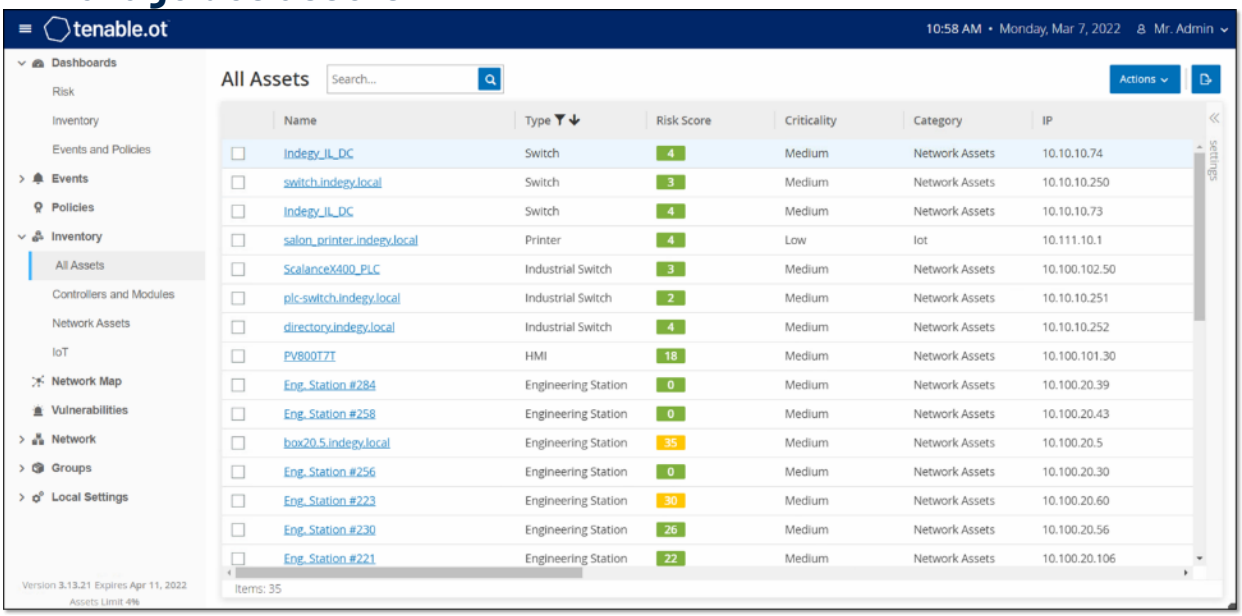



6. Cliquez sur **Supprimer**.
   Le groupe est définitivement supprimé du système.

# Inventaire

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

## Affichage des assets




Tous les assets du réseau sont affichés sur les écrans d'inventaire. Des données détaillées sur chaque asset sont affichées, permettant une gestion complète des assets ainsi que la surveillance de l'état de chaque asset et de ses événements associés. Les données affichées sur les écrans d'inventaire sont collectées à l'aide des fonctionnalités de détection de réseau et de requête active de Tenable.ot. L'écran **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**.

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

Pour chacun des écrans 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 une explication des fonctionnalités de personnalisation, voir **Utilisation des listes**.

Le tableau suivant décrit les paramètres affichés sur les écrans d'inventaire.

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

| Paramètre | Description |
|---|---|
| **Nom** | Le nom de l'asset sur le réseau. Cliquez sur le nom de l'asset pour afficher ses détails (voir **Affichage des détails d'un asset**.) |
| **IP** | L'adresse IP de l'asset.<br>**Remarque :** un asset peut avoir plusieurs adresses IP.<br>**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.<br>**Remarque :** les assets peuvent être filtrés par plage d'adresses IP. Pour plus d'informations sur le filtrage, voir **Filtrage**. |
| **MAC** | L'adresse MAC de l'asset. |
| **Segment réseau** | Le segment réseau auquel les adresses IP de cet asset sont attribuées. |
| **Type** | Le type d'asset, *contrôleur*, *E/S* ou *communication*, etc. Voir **Types d'assets**. |
| **Fond de panier*** | L'unité de fond de panier à laquelle l'asset est connecté. Des détails supplémentaires sur la configuration du fond de panier sont affichés sur l'écran 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 saisi par l'utilisateur dans les détails de l'asset Tenable.ot. Voir **Modification des détails d'un asset**. |
| **Dernière détection** | La date/heure à laquelle l'appareil a été détecté pour la dernière fois par Tenable.ot. 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 :<br>Backup (Sauvegarde) – Le contrôleur s'exécute en tant que sauvegarde d'un contrôleur principal.<br>Fault (Erreur) – Le contrôleur est en panne.<br>NoConfig (Pas de config) – Aucune configuration n'a été définie pour le contrôleur.<br>Running (En cours d'exécution) – Le contrôleur est en cours d'exécution.<br>Stopped (Arrêté) – Le contrôleur ne fonctionne pas.<br>Unknown (Inconnu) – L'état est inconnu. |
| **Description** | Une brève description de l'asset Tenable.ot, dont les détails ont été configurés par l'utilisateur. Voir **Modification des détails d'un asset**. |

| Paramètre | Description |
|---|---|
| **Risque** | Une mesure du degré de risque lié à cet asset sur une échelle de 0 (aucun risque) à 100 (risque extrêmement élevé). Pour une explication de la façon dont le score de risque est calculé, voir **Évaluation des risques**. |
| **Criticité** | Mesure de l'importance de l'asset pour le bon fonctionnement du système. Une valeur est attribuée automatiquement à chaque asset en fonction de son type. Vous pouvez ajuster manuellement la valeur. |
| **Niveau Purdue** | Le niveau Purdue de l'asset (0=Processus physique, 1=Appareils intelligents, 2=Systèmes de contrôle, 3=Systèmes d'exploitation de fabrication, 4=Systèmes logistiques d'entreprise). |
| **Champ personnalisé** | Vous pouvez créer des champs personnalisés pour étiqueter vos assets avec des informations pertinentes. Le champ personnalisé peut être un lien vers une ressource externe. |

## Types d'assets

Le tableau suivant décrit les différents types d'assets identifiés par Tenable.ot. Il affiche également l'icône par laquelle chaque type d'asset est représenté dans la console de gestion de Tenable.ot (par exemple sur l'écran Cartographie du réseau).

| Catégorie | Niveau de criticité/Niveau Purdue par défaut | Description | Sous-types | |
|---|---|---|---|---|
| **Contrôleurs** | High / 1 (Haut / 1) | Un système de contrôle informatique industriel qui surveille en permanence l'état des appareils d'entrée et prend des décisions basées sur un programme personnalisé pour contrôler l'état des appareils de sortie. Cette catégorie comprend tous les types de contrôleurs et leurs composants associés. |  | Contrôleur |
| | | |  | PLC |
| | | |  | DCS |
| | | |  | IED |
| | | |  | RTU |
| | | |  | Contrôleur BMS |
| | | |  | Robot |
| | | |  | Module de communication |
| | | |  | Module E/S |
| | | |  | CNC |

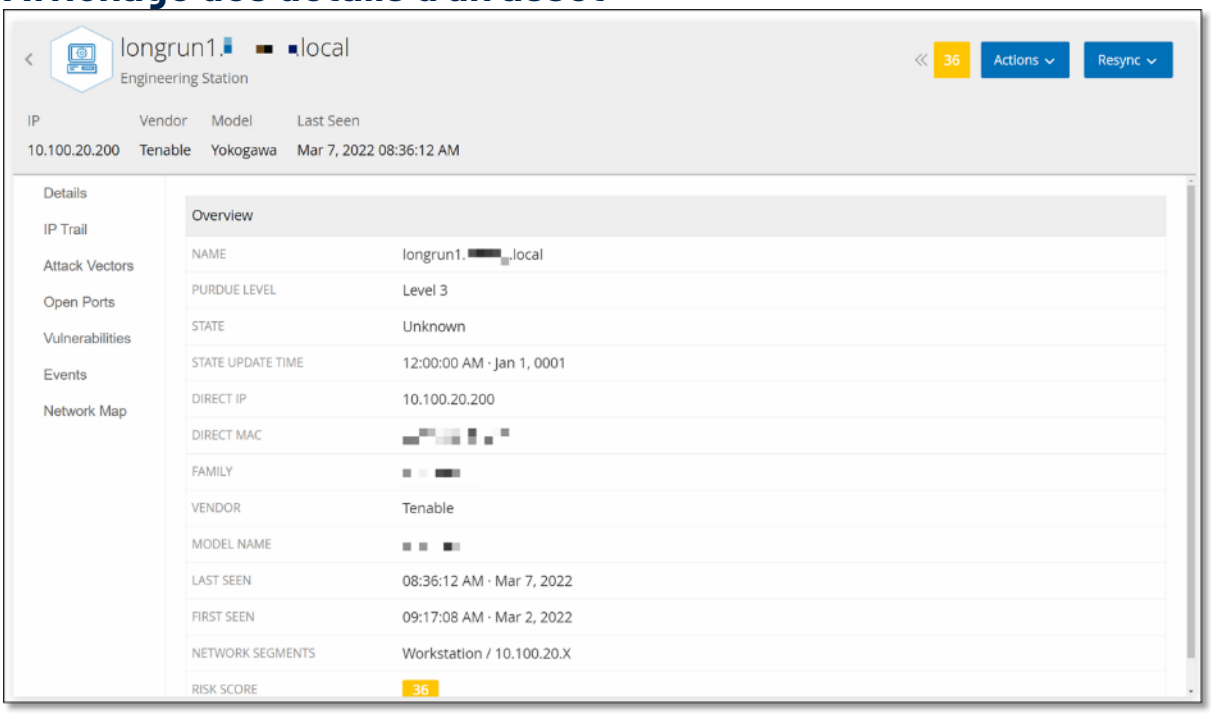
| Catégorie | Niveau de criticité/Niveau Purdue par défaut | Description | Sous-types | |
|---|---|---|---|---|
| | | |  | Alimentation |
| | | |  | Module de fond de panier |
| **Appareils de terrain** | High / 1(Haut / 1) | Appareil industriel (par exemple, capteur, actionneur, moteur électrique) qui utilise des protocoles industriels pour envoyer des informations aux systèmes ICS. |  | Appareil de terrain |
| | | |  | Wattmètre |
| | | |  | E/S à distance |
| | | |  | Relais |
| | | |  | Onduleur |
| | | |  | Capteur industriel |
| | | |  | Lecteur |
| | | |  | Actionneur |
| **Appareils OT** | Medium / 2 (Moyen / 2) | Cette catégorie comprend tous les types d'appareils OT. |  | Appareil OT |
| | | |  | Routeur industriel |
| | | |  | Commutateur industriel |
| | | |  | Passerelle industrielle |
| | | |  | Appareil réseau industriel |
| | | |  | Imprimante industrielle |
| **Serveurs OT** | Medium / 2 (Moyen / 2) | Ordinateur/appareil utilisé pour accéder aux |  | Serveur OT |

| Catégorie | Niveau de criticité/Niveau Purdue par défaut | Description | Sous-types | |
|---|---|---|---|---|
| | | données industrielles. Cette catégorie comprend tous les types de serveurs OT et leurs composants associés. |  | Historien opérationnel |
| | | |  | IHM |
| | | |  | Enregistreur de données |
| **Appareils réseau** | Medium / 3 (Moyen / 3) | Un appareil réseau (par exemple un commutateur ou un routeur). Cette catégorie comprend tous les types d'appareils réseau et leurs composants associés. |  | Appareil réseau |
| | | |  | Routeur |
| | | |  | Commutateur |
| | | |  | Pont Série-Ethernet |
| | | |  | Passerelle |
| | | |  | Hub |
| | | |  | Point d'accès sans fil |
| | | |  | Pare-feu |
| | | |  | Convertisseur |
| | | |  | Répétiteur |
| | | |  | Radio |
| **Postes de travail** | Low / 3 (Faible / 3) | Un ordinateur connecté au réseau et utilisé pour contrôler les PLC. Cette catégorie comprend tous les types de postes de travail et leurs composants associés. |  | Poste de travail |
| | | |  | Poste de travail OT |
| | | |  | Station d'ingénierie |

| Catégorie | Niveau de criticité/Niveau Purdue par défaut | Description | Sous-types | |
|---|---|---|---|---|
| | | |  | Poste de travail virtuel |
| **Serveurs** | Low / 3 (Faible / 3) | Cette catégorie comprend divers types de serveurs informatiques. |  | Serveur |
| | | |  | Serveur de fichiers |
| | | |  | Serveur web |
| | | |  | Serveur virtuel |
| | | |  | Appliance de sécurité |
| | | |  | Tenable ICP |
| | | |  | Tenable EM |
| | | |  | Capteur Tenable.ot |
| | | |  | Contrôleur de domaine |
| | | |  | Internet des objets (IoT) |
| **Internet des objets (IoTs)** | Low / 3 (Faible / 3) | Cette catégorie comprend divers types d'appareils interdépendants. |  | Caméra |
| | | |  | Panneau |
| | | |  | Projecteur |
| | | |  | Appareil VOIP |
| | | |  | Imprimante 3D |
| | | |  | Imprimante |

| Catégorie | Niveau de criticité/Niveau Purdue par défaut | Description | Sous-types | |
|---|---|---|---|---|
| | | |  | UPS |
| | | |  | Téléphone IP |
| | | |  | Capteur intelligent |
| | | |  | Lecteur de code-barres |
| | | |  | Système de contrôle d'accès |
| | | |  | Contrôle d'éclairage |
| | | |  | Module HVAC |
| | | |  | Smart Hub |
| | | |  | Smart TV |
| | | |  | Appareil médical |
| | | |  | Tablette |
| | | |  | Appareil mobile |
| | | |  | Périphérique de stockage |
| **Terminaux** | Low / 3 (Faible / 3) | Une adresse IP non identifiée sur le réseau. |  | Terminal |

# Affichage des détails d'un asset




L'écran **Détails de l'asset** affiche des détails complets sur toutes les données découvertes par Tenable.ot pour l'asset sélectionné. Les détails sont affichés 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.

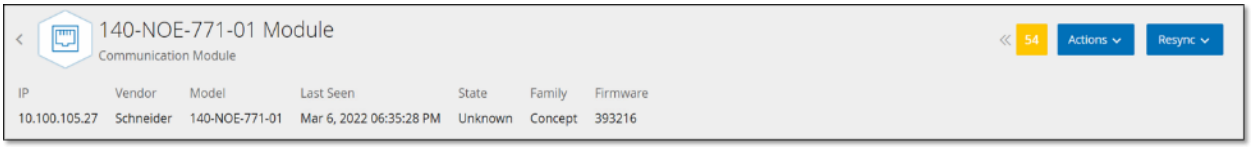
L'écran Détails de l'asset est accessible en cliquant sur le nom d'un asset partout où il apparaît sous forme de lien dans la console de gestion (par exemple, Inventaire, Événements, Réseau, etc.), ou en cliquant sur **Actions** > **Afficher** sur l'écran **Inventaire** pertinent.

Les éléments suivants sont inclus sur l'écran 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 Tenable.ot. Cela inclut des détails sur toutes les modifications spécifiques qui ont été 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 identifiées par le système pour l'asset sélectionné, telles que les systèmes d'exploitation Windows obsolètes, l'utilisation de protocoles vulnérables et les ports de communication ouverts connus pour être risqués ou non essentiels pour des types d'appareils spécifiques, voir **Vulnérabilités**.

- **Événements** – Une liste d'événements sur le réseau impliquant l'asset.
- **Cartographie du réseau** – Affiche une représentation graphique des connexions réseau de l'asset.
- **Ports du périphérique** (pour les commutateurs réseau) – Affiche des informations sur les ports du commutateur réseau.

## Volet d'en-tête



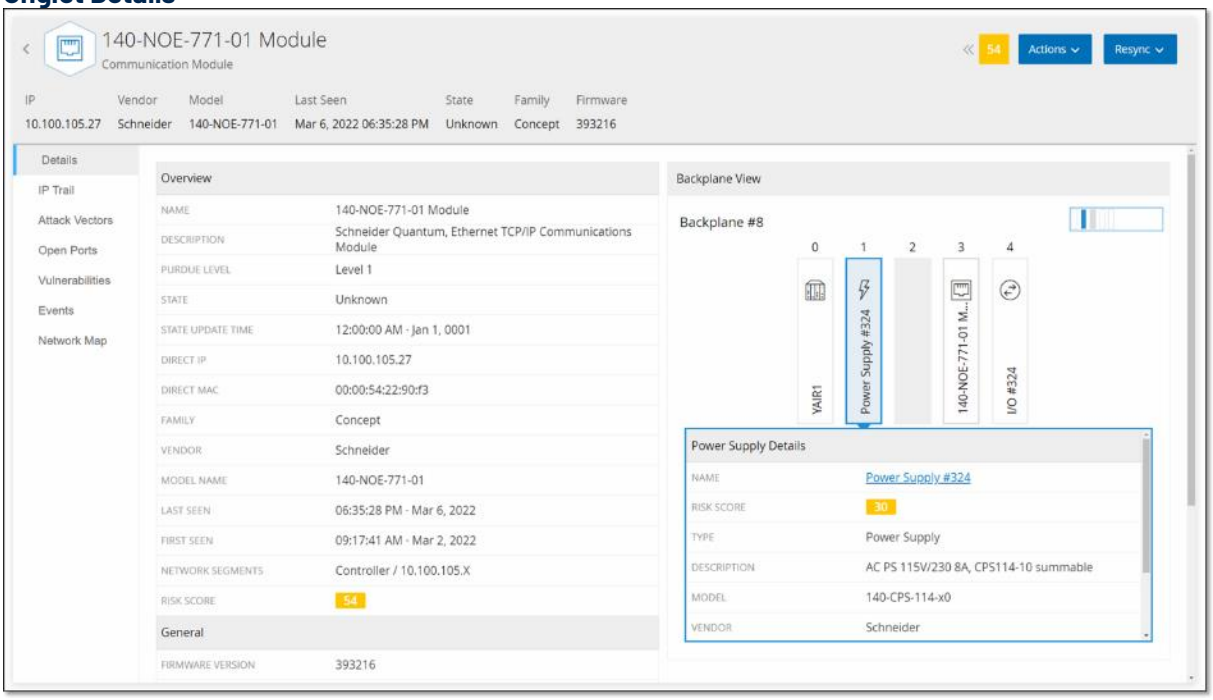

Le volet d'en-tête affiche un aperçu de l'état actuel de l'asset. L'affichage comprend les éléments suivants :

- **Nom** – Le nom de l'asset.
- **Retour (lien)** – Vous renvoie à l'écran à partir duquel vous avez accédé à cet écran d'asset.
- **Type d'asset** – Affiche l'icône et le nom du type d'asset.
- **Aperçu de l'asset** – Affiche des informations essentielles sur l'asset : adresses IP, fournisseur, famille, modèle, firmware et dernière détection (date et heure).
- **Widget Score de risque** – Affiche le score de risque de l'asset. Le score de risque est une évaluation (de 1 à 100) du degré de menace posé à l'asset. Pour une explication de la façon dont la valeur est déterminée, voir **Évaluation des risques**. Cliquez sur l'indicateur de score de risque pour afficher un widget étendu décrivant de façon exhaustive les facteurs qui permettent d'évaluer le niveau de risque (événements non résolus, vulnérabilités et criticité).

  Certains des éléments sont un lien vers l'écran correspondant, qui affiche des détails sur cet élément.
- **Menu Actions** – Vous permet de modifier les détails de l'asset ou d'exécuter un scan Nessus.
- **Bouton Resynchroniser** – Cliquez sur ce bouton pour exécuter manuellement une ou plusieurs des requêtes disponibles pour cet asset. Voir **Exécution d'une resynchronisation**.

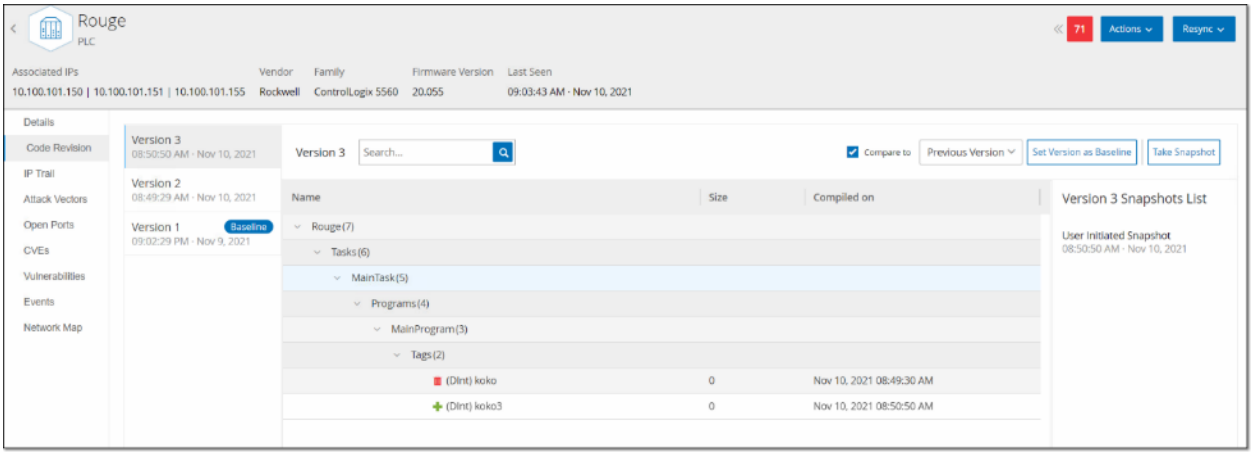
## Onglet Détails




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. Seules les sections pertinentes pour l'asset spécifié sont affichées. Voici une liste de toutes les catégories de section qui peuvent être affichées 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*.

Pour les assets connectés à un fond de panier, il existe également une section *Vue du fond de panier*, qui affiche une représentation graphique de la configuration du fond de panier avec l'emplacement de chaque appareil connecté. Sélectionnez un appareil pour afficher ses détails dans le volet inférieur.

## Révisions de code



L'onglet **Révision de code** (pour les contrôleurs uniquement) affiche les différentes versions du code du contrôleur capturées par les « instantanés » de Tenable.ot. Chaque version « instantanée » inclut des informations sur la révision du code au moment où « l'instantané » a été pris, en incluant des détails sur des sections spécifiques (blocs de code/séquences) et des tags. Chaque fois qu'un « instantané » n'est pas identique à « l'instantané » de ce contrôleur, une nouvelle *version* de la révision de code est créée. Vous pouvez comparer les versions pour voir quelles modifications ont été apportées au code du contrôleur.

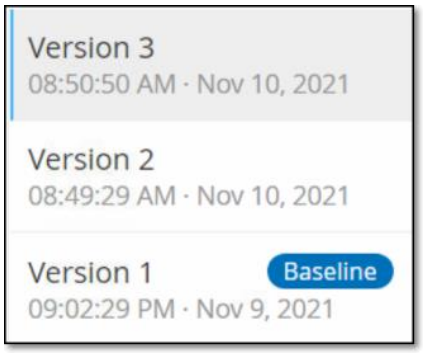
Un instantané peut être déclenché des manières suivantes :

- **Routine** – Les instantanés sont pris à intervalles réguliers, définis par l'utilisateur dans les paramètres du système.
- **Déclenché par une activité** – Le système déclenche un instantané lorsqu'une activité spécifique liée au code est détectée (par exemple, un téléchargement de code).
- **Lancé** par l'utilisateur – L'utilisateur peut déclencher manuellement un instantané en cliquant sur le bouton **Prendre un instantané** pour un asset spécifique.

Vous pouvez configurer une politique « Déviation par rapport à l'instantané » pour détecter les ajouts, les suppressions ou les modifications apportées au code d'un contrôleur, voir **Événement de configuration – Types d'événements liés à la validation** du contrôleur.

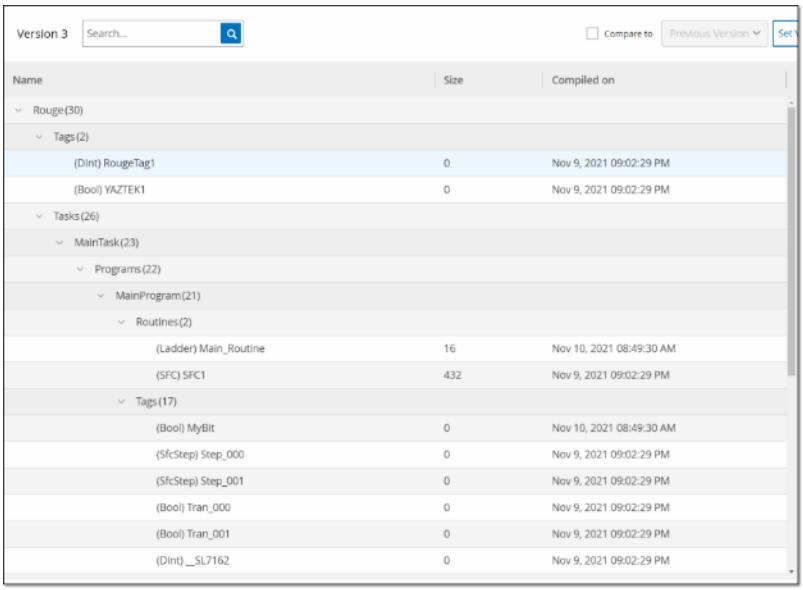
Les sections suivantes décrivent les différentes sections de l'affichage de la révision de code ainsi que la manière de comparer différentes versions « d'instantanés ».

## Volet de sélection de version



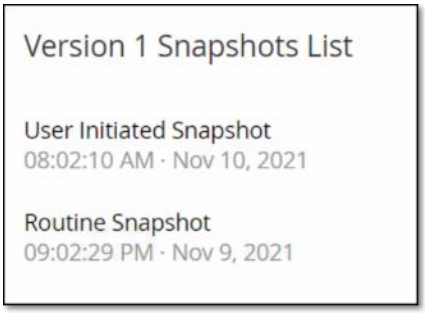

Ce volet affiche une liste de toutes les versions disponibles de la révision de code pour ce contrôleur. Pour chaque version, la date et l'heure de *début* d'application de la version apparaissent. Une nouvelle version est créée à chaque fois qu'un changement est détecté par rapport au précédent « instantané ». Le tag « Base de référence » indique quelle version est actuellement définie comme version de référence à des fins de comparaison. Sélectionnez une version pour afficher ses révisions de code dans le volet **Détails de l'instantané**.

## Volet des détails d'un instantané




Le volet de détails affiche des informations détaillées sur les blocs de code, les séquences, ainsi que les tags relatifs à la version d'instantané sélectionnée. Les éléments de code sont affichés dans une structure arborescente avec des flèches pour développer/réduire les détails affichés. Pour chaque élément, le nom, la taille et la date de compilation sont affichés. Vous pouvez comparer la version sélectionnée à la version précédente ou à la version « de référence » pour voir quelles modifications ont été apportées, voir **Comparaison des versions d'un instantané**.

## Volet d'historique des versions




Ce volet affiche des détails sur « l'instantané » ayant permis de capturer la version sélectionnée, y compris la méthode par laquelle il a été lancé, ainsi que la date et l'heure de la capture.

Si aucune modification n'a été apportée entre les instantanés, plusieurs instantanés sont regroupés en une seule version. Tous les instantanés identiques sont répertoriés dans le volet d'historique de l'instantané pour cette version.

## Comparaison des 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 :

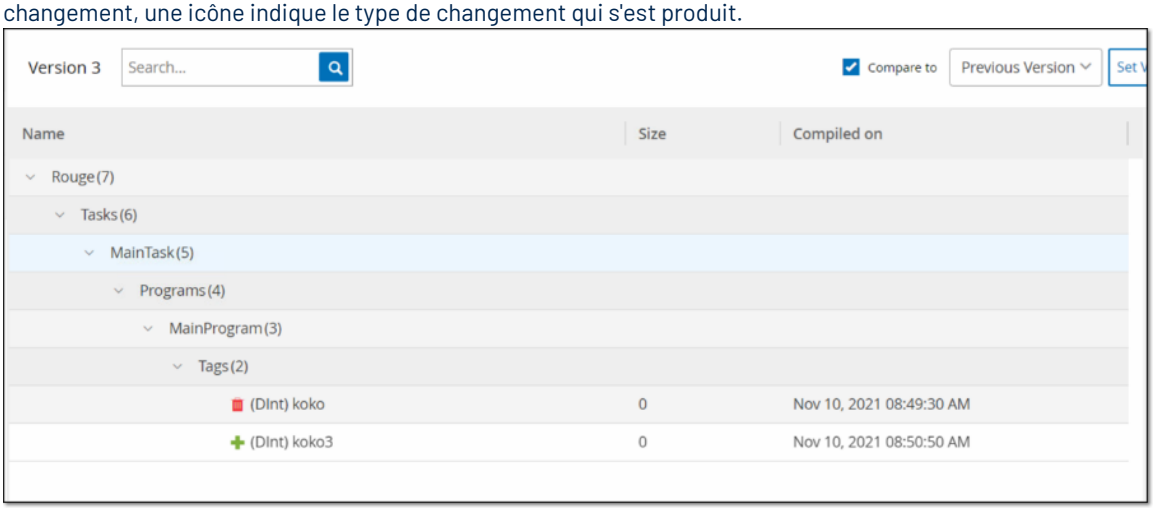
Ajouté – Nouveau code ajouté dans la version sélectionnée.

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.

> La définition d'une version comme base 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.

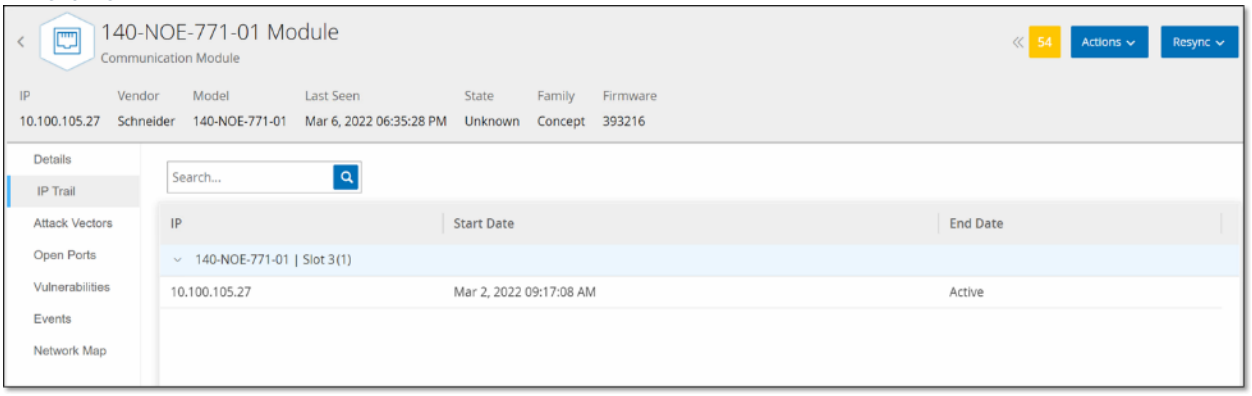
### Création d'un instantané

Un instantané peut être lancé manuellement par l'utilisateur. Par exemple, il est recommandé de prendre un instantané avant et après l'intervention d'un technicien sur un contrôleur.

#### Pour créer un instantané d'un contrôleur :

1. Sur l'écran **Inventaire** > **Contrôleurs**, sélectionnez le contrôleur souhaité.
2. Cliquez sur l'onglet **Révision de code**.
3. Dans le coin supérieur droit du volet des **détails de l'instantané**, cliquez sur **Prendre un instantané**. L'instantané lancé par l'utilisateur est créé.
4. Si aucune modification n'est identifiée, un nouvel instantané identifié par l'utilisateur est ajouté au volet d'historique des révisions pour la dernière version. Si des modifications sont identifiées, une nouvelle version est créée indiquant les modifications de révision du code.

### Itinéraire IP




L'onglet **Itinéraire IP** affiche toutes les adresses IP pertinentes pour cet asset. La colonne Carte réseau affiche une liste des cartes réseau utilisées par cet asset. Cliquez sur la flèche à côté d'une carte réseau pour développer la liste, afin d'afficher les adresses IP de tous les assets connectés au fond de panier partagé.

Les listes incluent les dates de début et de fin d'utilisation de l'adresse IP. Les options pour la date de fin sont :

- **Active** – L'adresse IP est actuellement utilisée pour cet asset.
- **{date/heure}** – La dernière date et heure à laquelle l'adresse IP a été active pour cet asset (si elle a été active au cours des 30 derniers jours).
- **{date/heure} (Inactive)** – La dernière date et heure à laquelle l'adresse IP a été active pour cet asset (si elle a été inactive pendant 30 jours ou plus).
- **Inactive** – L'adresse IP est actuellement utilisée par un autre asset.

### Vecteurs d'attaque

Un attaquant peut compromettre un accès critique en profitant d'un « maillon faible » vulnérable dans le réseau pour accéder à l'asset critique. L'asset critique est la cible (destination) de l'attaque, et le *vecteur d'attaque* est l'itinéraire que l'attaquant utilise pour accéder à cet asset.

#### Comment déterminer le vecteur d'attaque ?

Une fois l'asset cible spécifié, le système calcule tous les vecteurs d'attaque potentiels qui pourraient permettre l'accès à cet asset et identifie le chemin qui présente le potentiel de risque le plus élevé pour compromettre cet asset. Le calcul prend en compte plusieurs paramètres et utilise une approche basée sur le risque afin d'identifier le vecteur d'attaque le plus critique. Les paramètres utilisés 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 (ou leur inadéquation) 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 d'éliminer le chemin d'attaque potentiel.

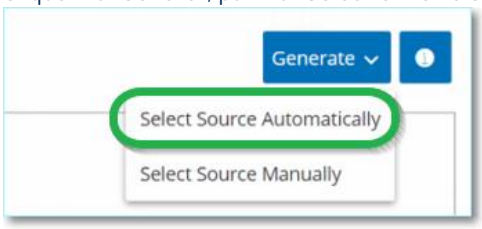
## Génération de vecteurs d'attaque

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** – Tenable.ot évalue tous les vecteurs d'attaque potentiels et identifie le chemin le plus vulnérable.
- **Manuel** – Vous spécifiez un asset source et Tenable.ot vous montre le chemin potentiel (le cas échéant) qui peut être utilisé pour y accéder.

### Pour générer un vecteur d'attaque automatique :

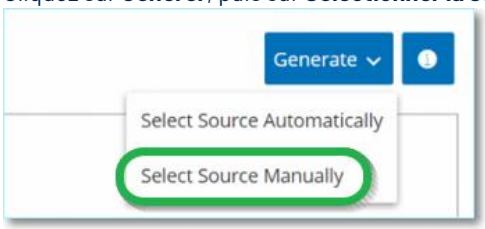
1. Accédez à la page **Détails de l'asset** pour l'asset cible souhaité et cliquez sur l'onglet **Vecteur d'attaque**.
2. Cliquez sur **Générer**, puis sur **Sélectionner la source automatiquement** dans la liste déroulante.



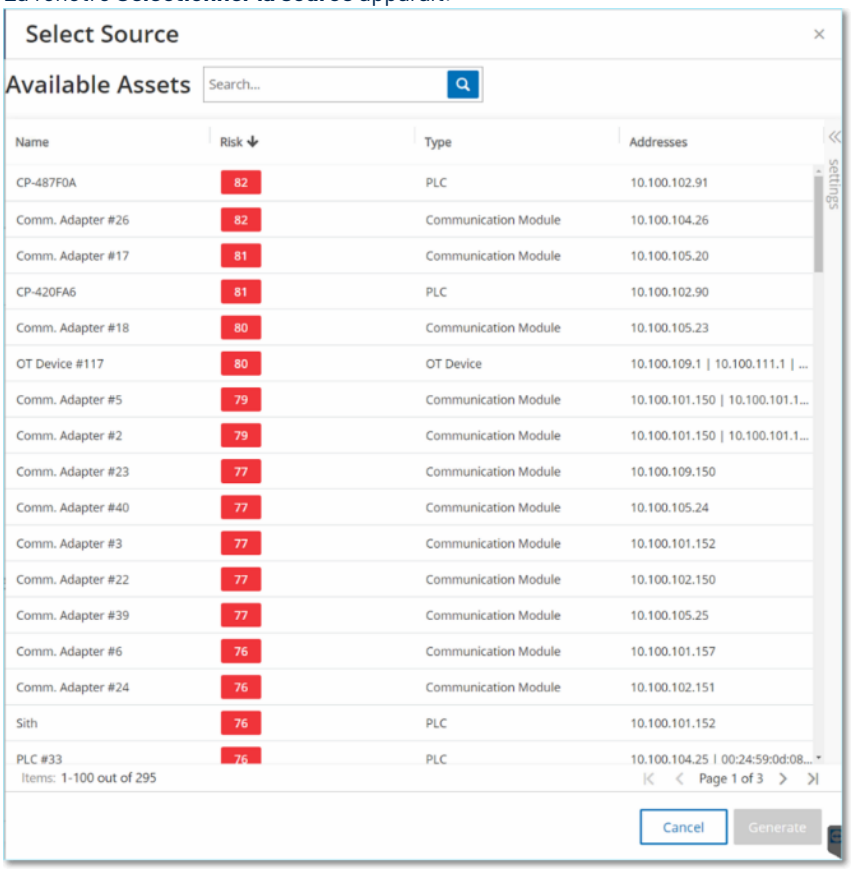

Le vecteur d'attaque est généré automatiquement et apparaît dans l'onglet **Vecteur d'attaque**.

### Pour générer un vecteur d'attaque manuel :

1. Accédez à la page **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.



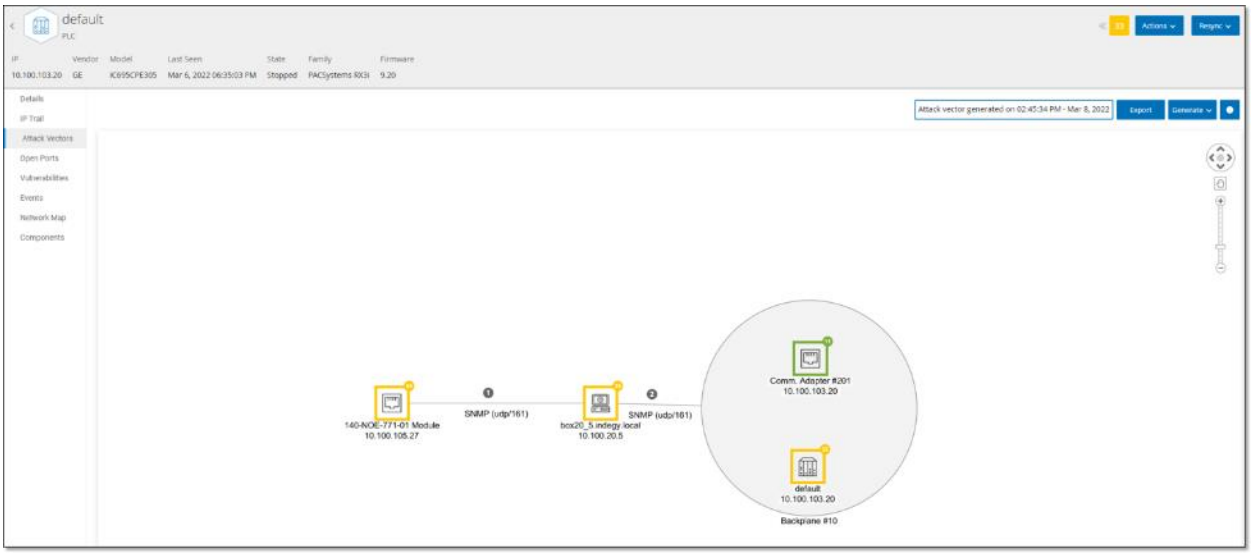
La fenêtre **Sélectionner la source** apparaît.




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

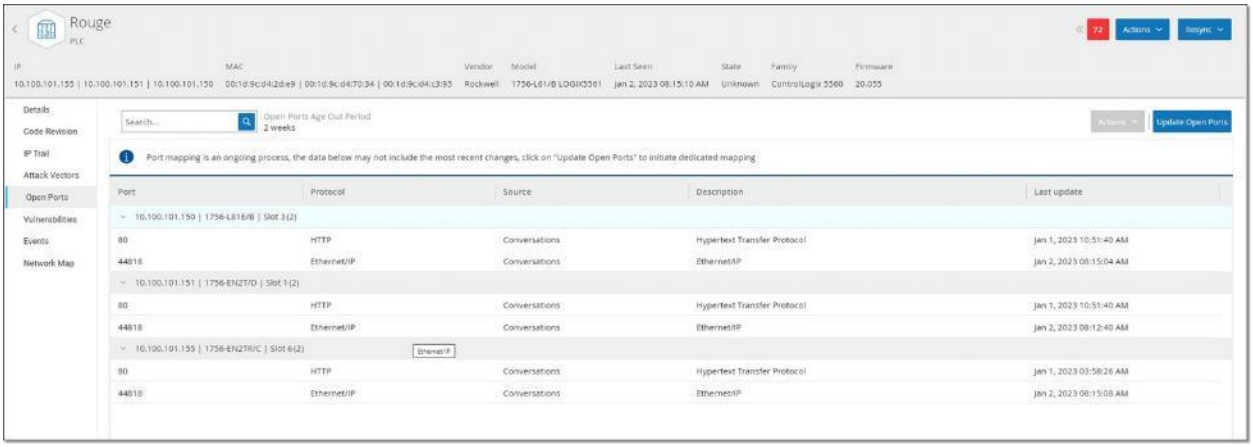



L'onglet **Vecteurs d'attaque** affiche un diagramme du vecteur d'attaque généré le plus récemment pour l'asset cible spécifié. La case à côté du bouton Générer indique la date et l'heure auxquelles le vecteur d'attaque affiché a été généré. Le diagramme Vecteur d'attaque comprend les éléments suivants :

- 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.

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, NNM ou scans Nessus) qui indique que le port est ouvert. Une liste distincte des ports ouverts apparaît pour chaque IP disponible pour l'asset (y compris les ports accessibles via un fond de panier partagé). Cliquez sur la flèche à côté d'une adresse IP pour développer la liste et afficher ses ports ouverts.

Il y a une **période d'expiration automatique des ports ouverts**, après laquelle une liste de ports ouverts sera automatiquement supprimée de la liste si aucune autre indication n'a été reçue que le port est toujours ouvert. La durée par défaut est de deux semaines. Pour ajuster la durée de la période d'expiration des ports ouverts, voir **Appareil**.

Les paramètres de scan des ports ouverts sont configurés dans l'onglet **Paramètres locaux**. Voir **Toutes les requêtes de contrôleur**. Vous pouvez également exécuter une requête manuelle de l'asset sélectionné pour mettre à jour la liste des ports ouverts.

### Pour mettre à jour manuellement la liste des ports ouverts :

1. Sur l'écran **Inventaire > Contrôleurs/Assets réseau**, sélectionnez l'asset souhaité.
   L'écran **Détails de l'asset** apparaît.
2. Cliquez sur l'onglet **Ports ouverts**.
3. Dans le coin supérieur droit du volet Ports ouverts, cliquez sur **Mettre à jour les ports ouverts**.
   Un nouveau scan est exécuté, mettant à jour les ports ouverts affichés pour ce contrôleur.

## Actions supplémentaires dans l'onglet Ports ouverts

Dans l'onglet Ports ouverts d'un asset spécifique, vous pouvez effectuer les actions supplémentaires suivantes pour un port ouvert spécifique.

- Scanner – Lance un scan du port sélectionné.
- Afficher – Affiche des détails et des diagnostics supplémentaires sur l'appareil en accédant à l'interface web de l'appareil.

### Pour lancer un scan sur un port spécifique :

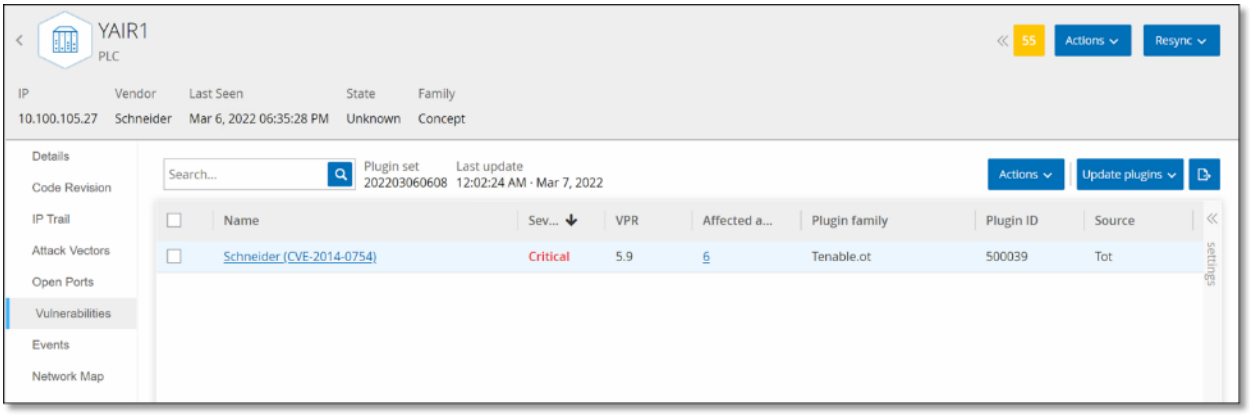
1. Sur l'écran **Inventaire > Contrôleurs/Assets réseau**, sélectionnez l'asset souhaité.
   L'écran **Détails de l'asset** apparaît.
2. Cliquez sur l'onglet **Ports ouverts**.
3. Sélectionnez un port spécifique.
4. Cliquez sur le menu **Actions**.
5. Dans le menu déroulant, sélectionnez **Scanner**.
   Tenable.ot exécute un scan sur le port sélectionné.

### Pour afficher le portail de l'asset :

Cette option n'est disponible que lorsque le port 80 (utilisé pour l'accès au Web) est l'un des ports ouverts.

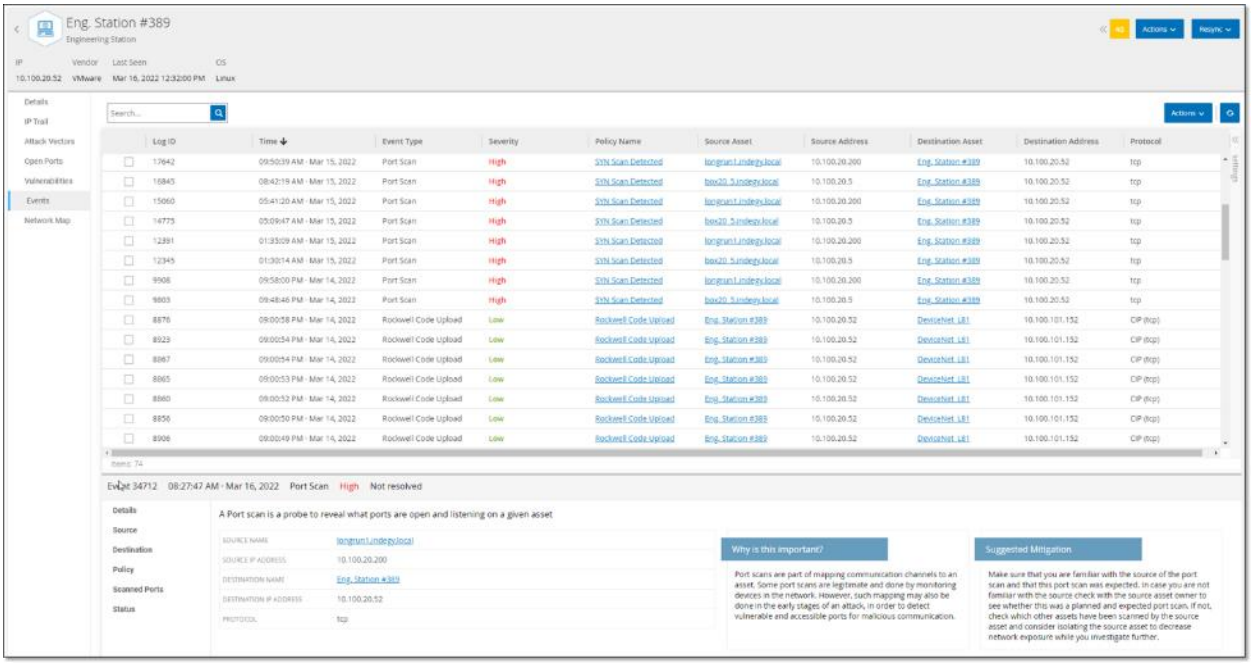
1. Sur l'écran **Inventaire > Contrôleurs/Assets réseau**, sélectionnez l'asset souhaité.
   L'écran **Détails de l'asset** apparaît.
2. Cliquez sur l'onglet **Ports ouverts**.
3. Sélectionnez un port spécifique.
4. Cliquez sur le menu **Actions**.
5. Dans le menu déroulant, sélectionnez **Afficher**.
   Un nouvel onglet de navigateur s'ouvre et affiche le portail de cet asset.

## Vulnérabilités




L'onglet **Vulnérabilités** affiche une liste de toutes les vulnérabilités qui affectent l'asset spécifié, telles qu'elles sont détectées par les plug-ins Tenable.ot. 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. Chaque liste affiche des détails sur la nature de la menace et sa sévérité. Les informations affichées dans cet onglet sont **identiques aux informations affichées sur l'écran Risque > Vulnérabilités**, mais seuls les événements pertinents pour l'asset spécifié sont affichés ici. Pour une explication des informations sur les vulnérabilités, voir **Vulnérabilités**.

## Événements




L'onglet **Événements** affiche une liste détaillée des événements du réseau impliquant l'asset, tels que détectés par les plugins Tenable.ot. 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 **Utilisation des listes**.

Le bas de l'écran affiche des informations détaillées sur l'événement sélectionné, divisées en onglets. Seuls les onglets correspondant au type de l'événement sélectionné sont affichés. Pour plus d'informations sur les événements, voir **Événements**.

Un bouton **Actions** en haut du volet vous permet d'effectuer l'action suivante sur le ou les événements sélectionnés :

- Résoudre – Marque cet événement comme résolu.
- Télécharger PCAP – Télécharge le fichier PCAP pour cet événement.
- Exclure – 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 :<br>Aucun – Aucune raison de s'inquiéter.<br>**Info** – Aucune raison de s'inquiéter dans l'immédiat. À vérifier au moment opportun.<br>**Avertissement** – Risque modéré qu'une activité potentiellement dangereuse se soit produite. À traiter au moment opportun.<br>**Critique** – Risque élevé qu'une activité potentiellement dangereuse se soit produite. À traiter immédiatement. |
| **Nom de la politique** | Le nom de la politique qui a généré l'événement. Le nom est un lien vers la liste de politiques. |
| **Asset source** | Le nom de l'asset qui a lancé l'événement. Ce champ est un lien vers les listes d'assets. |
| **Adresse source** | L'adresse IP ou MAC de l'asset qui a lancé l'événement. |
| **Asset cible** | Le nom de l'asset qui a été affecté par l'événement. Ce champ est un lien vers les listes d'assets. |
| **Adresse cible** | L'adresse IP ou MAC de l'asset qui a été affecté par l'événement. |
| **Protocole** | Lorsque c'est pertinent, montre le protocole utilisé pour la communication qui a généré cet événement. |

| Paramètre | Description |
|---|---|
| **Catégorie d'événement** | Affiche la catégorie générale de l'événement.<br>**Remarque :** sur l'écran Tous les événements, les événements de tous les types sont affichés. Chaque écran d'événement affiche uniquement les événements de la catégorie spécifiée.<br>Voici une brève explication des catégories d'événements (pour une explication plus détaillée, voir **Catégories**) :<br>• Événements de configuration – Cela comprend deux sous-catégories<br>• Événements de validation du contrôleur – Ces politiques concernent les changements ayant lieu au sein des contrôleurs du réseau.<br>• 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).<br>• Événements SCADA – Ces politiques identifient les modifications apportées au plan de données des contrôleurs.<br>• Événements de menaces réseau – Ces politiques identifient le trafic réseau qui indique des menaces d'intrusion.<br>• 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

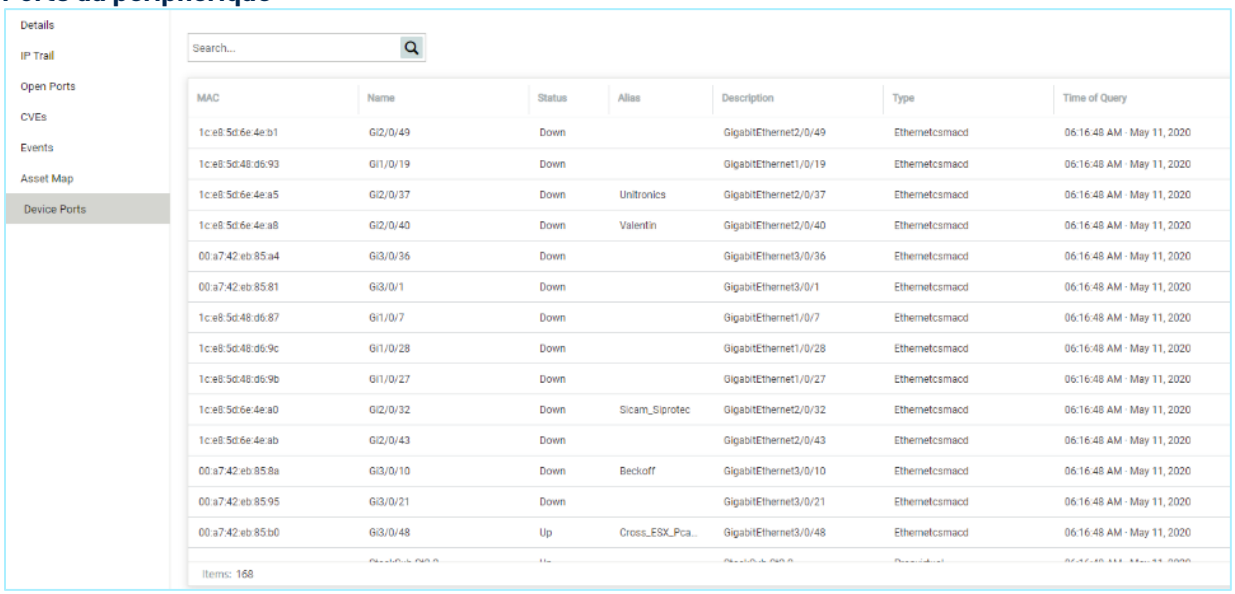
L'onglet **Cartographie du réseau** affiche une représentation graphique des connexions réseau de l'asset. Cette vue affiche toutes les connexions établies par l'asset sélectionné au cours des 30 derniers jours.

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** apparaît pour les commutateurs réseau. Il affiche des informations détaillées sur les ports du commutateur réseau. Ces données sont collectées à l'aide de requêtes SNMP adressées au commutateur. Pour chaque port, les informations suivantes sont affichées : l'adresse *MAC*, le *nom*, le *statut* de la connexion (actif ou inactif), l'*alias* et la *description*.

Cet onglet n'est disponible que s'il a été activé pour votre compte. Pour activer cette fonctionnalité, contactez votre agent d'assistance.

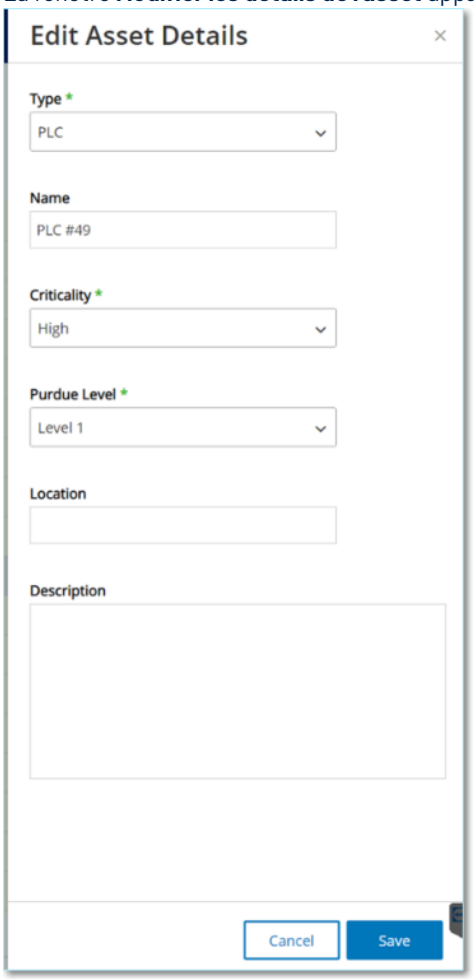
# Modification des détails d'un asset

Tenable.ot 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.

## Modification des 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 le champ **Type**, sélectionnez le type d'asset dans la liste déroulante.
6. Dans le champ **Nom**, saisissez un nom par lequel l'asset sera identifié dans l'interface utilisateur Tenable.ot.
7. Dans le champ **Criticité**, saisissez le niveau de criticité de cet asset pour le système.
8. Dans le champ **Niveau Purdue**, saisissez le niveau Purdue en fonction du type d'asset.
9. Dans le champ **Fond de panier** (pour les contrôleurs), saisissez le nom du fond de panier sur lequel l'asset est installé.

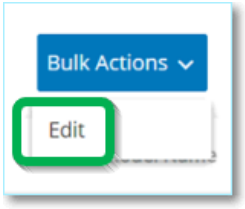
10. Dans le champ **Localisation**, saisissez une description de l'emplacement de l'asset. Ce champ n'est pas obligatoire. Les données sont affichées dans le tableau des assets ainsi que sur l'écran Détails de l'asset.
11. Dans le champ **Description**, saisissez une description de l'asset. Ce champ n'est pas obligatoire. Les données sont affichées sur l'écran Détails de l'asset.
12. Cliquez sur **Enregistrer**.
    Les détails modifiés sont enregistrés pour cet asset.

### 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.

> Vous pouvez également sélectionner plusieurs assets en appuyant sur la **touche Maj** tout en cliquant sur chacun des assets souhaités.

3. Cliquez sur le menu **Actions en bloc** et sélectionnez **Modifier** dans la liste déroulante.




L'écran **Modifier en bloc** apparaît avec les paramètres disponibles pour la modification en bloc.

4. Cochez la case à côté de chacun des paramètres que vous souhaitez modifier (*Type*, *Criticité*, *Niveau Purdue*, *Segments réseau*, *Localisation* et *Description*).

> 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 devrez modifier chaque élément manuellement.

5. Réglez chaque paramètre selon vos besoins.

> 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 de ce paramètre seront effacées.

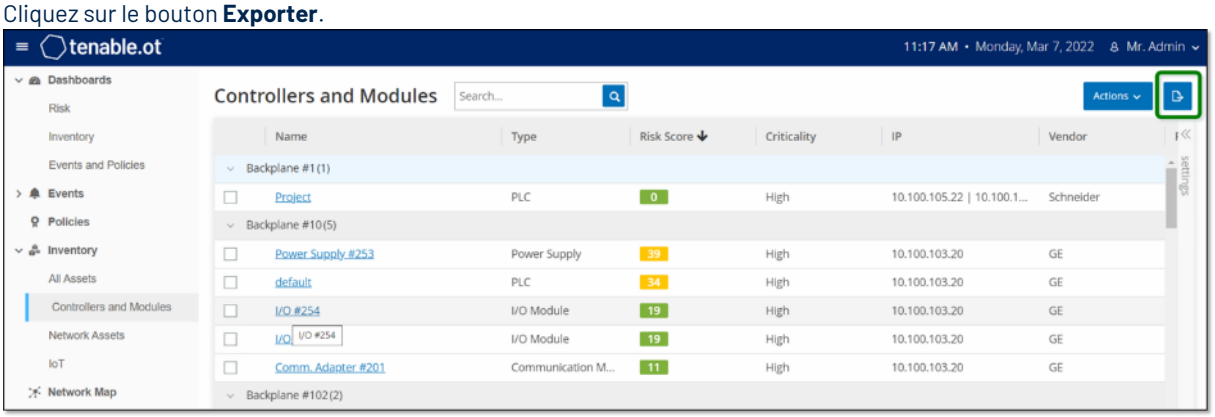
6. Cliquez sur **Enregistrer**.
   Les assets sont enregistrés avec la nouvelle configuration.

### Modification des détails d'un asset en téléchargeant un fichier CSV

Cette méthode de modification des détails des assets vous permet d'en modifier un grand nombre grâce à un fichier CSV, plutôt que de les modifier manuellement dans l'interface utilisateur. Les détails suivants peuvent être modifiés à l'aide de cette méthode : *Type*, *Nom*, *Criticité*, *Niveau Purdue*, *Localisation*, *Description* et tous les champs personnalisés.

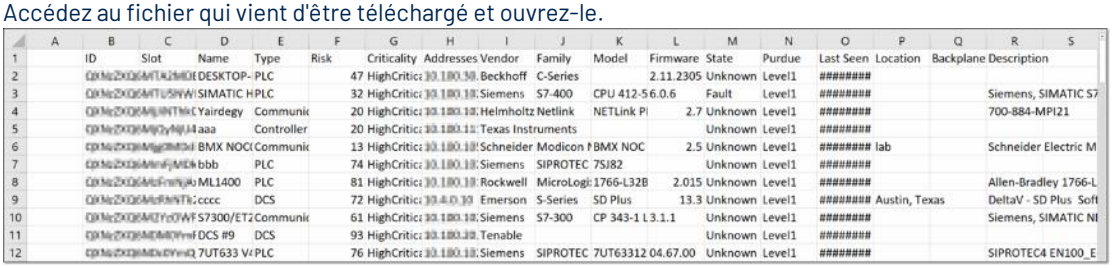
#### Pour modifier les détails d'un élément via un fichier CSV :

1. Sous **Inventaire**, cliquez sur **Tous les assets**, **Contrôleurs** et **Modules** ou **Assets réseau**.
2. Cliquez sur le bouton **Exporter**.




Un fichier CSV de l'inventaire est téléchargé.

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



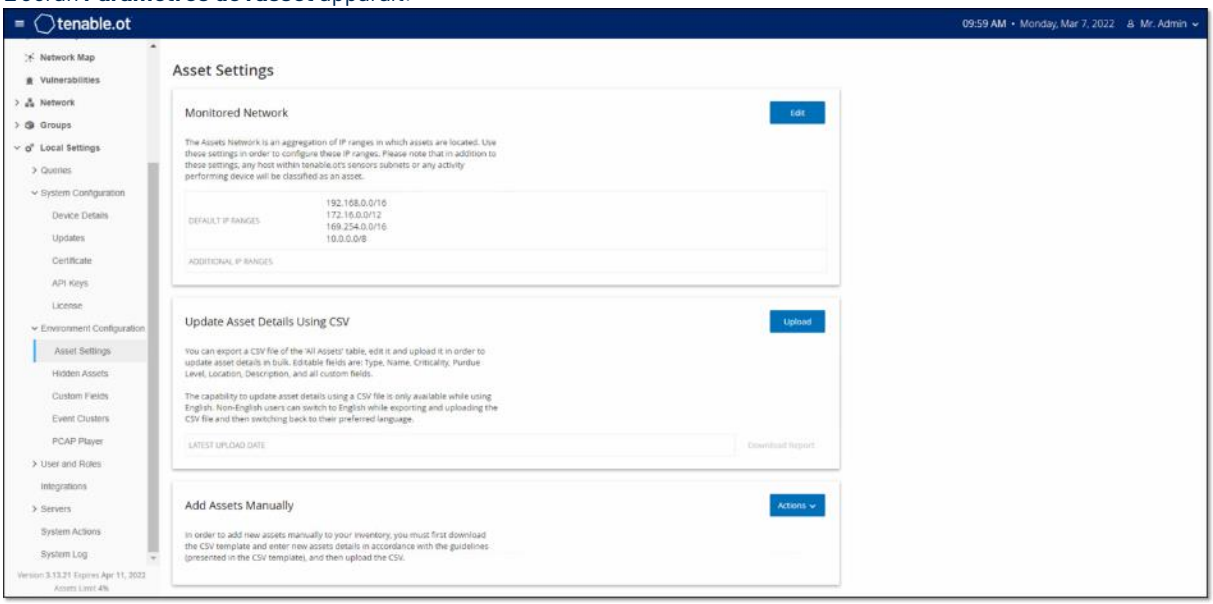

4. Modifiez les paramètres autorisés en modifiant le contenu des cellules. Les paramètres autorisés sont : *Type*, *Nom*, *Criticité*, *Niveau Purdue*, *Localisation*, *Description* et les champs personnalisés.

> 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.

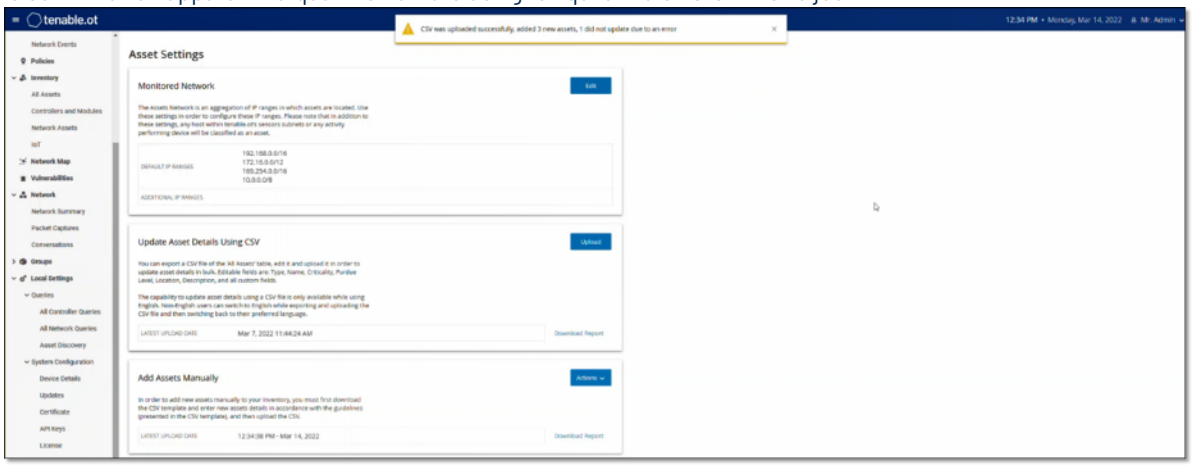
5. Enregistrez le fichier au format CSV.

> Seuls les assets que vous modifiez seront mis à jour dans le système. Les assets qui ne sont pas inclus dans le fichier CSV ou les lignes que vous n'avez pas modifiées resteront inchangés dans le système. Il n'est pas possible de supprimer des assets à l'aide de cette méthode.

6. Sous **Paramètres locaux**, accédez à **Configuration de l'environnement** > **Paramètres de l'asset**.
   L'écran **Paramètres de l'asset** apparaît.




7. Dans la section **Mettre à jour les détails d'un asset à l'aide d'un fichier CSV**, cliquez sur **Charger**.
8. Suivez les invites de navigation de votre appareil pour charger le fichier CSV que vous venez d'enregistrer.
   Une confirmation apparaît indiquant le nombre de lignes qui ont bien été 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**.
   Un fichier CSV est téléchargé. Il détaille les identifiants d'assets qui ont bien été mis à jour et ceux dont la modification 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.

Un asset qui était masqué peut être restauré à partir de l'écran **Paramètres locaux** > **Assets** > **Assets masqués**, voir **Paramètres locaux**.

### Pour masquer un ou plusieurs assets :

1. Sous **Inventaire**, cliquez sur **Contrôleurs** ou **Assets réseau**.
2. Cochez la case à côté d'un ou plusieurs assets que vous souhaitez supprimer.
3. Cliquez sur le bouton **Actions** dans la barre d'en-tête.
4. Dans le menu déroulant, sélectionnez **Masquer l'asset**.
   La fenêtre **Assets masqués** apparaît.
5. Dans le champ **Commentaires**, vous pouvez ajouter des commentaires en texte libre sur le ou les assets. (Facultatif)

> Les commentaires sont affichés dans la liste des assets supprimés, sur l'écran **Paramètres locaux** > **Assets** > **Assets masqués**.

6. Cliquez sur **Masquer**.
   Le ou les assets sont masqués dans l'inventaire et les groupes.

# Exécution d'un scan Nessus spécifique à un asset

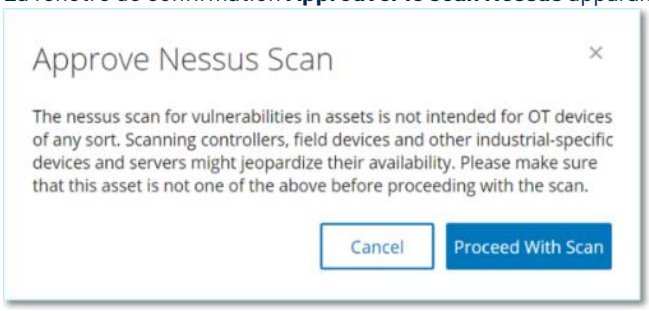
Nessus est un outil Tenable qui scanne les appareils informatiques pour détecter les vulnérabilités. Tenable.ot vous permet d'exécuter le « Basic Network Scan » (Scan réseau de base) de Nessus sur des assets informatiques spécifiques au sein de votre réseau OT. Il s'agit d'un scan actif de l'ensemble du système qui rassemble des informations supplémentaires à propos des vulnérabilités sur les serveurs et les appareils réseau. Cet scan utilisera les informations d'identification WMI et SNMP si elles ont été fournies par l'utilisateur. Cette action n'est disponible que pour les machines PC concernées. Les résultats du scan sont affichés sur l'écran **Vulnérabilités**. Vous pouvez également créer des scans personnalisés pour exécuter un ensemble spécifique de plug-ins Nessus sur un ensemble particulier d'assets réseau, voir **Scans de plug-ins Nessus**.

> Nessus est un outil invasif qui fonctionne mieux dans les environnements informatiques. Il n'est pas recommandé de l'utiliser sur les appareils OT, car cela peut interférer avec leur fonctionnement habituel.

### Pour exécuter manuellement un scan Nessus :

1. Sous **Inventaire**, cliquez sur **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 **Scan Nessus**.
   La fenêtre de confirmation **Approuver le scan Nessus** apparaît.




5. Cliquez sur **Procéder au scan**.
   Le scan Nessus est exécuté.

# Exécution d'une resynchronisation

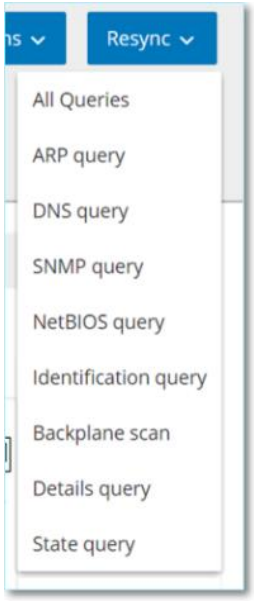
La fonction Resynchroniser lance une ou plusieurs requêtes au réseau et au contrôleur afin de capturer des informations à jour pour cet asset. Vous pouvez exécuter toutes les requêtes disponibles ou vous pouvez sélectionner des requêtes spécifiques à exécuter. Voici les requêtes disponibles pour la fonction « 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**, qui se trouve sur l'écran **Assets > Contrôleurs**.
- **Requête d'identification** – Utilise plusieurs protocoles pour tenter d'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, Pas de configuration et Test).
- **ARP** – Récupère l'adresse MAC des nouvelles IP détectées sur le réseau. Le résultat apparaît dans le champ **MAC**, qui se trouve sur l'écran **Détails > Vue d'ensemble**.

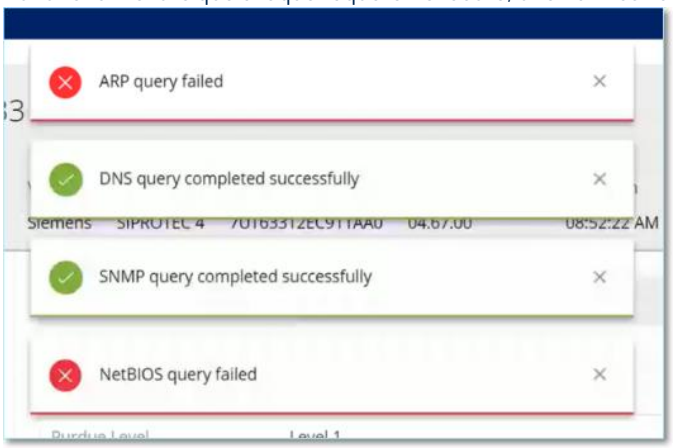
### ➡ Pour resynchroniser les données d'un asset :

1. Sur l'écran **Détails de l'asset** souhaité, cliquez sur le bouton **Resynchroniser** dans le volet d'en-tête.

2. Une liste déroulante de requêtes apparaît.




3. Cliquez sur la requête que vous souhaitez exécuter OU cliquez sur *Toutes les requêtes* pour exécuter toutes les requêtes disponibles.
4. Au fur et à mesure que chaque requête s'exécute, une notification contextuelle affiche son statut.



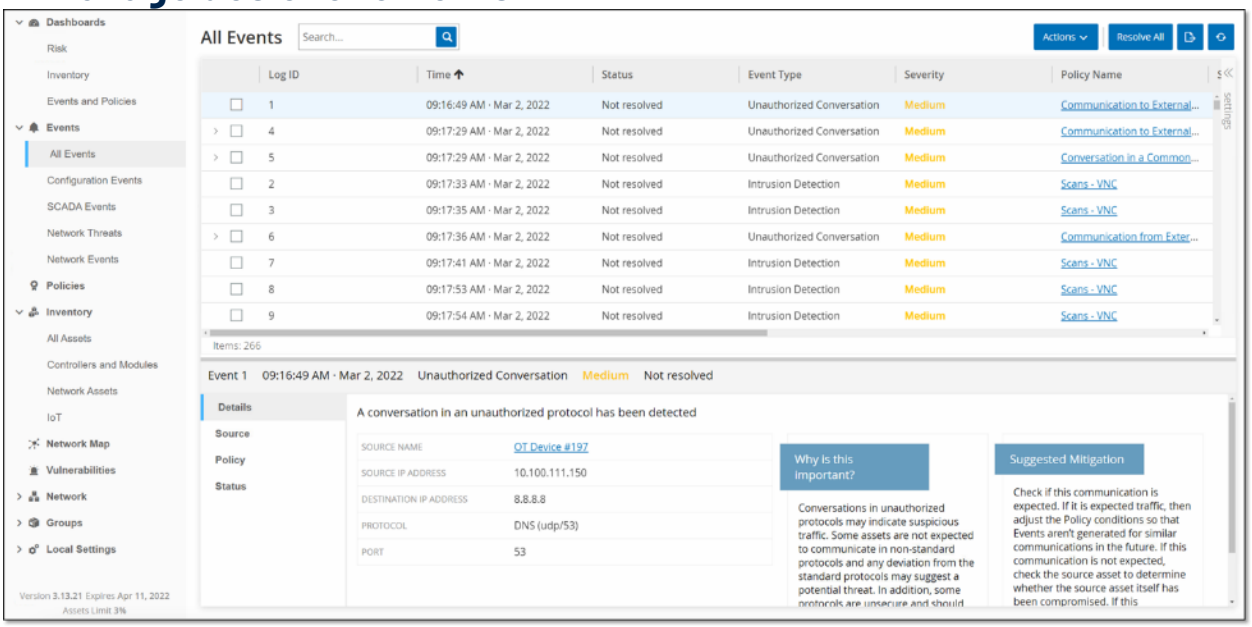

Pour chaque requête exécutée avec succès, les données système de cet asset sont mises à jour en fonction des nouvelles données.

# Événements

Les événements sont des notifications qui ont été générées dans le système pour attirer l'attention sur une activité potentiellement dangereuse sur le réseau. Les événements sont générés par les politiques configurées dans le système dans l'une des catégories suivantes : *Événements de configuration*, *Événements SCADA*, *Événements de menaces réseau* ou *Événements réseau*. Un niveau de sévérité est attribué à chaque politique, indiquant la sévérité de l'événement.

Une fois qu'une politique a été activée, tout événement dans le système qui correspond aux conditions de la politique déclenchera un journal d'événement. Plusieurs événements ayant les mêmes caractéristiques sont regroupés en un seul cluster.

## Affichage des événements




Tous les événements qui se sont produits dans le système sont affichés sur l'écran **Tous les événements**. Des sous-ensembles spécifiques d'événements sont affichés sur des écrans distincts pour chacune des catégories d'événements suivantes : **Événements de configuration**, **Événements SCADA**, **Menaces réseau** et **Événements réseau**.

Le haut de l'écran affiche des listes pour chaque événement. Pour chacun des écrans d'événements (Événements de configuration, Événements SCADA, Menaces réseau et Événements réseau), 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 **Utilisation des listes**.

Un bouton **Actions** en haut de la barre d'en-tête vous permet d'effectuer l'action suivante sur le ou les événements sélectionnés :

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

Des informations détaillées sur ces actions sont données dans les sections suivantes.

Le bas de l'écran affiche des informations détaillées 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*.

Vous pouvez faire glisser le séparateur de panneau vers le haut ou vers le bas pour agrandir/réduire l'affichage du panneau inférieur.

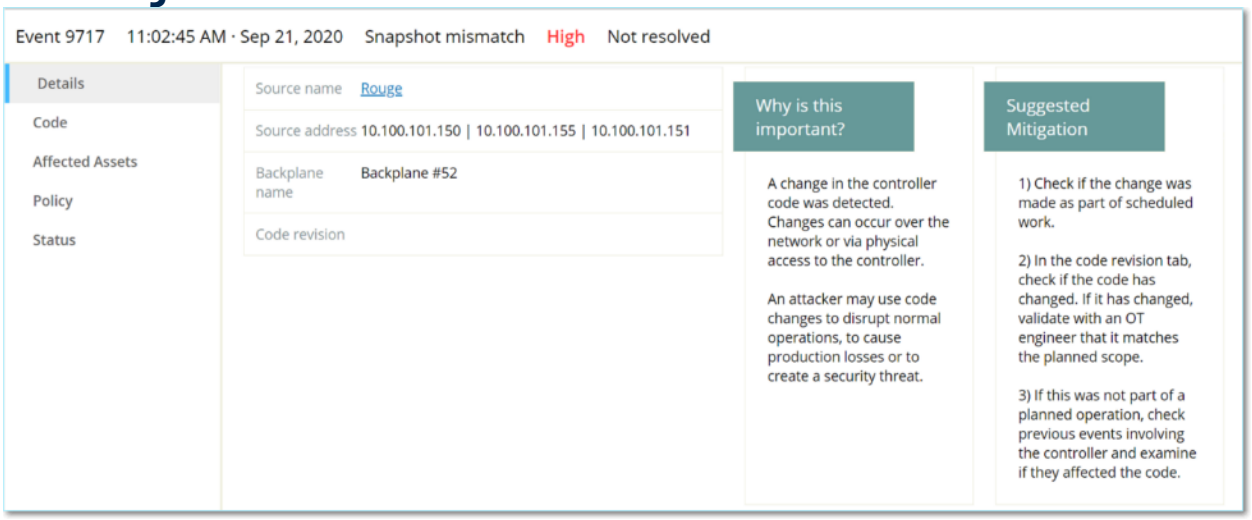
Vous pouvez télécharger le fichier de capture de paquets associé à chaque événement. Voir **Téléchargement de fichiers**.

Les informations affichées pour chaque liste d'événements sont décrites dans le tableau suivant :

| Paramètre | Description |
|---|---|
| **Nom** | Le nom de l'appareil sur le réseau. Cliquez sur le nom de l'asset pour afficher ses détails. voir **Affichage des détails d'un asset**. |
| **Adresses** | L'adresse IP et/ou MAC de l'asset.<br>**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 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** | La localisation de l'asset tel que saisi par l'utilisateur dans les détails de l'asset Tenable.ot. Voir **Modification des détails d'un asset**. |
| **Dernière détection** | La date et l'heure auxquelles l'appareil a été détecté pour la dernière fois par Tenable.ot. Il s'agit de la dernière fois que l'appareil s'est connecté au réseau ou a effectué une activité. |
| **OS** | Le système d'exploitation exécuté sur l'asset. |
| **Identifiant de journal** | Identifiant généré par le système pour faire référence à l'événement. |
| **Date/Heure** | La date et l'heure auxquelles l'événement s'est produit. |
| **Type d'événement** | Décrit le type d'activité qui a déclenché l'événement. Les événements sont générés par les politiques configurées dans le système. Pour une explication des différents types de politiques, voir **Types de politiques**. |

| Paramètre | Description |
|---|---|
| **Sévérité** | Affiche le niveau de sévérité de l'événement. Voici une explication des valeurs possibles :<br>Aucun – Aucune raison de s'inquiéter.<br>**Info** – Aucune raison de s'inquiéter dans l'immédiat. À vérifier au moment opportun.<br>**Avertissement** – Risque modéré qu'une activité potentiellement dangereuse se soit produite. À traiter au moment opportun.<br>**Critique** – Risque élevé qu'une activité potentiellement dangereuse se soit produite. À traiter immédiatement. |
| **Nom de la politique** | Le nom de la politique qui a généré l'événement. Le nom est un lien vers la liste de politiques. |
| **Asset source** | Le nom de l'asset qui a lancé l'événement. Ce champ est un lien vers les listes d'assets. |
| **Adresse source** | L'adresse IP ou MAC de l'asset qui a lancé l'événement. |
| **Asset cible** | Le nom de l'asset qui a été affecté par l'événement. Ce champ est un lien vers les listes d'assets. |
| **Adresse cible** | L'adresse IP ou MAC de l'asset qui a été affecté par l'événement. |
| **Protocole** | Lorsque c'est pertinent, montre le protocole utilisé pour la communication qui a généré cet événement. |
| **Catégorie d'événement** | Affiche la catégorie générale de l'événement.<br>**Remarque :** sur l'écran Tous les événements, les événements de tous les types sont affichés. Chaque écran d'événement affiche uniquement les événements de la catégorie spécifiée.<br>Voici une brève explication des catégories d'événements (pour une explication plus détaillée, voir **Catégories**) :<br>• Événements de configuration – Cela comprend deux sous-catégories.<br>• Événements de validation du contrôleur – Ces politiques concernent les changements ayant lieu au sein des contrôleurs du réseau.<br>• 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).<br>• Événements SCADA – Ces politiques identifient les modifications apportées au plan de données des contrôleurs.<br>• Événements de menaces réseau – Ces politiques identifient le trafic réseau qui indique des menaces d'intrusion.<br>• Événements réseau – Ces politiques concernent les assets du réseau et les flux de communication entre les assets. |
| **Statut** | Indique si l'événement a été marqué comme résolu ou non. |
| **Résolu par** | Pour les événements résolus, indique quel utilisateur a marqué l'événement comme résolu. |
| **Résolu le** | Pour les événements résolus, indique quand l'événement a été marqué comme résolu. |
| **Commentaire** | Affiche tous les commentaires qui ont été ajoutés lorsque l'événement a été résolu. |

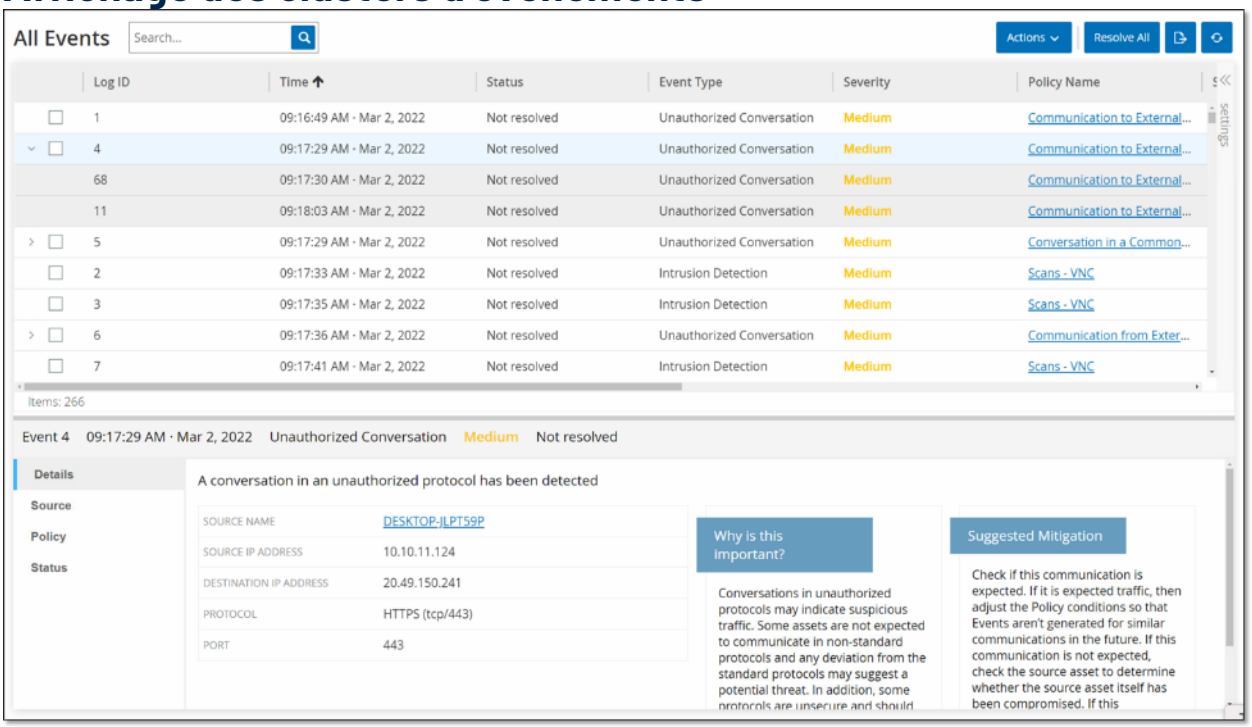
# Affichage des détails d'un événement




Le bas de l'écran 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 scannés.
- **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 **Clusters 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.

# Résolution d'événements

Une fois qu'un technicien autorisé a évalué un événement et pris les mesures nécessaires pour résoudre le problème, ou déterminé qu'il n'y a pas lieu d'agir, l'événement doit être marqué comme *Résolu*. Lorsqu'un événement faisant partie d'un cluster est résolu, tous les événements de ce cluster sont marqués comme résolus. Il est possible de sélectionner plusieurs événements à marquer comme résolus. Il est également possible de marquer tous les événements (ou tous les événements d'une catégorie donnée) comme résolus en une seule action.

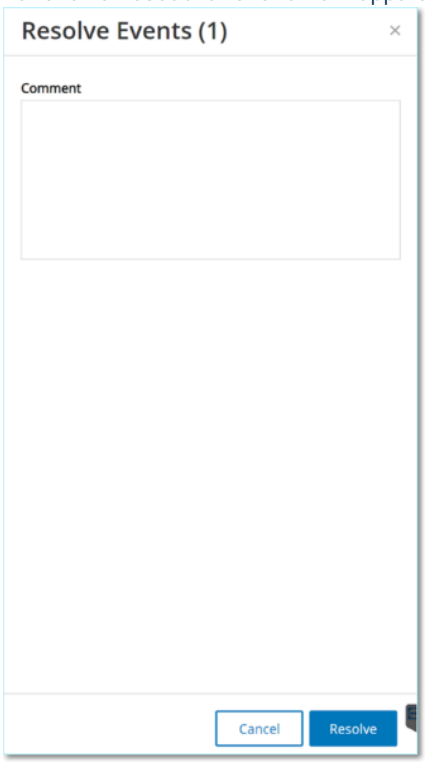
## Résolution d'événements individuels

### ➡ Pour marquer des événements spécifiques comme résolus :

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

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

3. Dans le menu déroulant, sélectionnez **Résoudre**.
   La fenêtre **Résoudre l'événement** apparaît.



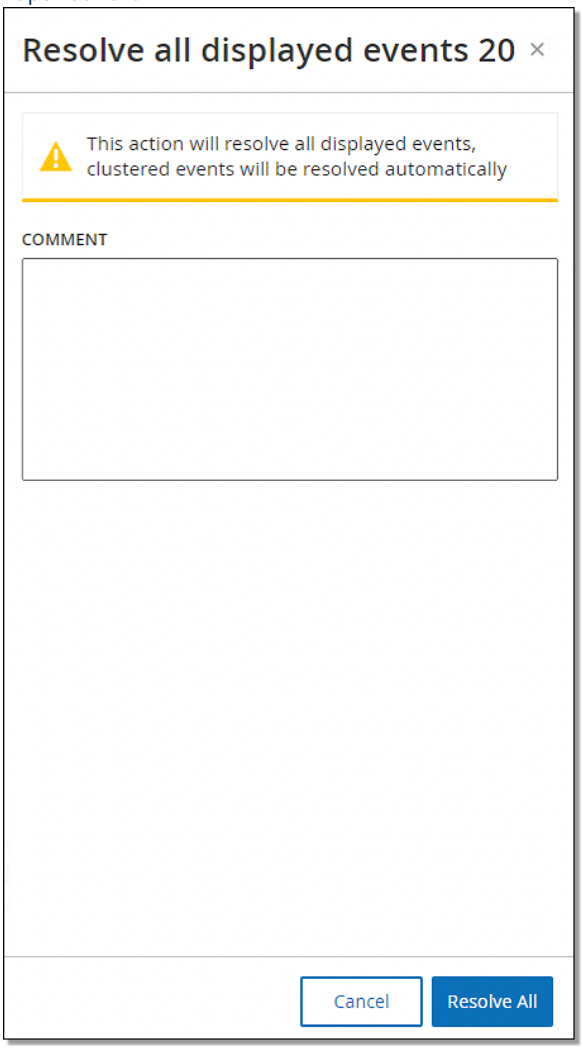

4. Dans le champ **Commentaire**, vous pouvez ajouter un commentaire décrivant les mesures d'atténuation prises pour résoudre le ou les problèmes (champ facultatif).
5. Cliquez sur **Résoudre**.
   Le statut du ou des événements sélectionnés est marqué comme *Résolu*.

### Résolution de tous les événements

L'action **Tout résoudre** s'applique à tous les événements de l'écran en cours (par exemple, si l'écran Événements de configuration est ouvert, alors l'option Tout résoudre permet de résoudre les événements de configuration, mais pas les événements SCADA, etc.) en fonction des filtres actuellement appliqués à l'affichage. Pour les événements en cluster, tous les événements du cluster sont marqués comme résolus.

### Pour marquer tous les événements comme résolus :

1. Sur l'écran **Événements** pertinent (Événements de configuration, Événements SCADA, Événements de menaces réseau ou Événements réseau), dans la barre d'en-tête, cliquez sur **Tout résoudre**.
2. La fenêtre **Résoudre tous les événements** apparaît avec le nombre d'événements à résoudre dans le coin supérieur droit.




3. Dans le champ **Commentaire**, vous pouvez ajouter un commentaire sur le groupe d'événements en cours de résolution (champ facultatif).
4. Cliquez sur **Résoudre**.
   Le message d'avertissement apparaît.
5. Cliquez sur **Résoudre**.
   Tous les événements de l'affichage en cours sont marqués comme résolus.

# Création d'exclusions de politique

Si vous constatez qu'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 de travail, 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.

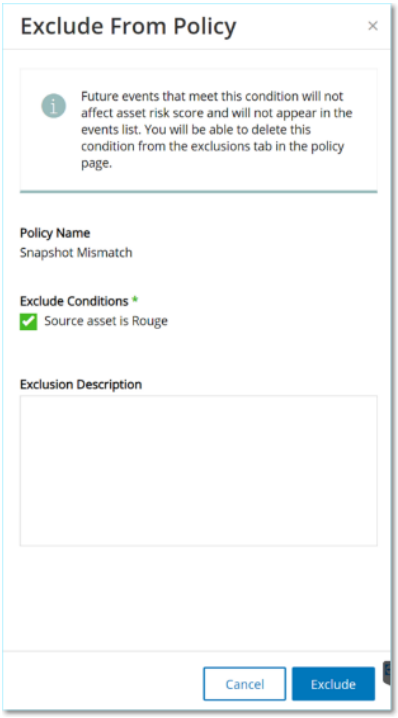
Les exclusions sont créées à partir de l'écran Événements, en fonction des événements qui ont été générés par vos politiques. Vous pouvez spécifier les conditions d'un événement spécifique que vous souhaitez exclure de la politique.

Si vous souhaitez reprendre la génération d'événements pour les conditions spécifiées ultérieurement, vous pouvez supprimer l'exclusion, voir **Suppression d'exclusions de politique**.

### Pour créer une exclusion de politique :

1. Sur l'écran **Événements** pertinent (Événements de configuration, Événements SCADA, Événements de menaces réseau ou Événements réseau), sélectionnez l'événement pour lequel vous souhaitez créer une exclusion.
2. Cliquez sur le bouton **Actions** dans la barre d'en-tête (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 (ce qui entraîne l'exclusion des événements avec l'*une* des conditions spécifiées de la politique). Vous pouvez **décocher** la case à côté de chaque condition pour laquelle vous souhaitez continuer à générer des événements.

Par exemple, dans la boîte de dialogue ci-dessous, si vous souhaitez exclure les assets et IP sources et cibles spécifiés de cette politique, mais que vous souhaitez continuer à appliquer cette politique aux communications UDP entre les autres assets du réseau, vous devez désélectionner « Le protocole est UDP ».



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

5. Dans le champ **Description de l'exclusion**, vous pouvez ajouter un commentaire sur l'exclusion (facultatif).
6. Cliquez sur **Exclure**.
   L'exclusion est créée.

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 (i.e. Activities) (Événements de configuration (Activités)) | • Asset source<br>• IP source<br>• Asset cible<br>• 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<br>• Identifiant du périphérique USB |
| | IP conflict (Conflit IP) | • Adresses MAC<br>• Adresse IP |
| | Network Baseline Deviation (Déviation par rapport à la base de référence réseau) | • Asset source<br>• IP source<br>• Asset cible<br>• IP cible<br>• Protocole |
| | Open Port (Port ouvert) | • Asset source<br>• IP source<br>• Port |
| | RDP Connection (Connexion RDP) | • Asset source<br>• IP source |

| Catégorie de politique | Type d'événement | Conditions d'exclusion |
|---|---|---|
| | | • Asset cible<br>• IP cible |
| | Unauthorized conversation (Communication non autorisée) | • Asset source<br>• IP source<br>• Asset cible<br>• IP cible<br>• Protocole |
| | FTP Log In (Failed and Successful) (Connexion FTP (échec et réussite)) | • Asset source<br>• IP source<br>• Asset cible<br>• IP cible |
| | Telnet Log In (Attempt, Failed and Successful) (Connexion Telnet (tentative, échec et réussite)) | • Asset source<br>• IP source<br>• Asset cible<br>• IP cible |
| **Menace réseau** | Intrusion Detection (Détection d'intrusion) | • Asset source<br>• IP source<br>• Asset cible<br>• IP cible<br>• SID |
| | ARP Scan (Scan ARP) | • Asset source<br>• IP source |
| | Port scan (Scan des ports) | • Asset source<br>• IP source |
| **SCADA** | Modbus illegal data address (Adresse de données Modbus non valide) | • Asset source<br>• IP source<br>• Asset cible<br>• IP cible |
| | Modbus illegal data value (Valeur de données Modbus non valide) | • Asset source<br>• IP source<br>• Asset cible<br>• IP cible |
| | Modbus illegal function (Fonction Modbus non valide) | • Asset source<br>• IP source<br>• Asset cible<br>• IP cible |

| Catégorie de politique | Type d'événement | Conditions d'exclusion |
|---|---|---|
| | Unauthorized write (Écriture non autorisée) | • Asset source<br>• Asset cible<br>• Nom du tag |
| | CEI60870-5-104 StartDT<br>CEI60870-5-104 StopDT | • Asset source<br>• IP source<br>• Asset cible<br>• IP cible |
| | IEC60870-5-104 function code based events (Événements basés sur le code de fonction CEI60870-5-104) | • Asset source<br>• IP source<br>• Asset cible<br>• IP cible<br>• COT |
| | DNP3 events (Événements DNP3) | • Asset source<br>• IP source<br>• Asset cible<br>• IP cible<br>• Adresse DNP3 source<br>• Adresse DNP3 cible |

# Téléchargement de fichiers de capture individuels

Tenable.ot stocke les données de capture de paquets associées à chaque événement du réseau. Les données sont stockées sous forme de fichiers PCAP qui peuvent être téléchargés et analysés à l'aide d'outils d'analyse de protocole réseau (par exemple Wireshark, etc.). Cette section explique comment télécharger le fichier PCAP associé à un événement particulier. Vous pouvez également télécharger des fichiers PCAP pour l'ensemble du réseau. Voir **Captures de paquets**.

Les fichiers PCAP ne sont disponibles que si la fonction Capture de paquets est activée. La fonction Capture de Paquets peut être activée à partir de l'écran **Paramètres locaux** > **Configuration système** > **Capture 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.

### Téléchargement d'un fichier PCAP

**Pour télécharger un fichier PCAP :**

1. Sur l'écran **Événements**, cochez la case à côté de l'événement pour lequel vous souhaitez télécharger le fichier PCAP.
2. Cliquez sur le bouton **Actions** dans la barre d'en-tête.
3. Dans le menu déroulant, sélectionnez **Télécharger le fichier de capture**.
   Le fichier PCAP compressé est téléchargé sur votre ordinateur local.

# Création de politiques FortiGate

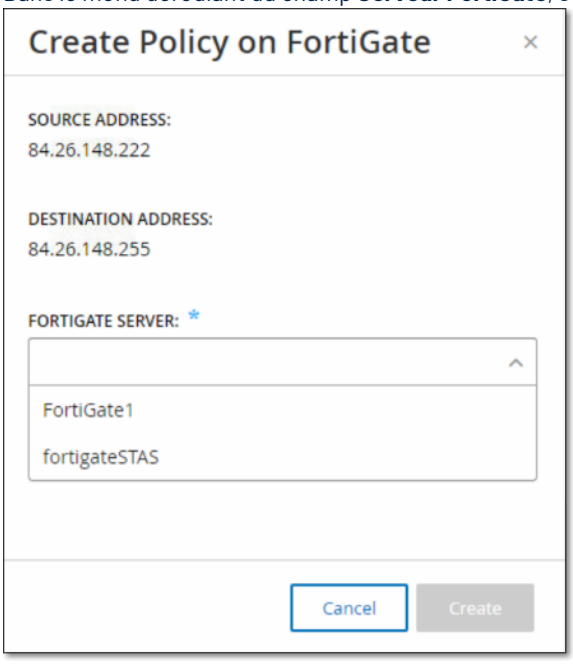
L'intégration FortiGate vous permet d'utiliser certains événements Tenable.ot pour créer des politiques/règles de pare-feu dans le pare-feu FortiGate nouvelle génération. Les types d'événements qui autorisent cette fonctionnalité (événements pris en charge) sont *Baseline Deviation* (Déviation par rapport 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 sera automatiquement configurée pour s'appliquer aux assets source et cible qui ont été impliqués dans l'événement Tenable.ot. Par défaut, la politique obligera 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 pouvoir suggérer des politiques FortiGate, vous devez configurer l'intégration de votre serveur de pare-feu FortiGate avec Tenable.ot. Voir **Pare-feu FortiGate**.

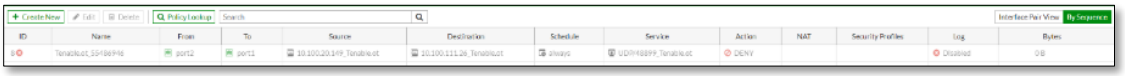
**Pour suggérer une politique FortiGate :**

1. Sur l'écran **Événements** pertinent (*Configuration Events* (Événements de configuration), *SCADA Events* (Événements SCADA), *Network Threats* ou *Network Events* (Événements de menaces réseau ou réseau), sélectionnez l'événement pour lequel vous souhaitez créer une politique FortiGate.
2. Cliquez sur le bouton **Actions** dans la barre d'en-tête (ou effectuez un clic droit sur l'événement).
3. Dans le menu déroulant, sélectionnez **Créer une politique FortiGate**.
   Le panneau **Créer une politique** sur FortiGate s'ouvre, avec l'**adresse source** et l'**adresse cible** des assets impliqués dans l'événement Tenable.ot déjà remplies.

4. Dans le menu déroulant du champ **Serveur FortiGate**, sélectionnez le serveur souhaité.




5. Cliquez sur **Créer**.
   La politique est créée dans FortiGate et le panneau se referme.
6. Vous pouvez consulter la nouvelle politique dans l'application FortiGate.



7. Un administrateur FortiGate peut ajuster les paramètres selon les besoins.

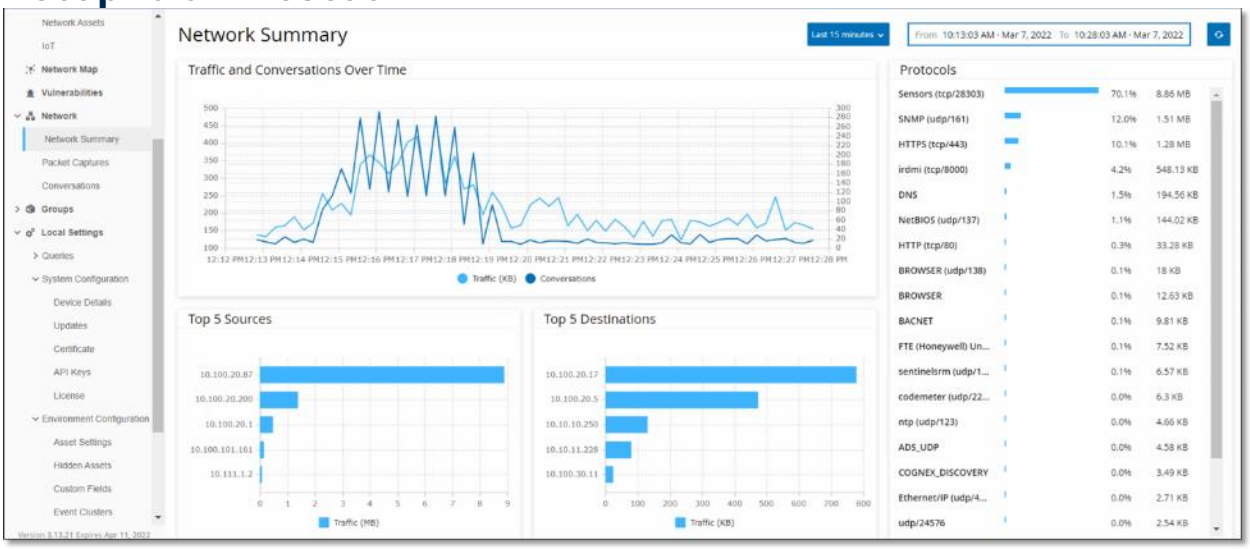
# Réseau

Tenable.ot surveille toutes les activités de votre réseau. Ces informations sont affichées dans la section **Réseau** de l'interface utilisateur.

Les données du réseau sont affichées sur trois écrans.

- **Récapitulatif réseau** – Affiche un aperçu du trafic réseau.
- **Captures de paquets** – Affiche une liste des fichiers PCAP capturés par le système.
- **Communications** – Affiche une liste de toutes les conversations detectees sur le reseau, avec des details sur la date/heure a laquelle elles se sont produites, les ressources impliquees, etc.

## Récapitulatif réseau




L'écran **Récapitulatif réseau** affiche des graphiques visuels qui résument l'activité du réseau. Vous pouvez définir la période pendant laquelle les données sont affichées. Vous pouvez également interagir avec les widgets pour afficher des détails supplémentaires.

L'écran comprend quatre widgets :

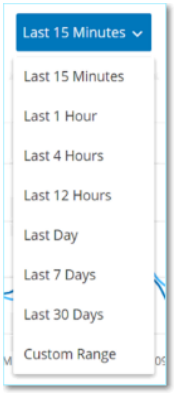
- **Trafic et communications au fil du temps** – Un graphique affichant la quantité de trafic en Go/Mo et le nombre de communications ayant lieu sur le réseau.
- **5 principales sources** – Un histogramme affichant les cinq assets source sous forme de colonnes qui ont lancé le plus d'activité sur le réseau. Pour chaque source, le graphique affiche des barres représentant la quantité de trafic. Lorsque vous survolez le graphique avec la souris, le nombre de communications apparaît dans une info-bulle.
- **5 principales cibles** – Un histogramme affichant les cinq assets cible sous forme de colonnes qui ont reçu le plus d'activité sur le réseau. Pour chaque cible, le graphique affiche des barres représentant la quantité de trafic entrant. Lorsque vous survolez le graphique avec la souris, le nombre de communications apparaît dans une info-bulle.
- **Protocoles** – Un histogramme affichant les protocoles de communication utilisés sur le réseau, classés par fréquence. Pour chaque protocole, le graphique affiche le taux auquel il a été utilisé (en pourcentage du trafic total) et le volume de trafic.

### Définition d'une période d'activité

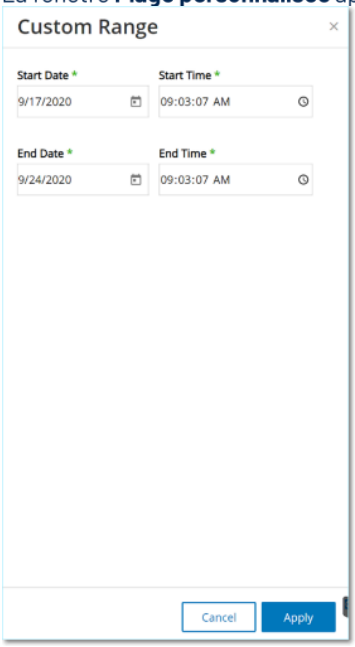
Toutes les données affichées sur l'écran Réseau représentent l'activité sur le réseau pendant une période spécifiée. La plage temporelle pour laquelle les données sont actuellement affichées est indiquée dans la barre d'en-tête. La période par défaut est définie sur les *15 dernières minutes*. Les dates/heures de *début* et de *fin* de la période sélectionnée sont affichées dans la barre d'en-tête.

### Pour définir la période :

1. Cliquez sur **Sélection de la période** dans la barre d'en-tête (par défaut, les 15 dernières minutes).
   Un menu déroulant avec des options de période apparaît.

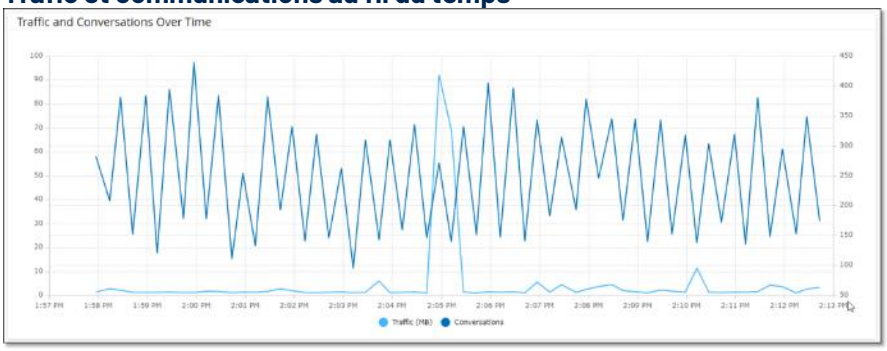



2. Sélectionnez une plage temporelle à l'aide de l'une des méthodes suivantes
   - Sélectionnez une plage temporaire prédéfinie en cliquant sur la plage souhaitée (les options sont : 15 dernières minutes, Dernière heure, 4 dernières heures, 12 dernières heures, Dernier jour, 7 derniers jours ou 30 derniers jours), OU
   - Définissez une plage temporelle personnalisée à l'aide de la procédure suivante :
     a. Cliquez sur **Plage personnalisée**.
        La fenêtre **Plage personnalisée** apparaît.




     b. Saisissez la **date** et l'**heure de début** ainsi que la **date** et l'**heure de fin** dans les champs appropriés.
     c. Cliquez sur **Appliquer**.
        La période est définie. Les dates et heures de début et fin sont affichées dans la barre d'en-tête à côté de la sélection de la période. L'écran est actualisé pour afficher uniquement les données de la période sélectionnée.

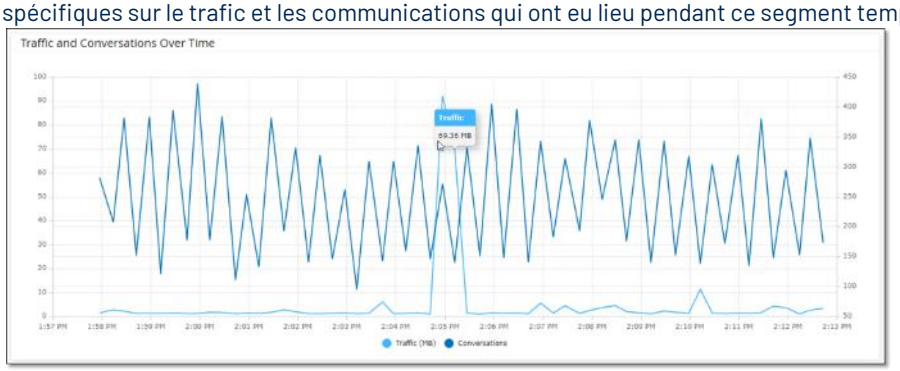
### Trafic et communications au fil du temps




Un graphique en courbes affiche la quantité de trafic (mesurée en Ko/Mo/Go) et le nombre de communications qui ont eu lieu sur le réseau au fil du temps. La clé d'affichage apparaît en haut du graphique.

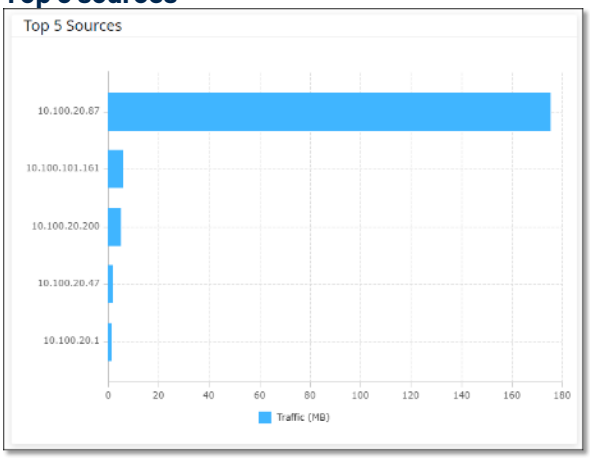
#### Pour afficher les données d'un segment temporel spécifique :

1. Survolez un point du graphique avec la souris pour afficher une fenêtre contextuelle contenant des données spécifiques sur le trafic et les communications qui ont eu lieu pendant ce segment temporel.



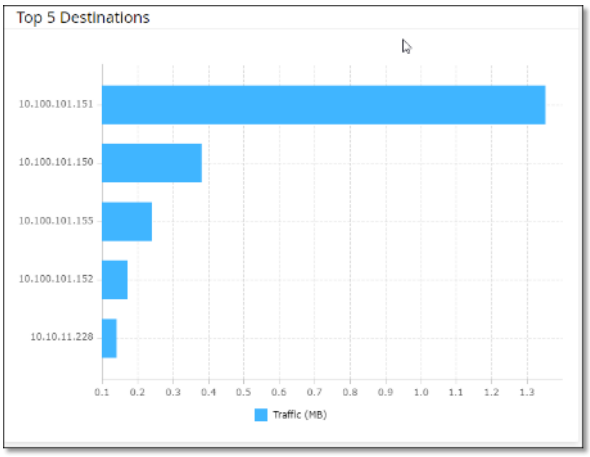

La longueur du segment temporel affiché est ajustée en fonction de l'échelle de temps affichée (par exemple, pour une période de 15 minutes, les données sont affichées pour chaque minute séparément, mais pour une période de 30 jours, elles sont affichées pour des segments de 6 heures).

### Top 5 sources



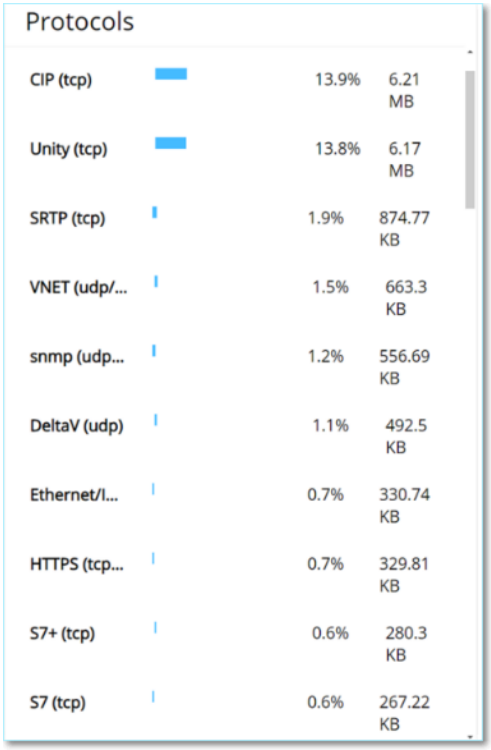
Le volet **Top 5 sources** affiche le nombre de communications et la quantité de trafic pour chacun des 5 principaux assets qui ont envoyé des communications via le réseau pendant la période spécifiée. Les assets sources sont identifiés par leurs adresses IP. Survoler le graphique à barres indique le nombre de communications et la quantité de trafic envoyés depuis cet asset.

## Top 5 cibles




Le volet **Top 5 cibles** affiche le nombre de communications et la quantité de trafic pour chacun des 5 principaux assets qui ont reçu des communications via le réseau pendant la période spécifiée. Les assets cibles sont identifiés par leurs adresses IP. Survoler le graphique à barres indique le nombre de communications et la quantité de trafic reçus par cet asset.

## Protocoles



Le volet **Protocoles** affiche des données sur l'utilisation de divers protocoles de communication au sein du réseau pendant la période spécifiée. Les protocoles sont répertoriés du plus utilisé (en haut) au moins utilisé (en bas). Pour chaque protocole, les informations suivantes sont affichées :

- Un graphique à barres montrant 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

# Captures de paquets

Le système stocke des fichiers contenant des captures de paquets complets d'activités sur le réseau. Les données sont stockées sous forme de fichiers PCAP qui peuvent être analysés à l'aide d'outils d'analyse de protocole réseau (par exemple Wireshark, etc.). Cela permet une analyse approfondie des événements critiques. Lorsque la capacité de stockage du système (1,8 To) est dépassée, le système supprime les anciens fichiers.

L'écran **Captures de paquets** affiche tous les fichiers de capture de paquets du système. L'*onglet Terminé* affiche des listes pour chaque fichier terminé disponible au téléchargement. L'*onglet En cours* affiche des détails sur la capture de paquets en cours dans le système.

La *barre d'en-tête* affiche le plus ancien fichier capturé encore disponible dans le système. Elle contient également un bouton pour télécharger des fichiers et pour arrêter manuellement la capture de paquets en cours.

Vous pouvez afficher/masquer les colonnes, trier et filtrer les listes d'assets, mais aussi rechercher des mots-clés. Pour une explication des fonctionnalités de personnalisation, voir **Utilisation des listes**.

Vous pouvez également télécharger le fichier PCAP d'un événement à partir de l'écran **Événements**. Voir **Téléchargement de fichiers**.

## Paramètres de capture de paquets

Le tableau suivant décrit les paramètres affichés pour les listes de capture de paquets.

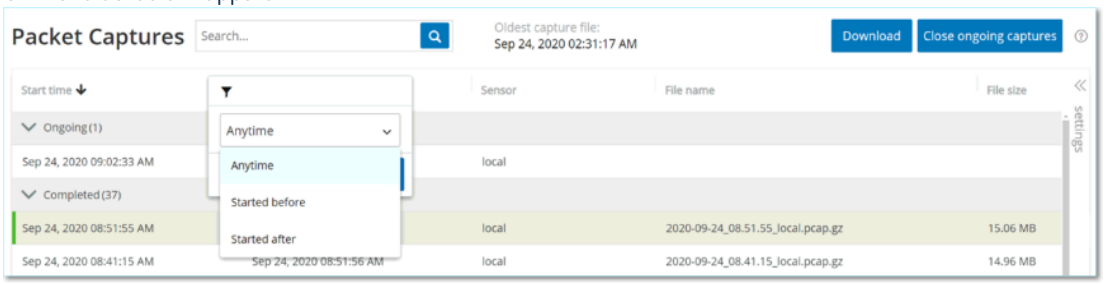
| Paramètre | Description |
|---|---|
| **Date/heure de début** | La date et l'heure auxquelles la capture de paquets a commencé. |
| **Date/heure de fin** | La date et l'heure auxquelles la capture de paquets a pris fin. |
| **Statut** | Le statut de la capture. Valeurs possibles : *Terminé* ou *En cours*. |
| **Capteur** | Le capteur Tenable.ot qui a capturé le paquet. Pour les paquets capturés directement par l'appliance Tenable.ot, la valeur est fournie comme *local*. |
| **Nom du fichier** | Le nom du fichier. |
| **Taille du fichier** | La taille du fichier, donnée en Ko/Mo. |

## Filtrage de l'affichage de la capture de paquets

L'affichage des **captures de paquets** peut être filtré pour trouver un fichier PCAP spécifique en saisissant les paramètres pour l'heure de début et/ou l'heure de fin.

### Pour filtrer les captures de paquets :

1. Sous **Réseau**, sélectionnez **Captures de paquets**.
2. Pour filtrer par date/heure de début, survolez **Date/heure de début** et cliquez sur l'icône de menu qui apparaît.
   Un menu déroulant apparaît.



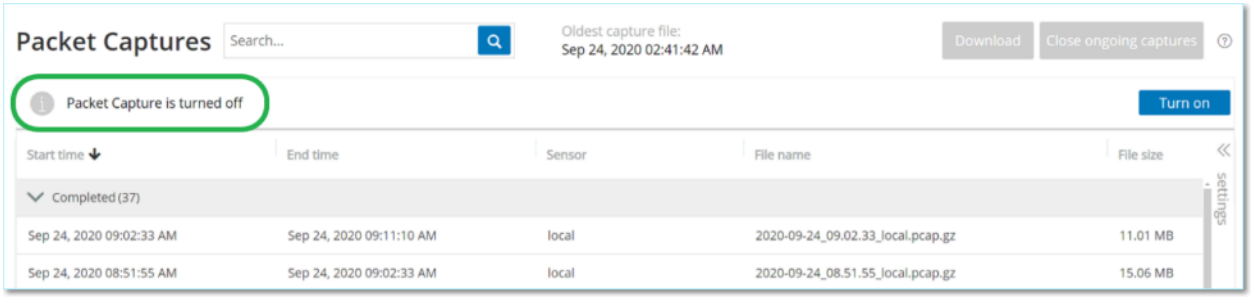

   Réglez le filtre comme suit :
   a. Sélectionnez dans la liste déroulante l'option de filtrage. Les options sont : *N'importe quand* (par défaut), *Début antérieur à* ou *Début postérieur à*.
   b. Si **Début antérieur à** ou **Début postérieur à** ont été sélectionnés, une fenêtre apparaît avec les champs **Date** et **Heure**, vous permettant de choisir la date et l'heure souhaitées.
   c. Cliquez sur **Appliquer**.
3. Pour filtrer par date/heure de fin, cliquez sur l'icône **Filtrer** à côté de **Date/heure de fin**.
   Un menu déroulant apparaît. Réglez le filtre comme suit :
   a. Sélectionnez dans la liste déroulante l'option de filtrage. Les options sont : *N'importe quand* (par défaut), *Début antérieur à* ou *Début postérieur à*.
   b. Si **Début antérieur à** ou **Début postérieur à** ont été sélectionnés, une fenêtre apparaît avec les champs **Date** et **Heure**, vous permettant de choisir la date et l'heure souhaitées.
   c. Cliquez sur **Appliquer**.

   Le filtre est appliqué et seuls les fichiers générés dans la période sélectionnée sont affichés.

## Activation/désactivation des captures de paquets

La capture de paquets peut être activée/désactivée sur l'écran **Paramètres locaux** > **Détails** de l'**appareil**, voir **Captures de paquets**.

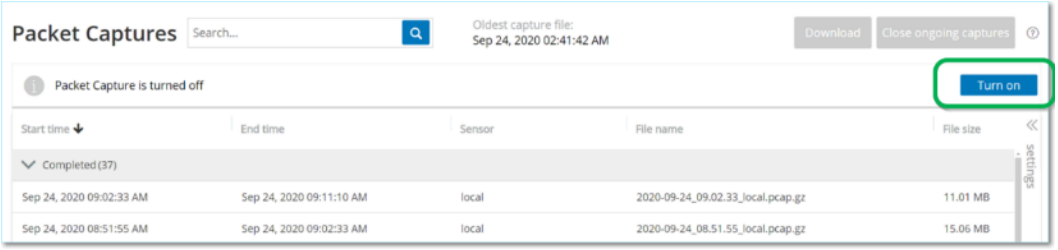
Si la fonction **Capture de paquets** est désactivée, l'écran **Captures de paquets** affiche un message vous informant qu'elle est désactivée.




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 à partir de l'écran Capture de paquets :

1. Sous **Réseau**, sélectionnez **Captures de paquets**.
2. Dans la barre **d'en-tête**, cliquez sur **Activer**.




Le système commence la capture de paquets.

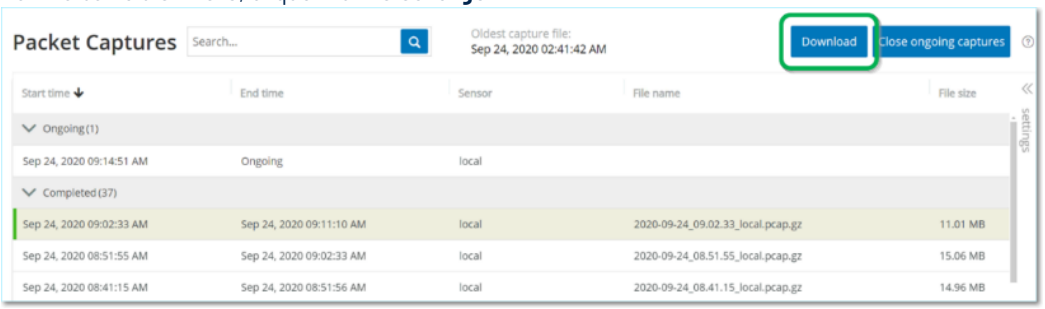
## Téléchargement de fichiers

Vous pouvez télécharger n'importe lequel des fichiers PCAP *terminés* sur votre ordinateur local. Les fichiers PCAP qui peuvent être analysés à l'aide d'outils d'analyse de protocole réseau (par exemple Wireshark, etc.).

Les captures de fichiers qui sont toujours en cours ne sont pas encore disponibles au téléchargement. Vous pouvez fermer manuellement une capture en cours afin de fermer le fichier en cours et commencer à capturer des informations pour un nouveau fichier.

### Pour télécharger un fichier terminé :

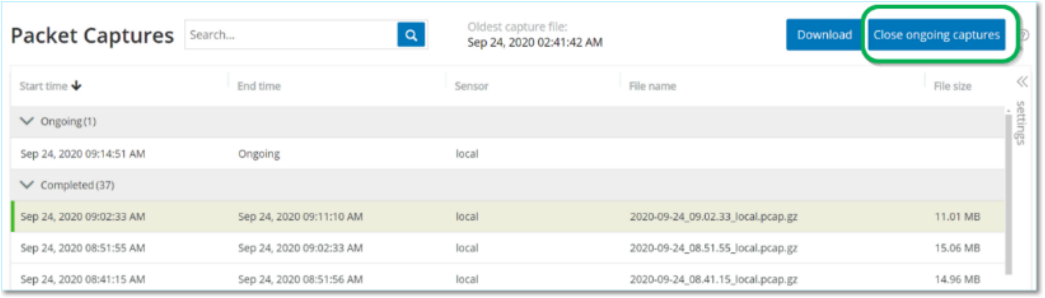
1. Sous **Réseau**, sélectionnez **Captures de paquets**.
2. Sélectionnez le fichier souhaité dans les listes de capture de paquets.
3. Dans la barre **d'en-tête**, cliquez sur **Télécharger**.




Le fichier PCAP compressé est téléchargé sur votre ordinateur local.

### Pour fermer manuellement la capture de paquets en cours :

1. Sous **Réseau**, sélectionnez **Captures de paquets**.
2. Dans la barre **d'en-tête**, cliquez sur **Fermer la capture en cours**.




La capture en cours est arrêtée et le fichier devient disponible pour le téléchargement. Une nouvelle capture de paquets est automatiquement lancée.

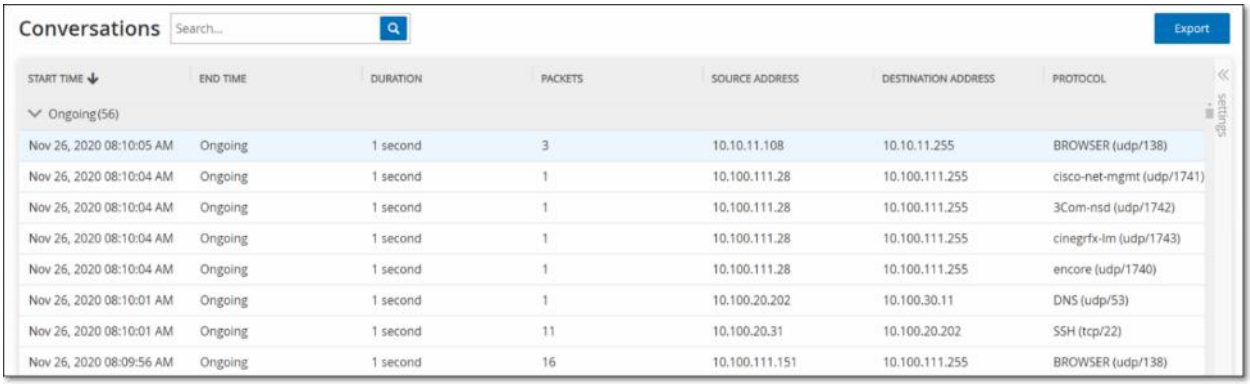
# Communications

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. L'écran **Communications** affiche une liste des communications actuelles et passées, avec des informations détaillées sur chacune d'entre elles.

L'écran Communications possède les fonctionnalités supplémentaires suivantes :

- **Rechercher** – Recherche des communications spécifiques en saisissant des informations précises dans la zone de **recherche**.
- **Exporter** – Exporte toutes les données de l'onglet Communications sur votre ordinateur local sous forme de fichier CSV en cliquant sur **Exporter**.

Le tableau Communication affiche les 10 000 dernières communications réseau.

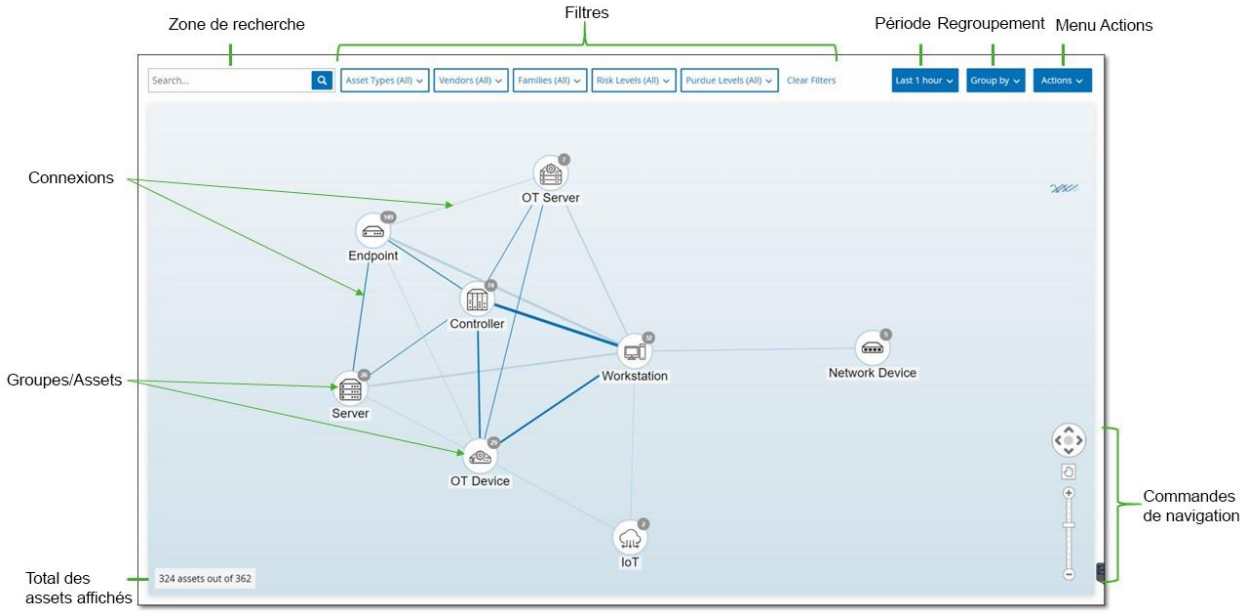



Les informations affichées dans l'onglet Communications sont décrites dans le tableau ci-dessous :

| 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 pendant laquelle la communication a été en cours. |
| **Paquets** | Le nombre de paquets de données envoyés. |
| **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 qui a été 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, telles que découvertes par les capacités de détection du réseau de Tenable.ot. La détection réseau fournit 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 du plan de contrôle. Cela inclut par exemple les chargements et téléchargements de firmware, les mises à jour apportées au code et les modifications de configuration effectuées sur des protocoles propriétaires spécifiques au fournisseur. Les assets peuvent être affichés par groupe d'assets associés ou en tant qu'assets individuels.




La cartographie du réseau affiche tous les assets et toutes les connexions découverts au cours de la période spécifiée.

Voici une explication des éléments affichés sur l'écran Cartographie du réseau.

- **Zone de recherche** – Saisissez du texte pour rechercher des assets dans l'affichage. Les résultats de la recherche sont indiqués en mettant en surbrillance tous les groupes dans lesquels une correspondance a été trouvée pour le texte de recherche. Vous pouvez explorer chaque groupe pour voir les assets pertinents.
- **Filtres** – Vous pouvez filtrer 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 qui ont été détectées pendant la plage temporelle spécifiée. La période par défaut est définie sur le *dernier mois*. Cliquez sur la **liste de sélection des périodes** pour sélectionner une autre période dans le menu déroulant.
- **Regroupements** – Vous pouvez spécifier la catégorie selon laquelle les assets sont regroupés 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 groupes qui ont été 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 **Définition d'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, chaque type d'asset étant représenté par une icône différente (comme décrit dans **Types d'assets**). Pour les groupes, le nombre situé en haut de l'icône indique le nombre d'assets inclus dans ce 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).

Vous pouvez faire glisser les groupes et les assets et les repositionner, pour obtenir une meilleure vue des assets et de leurs connexions.

- **Connexions** – Chaque communication entre des groupes d'assets et/ou des assets individuels, selon le degré de granularité actuellement affiché dans la carte. L'épaisseur de la ligne indique le volume de communication via cette connexion.
- **Total des assets affichés** – Affiche le nombre d'assets détectés sur le réseau (et affichés sur la carte) en fonction de la période et des filtres d'assets spécifiés. Ce nombre est affiché par rapport au nombre total d'assets détectés dans votre réseau.
- **Commandes de navigation** - Vous pouvez effectuer un zoom avant et arrière sur l'affichage et naviguer pour afficher les éléments souhaités à l'aide des commandes à l'écran ou à l'aide des commandes de souris standard.

## Regroupements d'assets

La cartographie du réseau peut afficher des assets regroupés selon de nombreuses catégories différentes. Des connexions sont affichées entre les groupes d'assets. Vous pouvez cliquer sur un asset pour accéder aux éléments inclus dans ce groupe. Plusieurs groupes peuvent être détaillés simultanément. Tenable.ot 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.

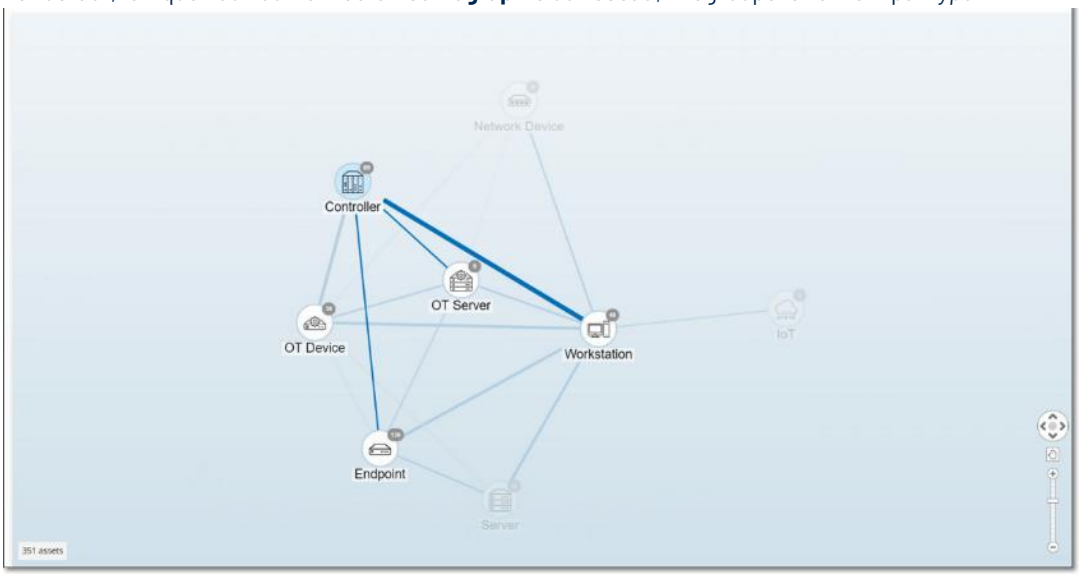
Lorsque l'affichage de la cartographie est regroupé par *type d'asset* (par défaut), la hiérarchie détaillée est la suivante : **Type d'asset** > **Fournisseur** > **Famille** > **Asset individuel**.

Lorsque l'affichage de la cartographie est regroupé par *niveau de risque* ou *niveau Purdue*, cela ajoute un niveau supplémentaire *au-dessus* du groupement par type d'asset, de sorte que la hiérarchie est : **Niveau Purdue/Niveau de risque** > **Type d'asset** > **Fournisseur** > **Famille** > **Asset individuel**. Chaque niveau est représenté par un cercle entourant les groupes/assets inclus.

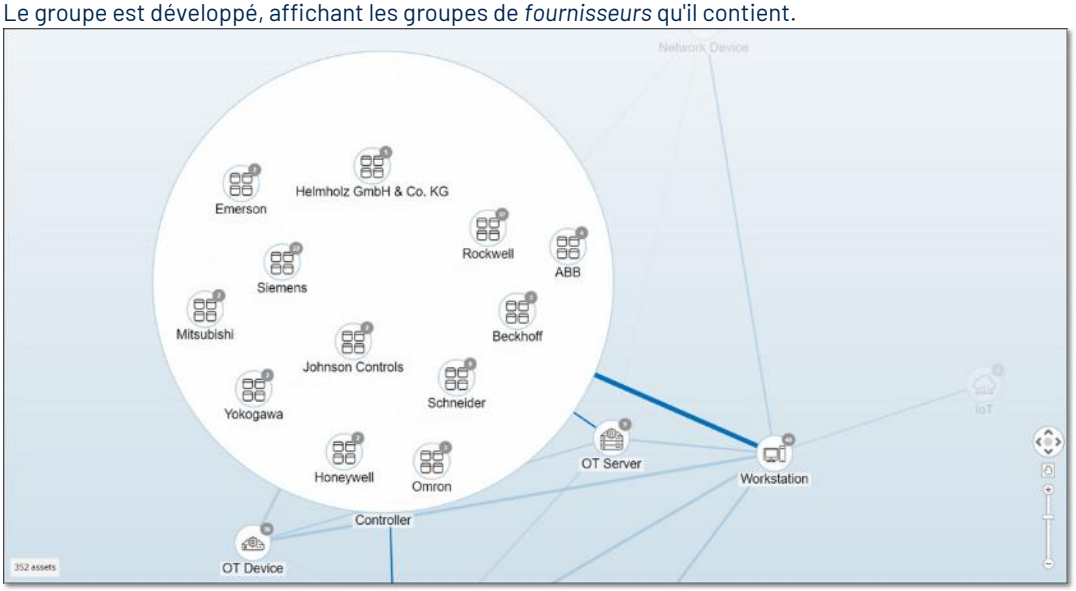
L'exemple suivant montre comment vous pouvez détailler l'affichage :

### Pour détailler un groupe de types d'assets :

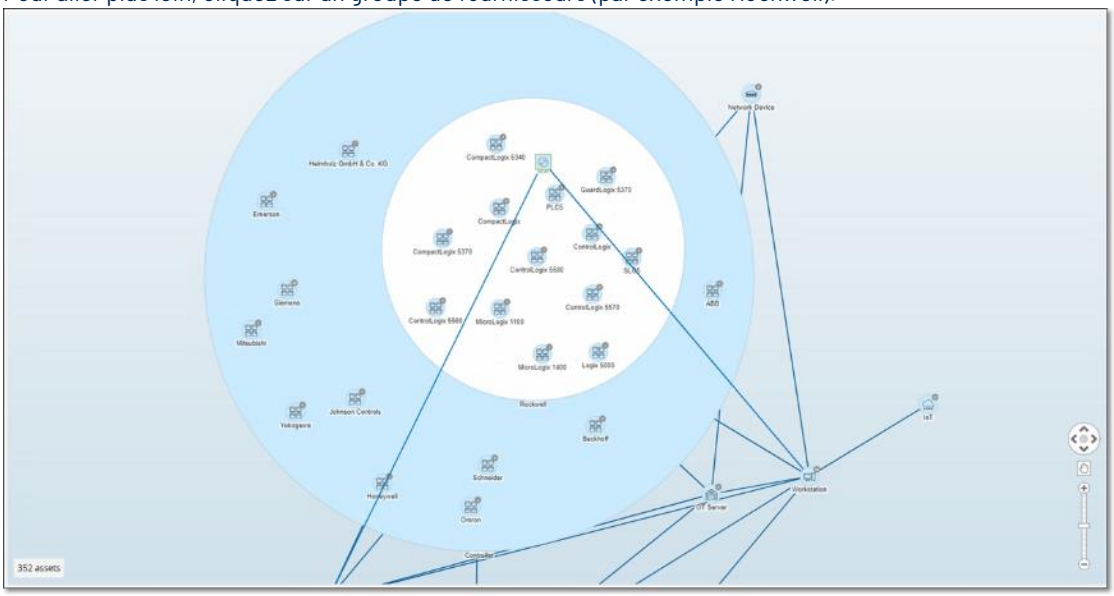
1. Par défaut, lorsque vous ouvrez l'écran **Cartographie du réseau**, il regroupe les assets par *type*.



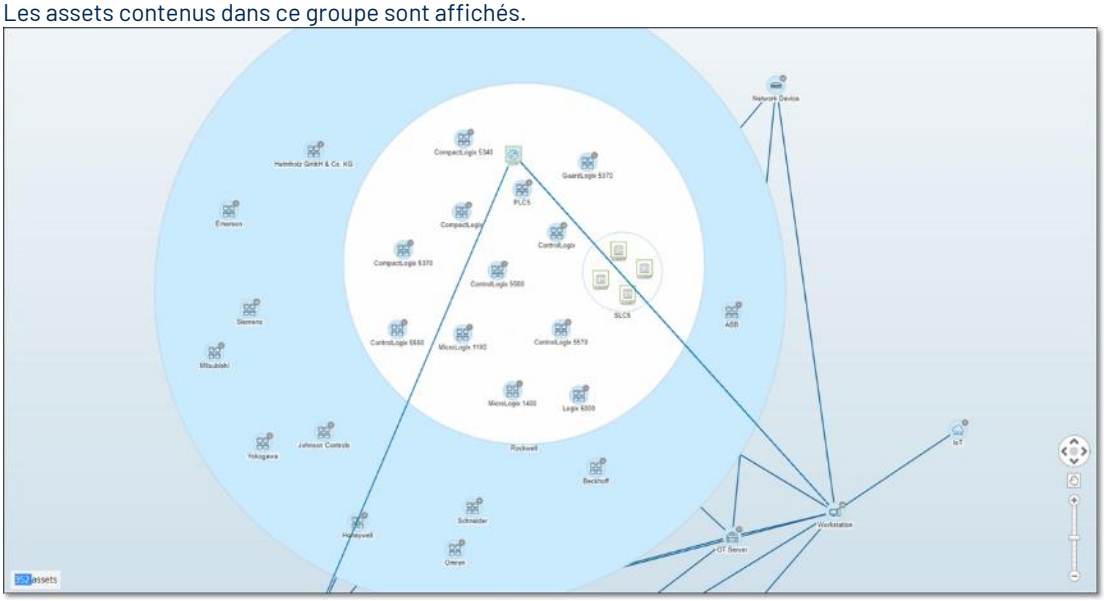

2. Double-cliquez sur l'icône du groupe que vous souhaitez détailler (par exemple **Contrôleur**).
Le groupe est développé, affichant les groupes de *fournisseurs* qu'il contient.



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).
5. Les assets contenus dans ce groupe sont affichés.



6. Vous pouvez maintenant cliquer sur un asset spécifique pour voir ses détails et ses connexions. Voir **Affichage des détails d'un asset**.

### Pour réduire l'affichage :

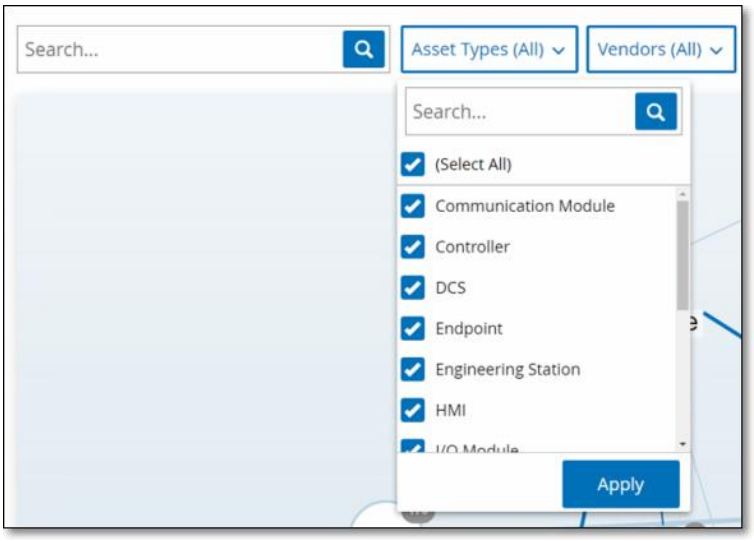
1. Cliquez sur **Grouper par**.
2. Cliquez sur **Réduire tous les groupes**.
   L'affichage retourne alors aux groupes de niveau supérieur.

### Pour supprimer tous les regroupements :

1. Cliquez sur le bouton **Grouper par**.
2. Sélectionnez **Pas de regroupement**.
   La carte affiche tous les assets uniques sans les regrouper.

# Application de filtres à l'affichage de la cartographie

Vous pouvez filtrer l'affichage de la cartographie selon une ou plusieurs des catégories spécifiées : Type d'asset, Fournisseurs, Familles, Niveaux de risque, Niveaux Purdue.




### Pour appliquer des filtres à la carte :

1. Cliquez sur la catégorie de filtre souhaitée.
2. Cochez/décochez les cases de chaque élément que vous souhaitez inclure/exclure de l'affichage.

> 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**.
   Seuls les éléments sélectionnés sont affichés sur la cartographie.

# Affichage des détails d'un asset

Cliquez 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 cartographie affiche les connexions depuis l'asset sélectionné vers tous les autres assets qui communiquent avec lui. Vous pouvez ensuite cliquer sur le lien dans le nom de l'asset pour accéder à l'écran **Détails de l'asset** où des informations plus détaillées sont affichées.


# Définition d'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**.

Toute communication entre les assets qui n'ont pas interagi pendant l'échantillonnage de la base de référence déclenche une alerte liée à une politique (en supposant qu'elle se situe dans le cadre des conditions de politique spécifiées). Une première base de référence réseau doit être créée sur l'écran Cartographie du réseau, afin de permettre la création de politiques de déviation de la base de référence réseau. Une nouvelle base de référence réseau mise à jour peut être définie à tout moment. Vous devez définir une nouvelle base de référence réseau chaque fois que de nouveaux assets ou de nouvelles connexions sont ajoutés à votre réseau.

### Pour définir une base de référence réseau :

1. Sur l'écran **Cartographie du réseau**, sélectionnée la plage temporelle des communications que vous souhaitez inclure dans la base de référence réseau à l'aide de la **liste de sélection de périodes** située en haut de l'écran.
   La **Cartographie du réseau** apparaît sur l'écran pour la période sélectionnée.
2. Cliquez sur **Actions** > **Définir comme base de référence** en haut de l'écran.
   La nouvelle base de référence réseau est établie dans le système et s'applique à toutes les politiques de déviation de la base de référence réseau.

# Vulnérabilités

Tenable.ot identifie différents types de menaces qui affectent les assets de 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, Inc. conçoit des programmes pour permettre à Nessus de les détecter.

Ces programmes sont nommés *Plug-ins* et sont écrits dans le langage de script propriétaire de Nessus, appelé *Nessus Attack Scripting Language* (NASL). Les plug-ins détectent les CVE ainsi que les autres menaces pesant sur les assets de votre réseau (par exemple, systèmes d'exploitation obsolètes, utilisation de protocoles vulnérables, ports ouverts vulnérables, etc.)

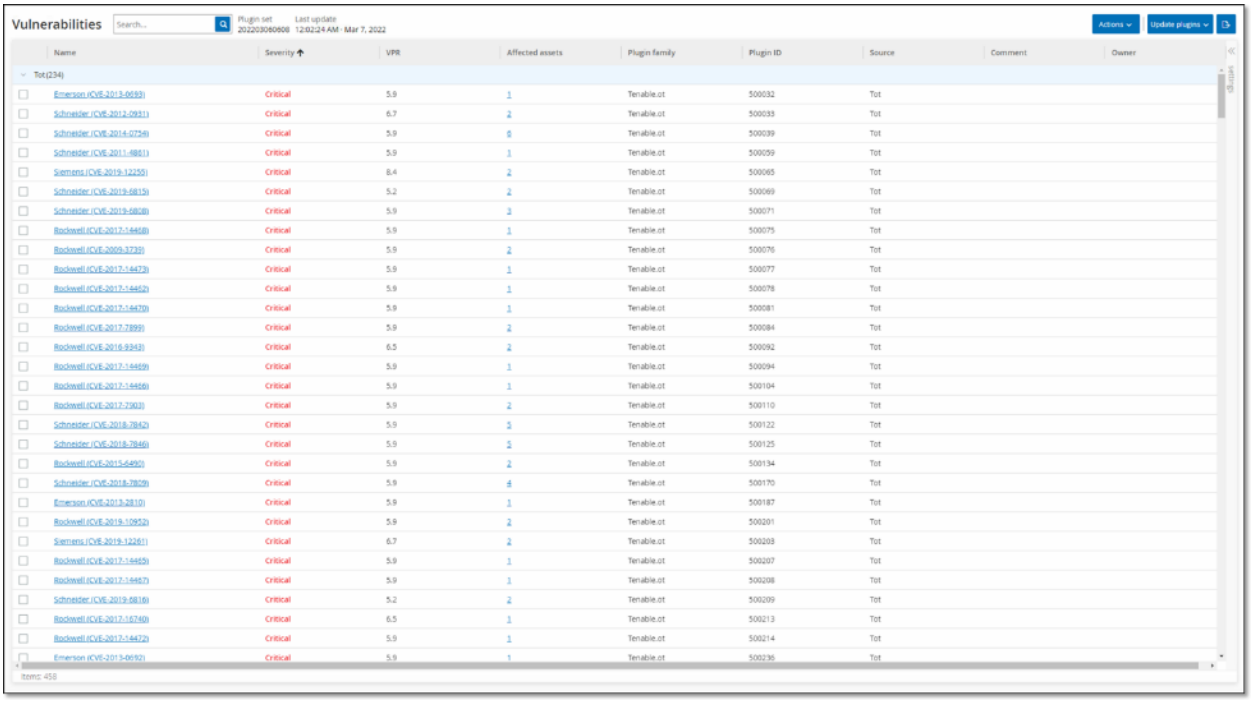
Les plug-ins contiennent des informations sur la vulnérabilité, un ensemble générique d'actions de remédiation et l'algorithme pour tester la présence du problème de sécurité.

Pour plus d'informations sur la mise à jour de votre ensemble de plug-ins, voir **Mises à jour**.

## Écran Vulnérabilités

L'écran **Vulnérabilités** affiche une liste de toutes les vulnérabilités détectées par les plug-ins Tenable.ot 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 **Utilisation des listes**.




Les informations affichées sur l'onglet **Vulnérabilités** sont décrites dans le tableau suivant :

| Paramètre | Description |
|---|---|
| **Nom** | Le nom de la vulnérabilité. Le nom est un lien permettant d'afficher la liste complète des vulnérabilités. |

| Paramètre | Description |
|---|---|
| **Sévérité** | Ce score indique la sévérité de la menace détectée par ce plug-in. Les valeurs possibles sont : *Info*, *Faible*, *Moyenne* ou *Haute*. |
| **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. Cette valeur est générée par Tenable en tant que sortie du service Predictive Priorization de Tenable, qui évalue l'impact technique et la menace posée par la vulnérabilité.<br>Les valeurs VPR vont de 0,1 à 10,0, une valeur plus élevée représentant une plus grande probabilité d'exploitation. |
| **ID de plug-in** | L'identifiant unique du plug-in. |
| **Assets affectés** | Le nombre d'assets de votre réseau qui sont affectés par cette vulnérabilité. |
| **Famille du plug-in** | 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

Cliquez sur un nom de plug-in pour afficher ses informations détaillées.

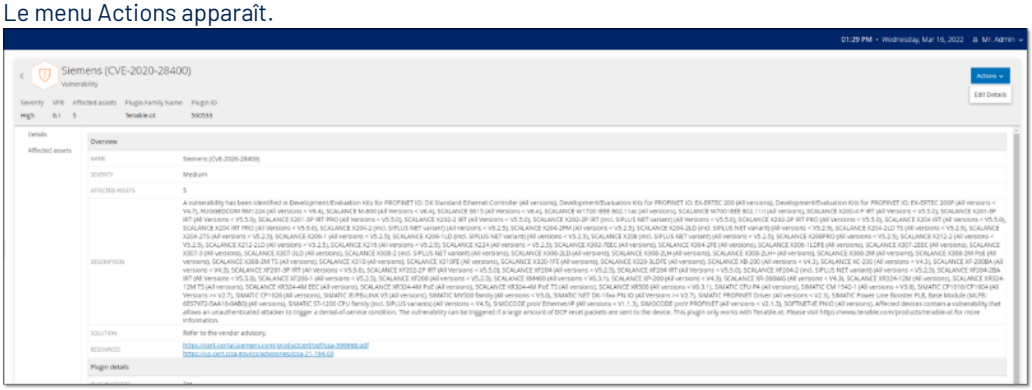

Cet écran contient trois éléments :

- **Barre d'en-tête** – Affiche des informations de base sur la vulnérabilité spécifiée et contient le bouton **Actions**, qui vous permet de modifier les détails de la vulnérabilité. Voir **Modification des 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 une 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 Détails de l'asset.

# Modification des détails d'une vulnérabilité

## Pour modifier les détails de la vulnérabilité :

1. Sur la page **Détails de la vulnérabilité** pertinente, cliquez sur le bouton **Actions** dans le coin supérieur droit.
   Le menu Actions apparaît.




2. Dans le menu **Actions**, cliquez sur **Modifier les détails**.
   Le panneau latéral **Modifier les détails de la vulnérabilité** apparaît.


3. Dans le champ **Commentaires**, saisissez des commentaires sur la vulnérabilité.
4. Dans le champ **Propriétaire**, saisissez le nom de la personne désignée pour traiter la vulnérabilité.
5. Cliquez sur **Enregistrer**.

# Paramètres locaux

Les différents écrans de paramètres sont répertoriés sous **Paramètres locaux** dans la navigation principale.

Voici une brève description des informations affichées et des actions disponibles dans chacun des onglets.

- **Requêtes** – Activez/désactivez les fonctions de requête et ajustez leur fréquence et leurs paramètres. Les requêtes sont divisées en écrans distincts pour *Découverte des assets*, *Contrôleur* et *Réseau*. Voir **Requêtes**.
- **Configuration système**
    - **Appareil** – Affichez et modifiez les détails de l'appareil et les informations sur le réseau (par exemple, l'heure du système, les serveurs DNS, la déconnexion automatique (c'est-à-dire le délai d'inactivité)).
    - **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 des ports** – Affichez la manière dont les ports de l'appareil sont configurés. Pour plus d'informations sur la configuration des ports, voir **Installation de l'appliance Tenable.ot** > **Étape 4 – Assistant d'installation** > **Écran 2 – 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 **Certificat**.
    - **Clés API** – Générez des clés API pour permettre aux applications tierces d'accéder à Tenable.ot via l'API. Tous les utilisateurs peuvent créer des clés API. La clé API aura les mêmes autorisations que l'utilisateur qui l'a créée, selon son rôle. Une clé API apparaît une seule fois, lorsqu'elle est générée pour la première fois ; l'utilisateur doit l'enregistrer dans un emplacement sécurisé pour une utilisation ultérieure.
    - **Licence** – Affichez, mettez à jour et renouvelez votre licence. Voir **Licence**.
- **Configuration de l'environnement**
    - **Paramètres des assets** –
        - **Réseau surveillé** – Affichez et modifiez l'agrégation des plages d'adresses IP dans lesquelles le système classe les assets.
        - **Mettre à jour les détails d'un asset à l'aide d'un fichier CSV** – Mettez à jour les détails de vos assets à l'aide d'un modèle CSV.
        - **Ajouter des assets manuellement** – Ajoutez de nouveaux assets à votre liste d'assets à l'aide d'un modèle CSV.

Le nombre maximal de plages d'adresses IP pouvant être envoyées au NNM est de 128, nous vous recommandons donc de ne pas dépasser cette limite.

En plus des plages d'adresses IP spécifiées, tout hôte au sein des sous-réseaux de la plateforme Tenable.ot ou tout appareil exécutant une activité sera classé comme un asset.

  - **Assets masqués** – Affiche une liste des assets qui étaient masqués dans le système (c'est-à-dire que l'utilisateur a choisi de supprimer des listes d'assets), voir **Masquer des assets**. Vous pouvez restaurer les assets masqués à partir de cet écran.
  - **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 faciliter leur surveillance. Voir **Clusters d'événements**.
  - **Lecteur PCAP** – Vous permet d'importer un fichier PCAP contenant une activité réseau enregistrée et de le « lire » sur Tenable.ot, 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 **Utilisateurs locaux**.
  - **Groupes d'utilisateurs** – Un utilisateur administrateur peut afficher, modifier, ajouter et supprimer des groupes d'utilisateurs. Voir **Groupes d'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 **Serveurs d'authentification**.

- **Intégrations** – Configurez l'intégration avec d'autres plates-formes. Tenable.ot 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.sc et Tenable.io). 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 Tenable.ot-FortiGate permet aux utilisateurs d'envoyer des suggestions de politique de pare-feu à un pare-feu FortiGate en fonction des événements réseau de Tenable.ot.

- **Actions système** – Affiche un sous-menu des activités du système. Le sous-menu comprend les options suivantes :

  - **Sauvegarde système** – Vous permet de sauvegarder votre appliance Tenable.ot (à l'exception des données de capture de paquets). Pour restaurer le système à partir d'un fichier de sauvegarde, voir https://www.fr.tenable.com/products/tenable-ot. Veuillez noter que pendant le processus de sauvegarde, Tenable.ot sera indisponible pour tous les utilisateurs.
  - **Paramètres d'exportation** – Exporte les paramètres de configuration de la plateforme Tenable.ot sous forme de fichier .ndg vers l'ordinateur local. Cela servira de sauvegarde en cas de réinitialisation du système ou pour importer vers une nouvelle plateforme Tenable.ot.
  - **Paramètres d'importation** – Importe les paramètres de configuration de la plateforme Tenable.ot sous forme de fichier .ndg vers l'ordinateur local.
  - **Télécharger les données de diagnostic** – Crée un fichier avec des données de diagnostic sur la plateforme Tenable.ot et le stocke sur l'ordinateur local.
  - **Redémarrer** – Redémarre la plateforme Tenable.ot. Ceci est nécessaire pour l'activation de 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 Tenable.ot. Pour mettre l'appliance Tenable.ot sous tension, appuyez sur le bouton d'alimentation.
- **Réinitialisation d'usine** – Rétablit tous les paramètres aux paramètres d'usine par défaut. Attention : cette opération est irréversible et toutes les données du système seront perdues.

- **Journal système** – Affiche un journal de tous les événements système (par exemple, politique activée, politique modifiée, événement résolu, etc.) qui se sont produits sur le système. Vous pouvez exporter le journal sous forme de fichier CSV ou l'envoyer à un serveur Syslog. Voir **Journal système**.

# Requêtes

Les écrans Requêtes de Tenable.ot vous permettent de configurer et d'activer les fonctionnalités de requêtes. Pour une explication générale de la technologie de requêtes, voir **Technologies Tenable.ot**. Dans le cadre de la configuration initiale, il a été recommandé d'activer toutes les fonctionnalités de requête. À tout moment, vous pouvez activer/désactiver n'importe laquelle des fonctions de requête. Vous pouvez également ajuster les paramètres pour définir quand et comment les requêtes sont exécutées.

En plus des requêtes automatiques qui sont exécutées périodiquement, la plupart des requêtes peuvent être lancées à la demande par l'utilisateur en cliquant sur le bouton **Exécuter maintenant** à côté de la requête.

Les scans de vulnérabilités Log4J et Ripple20 ne peuvent être exécutées que **manuellement**, et non selon un calendrier périodique. Elles sont activées à partir de l'écran **Paramètres locaux** > **Requêtes** > **Réseau**. Voir **Tableau des fonctions de requête réseau**.

La désactivation des requêtes empêchera le système de détecter des événements significatifs sur le réseau. Cela entraînera l'indisponibilité de nombreuses fonctionnalités.

L'activation et la configuration de la requête se font sous **Paramètres locaux** > **Requêtes**. Les requêtes sont divisées en trois écrans distincts. Les sections suivantes expliquent les différents types de requêtes et donnent les procédures d'activation et de configuration de chaque type de requête.

## Toutes les requêtes de contrôleur

### Pour activer les requêtes de contrôleur :

1. Sous **Paramètres locaux**, accédez à l'écran **Requêtes** > **Contrôleur**.
2. **Activez** le curseur **Toutes les requêtes du contrôleur**.
3. **Activez/désactivez** des types spécifiques de requêtes en déplaçant le curseur pour chaque type de requête. Pour obtenir une description des différents types de requêtes du contrôleur, voir **Tableau des fonctions de requête de contrôleur**.
4. Vous pouvez modifier les paramètres de chaque type de requête de contrôleur en procédant comme suit :
   a. Cliquez sur **Modifier** à côté du type de requête souhaité.
   b. Ajustez la fréquence et la planification des requêtes (pour une explication des options de configuration disponibles, voir **Tableau des fonctions de requête de contrôleur**).
   c. Cliquez sur **Enregistrer**.

### Tableau des fonctions de requête de contrôleur

| Fonction | Description | Fréquence (min.-max.) |
|---|---|---|
| **Toutes les requêtes de contrôleur** | Active toutes les fonctions de requête liées aux contrôleurs, comme décrit ci-dessous. | S/O |
| **Instantanés périodiques** | Capture le programme actuel déployé sur chaque contrôleur. En prenant périodiquement des instantanés, Tenable.ot peut détecter les modifications apportées au programme d'un contrôleur même si les modifications n'ont pas été envoyées via le réseau. | 1/jour – 1/6 semaines |
| **Instantanés déclenchés par la politique** | Permet à l'utilisateur de configurer des politiques qui déclenchent un instantané lorsque les conditions d'une politique sont remplies. | S/O |
| **Découverte des contrôleurs** | Une diffusion qui recherche de nouveaux contrôleurs et aide à classer les assets inconnus. | 1/hr. – 1/6 semaines |
| **Requête sur l'état du contrôleur** | Détecte le statut actuel du PLC (les options sont : *En cours d'exécution*, *Arrêté*, *Défaut*, *Pas de configuration* et *Test*). | 1/5 min. – 1/h. |
| **Requête de tampon de diagnostic** | Interroge les journaux d'événements du tampon de diagnostic tels que définis dans les contrôleurs Siemens. | 1/jour – 1/6 semaines |
| **Requête sur les détails du contrôleur** | Récupère les détails du matériel et du firmware du contrôleur. | 1/hr. – 1/6 semaines |
| **Requête sur le fond de panier** | Découvre les modules et leurs spécifications au sein d'un fond de panier. La requête permet une identification rapide de l'ensemble de la configuration du fond de panier. | 1/15 min. – 1 semaine |

## Toutes les requêtes réseau

### ➡ Pour activer les requêtes réseau :

1. Sous **Paramètres locaux**, accédez à l'écran **Requêtes** > **Réseau**.
2. **Activez** le curseur **Toutes les requêtes réseau**.
3. **Activez/désactivez** des types spécifiques de requêtes en déplaçant le curseur pour chaque type de requête que vous souhaitez activer. Pour obtenir une description des diverses fonctionnalités de requête réseau, voir **Tableau des fonctions de requête réseau**.
4. Vous pouvez modifier les paramètres de chaque type de requête réseau en procédant comme suit :
    a. Cliquez sur **Modifier** à côté du type de requête souhaité.
    b. Ajustez la fréquence et la planification des requêtes (pour une explication des options de configuration disponibles, voir **Tableau des fonctions de requête réseau**).
    c. Cliquez sur **Enregistrer**.

### Tableau des fonctions de requête réseau

| Fonction | Description | Paramètres |
|---|---|---|
| **Toutes les requêtes réseau** | Active toutes les fonctions de requête liées aux assets réseau hors contrôleurs, comme décrit ci-dessous. | S/O |

| Fonction | Description | Paramètres |
|---|---|---|
| **Mappage de port** | identifie tous les ports ouverts dans les assets du réseau. Cela vous permet de minimiser les risques de sécurité en fermant les ports inutilisés. | Plage de mappage – Définissez si le mappage est effectué pour tous les ports ou uniquement pour les 1000 ports les plus fréquemment utilisés.<br>Taux de mappage – Définissez le nombre par défaut de ports mappés par seconde et le taux maximum de mappage à la demande. |
| **Requête SNMP** | Collecte les informations de configuration des assets compatibles SNMP sur le réseau. | Chaînes de communauté SNMP v2<br>Noms d'utilisateur SNMP v3<br>Fréquence et planification – 1/jour – 1/6 semaines |
| **Requête DNS** | Recherche les noms DNS des assets du réseau. | S/O |
| **Requête ARP** | Récupère l'adresse MAC des nouvelles IP détectées sur le réseau. | S/O |
| **NetBIOS** | Cette requête envoie un paquet Netbios Unicast utilisé pour classer et détecter les machines Windows sur le réseau. | Fréquence et planification – 1/hr. – 1/6 semaines |
| **Suivi des assets actifs** | Détecte les assets inactifs sur le réseau pendant la période spécifiée et les interroge pour vérifier s'ils sont toujours actifs. | Fréquence et planification – 1/5 min. – 1/semaine |
| **Requête WMI** | Collecte des informations sur les machines Windows du réseau. | Nom d'utilisateur WMI – Fourni par le service informatique<br>Mot de passe – Fourni par le service informatique<br>Fréquence et planification – 1/jour – 1/6 semaines<br>Tester l'adresse IP – Vous pouvez tester la configuration WMI en cliquant sur Tester l'adresse IP. Saisissez l'adresse IP d'une machine Windows connue de votre réseau, puis cliquez sur Tester l'adresse IP en bas de l'écran. Vous pouvez ensuite ouvrir les détails de cet asset et vérifier que les informations WMI ont bien été ajoutées. |
| **Requête de connexions USB** | Détecte la connexion des périphériques USB/DoK aux PC Windows du réseau. | Fréquence et planification – 1/jour – 1/6 semaines |
| **Scan des vulnérabilités Ripple20** | Ce scan identifie les CVE liées aux vulnérabilités Ripple20. Il utilise un plug-in Nessus.<br>**Remarque :** ce scan doit être exécuté **manuellement** et uniquement sur les assets au sein des adresses IP et/ou des CIDR spécifiés. | Adresses IP ou CIDR |

| Fonction | Description | Paramètres |
|---|---|---|
| **Scan des vulnérabilités Log4j** | Ce scan identifie les CVE liées aux vulnérabilités Log4j. Il utilise un plug-in Nessus.<br>**Remarque :** ce scan doit être exécuté manuellement et uniquement sur les assets au sein des adresses IP et/ou des CIDR spécifiés. | Adresses IP ou CIDR |

### Découverte des assets

Tenable.ot identifie automatiquement les assets du réseau en détectant leurs interactions avec d'autres assets du réseau. Tenable.ot a également la capacité d'identifier les assets qui ne sont pas actifs sur le réseau, ou dont les flux de communications ne sont pas capturés par les ports de mise en miroir à l'aide de la requête **Découverte des assets**. Vous pouvez configurer la fréquence d'exécution automatique de la requête. Vous pouvez également exécuter manuellement la requête à tout moment à partir de cet écran.

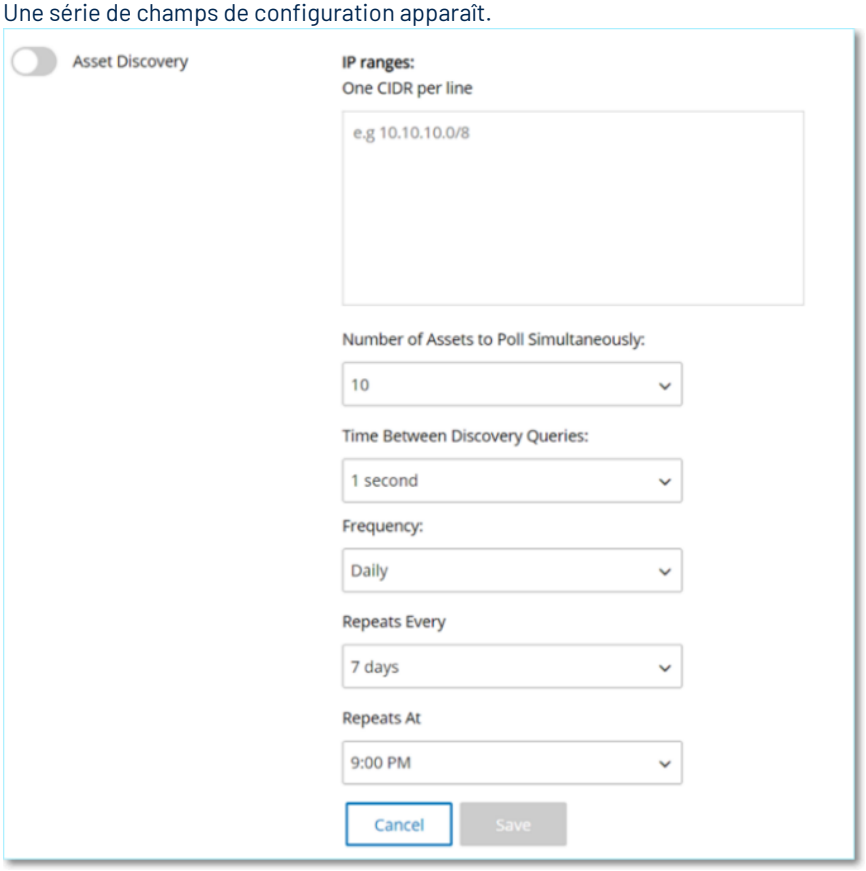
Quand un nouvel asset est découvert, la fonction **Enrichissement initial des assets** exécute les requêtes suivantes pour déterminer des informations précises à propos de l'asset : SNMP, vérification minimale de port ouvert, CIP/DCP, NetBIOS, requête de fond de panier, identification Unicast, détails du contrôleur, état du contrôleur.

Seules les adresses IP définies comme réseaux surveillés dans les **paramètres de l'asset** seront incluses dans le scan.

La désactivation des requêtes empêchera le système de détecter des événements significatifs sur le réseau. Cela entraînera l'indisponibilité de nombreuses fonctionnalités.

### Pour activer la requête de découverte des assets :

1. Sous **Paramètres locaux**, accédez à l'écran **Requêtes** > **Découverte des assets**.
2. Cliquez sur **Modifier** dans la section **Découverte des assets**.
   Une série de champs de configuration apparaît.




3. Dans la zone **Plages d'adresses IP**, saisissez une ou plusieurs plages d'adresses IP (chaque plage étant sur une ligne distincte).

> Les segments de votre réseau surveillés par le port miroir n'ont pas besoin d'être saisis et sont automatiquement interrogés par Tenable.ot. Pour exécuter la requête de découverte des assets sur des segments **supplémentaires** de votre réseau qui ne sont pas surveillés par le port miroir, saisissez la plage d'adresses IP pour ces segments dans cette zone.

4. Vous pouvez ajuster les paramètres de configuration suivants (facultatif) en sélectionnant une valeur dans le menu déroulant.
   - **Nombre d'assets à interroger simultanément** (options : 10, 20, 30)
   - **Temps entre les requêtes de découverte** (options : 1 à 3 secondes)
   - **Répétitions** – Définissez le type d'intervalle utilisé pour définir la fréquence de la requête (quotidienne ou hebdomadaire)
   - **Répéter chaque** – Définissez la fréquence de la requête (quotidienne : 1 à 31 jours, hebdomadaire : 1 à 6 semaines)
   - **Le** – Pour un intervalle hebdomadaire, définissez le jour de la semaine où la requête est exécutée
   - **À** – Définissez l'heure de la journée à laquelle la requête est exécutée
5. Cliquez sur **Enregistrer**.
6. **Activez** le curseur **Découverte des assets**.

### Pour activer l'enrichissement initial des assets :

1. Sous **Paramètres locaux**, accédez à l'écran **Requêtes** > **Découverte des assets**.
2. **Activez** le curseur **Enrichissement initial des actifs**.

## Scans de plug-in Nessus

Le scan de plug-in Nessus lance un scan Nessus avancé qui exécute une liste définie par l'utilisateur de plug-ins sur les assets spécifiés dans la liste de CIDR et d'adresses IP.

Le scan est exécuté sur les assets sensibles au sein des CIDR désignés. Cependant, afin de protéger vos appareils OT, seuls les assets réseau confirmés dans la plage donnée (hors PLC) seront scannés. Les ressources de type « Terminal » (Endpoint) ne seront pas scannées.

Nessus est un outil invasif qui fonctionne mieux dans les environnements informatiques. Il n'est pas recommandé de l'utiliser sur les appareils OT, car cela peut interférer avec leur fonctionnement habituel.

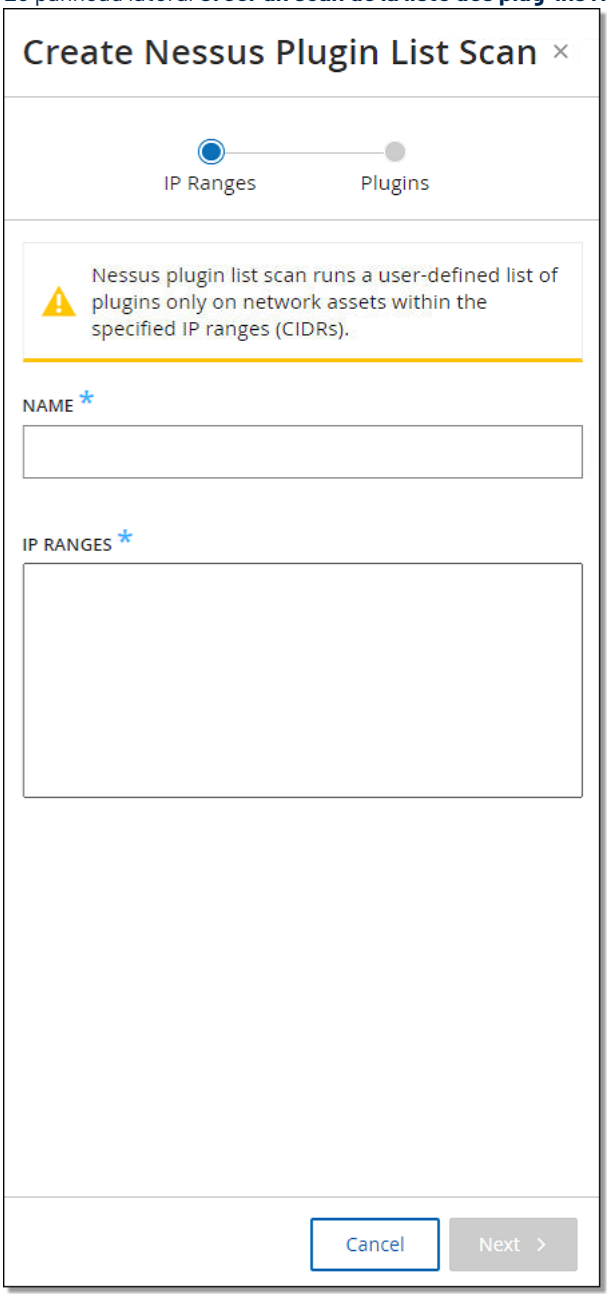
Pour exécuter un scan Nessus sur n'importe quel asset, voir **Exécution d'un scan Nessus spécifique à un asset**.

Le scan de base peut être exécuté sur des assets de type « Terminal » (Endpoint).

### Pour créer un scan de plug-in Nessus :

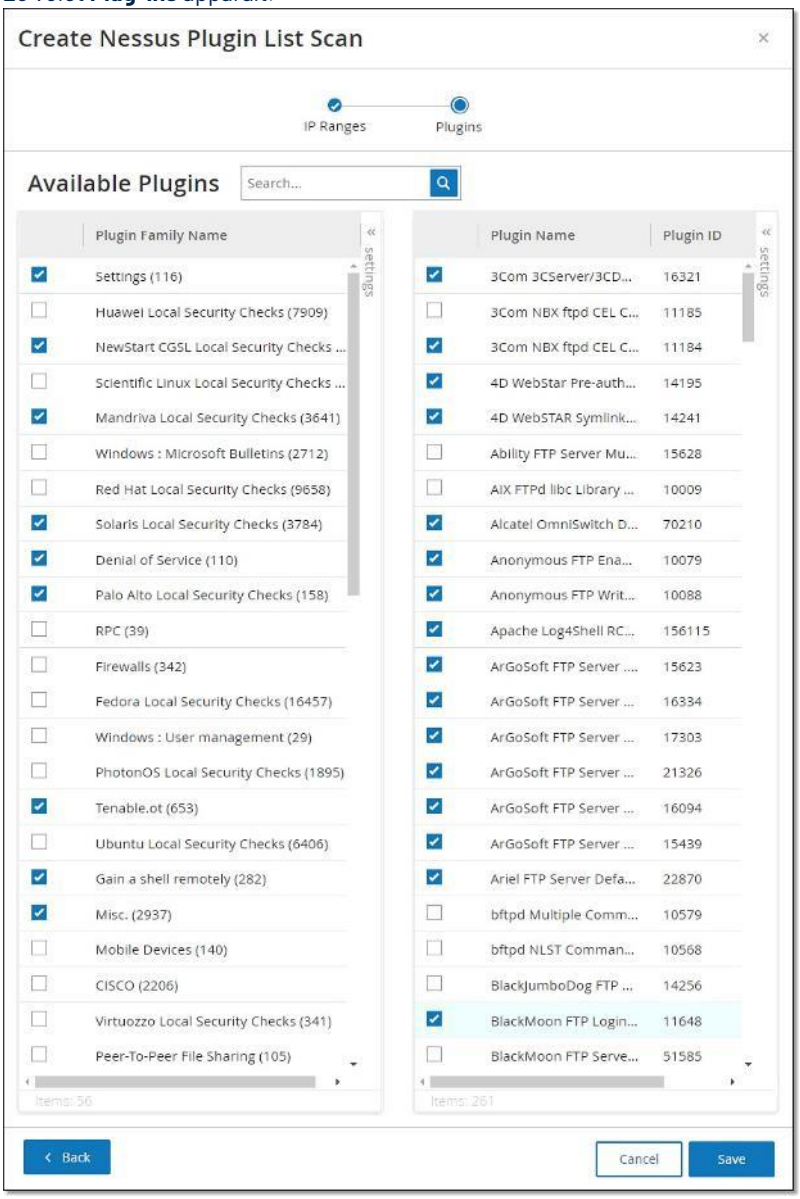
1. Accédez à **Paramètres locaux** > **Requêtes** > **Scans Nessus**.

2. Cliquez sur le bouton **Créer un scan**.
   Le panneau latéral **Créer un scan de la liste des plug-ins Nessus** apparaît.




3. Dans le champ **Nom**, saisissez un nom pour le scan Nessus.
4. Dans le champ **Plages d'adresses IP**, saisissez une plage de CIDR ou d'adresses IP.

5. Cliquez sur **Suivant**.
   Le volet **Plug-ins** apparaît.




> Les plug-ins affichés sont spécifiques à l'appareil. Votre licence doit être à jour pour recevoir de nouveaux plug-ins. Pour mettre à jour votre licence, voir **Mise à jour de la licence**.

6. Sélectionnez les familles de plug-ins de votre choix dans la colonne de gauche pour les inclure dans le scan. Désélectionnez individuellement des plug-ins dans la colonne de droite.

> Pour plus d'informations sur les familles de plug-ins Nessus, voir https://www.tenable.com/plugins/nessus/families.

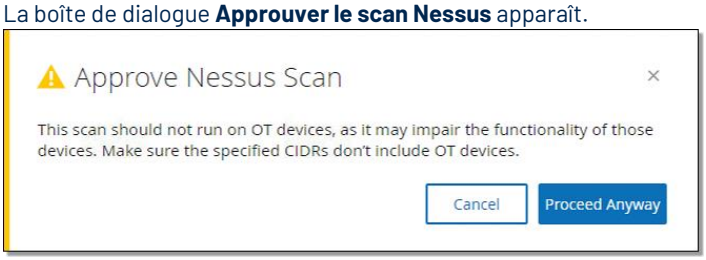
7. Cliquez sur **Enregistrer**.
   Le nouveau scan Nessus apparaît sur l'écran **Scans Nessus**.

Pour modifier ou supprimer un scan Nessus existant, cliquez avec le bouton droit sur la ligne Scan souhaitée et sélectionnez **Modifier** ou **Supprimer**.

### Pour exécuter un scan de plug-in Nessus :

1. Sur l'écran Scans **Nessus**, sélectionnez la ligne Scan souhaitée, effectuez un clic droit et sélectionnez **Exécuter maintenant**, ou cliquez sur **Actions > Exécuter maintenant**.


La boîte de dialogue **Approuver le scan Nessus** apparaît.



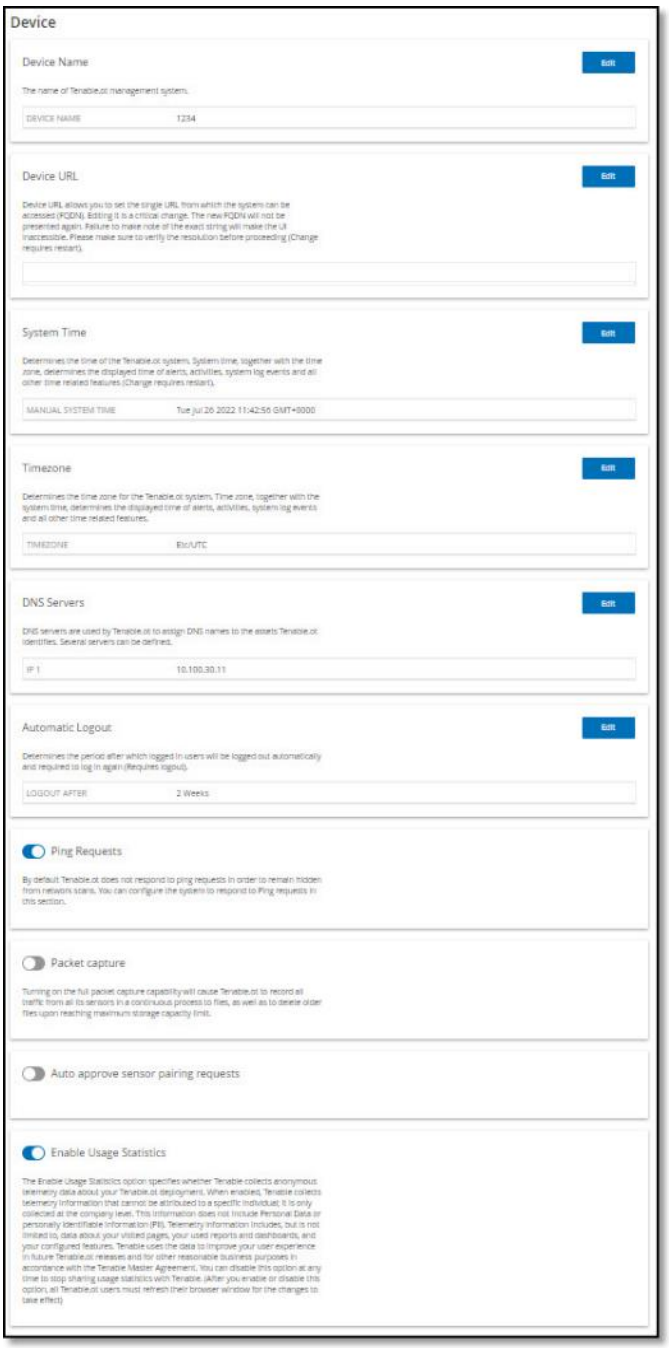

2. Si vous savez qu'aucun appareil OT n'est inclus dans le scan, cliquez sur **Continuer quand même**.
   La boîte de dialogue se referme et le scan est enregistré.
3. Pour exécuter le scan, effectuez de nouveau un clic droit sur la ligne du scan et sélectionnez **Exécuter maintenant**.
   La boîte de dialogue **Approuver le scan Nessus** réapparaît.
4. Cliquez sur **Continuer quand même**.
   Le scan commence alors à s'exécuter. Les scans peuvent être mis en pause, repris, arrêtés et annulés en fonction de leur statut en cours.

# Configuration système

Les écrans de configuration système de Tenable.ot vous permettent de configurer automatiquement et d'effectuer manuellement les mises à jour des plug-ins, ainsi que d'afficher et de mettre à jour les détails concernant votre appareil, le certificat HTTPS, les clés API et la licence.

## Appareil

Cet écran affiche des informations détaillées sur votre configuration Tenable.ot. Vous pouvez afficher les informations et modifier la configuration sur cet écran.



Les informations suivantes sont affichées :

- **Nom de l'appareil** – Un identifiant unique pour l'appliance Tenable.ot.
- **URL de l'appareil** – Vous permet de définir l'URL unique à partir de laquelle le système est accessible (FQDN).

La modification de l'URL de l'appareil est un changement critique. Le nouveau FQDN ne sera plus jamais présenté. Si vous ne notez pas la chaîne exacte, l'interface utilisateur deviendra inaccessible. Assurez-vous de vérifier la résolution avant de continuer.

- **Heure système** – L'heure et la date correctes sont généralement définies automatiquement, mais peuvent être modifiées.

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

- **Fuseau horaire** – Sélectionnez le fuseau horaire local correspondant à l'emplacement du site dans la liste déroulante.
- **Serveurs DNS** – Les serveurs DNS sont utilisés par le système Tenable.ot pour attribuer des noms DNS aux assets identifiés par Tenable.ot. Plusieurs serveurs peuvent être identifiés.
- **Déconnexion automatique** – Détermine la période après laquelle les utilisateurs connectés seront automatiquement déconnectés et devront se reconnecter.
- **Période d'expiration des ports ouverts** – Détermine la période après laquelle les listes de ports ouverts seront supprimées de l'écran Détails de l'asset en l'absence de signal indiquant que le port est toujours ouvert. Le réglage par défaut est de deux semaines. Pour plus d'informations, voir **Ports ouverts**.

### Requêtes ping

L'activation des requêtes Ping active la réponse automatique de la plateforme Tenable.ot aux requêtes Ping.

#### ➡ Pour activer les requêtes Ping :

1. Accédez à l'écran **Paramètres locaux** > **Configuration système** > **Appareils**.
2. **Activez** le curseur **Requêtes Ping**.

### Captures 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 approfondie. Lorsque la capacité de stockage est dépassée (1,8 To), le système supprime les anciens fichiers. Vous pouvez afficher et télécharger les fichiers disponibles sur l'écran **Réseau** > **Captures de paquets**, voir la section **Captures de paquets**.

#### ➡ Pour activer les captures de paquets :

1. Accédez à l'écran **Paramètres locaux** > **Configuration système** > **Appareils**.
2. **Activez** le curseur **Capture de paquets**.

Vous pouvez arrêter la fonction de capture de paquets à tout moment en **désactivant** 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 aucune mesure supplémentaire prise par l'administrateur. Si cette option n'est pas sélectionnée, une approbation manuelle finale est requise pour que tout nouveau capteur se connecte à votre réseau.

**Pour activer l'approbation automatique pour les demandes d'appairage de capteur entrantes :**

1. Accédez à l'écran **Paramètres locaux** > **Configuration système** > **Appareils**.
2. **Activez** le curseur **Approuver automatiquement les demandes d'appairage des capteurs**.

Vous pouvez interrompre à tout moment l'approbation automatique des demandes d'appairage entrantes des capteurs en **désactivant** le curseur.

### Activer les statistiques d'utilisation

L'option Activer les statistiques d'utilisation précise si Tenable collecte des données de télémétrie anonymes sur votre déploiement Tenable.ot. 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 informations personnelles identifiables (IPI). Les informations de télémétrie comprennent, sans s'y limiter, des 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 de Tenable.ot 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 les statistiques d'utilisation :**

1. Accédez à l'écran **Paramètres locaux** > **Configuration système** > **Appareils**.
2. **Activez** le curseur **Activer les statistiques d'utilisation**.

Vous pouvez désactiver le partage des statistiques d'utilisation à tout moment en **désactivant** le curseur.

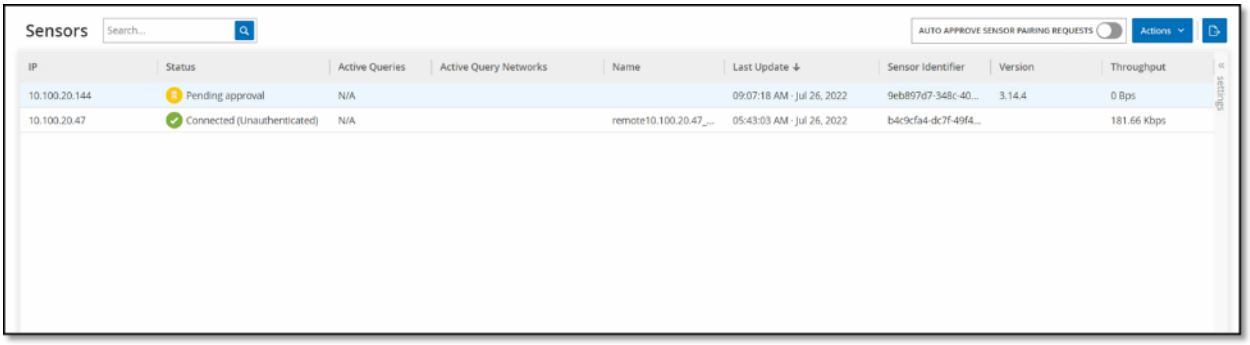
### Capteurs

Une fois que les capteurs ont été appairés à l'aide de l'interface utilisateur de Tenable Core, vous pouvez approuver les nouveaux appairages, mais aussi 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.

Les modèles de capteurs antérieurs à la version 2.214 n'apparaîtront pas sur la page **Capteurs** ICP. Cependant, ils peuvent toujours être utilisés en mode non authentifié.

## Affichage de l'écran des capteurs

Le tableau Capteurs affiche une liste de tous les capteurs v. 2.214 et ultérieure sur le système.




Les informations affichées sur cet écran sont décrites dans le tableau suivant :

| Paramètre | Description |
|---|---|
| **IP** | L'adresse IPv4 du capteur. |
| **Statut** | L'état du capteur : Connecté, Connecté (non authentifié), En attente d'approbation, Déconnecté ou En pause. |
| **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. |
| **Identificateur de 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). |

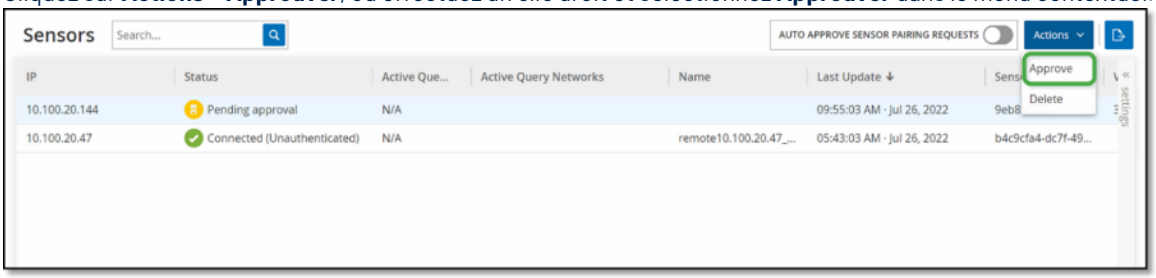
## Approuver manuellement les demandes d'appairage entrantes des capteurs

Si le paramètre **Approuver automatiquement les demandes d'appairage des capteurs** est **désactivé**, les demandes d'appairage entrantes des capteurs doivent être approuvées manuellement avant toute connexion.

### Pour approuver manuellement une demande d'appairage entrante des capteurs :

1. Accédez à l'écran **Paramètres locaux** > **Configuration système** > **Capteurs**.
2. Cliquez sur une ligne du tableau dont le statut est **En attente d'approbation**.

3. Cliquez sur **Actions** > **Approuver**, ou effectuez un clic droit et sélectionnez **Approuver** dans le menu contextuel.




Pour supprimer un capteur, cliquez sur **Actions** > **Supprimer**, ou effectuez un clic droit et sélectionnez **Supprimer** dans le menu contextuel.

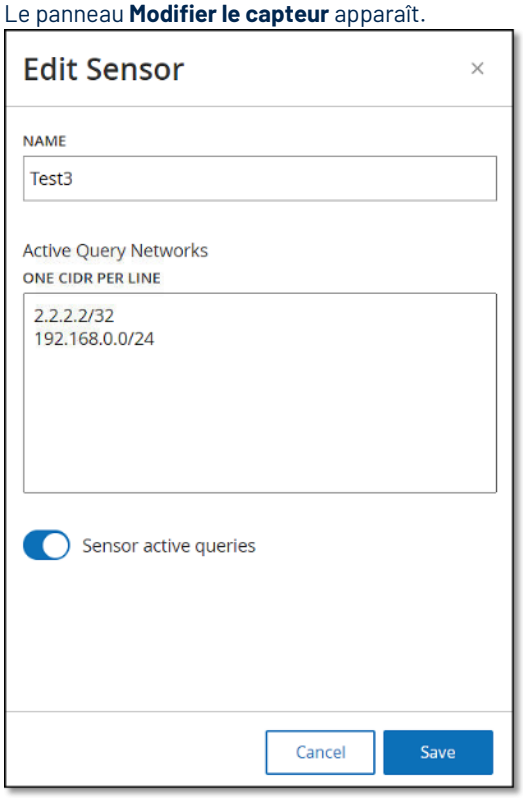
## Configuration des requêtes actives

Une fois qu'un capteur est connecté en mode *authentifié*, il peut être configuré pour effectuer des requêtes actives dans les segments réseau auxquels il est affecté. Vous devez spécifier les segments réseau qu'il interrogera.

Les capteurs effectueront une détection de réseau passive sur tous les segments disponibles indépendamment de cette configuration.

### Pour configurer les requêtes actives :

1. Sous **Paramètres locaux**, accédez à **Configuration système** > **Capteurs**.
2. Cliquez sur une ligne du tableau dont le statut est **Connecté**.
3. Cliquez sur **Actions** > **Modifier**, ou effectuez un clic droit et sélectionnez **Modifier** dans le menu contextuel.
   Le panneau **Modifier le capteur** apparaît.



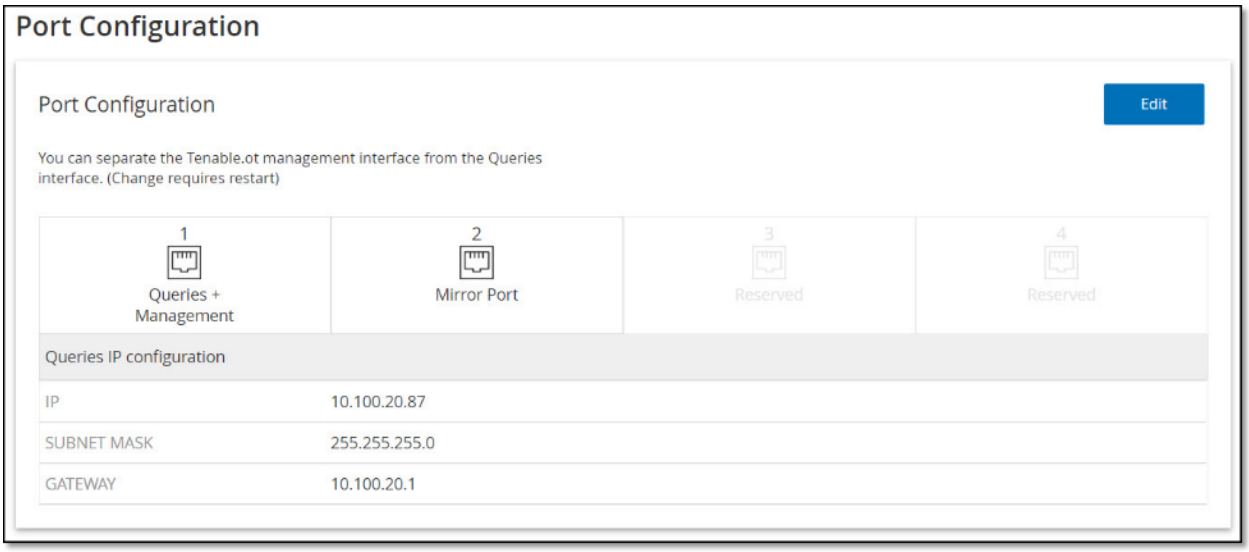
4. Pour renommer le capteur, modifiez le texte dans le champ **Nom**.
5. Dans le champ **Réseau de requêtes actives**, ajoutez ou modifiez les segments réseau pertinents auxquels le capteur enverra des requêtes actives, en utilisant la notation CIDR et en ajoutant chaque sous-réseau sur une ligne distincte.

> Les requêtes ne peuvent être effectuées que sur les CIDR inclus dans les plages de réseau surveillées. Assurez-vous d'ajouter uniquement les CIDR accessibles via ce capteur. L'ajout de CIDR qui ne sont pas accessibles peut interférer avec la capacité de l'ICP à interroger ces segments par d'autres moyens.

6. **Activez** le curseur **Requêtes actives du capteur** pour activer les requêtes actives.
7. Cliquez sur **Enregistrer**.
   Le panneau se referme.
   Dans le tableau **Capteurs**, sous l'en-tête **Requêtes actives**, les capteurs activés afficheront désormais **Activé**.

## Configuration des ports

L'écran **Configuration des ports** montre la manière dont les ports de l'appareil sont configurés. Pour plus d'informations sur la configuration des ports, voir **Installation de l'appliance Tenable.ot** > **Étape 4 – Assistant de configuration** > **Écran 2 – Appareil**.




## Mises à jour

La mise à jour des plug-ins et de l'ensemble de règles du moteur IDS garantit que vos assets sont surveillés pour toutes les dernières vulnérabilités connues. Les mises à jour peuvent être effectuées via le cloud, à la fois automatiquement et manuellement, et peuvent également être effectuées hors ligne.

> Les mises à jour peuvent également être effectuées à partir de l'écran **Vulnérabilités** en cliquant sur le bouton **Mettre à jour les plug-ins**.

> Si la licence utilisateur expire, l'option de téléchargement de nouvelles mises à jour sera bloquée et l'utilisateur ne pourra pas mettre à jour ses plug-ins.

## Mises à jour de l'ensemble de plug-ins Nessus

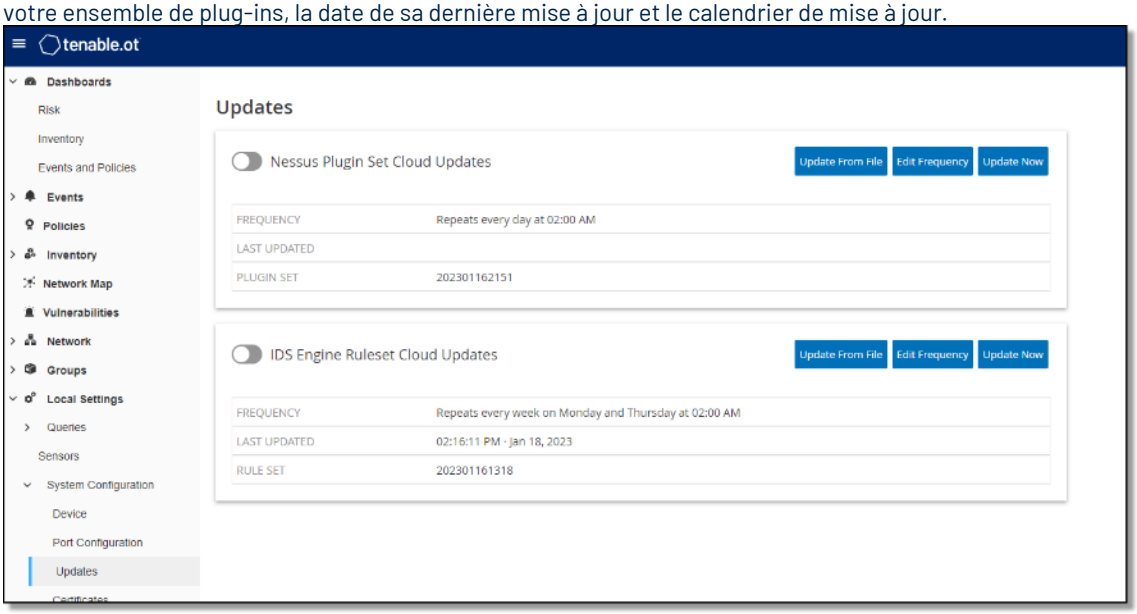
### Mises à jour cloud

Les utilisateurs disposant d'une connexion Internet peuvent mettre à jour les plug-ins via le cloud. Lorsque les mises à jour automatiques sont activées, les plug-ins seront mis à jour à l'heure et selon la fréquence définies par l'utilisateur (par défaut : tous les jours à 02h00).

*Configuration des mises à jour cloud automatiques des plug-ins*

**Pour activer les mises à jour automatiques des plug-ins :**

1. Sous **Paramètres locaux**, accédez à **Configuration système** > **Mises à jour**.
   L'écran **Mises à jour** apparaît avec **Mises à jour cloud de l'ensemble de plug-ins Nessus**, indiquant le numéro de votre ensemble de plug-ins, la date de sa dernière mise à jour et le calendrier de mise à jour.

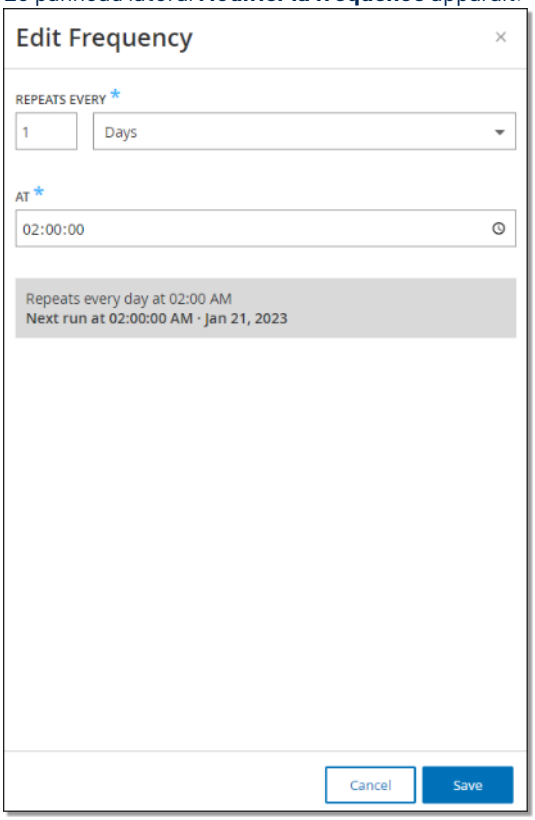



2. Si le curseur en regard est « désactivé », cliquez dessus pour activer les mises à jour automatiques.

**Pour modifier le calendrier des mises à jour automatiques des plug-ins :**

1. Sous **Paramètres locaux**, accédez à **Configuration système** > **Mises à jour**.
   L'écran **Mises à jour** apparaît avec **Mises à jour cloud de l'ensemble de plug-ins Nessus**, indiquant le numéro de votre ensemble de plug-ins, la date de sa dernière mise à jour et le calendrier de mise à jour.

2. Cliquez sur le bouton **Modifier la fréquence**.
   Le panneau latéral **Modifier la fréquence** apparaît.




3. Sous **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.
4. Si vous sélectionnez **Semaines**, sélectionnez le ou les jours de la semaine où vous souhaitez effectuer une mise à jour hebdomadaire des plug-ins.
5. Sous **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.
6. Cliquez sur **Enregistrer**.
   Une boîte de dialogue apparaît, vous informant 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. Sous **Paramètres locaux**, accédez à **Configuration système** > **Mises à jour**.
   L'écran **Mises à jour** apparaît avec **Mises à jour cloud de l'ensemble de plug-ins Nessus**, indiquant la dernière version mise à jour de votre ensemble de plug-ins, la date de sa dernière mise à jour et le calendrier de mise à jour.
2. Cliquez sur le bouton **Mettre à jour maintenant**.
   Une boîte de dialogue apparaît, vous informant que la fréquence a bien été mise à jour. Une fois la mise à jour terminée, le champ **Ensemble de plug-ins** affichera le numéro de l'ensemble de plug-ins actuel.

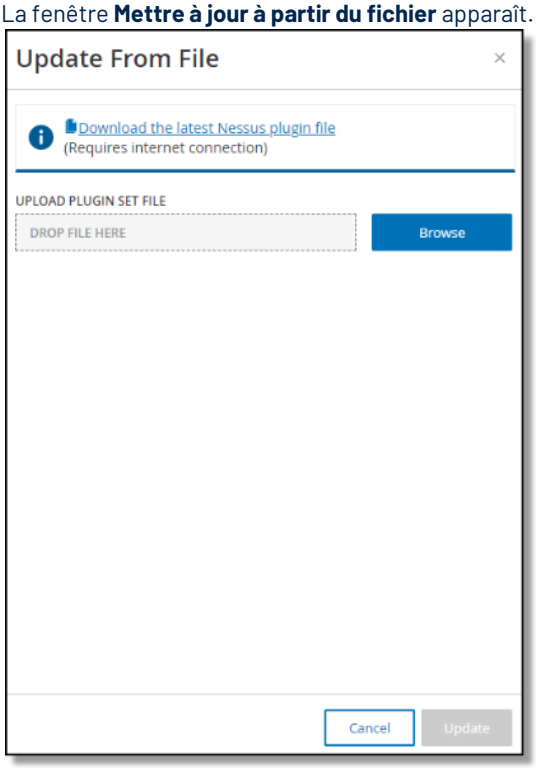
> Pendant que la mise à jour de l'ensemble de plug-ins est en cours, gardez la fenêtre du navigateur ouverte et n'actualisez pas la page.

## Mises à jour hors ligne

Les utilisateurs sans connexion Internet sur leur appareil Tenable.ot peuvent mettre à jour manuellement leurs plug-ins en téléchargeant le dernier ensemble de plug-ins depuis le portail client de Tenable puis en chargeant le fichier.

### Pour mettre à jour les plug-ins sans connexion Internet :

1. Sous **Paramètres locaux**, accédez à **Configuration système** > **Mises à jour**.
   L'écran **Mises à jour** apparaît avec **Mises à jour cloud de l'ensemble de plug-ins Nessus**, indiquant le numéro de votre ensemble de plug-ins, la date de sa dernière mise à jour et le calendrier de mise à jour.
2. Cliquez sur le bouton **Mettre à jour à partir du fichier**.
   La fenêtre **Mettre à jour à partir du fichier** apparaît.




3. Si vous ne l'avez pas encore fait, cliquez sur le lien pour télécharger le dernier fichier de plug-in, puis revenez à la fenêtre **Mettre à jour à partir du fichier**.

> 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 Tenable.ot.
5. Cliquez sur **Mettre à jour**.

## Mises à jour de l'ensemble de règles du moteur IDS

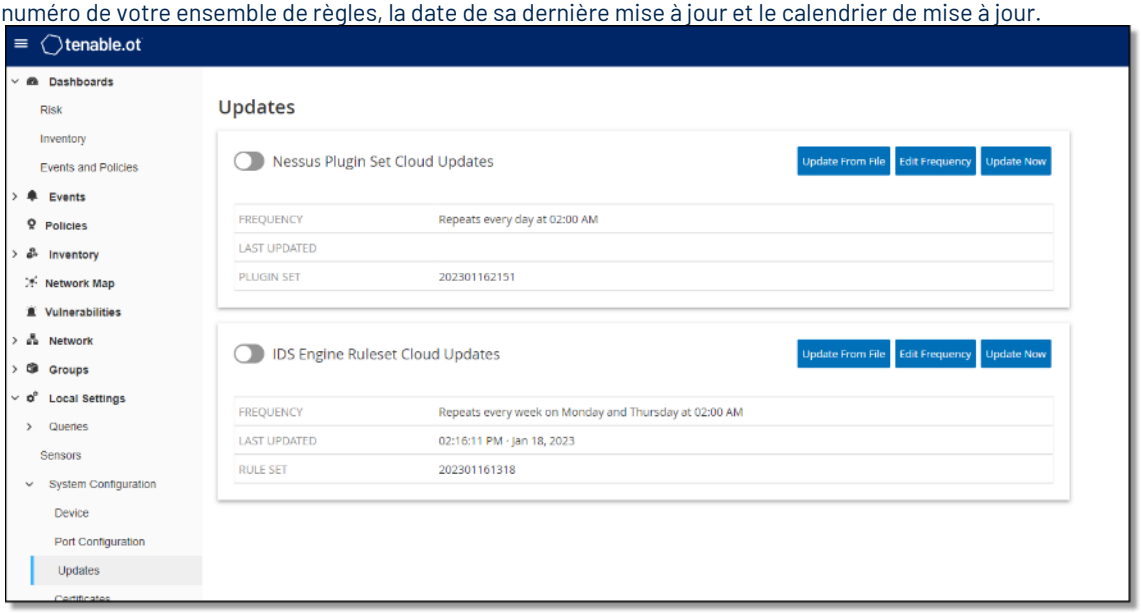
### Mises à jour cloud

Les utilisateurs disposant d'une connexion Internet peuvent mettre à jour leur ensemble de règles (Ruleset) du moteur IDS via le cloud. Lorsque les mises à jour automatiques sont activées, l'ensemble de règles du moteur IDS sera mis à jour à l'heure et selon la fréquence définies par l'utilisateur (par défaut : toutes les semaines, le mardi et le jeudi à 02h00).

*Configuration des 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. Sous **Paramètres locaux**, accédez à **Configuration système** > **Mises à jour**.
   L'écran **Mises à jour** apparaît avec **Mises à jour cloud de l'ensemble de règles du moteur IDS**, indiquant le numéro de votre ensemble de règles, la date de sa dernière mise à jour et le calendrier de mise à jour.

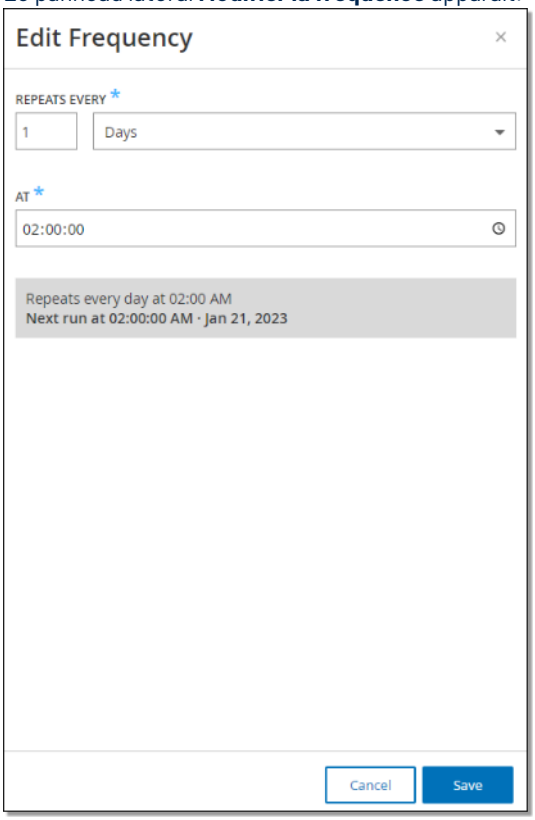



2. Si le curseur en regard est « désactivé », cliquez dessus pour activer les mises à jour automatiques.

**➡ Pour modifier le calendrier de mises à jour automatiques de l'ensemble de règles du moteur IDS :**

1. Sous **Paramètres locaux**, accédez à **Configuration système** > **Mises à jour**.
   L'écran **Mises à jour** apparaît avec **Mises à jour cloud de l'ensemble de règles du moteur IDS**, indiquant le numéro de votre ensemble de règles, la date de sa dernière mise à jour et le calendrier de mise à jour.

2. Cliquez sur le bouton **Modifier la fréquence**.
   Le panneau latéral **Modifier la fréquence** apparaît.




3. Sous **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.
4. 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.
5. Sous **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.
   Cliquez sur **Enregistrer**.
   Une boîte de dialogue apparaît, vous informant que la fréquence a bien été mise à jour.

*Mise à jour manuelle de l'ensemble de règles du moteur IDS via le cloud*

### Pour mettre à jour manuellement l'ensemble de règles du moteur IDS :

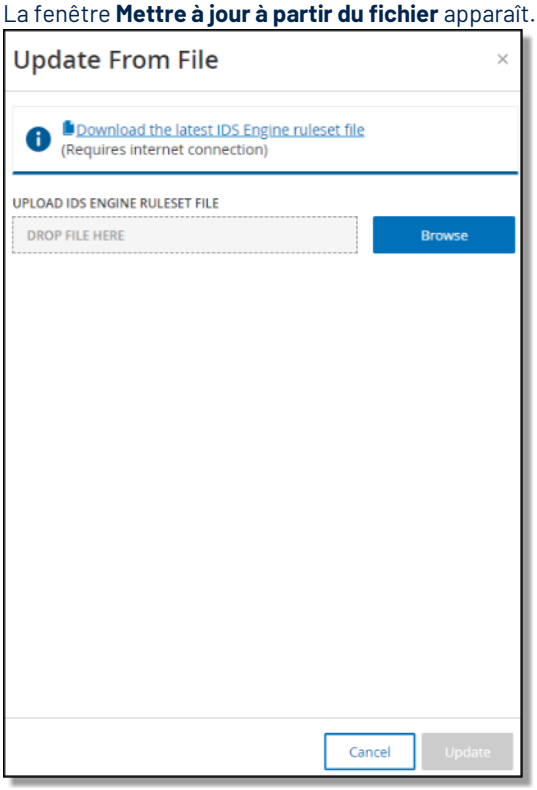
1. Sous **Paramètres locaux**, accédez à **Configuration système** > **Mises à jour**.
   L'écran **Mises à jour** apparaît avec **Mises à jour cloud de l'ensemble de règles du moteur IDS**, indiquant le numéro de votre ensemble de règles, la date de sa dernière mise à jour et le calendrier de mise à jour.
2. Cliquez sur le bouton **Mettre à jour maintenant**.
   Une boîte de dialogue apparaît, vous informant que la fréquence a bien été mise à jour. Une fois la mise à jour terminée, le champ **Ensemble de règles** affichera le numéro de l'ensemble de règles actuel du moteur IDS.

## Mises à jour hors ligne

Les utilisateurs sans connexion Internet sur leur appareil Tenable.ot peuvent mettre à jour manuellement leur 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 sans connexion Internet :

1. Sous **Paramètres locaux**, accédez à **Configuration système** > **Mises à jour cloud de l'ensemble de règles du moteur IDS.**
   L'écran **Mises à jour** apparaît, indiquant le numéro de votre ensemble de règles, la date de sa dernière mise à jour et le calendrier de mise à jour.
2. Cliquez sur le bouton **Mettre à jour à partir du fichier**.
   La fenêtre **Mettre à jour à partir du fichier** apparaît.




3. Si vous ne l'avez pas encore fait, cliquez sur le lien pour télécharger le dernier fichier d'ensemble de règles du moteur IDS.

> 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 Tenable.ot.
5. Cliquez sur **Mettre à jour**.

## Certificat

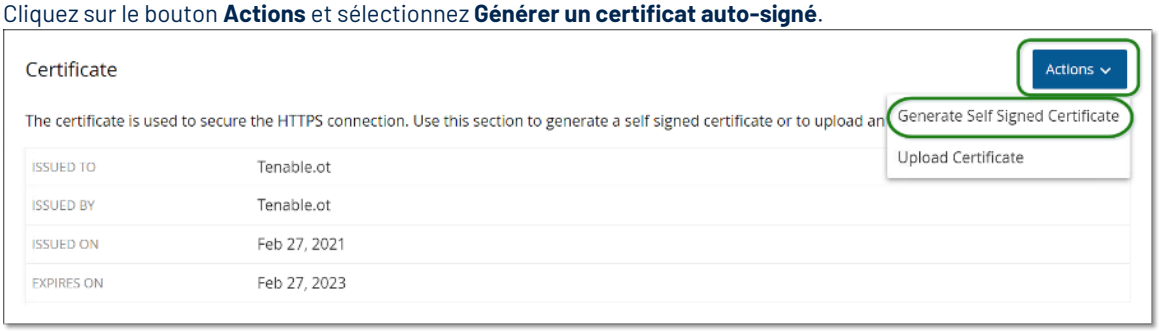
### Génération d'un certificat HTTPS

Le certificat HTTPS garantit que le système utilise une connexion sécurisée à l'appliance et au serveur Tenable.ot.
Le certificat initial expire après deux ans. Vous pouvez générer un nouveau certificat auto-signé à tout moment.
Le nouveau certificat est valable un an.

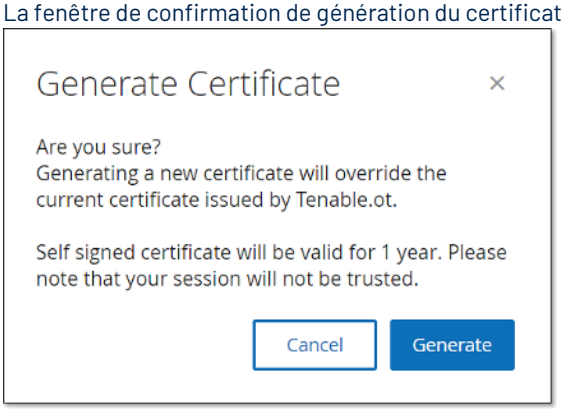
> La génération d'un nouveau certificat remplacera le certificat actuel.

**Pour générer un certificat auto-signé :**

1. Sous **Paramètres locaux**, accédez à l'écran **Configuration système** > **Certificat**.
2. Cliquez sur le bouton **Actions** et sélectionnez **Générer un certificat auto-signé**.




La fenêtre de confirmation de génération du certificat apparaît.




3. Cliquez sur **Générer**.
   Le certificat auto-signé est généré et peut être affiché sur l'écran **Paramètres locaux** > **Configuration système** > **Certificat**.

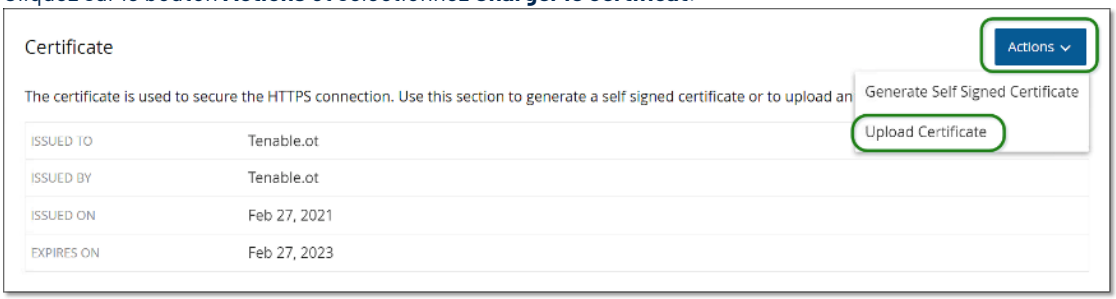
### Chargement d'un certificat HTTPS

En plus de générer un certificat HTTPS auto-signé, les utilisateurs peuvent charger leur propre certificat HTTPS via l'interface utilisateur (Paramètres locaux > Configuration système > Certificat). Le certificat est utilisé pour sécuriser les connexions HTTPS à d'autres appareils, y compris votre navigateur, entre l'ICP et l'IM, etc.

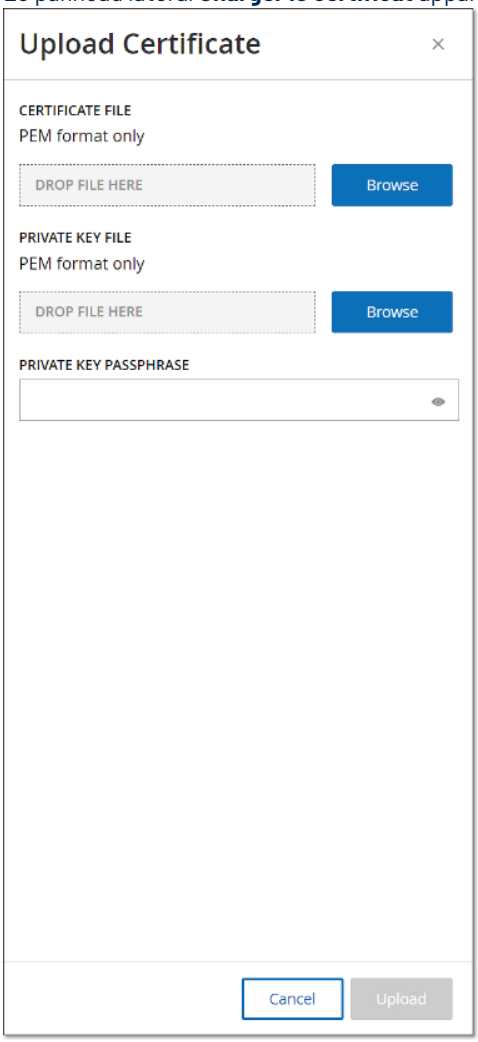
**Pour charger un certificat HTTPS :**

1. Sous **Paramètres locaux**, accédez à l'écran **Configuration système** > **Certificat**.

2. Cliquez sur le bouton **Actions** et sélectionnez **Charger le certificat**.




Le panneau latéral **Charger le certificat** apparaît.




3. Sous **Fichier de certificat**, cliquez sur le bouton **Parcourir** et accédez au fichier de certificat que vous souhaitez charger.
4. Sous **Fichier de clé privée**, cliquez sur le bouton **Parcourir** et accédez au fichier de clé privée que vous souhaitez charger.
5. Saisissez le mot de passe de la clé privée dans le champ **Mot de passe de la clé privée**.
6. Cliquez sur le bouton **Charger** pour importer les fichiers.
   Le panneau latéral se referme.

Après avoir remplacé le certificat, il est recommandé de recharger l'onglet du navigateur pour s'assurer que la mise à jour du certificat HTTP a réussi. Si ce n'est pas le cas, un avertissement apparaîtra.

## Licence

Il peut arriver que vous deviez mettre à jour ou réinitialiser votre licence Tenable.ot. Après avoir contacté votre responsable de compte Tenable, vous devrez suivre l'une des procédures suivantes pour mettre à jour ou réinitialiser votre licence.

### Mise à jour de la licence

Si vous devez mettre à jour votre licence existante (par exemple pour augmenter votre limite d'assets, prolonger votre période de licence ou modifier votre type de licence), suivez la procédure suivante.

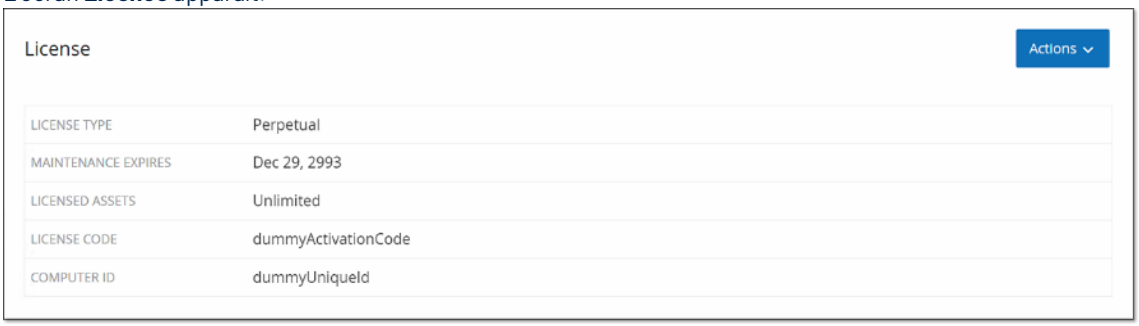
#### Conditions préalables

- Votre responsable de compte Tenable doit déjà avoir mis à jour vos informations de licence dans son système avant que vous puissiez enregistrer la nouvelle licence.
- Vous devez avoir accès à Internet. Si votre appareil Tenable.ot n'est pas connecté à Internet, vous pouvez enregistrer la licence depuis n'importe quel PC.

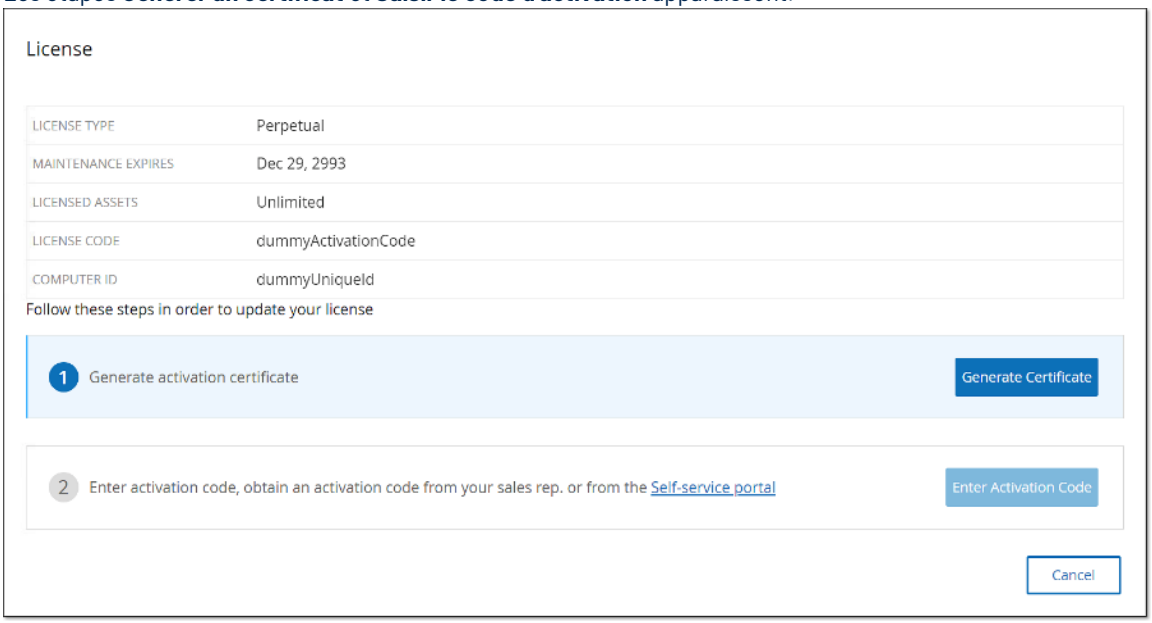
#### Enregistrement d'une nouvelle licence

**Pour enregistrer votre licence :**

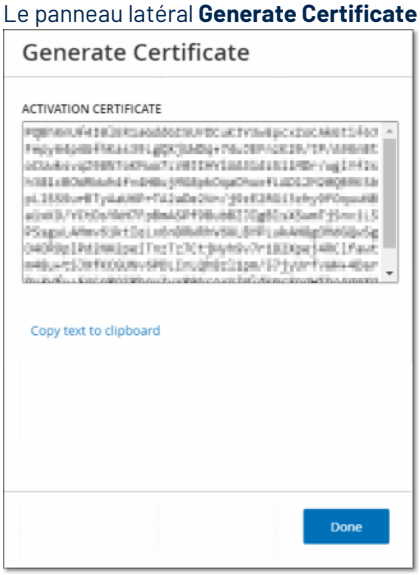
1. Sous **Paramètres locaux**, accédez à **Configuration système** > **Licence**.
   L'écran **Licence** apparaît.



2. Cliquez sur le bouton **Actions** et sélectionnez **Mettre à jour la licence**.
   Les étapes **Générer un certificat** et **Saisir le code d'activation** apparaissent.

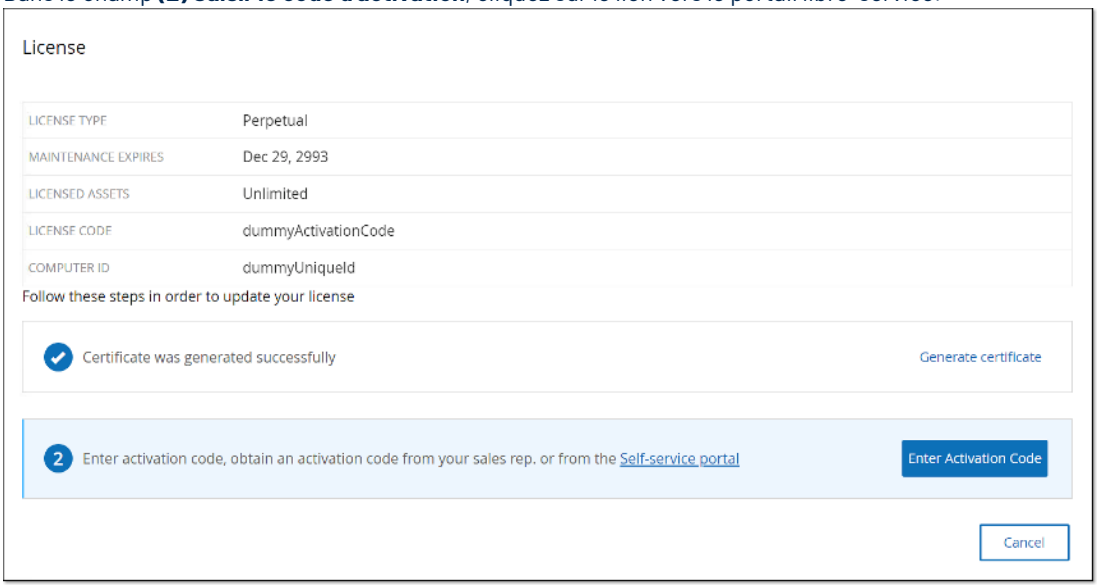



3. Dans le champ **(1) Generate activation certificate** (Générer un certificat d'activation), cliquez sur le bouton **Generate Certificate** (Générer un certificat).
   Le panneau latéral **Generate Certificate** (Générer un certificat) apparaît avec le certificat d'activation.

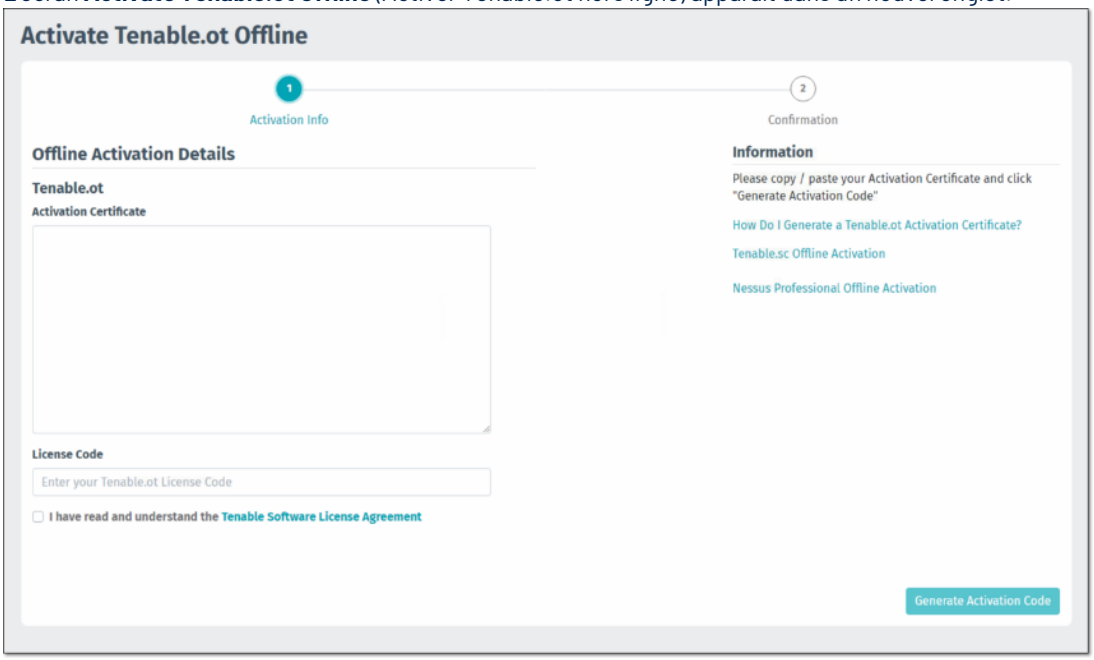



4. Cliquez sur le bouton **Copier le texte dans le presse-papiers**, puis sur **Terminé**.
   Le panneau latéral se referme.

5. Dans le champ **(2) Saisir le code d'activation**, cliquez sur le lien vers le portail libre-service.




L'écran **Activate Tenable.ot Offline** (Activer Tenable.ot hors ligne) apparaît dans un nouvel onglet.

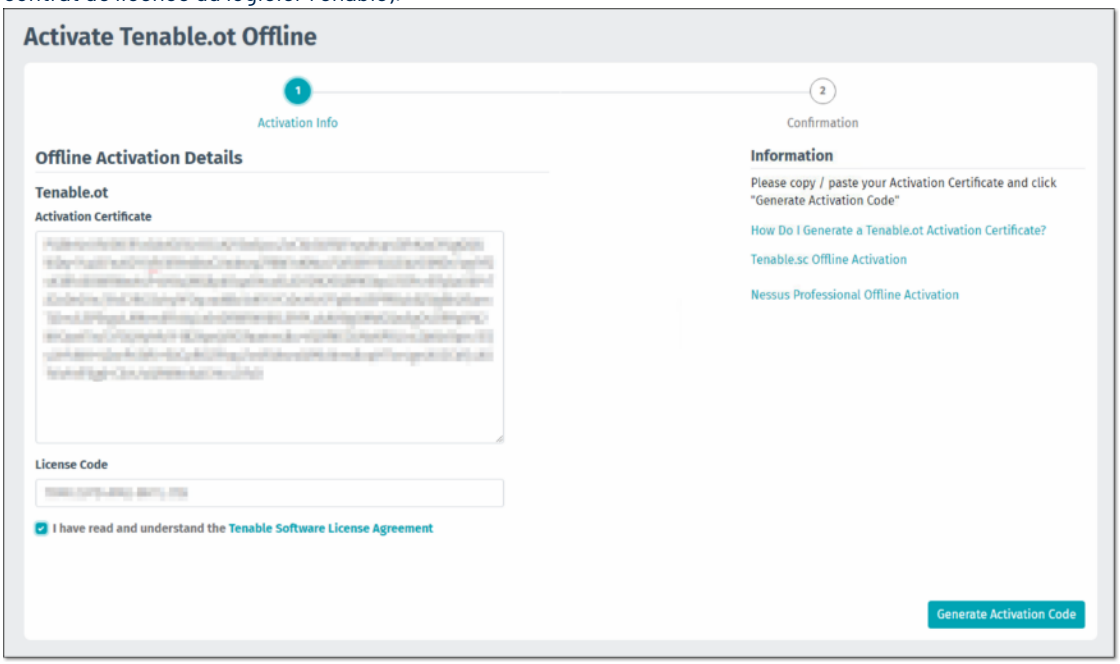



Vous devrez accéder à l'écran Activate Tenable.ot Offline à partir d'un appareil connecté à Internet via l'URL suivante : https://provisioning.tenable.com/activate/offline/tenable-ot.

Si vous n'êtes pas connecté à tenable.com actuellement, vous devez vous connecter à l'aide de votre adresse e-mail et de votre mot de passe. Vous devez utiliser le compte de messagerie sur lequel vous avez reçu votre code de licence.

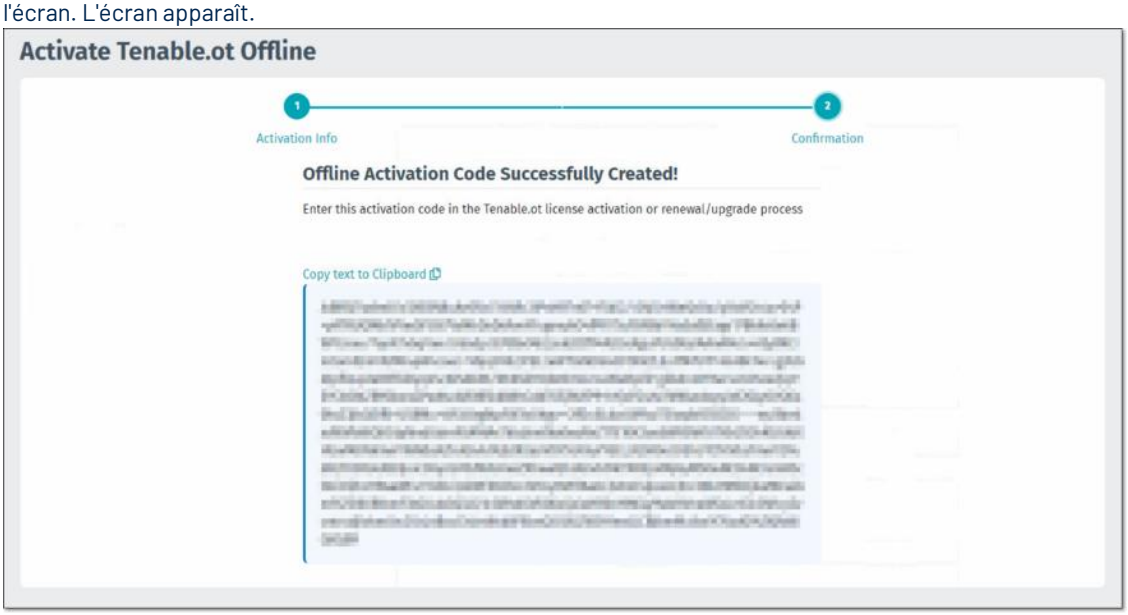
Si vous n'avez pas d'identifiants de connexion, vous pouvez soit cliquer sur **Don't remember your password** (Mot de passe oublié) et suivre les instructions, soit contacter votre responsable de compte Tenable.

6. Dans le champ **Activation Certificate** (Certificat d'activation), saisissez le certificat d'activation.
7. Dans le champ **Licence Code** (Code de licence), saisissez votre **code de licence** à 20 caractères (qui peut être copié et collé à partir de l'écran **Licence**).
8. 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).



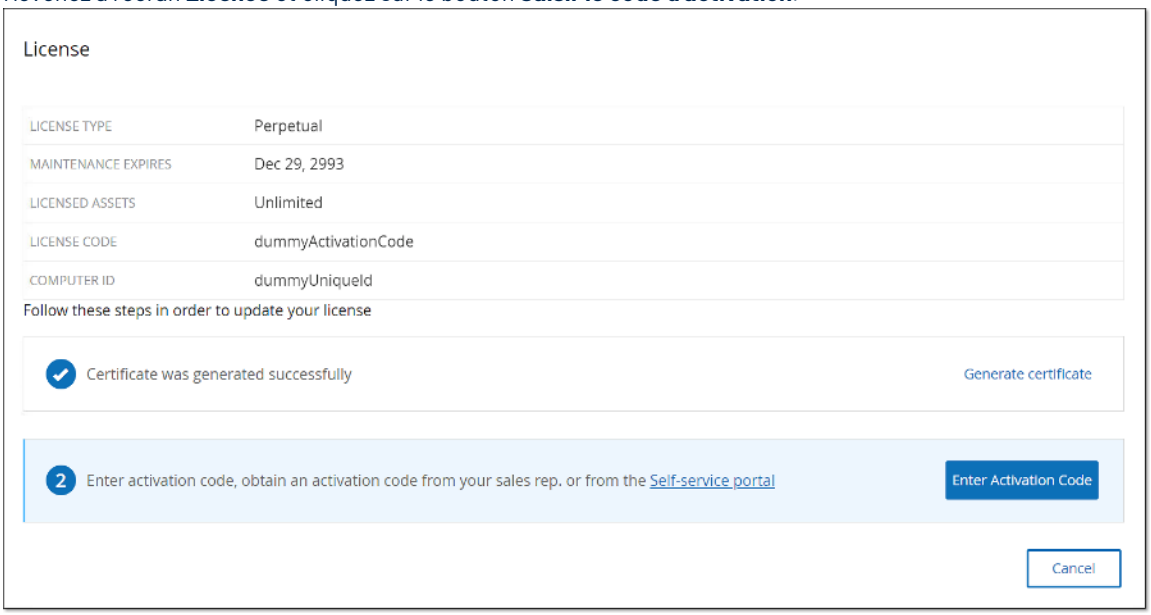

Pour afficher le contrat de licence, cliquez sur le lien **Tenable Software License Agreement** (Contrat de licence du logiciel Tenable).

9. Cliquez sur le bouton **Generate Activation Code** (Générer un code d'activation).
Le message « Offline Activation Code Successfully Created! » (Code d'activation hors ligne créé) apparaît à l'écran. L'écran apparaît.



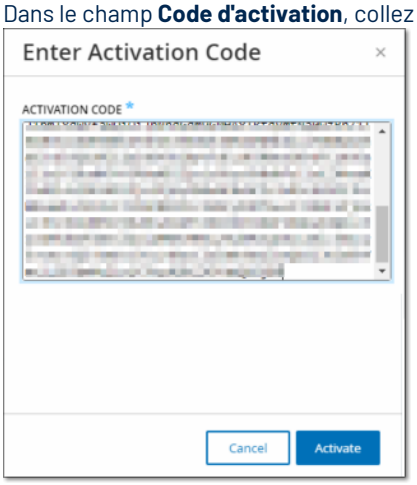

10. Cliquez sur **Copier le texte dans le presse-papiers**.

11. Revenez à l'écran **Licence** et cliquez sur le bouton **Saisir le code d'activation**.




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

12. Dans le champ **Code d'activation**, collez votre code d'activation et cliquez sur le bouton **Activer**.




Le panneau latéral se referme et la licence est mise à jour.

## Réinitialisation de la 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 une nouvelle licence vous a été délivrée), utilisez la procédure suivante.

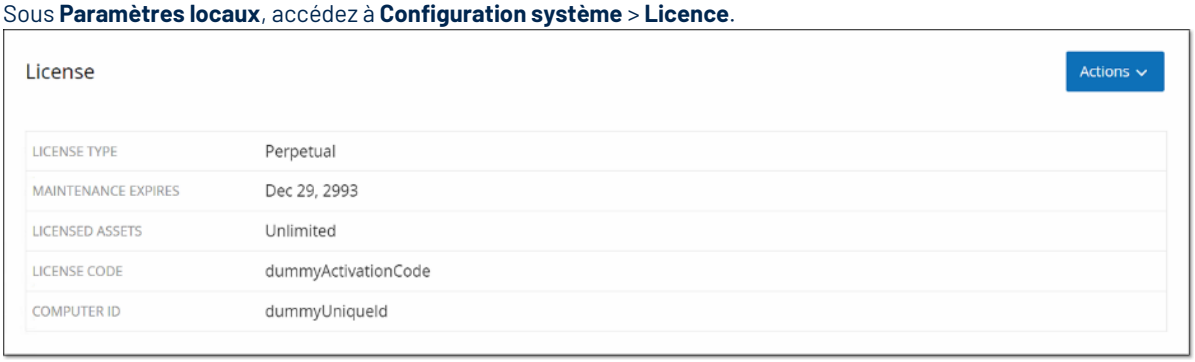
### Conditions préalables

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

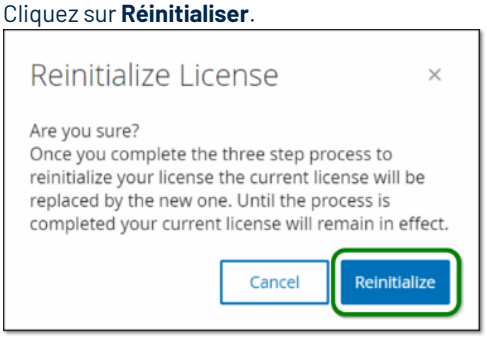
## Réinitialisation d'une licence

### Pour réinitialiser votre licence :

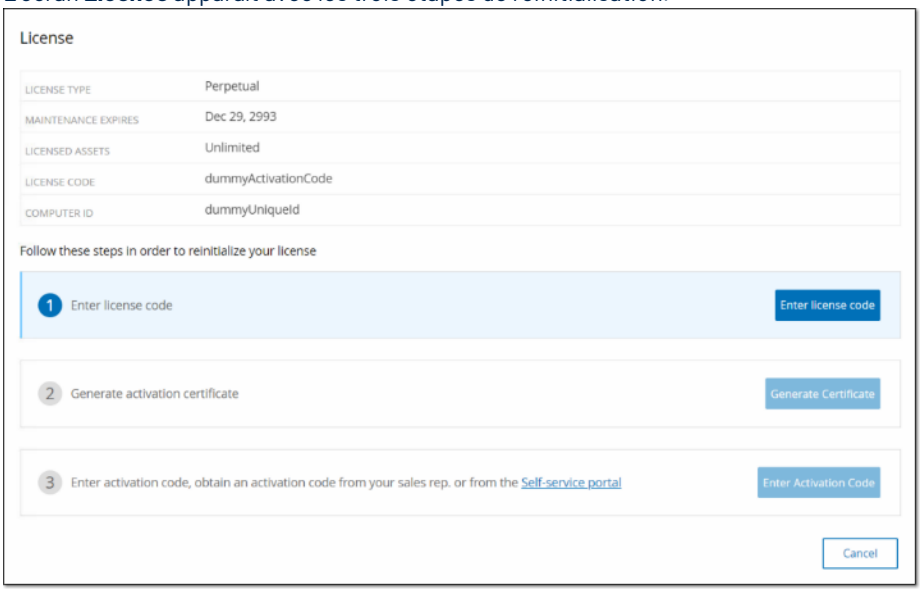
1. Sous **Paramètres locaux**, accédez à **Configuration système** > **Licence**.




   Cliquez sur le bouton **Actions** et sélectionnez **Réinitialiser la licence**.
   Une fenêtre de confirmation apparaît.
2. Cliquez sur **Réinitialiser**.




   L'écran **Licence** apparaît avec les trois étapes de réinitialisation.




3. Suivez les étapes de démarrage du système pour activer votre licence. Voir **Activation de votre licence**.
   Après avoir saisi votre code d'activation, votre licence actuelle sera remplacée par votre nouvelle licence.

### Calcul des licences

Les licences pour les comptes Tenable sont calculées en fonction du nombre d'adresses IP uniques dans le système. Chaque adresse IP nécessite une licence distincte. Ainsi, même si plusieurs appareils partagent les mêmes adresses IP (par exemple, plusieurs appareils connectés au même fond de panier qui partagent les trois mêmes adresses IP), les licences seront toujours basées sur le nombre d'adresses IP, dans ce cas 3 licences, indépendamment du nombre d'appareils.

# Configuration de l'environnement

## Paramètres d'un asset

### Ajouter des assets manuellement

Pour mieux suivre votre inventaire, vous souhaiterez peut-être afficher d'autres assets que vous possédez, même s'ils n'ont pas encore été détectés par Tenable.ot. 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.

Les utilisateurs ne peuvent importer que des assets dont les adresses IP ne sont pas déjà utilisées par un asset existant du système. Si le système détecte un asset communiquant sur le réseau avec la même adresse IP, il utilisera les informations récupérées sur l'asset détecté et écrasera les informations précédemment chargées. Le système commencera alors à voir l'asset comme un élément normal lorsqu'il détectera ses communications sur le réseau.

Les adresses IP des assets importés sont comptabilisées dans la licence du système.

Les assets importés afficheront un score de risque de 0 jusqu'à ce qu'ils soient détectés par le système.

Lorsque des assets sont ajoutés manuellement, leurs événements ne sont pas détectés tant que Tenable.ot n'a pas détecté leur communication sur le réseau.

**Pour ajouter des assets manuellement :**

1. Sous **Paramètres locaux**, accédez à **Configuration de l'environnement** > **Paramètres des assets**. L'écran **Paramètres des assets** apparaît.
2. Dans **Ajouter des assets manuellement**, cliquez sur le bouton **Actions** et sélectionnez **Télécharger le modèle CSV**.
3. Le document modèle tot_Assets est téléchargé.
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 (Nom, Type, etc.) et les valeurs que vous saisissez.
6. Enregistrez le fichier modifié.
7. Revenez à l'écran **Paramètres des assets**.
8. Cliquez sur le bouton **Actions**, sélectionnez **Charger un fichier CSV**, puis accédez au fichier CSV souhaité et ouvrez-le pour l'importer.
9. Dans **Ajouter des assets manuellement,** cliquez sur **Télécharger le rapport**.
   Un fichier CSV avec rapport apparaît, indiquant les réussites et les échecs dans la colonne Result (Résultat). Les détails des erreurs sont affichés dans la colonne Error (Erreur).

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Name | Type | Criticality | IPs | MAC | Family | Model | Firmware | OS | Purdue Le | Location | Descriptic | Result | Error |
| 2 | AAA | Plc | HighCritic | 10.100.20. | aa:bb:cc:d | Siemens | S7300 | 2.3.1 | | Level1 | Italy | Siemens, | Failure | IP 10.100.20.21 already exists |
| 3 | BBB | Server | MediumC | 10.200.30.30 | | VMware | | | Windows Server 2012 | | | | Success | |
| 4 | CCC | Switch | | | AA:bb:cd: | Catalyst | C2960 | 12.3 | | Level3 | | | Success | |
| 5 | DDDD | Unknown | NoneCriticality | | | | | | Linux | Level4 | Israel | | Success | |
| 6 | | | | | | | | | | | | | | |

### Clusters d'événements

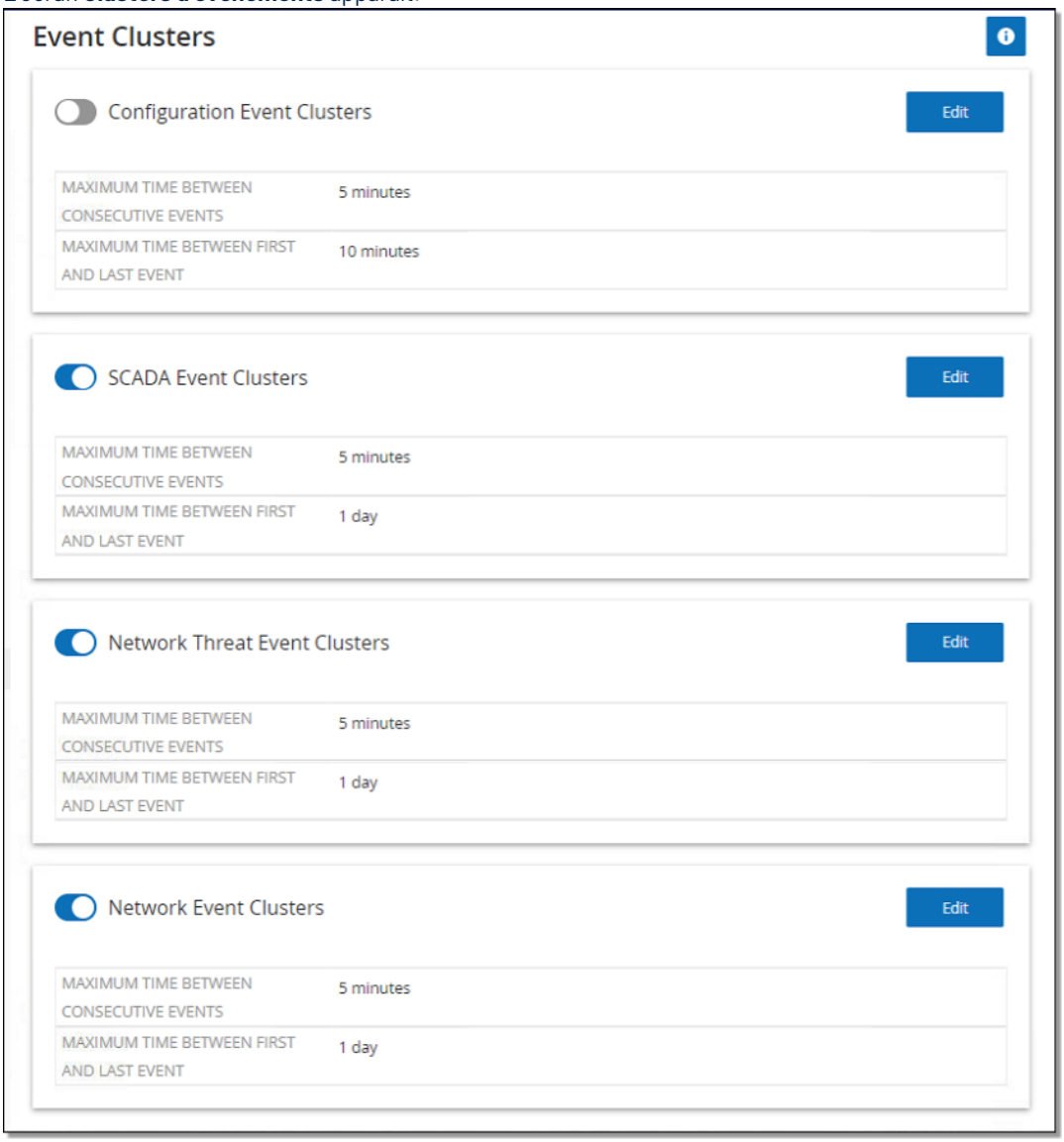
Pour faciliter le suivi des événements, plusieurs événements aux caractéristiques communes sont regroupés pour former un cluster. Le clustering est basé sur le type d'événement (c'est-à-dire ceux qui partagent la même politique), les assets sources et cibles, etc.

Pour que les événements soient regroupés en 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 temps, les événements consécutifs ne seront pas regroupés.
- **Temps maximum entre le premier et le dernier événement** – Définit l'intervalle de temps maximal pour que tous les événements soient affichés sous forme de cluster. Un événement généré après cet intervalle de temps ne fera pas partie du cluster.

#### Pour activer le clustering :

1. Sous **Paramètres locaux**, accédez à **Configuration de l'environnement** > **Clusters d'événements**. L'écran **Clusters d'événements** apparaît.



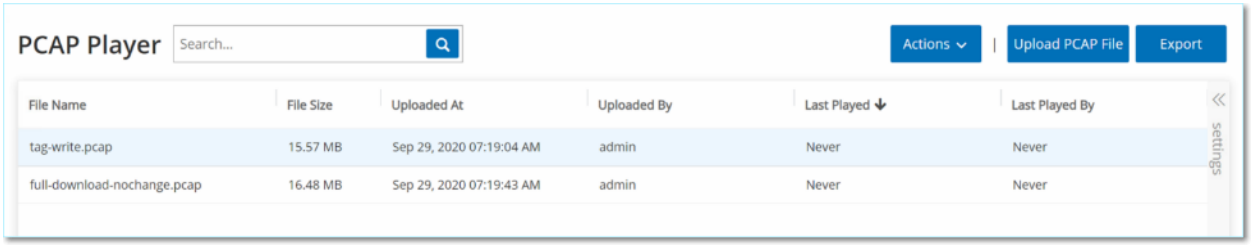

2. Cliquez sur le curseur pour activer les catégories souhaitées pour le clustering.

3. Pour configurer les intervalles de temps pour une catégorie, cliquez sur le bouton **Modifier**.
   La fenêtre de **modification des clusters** apparaît.
4. Saisissez la valeur numérique souhaitée dans le champ numérique et modifiez l'unité de temps à l'aide de la liste déroulante.

> Pour plus d'informations sur le clustering et les intervalles de temps, cliquez sur le bouton .

5. Cliquez sur **Enregistrer**.

## Lecteur PCAP




Tenable.ot vous permet de charger un fichier PCAP contenant l'activité réseau enregistrée et de le « lire » sur Tenable.ot. Lorsque vous « lisez » un fichier PCAP, Tenable.ot surveille le trafic réseau et enregistre toutes les informations sur les assets détectés, l'activité réseau et les vulnérabilités comme si le trafic s'était produit au sein de votre réseau. Cette fonctionnalité peut être utilisée à des fins de simulation ou pour analyser le trafic qui se produit en dehors du réseau surveillé par votre déploiement Tenable.ot (par exemple, des usines distantes).

> Les types de fichiers suivants sont pris en charge pour cette fonctionnalité : .pcap, .pcapng, .pcap.gz, .pcapng.gz. Vous pouvez utiliser des fichiers qui ont été enregistrés par une instance de Tenable.ot ou d'autres outils de surveillance du réseau.

### Charger un fichier PCAP

**Pour charger un fichier PCAP :**

1. Sous **Paramètres locaux**, accédez à **Configuration de l'environnement** > **Lecteur PCAP**.
2. Cliquez sur **Charger le fichier PCAP**.
   L'explorateur de fichiers apparaît.
3. Sélectionnez l'enregistrement PCAP souhaité.
4. Cliquez sur **Ouvrir**.
   Le fichier PCAP est chargé sur le système.

### Lecture d'un fichier PCAP

**Pour lire un fichier PCPAP :**

1. Sous **Paramètres locaux**, accédez à **Configuration de l'environnement** > **Lecteur PCAP**.
2. Sélectionnez l'enregistrement PCAP que vous souhaitez lire.
3. Cliquez sur **Actions** > **Lire**.
4. L'assistant **Lire le PCAP** apparaît.
5. Dans le champ **Vitesse de lecture**, sélectionnez dans la liste déroulante la vitesse à laquelle vous souhaitez que le système lise le fichier. Les options sont : *1X*, *2X*, *4X*, *8X* ou *16X*.

La lecture d'un fichier PCAP injecte des données dans le système, cette opération ne peut pas être annulée ni arrêtée une fois exécutée.

6. Cliquez sur **Lire**.
   Le fichier PCAP est « lu » dans le système. 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.

Vous ne pouvez pas lire un autre fichier PCAP pendant la lecture d'un fichier.

# Utilisateurs et rôles

L'accès à la console de Tenable.ot (IU) est contrôlé par des comptes utilisateur qui désignent les autorisations disponibles pour cet utilisateur. Les autorisations de l'utilisateur sont déterminées par le ou les groupes d'utilisateurs auxquels ils sont affectés. Chaque groupe d'utilisateurs se voit attribuer un rôle qui définit l'ensemble des autorisations qui seront 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 auront 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 *Administrateurs* (Groupe d'utilisateur > Rôle *Administrateur*), *Opérateurs de site* (Groupe d'utilisateur > rôle *Opérateur de site*), etc. Vous pouvez également créer des groupes d'utilisateurs personnalisés et spécifier leurs rôles.

Il existe trois méthodes pour créer des utilisateurs dans le système :

- **Ajouter des utilisateurs locaux** – Créez des comptes utilisateur afin d'autoriser les utilisateurs individuels à accéder au système. Affectez des utilisateurs à des groupes d'utilisateurs qui définissent leurs rôles.
- **Serveurs d'authentification** – Utilisez les serveurs d'authentification de votre organisation (par ex. Active Directory, LDAP) pour autoriser les utilisateurs à accéder au système. Vous pouvez attribuer des rôles Tenable.ot en fonction de vos groupes existants dans Active Directory.
- **SAML** – Configurez une intégration avec votre fournisseur d'identité (par exemple, Azure Active Directory) et affectez des utilisateurs à votre application Tenable.ot.

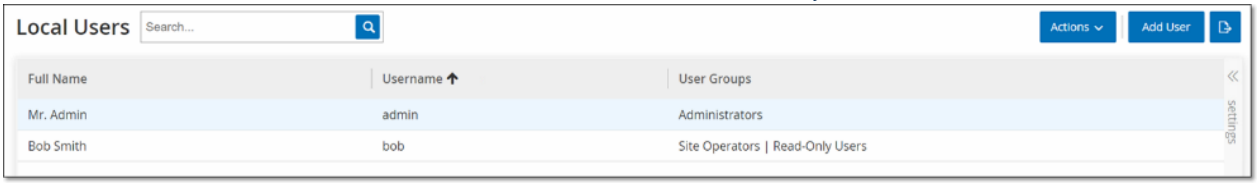
## Utilisateurs locaux

Un utilisateur administrateur peut créer de nouveaux comptes utilisateur et modifier les comptes existants. Chaque utilisateur est affecté à un ou plusieurs groupes d'utilisateurs qui déterminent son ou ses rôles.

Les utilisateurs peuvent être ajoutés aux groupes d'utilisateurs lors de la création/modification de leur compte ou du groupe d'utilisateurs.

### Affichage des utilisateurs locaux

L'écran **Utilisateurs locaux** affiche une liste de tous les utilisateurs locaux du système.



Les informations affichées sur cet écran sont décrites dans le tableau suivant :

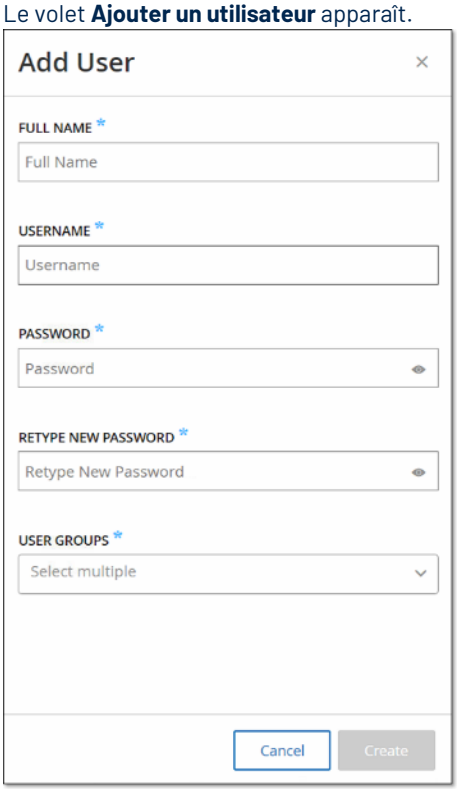
| Paramètre | Description |
|---|---|
| Nom et prénom | Le nom complet de l'utilisateur. |
| Nom d'utilisateur | Le nom d'utilisateur de l'utilisateur, pour la connexion. |
| Groupes d'utilisateurs | Le ou les groupes d'utilisateurs auxquels l'utilisateur est affecté. |

### Ajout d'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. Sous **Paramètres locaux**, accédez à l'écran **Gestion des utilisateurs** > **Utilisateurs locaux**.
2. Cliquez sur le bouton **Ajouter un utilisateur**.
   Le volet **Ajouter un utilisateur** apparaît.




3. Dans le champ **Nom complet**, saisissez vos prénom et nom de famille.

> Le nom que vous saisissez apparaît dans la barre d'en-tête lorsque l'utilisateur est connecté.

4. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur pour vous connecter au système.
5. Dans le champ **Mot de passe**, saisissez un mot de passe.
6. Dans le champ **Confirmer le mot de passe**, ressaisissez le même mot de passe.

> Il s'agit du mot de passe que l'utilisateur utilisera pour la première connexion. L'utilisateur peut modifier le mot de passe sur l'écran **Paramètres** après s'être connecté au système.

7. Cliquez sur le champ **Groupes d'utilisateurs** et cochez la case de chaque groupe d'utilisateurs auquel vous souhaitez affecter cet utilisateur.

> Le système est livré avec un ensemble de groupes d'utilisateurs pré-définis, correspondant à chacun des rôles disponibles, à savoir *Administrateurs* (Groupe d'utilisateurs > rôle *Administrateur*), *Opérateurs de site* (Groupe d'utilisateur > rôle *Opérateur de site*), etc. Pour une explication des rôles disponibles, voir **Rôles d'utilisateur**.

8. Cliquez sur **Créer**.
   Le nouveau compte utilisateur est créé dans le système et est ajouté à la liste des utilisateurs affichée 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.

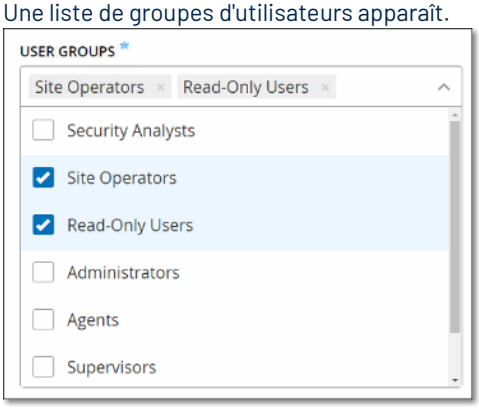
**Pour modifier les groupes utilisateur d'un utilisateur :**

1. Sous **Paramètres locaux**, accédez à l'écran **Gestion des utilisateurs** > **Utilisateurs locaux**.
   L'écran **Utilisateurs locaux** apparaît.
2. Effectuez un clic droit sur l'utilisateur souhaité et sélectionnez **Modifier l'utilisateur** dans le menu.

> Vous pouvez également sélectionner un utilisateur, puis cliquer sur le bouton **Actions** > **Modifier l'utilisateur**.

3. Le volet **Modifier l'utilisateur** apparaît, indiquant les groupes d'utilisateurs auxquels l'utilisateur est affecté.

4. Cliquez sur le champ **Groupes d'utilisateurs**.
   Une liste de groupes d'utilisateurs apparaît.




5. Sélectionnez/désélectionnez les groupes d'utilisateurs souhaités.
6. Cliquez sur **Enregistrer**.

## Modification du mot de passe d'un utilisateur

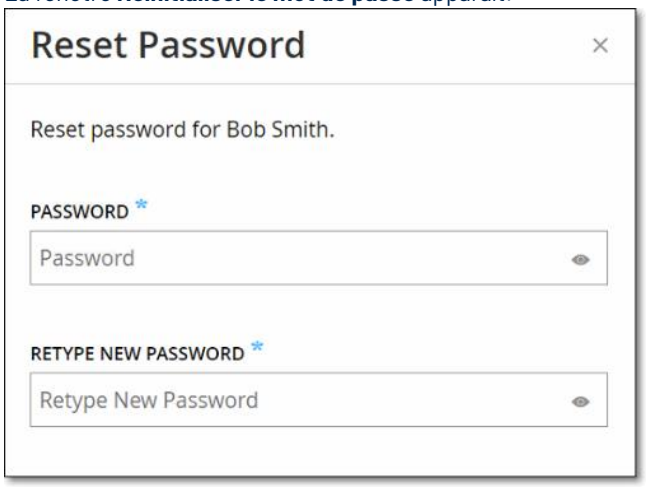
> La procédure décrite ci-dessous est prévue pour qu'un utilisateur administrateur puisse modifier le mot de passe de n'importe quel compte du système. Tout utilisateur peut modifier son propre mot de passe en accédant à **Paramètres locaux** > **Gestion des utilisateurs**.

### Pour modifier le mot de passe d'un utilisateur :

1. Sous **Paramètres locaux**, accédez à l'écran **Gestion des utilisateurs** > **Utilisateurs locaux**.
   L'écran **Utilisateurs locaux** apparaît.
2. Effectuez un clic droit sur l'utilisateur souhaité et sélectionnez **Réinitialiser le mot de passe** dans le menu.

> Vous pouvez également sélectionner un utilisateur, puis cliquer sur le bouton **Actions** > **Réinitialiser le mot de passe**.

La fenêtre **Réinitialiser le mot de passe** apparaît.




3. Dans le champ **Nouveau mot de passe**, saisissez un nouveau mot de passe.
4. Dans le champ **Confirmer le nouveau mot de passe**, ressaisissez le même nouveau mot de passe.
5. Cliquez sur **Réinitialiser**.
   Le nouveau mot de passe est appliqué au compte utilisateur spécifié.

### Suppression d'utilisateurs locaux

**Pour supprimer un compte utilisateur :**

1. Sous **Paramètres locaux**, accédez à l'écran **Gestion des utilisateurs** > **Utilisateurs locaux**.
   L'écran **Utilisateurs locaux** apparaît.
2. Effectuez un clic droit sur l'utilisateur souhaité et sélectionnez **Supprimer l'utilisateur** dans le menu.

> Vous pouvez également sélectionner un utilisateur, puis cliquer sur le bouton **Actions** > **Supprimer l'utilisateur**.

   Une fenêtre de confirmation apparaît.
3. Cliquez sur **Supprimer**.
   Le compte utilisateur est supprimé du système.

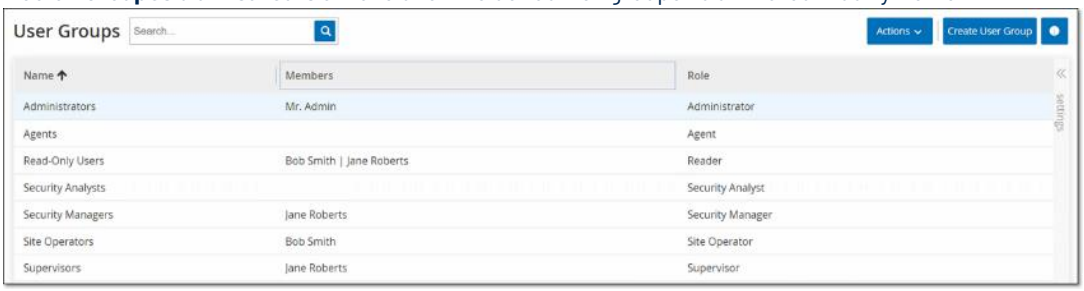
## Groupes d'utilisateurs

Un utilisateur administrateur peut créer de nouveaux groupes d'utilisateurs et modifier les groupes existants. Chaque utilisateur est affecté à un ou plusieurs groupes d'utilisateurs qui déterminent son ou ses rôles.

Le système est livré avec un ensemble de groupes d'utilisateurs pré-définis, correspondant à chacun des rôles disponibles, à savoir *Administrateurs* (Groupe d'utilisateurs > rôle *Administrateur*), *Opérateurs de site* (Groupe d'utilisateur > rôle *Opérateur de site*), etc. Pour une explication des rôles disponibles, voir **Rôles d'utilisateur**.

### Affichage des groupes d'utilisateurs

L'écran **Groupes d'utilisateurs** affiche une liste de tous les groupes d'utilisateurs du système.




Les informations affichées sur cet écran sont décrites dans le tableau suivant :

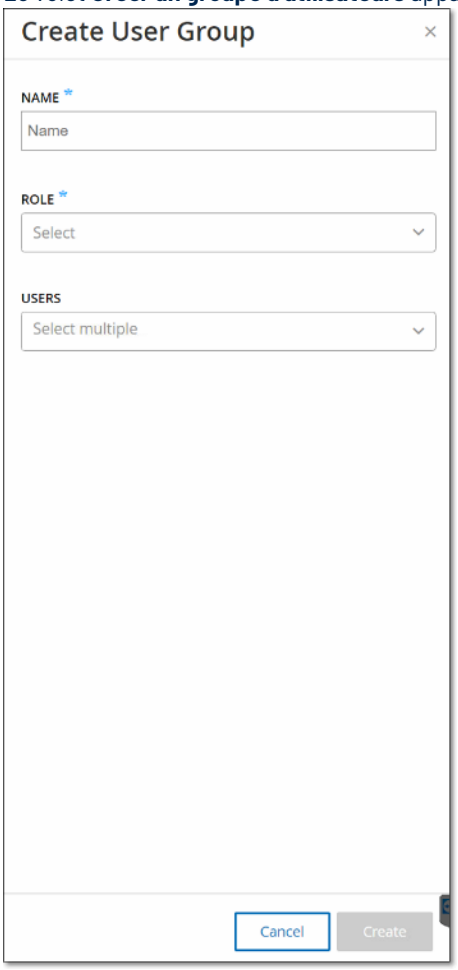
| Paramètre | Description |
|---|---|
| **Nom** | Le nom du groupe d'utilisateurs. |
| **Membres** | Une liste de tous les membres affectés au groupe. |
| **Rôle** | Le rôle donné à ce groupe. Pour une explication des autorisations associées à chaque rôle, voir **Tableau des rôles d'utilisateur**. |

## Ajout de groupes d'utilisateurs

Vous pouvez créer des groupes d'utilisateurs et affecter des utilisateurs à ce groupe.

### Pour créer un compte utilisateur :

1. Sous **Paramètres locaux**, accédez à l'écran **Gestion des utilisateurs** > **Groupes d'utilisateurs**.
   L'écran **Groupes d'utilisateurs** apparaît.
2. Cliquez sur le bouton **Créer un groupe d'utilisateurs**.
   Le volet **Créer un groupe d'utilisateurs** apparaît.




3. Dans le champ **Nom**, saisissez un nom pour ce groupe.
4. Dans le champ **Rôle**, sélectionnez dans la liste déroulante le rôle que vous souhaitez affecter à ce groupe.
5. Dans le champ **Utilisateurs**, sélectionnez dans la liste déroulante un ou plusieurs utilisateurs que vous souhaitez affecter à ce groupe.
6. Cliquez sur **Créer**.
   Le nouveau groupe d'utilisateurs est créé dans le système et est ajouté à la liste des groupes affichée sur l'écran **Groupes d'utilisateurs**.

## Actions supplémentaires sur les groupes d'utilisateurs

### Modification de groupes d'utilisateurs

Vous pouvez modifier les paramètres, ajouter ou supprimer des membres à un groupe d'utilisateurs existant en modifiant le groupe.

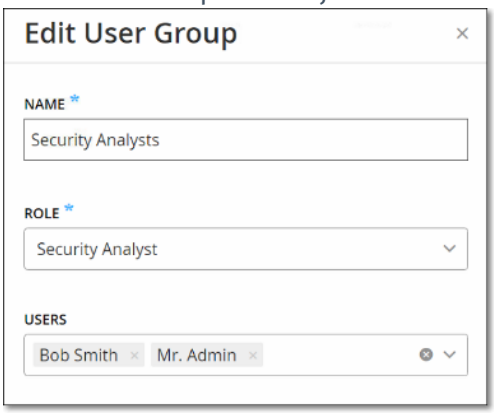
Vous pouvez également sélectionner un utilisateur, puis cliquer sur le bouton **Actions** > **Supprimer l'utilisateur**.

### Pour modifier un groupe d'utilisateurs :

1. Sous **Paramètres locaux**, accédez à l'écran **Gestion des utilisateurs** > **Groupes d'utilisateurs**. L'écran **Groupes d'utilisateurs** apparaît.
2. Effectuez un clic droit sur l'utilisateur souhaité et sélectionnez **Modifier le groupe d'utilisateurs** dans le menu.

Vous pouvez également sélectionner un utilisateur, puis cliquer sur le bouton Actions > Modifier le groupe d'utilisateurs.

3. Le volet **Modifier les groupes d'utilisateurs** apparaît, indiquant les paramètres du groupe.
4. Vous pouvez modifier le **nom** et le **rôle**. Vous pouvez également sélectionner/désélectionner des **utilisateurs** pour les ajouter ou les supprimer du groupe.




5. Cliquez sur **Enregistrer**.

## Supprimer des groupes d'utilisateurs

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 devrez d'abord retirer les utilisateurs du groupe avant de pouvoir le supprimer.

### Pour supprimer un groupe d'utilisateurs :

1. Sous **Paramètres locaux**, accédez à l'écran **Gestion des utilisateurs** > **Groupes d'utilisateurs**. L'écran **Groupes d'utilisateurs** apparaît.
2. Effectuez un clic droit sur le groupe d'utilisateurs souhaité et sélectionnez **Supprimer le groupe d'utilisateurs** dans le menu.
   Une fenêtre de confirmation apparaît.

Vous pouvez également sélectionner un utilisateur, puis cliquer sur le bouton Actions > Supprimer le groupe d'utilisateurs.

3. Cliquez sur **Supprimer**.
   Le groupe d'utilisateurs est supprimé du système.

## Rôles d'utilisateur

Voici une brève description des différents rôles 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 intervenir 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** | ✓ | ✓ | ✓ | ✓ | ✓ | X | X |
| **Télécharger le fichier de capture** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Exclure de la politique** | ✓ | ✓ | ✓ | ✓ | X | X | X |
| **Tout résoudre** | ✓ | ✓ | ✓ | ✓ | ✓ | X | X |
| **Exporter** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Créer une politique sur FortiGate** | ✓ | ✓ | ✓ | ✓ | X | X | X |
| **Actualiser** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Politiques** | | | | | | | |
| **Afficher les politiques** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Autorisation | Administrateur (local) | Administrateur (externe/AD) | Superviseur | Responsable sécurité | Analyste sécurité | Opérateur de site | Lecture seule |
|---|---|---|---|---|---|---|---|
| **Activer/ Désactiver** | ✓ | ✓ | ✓ | ✓ | X | X | X |
| **Afficher l'action** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Modifier** | ✓ | ✓ | ✓ | ✓ | X | X | X |
| **Dupliquer** | ✓ | ✓ | ✓ | ✓ | X | X | X |
| **Supprimer** | ✓ | ✓ | ✓ | ✓ | X | X | X |
| **Créer une politique** | ✓ | ✓ | ✓ | ✓ | X | X | X |
| **Exporter** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Assets** | | | | | | | |
| **Afficher les assets** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Afficher l'action** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Modifier** | ✓ | ✓ | ✓ | X | X | ✓ | X |
| **Supprimer** | ✓ | ✓ | ✓ | X | X | ✓ | X |
| **Importer (charger de nouveaux assets via csv)** | ✓ | ✓ | ✓ | X | X | ✓ | X |
| **Masquer** | ✓ | ✓ | ✓ | X | X | ✓ | X |
| **Exporter** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Resynchroniser** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | X |
| **Scan Nessus** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | X |
| **Prendre un instantané (un seul asset)** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | X |

| Autorisation | Administrateur (local) | Administrateur (externe/AD) | Superviseur | Responsable sécurité | Analyste sécurité | Opérateur de site | Lecture seule |
|---|---|---|---|---|---|---|---|
| **Mettre à jour les ports ouverts (un seul asset)** | ✓ | ✓ | ✓ | ✓ | ✓ | X | X |
| **Mettre à jour l'état des ports (un seul asset)** | ✓ | ✓ | ✓ | ✓ | ✓ | X | X |
| **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** | ✓ | ✓ | ✓ | ✓ | ✓ | X | X |
| **Mettre à jour l'ensemble de plug-ins** | ✓ | ✓ | ✓ | ✓ | X | X | X |
| **Exporter** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Réseau** | | | | | | | |
| **Activer la capture de paquets** | ✓ | ✓ | ✓ | X | X | X | X |
| **Fermer les captures en cours** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | X |
| **Télécharger le fichier PCAP** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Autorisation | Administrateur (local) | Administrateur (externe/AD) | Superviseur | Responsable sécurité | Analyste sécurité | Opérateur de site | Lecture seule |
|---|---|---|---|---|---|---|---|
| **Exporter le tableau des communi-cations** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Définir comme base de référence** | ✓ | ✓ | ✓ | ✓ | X | X | X |
| **Générer une cartographie** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Actualiser la cartographie** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Groupes** | | | | | | | |
| **Afficher les groupes** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Afficher l'action** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Modifier** | ✓ | ✓ | ✓ | ✓ | X | X | X |
| **Dupliquer** | ✓ | ✓ | ✓ | ✓ | X | X | X |
| **Supprimer** | ✓ | ✓ | ✓ | ✓ | X | X | X |
| **Créer un groupe** | ✓ | ✓ | ✓ | ✓ | X | X | X |
| **Exporter** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Rapport** | | | | | | | |
| **Afficher les rapports** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Générer** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Télécharger** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Exporter** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Segments réseau** | | | | | | | |
| **Afficher les segments réseau** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

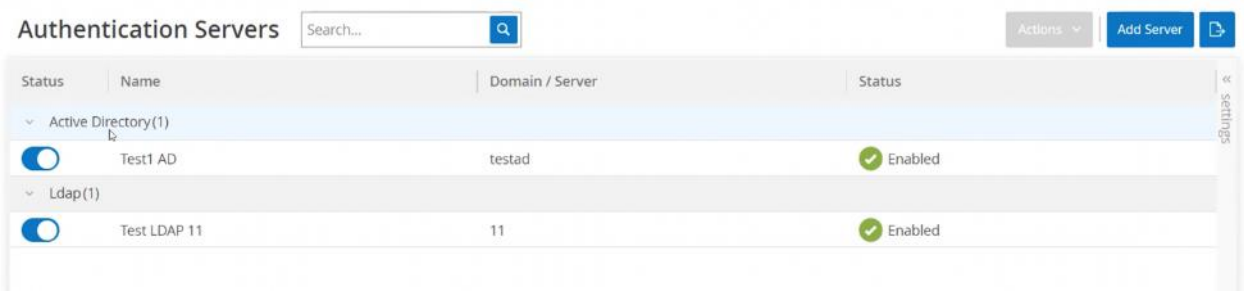
| Autorisation | Administrateur (local) | Administrateur (externe/AD) | Superviseur | Responsable sécurité | Analyste sécurité | Opérateur de site | Lecture seule |
|---|---|---|---|---|---|---|---|
| **Modifier** | ✓ | ✓ | ✓ | ✓ | X | X | X |
| **Supprimer** | ✓ | ✓ | ✓ | ✓ | X | X | X |
| **Créer** | ✓ | ✓ | ✓ | ✓ | X | X | X |
| **Exporter** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **En savoir plus** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Paramètres locaux** | | | | | | | |
| **Requêtes** | ✓ | ✓ | ✓ | X | X | X | X |
| **Configuration système – Détails de l'appareil** | ✓ | ✓ | ✓ | X | X | X | X |
| **Configuration système – Capteurs** | ✓ | ✓ | ✓ (Aucune action) | ✓ (Aucune action) | ✓ (Aucune action) | ✓ (Aucune action) | ✓ (Aucune action) |
| **Configuration système – Configuration des ports** | ✓ | ✓ | ✓ | X | X | X | X |
| **Configuration système –Mises à jour** | ✓ | ✓ | ✓ | X | X | X | X |
| **Configuration système – Certificat (HTTPS)** | ✓ | ✓ | X | X | X | X | X |
| **Configuration système – Clés API** | ✓ | X | ✓ (Utilisateurs locaux uniquement) | ✓ (Utilisateurs locaux uniquement) | ✓ (Utilisateurs locaux uniquement) | ✓ (Utilisateurs locaux uniquement) | ✓ (Utilisateurs locaux uniquement) |
| **Configuration système – Licence** | ✓ | ✓ | X | X | X | X | X |

| Autorisation | Administrateur (local) | Administrateur (externe/AD) | Superviseur | Responsable sécurité | Analyste sécurité | Opérateur de site | Lecture seule |
|---|---|---|---|---|---|---|---|
| **Configuration de l'environnement – Paramètres de l'asset** | ✓ | ✓ | ✓ | X | X | X | X |
| **Configuration de l'environnement – Assets masqués** | ✓ | ✓ | ✓ | ✔ - pas de restauration | ✔ - pas de restauration | ✓ | ✔ - pas de restauration |
| **Configuration de l'environnement – Champs personnalisés** | ✓ | ✓ | ✓ | X | X | X | X |
| **Configuration de l'environnement – Clusters d'événements** | ✓ | ✓ | ✓ | X | X | X | X |
| **Configuration de l'environnement – Lecteur PCAP** | ✓ | ✓ | ✓ | X | X | X | X |
| **Utilisateurs et rôles – Paramètres de l'utilisateur** | ✓ | ✓ | ✓ | X | X | X | X |
| **Utilisateurs et rôles – Utilisateurs locaux** | ✓ | X | X | X | X | X | X |
| **Utilisateurs et rôles – Groupes d'utilisateurs** | ✓ | X | X | X | X | X | X |
| **Utilisateurs et rôles – Active Directory** | ✓ | X | X | X | X | X | X |
| **Intégrations** | ✓ | ✓ | X | X | X | X | X |
| **Serveurs** | ✓ | ✓ | ✓ | ✔ (Aucune action) | ✔ (Aucune action) | ✔ (Aucune action) | ✔ (Aucune action) |
| **Actions système** | ✓ | ✔ - sans réinitialisation d'usine | ✔ - sauvegarde et diagnostics uniquement | ✔ - diagnostics uniquement | X | X | X |

| Autorisation | Administrateur (local) | Administrateur (externe/AD) | Superviseur | Responsable sécurité | Analyste sécurité | Opérateur de site | Lecture seule |
|---|---|---|---|---|---|---|---|
| **Journal système** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ - pas de journal système |
| **Activer (lors de la configuration et après la désactivation)** | ✓ | ✓ | X | X | X | X | X |
| **Supprimer les assets** | ✓ | ✓ | ✓ | X | X | X | X |

## Serveurs d'authentification

L'écran 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 Tenable.ot à l'Active Directory de votre organisation. Cela permet aux utilisateurs de se connecter à Tenable.ot à l'aide de leurs identifiants Active Directory. La configuration implique la mise en place de l'intégration, puis le mappage des groupes dans votre AD aux groupes d'utilisateurs dans Tenable.ot.

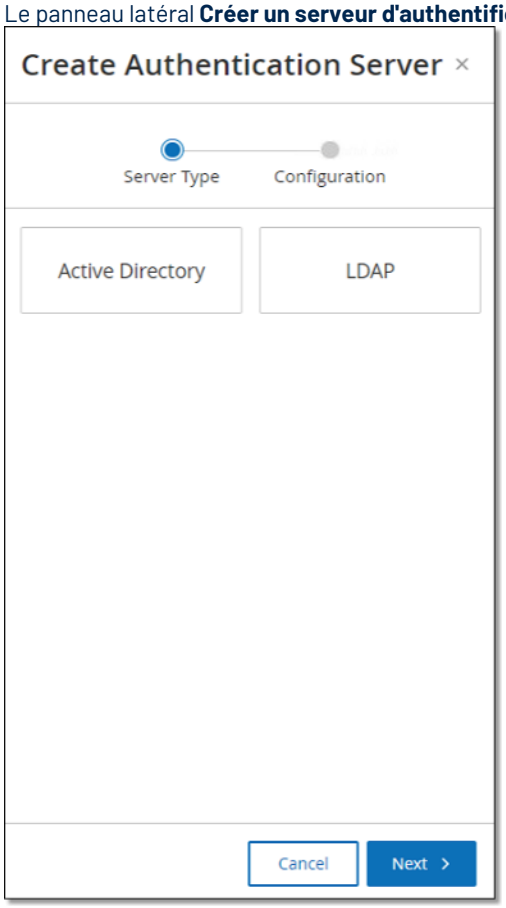
Le système est livré avec un ensemble de groupes d'utilisateurs pré-définis, correspondant à chacun des rôles disponibles, à savoir *Administrators* (Groupe d'utilisateurs > rôle *Administrator*), *Site Operators* (Groupe d'utilisateurs > rôle *Site Operator*), etc. Pour une explication des rôles disponibles, voir **Rôles d'utilisateur**.

**Pour configurer Active Directory :**

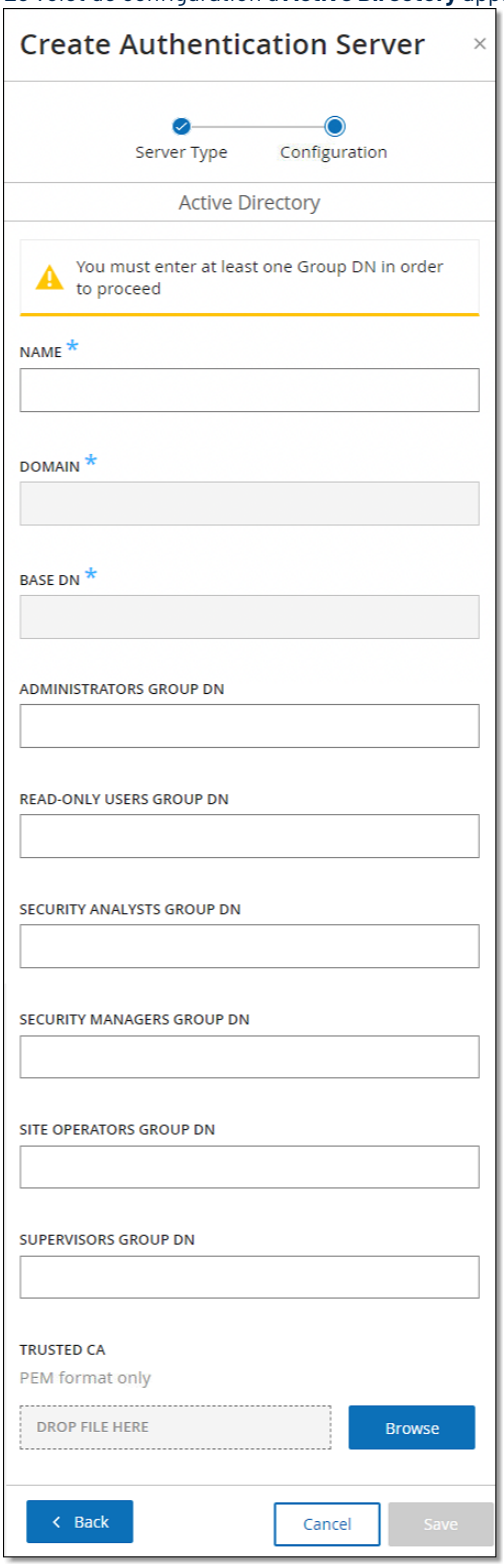
1. **En option**, vous pouvez obtenir un certificat CA auprès de l'autorité de certification ou de l'administrateur réseau de votre organisation et le charger sur votre ordinateur local.

Le système est livré avec un ensemble de groupes d'utilisateurs pré-définis, correspondant à chacun des rôles disponibles, à savoir Administrators (Groupe d'utilisateurs> rôle *Administrator*), *Site Operators* (Groupe d'utilisateurs > rôle *Site Operator*), etc. Pour une explication des rôles disponibles, voir **Rôles d'utilisateur**.

2. Sous **Paramètres locaux**, accédez à l'écran **Utilisateurs et rôles** > **Serveurs d'authentification**.
3. Cliquez sur **Ajouter un serveur**.
   Le panneau latéral **Créer un serveur d'authentification** s'ouvre, avec le volet **Type de serveur** affiché.



4. Cliquez sur **Active Directory**.
   Le volet de configuration d'**Active Directory** apparaît.




5. Dans le champ **Nom**, saisissez le nom à utiliser sur l'écran de connexion.
6. Dans le champ **Nom de domaine**, saisissez le FQDN du domaine de l'organisation (par exemple, société.com).

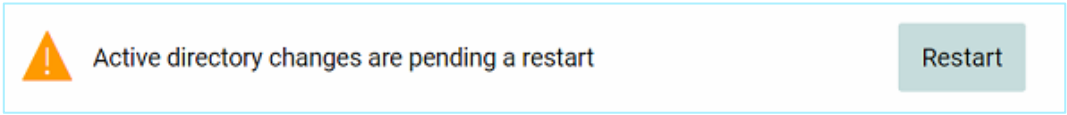
Si vous ne connaissez pas votre nom de domaine, vous pouvez le trouver en saisissant la commande « set » dans l'invite de commandes/Windows CMD. La valeur donnée pour l'attribut « USERDNSDOMAIN » est le nom de domaine.

7. Dans le champ **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 Tenable.ot, saisissez le DN du groupe AD dans le champ approprié. 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 le champ **DN du groupe Administrateurs**.

Si vous ne connaissez pas le DN du groupe auquel vous souhaitez attribuer des privilèges Tenable.ot, vous pouvez afficher une liste de tous les groupes configurés dans votre Active Directory qui contiennent des utilisateurs en saisissant la commande « dsquery group -name Users* » dans l'invite de commandes/Windows CMD. Le nom du groupe que vous souhaitez attribuer doit être saisi dans le champ dans le format identique 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.

Ces champs ne sont pas obligatoires. Si un champ n'est pas rempli, aucun utilisateur AD ne sera affecté à ce groupe d'utilisateurs. Vous pouvez configurer une intégration sans groupe mappé, mais dans ce cas, aucun utilisateur ne pourra accéder au système tant que vous n'aurez pas ajouté au moins un mappage de groupe.

9. Dans la section **CA de confiance**, cliquez sur **Parcourir** et accédez au fichier contenant le certificat CA de votre organisation (que vous avez obtenu auprès de votre autorité de certification ou de votre administrateur réseau) (facultatif).
10. Cochez la case **Activer Active Directory**.
11. Cliquez sur **Enregistrer**.
    Une fenêtre contextuelle vous invite à redémarrer l'unité afin d'activer Active Directory.




12. Cliquez sur **Redémarrer**.
    L'unité redémarre. Au redémarrage, les paramètres d'Active Directory seront activés. Tout utilisateur affecté aux groupes désignés peut accéder à la plateforme Tenable.ot à l'aide de ses identifiants d'entreprise.

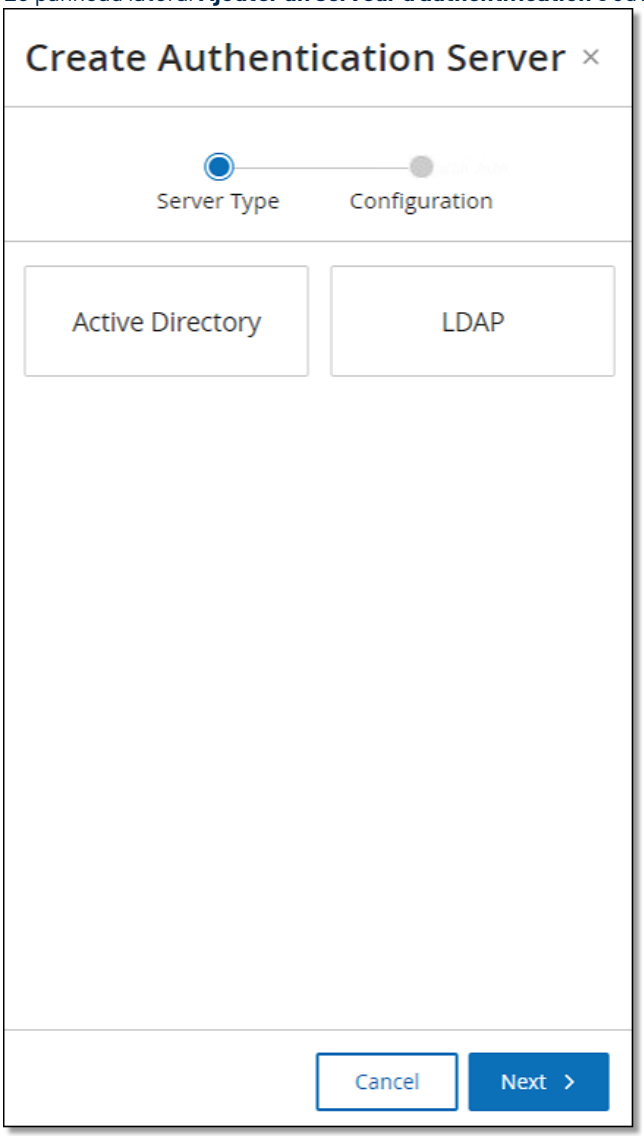
Pour vous connecter à l'aide d'Active Directory, le nom d'utilisateur principal (UPN) doit être utilisé sur la page de connexion. Dans certains cas, cela revient simplement à ajouter @<domaine>.com au nom d'utilisateur.

## LDAP

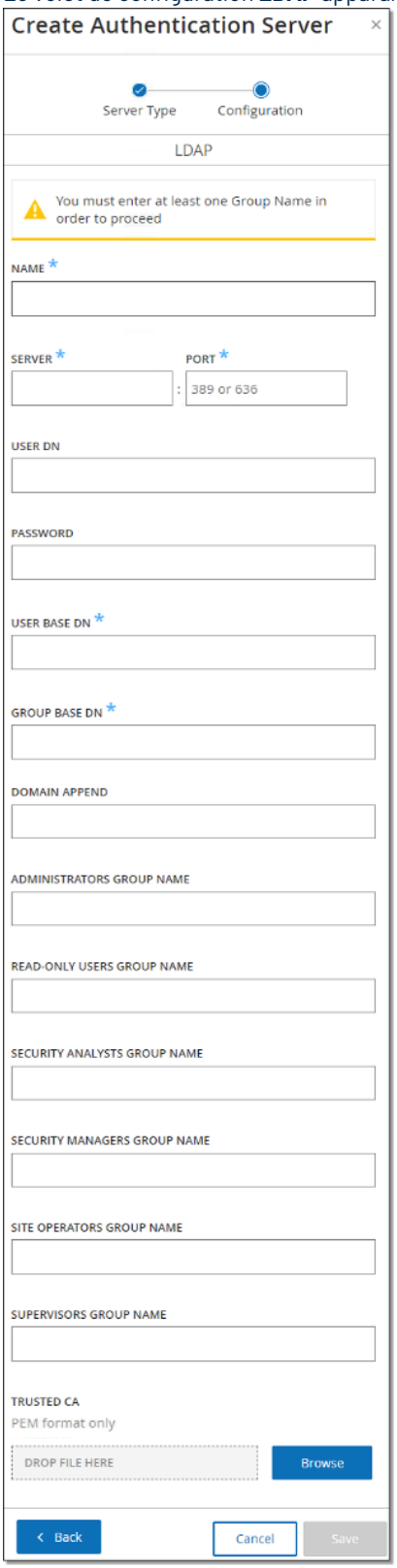
Vous pouvez intégrer Tenable.ot au LDAP de votre organisation. Cela permet aux utilisateurs de se connecter à Tenable.ot à l'aide de leurs identifiants LDAP. La configuration implique la mise en place de l'intégration, puis le mappage des groupes dans votre AD aux groupes d'utilisateurs dans Tenable.ot.

### Pour configurer LDAP :

1. Sous Paramètres locaux, accédez à l'écran **Utilisateurs et rôles** > **Serveurs d'authentification**.
2. Cliquez sur **Ajouter un serveur**.
   Le panneau latéral **Ajouter un serveur d'authentification** s'ouvre, avec le volet **Type de serveur** affiché.



3. Sélectionnez **LDAP**.
   Le volet de configuration **LDAP** apparaît.



4. Dans le champ **Nom**, saisissez le nom à utiliser sur l'écran de connexion.

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 différenciera les différentes configurations sur l'écran de connexion.

5. Dans le champ **Serveur**, saisissez le FQDN ou l'adresse de connexion.

Si vous utilisez une connexion sécurisée, il est recommandé d'utiliser le FQDN et non une adresse IP pour garantir que le certificat sécurisé fourni sera vérifié.

Si un nom d'hôte est utilisé, il doit figurer dans la liste des serveurs DNS du système Tenable.ot. Voir **Configuration système** > **Appareil**.

6. Dans le champ **Port**, saisissez 389 pour utiliser une connexion non sécurisée ou 636 pour utiliser une connexion SSL sécurisée.

Si le port 636 est choisi, un certificat sera requis pour terminer l'intégration.

7. Dans le champ **DN de l'utilisateur**, saisissez le DN avec des paramètres au format DN (par exemple, pour un nom de serveur AD_1.qa.com, le DN de l'utilisateur peut être CN=Administrateur,CN=Utilisateurs,DC=qa,DC=com).
8. Dans le champ **Mot de passe**, saisissez le mot de passe du DN de l'utilisateur.

La configuration de Tenable.ot avec LDAP ne fonctionnera que tant que le mot de passe du DN de l'utilisateur est valide. Par conséquent, si le mot de passe du DN de l'utilisateur change ou expire, la configuration de Tenable.ot doit également être mise à jour.

9. Dans le champ **DN de base de l'utilisateur**, saisissez le nom de domaine de base au format DN (par exemple DC=qa,DC=com).
10. Dans le champ **DN de base du groupe**, saisissez le nom de domaine de base du groupe au format DN.
11. Dans le champ **Ajout de domaine**, saisissez le domaine par défaut qui sera 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 champs de nom de groupe pertinents, saisissez les noms de groupe Tenable que l'utilisateur doit utiliser 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**.
    Le serveur est démarré 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.

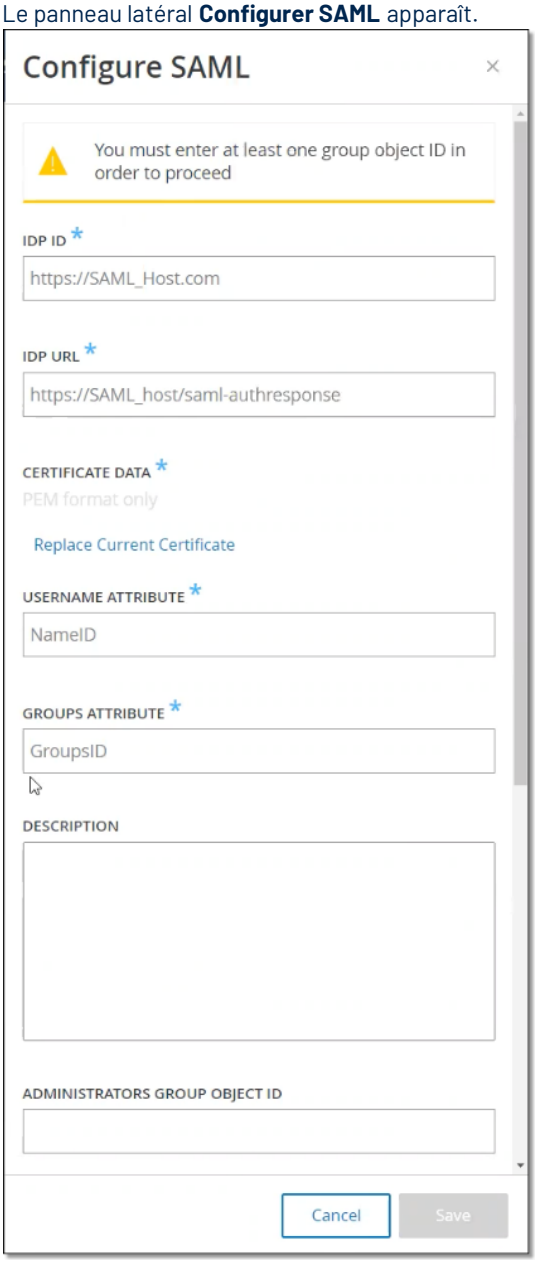
L'activation/la désactivation de la configuration LDAP ne sera pas terminée tant que le système n'aura pas redémarré. Si vous ne redémarrez pas le système immédiatement, cliquez sur le bouton **Redémarrer** sur la bannière en haut de l'écran lorsque vous êtes prêt à redémarrer.

## SAML

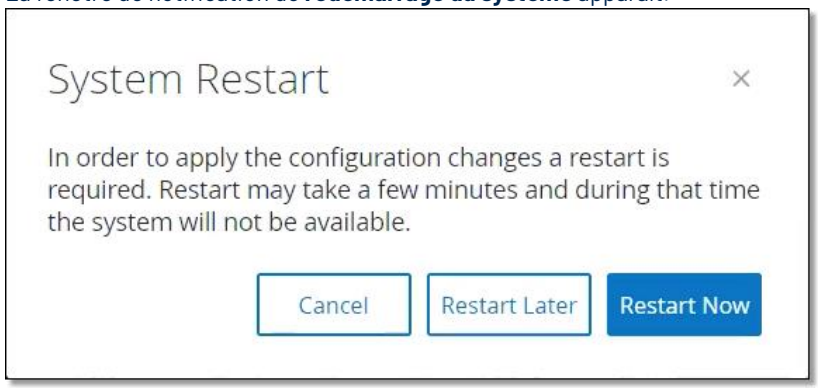
Vous pouvez intégrer Tenable.ot au fournisseur d'identité de votre organisation (par exemple, Microsoft Azure). Cela permet aux utilisateurs de s'authentifier via leur fournisseur d'identité. La configuration implique la mise en place de l'intégration en créant une application Tenable.ot au sein de votre fournisseur d'identité. Ensuite, vous devrez saisir des informations sur votre application Tenable.ot nouvellement créée, puis charger le certificat de votre fournisseur d'identité à la page **SAML** de Tenable.ot, et enfin mapper les groupes de votre fournisseur d'identité aux groupes d'utilisateurs dans Tenable.ot. Pour un tutoriel détaillé sur l'intégration de Tenable.ot à Microsoft Azure, voir **l'Annexe 2 – Intégration SAML pour Azure Active Directory.**

### Pour configurer SAML :

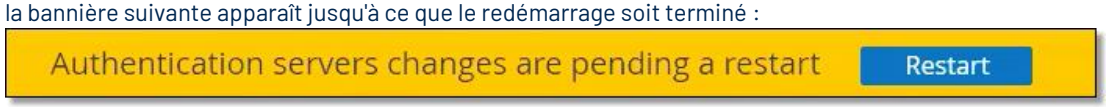
1. Sous **Paramètres locaux**, accédez à l'écran **Utilisateurs et rôles** > **SAML**.
2. Cliquez sur **Configurer**.
   Le panneau latéral **Configurer SAML** apparaît.



3. Dans le champ **ID IDP**, saisissez l'identifiant du fournisseur d'identité pour l'application Tenable.ot.
4. Dans le champ **URL IDP**, saisissez l'URL du fournisseur d'identité pour l'application Tenable.ot.
5. Sous **Données de certificat**, cliquez sur **Remplacer le certificat actuel**, accédez au fichier de certificat du fournisseur d'identité que vous avez téléchargé pour l'utiliser avec l'application Tenable.ot et ouvrez-le.
6. Dans le champ **Attribut de nom d'utilisateur**, saisissez l'attribut de nom d'utilisateur du fournisseur d'identité pour l'application Tenable.ot.
7. Dans le champ **Attribut des groupes**, saisissez l'attribut des groupes du fournisseur d'identité pour l'application Tenable.ot.
8. Saisissez une description dans le champ **Description**. (Facultatif)
9. Pour chaque mappage de groupe que vous souhaitez configurer, accédez à **l'ID d'objet de groupe** du fournisseur d'identité pour un groupe d'utilisateurs et saisissez-le dans le champ **ID d'objet de groupe** souhaité pour le mapper au groupe d'utilisateurs Tenable.ot souhaité.
10. Cliquez sur **Enregistrer** pour enregistrer et refermer le panneau latéral.
11. Sur l'écran **SAML**, **activez** le curseur **Connexion unique SAML**.
    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 plus tard, la bannière suivante apparaît 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 Tenable.ot à l'aide de ses identifiants de fournisseur d'identité.

# Intégrations

Vous pouvez configurer des intégrations avec d'autres plateformes prises en charge afin de permettre à Tenable.ot de se synchroniser avec vos autres plateformes de cybersécurité.

## Produits Tenable

Vous pouvez intégrer Tenable.ot à Tenable.sc et Tenable.io. Cela permet à Tenable.ot de partager des données avec les autres plateformes. Les données synchronisées incluent les vulnérabilités OT ainsi que les données découvertes par les scans Nessus informatiques lancés à partir de Tenable.ot.

Les données des assets qui ont été « masqués » dans Tenable.ot ne seront pas envoyées à Tenable.sc ni Tenable.io via l'intégration.

Afin d'intégrer les plateformes, Tenable.ot doit pouvoir accéder à Tenable.sc et/ou Tenable.io via le port 443. Il est recommandé de créer un utilisateur spécifique sur Tenable.sc et/ou Tenable.io à utiliser comme utilisateur d'intégration à Tenable.ot.

### Tenable.sc

Pour intégrer Tenable.sc, créez un nouveau référentiel d'agent pour les données Tenable.ot. Prenez note de l'ID du référentiel. Dans Tenable.ot, créez une nouvelle intégration, en renseignant l'adresse IP ou le nom d'hôte de votre système Tenable.sc ainsi que les informations d'identification de votre compte et l'ID du référentiel, puis définissez la fréquence de synchronisation. Ensuite, effectuez un clic droit sur l'intégration nouvellement ajoutée et cliquez sur « Synchroniser ».

Il est recommandé de créer un utilisateur spécifique sur Tenable.sc à utiliser comme utilisateur d'intégration à Tenable.ot. L'utilisateur doit avoir le rôle de *Responsable sécurité/Analyste sécurité* ou *Analyste vulnérabilité* et être affecté au groupe « Accès complet ».

### Tenable.io

Pour intégrer Tenable.io, saisissez votre clé d'accès et votre clé secrète, puis définissez la fréquence de synchronisation.

Vous devez d'abord générer une clé API dans la console Tenable.io (**Paramètres** > **My account (Mon compte)** > **Clés API** > **Générer**). Vous recevrez une clé d'accès et une clé secrète que vous saisirez dans la console Tenable.ot lors de la configuration de l'intégration.

## Palo Alto Networks – Pare-feu de nouvelle génération (NGFW)

Vous pouvez partager les informations d'inventaire des assets découvertes par Tenable.ot avec votre système Palo Alto.

Pour intégrer Tenable.ot à votre Palo Alto NGFW, renseignez l'adresse IP ou le nom d'hôte de votre Palo Alto NGRW ainsi que les informations d'identification pour accéder à votre compte NGRW.

## Aruba – Gestionnaire de politiques ClearPass

Vous pouvez partager les informations d'inventaire des assets découvertes par Tenable.ot avec votre système Aruba.

Pour intégrer Tenable.ot à votre système Aruba ClearPass, renseignez l'adresse IP ou le nom d'hôte de votre système Aruba ClearPass ainsi que les informations d'identification pour accéder à votre compte Aruba ClearPass.

# Serveurs

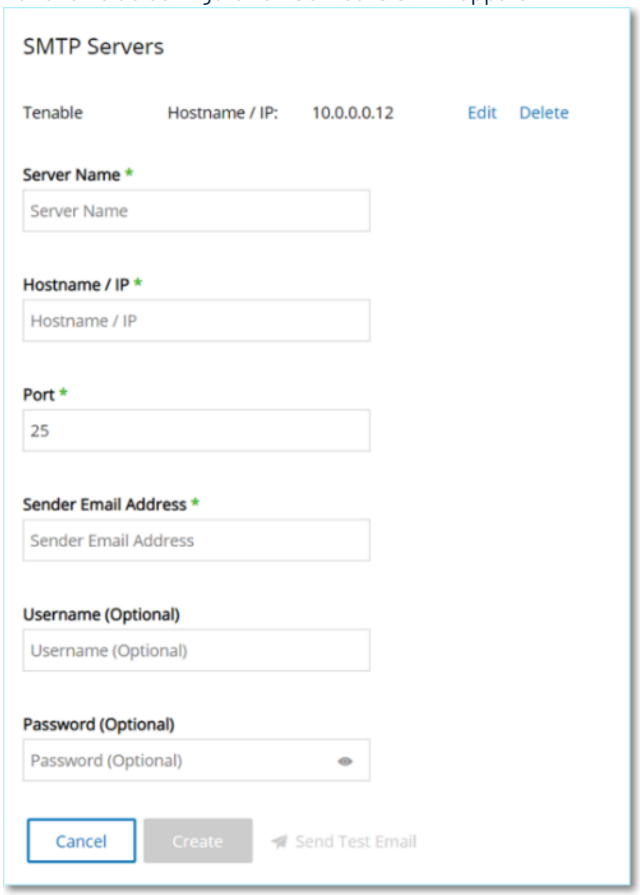
Vous pouvez configurer des serveurs SMTP et des serveurs Syslog dans le système pour permettre aux notifications d'événement d'être envoyées par e-mail et/ou connectées à un SIEM. Vous pouvez également configurer des pare-feu FortiGate afin d'envoyer des suggestions de politique de pare-feu à FortiGate en fonction des événements réseau de Tenable.ot.

## Serveurs SMTP

Afin de permettre l'envoi de notifications d'événement par e-mail aux parties pertinentes, vous devrez configurer un *serveur SMTP* dans le système. Si vous ne configurez pas de serveur SMTP, les événements générés par le système ne peuvent pas être envoyés par e-mail. Dans tous les cas, tous les événements peuvent être visualisés dans la console de gestion (IU) sur l'écran des événements.

### ➡ Pour configurer un serveur SMTP :

1. Sous **Paramètres locaux**, accédez à l'écran **Utilisateurs et rôles** > **Serveurs SMTP**.
2. Cliquez sur **Ajouter un serveur SMTP**.
   La fenêtre de configuration **Serveurs SMTP** apparaît.




3. Dans le champ **Nom du serveur**, saisissez le nom d'un serveur SMTP à utiliser pour les notifications par e-mail.
4. Dans le champ **Nom d'hôte/IP**, saisissez un nom d'hôte ou une adresse IP du serveur SMTP.
5. Dans le champ **Port**, saisissez le numéro de port sur lequel le serveur SMTP écoutera les événements (par défaut : 25).
6. Dans le champ **Adresse e-mail de l'expéditeur**, saisissez une adresse e-mail qui apparaît comme expéditeur de l'e-mail de notification d'événement.

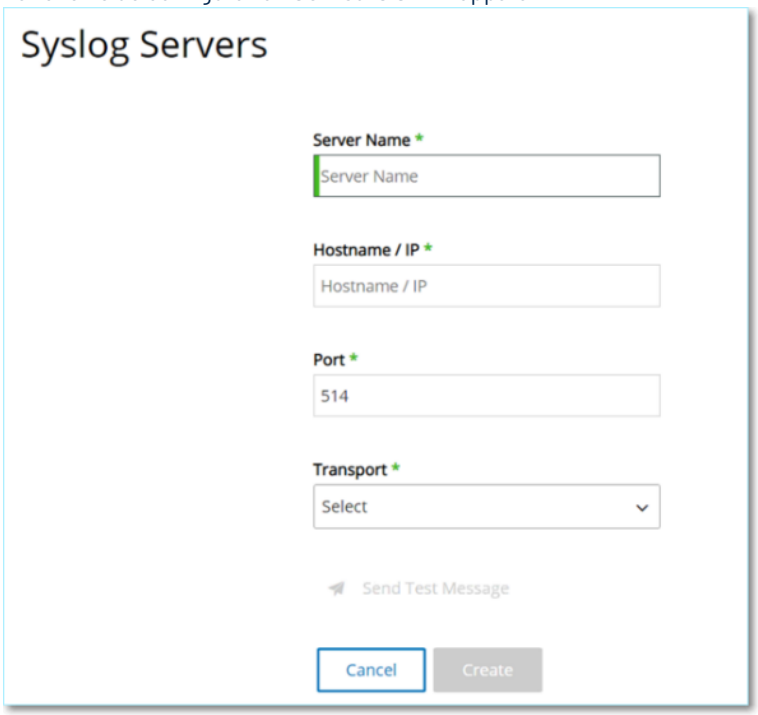
7. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez un nom d'utilisateur et un mot de passe qui seront utilisés pour accéder au serveur SMTP. Ces champs sont facultatifs.
8. À ce stade, vous pouvez essayer d'envoyer un e-mail de test pour vérifier que la configuration a réussi. Cliquez sur **Envoyer un e-mail de test**, puis saisissez l'adresse e-mail à laquelle l'envoyer et vérifiez la boîte de réception pour voir si l'e-mail est arrivé. Si l'e-mail n'est pas arrivé, dépannez pour découvrir la cause du problème et corrigez-le.
9. Cliquez sur **Enregistrer**.
   Vous pouvez configurer des serveurs SMTP supplémentaires en répétant la procédure décrite ci-dessus.

## Serveurs Syslog

Afin d'activer la collecte des événements du journal sur un serveur externe, vous devrez configurer un *serveur Syslog* dans le système. Si vous ne souhaitez pas configurer de serveur Syslog, les journaux d'événements ne seront enregistrés que sur la plateforme Tenable.ot.

### Pour configurer un serveur Syslog :

1. Sous **Paramètres locaux**, accédez à l'écran **Utilisateurs et rôles** > **Serveurs Syslog**.
2. Cliquez sur **+ Ajouter un serveur Syslog**.
   La fenêtre de configuration **Serveurs SMTP** apparaît.

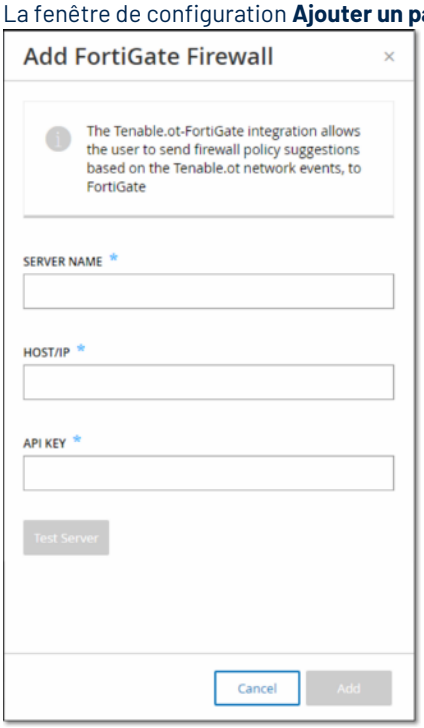



3. Dans le champ **Nom du serveur**, saisissez le nom d'un serveur Syslog à utiliser pour consigner les événements système.
4. Dans le champ **Nom d'hôte\IP**, saisissez un nom d'hôte ou une adresse IP du serveur Syslog.
5. Dans le champ **Port**, saisissez le numéro de port du serveur Syslog auquel les événements seront envoyés (par défaut : 514).
6. Dans le champ **Transport**, sélectionnez dans la liste déroulante le protocole de transport à utiliser. Les options sont *TCP* ou *UDP*.
7. Si vous souhaitez 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 le message n'est pas arrivé, dépannez pour découvrir la cause du problème et corrigez-le.
8. Cliquez sur **Enregistrer**.
   Vous pouvez configurer des serveurs Syslog supplémentaires en répétant la procédure décrite ci-dessus.

## Pare-feu FortiGate

### Pour configurer un serveur FortiGate :

1. Sous **Paramètres locaux**, accédez à l'écran **Utilisateurs et rôles** > **Pare-feu FortiGate**.
2. Cliquez sur le bouton **Ajouter un pare-feu**.
   La fenêtre de configuration **Ajouter un pare-feu Fortigate** apparaît.



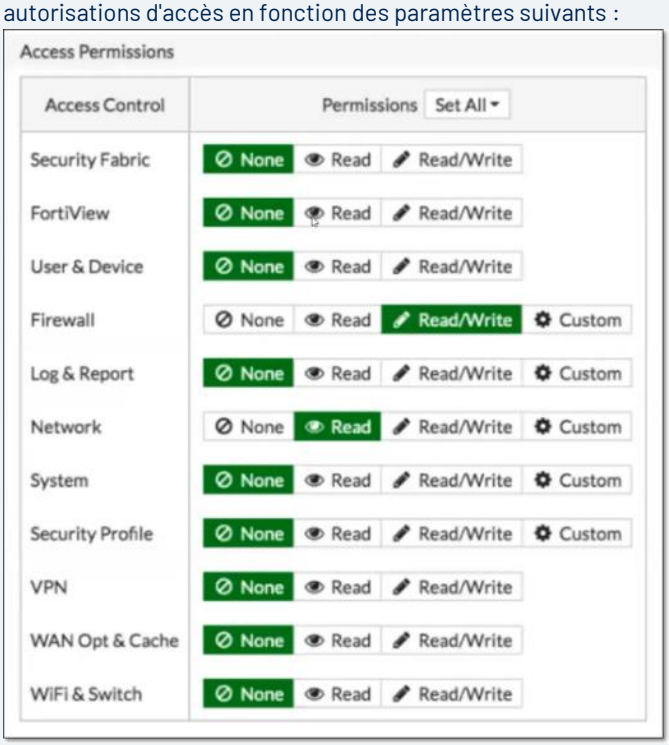

3. Dans le champ **Nom du serveur**, saisissez le nom d'un serveur FortiGate à utiliser pour consigner les événements système.
4. Dans le champ **Nom d'hôte/IP**, saisissez un nom d'hôte ou une adresse IP du serveur FortiGate.
5. Dans le champ **Clé API**, saisissez le **jeton API** que vous avez généré à partir de FortiGate. Pour plus d'informations, voir la note ci-dessous.
6. Cliquez sur **Ajouter**.
   Le serveur FortiGate Firewall est créé.

Les instructions pour générer un jeton API FortiGate se trouvent sur la page suivante : https://registry.terraform.io/providers/fortinetdev/fortios/latest/docs/guides/fgt_token

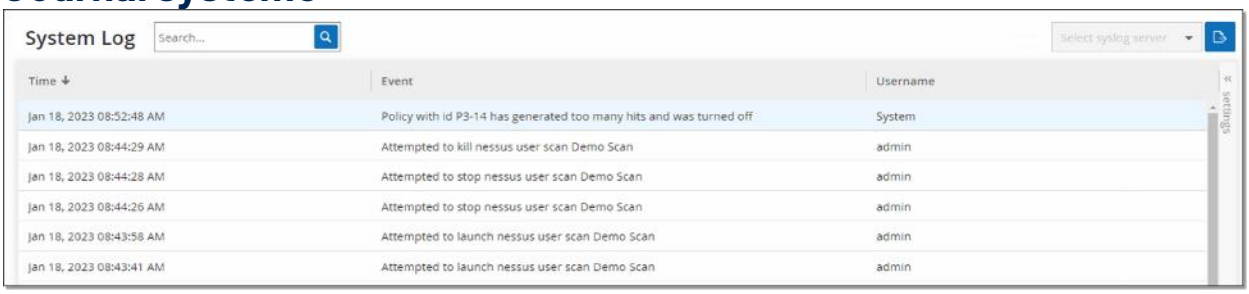
Veuillez noter :

- Pour l'adresse source (qui est nécessaire pour garantir que le jeton API ne puisse être utilisé qu'à partir d'hôtes de confiance), veuillez utiliser l'adresse IP de votre unité Tenable.ot.

Lors de la création d'un profil administrateur pour Tenable.ot, assurez-vous d'appliquer les autorisations d'accès en fonction des paramètres suivants :



# Journal système




L'écran **Journal système** affiche un journal de tous les événements système (par exemple, politique activée, politique modifiée, événement résolu, etc.) qui se sont produits sur le système. Ce journal inclut à la fois les événements déclenchés par l'utilisateur et les événements système qui se produisent automatiquement (par exemple, la stratégie s'est automatiquement désactivée en raison d'un trop grand nombre de correspondances). Ce journal n'inclut **pas** les événements générés par des politiques qui sont affichés sur l'écran *Événements*. Les journaux peuvent être exportés sous forme de fichier CSV. Vous pouvez également configurer le système pour envoyer les événements du journal système à un serveur Syslog.

Les informations affichées pour chaque événement consigné sont décrites dans le tableau suivant :

| Paramètre | Description |
|---|---|
| **Date/Heure** | La date et l'heure auxquelles l'événement s'est produit. |
| **Événement** | Une brève description de l'événement qui s'est produit. |
| **Nom d'utilisateur** | Le nom de l'utilisateur qui a lancé l'événement. Pour les événements qui se produisent automatiquement, aucun nom d'utilisateur n'est donné. |

## Envoi du journal système à un serveur Syslog

### ➡ Pour configurer l'envoi des événements système à un serveur Syslog :

1. Accédez à l'écran **Paramètres locaux** > **Journal système**.
2. Dans la barre d'en-tête, cliquez sur **Sélectionnez le serveur Syslog**.
   Une liste déroulante de serveurs apparaît.

> Pour ajouter un serveur Syslog, voir **Serveurs Syslog**.

3. Sélectionnez le serveur souhaité.
   Les événements du journal système seront envoyés au serveur Syslog spécifié.

# Annexe 1 – Installation d'un capteur (Versions 3.13 et antérieures)

La procédure suivante explique le processus complet de configuration d'un capteur v. 3.13 et antérieures. Certaines des étapes initiales sont également pertinentes pour les nouveaux capteurs. Cependant, l'assistant de configuration a été remplacé par la procédure d'appairage décrite dans **Appairage du capteur.**

## Étape 1 - Configuration du capteur

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

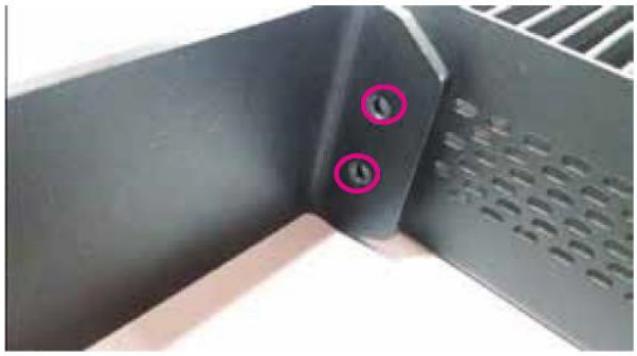
### Configuration d'un capteur pour montage en rack

Un capteur pour montage en rack peut être monté sur un rack standard de 19 pouces ou simplement posé sur une surface plane (comme un bureau).

#### Montage en rack (modèle pour montage en rack)

➡ **Pour monter le capteur Tenable.ot sur un rack standard (19 pouces) :**

1. Fixez les supports en L aux trous de vis de chaque côté du capteur, comme indiqué sur l'image ci-dessous.



2. Insérez deux vis de chaque côté et fixez-les avec un tournevis pour maintenir les supports en place.
3. Insérez le capteur avec les supports dans un emplacement 1U disponible du rack.

4. Installez l'unité en fixant les supports de montage en rack (fournis) au cadre du rack, à l'aide des vis adéquates (non fournies).

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

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

## Surface plane

**Pour installer le capteur Tenable.ot sur une surface plane :**

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

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

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

## Configuration d'un capteur configurable

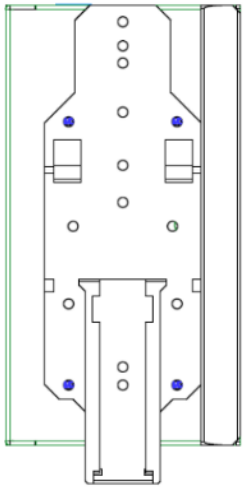
Un capteur configurable peut être monté sur un rail DIN ou sur un rack de montage 19 pouces standard (à l'aide du kit d'adaptation « oreilles de montage »).

### Montage sur rail DIN

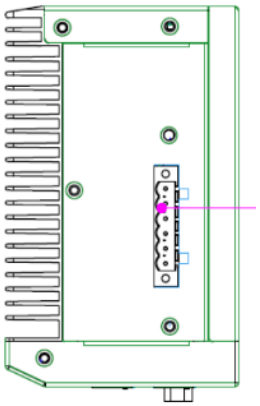
Le modèle configurable peut être monté sur un rail DIN en suivant la procédure suivante.

**➡ Pour monter le Capteur configurable Tenable.ot 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) :

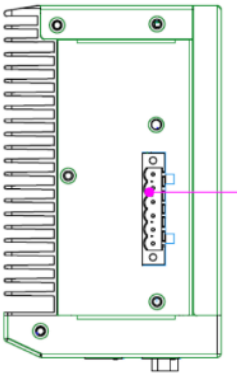
1. Préparez l'unité pour le montage en rack, comme suit :
   a. Retirez les 3 vis de chaque côté de l'appareil.
   b. Fixez les « oreilles de montage » des deux côtés de l'appareil à l'aide de nouvelles vis (fournies).

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

> 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.

# Étape 2 – Connexion du capteur au réseau

Le capteur Tenable.ot est utilisé pour collecter et transférer le trafic réseau vers l'appliance Tenable.ot. Pour assurer la surveillance du réseau, vous devrez connecter l'unité à un port de mise en miroir sur le commutateur réseau, qui est connecté aux contrôleurs/automates pertinents.

Pour gérer le capteur, vous devrez connecter l'unité à un réseau (il peut s'agir d'un réseau différent de celui utilisé pour effectuer la surveillance du réseau).

### ➡ Pour connecter le capteur pour montage en rack au commutateur réseau :

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

### ➡ Pour connecter le capteur configurable au commutateur réseau :

1. Sur le capteur Tenable.ot, 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.

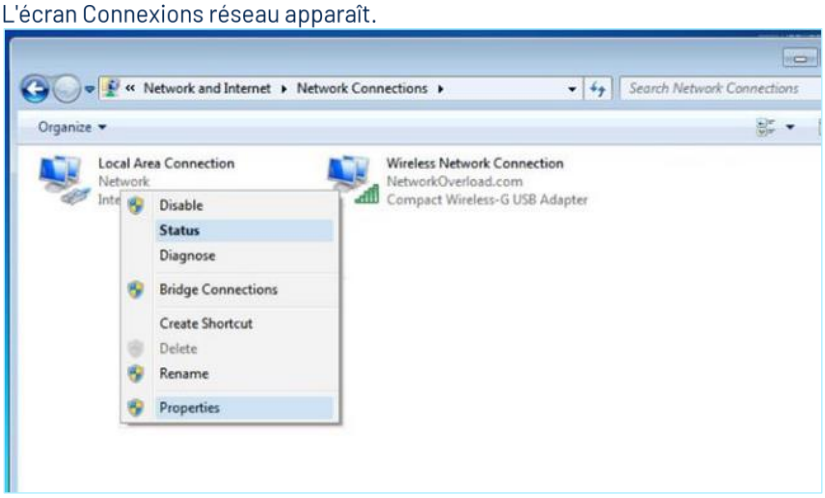
# Étape 3 – Accès à l'assistant de configuration du capteur

➡ **Pour se connecter à la console de gestion :**

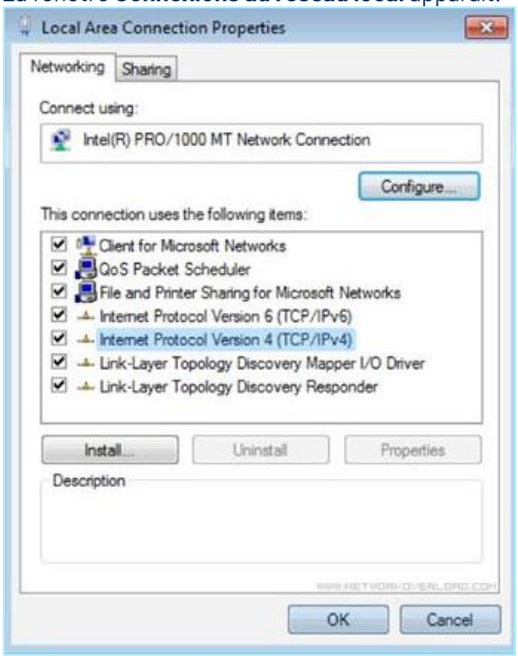
1. Effectuez l'une des actions suivantes :
   - Connectez le poste de travail de la console de gestion (PC, ordinateur portable, etc.) directement au port 1 du capteur Tenable.ot à l'aide du câble Ethernet, OU
   - Connectez le poste de travail de la console de gestion au commutateur réseau.
2. Assurez-vous que le poste de travail de la console de gestion fait partie du même sous-réseau que le capteur Tenable.ot (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 Tenable.ot) :
   a. Accédez à **Réseau et Internet** > **Centre Réseau et partage** > **Modifier les paramètres de la carte**.

> La navigation peut varier légèrement selon la version de Windows.

L'écran Connexions réseau apparaît.




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



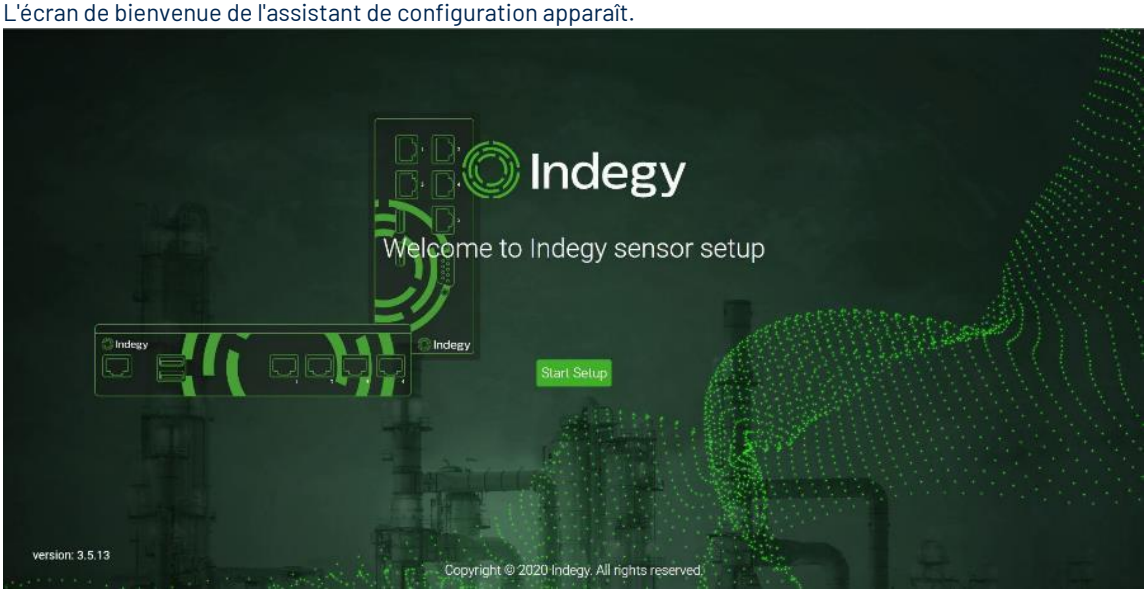
c. Sélectionnez **Protocole Internet version 4 (TCP/IPv4)** et cliquez sur **Propriétés**.
La fenêtre Propriétés d'Internet Protocol Version 4 (TCP/IPv4) apparaît.


d. Sélectionnez Utiliser l'adresse IP suivante.
e. Dans le champ Adresse IP, saisissez *192.168.1.10*
f. Dans le champ Masque de sous-réseau, saisissez *255.255.255.0*.
g. Cliquez sur **OK**.
Les nouveaux paramètres sont appliqués.

4. À partir de votre navigateur web Chrome, accédez à 192.168.1.5.

> L'interface utilisateur n'est accessible qu'à partir d'un navigateur Chrome. Vous devez également utiliser la dernière version de Chrome.

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




5. Cliquez sur **Démarrer l'assistant de configuration**.
L'assistant de configuration apparaît et affiche la page **Informations utilisateur**.

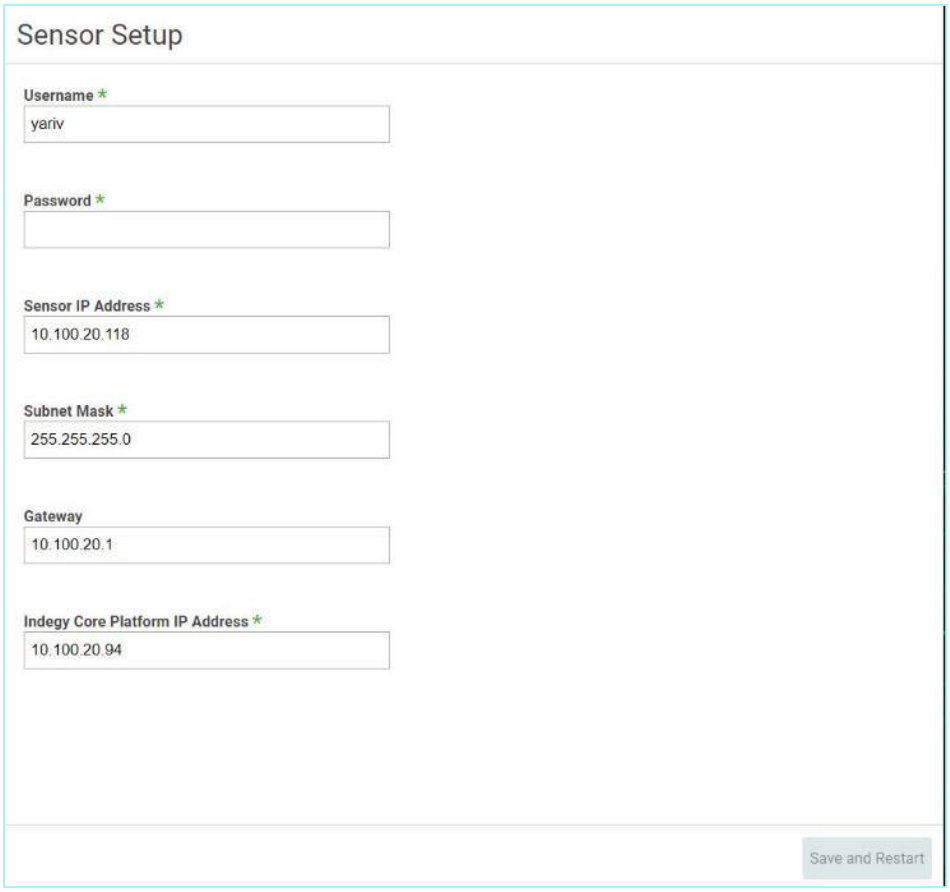
# Étape 4 – Assistant de configuration du capteur

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

Si vous souhaitez modifier la configuration ultérieurement, vous pourrez le faire dans l'écran **Paramètres** de la console de gestion (IU).

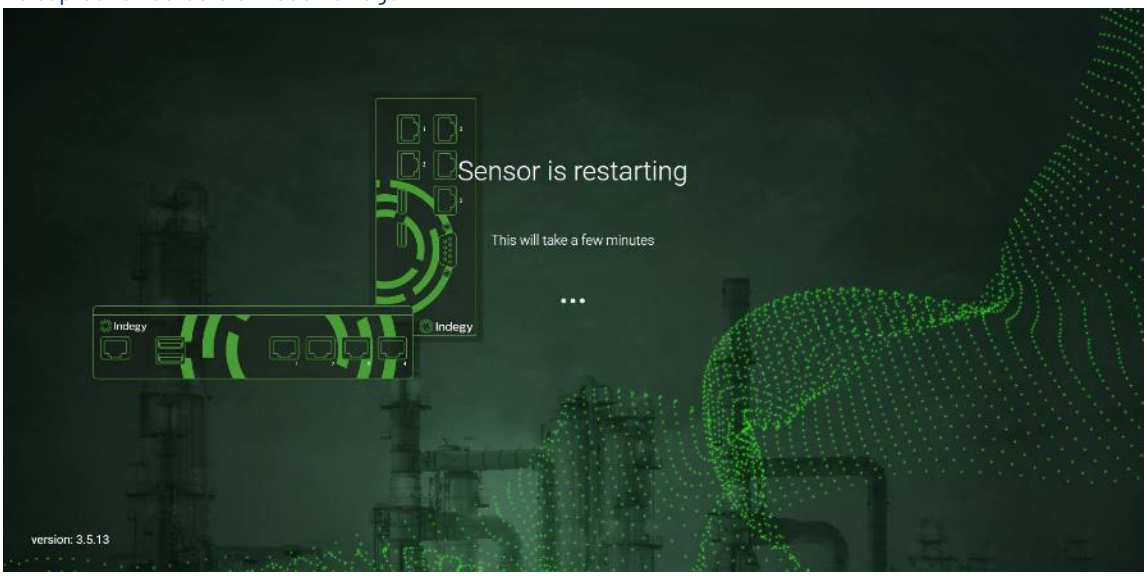
### Pour configurer le capteur :

1. Sur l'écran de bienvenue, cliquez sur **Start Setup** (Démarrer la configuration).
   L'écran de configuration apparaît :

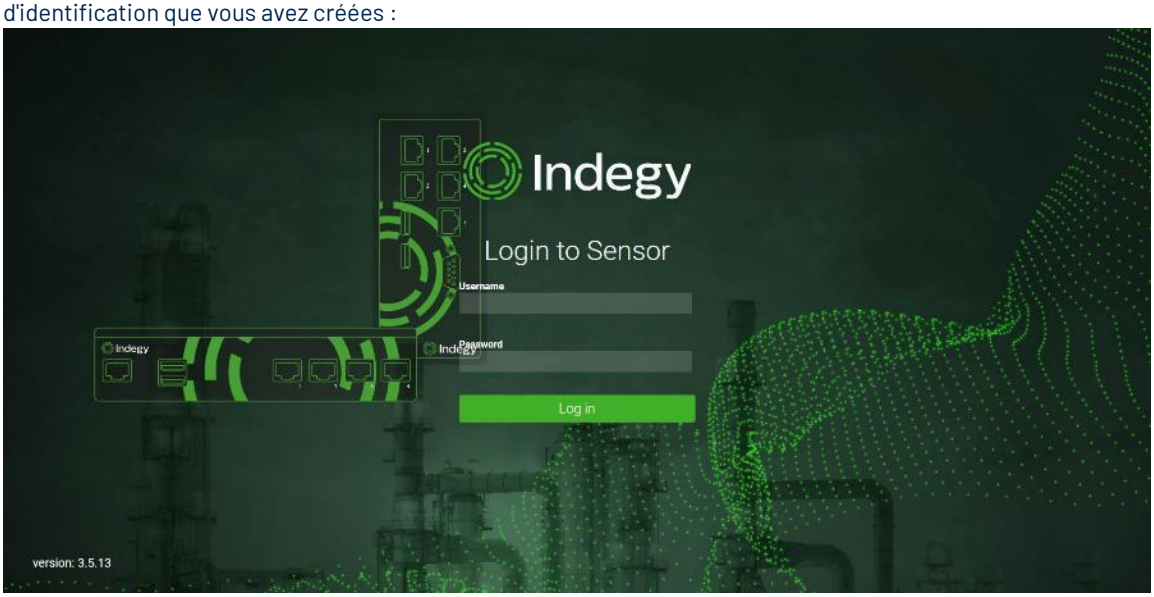



2. Dans le champ **Username** (Nom d'utilisateur), saisissez le nom d'utilisateur pour vous connecter au système. Le nom d'utilisateur peut comporter jusqu'à 12 caractères et ne doit inclure que des lettres minuscules et des chiffres.
3. Dans le champ **Password** (Mot de passe), saisissez le mot de 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
4. Dans le champ **Retype Password** (Confirmer le mot de passe), ressaisissez le même mot de passe.
5. Dans le champ **Sensor IP Address** (Adresse IP du capteur), saisissez l'adresse IP (dans le sous-réseau du réseau) à appliquer au capteur Tenable.ot. Il est fortement recommandé de changer l'adresse IP par défaut.

6. Dans le champ **Subnet Mask** (Masque de sous-réseau), saisissez le masque de sous-réseau du réseau.
7. Pour configurer une passerelle (facultatif), saisissez l'adresse IP de la passerelle du réseau dans le champ **Gateway** (Passerelle).
8. Dans le champ **IP Address** (Adresse IP), saisissez l'adresse IP de la plateforme Tenable.ot.
9. Cliquez sur **Save and Restart** (Enregistrer et redémarrer).
   Le capteur effectuera un redémarrage :




10. Après le redémarrage, le trafic réseau sera transféré vers la plateforme Tenable.ot. Pour modifier la configuration, connectez-vous au capteur en utilisant l'adresse IP configurée et les informations d'identification que vous avez créées :



# Annexe 2 – Intégration SAML pour Azure Active Directory

Tenable.ot prend en charge l'intégration avec Microsoft Azure Active Directory via le protocole SAML. Cela permet aux utilisateurs Azure qui ont été affectés à Tenable.ot de se connecter à Tenable.ot via SSO. Vous pouvez utiliser le mappage de groupe pour attribuer des rôles dans Tenable.ot en fonction des groupes auxquels les utilisateurs sont attribués dans Azure.

## Configuration de l'intégration

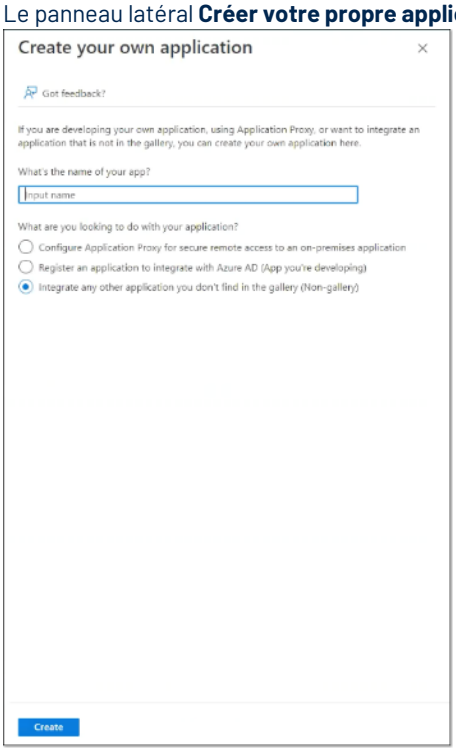
Cette section explique le processus complet de configuration d'une intégration d'authentification unique (SSO) pour Tenable.ot avec Microsoft Azure Active Directory. La configuration implique la mise en place de l'intégration en créant une application Tenable.ot dans Azure Active Directory. Ensuite, vous devrez saisir des informations sur votre application Tenable.ot nouvellement créée, puis charger le certificat de votre fournisseur d'identité à la page SAML de Tenable.ot, et enfin mapper les groupes de votre fournisseur d'identité aux groupes d'utilisateurs dans Tenable.ot.

Pour mettre en place la configuration, vous devez être connecté en tant qu'utilisateur administrateur dans Azure Active Directory et Tenable.ot.

### Étape 1 – Création de l'application Tenable dans Azure

➡ **Pour créer l'application Tenable dans Azure :**

1. Dans **Microsoft Azure Active Directory,** accédez à **Azure Active Directory** > **Applications d'entreprise,** cliquez sur **+ Nouvelle application** pour afficher **Parcourir la galerie Azure AD**, puis cliquez sur **+ Créer votre propre application**.
   Le panneau latéral **Créer votre propre application** apparaît.




2. Dans la section **Quel est le nom de votre application ?**, saisissez un nom pour l'application (ex. : 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.

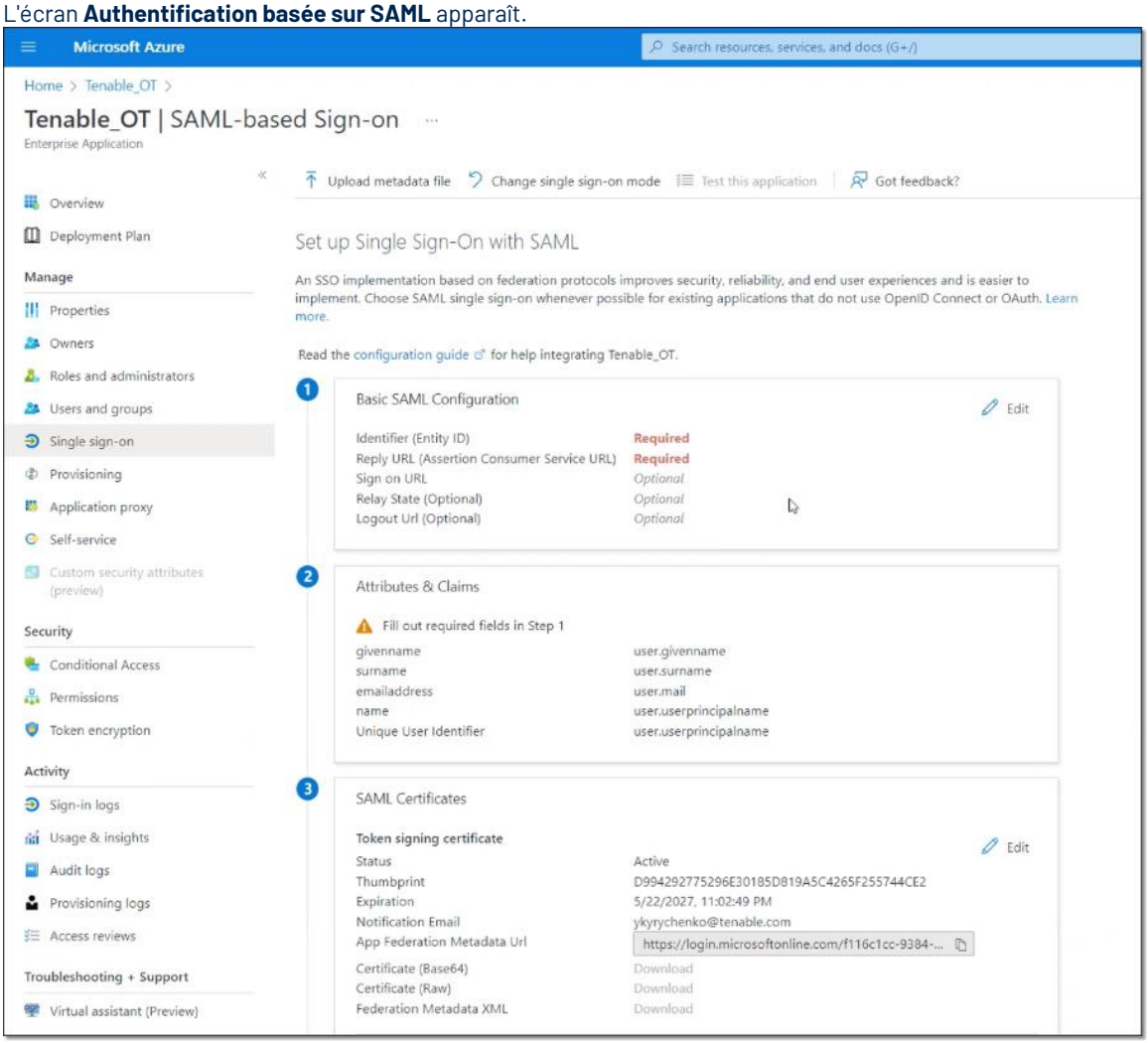
### Étape 2 – Configuration initiale

Cette étape est la configuration initiale de l'application Tenable.ot dans Azure, consistant à créer des valeurs temporaires pour l'identifiant et l'URL de réponse de la configuration SAML de base, afin de permettre le téléchargement du certificat requis.

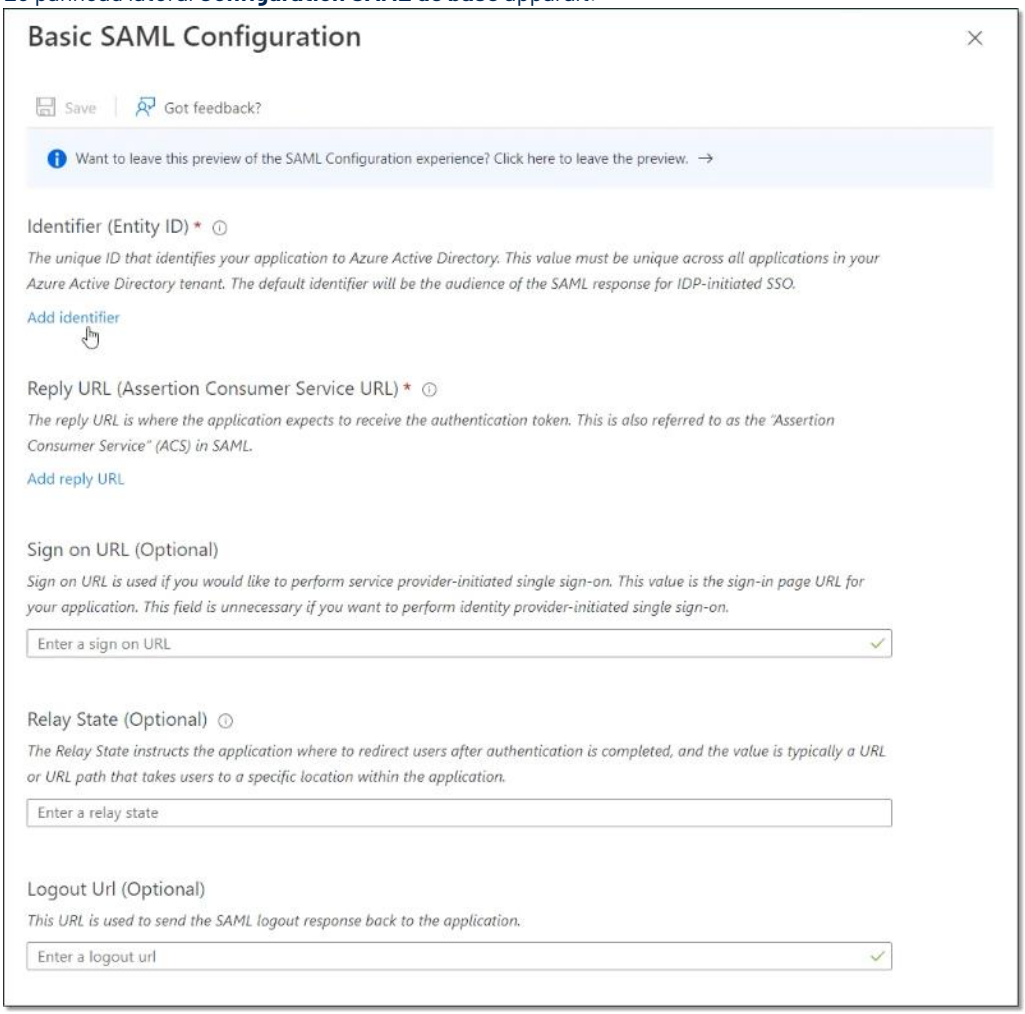
> Seuls les champs spécifiés dans cette procédure doivent être configurés. D'autres champs peuvent conserver leurs valeurs par défaut.

#### Pour réaliser la configuration initiale :

1. Dans le menu de navigation de **Microsoft Azure Active Directory**, cliquez sur **Authentification unique**, puis sélectionnez **SAML** comme méthode d'authentification unique.
   L'écran **Authentification basée sur SAML** apparaît.



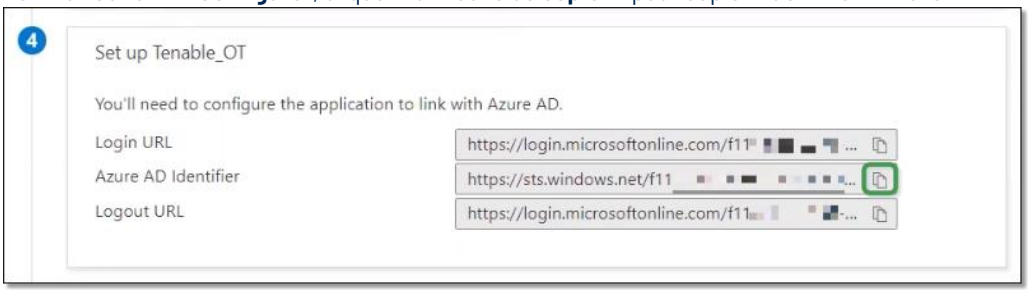
2. Dans la section 1 – **Configuration SAML de base**, cliquez sur Modifier.
Le panneau latéral **Configuration SAML de base** apparaît.



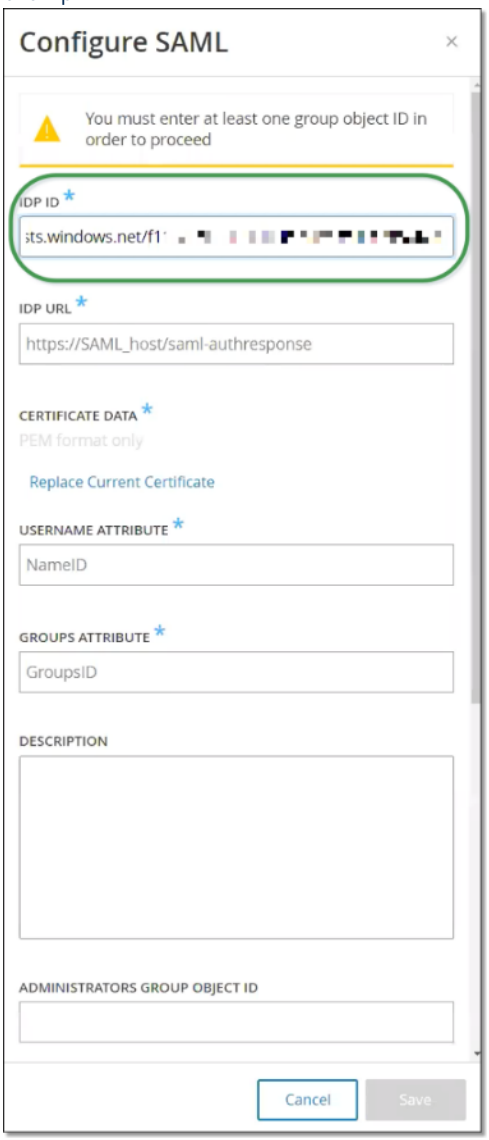

3. Dans le champ **Identificateur (ID de l'entité)**, saisissez un identifiant temporaire pour l'application Tenable (par exemple, tenable_ot).
4. Dans le champ **URL de réponse (URL du service consommateur d'assertion)**, saisissez une URL valide (par exemple, https://tenable.ot).

> L'identifiant et l'URL de réponse seront modifiés plus tard dans le processus de configuration.

5. Cliquez sur **Enregistrer** pour enregistrer les valeurs temporaires et fermer le panneau latéral **Configuration SAML de base**.
6. Dans la section 4 – **Configurer**, cliquez sur l'icône de **copie** pour copier l'**identifiant Azure AD**.

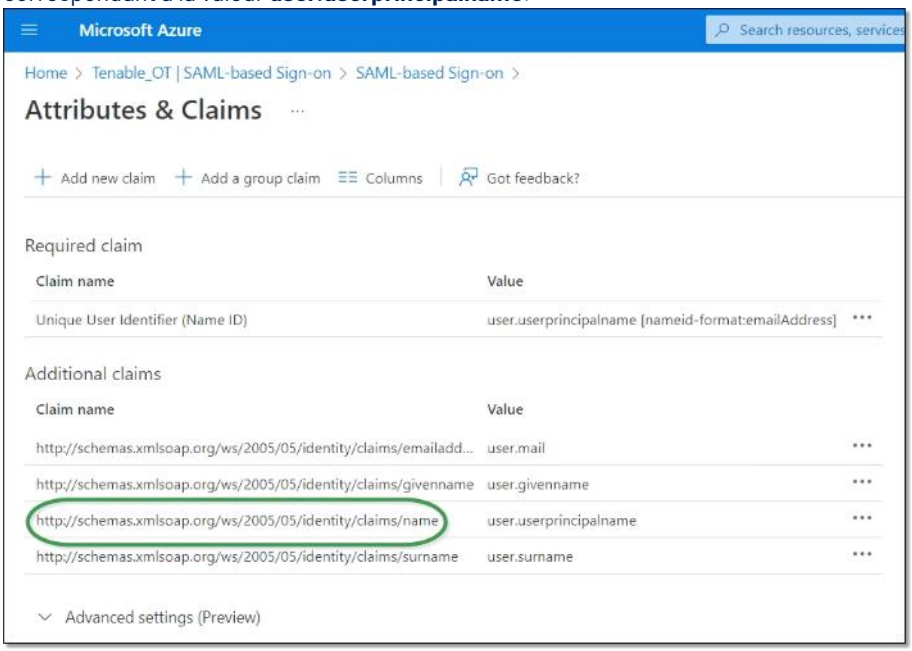


7. Basculez vers la console **Tenable.ot** et accédez à **Utilisateurs et rôles > SAML.**
8. Cliquez sur **Configurer** pour afficher le panneau latéral **Configurer SAML** et collez la valeur copiée dans le champ **ID IDP**.

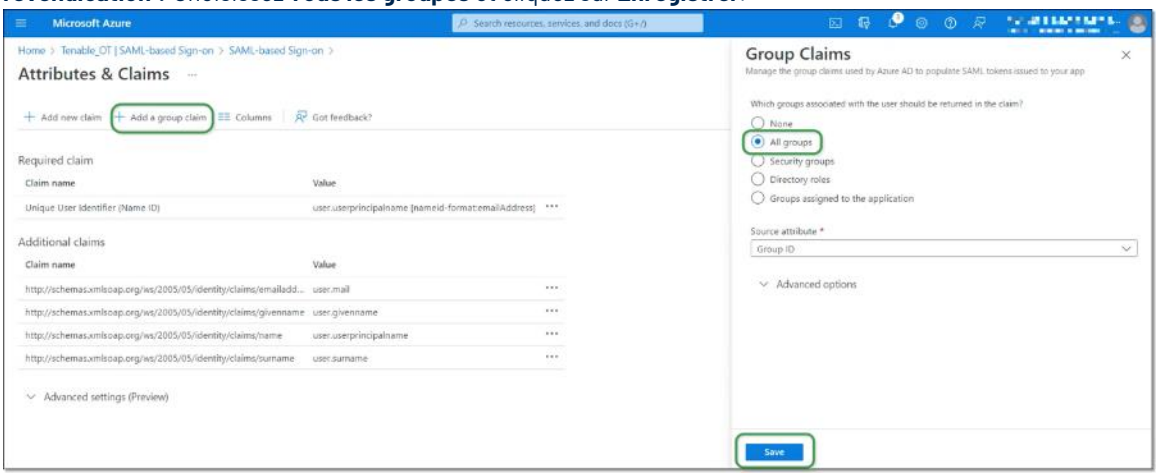



9. Dans la console **Azure**, cliquez sur l'icône pour copier l'**URL de connexion**.
10. Revenez à la console **Tenable.ot** et collez la valeur copiée dans le champ **URL IDP**.
11. Dans la console **Azure**, dans la section 3 – **Certificats SAML**, pour **Certificat (Base64)**, cliquez sur **Télécharger**.
12. Revenez à la console **Tenable.ot** et sous **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. Sous **Revendications supplémentaires**, sélectionnez et copiez l'URL du **nom de la revendication** correspondant à la valeur **user.userprincipalname**.

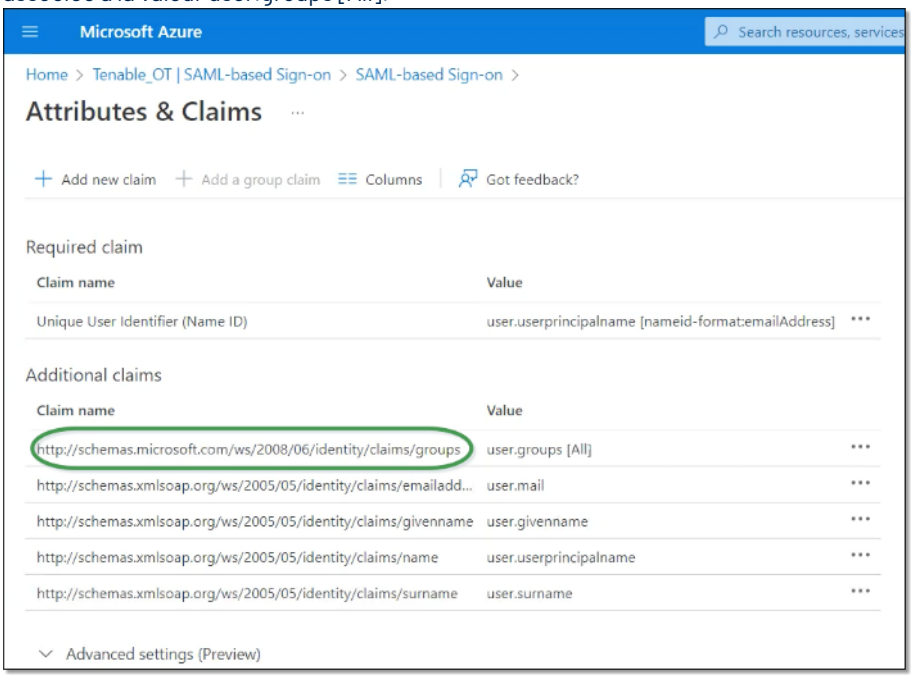



15. Revenez à la console **Tenable** et collez cette URL dans le champ **Attribut de nom d'utilisateur**.
16. Dans la console Azure, cliquez sur **+ Ajouter une revendication de groupe** pour afficher le panneau latéral **Revendications de groupe**, et sous **Quels groupes associés à l'utilisateur doivent être retournés dans la revendication ?** Choisissez **Tous les groupes** et cliquez sur **Enregistrer**.




Si des paramètres de groupes sont activés dans Microsoft Azure, vous pouvez choisir **Groupes attribués à l'application** au lieu de **Tous les groupes** ; Azure fournira alors uniquement les groupes d'utilisateurs qui sont attribués à l'application.

17. Sous **Revendications supplémentaires**, mettez en surbrillance et copiez l'URL du **nom de la revendication** associée à la valeur user.groups [All].




18. Revenez à la console **Tenable** et collez cette URL dans le champ **Attribut des groupes**.
19. Pour ajouter une description de la configuration SAML, saisissez-la dans le champ **Description**.

### Étape 3 – Mappage des utilisateurs Azure aux groupes Tenable

Dans cette étape, les utilisateurs d'Azure Active Directory sont assignés à l'application Tenable.ot. Les autorisations accordées à chaque utilisateur sont désignées par mappage entre les groupes Azure auxquels ils sont affectés et un groupe d'utilisateurs Tenable.ot prédéfini, auquel est associé un rôle et un ensemble d'autorisations. Les groupes d'utilisateurs prédéfinis de Tenable.ot sont : *Administrateurs*, *Utilisateurs en lecture seule*, *Analystes de sécurité*, *Gestionnaires de sécurité*, *Opérateurs de site* et *Superviseurs*. Pour plus d'informations, voir **Groupes d'utilisateurs**. Chaque utilisateur Azure doit être affecté à au moins un groupe mappé à un groupe d'utilisateurs Tenable.ot.

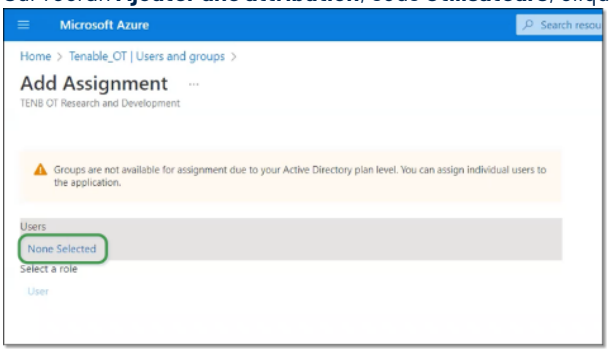
Les utilisateurs administrateurs connectés via SAML sont considérés comme des utilisateurs administrateurs (externes) et ne bénéficient pas de tous les privilèges des administrateurs locaux.

Les utilisateurs affectés à plusieurs groupes d'utilisateurs reçoivent les autorisations les plus élevées possibles parmi leurs groupes.

#### ➡ Pour mapper les utilisateurs Azure à Tenable.ot :

1. Dans **Microsoft Azure**, accédez à la page **Utilisateurs et groupes** et cliquez sur **+ Ajouter un utilisateur/groupe**.

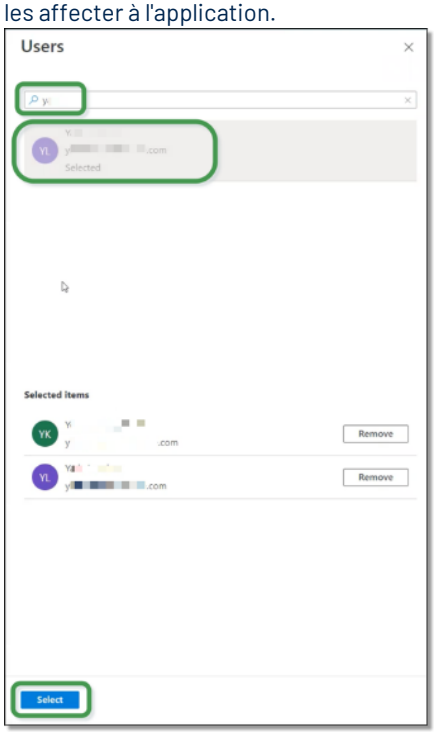
2. Sur l'écran **Ajouter une attribution**, sous **Utilisateurs**, cliquez sur **Aucune sélection**.




Le panneau latéral **Utilisateurs** apparaît.

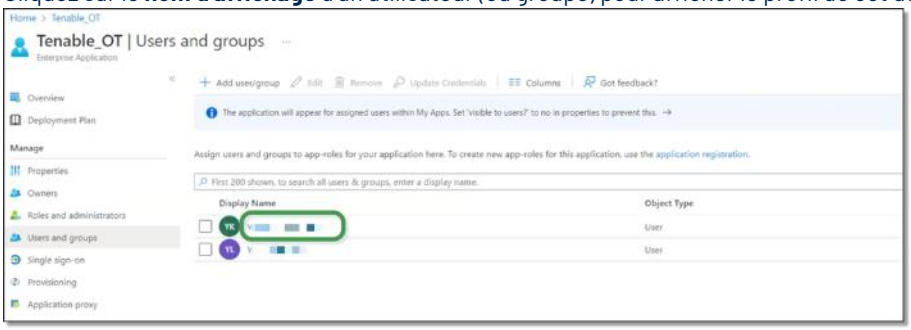
> Si des paramètres de groupes sont activés dans Microsoft Azure et que vous avez précédemment sélectionné **Groupes attribués à l'application** au lieu de Tous les groupes, vous pouvez choisir d'attribuer des groupes plutôt que des utilisateurs individuels.

3. Recherchez et cliquez sur tous les utilisateurs souhaités, puis cliquez sur **Sélectionner**, puis sur **Attribuer** pour les affecter à l'application.

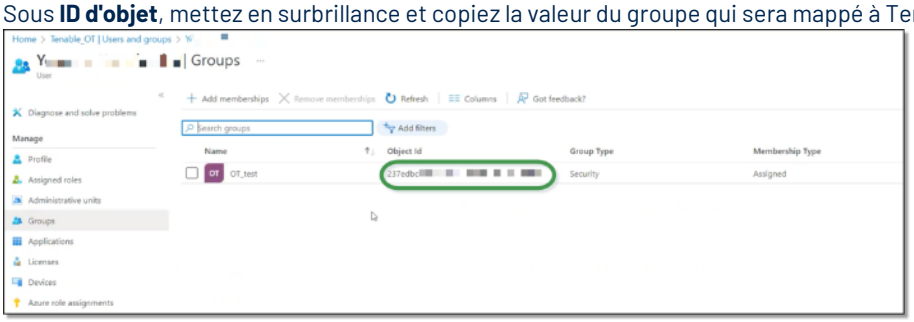



La page **Utilisateurs et groupes** apparaît.

4. Cliquez sur le **nom d'affichage** d'un utilisateur (ou groupe) pour afficher le profil de cet utilisateur (ou groupe).

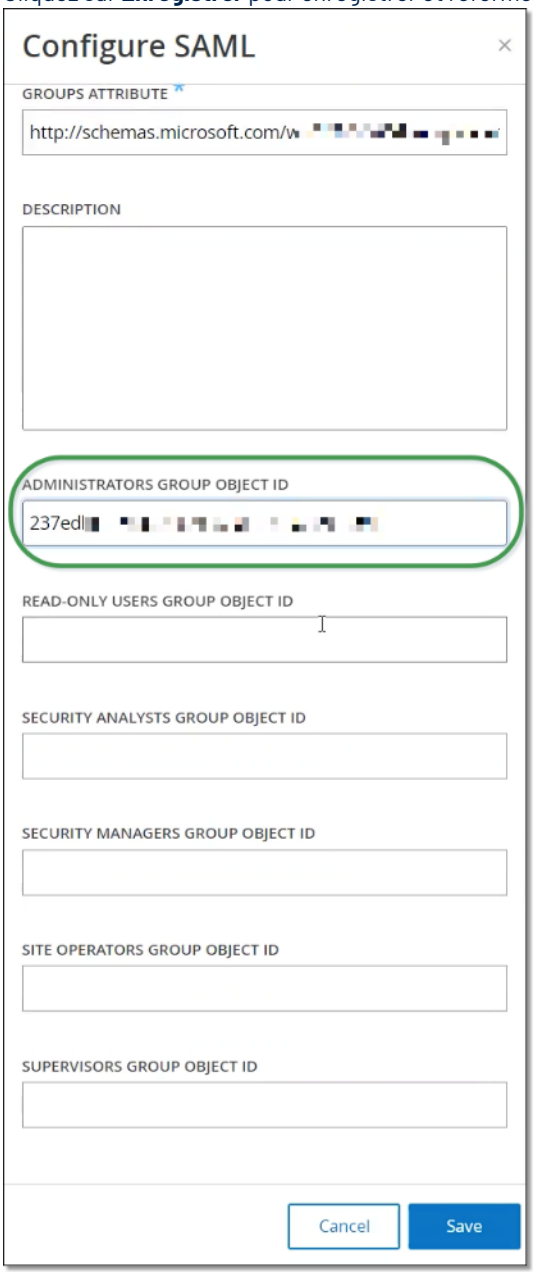



5. Sur l'écran **Profil**, dans la barre de navigation de gauche, sélectionnez **Groupes** pour afficher l'écran **Groupes**.
6. Sous **ID d'objet**, mettez en surbrillance et copiez la valeur du groupe qui sera mappé à Tenable.

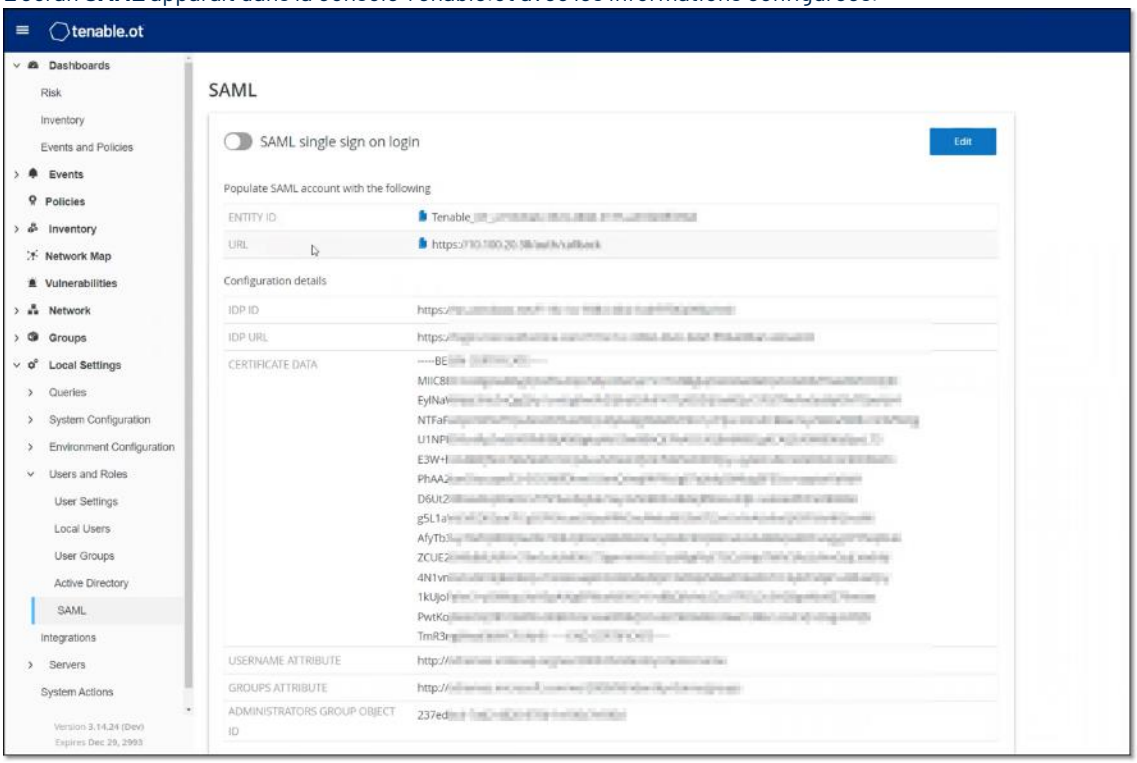



7. Revenez à la console **Tenable.ot** et collez la valeur copiée dans le champ **ID d'objet de groupe** souhaité (par exemple, ID d'objet de groupe d'administrateurs).
8. Répétez les étapes 1 à 7 pour chaque groupe que vous souhaitez mapper à un groupe d'utilisateurs distinct dans Tenable.ot.

9. Cliquez sur **Enregistrer** pour enregistrer et refermer le panneau latéral.



L'écran **SAML** apparaît dans la console Tenable.ot avec les informations configurées.



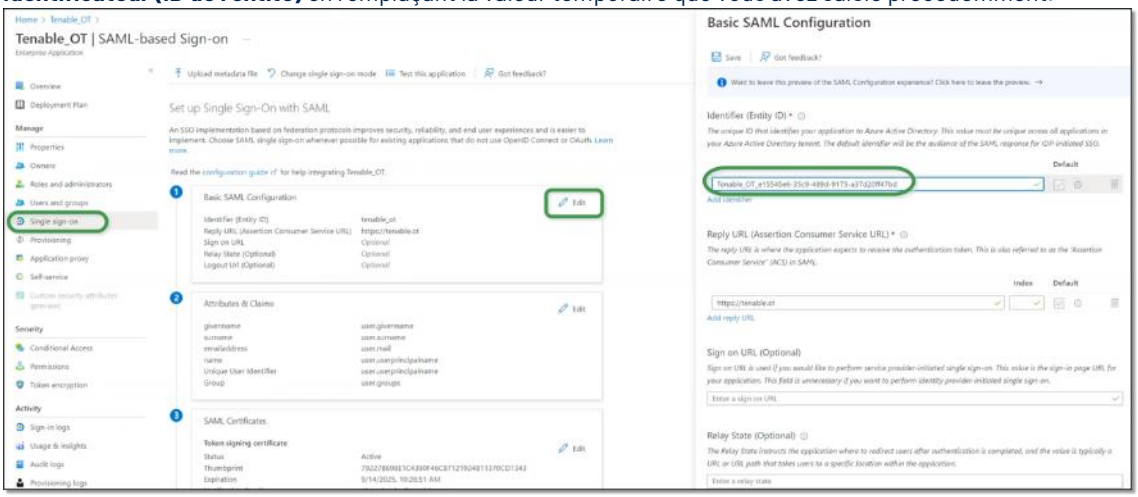

## Étape 4 – Finalisation de la configuration dans Azure

### ➡ Pour finaliser la configuration dans SAML :

1. Sur l'écran Tenable.ot **SAML**, sous **ID de l'entité**, cliquez sur l'icône de copie .


2. Basculez vers l'écran **Azure** et cliquez sur **Authentification unique** dans le menu de navigation de gauche pour ouvrir la page **Authentification basée sur SAML**.

3. Dans la section 1 – **Configuration SAML de base**, cliquez sur **Modifier** et collez la valeur copiée dans le champ **Identificateur (ID de l'entité)** en remplaçant la valeur temporaire que vous avez saisie précédemment.



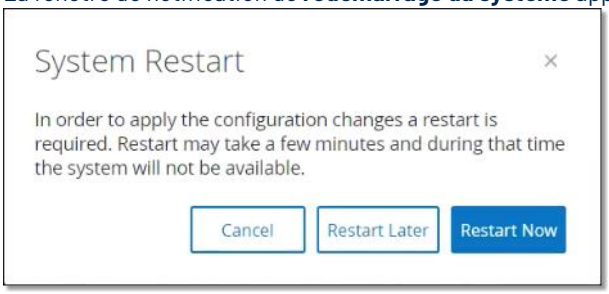

4. Retournez sur l'écran **SAML**, et sous **URL**, cliquez sur l'icône de copie .
5. Dans la console **Azure**, et dans le panneau latéral **Configuration SAML de base**, sous **URL de réponse (URL du service consommateur d'assertion)**, collez l'URL copiée en remplaçant l'URL temporaire que vous avez saisie précédemment.
6. Cliquez sur **Enregistrer** pour enregistrer la configuration et fermer le panneau latéral.
   La configuration est terminée et la connexion apparaît sur l'écran **Applications Azure Enterprise**.

## Étape 5 – Activation de l'intégration

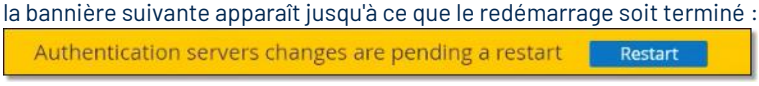
Pour activer l'intégration SAML, Tenable.ot doit être redémarré. L'utilisateur peut redémarrer le système immédiatement ou choisir de le redémarrer plus tard.

### Pour activer l'intégration :

1. Dans la console Tenable.ot, sur l'écran **SAML**, **activez** le curseur **Connexion unique 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 :



# Connexion à l'aide d'une authentification unique (SSO)

Au redémarrage, la fenêtre de connexion **Tenable.ot** comporte un nouveau lien **Sign in via SSO** (Se connecter via SSO) sous le bouton Se connecter. Les utilisateurs Azure qui ont été affectés à Tenable.ot peuvent se connecter à Tenable.ot à l'aide de leur compte Azure.

### Pour se connecter via SSO :

1. Sur l'écran de connexion **Tenable.ot**, cliquez sur le lien **Sign in via SSO** (Se connecter via SSO).


Si vous êtes déjà connecté à Azure, vous êtes dirigé directement vers la console Tenable.ot, sinon vous êtes redirigé vers la page de connexion Azure.
Les utilisateurs possédant plusieurs comptes sont redirigés vers la page Microsoft **Choisir un compte**, où ils peuvent sélectionner le compte souhaité pour la connexion.