



Fore Scout®

シングルライセンス
クイックインストールガイド

バージョン 8.2



お問い合わせ先

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

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

フリーダイヤル（米国内から）：1.866.377.8771

電話（米国外から）：1.408.213.3191

サポート：1.708.237.6591

本書について

- 本書以外の参考文書については、Forescout ウェブサイトの Resources（リソース）ページをご参照ください：<https://www.forescout.com/company/resources/>
- フィードバックまたはご質問がありますか？ documentation@forescout.com までご連絡ください。

法律上の注意

© 2019 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc.は、デラウェア州の法人です。商標と特許は、こちらで確認いただけます。

<https://www.forescout.com/company/legal/intellectual-property-patents-trademarks> その他のブランド、製品、またはサービスの名称は、各所有者の商標またはサービスマークの場合があります。

2020年2月11日 12:13:31

目次

バージョン 8.2 へようこそ	5
Forescout パッケージの内容	5
概要	6
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	10
レスポンスインターフェイス	10
2. スイッチの設定	11
A. スイッチ接続の選択	11
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）	11
2 パッシブインラインタップ	11
3 アクティブ（インジェクション対応）インラインタップ	11
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）	11
B. スイッチ設定時の注意事項	12
VLAN（802.1Q）タグ	12
追加ガイドライン	12
3. ネットワークケーブルの接続と電源投入	13
A. アプライアンスを開梱してケーブルを接続する	13
B. インターフェイスの割り当てを記録する	13
C. アプライアンスの電源を入れる	14
4. アプライアンスの設定	15
5. リモート管理	20
iDRAC の設定	20
iDRAC モジュールを有効化し設定する	20
モジュールをネットワークに接続する	23
iDRAC へのログイン	23
6. 接続の検証	25
管理インターフェイスの接続の検証	25
Ping テストの実行	25
7. Forescout コンソールの設定	26
コンソールのインストール	26
ログイン	26

初期設定の実行	27
初期設定開始の前に	28
Forescout の追加ドキュメント	29
ドキュメントのダウンロード	29
ドキュメントポータル	30
Forescout ヘルプツール	30

バージョン 8.2 へようこそ

Forescout 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。このプラットフォームは、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定義されます。

このガイドでは、バージョン 8.0 がプレインストールされている、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。一部のアプライアンスには、以降のバージョンがプレインストールされている場合があります。バージョン 8.2 を使用するには、同バージョンのリリースノートに概説された、承認済みのアップグレードパスに従ってください。



詳細、アップグレードの詳細、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『ForeScout Installation Guide (ForeScout インストールガイド)』および『ForeScout Administration Guide (ForeScout 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、[ForeScout の追加ドキュメント](#)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。

Forescout パッケージの内容

Forescout 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 (ハードウェアベースの CT-xxxx アプライアンス改訂 5x と ForeScout 51xx アプライアンス専用)

概要

Forescout 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. Forescout 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、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、『[Forescout Installation Guide \(Forescout インストールガイド\)](#)』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、[Forescout の追加ドキュメント](#)をご参照ください。

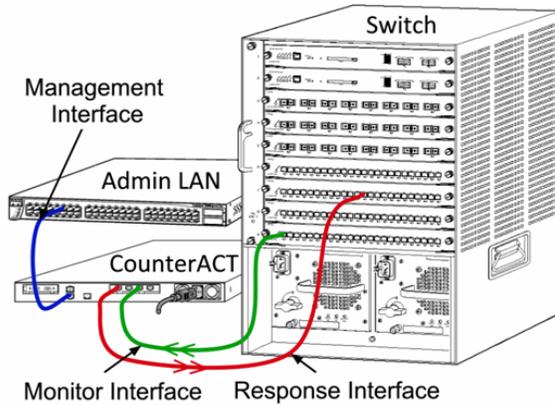
アプライアンスのインターフェイス接続

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、Forescout プラットフォーム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、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	Forescout プラットフォーム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。 Forescout プラットフォーム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	Forescout プラットフォーム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アプライアンスにアクセスできるようにします。 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	Forescout プラットフォーム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	Forescout プラットフォームが内部 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	Forescout プラットフォーム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、Forescout プラットフォームは ntp.foreScout.net にアクセスします。

ポート	サービス	Forescout プラットフォーム接続先または接続元	機能
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	Forescout プラットフォーム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、 『Forescout Administration Guide (Forescout 管理ガイド)』をご参照ください。
162/UDP	SNMP	接続先	Forescout プラットフォーム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、 『Forescout Administration Guide (Forescout 管理ガイド)』をご参照ください。
389/TCP (636)	LDAP	接続元	Forescout プラットフォームが Active Directory と通信できるようにします。 Forescout プラットフォームのウェブベースの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 マシンからアプリケーションへのセキュアな (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。

ポート	サービス	Forescout プラットフォーム接続先または接続元	機能
10003/TCP	Windows 用 SecureConnector	接続先	<p>SecureConnector が Windows マシンからライセ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、『<i>Forescout Administration Guide (Forescout 管理ガイド)</i>』をご参照ください。</p> <p>SecureConnector がライセ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ライセンスにリダイレクトされます。このポートをすべてのライセ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。</p>
10005/TCP	OS X 用 SecureConnector	接続先	<p>SecureConnector が OS X マシンからライセ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、『<i>Forescout Administration Guide (Forescout 管理ガイド)</i>』をご参照ください。</p> <p>SecureConnector がライセ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ライセンスにリダイレクトされます。このポートをすべてのライセ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。</p>
13000/TCP	Forescout プラットフォーム	接続元/接続先	<p>単独のライセンスのみが存在する展開用 - コンソールからライセンス。</p> <p>複数のライセンスが存在する展開用 - コンソールからライセンス、特定のライセンスから別のライセンス。ライセンスの通信には、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。</p>

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、ライセ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、ライセ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、ライセ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

ライセンスは、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、ライセンスは、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。ライセンスは、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

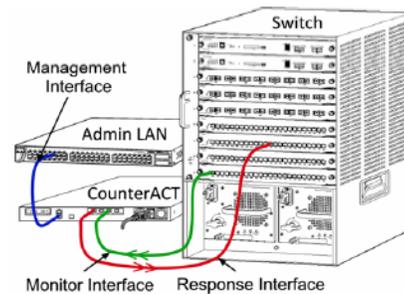
A. スイッチ接続の選択

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）

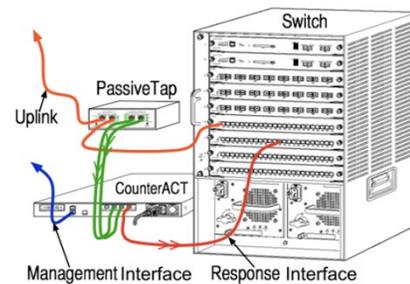
展開には3つの個別のポートを使用することが推奨されます。これらのポートの説明は、[アプライアンスのインターフェイス接続](#)でご確認ください。



2 パッシブインラインタップ

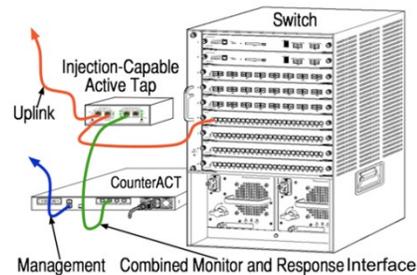
アプライアンスでは、スイッチモニターポートに接続する代わりに、パッシブインラインタップを使用できます。

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

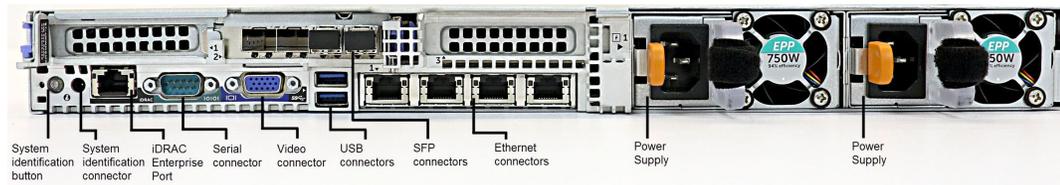
- 以下の場合、1 つのインターフェイス（送信／受信を可能にする）のみをミラーリングするようにします。
 - スイッチが送信トラフィックと受信トラフィックの両方をミラーリングできない場合
 - スイッチがすべてのスイッチトラフィックをミラーリングできない場合
 - スイッチがすべてのトラフィックを VLAN を通じてミラーリングできない場合
- ミラーリングポートに負荷がかかりすぎていないか確認してください。
- スイッチによっては（例：Cisco 6509）、新しい設定を入力する前に現在のポート設定を完全に削除する必要がある場合があります。古いポート情報を削除しないと、多くの場合、スイッチが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



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、『*Forescout Installation Guide (Forescout 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 Forescout 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、*チャンネルの定義*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ン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、『*Forescout Installation Guide* (Forescout 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	
Forescout 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。

- ☞ 以下のプロンプトは、バージョン8.0をベースにしています。一部のアプライアンスには、プロンプトの内容が若干異なるバージョンがプレインストールされている場合があります。

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

1. **Enter** キーを押します。Forescout 51xx アプライアンスの場合、以下のメニューが表示されます。

```
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
```

CT-xxxx アプライアンスの場合、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、『*Forescout Installation Guide (Forescout 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 7.0.0 をインストールするか 8.0.0 を設定するかの選択肢が表示されます。7.0.0 を選択すると、[Configuration (設定)]メニューから 8.0.0 を再インストールできなくなります。バージョン 7.0.0 の設定の詳細については、『*Forescout Installation Guide version 7.0.0 (Forescout 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ライセンスの再イメージ化が必要になります。ライセンスの再イメージ化の詳細については、『*Forescout Installation Guide (Forescout インストールガイド)*』をご参照ください。

2. 1 と入力して **Enter** キーを押します。

```
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] :
```

3. 1 (Standard Installation) と入力して **Enter** キーを押します。

```
>>>>> 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):
```

4. Yes (はい) と入力して Enter キーを押します。

☞ クリーンな 8.2 のインストールを実行する際に以下のプロンプトが表示されます。

```
Certification Compliance Mode? (yes/no) [no] :
```

5. 組織が共通の基準および DoDIN APL 認証に準拠する必要がある場合を除いて、No (いいえ) と入力して Enter キーを押します。

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

- 1) CounterACT Appliance
- 2) CounterACT Enterprise Manager

6. 1 と入力して Enter キーを押します。設定が初期化されます。初期化には少々時間がかかります。

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

- 1) Per Appliance licensing mode
- 2) Flexx licensing mode

```
Choice (1-2) [1]:
```

7. 展開に使用するライセンスモードを選択します。ライセンスモードは購入時に決定されます。展開に使用するライセンスモードの種類の検証が終わるまで、値を入力しないでください。ライセンスモードを検証したい場合、または間違ったモードを入力したためサポートが必要な場合は、御社担当の Forescout レプレゼンタティブにご連絡ください。

☞ このオプションは、Forescout 51xx のアプライアンスには表示されません。

8. 個別アプライアンス型ライセンス許諾モードの場合は 1 を、Flexx ライセンス許諾モードの場合は 2 を入力して Enter キーを押します。

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

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

```
Description :
```

9. 説明を入力して **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 '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 :
```

10.[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。

■ **cliadmin** 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。

11.[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。

12.[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。

- **Forescout** プラットフォームコンポーネントは、管理インターフェイスから通信します。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、**Forescout** プラットフォームコンポーネントが通信に使用するインターフェイスのアドレスです。この例では、**Forescout** プラットフォーム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。

13.[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、アプライアンスに有効なライセンスがあることを確認してください。アプライアン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。

- Forescout 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ようになります。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）。

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、『*Forescout Administration Guide (Forescout 管理ガイド)*』をご参照ください。

Forescout 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 Forescout 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。Forescout プラットフォームは 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、『*Forescout Installation Guide (Forescout インストールガイド)*』をご参照ください。

個別アプライアンス型ライセンス許諾モードのライセンス管理の詳細については、『*Forescout Administration Guide (Forescout 管理ガイド)*』をご参照ください。

- 御社の Forescout が **Flexx 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。利用可能になった後、**展開管理者**はコンソール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、ライセンスの強制行使が適用され、コンソール設定の特定の変更は制限される場合があります。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。

詳細については、『*Forescout Flexx Licensing How-to Guide (Forescout Flexx ライセンス許諾のハウツーガイド)*』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

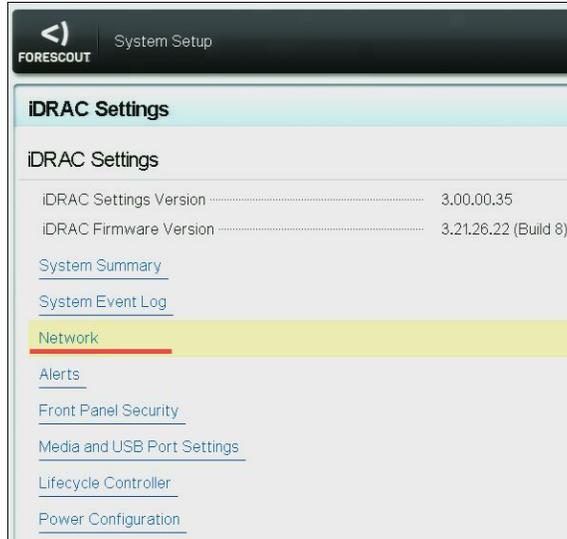
iDRAC の設定を変更して、CounterACT デバイスへのリモートアクセスを有効にします。このセクションでは、Forescout プラットフォームで作業を行うために必要な基本的な統合設定について説明します。

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。



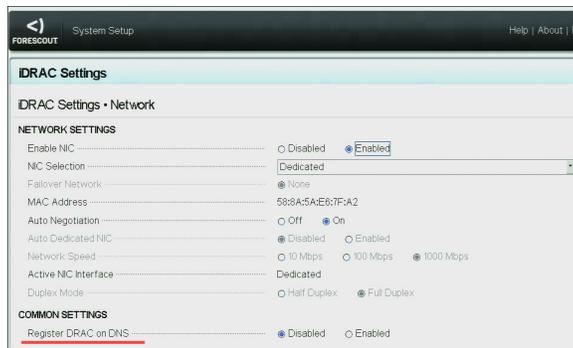
5. 以下のようにネットワークを設定します：

- 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。



6. (オプション) [iDRAC Settings (iDRAC 設定)] > [Network (ネットワーク)] > [Common Settings (共通設定)]で、動的 DNS をアップデートします：

- a. [Register iDRAC on DNS (iDRAC を DNS に記録)]を[Enabled (有効)]に設定します。
- b. [DNS iDRAC Name (DNS iDRAC 名)]フィールドに動的 DNS を入力します。



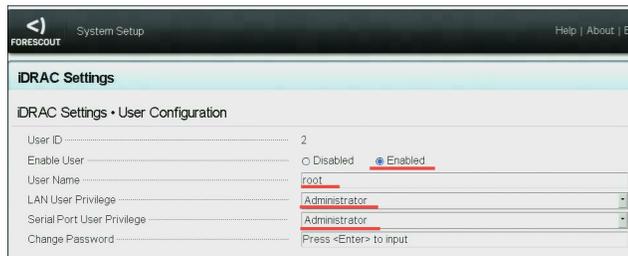
7. [iDRAC Settings (iDRAC 設定)] > [Network (ネットワーク)] > [IPv4 Settings (IPv4 設定)]で、以下の設定をします：



- **[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。
- 動的 IP アドレス指定を使用するには、**[Enable DHCP (DHCP の有効化)]**フィールドを**[Enabled (有効)]**に設定します。DHCP が自動的に IP アドレス、ゲートウェイ、サブネットマスクを iDRAC に割り当てます。
または
[Enable DHCP (DHCP の有効化)]フィールドを**[Disabled (無効)]**に設定して静的 IP アドレス指定を使用し、**[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)]**フィールドに任意の値を入力します。

8. **[Back (戻る)]**を選択します。

9. **[iDRAC Settings (iDRAC 設定)]** > **[User Configuration (ユーザー設定)]**で以下の操作をします：



以下のユーザー設定フィールドで「ルート」ユーザーの設定をします：

- **[Enable User (ユーザーの有効化)]**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。
- ☞ ここで設定するユーザー名 (ルート) は、*Forescout* のユーザー名とは異なります。
- **[LAN User Privilege (LAN ユーザー権限)]**で、**[Administrator (管理者)]**を選択します。
- **[Serial Port User Privilege (シリアルポートユーザー権限)]**で、**[Administrator (管理者)]**を選択します。
- **[Change Password (パスワード変更)]**で、ユーザーがログインする際のパスワードを設定します。

10. **[Back (戻る)] > [Finish (完了)]**を選択します。変更した設定を確認します。
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

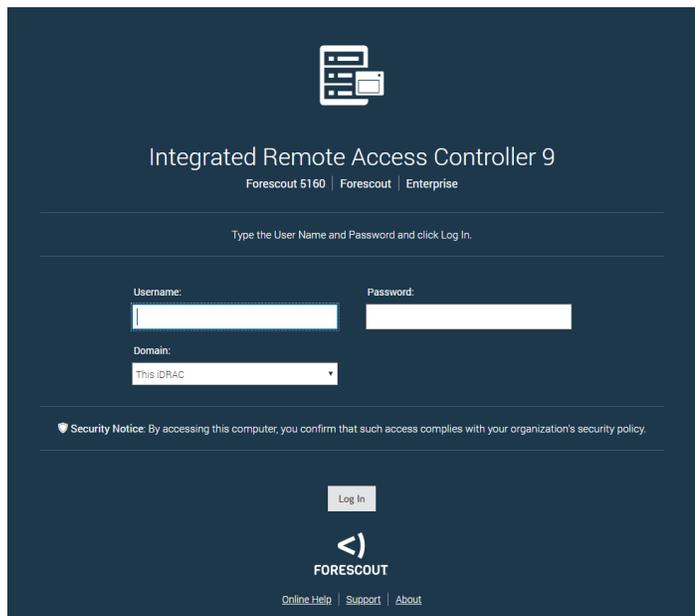
iDRAC はイーサネットネットワークに接続します。通常は、そこから管理ネットワークに接続されます。以下の画像は、CT-1000 アプライアンスの後部パネル上の iDRAC ポートの位置を示しています。



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。このガイドへは、以下からアクセスできます。

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

ライセンス許諾モードを確認するには：

- コンソールで、**[Help (ヘルプ)] > [About Forescout (Forescout について)]** を選択します。
- ☞ 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이스の接続の検証

管理インターフェ이스の接続をテストするには、ライセ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

ライセ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. Forescout コンソールの設定

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 Forescout 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、『*Forescout Administration Guide (Forescout 管理ガイド)*』をご参照ください。

Forescout 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 R2/2016/2019
 - 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

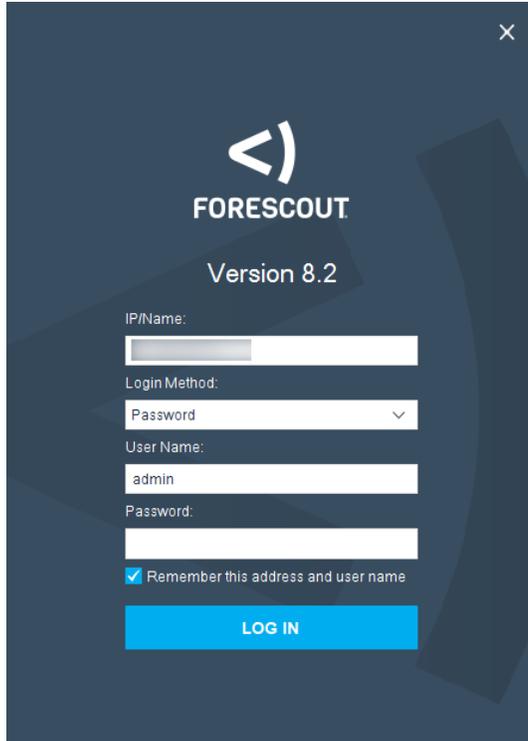
Appliance_ip がこのアプライアンスの IP アドレスの場合、ブラウザで [Console installation (コンソールインストール)]ウィンドウが表示されます。

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、コンソールにログインできるようになります。

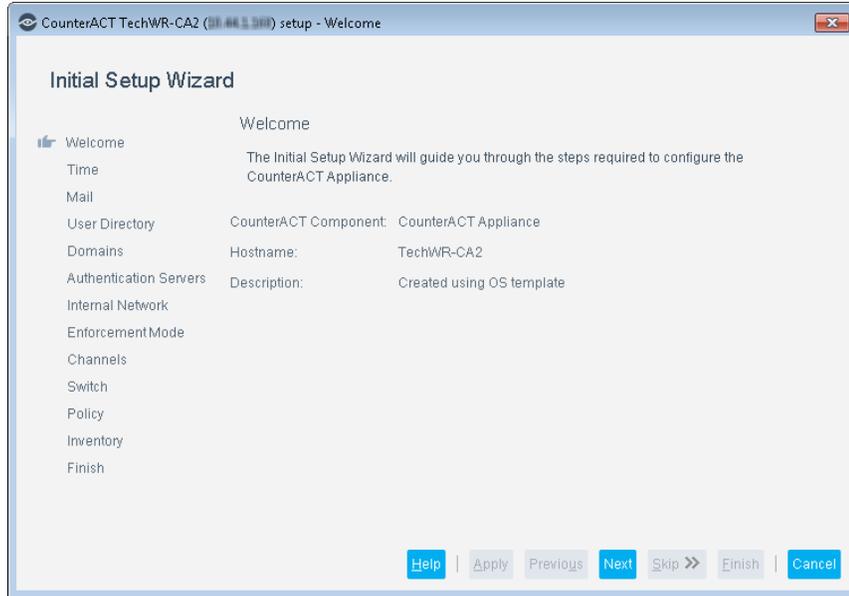
1. 作成したショートカットから Forescout アイコンを選択します。



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、ライセ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、Forescout プラットフォーム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)	
ライセンスからの 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)	
Forescout 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 Forescout プラットフォームが使用する恒久 IP アドレス	
ライセ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 Forescout プラットフォームが解析するための、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、『*Forescout Administration Guide (Forescout 管理ガイド)*』またはオンラインヘルプをご参照ください。

Forescout の追加ドキュメント

Forescout 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](#)
- [Forescout 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、[Forescout Technical Documentation ページ](#)、または以下の 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](#)
- **Flexx ライセンス許諾モード** - [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。

ライセンス許諾モードを確認するには：

- コンソールで、**[Help (ヘルプ)] > [About Forescout (Forescout について)]** を選択します。

Forescout Technical Documentation ページ

Forescout Technical Documentation ページは、検索可能なウェブベースの [Documentation Portal](#) へのアクセスと、すべての技術ドキュメントへの PDF リンクを提供します。

Technical Documentation ページにアクセスするには：

- <https://www.Forescout.com/company/technical-documentation/>を開きます。

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、Forescout 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、eyeExtend 製品、および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：

- <https://updates.forescout.com/support/index.php?url=counteract> を開き、探している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 Forescout 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、eyeExtend 製品、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。

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：

- <https://Forescout.force.com/support/>を開き、**[Downloads (ダウンロード)]**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、Forescout のツール、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。

- ▣ 展開しているライセンスが **Flexx** 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を受け取ってい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：

- https://updates.forescout.com/support/files/counteract/docs_portal/を開き、カスタマサポート認証情報を使用してログインします。

Forescout ヘルプツール

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。

Forescout 管理ガイド

- **[Help (ヘルプ)]** メニューで **[Administration Guide (管理ガイド)]** を選択します。

プラグインヘルプファイル

- プラグインのインストール後、**[Tools (ツール)]** > **[Options (オプション)]** > **[Modules (モジュール)]** を選択し、プラグインを選択してから **[Help (ヘルプ)]** を選択します。

ドキュメントポータル

- **[Help (ヘルプ)]** メニューから **[Documentation Portal (ドキュメントポータル)]** を選択し、[ドキュメントポータル](#) にアクセスします。