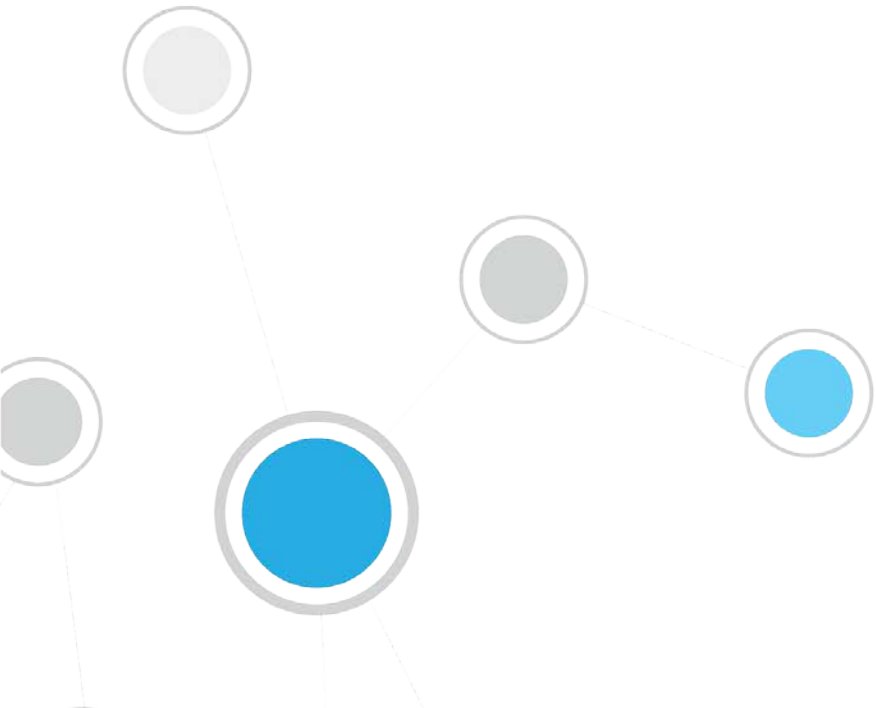
ForeScout CounterACT®

シングル CounterACT アプライアンス

クイックインストールガイド

バージョン 8.0



目次

CounterACT バージョン 8.0 へようこそ 4
CounterACT パッケージの内容 4

概要 5

1. 展開計画の作成 6
アプライアンスの展開先の決定 6
アプライアンスのインターフェイス接続 6
管理インターフェイス 6
モニターインターフェイス 9
レスポンスインターフェイス 9

2. スイッチの設定 10
A. スイッチ接続の選択 10
1 標準展開（個別の管理、モニター、レスポンスインターフェイス） 10
2 パッシブインラインタップ 10
3 アクティブ（インジェクション対応）インラインタップ 10
4 IP レイヤーレスポンス（レイヤ-3 スイッチのインストール用） 10
B. スイッチ設定時の注意事項 11
VLAN（802.1Q）タグ 11
追加ガイドライン 11

3. ネットワークケーブルの接続と電源投入 12
A. アプライアンスを開梱してケーブルを接続する 12
B. インターフェイスの割り当てを記録する 12
C. アプライアンスの電源を入れる 13

4. アプライアンスの設定 14

5. リモート管理 18
iDRAC の設定 18
iDRAC モジュールを有効化し設定する 18
モジュールをネットワークに接続する 21
iDRAC へのログイン 21

6. 接続の検証 23
管理インターフェイスの接続の検証 23
Ping テストの実行 23

7. CounterACT コンソールの設定 24
CounterACT コンソールのインストール 24
ログイン 24

初期設定の実行 25
初期設定開始の前に 26

追加の CounterACT ドキュメント 27
ドキュメントのダウンロード 27
ドキュメントポータル 28
CounterACT ヘルプツール 28

CounterACT バージョン 8.0 へようこそ

CounterACT プラットフォームを使用すると、インフラストラクチャとデバイスを可視化し、ポリシーを管理し、オーケストレーションとワークフローを合理化して、ネットワークセキュリティを向上させることができます。CounterACT は、企業にネットワーク上のデバイスとユーザーのコンテキスト情報をリアルタイムで提供します。ポリシーは、コンプライアンス、修復、適切なネットワークアクセス、サービス操作の合理化を確実にするのに役立つこのコンテキスト情報を使用して CounterACT で定義されます。

このガイドでは、シングルスタンドアロン CounterACT アプライアンスのインストール方法を説明します。

詳細または企業内ネットワーク保護のための複数アプライアンスの導入については *『CounterACT Installation Guide（CounterACT インストールガイド）』* および *『CounterACT Administration Guide（CounterACT 管理ガイド）』* をご参照ください。これらのガイドへのアクセス方法については、追加の CounterACT ドキュメントをご参照ください。

さらに、アプライアンスの最新資料、ナレッジベース記事、アップデートについては、http://www.forescout.com/support のサポートウェブサイトもご参照いただけます。

CounterACT パッケージの内容

CounterACT パッケージには、以下のコンポーネントが含まれています。

- CounterACT アプライアンス
- フロントベゼル
- レールキット（取付ブラケット）
- 電源コード
- DB9 コンソール接続ケーブル（シリアル接続専用）
- 企業向け製品安全、環境、規制情報
- スタートガイド（51xx デバイス専用）

概要

CounterACT を設定するには、以下を行います。

1. 展開計画の作成
2. スイッチの設定
3. ネットワークケーブルの接続と電源投入
4. アプライアンスの設定
5. リモート管理
6. 接続の検証
7. CounterACT コンソールの設定

1. 展開計画の作成

インストールを実行する前に、アプライアンスの展開先を決定し、アプライアンスのインターフェイス接続について学びます。

アプライアンスの展開先の決定

アプライアンスのインストール先として適切なネットワーク上の場所を選択することは、CounterACT を正常に展開し、パフォーマンスを最適化するために非常に重要です。適切なインストール先は、お客様が望む実装目標とネットワークアクセスポリシーによって異なります。アプライアンスが、お客様にとって望ましいポリシーの観点から関連性のあるトラフィックをモニターできるようにすべきです。例えば、お客様のポリシーがエンドポイントから企業認証サーバーへの認証イベントのモニタリングに依存している場合、認証サーバーへのエンドポイントトラフィックがモニターできるようにアプライアンスをインストールする必要があります。

インストールと展開の詳細については、*『CounterACT Installation Guide （CounterACT インストールガイド）』*をご参照ください。このガイドへのアクセス方法についての詳細は、追加の CounterACT ドキュメントをご参照ください。

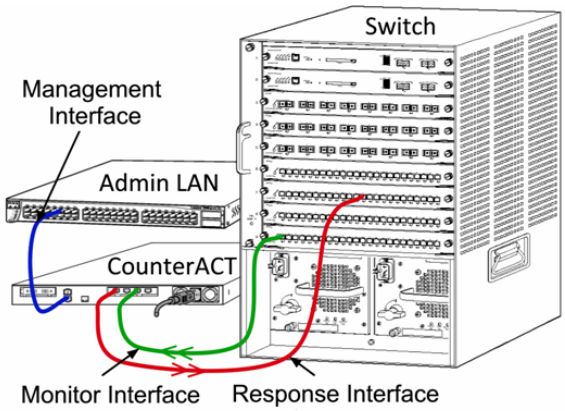
アプライアンスのインターフェイス接続

アプライアンスは、一般的に 3 つのネットワークスイッチへの接続で構成されます。

管理インターフェイス

管理インターフェイスを使用すれば、CounterACT を管理してエンドポイントのクエリと詳細な検査を実行できます。すべてのネットワークエンドポイントにアクセスできるスイッチポートにこのインターフェイスを接続する必要があります。

各アプライアンスに、ネットワークへの共通管理接続が必要です。この接続には、ローカル LAN 上の IP アドレスと、CounterACT コンソール管理アプリケーションを実行するマシンからのポート 13000/TCP アクセスが必要です。管理ポートには追加のネットワークサービスへのアクセスが必要です。



ネットワークアクセス要件

ポート	サービス	ACT 接続先または接続元	機能
22/TCP	SSH	接続元	OS X と Linux エンドポイントのリモート検査を可能にします。 CounterACT がネットワークスイッチとルーターに通信できるようにします。
		接続先	CounterACT コマンドラインインターフェイスにアクセスできるようにします。
2222/TCP	SSH	接続先	（高可用性）高可用性ペアの一部である物理 CounterACT デバイスにアクセスできるようになります。 22/TCP を使用してそのペアの共有（仮想）IP アドレスにアクセスします。
25/TCP	SMTP	接続元	CounterACT がエンタープライズメールリレーにアクセスできるようにします。
53/UDP	DNS	接続元	CounterACT が内部 IP アドレスを解決できるようにします。
80/TCP	HTTP	接続先	HTTP のリダイレクトを可能にします。
123/UDP	NTP	接続元	CounterACT がローカルタイムサーバーまたは ntp.forescout.net にアクセスできるようにします。 デフォルトでは、CounterACT は ntp.foreScout.net にアクセスします。
135/TCP	MS-WMI	接続元	Windows エンドポイントのリモート検査を可能にします。
139/TCP	SMB、MS-RPC	接続元	Windows エンドポイントのリモート検査を可能にします（Windows 7 以前のバージョンを実行するエンドポイント用）。
445/TCP			Windows エンドポイントのリモート検査を可能にします。
161/UDP	SNMP	接続元	CounterACT がネットワークスイッチとルーターに通信できるようにします。 SNMP の構成の詳細については、*『CounterACT Administration Guide（CounterACT 管理ガイド）』*をご参照ください。
162/UDP	SNMP	接続先	CounterACT がネットワークスイッチとルーターから SNMP トラップを受信できるようにします。 SNMP の構成の詳細については、*『CounterACT Administration Guide（CounterACT 管理ガイド）』*をご参照ください。

ポート	サービス	ACT 接続先または接続元	機能
389/TCP (636)	LDAP	接続元	CounterACT が Active Directory と通信できるようにします。 CounterACT ウェブベースポータルと通信できるようにします。
443/TCP	HTTPS	接続先	TLS を使用して HTTP リダイレクトができるようにします。
2200/TCP	Linux 用 SecureConnector	接続先	SecureConnector が Linux マシンからアプライアンスへのセキュアな（暗号化された SSH）接続を確立できるようにします。*SecureConnector* はネットワークに接続して Linux エンドポイントの管理を可能にするスクリプトベースのエージェントです。
10003/TCP	Windows 用 SecureConnector	接続先	SecureConnector が Windows マシンからアプライアンスへのセキュアな（暗号化された TLS）接続を確立できるようにします。*SecureConnector* はネットワークに接続して Windows エンドポイントの管理を可能にするエージェントです。SecureConnector の詳細については、*『CounterACT Administration Guide（CounterACT 管理ガイド）』*をご参照ください。 SecureConnector がアプライアンスまたはエンタープライズマネージャに接続すると、ホストが割り当てられているアプライアンスにリダイレクトされます。このポートをすべてのアプライアンスとエンタープライズマネージャに対して必ずオープンにし、組織内で透明なモビリティが実現するようにします。
10005/TCP	OS X 用 SecureConnector	接続先	SecureConnector が OS X マシンからアプライアンスへのセキュアな（暗号化された TLS）接続を確立できるようにします。*SecureConnector* はネットワークに接続して OS X エンドポイントの管理を可能にするエージェントです。SecureConnector の詳細については、*『CounterACT Administration Guide（CounterACT 管理ガイド）』*をご参照ください。 SecureConnector がアプライアンスまたはエンタープライズマネージャに接続すると、ホストが割り当てられているアプライアンスにリダイレクトされます。このポートをすべてのアプライアンスとエンタープライズマネージャに対して必ずオープンにし、組織内で透明なモビリティが実現するようにします。

ポート	サービス	ACT 接続先または接続元	機能
13000/TCP	CounterACT	接続元／接続先	単独のアプライアンスのみが存在する環境用 - コンソールからアプライアンス。 複数の CounterACT デバイスが存在する環境用 - コンソールから CounterACT デバイス、CounterACT デバイスから別の CounterACT デバイス。CounterACT デバイスの通信には、TLS を使用するエンタープライズマネージャとリカバリエンタープライズマネージャが含まれています。

モニターインターフェイス

モニターインターフェイスを使用すれば、アプライアンスでネットワークトラフィックをモニターしてトラックできるようになります。どのインターフェイスでもモニターインターフェイスとして使用できます。

トラフィックはスイッチ上のポートにミラーリングされ、アプライアンスによってモニターされます。802.1Q VLAN タグ付けの使用はミラーリングされている VLAN の数によって異なります。

- ***単独の VLAN***: モニター対象のトラフィックが単独の VLAN からのものである場合、ミラーリングされたトラフィックに VLAN タグ付けを行う必要はありません。
- ***複数の VLAN***: モニター対象のトラフィックが複数の VLAN からのものである場合、ミラーリングされたトラフィックには 802.1Q VLAN タグ付けを行う必要があります。

2 つのスイッチが冗長ペアとして接続される場合、アプライアンスは両方のスイッチからのトラフィックをモニターする必要があります。

モニターインターフェイスには IP アドレスは必要ありません。

レスポンスインターフェイス

アプライアンスは、レスポンスインターフェイスを使用しているトラフィックに反応します。レスポンスとトラフィックは、悪意のあるアクティビティから保護し、ポリシーアクションを実行するにために使用されます。これらのアクションには、例えば、ウェブブラウザのリダイレクトやセッションブロックが含まれる場合があります。関連するスイッチポートの構成は、モニター対象のトラフィックにより異なります。

どのインターフェイスでもレスポンスインターフェイスとして使用できます。

- ***単独の VLAN***: モニター対象のトラフィックが単独の VLAN からのものである場合、レスポンスポートは同じ VLAN に属する必要があります。この場合、アプライアンスは、その VLAN 上に IP アドレスを 1 つ持つ必要があります。
- ***複数の VLAN***: モニター対象のトラフィックが複数の VLAN からのものである場合、レスポンスポートも同じ VLAN 用の 802.1Q VLAN タグ付けで設定する必要があります。アプライアンスは、モニター対象の各 VLAN で IP アドレスを持つ必要があります。

2. スイッチの設定

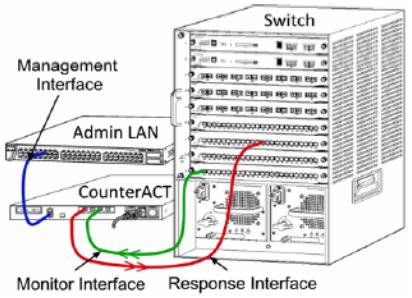
A. スイッチ接続の選択

このアプライアンスは様々なネットワーク環境とシームレスに統合するように設計されています。このアプライアンスをお客様のネットワークに統合させるために、必要なトラフィックをモニターするようにスイッチが設定されていることをご確認ください。

アプライアンスのスイッチへの接続については、複数の選択肢があります。

1 標準展開（個別の管理、モニター、レスポンスインターフェイス）

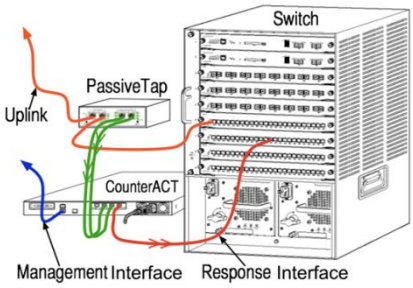
展開には 3 つの個別のポートを使用することが推奨されます。これらのポートの説明は、アプライアンスのインターフェイス接続でご確認ください。



2 パッシブインラインタップ

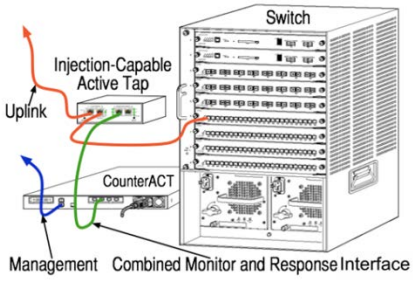
アプライアンスでは、スイッチモニターポートに接続する代わりに、パッシブインラインタップを使用できます。

パッシブインラインタップには、2 つのモニターポート（上流トラフィック用に 1 つと下流トラフィック用に 1 つ）が必要ですが、*リコンビネーション*タップは例外で、このタップは 2 つの二重ストリームを 1 つのポートに結合します。タップしたポートで 802.1Q VLAN タグ付けがされている場合は、レスポンスポートでも 802.1Q VLAN タグ付けをする必要があることにご注意ください。



3 アクティブ（インジェクション対応）インラインタップ

アプライアンスではアクティブインラインタップを使用できます。タップがインジェクション対応であれば、スイッチ上の別のレスポンスポートを設定する必要がないようにアプライアンスはモニターポートとレスポンスポートを結合します。この選択肢は、スイッチのタイプが上流、下流のいずれであっても選択できます。



4 IP レイヤーレスポンス（レイヤ-3 スイッチのインストール用）

アプライアンスでは、トラフィックに対応するためにアプライアンス自体の管理インターフェイスを使用できます。この選択肢はモニター対象のトラックで選択できますが、アプライアンスが VLAN の一部ではないポートをモニターして、他のスイッチポートを使用しているモニター対象のトラフィックに対応できない場合のみ、選択することをお勧めします。典型的には、2 つのル

ーターを接続しているリンクをモニターしている場合です。この選択肢では Address Resolution プロトコル（ARP）リクエストに対応できません。アプライアンスがモニター対象のサブネットに含まれる IP アドレスを対象としたスキャンを検出する機能が制限されます。2 つのルーター間のトラフィックがモニターされている時は、この制限は適用されません。

B. スイッチ設定時の注意事項

VLAN（802.1Q）タグ

- ***単独の VLAN のモニタリング***：モニター対象のトラフィックが単独の VLAN からのものである場合、トラフィックには 802.1Q VLAN タグ付けは必要ありません。
- ***複数の VLAN のモニタリング***：モニター対象のトラフィックが複数の VLAN からのものである場合、モニター対象のポートとレスポンスポートの*両方*で 802.1Q VLAN タグ付けを有効にする必要があります。モニタリングポートの数を最小限にしながら全体的に最善な結果が得られる、複数の VLAN のモニタリングをお勧めします。
- ミラーリングポートで 802.1Q VLAN タグをスイッチが使用できない場合は、以下のうちのいずれかを行ってください。
  - 単独の VLAN のみをミラーリングする
  - 単独のタグ付けされていないアップリンクポートをミラーリングする
  - IP レイヤーレスポンスを選択する
- スイッチで 1 つのポートしかミラーリングできない場合は、単独のアップリンクポートをミラーリングします。これはタグ付けすることもできます。一般に、スイッチが 802.1Q VLAN タグをストリップする場合は、IP レイヤーレスポンスを選択する必要があります。

追加ガイドライン

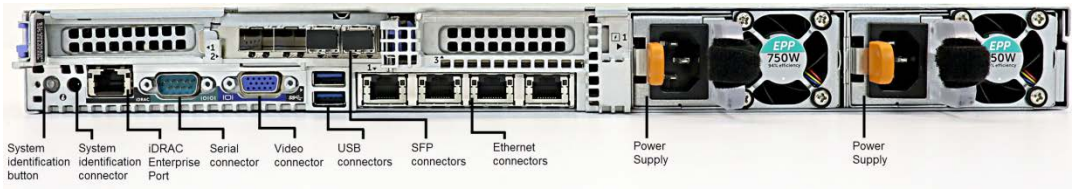
- 以下の場合、1 つのインターフェイス（送信／受信を可能にする）のみをミラーリングするようにします。
  - スイッチが送信トラフィックと受信トラフィックの両方をミラーリングできない場合
  - スイッチがすべてのスイッチトラフィックをミラーリングできない場合
  - スイッチがすべてのトラフィックを VLAN を通じてミラーリングできない場合
- ミラーリングポートに負荷がかかりすぎていないか確認してください。
- スイッチによっては（例：Cisco 6509）、新しい設定を入力する前に現在のポート設定を完全に削除する必要がある場合があります。古いポート情報を削除しないと、多くの場合、スイッチが 802.1Q タグをストリップする原因となることがあります。

3. ネットワークケーブルの接続と電源投入

A. アプライアンスを開梱してケーブルを接続する

1. アプライアンスと電源ケーブルを梱包箱から取り出します。
2. アプライアンスに付属のレールキットを取り出します。
3. アプライアンス上でレールキットを組み立て、アプライアンスをラックに取り付けます。
4. アプライアンスの後部パネルとスイッチポート上のネットワークインターフェイスの間にネットワークケーブルを接続します。

後部パネルのサンプル - CounterACT デバイス



ForeScout が提供した SFP は、ForeScout がテスト、承認した Finisar SFP と交換できます。詳細については、*『CounterACT Installation Guide（CounterACT インストールガイド）』*をご参照ください。

B. インターフェイスの割り当てを記録する

データセンターでアプライアンスと CounterACT コンソールの設置を完了すると、インターフェイスの割り当てを登録するように促されます。これらの割り当ては、*チャネルの定義*と呼ばれるように、コンソールに最初のログオンした時点で開く初期設定ウィザードに入力されます。

以下の物理インターフェイスの割り当てを記録して、コンソールでのチャネル設定完了時に使用します。

Eth インターフェイス	インターフェイス割り当て（例：管理、モニター、レスポンス）
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	

Eth6	
Eth7	

C. アプライアンスの電源を入れる

1. 電源ケーブルをアプライアンスの前面パネル上の電源コネクタに接続します。
2. 電源ケーブルのもう一方の端を接地された AC コンセントに接続します。
3. キーボードとモニターをアプライアンスに接続するか、シリアル接続用にアプライアンスを設定します。詳細については、*『CounterACT Installation Guide（CounterACT インストールガイド）』*をご参照ください。
4. 前部パネルでアプライアンスの電源を入れます。

4. アプライアンスの設定

アプライアンスを設定する前に、以下の情報を確認しておきます。

アプライアンスのホスト名	
CounterACT の管理パスワード	パスワードは安全な場所に保管してください
管理インターフェイス	
アプライアンスの IP アドレス	
ネットワークマスク	
デフォルトのゲートウェイ IP アドレス	
DNS のドメイン名	
DNS のサーバーアドレス	

電源を入れると、以下のメッセージが表示され、設定を開始するように促されます。

```
CounterACT Appliance boot is complete.
Press <Enter> to continue.
```

1. **Enter** キーを押します。51xx CounterACT デバイスで、以下のメニューが表示されます。

```
CounterACT 8.0.0-<build> options:


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

Choice (1-6) :1
```

CT-xxxx CounterACT デバイスの場合、バージョン情報として、CounterACT 7.0.0 または CounterACT 8.0.0 がメニュー上部に表示されます。

- CounterACT 7.0.0 と表示される場合は、バージョン 8.0.0 にアップグレードするか、バージョン 8.0.0 を新規にインストールするかのどちらかが可能です。詳細については、*『CounterACT Installation Guide（CounterACT インストールガイド）』*をご参照ください。バージョン 8.0.0 へのアップグレード後またはバージョン 8.0.0 をインストール後に、上記のメニューが表示されます。

– CounterACT 8.0.0 と表示される場合、以下に示すように、メニューには CounterACT 7.0.0 をインストールするか CounterACT 8.0.0 を設定するかの選択肢が表示されます。[CounterACT 7.0.0]を選択すると、[Configuration（設定）]メニューから CounterACT 8.0.0 を再インストールできなくなります。CounterACT 7.0.0 の設定の詳細については、*『CounterACT Installation Guide version 7.0.0（CounterACT インストールガイドバージョン 7.0.0）』*をご参照ください。

```
CounterACT 8.0.0-<build> options:


1) Install CounterACT 7.0.0-<build>
2) Configure CounterACT 8.0.0-<build>
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) :
```

設定が中断されたり、誤った CounterACT バージョンを選択した場合は、ISO ファイルの該当するバージョンを使用したアプライアンスの再イメージ化が必要になります。アプライアンスの再イメージ化の詳細については、『CounterACT Installation Guide（CounterACT インストールガイド）』をご参照ください。

2. **[Configure CounterACT（CounterACT の設定）]**を選択します。プロンプトには以下のメッセージが表示されます。

   [Continue（続行しますか）]: （yes（はい）/no（いいえ））?

   Enter キーを押して設定を開始します。

3. [High Availability Mode（高可用性モード）]のプロンプトが開きます **Enter** キーを押して[Standard Installation（標準インストール）]を選択します。

4. [CounterACT Initial Setup（CounterACT 初期設定）]プロンプトが表示されます。**Enter** キーを押して続行します。

5. [Select CounterACT Installation Type（CounterACT のインストールタイプ選択）]プロンプトが開きます。**1** と入力して **Enter** キーを押し、標準 CounterACT アプライアンスをインストールします。

   設定が開始されます。これにはしばらく時間がかかる場合があります。

6. [Select Licensing Mode（ライセンス許諾モード選択）]プロンプトが開きます。展開しているアプライアンスで使用するライセンス許諾モードを選択します。ライセンス許諾モードは購入時に決定します。***展開しているアプライアンスでどのライセンス許諾モードを使用するかを確認するまで、値を入力しないでください***。ライセンス許諾モードを確認したい場合や誤ったモードを入力した場合は、御社担当の ForeScout レプレゼンタティブまでご連絡ください。

7. [Enter Machine Description（マシンの説明入力）]プロンプトが表示されたら、このデバイスを識別するための短いテキストを入力し、**Enter** キーを押します。

   以下のメッセージが表示されます。

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

```
This password will be used to log in as 'root' 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 :
```

8. [Set Administrator Password（管理パスワード設定）]プロンプトが表示されたら、パスワード（文字列は画面に表示されません）を入力し、**Enter** キーを押します。パスワードを確認するよう促されます。このパスワードは 6～15 文字で、アルファベット以外の文字が 1 つ以上含まれている必要があります。

   ルートとしてアプライアンスにログインし、 管理者としてコンソールにログインします。

9. [Set Host Name（ホスト名設定）]プロンプトでホスト名を入力し、**Enter** キーを押します。コンソールへのログイン時にホスト名を使用できます。このホスト名はコンソールに表示され、表示中の CounterACT の識別に役立ちます。ホスト名は 13 文字以内で設定してください。

10. [Configure Network Settings（ネットワーク設定構成）]画面が表示され、一連の設定パラメータを入力するよう促されます。各プロンプトに値を入力し、**Enter** キーを押して次のプロンプトを表示します。

    – CounterACT のコンポーネントは管理インターフェイスを介して通信します。表示される管理インターフェイスの数はアプライアンスのモデルにより異なります。

    – **管理 IP アドレス**は、CounterACT コンポーネントが通信に使用するアドレスです。この例では、CounterACT のコンポーネント間の通信に使用されるインターフェイスがタグ付けされたポートに接続する場合のみ、このインターフェイス用に VLAN ID を追加します。

    – 複数の **DNS サーバーアドレス**がある場合は、各アドレスをスペースで区切ってください。ほとんどの内部 DNS サーバーは外部アドレスと内部アドレスを解決しますが、外部解決 DNS サーバーを含める必要がない場合があります。アプライアンスが実行するほぼすべての DNS クエリは内部アドレス用であるため、外部 DNS サーバーは一番最後に表示されます。

11. [Setup Summary（設定概要）]画面が表示されます。全体的な接続テストの実行、再設定、または設定完了のいずれかを促されます。**D** と入力して設定を完了します。

ライセンス

設定後に、CounterACT デバイスに有効なライセンスがあることを確認してください。CounterACT デバイスのデフォルトのライセンス許諾ステータスは、展開にどのライセンス許諾モードを使用しているかによって異なります。

- CounterACT 展開が***個別アプライアンス型ライセンス許諾モード***で稼働している場合、30 日間有効なこのデモライセンスを使用してすぐに作業を開始できます。デモ期間中に ForeScout からの恒久ライセンスを受け取ることになります。恒久ライセンスはディスクまたはネットワーク上のアクセス可能なフォルダ内に保存してください。30 日間のデモライセンスが期限切れとなる前にこの場所からライセンスをインストールしてください（必要に応じて、デモライセンスの期間延長を要求できます）。

  複数の方法でライセンスデモが期限切れ間近であるというアラートが発せられます。デモライセンスアラートの詳細については、*『CounterACT Administration Guide（CounterACT 管理ガイド）』*をご参照ください。

CounterACT バーチャルシステムで作業している場合：

- デモライセンスは、この段階では自動的にインストールされません。御社担当の ForeScout レプレゼンタティブから電子メールで受け取ったデモラインセンスをインストールする必要があります。
- 1 台以上の CounterACT デバイスがインターネットにアクセス可能となっている必要があります。この接続は ForeScout のライセンスサーバーが CounterACT ライセンスを検証するためのものです。1 カ月間認証されないライセンスは取り消されます。CounterACT は 1 日に 1 度、サーバーとの通信エラーが存在することを示す警告メールを送信します。

  詳細については、*『CounterACT Installation Guide（CounterACT インストールガイド）』*をご参照ください。

- 御社の CounterACT が***集中ライセンス許諾モード***で稼働している場合、ライセンスが ForeScout のカスタマーポータルで生成され利用可能となった時点で、*権限管理者*に電子メールが送信されます。利用可能となった時点で、御社の *CounterACT 管理者*は CounterACT コンソール内でライセンスを有効化できます。ライセンスが有効化されるまで、CounterACT の機能は適切に機能しません。例えば、ポリシーは評価されず、アクションも実行されません。*デモライセンスはシステムをインストールする際に自動的にインストールされません。*

ライセンス管理の詳細については、*『CounterACT Administration Guide（CounterACT 管理ガイド）』*をご参照ください。

5. リモート管理

iDRAC の設定

Integrated Dell Remote Access Controller（iDRAC）は、CounterACT アプライアンスへの LAN やネットワークを通じた位置や OS に依存しないリモートアクセスを可能にする統合サーバーシステムソリューションです。モジュールを使用して、KVM アクセス、電源のオン／オフ／リセットを行い、トラブルシューティングとメンテナンスタスクを実行します。

iDRAC モジュールを操作できるようにするには、以下を実行します。

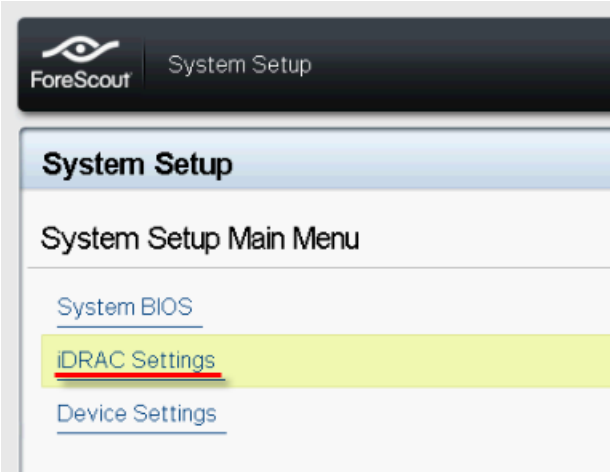
- iDRAC モジュールを有効化し設定する
- モジュールをネットワークに接続する
- iDRAC へのログイン

iDRAC モジュールを有効化し設定する

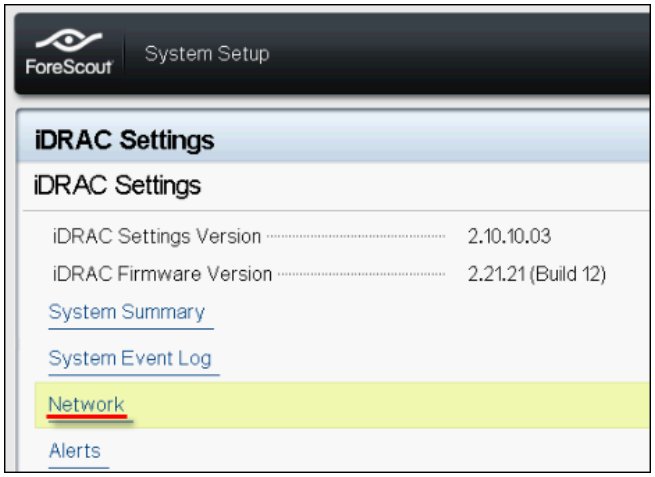
iDRAC の設定を変更して、CounterACT デバイスへのリモートアクセスを有効にします。このセクションでは、CounterACT で作業を行うために必要な基本的な統合設定について説明します。

iDRAC の設定方法：

1. 管理対象のアプライアンスをオンにします。
2. 起動時に F2 キーを選択します。
3. [System Setup Main Menu（システム設定メインメニュー）]ページで、**[iDRAC Settings（iDRAC 設定）]**を選択します。

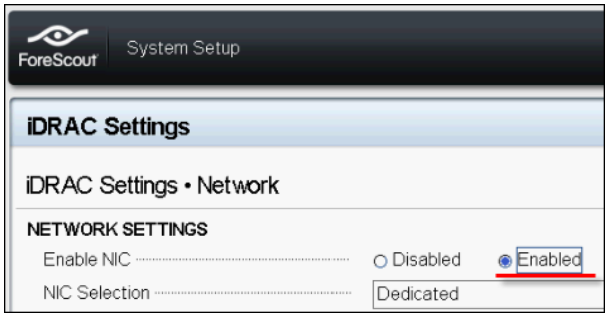


4. [iDRAC Settings（iDRAC の設定）]ページで**[Network（ネットワーク）]**を選択します。



5. 以下のようにネットワークを設定します:

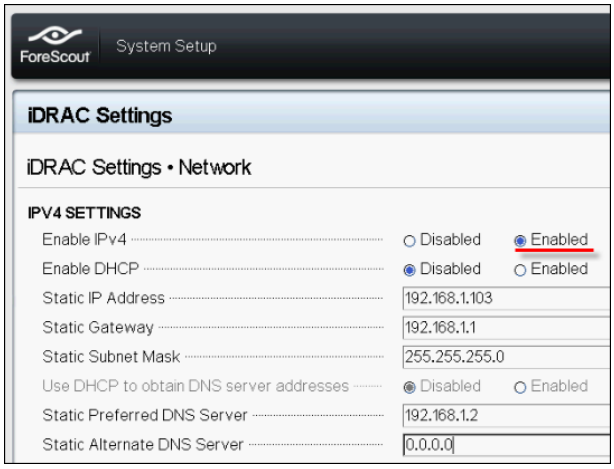
   – ***ネットワークの設定***[Enable NIC（NIC の有効化）]フィールドが[Enabled（有効）]に設定されていることを確認します。



   – ***共通の設定***.[DNS DRAC Name（DNS DRAC 名）]フィールドで、動的 DNS をアップデートできます（オプション）。

   – ***IPV4 の設定***[Enable IPv4（IPv4 の有効化）]フィールドが[Enabled（有効）]に設定されていることを確認します。

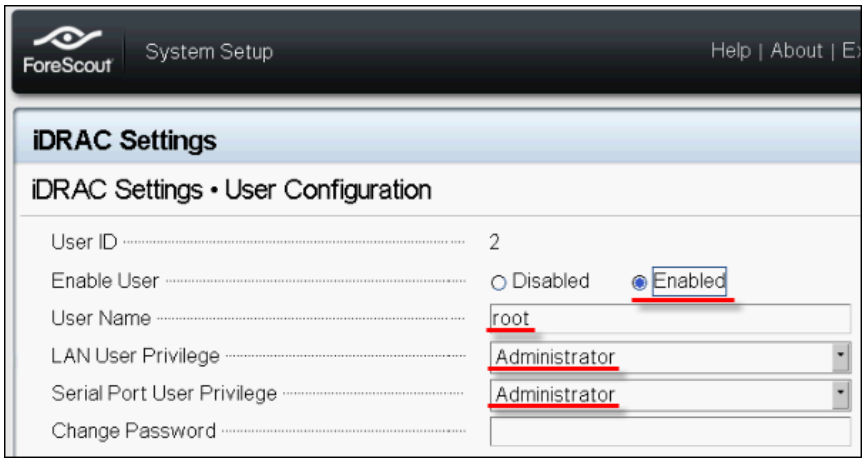
     [Enable DHCP（DHCP の有効化）]フィールドを[Enabled（有効）]に設定して動的 IP アドレス指定を使用するか、[Disabled（無効）]にして静的 IP アドレス指定を使用します。IP アドレス、ゲートウェイ、サブネットマスクが有効になっている場合、DHCP が自動的に iDRAC に割り当てます。無効になっている場合は、[Static IP Address（静的 IP アドレス）]、[Static Gateway（静的ゲートウェイ）]、[Static Subnet Mask（静的サブネットマスク）]フィールドの値を入力します。



6. **[Back（戻る）]**を選択します。
7. **[User Configuration（ユーザー設定）]**を選択します。
8. ルートユーザー向けに以下の[User Configuration（ユーザー設定）]フィールドを設定します。
   - ***ユーザーの有効化***. このフィールドが[Enabled（有効）]に設定されていることを確認します。

     ここで設定されるユーザー名は CounterACT のユーザー名と同じではありません。

   - ***LAN およびシリアルポートユーザーの権限***管理者の権限レベルを設定します。
   - ***パスワードの変更***ユーザーログイン用のパスワードを設定します。



9. **[Back（戻る）]**を選択し、次に**[Finish（完了）]**を選択します。設定の変更内容を確認します。

   設定が保存され、システムが再起動します。

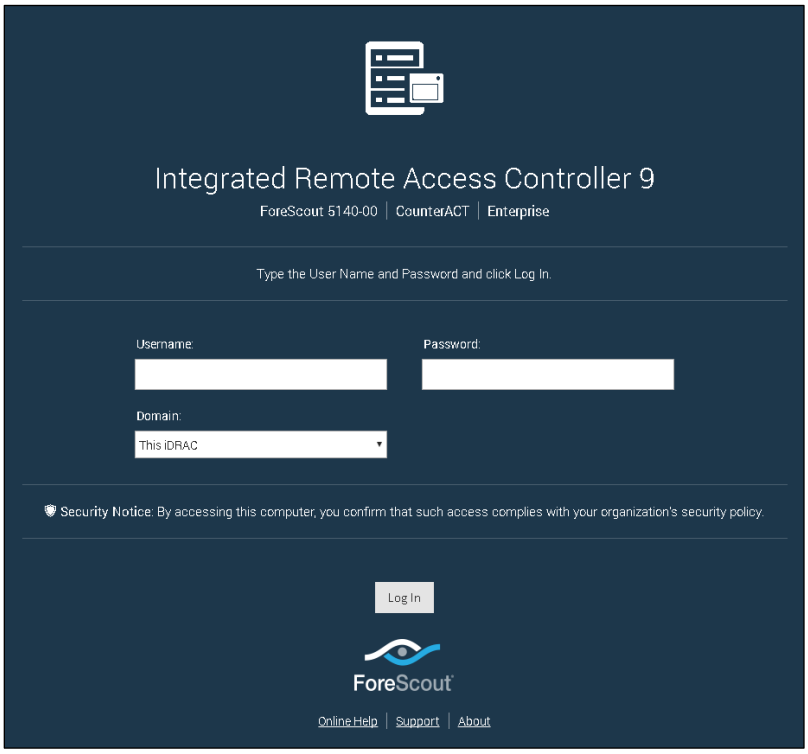
モジュールをネットワークに接続する

iDRAC はイーサネットネットワークに接続します。通常は、そこから管理ネットワークに接続されます。以下の画像は、CT-1000 アプライアンスの後部パネル上の iDRAC ポートの位置を示しています。

iDRAC へのログイン

iDRAC へのログイン方法：

1. **[iDRAC Settings（iDRAC 設定）]** > **[Network（ネットワーク）]**で設定された IP アドレスまたはドメイン名を検索します。



2. iDRAC システム設定の[User Configuration（ユーザー設定）]ページで設定したユーザー名とパスワードを入力します。
3. **[Submit（送信）]** を選択します。

iDRAC の詳細については、*『iDRAC User's Guide（iDRAC ユーザーガイド）』*をご参照ください。展開しているアプライアンスが使用しているライセンス許諾モードにより異なりますが、このガイドは以下の場所のうちのいずれかにあり、そこからアクセスできます。

- 個別アプライアンスライセンス許諾モード - https://updates.forescout.com/downloads/support/iDRAC_user_guide.pdf
- 集中ライセンス許諾モード - [Customer Portal（カスタマーポータル）]、[Documentation（ドキュメント）]ページ

展開しているアプライアンスがどのラインセンス許諾を使用しているかを知るには、追加の CounterACT ドキュメント（*コンソールのライセンス許諾モードの確認*）をご参照ください。

まだこの操作を実行していない場合は、デフォルトのルートパスワードをアップデートすることが非常に重要です。

6. 接続の検証

管理インターフェイスの接続の検証

管理インターフェイスの接続をテストするには、アプライアンスにログインして、以下のコマンドを実行します。

fstool linktest

以下の情報が表示されます。

```
Management Interface status
Pinging default gateway information
Ping statistics
Performing Name Resolution Test
Test summary
```

Ping テストの実行

アプライアンスでネットワークデスクトップに以下のコマンドを実行して接続を検証します。

Ping <network_desktop_IP_address>

7. CounterACT コンソールの設定

CounterACT コンソールのインストール

コンソールは、エンドポイントに関する重要な情報を表示し管理するための CounterACT 管理アプリケーションです。CounterACT デバイスがこの情報を収集します。詳細については、*『CounterACT Administration Guide（CounterACT 管理ガイド）』*をご参照ください。

CounterACT コンソールアプリケーションソフトウェアをホストするためのマシンは御社でご用意ください。最低限のハードウェア要件は以下の通りです。

- 以下を実行できるマシン（専用に別途用意する必要はありません）：
  - Windows 7／8／8.1／10
  - Windows Server 2008／2008 R2／2012／2012 R2／2016
  - Linux RHEL／CentOS 7
- 2GB RAM
- 1GB のディスク空き領域

コンソールのインストールは、以下の方法で実行します。

御社のアプライアンス用に構築されたインストールソフトウェアを使用します。

1. コンソールコンピュータからブラウザのウィンドウを開きます。
2. ブラウザのアドレス入力欄に以下を入力します。

   http://<Appliance_ip>/install

   Appliance_ip がこのアプライアンスの IP アドレスの場合、ブラウザで[Console installation（コンソールインストール）]ウィンドウが表示されます。
3. 画面の指示に従います。

ログイン

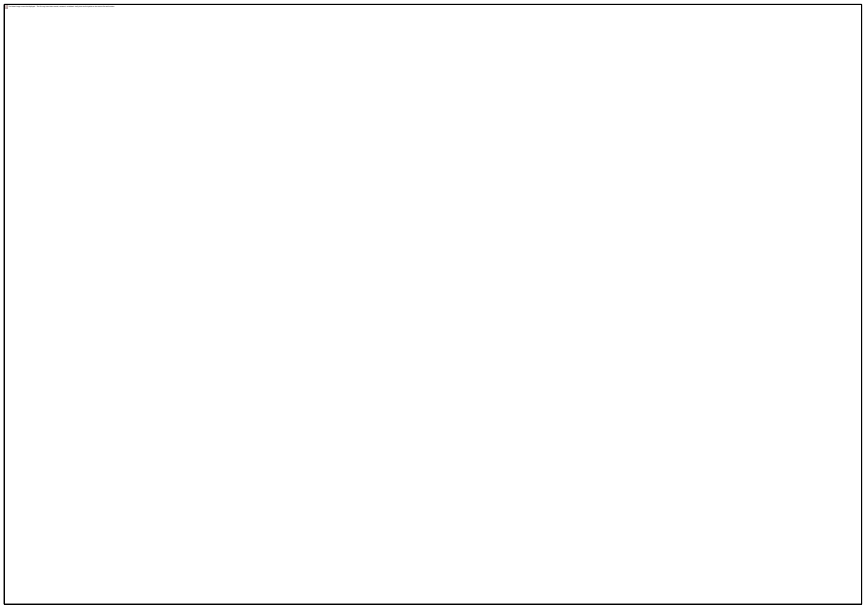
インストールが完了すると、CounterACT コンソールにログインできるようになります。

1. 作成したショートカットから CounterACT アイコンを選択します。

2. **[IP/Name（IP／名前）]**フィールドにアプリケーションの IP アドレスまたはホスト名を入力します。
3. **[User Name（ユーザー名）]**フィールドに「admin」と入力します。
4. **[Password（パスワード）]**フィールドに、アプライアンスのインストール時に作成したパスワードを入力します。
5. **[Login（ログイン）]**を選択してコンソールを起動します。

初期設定の実行

初回ログイン時に、[Initial Setup（初期設定）]ウィザードが開きます。このウィザードは、CounterACT が素早く効率的に稼働するために欠かせない設定手順をガイドします。



初期設定開始の前に

ウィザードで作業を行う前に、以下の情報を確認しておきます。

ウィザードで必要となる情報	値
お客様の組織がお使いの NTP サーバーアドレス（オプション）	
アプライアンスからの SMTP トラフィックが拒否される場合に、電子メールのアラートが配信されるようにするための内部メールリレーIP アドレス（オプション）	
CounterACT 管理者の電子メールアドレス	
モニターインターフェイスとレスポンスインターフェイス	
DHCP がないセグメント／VLAN については、レスポンスインターフェイスが直接接続されているネットワークセグメント／VLAN と各 VLAN で CounterACT が使用する恒久 IP アドレス	
アプライアンスがモニターする IP アドレスの範囲（未使用のアドレスを含むすべての内部アドレス）	
LDAP ユーザーアカウント情報と LDAP サーバーIP アドレス	
ドメイン管理アカウント名とパスワードを含むドメイン認証情報	
どのネットワークホストが認証に成功したかを CounterACT が解析するための、認証サーバー	
スイッチ IP アドレス、ベンダーおよび SNMP のパラメータ	

このウィザードを通じた操作の詳細については、*『CounterACT Administration Guide（CounterACT 管理ガイド）』*またはオンラインヘルプをご参照ください。

追加の CounterACT ドキュメント

CounterACT のその他の機能とモジュールの詳細については、以下の資料をご参照ください。

- ドキュメントのダウンロード
- ドキュメントポータル
- CounterACT ヘルプツール

ドキュメントのダウンロード

ダウンロード可能なドキュメントへは以下の 2 つの ForeScout ポータルからアクセスできますが、どちらのポータルが利用できるかは、展開しているアプライアンスがどのライセンス許諾モードを使用しているかによって異なります。

- ***個別アプライアンス型ライセンス許諾モード*** – 製品アップデートポータル
- ***集中ラインセンス許諾モード*** – カスタマーポータル

このポータルからはソフトウェアも入手できます。

展開しているアプライアンスがどのライセンス許諾モードを使用しているかを知るには、コンソールでのライセンス許諾モードの確認をご参照ください。

製品アップデートポータル

製品アップデートポータルには、CounterACT バージョンリリース、ベースモジュールとコンテンツモジュール、拡張モジュール、関連ドキュメントへのリンクがあります。このポータルには様々な追加ドキュメントもあります。

製品アップデートポータルにアクセスするには：

1. https://updates.forescout.com/support/index.php?url=counteract を開きます。
2. 希望の CounterACT バージョンを選択します。

カスタマーポータル

ForeScout カスタマーポータルのダウンロードページには、購入した CounterACT バージョンリリース、ベースモジュールとコンテンツモジュール、拡張モジュール、関連ドキュメントへのリンクがあります。ソフトウェアのライセンスを有している場合は、ソフトウェアと関連のドキュメントは、ダウンロードページ上に表示されるのみです。このポータルのドキュメントページには、様々な追加ドキュメントがあります。

ForeScout カスタマーポータル上のドキュメントにアクセスするには：

1. https://forescout.force.com/support/を開きます。
2. **[Downloads（ダウンロード）]**または**[Documentation（ドキュメント）]**を選択します。

ドキュメントポータル

ForeScout ドキュメントポータルは、CounterACT ツール、特長、機能、統合についての情報が含まれる検索可能なウェブベースのライブラリです。

> *展開しているアプライアンスが集中ライセンス許諾モードを使用している場合は、このポータルにアクセスする権限がない場合があります。*

ドキュメントポータルにアクセスするには：

1. www.forescout.com/docportal を開きます。
2. カスタマサポート認証情報を使用してログインします。
3. 希望の CounterACT バージョンを選択します。

CounterACT ヘルプツール

CounterACT コンソールから直接情報にアクセスします。

コンソールヘルプボタン

コンテキスト依存の *[Help（ヘルプ）]*ボタンを使用して、作業中のタスクとトピックについての情報に素早くアクセスします。

CounterACT 管理ガイド

[Help（ヘルプ）]メニューで**[CounterACT Help（CounterACT ヘルプ）]**を選択します。

プラグインヘルプファイル

1. プラグインをインストールし、**[Tools（ツール）]**メニューで**[Options（オプション）]**を選択し、**[Modules（モジュール）]**を選択します。
2. プラグインを選択し、**[Help（ヘルプ）]**を選択します。

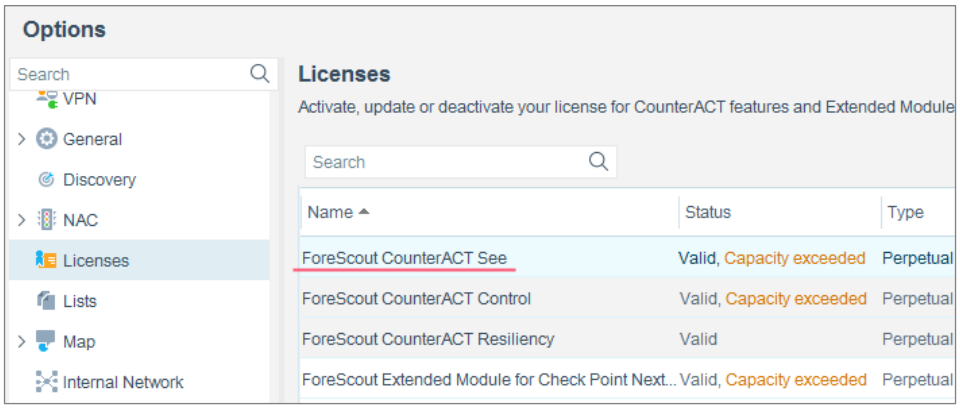
ドキュメントポータル

[Help（ヘルプ）]メニューで**[Documentation Portal（ドキュメントポータル）]**を選択します。

コンソールでのライセンス許諾モードの確認

コンソールに表示された *ForeScout CounterACT See* ライセンスがエンタープライズマネージャにあれば、展開しているアプライアンスは集中ライセンス許諾モードで稼働しています。それ以外の場合は、展開しているアプライアンスは個別アプライアンスライセンス許諾モードで稼働しています。

[Options（オプション）]> **[Licenses（ライセンス）]**を選択し、表に *ForeScout CounterACT See* ライセンスが含まれているかを確認します。



ライセンス許諾モードの確認方法についてご不明な点がありましたら、御社担当の ForeScout レプレゼンタティブまでお問い合わせください。

法律上の注意

本文書についてのご意見、お問い合わせは以下宛にお願いします。support@forescout.com

2018-03-27 15:05