



# Fore Scout®

## Appliance unique

### Guide d'installation rapide

Version 8.2



## Informations de contact

Forescout Technologies, Inc.

190 West Tasman Drive

San José, CA 95134, États-Unis

<https://www.forescout.com/support/>

Numéro gratuit (États-Unis) : 1.866.377.8771

Tél. (international) : 1.408.213.3191

Assistance : 1.708.237.6591

## À propos de la documentation

- Pour obtenir de la documentation technique supplémentaire, consultez la page Ressources à l'adresse <https://www.forescout.com/company/resources/>.
- Vous avez des commentaires ou des questions ? Écrivez-nous à l'adresse [documentation@forescout.com](mailto:documentation@forescout.com).

## Mentions légales

© 2019 Forescout Technologies, Inc. Tous droits réservés. Forescout Technologies, Inc. est une société du Delaware. Vous trouverez une liste de nos marques commerciales et brevets à l'adresse <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Les autres noms de marques, produits ou services peuvent être des marques de commerce ou de service de leurs propriétaires respectifs.

2020-02-11 12:08

# Table des matières

<b>Bienvenue dans la version 8.2</b> .....	<b>5</b>
Inclus dans votre pack Forescout.....	5
<b>Présentation</b> .....	<b>6</b>
<b>1. Créer un plan de déploiement</b> .....	<b>6</b>
Décider de l'endroit où vous souhaitez déployer l'appliance .....	6
Connexions de l'interface de l'appliance.....	6
Interface de gestion.....	6
Interface de surveillance .....	10
Interface de réponse.....	10
<b>2. Configurer votre commutateur</b> .....	<b>11</b>
A. Options de connexion du commutateur.....	11
1 Déploiement standard (interfaces de gestion, de surveillance et de réponse séparées).....	11
2 Prise de ligne passive.....	11
3 Prise de signal active (à capacité d'injection) .....	11
4 Réponse de couche IP (pour les installations de commutateur de couche 3) .....	12
B. Notes sur le réglage du commutateur.....	12
Balises VLAN (802.1Q).....	12
Consignes supplémentaires.....	12
<b>3. Brancher les câbles réseau et mettre sous tension</b> .....	<b>14</b>
A. Déballez l'appliance et branchez les câbles .....	14
B. Enregistrer les affectations d'interface .....	14
C. Mettre l'appliance sous tension.....	15
<b>4. Configurer l'appliance</b> .....	<b>16</b>
<b>5. Gestion à distance</b> .....	<b>22</b>
Configuration d'iDRAC.....	22
Activer et configurer le module iDRAC .....	22
Connecter le module au réseau .....	25
Se connecter à iDRAC .....	25
<b>6. Vérifier la connectivité</b> .....	<b>27</b>
Vérifier la connexion de l'interface de gestion .....	27
Exécuter un test ping.....	27
<b>7. Configurer la console Forescout</b> .....	<b>28</b>
Installer la console .....	28
Se connecter .....	28
Exécuter la configuration initiale.....	29
Avant de procéder à la configuration initiale .....	30

<b>Documentation supplémentaire de Forescout .....</b>	<b>31</b>
Modules de téléchargement de documents .....	31
Portail de documentation .....	32
Outils Help (Aide) de Forescout .....	32

## Bienvenue dans la version 8.2

La plateforme Forescout offre une visibilité de l'infrastructure et des périphériques, une gestion des politiques, une orchestration et une rationalisation des flux de travail pour améliorer la sécurité des réseaux. Cette plateforme fournit aux entreprises des informations contextuelles en temps réel au sujet des périphériques et des utilisateurs sur le réseau. Les politiques sont définies à l'aide de ces informations contextuelles qui permettent de garantir la conformité, une correction, un accès réseau approprié et la rationalisation des opérations de service.

**Ce guide décrit l'installation d'une appliance CounterACT unique et autonome préinstallée avec la version 8.0. Il se peut que certaines appliances soient préinstallées avec une version ultérieure. Pour utiliser la version 8.2, suivez le chemin de mise à niveau approuvé indiqué dans les Notes de publication de cette dernière.**



Pour plus d'informations sur la mise à niveau ou le déploiement de plusieurs appliances pour la protection d'un réseau d'entreprise, consultez le *Guide d'installation de Forescout* et le *Guide d'administration de Forescout*. Pour plus d'informations sur l'accès à ces guides, consultez la section [Documentation supplémentaire de Forescout](#).

Vous pouvez, en outre, accéder au site Web d'assistance à l'adresse <http://www.forescout.com/support> pour obtenir la documentation, les articles de base de connaissances et les mises à jour les plus récents concernant votre appliance.

## Inclus dans votre pack Forescout

Le pack Forescout comprend les éléments suivants :

- Appliance CounterACT
- Panneau frontal
- Kits de rail (supports de montage)
- Cordon(s) d'alimentation
- Câble de connexion de console DB9 (pour connexions série uniquement)
- Informations en matière de sécurité, d'environnement et de réglementation sur les produits de l'entreprise
- Document de prise en main (appliances CT-xxxx basées sur la révision matérielle des appliances 5x et Forescout 51xx uniquement)

# Présentation

Procédez comme suit pour configurer Forescout :

1. Créer un plan de déploiement
2. Configurer votre commutateur
3. Brancher les câbles réseau et mettre sous tension
4. Configurer l'appliance
5. Gestion à distance
6. Vérifier la connectivité
7. Configurer la console Forescout

## 1. Créer un plan de déploiement

Avant l'installation, vous devez décider de l'endroit où vous souhaitez déployer l'appliance et connaître les connexions de l'interface de l'appliance.

### Décider de l'endroit où vous souhaitez déployer l'appliance

Il est essentiel de choisir le bon emplacement d'installation de l'appliance pour garantir la réussite du déploiement et des performances optimales. L'emplacement approprié dépend de vos objectifs de mise en œuvre et des politiques d'accès au réseau. L'appliance doit pouvoir surveiller le trafic pertinent pour la politique de votre choix. Par exemple, si votre politique dépend de la surveillance d'événements d'autorisation entre des points de terminaison et des serveurs d'authentification d'entreprise, l'appliance devra être installée de façon à ce qu'elle voie le trafic des points de terminaison se diriger vers le ou les serveurs d'authentification.

Pour plus d'informations sur l'installation et du déploiement, consultez le *Guide d'installation de Forescout*. Consultez la section [Documentation supplémentaire de Forescout](#) pour obtenir des informations sur l'accès à ce guide.

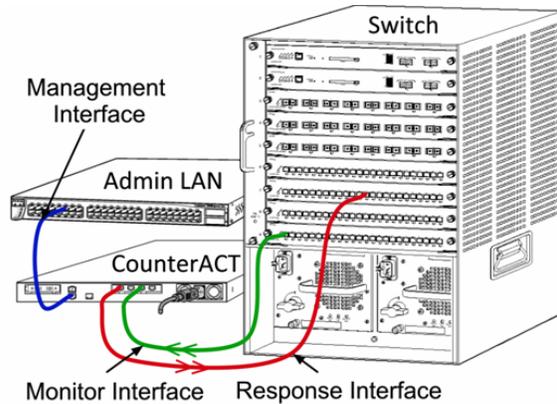
### Connexions de l'interface de l'appliance

En règle générale, l'appliance est configurée avec trois connexions vers le commutateur réseau.

#### Interface de gestion

L'interface de gestion vous permet de gérer la plateforme Forescout et d'exécuter des requêtes ainsi qu'une inspection approfondie des points de terminaison. L'interface doit être connectée à un port de commutation qui dispose d'un accès à tous les points de terminaison du réseau.

Chaque appliance requiert une connexion de gestion unique vers le réseau. Cette connexion nécessite une adresse IP sur le réseau local et un accès au port 13000/TCP depuis des machines qui exécuteront l'application de gestion de la console. Le port de gestion doit avoir accès à d'autres services réseau.



### Exigences d'accès au réseau

Port	Service	Depuis ou vers la plateforme Forescout	Fonction
22/TCP	SSH	Depuis	Permet une inspection à distance des points d'extrémité OS X et Linux. Permet à la plateforme Forescout de communiquer avec les commutateurs réseau et les routeurs.
		Vers	Permet d'accéder à l'interface de ligne de commande de la plateforme Forescout.
2222/TCP	SSH	Vers	(Haute disponibilité) Permet d'accéder aux appliances physiques qui font partie de la paire à haute disponibilité. Utilisez 22/TCP pour accéder à l'adresse IP partagée (virtuelle) de la paire.
25/TCP	SMTP	Depuis	Permet à la plateforme Forescout d'accéder au relais de messagerie de l'entreprise.
53/UDP	DNS	Depuis	Permet à la plateforme Forescout de résoudre des adresses IP internes.
80/TCP	HTTP	Vers	Autorise la redirection HTTP.
123/UDP	NTP	Depuis	Permet à la plateforme Forescout d'accéder à un serveur de temps local ou à ntp.forescout.net. La plateforme Forescout utilise ntp.forescout.net par défaut.

Port	Service	Depuis ou vers la plateforme Forescout	Fonction
135/TCP	MS-WMI	Depuis	Permet une inspection à distance des points de terminaison Windows.
139/TCP	SMB, MS-RPC	Depuis	Permet une inspection à distance des points de terminaison Windows (pour les points de terminaison exécutant Windows 7 et versions antérieures).
445/TCP			Permet une inspection à distance des points de terminaison Windows.
161/UDP	SNMP	Depuis	Permet à la plateforme Forescout de communiquer avec les commutateurs réseau et les routeurs. Pour plus d'informations sur la configuration du protocole SNMP, consultez le <i>Guide d'administration de Forescout</i> .
162/UDP	SNMP	Vers	Permet à la plateforme Forescout de recevoir des interruptions SNMP provenant des commutateurs réseau et des routeurs. Pour plus d'informations sur la configuration du protocole SNMP, consultez le <i>Guide d'administration de Forescout</i> .
389/TCP (636)	LDAP	Depuis	Permet à la plateforme Forescout de communiquer avec Active Directory. Permet la communication avec les portails Web de la plateforme Forescout.
443/TCP	HTTPS	Vers	Permet la redirection HTTP à l'aide de TLS.
2200/TCP	SecureConnector pour Linux	Vers	Permet à SecureConnector de créer une connexion sécurisée (SSH chiffré) vers l'appliance depuis des ordinateurs Linux. <i>SecureConnector</i> est un agent basé sur un script qui permet de gérer des points de terminaison Linux lorsqu'ils sont connectés au réseau.

Port	Service	Depuis ou vers la plateforme Forescout	Fonction
10003/TCP	SecureConnector pour Windows	Vers	<p>Permet à SecureConnector de créer une connexion sécurisée (TLS chiffré) à l'apppliance à partir d'ordinateurs Windows. <i>SecureConnector</i> est un agent qui permet de gérer des points de terminaison Windows lorsqu'ils sont connectés au réseau. Pour plus d'informations sur SecureConnector, consultez le <i>Guide d'administration de Forescout</i>.</p> <p>Lorsque SecureConnector se connecte à une alliance ou à Enterprise Manager, il est redirigé vers l'apppliance à laquelle son hôte est affecté. Vérifiez que ce port est ouvert pour toutes les appliances et pour Enterprise Manager afin d'assurer la transparence de la mobilité dans toute l'entreprise.</p>
10005/TCP	SecureConnector pour OS X	Vers	<p>Permet à SecureConnector de créer une connexion sécurisée (TLS chiffré) à l'apppliance à partir d'ordinateurs OS X. <i>SecureConnector</i> est un agent qui permet de gérer des points de terminaison OS X lorsqu'ils sont connectés au réseau. Pour plus d'informations sur SecureConnector, consultez le <i>Guide d'administration de Forescout</i>.</p> <p>Lorsque SecureConnector se connecte à une alliance ou à Enterprise Manager, il est redirigé vers l'apppliance à laquelle son hôte est affecté. Vérifiez que ce port est ouvert pour toutes les appliances et pour Enterprise Manager afin d'assurer la transparence de la mobilité dans toute l'entreprise.</p>
13000/TCP	Plateforme Forescout	Depuis/Vers	<p>Pour les déploiements avec une seule appliance : depuis la console vers l'apppliance.</p> <p>Pour les déploiements avec plusieurs appliances : depuis la console vers l'apppliance et depuis une appliance vers une autre. La communication de l'apppliance comprend la communication avec Enterprise Manager et Recovery Enterprise Manager, à l'aide de TLS.</p>

## Interface de surveillance

L'interface de surveillance permet à l'appliance de surveiller et de suivre le trafic réseau. Toute interface disponible peut être utilisée en tant qu'interface de surveillance.

Le trafic est mis en miroir sur un port du commutateur et surveillé par l'appliance. L'utilisation d'un balisage VLAN 802.1Q dépend du nombre de réseaux locaux virtuels (VLAN) mis en miroir.

- **VLAN unique** : lorsque le trafic surveillé est généré à partir d'un seul VLAN, le trafic mis en miroir n'a pas besoin de balisage VLAN.
- **Plusieurs VLAN** : si le trafic surveillé provient de plusieurs VLAN, le trafic mis en miroir doit avoir un balisage VLAN 802.1Q.

Lorsque deux commutateurs sont connectés sous forme de paire redondante, l'appliance doit surveiller le trafic provenant des deux commutateurs.

L'interface de surveillance ne nécessite pas d'adresse IP.

## Interface de réponse

L'appliance répond au trafic à l'aide de l'interface de réponse. Le trafic de réponse permet de se protéger contre les activités malveillantes et d'exécuter les actions de politique. Ces actions peuvent inclure, par exemple, la redirection de navigateurs Web ou l'exécution du blocage d'une session. La configuration du port de commutateur liée dépend du trafic surveillé.

Toute interface disponible peut être utilisée en tant qu'interface de réponse.

- **VLAN unique** : lorsque le trafic surveillé est généré à partir d'un seul VLAN, le port de réponse doit appartenir au même VLAN. Dans ce cas, l'appliance nécessite une adresse IP unique sur ce VLAN.
- **Plusieurs VLAN** : si le trafic surveillé provient de plusieurs VLAN, le port de réponse doit également être configuré avec un balisage VLAN 802.1Q pour les mêmes VLAN. L'appliance nécessite une adresse IP pour chaque VLAN surveillé.

## 2. Configurer votre commutateur

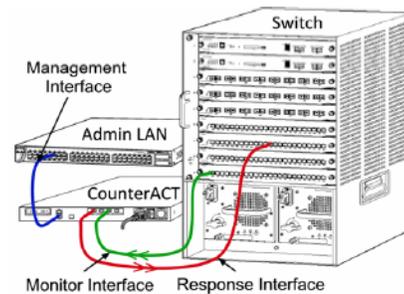
### A. Options de connexion du commutateur

L'appliance a été conçue pour s'intégrer de façon transparente à une grande variété d'environnements réseau. Pour intégrer correctement l'appliance dans votre réseau, vérifiez que votre commutateur est configuré pour surveiller le trafic requis.

Plusieurs options sont disponibles pour connecter l'appliance à votre commutateur.

#### 1 Déploiement standard (interfaces de gestion, de surveillance et de réponse séparées)

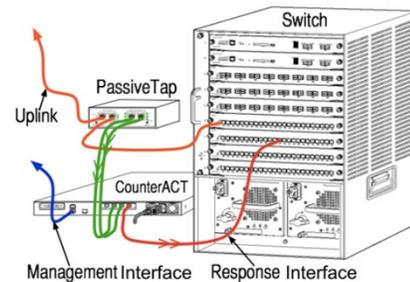
Le déploiement recommandé utilise trois ports séparés. Ces ports sont décrits dans la section [Connexions de l'interface](#) de l'appliance.



#### 2 Prise de ligne passive

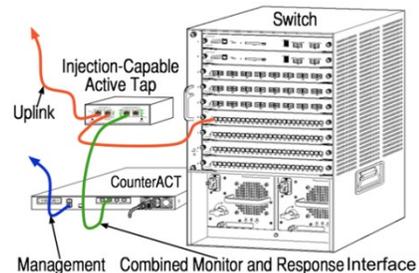
Au lieu de se connecter à un port de surveillance de commutateur, l'appliance peut utiliser une prise de signal passive.

Une prise passive nécessite deux ports de surveillance (un pour le trafic dans le sens ascendant et un pour le trafic dans le sens descendant), sauf dans le cas de prise de *recombinaison*, qui combine les deux flux duplex en un seul port. Notez que si le trafic sur le port de prise comporte un balisage VLAN 802.1Q, le port de réponse doit également avoir un balisage VLAN 802.1Q.



#### 3 Prise de signal active (à capacité d'injection)

L'appliance peut utiliser une prise de signal active. Si la prise est à capacité d'injection, l'appliance combine alors les ports de surveillance et de réponse, afin que la configuration d'un port de réponse séparé sur le commutateur ne soit pas nécessaire. Cette option peut être utilisée indépendamment du type de configuration de commutateur (en amont ou en aval).



## 4 Réponse de couche IP (pour les installations de commutateur de couche 3)

L'appliance peut utiliser sa propre interface de gestion pour répondre au trafic. Bien que cette option puisse être utilisée avec n'importe quel trafic surveillé, elle est recommandée uniquement lorsque l'appliance surveille des ports qui ne font partie d'aucun VLAN et que, par conséquent, elle ne peut pas répondre au trafic surveillé à l'aide d'un autre port de commutateur. Cette situation est typique lors de la surveillance d'une liaison connectant deux routeurs. Cette option ne peut pas répondre aux demandes de protocole ARP (Address Resolution Protocol), ce qui limite la capacité de l'appliance à détecter les analyses destinées aux adresses IP incluses dans le sous-réseau surveillé. Cette limite ne s'applique pas lorsque le trafic entre deux routeurs est surveillé.

## B. Notes sur le réglage du commutateur

### Balises VLAN (802.1Q)

- **Surveillance d'un VLAN unique** : si le trafic surveillé provient d'un VLAN unique, le trafic n'a pas besoin de balises VLAN 802.1Q.
- **Surveillance de plusieurs VLAN** : si le trafic surveillé provient de deux VLAN ou plus, le port de surveillance et le port de réponse doivent accepter les balises VLAN 802.1Q. La surveillance de plusieurs VLAN est l'option recommandée, car elle offre la meilleure couverture globale tout en minimisant le nombre de ports de mise en miroir.
- Si le commutateur ne peut pas utiliser de balise VLAN 802.1Q sur le port de mise en miroir, effectuez l'une des actions suivantes :
  - Mettre en miroir un seul VLAN
  - Mettre en miroir un seul port de liaison montante sans balise
  - Utiliser l'option de réponse de couche IP
- Si le commutateur ne peut mettre en miroir qu'un seul port, mettez en miroir un port de liaison montante unique. Celui-ci peut comporter une balise. En général, si le commutateur supprime les balises VLAN 802.1Q, vous devez utiliser l'option de réponse de couche IP.

### Consignes supplémentaires

- Dans les cas suivants, vous devez mettre en miroir juste une interface (cela autorise la transmission/réception) :
  - Si le commutateur ne peut pas mettre en miroir le trafic transmis et le trafic reçu
  - Si le commutateur ne peut pas mettre en miroir tout le trafic de commutateur
  - Si le commutateur ne peut pas mettre en miroir tout le trafic sur un VLAN
- Veillez à ne pas surcharger le port de mise en miroir.

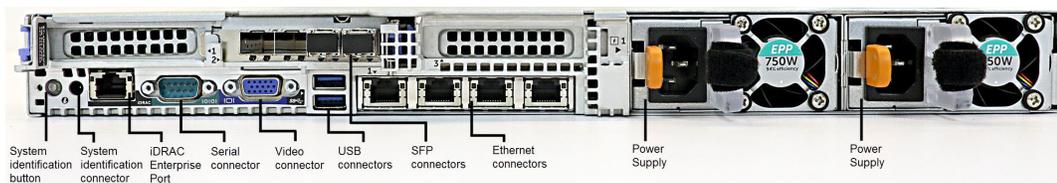
- Pour certains commutateurs (tels que Cisco 6509), il peut être nécessaire de supprimer complètement la configuration existante du port avant d'en entrer une nouvelle. La non-suppression des anciennes informations sur le port résulte souvent à la suppression des balises 802.1Q par le commutateur.

## 3. Brancher les câbles réseau et mettre sous tension

### A. Débarrer l'appliance et brancher les câbles

1. Sortez l'appliance et le câble d'alimentation de leur emballage de transport.
2. Sortez le kit de rails que vous avez reçu avec l'appliance.
3. Montez le kit de rails sur l'appliance et fixez l'appliance sur le support.
4. Branchez les câbles réseau entre les interfaces réseau sur le panneau arrière de l'appliance et les ports de commutateur.

#### Exemple de panneau arrière – Appliance Forescout



Vous pouvez remplacer les modules SFP fournis par Forescout par des modules SFP de Finisar qui ont été testés et approuvés par Forescout. Pour plus d'informations, consultez le *Guide d'installation de Forescout*.

### B. Enregistrer les affectations d'interface

Après avoir terminé l'installation de l'appliance sur le centre de données et installé la console Forescout, vous êtes invité à enregistrer les affectations d'interface. Ces affectations, appelées *définitions de canal*, sont entrées dans l'assistant de configuration initiale qui s'ouvre lors de votre première session sur la console.

Enregistrez les affectations d'interface physique ci-dessous et utilisez-les lorsque vous avez terminé la configuration de canal sur la console.

Interface Ethernet	Affectation d'interface (p. ex. Gestion, Surveillance, Réponse)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	

## C. Mettre l'apppliance sous tension

1. Branchez le câble d'alimentation à la prise d'alimentation sur le panneau arrière de l'apppliance.
2. Branchez l'autre extrémité du câble d'alimentation à une prise secteur mise à la terre.
3. Branchez le clavier et l'écran à l'apppliance ou configurez l'apppliance pour une connexion série. Pour plus d'informations, consultez le *Guide d'installation de Forescout*.
4. Mettez l'apppliance sous tension depuis le panneau avant.

## 4. Configurer l'appliance

Préparez les informations suivantes avant de configurer l'appliance.

Nom d'hôte de l'appliance	
Mot de passe d'administrateur de Forescout	Conserver le mot de passe dans un endroit sûr
Interface de gestion	
Adresse IP de l'appliance	
Masque de réseau	
Adresse IP de la passerelle par défaut	
Nom de domaine DNS	
Adresses du serveur DNS	

Après la mise sous tension, vous êtes invité à démarrer la configuration avec le message suivant :

- ☞ *Les invites suivantes sont basées sur la version 8.0. Il se peut que certaines appliances soient préinstallées avec une version comportant des invites légèrement différentes.*

```
CounterACT Appliance boot is complete.
Press <Enter> to continue. (Le démarrage de l'appliance
CounterAct est terminé. Appuyez sur <Entrée> pour continuer.)
```

- 1. Appuyez sur **Enter** (Entrée).** Si votre appliance est Forescout 51xx, le menu suivant s'affiche :

```
CounterACT <version>-<build> options:

1) Configure Forescout Device
2) Restore saved Forescout configuration
3) Identify and renumber network interfaces
4) Configure keyboard layout
5) Turn machine off
6) Reboot the machine

Choice (1-6) :1
```

```
(Options de CounterAct <version>-<build> :
1) Configurer le dispositif Forescout
2) Restaurer la configuration Forescout enregistrée
3) Identifier et renuméroter les interfaces réseau
4) Configurer la disposition du clavier
5) Éteindre la machine
6) Redémarrer la machine
Choix (1 à 6) :1)
```

Si votre appliance est CT-xxxx, la version répertoriée CounterACT 7.0.0 ou CounterACT 8.0.0 apparaîtra en haut du menu.

- Si CounterACT 7.0.0 s'affiche, vous pouvez mettre à niveau vers la version 8.0.0 ou installer cette nouvelle version. Pour plus d'informations, consultez le *Guide d'installation de Forescout*. Après avoir installé la version 8.0.0 ou effectué une mise à niveau vers cette nouvelle version, le menu mentionné ci-dessus apparaîtra.
- Si CounterACT 8.0.0 s'affiche, le menu offre la possibilité d'installer la version 7.0.0 ou de configurer la version 8.0.0, comme indiqué ci-dessous. Si vous choisissez la version 7.0.0, vous ne pourrez plus réinstaller la version 8.0.0 via le menu Configuration. Pour plus d'informations sur la configuration de la version 7.0.0, consultez le *Guide d'installation de Forescout, version 7.0.0*.

```
CounterACT 8.0.0-<version> options:

1) Install CounterACT 7.0.0-<version>
2) Configure CounterACT 8.0.0-<version>
3) Restore saved CounterACT configuration
4) Identify and renumber network interfaces
5) Configure keyboard layout
6) Turn machine off
7) Reboot the machine
Choice (1-7) :

(Options de CounterACT 8.0.0-<version>
1) Installer CounterAct 7.0.0-<version>
2) Configurer CounterACT 8.0.0-<version>
3) Restaurer la configuration CounterACT enregistrée
4) Identifier et renuméroter les interfaces réseau
5) Configurer la disposition du clavier
6) Éteindre la machine
7) Redémarrer la machine
Choix (1 à 7) :)
```

📖 *En cas d'interruption de la configuration ou si vous avez choisi la mauvaise version, vous devrez réinitialiser l'appliance avec la version adéquate du fichier ISO. Pour plus d'informations sur la réinitialisation d'une appliance, consultez le Guide d'installation de Forescout.*

**2.** Saisissez **1** et appuyez sur **Enter** (Entrée).

```

Select High Availability mode:

1) Standard Installation
2) High Availability - Primary Node
3) Add node to existing Active Node (Primary or Secondary)

Choice (1-3) [1] :

(Sélectionnez le mode Haute disponibilité :

1) Installation standard
2) Haute disponibilité - Nœud primaire
3) Ajouter le nœud au nœud actif existant (primaire ou
secondaire)

Choix (1 à 3) [1] :)

```

### 3. Saisissez **1** (Installation standard) et appuyez sur **Enter** (Entrée).

```

>>>>> Forescout platform Initial Setup <<<<<<

You are about to setup the Forescout platform. During the
initial setup process you will be prompted for basic parameters
used to connect this machine to the network.
When this phase is complete, you will be instructed to complete
the setup from the Forescout Console.
Continue ? (yes/no):

(>>>>> Configuration initiale de la plateforme Forescout <<<<<<

Vous êtes sur le point de configurer la plateforme Forescout. Au
cours du processus de configuration initiale, les paramètres de
base utilisés pour connecter cette machine au réseau vous seront
demandés.
À la fin de cette phase, il vous sera demandé de terminer la
configuration à partir de la console Forescout.
Continuer ? (oui/non):)

```

### 4. Saisissez **Yes** (Oui) et appuyez sur **Enter** (Entrée).

 L'invite suivante s'ouvre lors de l'exécution d'une installation 8.2 propre.

```

Certification Compliance Mode? (yes/no) [no] :
(Mode de conformité de la certification ? (oui/non) [non] :)

```

### 5. À moins que votre entreprise n'ait à se conformer à des critères communs et une certification DoDIN APL, saisissez **No** (Non) et appuyez sur **Enter** (Entrée).

```

>>>>> Select CounterACT Installation Type <<<<<<

1) CounterACT Appliance
2) CounterACT Enterprise Manager

Choice (1-2) :

```

```
(>>>>> Sélectionner le type d'installation CounterACT <<<<<<

1) Appliance CounterACT
2) Enterprise Manager CounterACT

Choix (1 à 2) :)
```

- 6.** Saisissez **1** et appuyez sur **Enter** (Entrée). La configuration est initialisée. Ce processus peut prendre quelques minutes.

```
>>>>> Select Licensing Mode <<<<<<

1) Per Appliance licensing mode
2) Flexx licensing mode

Choice (1-2) [1]:

(>>>>> Sélectionner le mode de licence <<<<<<

1) Mode de licence selon l'apppliance
2) Mode de licence Flexx

Choix (1 à 2) [1]:)
```

- 7.** Sélectionnez le mode de licence utilisé par votre déploiement. Le mode de licence est déterminé lors de l'achat. **Ne saisissez aucune valeur tant que vous n'avez pas vérifié le mode de licence utilisé par votre déploiement.** Contactez votre représentant des ventes Forescout pour vérifier votre mode de licence ou si vous avez saisi le mauvais mode.

 Cette option ne s'affiche pas sur les appliances Forescout 51xx.

- 8.** Saisissez **1** pour le mode de licence selon l'apppliance ou **2** pour le mode de licence Flexx, puis appuyez sur **Enter** (Entrée).

```
>>>>> Enter Machine Description <<<<<<

Enter a short description of this machine (e.g. New York office).

Description :

(>>>>> Saisir une description de la machine <<<<<<

Saisissez une courte description de cette machine (p. ex. : bureau
de New York).

Description :)
```

- 9.** Saisissez une description et appuyez sur **Enter** (Entrée).

Le message suivant s'affiche :

```
>>>>> Set Administrator Password <<<<<<
```

```

This password will be used to log in as 'cliadmin' to the
machine Operating System and as 'admin' to the CounterACT
Console.
The password must be between 6 and 15 characters long and should
contain at least one non-alphabetic character.
Administrator password :
(>>>>> Définir le mot de passe d'administrateur <<<<<<<
Ce mot de passe est utilisé pour se connecter en tant
qu'utilisateur « racine » au système d'exploitation de la
machine et en tant qu'utilisateur « admin » à la console
CounterACT. Le mot de passe doit contenir entre 6 et
15 caractères, dont au moins un caractère non alphabétique.
Mot de passe d'administrateur :)

```

**10.**À l'invite Set Administrator Password (Définir le mot de passe d'administrateur), saisissez la chaîne qui sera votre mot de passe (la chaîne de caractères n'apparaît pas à l'écran) et appuyez sur **Enter** (Entrée). Vous êtes invité à confirmer le mot de passe. Le mot de passe doit contenir entre 6 et 15 caractères, dont au moins un caractère non alphabétique.

 *Connectez-vous à l'appliance en tant qu'utilisateur cliadmin et connectez-vous à la console en tant qu'utilisateur admin.*

**11.**À l'invite Set Host Name (Définir le nom d'hôte), saisissez un nom d'hôte et appuyez sur **Enter** (Entrée). Le nom d'hôte peut être utilisé lors de la connexion à la console. Il est affiché sur la console pour vous aider à identifier l'appliance CounterACT que vous voyez. Le nom d'hôte ne doit pas dépasser 13 caractères.

**12.**L'écran Configure Network Settings (Configurer les paramètres réseau) vous invite à entrer une série de paramètres de configuration. Saisissez une valeur à chaque invite et appuyez sur **Enter** (Entrée) pour afficher la prochaine invite.

- Les composants de la plateforme Forescout communiquent via des interfaces de gestion. Le nombre d'interfaces de gestion répertoriées dépend du modèle de l'appliance.
- **Management IP address** (Adresse IP de gestion) est l'adresse de l'interface via laquelle les composants de la plateforme Forescout communiquent. Ajoutez un ID VLAN pour cette interface seulement si l'interface utilisée pour communiquer entre les composants de la plateforme Forescout est connectée à un port avec balise.
- S'il y a plusieurs **DNS server address** (adresses de serveur DNS), séparez-les avec un espace. La plupart des serveurs DNS internes résolvent les adresses externes et internes, mais il peut être nécessaire d'inclure un serveur DNS résolvant en externe. Comme la grande majorité des requêtes DNS exécutées par l'appliance sont destinées à des adresses internes, le serveur DNS externe doit être répertorié en dernier.

**13.**L'écran Setup Summary (Résumé de la configuration) s'affiche. Vous êtes invité à effectuer des tests de connectivité générale, à reconfigurer les paramètres ou à terminer la configuration. Saisissez **D** pour terminer la configuration.

## **Licence**

Après la configuration, vérifiez si une licence valide est disponible sur votre appliance. L'état de la licence par défaut de votre périphérique appliance dépend du mode de licence utilisé par votre déploiement.

- Si votre déploiement Forescout fonctionne avec **Per-Appliance Licensing Mode** (Mode de licence selon l'appliance), vous pouvez déjà commencer à travailler avec la licence de démo, qui est valide pendant 30 jours. Pendant cette période, Forescout doit vous fournir une licence permanente, et vous devez la placer dans un dossier accessible sur votre disque ou réseau. Installez la licence depuis cet emplacement avant l'expiration de la licence de démo de 30 jours (vous pouvez demander une prolongation de la licence de démo, au besoin).

Vous serez informé de différentes manières lorsque votre licence de démo arrivera à expiration. Pour plus d'informations sur les alertes de la licence de démo, consultez le *Guide d'administration de Forescout*.

Si vous travaillez avec un système virtuel Forescout :

- Pour l'instant, la licence de démo n'est pas automatiquement installée. Vous devez installer la licence de démo envoyée par e-mail par votre représentant Forescout.
- Au moins un périphérique CounterACT doit pouvoir accéder à Internet. Cette connexion est utilisée pour valider les licences Forescout par rapport au serveur de licences Forescout. Les licences ne pouvant pas être authentifiées pendant un mois seront révoquées. La plateforme Forescout envoie un e-mail d'avertissement une fois par jour indiquant qu'il existe une erreur de communication avec le serveur.  
Pour plus d'informations, consultez le *Guide d'installation de Forescout*  
Pour plus d'informations sur Per-Appliance Licensing Mode (Mode de licence selon l'appliance), consultez le *Guide d'administration de Forescout*.
- Si votre déploiement Forescout fonctionne avec **Flexx Licensing Mode** (Mode de licence Flexx), l'*administrateur des droits* doit recevoir un e-mail lorsque le droit de licence est créé et disponible sur le portail client Forescout. Une fois disponible, l'*administrateur du déploiement* peut activer la licence sur la console. Les contraintes de licence s'appliquent et certaines modifications de configuration de la console peuvent être restreintes jusqu'à l'activation de la licence. *Aucune licence de démo n'est automatiquement installée lors de l'installation du système.*  
Pour plus d'informations, consultez le *Guide pratique des licences Forescout Flexx*.

## 5. Gestion à distance

### Configuration d'iDRAC

iDRAC (Integrated Dell Remote Access Controller) est une solution de système de serveur intégrée qui vous donne un accès à distance, quels que soient l'emplacement et le système d'exploitation via le réseau local ou Internet à des appliances CounterACT. Utilisez le module pour gérer l'accès KVM, mettre sous tension/hors tension/réinitialiser, et réaliser des tâches de dépannage et de maintenance.

Procédez comme suit pour utiliser le module iDRAC :

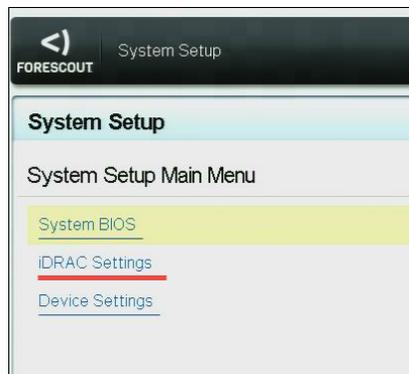
- [Activer et configurer le module iDRAC](#)
- [Connecter le module au réseau](#)
- [Se connecter à iDRAC](#)

### Activer et configurer le module iDRAC

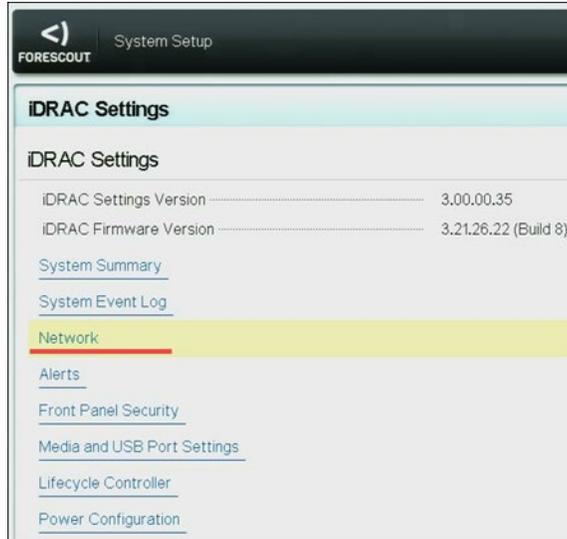
Modifiez les paramètres iDRAC pour activer l'accès à distance sur le périphérique CounterACT. Cette section décrit les paramètres d'intégration de base requis pour utiliser la plateforme ForeScout.

#### Pour configurer iDRAC :

1. Mettez l'appliance gérée sous tension.
2. Sélectionnez F2 lors du processus de démarrage.
3. Sur la page System Setup Main Menu (Menu principal de configuration du système), sélectionnez **iDRAC Settings** (Paramètres iDRAC).



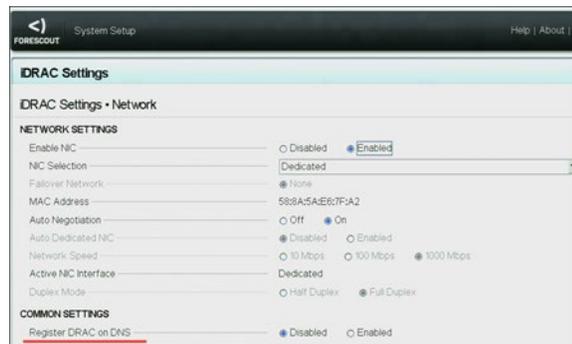
4. Sur la page iDRAC Settings (Paramètres iDRAC), sélectionnez **Network** (Réseau).



5. En suivant **iDRAC Settings** (Paramètres iDRAC) > **Network** (Réseau) > **Network settings** (Paramètres réseau), vérifiez que le champ *Enable NIC* (Activer la carte réseau) est réglé sur **Enabled** (Activé).



6. (facultatif) Suivez **iDRAC Settings** (Paramètres iDRAC) > **Network** (Réseau) > **Common Settings** (Paramètres communs) pour mettre à jour un DNS dynamique :
- Réglez *Register iDRAC on DNS* (Enregistrer iDRAC sur DNS) sur **Enabled** (Activé).
  - Dans le champ *DNS iDRAC Name* (Nom iDRAC DNS), saisissez le DNS dynamique.



7. En suivant **iDRAC Settings** (Paramètres iDRAC) > **Network** (Réseau) > **IPv4 Settings** (Paramètres IPV4) :



- Vérifiez que le champ **Enable IPv4** (Activer IPv4) est réglé sur **Enabled** (Activé).
- Réglez le champ *Enable DHCP* (Activer DHCP) sur **Enabled** (Activé) pour utiliser l'adressage IP dynamique. Le DHCP affectera automatiquement l'adresse IP, la passerelle et le masque de sous-réseau à iDRAC.  
OU  
Réglez le champ *Enable DHCP* (Activer DHCP) sur **Disabled** (Désactivé) pour utiliser l'adressage IP statique et entrez des valeurs dans les champs **Static IP Address** (Adresse IP statique), **Static Gateway** (Passerelle statique) et **Static Subnet Mask** (Masque de sous-réseau statique).

8. Sélectionnez **Back** (Retour).

9. Suivez **iDRAC Settings** (Paramètres iDRAC) > **User Configuration** (Configuration utilisateur) :



Configurez les champs de configuration utilisateur suivants pour l'utilisateur racine :

- Vérifiez que le champ *Enable User* (Activer l'utilisateur) est réglé sur **Enabled** (Activé).
- 📄 *Le nom d'utilisateur (racine) configuré ici est différent du nom d'utilisateur Fore Scout.*
- Pour *LAN User Privileges* (Privilèges d'utilisateur du réseau local), sélectionnez **Administrator** (Administrateur).
- Pour *Serial Port User Privileges* (Privilèges d'utilisateur du port série), sélectionnez **Administrator** (Administrateur).
- Pour *Change Password* (Modifier le mot de passe), définissez un mot de passe pour la connexion utilisateur.

10. Sélectionnez **Back** (Retour), puis **Finish** (Terminer). Confirmez les paramètres modifiés.

Les paramètres configurés sont enregistrés et le système redémarre.

## Connecter le module au réseau

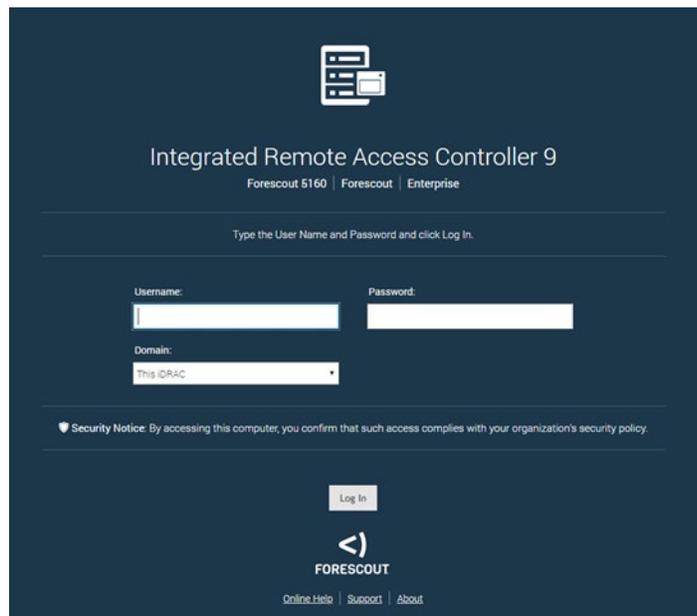
Le module iDRAC se connecte à un réseau Ethernet. Il est habituel de le connecter à un réseau de gestion. L'image suivante montre l'emplacement du port iDRAC sur le panneau arrière de l'appliance CT-1000 :



## Se connecter à iDRAC

**Pour se connecter à iDRAC :**

1. Accédez à l'adresse IP ou au nom de domaine configuré dans **iDRAC Settings** (Paramètres iDRAC) > **Network** (Réseau).

A screenshot of the iDRAC login page. The page has a dark blue background. At the top, there is a server icon and the text 'Integrated Remote Access Controller 9' followed by 'Forescout 5160 | Forescout | Enterprise'. Below this, it says 'Type the User Name and Password and click Log In.' There are three input fields: 'Username:', 'Password:', and 'Domain:' (with a dropdown menu showing 'This iDRAC'). A 'Log In' button is centered below the fields. At the bottom, there is a 'Security Notice' and the Forescout logo with links for 'Online Help', 'Support', and 'About'.

2. Entrez le nom d'utilisateur et le mot de passe configurés sur la page User Configuration (Configuration utilisateur) de la configuration du système iDRAC.
3. Sélectionnez **Submit** (Envoyer).

Pour plus d'informations sur iDRAC, consultez le *Guide d'utilisateur iDRAC*. Vous pouvez accéder à ce guide à l'emplacement suivant :

<https://forescout.com/company/resources/idrac-9-user-guide/>

**Pour identifier votre mode de licence :**

- Depuis la console, sélectionnez **Help (Aide) > About Forescout (À propos de Forescout)**.

 *Il est capital que vous mettiez à jour le mot de passe racine par défaut, si vous ne l'avez pas encore fait.*

## 6. Vérifier la connectivité

### Vérifier la connexion de l'interface de gestion

Pour tester la connexion de l'interface de gestion, connectez-vous à l'appliance et exécutez la commande suivante :

```
fstool linktest
```

Les informations suivantes s'affichent :

```
Management Interface status (État de l'interface de gestion)
Pinging default gateway information (Test ping des informations
de passerelle par défaut)
Ping statistics (Statistiques ping)
Performing Name Resolution Test (Exécution d'un test de
résolution de nom)
Test summary (Résumé du test)
```

### Exécuter un test ping

Exécutez la commande suivante entre l'appliance et un poste de travail réseau pour vérifier la connectivité :

```
Ping <adresse_IP_de_l_ordinateur_réseau>
```

## 7. Configurer la console Forescout

### Installer la console

La console est une application de gestion Forescout qui sert à afficher d'importantes informations détaillées sur les points de terminaison et à les contrôler. Ces informations sont collectées par les périphériques CounterACT. Pour plus d'informations, consultez le *Guide d'administration de Forescout*.

Vous devez fournir une machine pour héberger le logiciel d'application de la console Forescout. Voici la configuration matérielle minimale requise :

- Machine non dédiée, exécutant :
  - Windows 7/8/8.1/10
  - Windows Server 2008/2008 R2/2012/2012 R2/2016/2019
  - Linux RHEL/CentOS 7
- 2 Go de mémoire RAM
- 1 Go d'espace disque

Vous pouvez utiliser la méthode suivante pour installer la console :

#### Utilisez le logiciel d'installation intégré à votre appliance.

1. Ouvrez une fenêtre de navigateur sur l'ordinateur de la console.
2. Saisissez ce qui suit dans la ligne d'adresse du navigateur :

```
http://<ip_appliance>/install
```

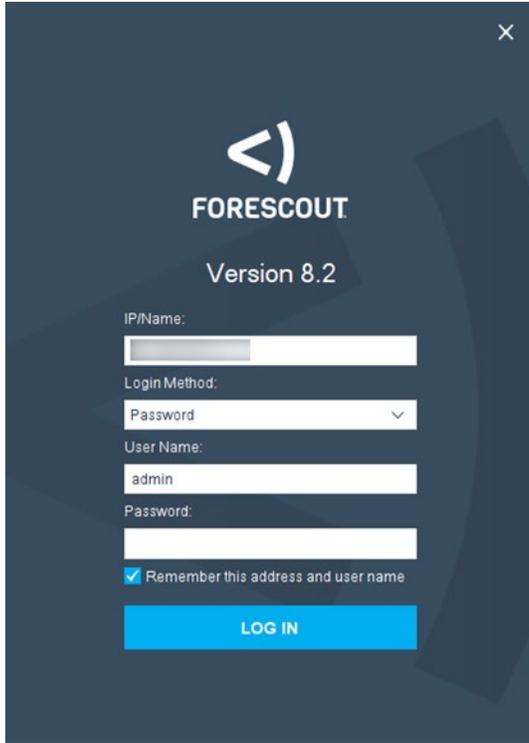
Où ip\_appliance est l'adresse IP de cette appliance. Le navigateur affiche la fenêtre d'installation de la console.

3. Suivez les instructions à l'écran.

### Se connecter

Une fois l'installation terminée, vous pouvez vous connecter à la console.

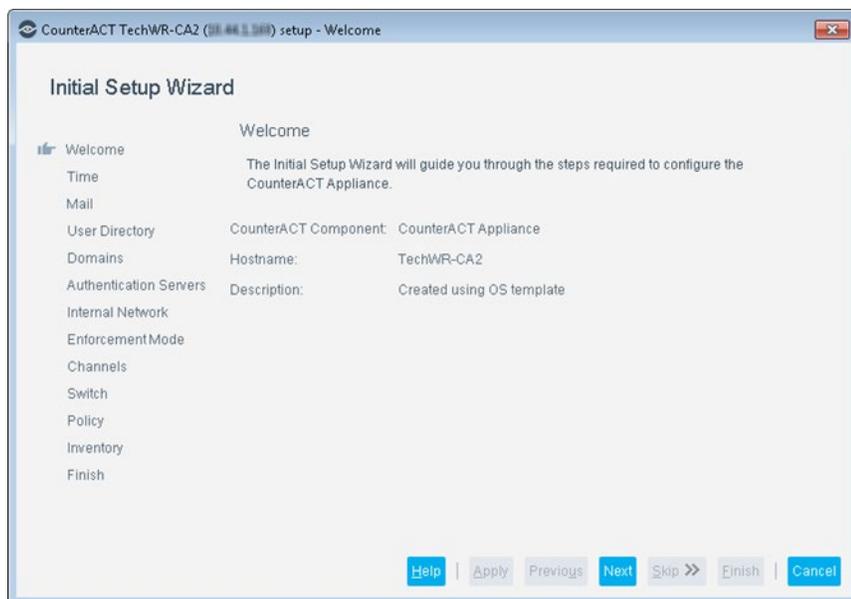
1. Sélectionnez l'icône Forescout depuis l'emplacement de raccourci que vous avez créé.



2. Entrez l'adresse IP ou le nom d'hôte de l'appliance dans le champ **IP/Name** (IP/Nom).
3. Dans le champ **User Name** (Nom d'utilisateur), entrez admin.
4. Dans le champ **Password** (Mot de passe), entrez le mot de passe créé lors de l'installation de l'appliance.
5. Sélectionnez **Login** (Se connecter) pour lancer la console.

## Exécuter la configuration initiale

Lorsque vous vous connectez pour la première fois, l'assistant Initial Setup (Configuration initiale) apparaît. Ce dernier vous guide à travers les étapes de configuration essentielles pour s'assurer que la plateforme Forescout fonctionne rapidement et efficacement.



## Avant de procéder à la configuration initiale

Préparez les informations suivantes avant d'utiliser l'assistant :

Informations requises par l'assistant	Valeur
Adresse de serveur NTP utilisée par votre entreprise (facultatif)	
Adresse IP de relais de messagerie interne. Cela permet d'envoyer des alertes par e-mail si le trafic SMTP n'est pas autorisé depuis l'appliance (facultatif)	
Adresse e-mail de l'administrateur Forescout	
Interfaces de surveillance et de réponse	
Pour les segments ou les VLAN sans DHCP, le segment réseau ou les VLAN auxquels l'interface de réponse est directement connectée et une adresse IP permanente que la plateforme Forescout doit utiliser sur chaque VLAN	
Plage d'adresses IP que cette appliance surveillera (toutes les adresses internes, y compris les adresses inutilisées)	
Informations sur le compte utilisateur LDAP et adresse IP du serveur LDAP	
Informations d'identification de domaine, y compris le nom et le mot de passe du compte administratif de domaine	
Serveurs d'authentification pour que la plateforme Forescout puisse analyser les hôtes réseau qui ont été correctement authentifiés	

Adresse IP, fournisseur et paramètres SNMP du commutateur	
---	--

Pour plus d'informations sur l'utilisation de l'assistant, consultez le *Guide d'administration de Forescout*.

## Documentation supplémentaire de Forescout

Pour plus d'informations sur les fonctionnalités et les modules Forescout, consultez les ressources suivantes :

- [Modules de téléchargement de documents](#)
- [Portail de documentation](#)
- [Outils Help \(Aide\) de Forescout](#)

### Modules de téléchargement de documents

Vous pouvez accéder aux modules de téléchargement de documents depuis la [Page de documentation technique de Forescout](#), ou l'un des deux portails Forescout, en fonction du mode de licence utilisé par votre déploiement.

- **Mode de licence selon l'appliance** – [Portail des mises à jour des produits](#)
- **Mode de licence Flexx** – [Portail client](#)

📖 Vous pouvez également accéder aux modules de téléchargement de logiciels depuis ces portails.

#### Pour identifier votre mode de licence :

- Depuis la console, sélectionnez **Help (Aide) > About Forescout (À propos de Forescout)**.

### Page de documentation technique de Forescout

La page de documentation technique de Forescout fournit un accès à un [Portail de documentation](#) consultable basé sur le Web, ainsi que des liens PDF vers l'ensemble de la documentation technique.

#### Pour accéder à la page de documentation technique de Forescout :

- Rendez-vous à l'adresse <https://www.Forescout.com/company/technical-documentation/>

### Portail des mises à jour des produits

Le portail des mises à jour des produits fournit des liens vers les versions de Forescout, les modules de contenu et de base, les produits eyeExtend, ainsi que les documents connexes. Le portail comprend également de nombreux autres documents.

**Pour accéder au portail des mises à jour des produits :**

- Rendez-vous à l'adresse <https://updates.forescout.com/support/index.php?url=counteract>, puis sélectionnez la version que vous souhaitez découvrir.

**Portail client**

La page Téléchargements du portail client de Forescout fournit des liens vers les versions de Forescout, les modules de contenu et de base, les produits eyeExtend, ainsi que les documents connexes. Le logiciel et les documents connexes n'apparaissent sur la page Téléchargements que si vous disposez des droits de licence du logiciel.

**Pour accéder à la documentation sur le portail client de Forescout :**

- Rendez-vous à l'adresse <https://Forescout.force.com/support/>, puis sélectionnez **Téléchargements**.

**Portail de documentation**

Le portail de documentation de Forescout est une bibliothèque consultable en ligne qui permet d'obtenir des informations sur les outils, les caractéristiques, les fonctionnalités et les intégrations de Forescout.

- 📖 *Si votre déploiement utilise Flexx Licensing Mode (Mode de licence Flexx), vous ne disposez probablement pas des informations d'identification nécessaires pour accéder à ce portail.*

**Pour accéder au portail de documentation :**

- Rendez-vous à l'adresse [https://updates.forescout.com/support/files/counteract/docs\\_portal/](https://updates.forescout.com/support/files/counteract/docs_portal/), puis utilisez vos informations d'identification du service client pour vous ouvrir une session.

**Outils Help (Aide) de Forescout**

Accédez aux informations directement depuis la console.

**Boutons Help (Aide) de la console**

Utilisez les boutons *Help* (Aide contextuelle) pour accéder rapidement aux informations concernant les tâches et les rubriques avec lesquelles vous travaillez.

**Guide d'administration de Forescout**

- Sélectionnez **Administration Guide** (Guide d'administration) dans le menu **Help** (Aide).

**Fichiers d'aide du plug-in**

- Après l'installation du plug-in, sélectionnez **Tools** (Outils) > **Options** (Options) > **Modules** (Modules), choisissez le plug-in puis cliquez sur **Help** (Aide).

**Portail de documentation**

- Sélectionnez **Documentation Portal** (Portail de documentation) dans le menu **Help** (Aide) pour accéder au [Portail de documentation](#).