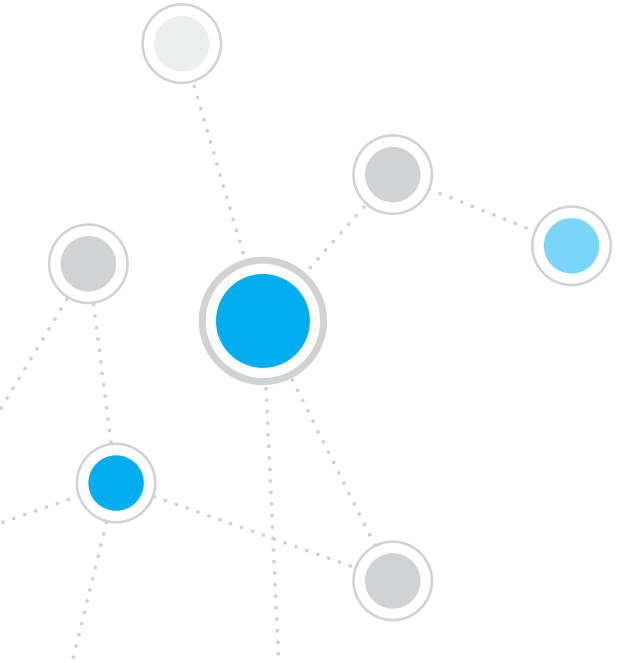
ForeScout

ForeScout CounterACT® 7

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



目次

ForeScout CounterACT® バージョン 7 へようこそ

ForeScout CounterACTは、物理的または仮想のセキュリティ・アプライアンスで、お客様のネットワークに接続された瞬間に、ネットワーク・デバイスとアプリケーションをダイナミックに検知し評価します。CounterACTはエージェントを必要としないので、組み込みの、また仮想の、お客様のデバイス（管理対象か非管理対象化を問わず、また既知か既知でないかを問わず）、PCおよびモバイルと共に動作します。CounterACTは、ユーザー、オーナー、オペレーティング・システム、デバイス構成、ソフトウェア、サービス、パッチ・ステート、およびセキュリティ・エージェントの存在を迅速に判断します。次に、デバイスがネットワークを行き来するに従い、デバイスの修復、制御と継続的な監視を提供します。お客様の既存の IT インフラストラクチャとシームレスに統合しつつ、これらのすべてを実行します。

このガイドでは、1台のスタンドアローン CounterACT アプライアンスの設置について説明します。

より詳しい情報、または企業全体のネットワーク保護のための複数アプライアンスの配置に関する詳細は、『*CounterACT Installation Guide*（CounterACT インストール・ガイド）』、および『*Console User Manual*（コンソール・ユーザー・マニュアル）』を参照してください。これらのマニュアルは、CounterACT CD の / docs ディレクトリにあります。

また、サポート・ウェブサイト https://www.forescout.com/support から、最新のマニュアル、知識ベース記事、そして、使用アプライアンスのアップデートを入手することもできます。

CounterACT パッケージの付属品

- CounterACT アプライアンス
- クイック・インストール・ガイド
- CounterACT CD（コンソール・ソフトウェア、CounterACT Console User Manual（CounterACT コンソール・ユーザー・マニュアル）、CounterACT Installation Guide（CounterACT インストール・ガイド））
- 保証書
- 取り付け用ブラケット
- 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）

概要

CounterACT の設定には、次の作業を行います。

1. 配置プランの作成
2. 使用スイッチの設定
3. ネットワーク・ケーブルの接続と電源オン
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. 配置プランの作成

インストールする前に、アプライアンスをどこに配置するかを決定し、アプライアンスのインターフェース接続を理解することが必要です。

アプライアンス配置位置の決定

ネットワーク上で、アプライアンスの適正な位置を選択することは、CounterACT の正しい配置と最適な性能を左右する極めて重要な事項です。適切な位置は、実装の目的とネットワーク・アクセス・ポリシーによって異なります。アプライアンスは、適用するポリシーに関連するトラフィックをモニターできなければなりません。たとえば、ポリシーが、エンドポイントから企業の認証サーバーまでの承認イベントの監視に依存する場合は、アプライアンスは、認証サーバーに流れるエンドポイント・トラフィックが見える位置に設置する必要があります。

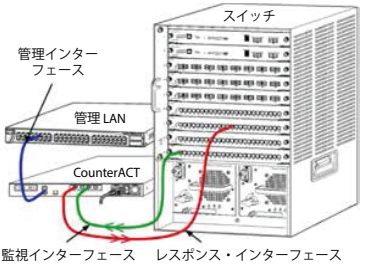
インストールおよび配置に関する詳細は、本パッケージに付属の CounterACT CDに収録されている、『CounterACT Installation Guide（CounterACT インストール・ガイド）』を参照してください。

アプライアンス・インターフェースの接続

アプライアンスは、通常、ネットワーク・スイッチとの3つの接続で設定されます。

管理インターフェース

このインターフェースは、CounterACT の管理とエンドポイントのクエリおよび徹底監視の実施を可能にします。このインターフェースは、すべてのネットワーク・エンドポイントにアクセスのあるスイッチ・ポートに接続する必要があります。



各アプライアンスに、ネットワークに対して単一の管理接続が必要です。この接続には、ローカル LAN 上の IP アドレスが1つと、CounterACT コンソール管理アプリケーション実行用マシンからの 13000/TCP ポートへのアクセスが必要です。管理インターフェースは、使用ネットワークの次にアクセスできることが必要です。

ポート	サービス	CounterACT 着/発	機能
22/TCP	SSH	着	CounterACT コマンド・ライン・インターフェースへのアクセスを可能にします。
2222/TCP			（高可用性）高可用性クラスターの一部となっている物理 CounterACT デバイスへの アクセスを可能にします。22/TCP ポートを使用して、クラスターの共有（仮想）IP アドレスにアクセスします。

ポート	サービス	CounterACT 着/発	機能
25/TCP	SMTP	発	CounterACT からのメールの送信に使用します。
53/UDP	DNS	発	CounterACT が内部 IP アドレスを解決することを可能にします。
80/TCP	HTTP	着	HTTP のリダイレクションを可能にします。
123/UDP	NTP	発	CounterACT が NTP タイムサーバーにアクセスすることを可能にします。デフォルトでは、CounterACTは ntp.foreScout.net を使用します。
135	WMI	発	CounterACT が WMI を使用して Windows エンドポイントの徹底調査と制御を可能にします。
139/TCP	SMB, MS-RPP	発	Windowsエンドポイントのリモート検査を可能にします（Windows 7以前で実行されているエンドポイントに対して）。
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	発	CounterACT が、*スイッチやルーターなどのネットワーク・インフラ機器と通信することを可能にします。* SNMP *の設定に関する詳細は、『CounterACT Console User Manual（CounterACT コンソール・ユーザー・マニュアル）』を参照してください。*
162/UDP	SNMP	着	CounterACT が、*スイッチやルーターなどのネットワーク・インフラ機器から* SNMP *トラップを受信することを可能にします。* SNMP *の設定に関する詳細は、『CounterACT Console User Manual（CounterACT コンソール・ユーザー・マニュアル）』を参照してください。*
443/TCP	HTTPS	着	TLS を使用する HTTP のリダイレクションを可能にします。
2200/TCP	Secure Connector	着	SecureConnector が、Macintosh/Linux マシンからアプライアンスまでの安全な（暗号化SSH）接続を作成することを可能にします。SecureConnectorは、ホストがネットワークに接続されている間、管理できないエンドポイントへのアクセスを、デスクトップ上で実行されるシェル・スクリプトを経由して可能にします。SecureConnectorは、MacintoshおよびLinuxのエンドポイントの管理を有効にするエージェントに基づくスクリプトで、その一方、エンドポイントはネットワークに接続されています。
10003/TCP	Secure Connector for Windows	着	SecureConnectorが、Windowsマシンから、アプライアンスに対しセキュアな（暗号化TLS）接続を作成することを可能にします。SecureConnectorは、Windowsのエンドポイントの管理を有効にするエージェントに基づくスクリプトで、その一方、エンドポイントはネットワークに接続されています。

			SecureConnectorに関する詳細については、*CounterACT Console User Manual* を参照してください。 SecureConnectorが、アプライアンスに、またはEnterprise Managerに接続する場合は、その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。このポートが、全アプライアンスとEnterprise Managerに対しオープンになっていることを確認し、組織内で、透明性の高いモビリティを可能にします。
13000/TCP	CounterACT	着	コンソールからアプライアンスまでの接続を可能にします。 複数の CounterACT アプライアンスを使用するシステムでは、コンソールから Enterprise Manager までの接続と、Enterprise Manager から各アプライアンスまでの接続を可能にします。

監視インターフェース
この接続は、アプライアンスがネットワーク・トラフィックを監視し、追跡することを可能にします。
トラフィックはスイッチのポートにミラーリングされ、アプライアンスにより監視されます。ミラーリングされる VLAN の数によって、トラフィックは 802.1Q VLAN タギングが可能な場合と可能でない場合があります。

- **単一の VLAN（タギングなし）：** 監視されるトラフィックが単一の VLAN から生成される場合は、ミラーリングされるトラフィックは、VLAN タギングされる必要はありません。
- **複数の VLAN（タギングあり）：** 監視されるトラフィックが複数の VLAN発の場合、ミラーリングされるトラフィックは、タギングされた 802.1Q VLAN であることが必要です。

2つのスイッチが冗長ペアとして接続されている場合、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監視する必要があります。
通常、監視インターフェースには IP アドレスは必要ありません。監視インターフェースには、IPアドレスは必要ありません。

レスポンス・インターフェース
アプライアンスは、このインターフェースを使用してトラフィックに応答します。レスポンス・トラフィックは、悪意のある行為からの保護と、NAC ポリシー・アクションの実行に使用されます。このようなアクションには、たとえば、ウェブ・ブラウザーのリダイレクト、またはファイアウォールのブロックが挙げられます。関連するスイッチ・ポートの設定は、監視されるトラフィックによって異なります。

- **単一の VLAN（タギングなし）：** 監視するトラフィックが単一の **VLAN** から生成される場合には、レスポンス・インターフェースは同じ **VLAN** の一部として設定されることが必要です。この場合、アプライアンスは、その **VLAN** 上で単一の **IP** アドレスが必要です。

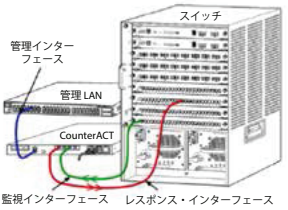
- **複数のVLAN（タギングあり）：** 監視するトラフィックが複数の **VLAN** からであれば、レスポンス・インターフェースも、同じ **VLAN** 群のために **802.1Q** タギング設定されていることが必要です。アプライアンスには、保護される **VALN** それぞれの IP アドレスが必要です。

2. 使用スイッチの設定

A. スイッチ接続オプション

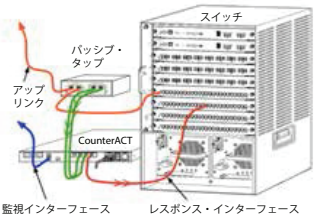
アプライアンスは、さまざまなネットワーク環境にシームレスに統合されるように設計されています。アプライアンスをネットワークに適切に統合するためには、使用スイッチが、必要なトラフィックを監視するように設定されていることを確認してください。アプライアンスを使用スイッチに接続するには、いくつかのオプションがあります。

1. **標準配置（個別の管理、監視、レスポンスのインターフェース）**
   推奨される配置では、3つの別々のポートを使用します。これらのポートは、「アプライアンス・インターフェースの接続」で説明します。

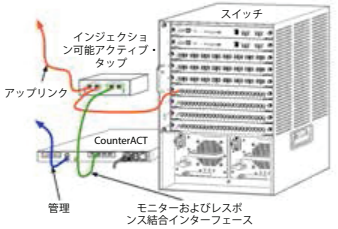


2. **パッシブ・インライン・タップ**
   スイッチの監視ポートに接続する代わりに、アプライアンスはパッシブ・インライン・タップを使用することができます。

   パッシブ・タップには、2つの二重ストリームを1つのポートに結合する「リコンビネーション」タップの場合を除き、2個の監視ポートが必要です。タップさいるポートとレスポンス・インターフェースのトラフィックは、同じ方法で設定されることが必要です。たとえば、タップされているポートでのトラフィックが VLAN (802.1Q)でタギングされている場合、レスポンス・インターフェースも VLAN タギングポートでなければなりません。



3. **アクティブ（インジェクション可能）インライン・タップ**
   アプライアンスが、インジェクション可能なインライン・タップを使用する場合は、監視とレスポンスのインターフェースは結合することができます。スイッチ上で、個別のレスポンス・ポートを設定する必要はありません。このオプションは、どのタイプのアップストリームまたはダウンストリーム・スイッチ構成にも使用することができます。



4. **IP レイヤー・レスポンス（レイヤー 3 スイッチ・インストール用）**
アプライアンスは、自身の管理インターフェースを使用してトラフィックに応答することができます。このオプションは、監視するどのトラフィックにも使用することができますが、アプライアンスがいずれかの VALNの一部ではないポートを監視するため、アプライアンスが別のスイッチ・ポートを使用して監視するトラフィックに応答できない場合に推奨されます。この状況は、2台のルーターを接続するリンクを監視する場合によく発生します。

   このオプションは、アドレス解決プロトコル（ARP）の要求には応答できず、アプライアンスが、監視するサブネットに含まれる IP アドレスを狙ったスキャンを検出する機能を制限します。この制限は、2台のルーターの間のトラフィックが監視されている場合は適用されません。

B. スイッチ設定上の注意

VLAN (802.1Q) タギング

- **単一VLAN（タギングなしのトラフィック）**の監視 監視されるトラフィックが単一の VALN 発であれば、トラフィックには802.1Q タギングの必要はありません。
- **複数の VLAN（タギングされたトラフィック）**の監視 監視されるトラフィックが 2つ以上の VLAN 発であれば、監視とレスポンスのインターフェースの両方に 802.1Q タギングが有効になっていることが必要です。複数 VLAN の監視は、ミラーリング・ポートの数を最小にしながら全体的な監視範囲が最大になるため、推奨されるオプションです。
- スイッチが、ミラーリング・ポートで802.1Q VLANタギングを使用できない場合は、次の内1つを行います。
  - 1つの VLAN のみをミラーリング
  - 1つのタギングされていないアップリンク・ポートをミラーリング
  - IP レイヤー・レスポンス・オプションを使用
- スイッチが1つのポートしかミラーリングできない場合は、1つのアップリンク・ポートをミラーリングします。これはタギングすることもできます。通常、スイッチが 802.1Q VLAN タギングをストリップする場合は、IPレイヤー・レスポンス・オプションを使用する必要があります。

追補

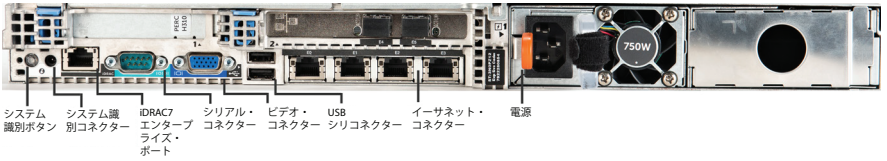
- スイッチが送信と受信の両方のトラフィックをミラーリングできない場合は、スイッチ全体、完全な VLAN（これは送信／受信を可能にします）、または、1つのインターフェースのみ（送信/受信は可能になりません）を監視します。ミラーリング・ポートが過負荷にならないことを確認してください。
- 一部のスイッチ（たとえば、Cisco 6509）では、新しい設定を入力する前に以前のポート設定を完全にクリアする必要があります。古いポート情報をクリアしなかった場合、スイッチによる802.1Q タギングのストリップが最も頻繁に起こります。

3. ネットワーク・ケーブルの接続と電源オン

A. アプライアンスの開梱とケーブル接続

1. アプライアンスと電源ケーブルを輸送用カートンから取り出します。
2. アプライアンスに同梱された、レール・キットを取り出します。
3. レール・キットをアプライアンスに取り付けて、アプライアンスをラックに取り付けます。
4. ネットワーク・ケーブルで、アプライアンス背面パネルのネットワーク・インターフェースとスイッチ・ポートの間を接続します。

背面パネルの例 — CounterACT デバイス



B. インターフェース割当ての記録

データ・センターでのアプライアンスの設置と CounterACT コンソールのインストールが完了したら、インターフェース割り当てを登録するプロンプトが表示されます。このような割り当ては、チャンネル定義と呼ばれ、コンソールに最初にログインする際に開く Initial Setup Wizard（初期セットアップ・ウィザード）に入力します。

以下に、物理インターフェース割り当てを記録し、コンソールでチャンネル・セットアップを行う際に使用します。

イーサネット・インターフェース	インターフェース割り当て（例：管理、監視、レスポンス）
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

C. アプライアンス電源オン

1. 電源ケーブルをアプライアンス背面パネルの電源コネクターに接続します。
2. 電源ケーブルの反対の端をアース付き 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、アプライアンスをシリアル接続用に設定します。*CounterACT CD* に収録されている『*CounterACT Installation Guide*（*CounterACT* インストール・ガイド）』を参照してください。
4. アプライアンスの電源を、前面パネルからオンにします。

重要：電源プラグを抜く前にマシンの電源をオフにしてください。

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、以下の情報を用意します。

□ アプライアンスのホスト名	
□ CounterACT 管理パスワード	**パスワードは安全な場所に保存してください**
□ 管理インターフェース	
□ アプライアンス IP アドレス	
□ ネットワーク・マスク	
□ デフォルト・ゲートウェイ IP アドレス	
□ DNS ドメイン名	
□ DNS サーバー・アドレス	

電源をオンにした後、次のメッセージが表示され、設定の開始が要請されます。

```
CounterACT Appliance boot is complete.
(CounterACT アプライアンスの起動が完了しました)
Press <Enter> to continue.(<Enter>を押して続行します)
```

1. **Enter** を押すと、次のメニューが表示されます。

```
1) Configure CounterACT (CounterACTの設定)
2) Restore saved CounterACT configurtion (保存されたCounterACT 設定の復元)
3) Identify and renumber network interfaces
   (ネットワーク・インターフェースの識別と番号再設定)
4) Configure keyboard layout (キーボード・レイアウトの設定)
5) Turn machine off (マシンの電源オフ)
6) Reboot the machine (マシンの再起動)
Choice (1-6) :1((1 - 6)から選択:1)
```

2. **1** –Configure CounterACT (CounterACT の設定) を選択します。
   次のプロンプトが表示されます。

   Continue:(続けますか:) (yes/no)?((はい/いいえ)?)

   Enter を押してセットアップを開始します。

3. **High Availability Mode** (高可用性モード) メニューが開きます。**Enter**を押して標準インストールを選択します。

4. **CounterACT Initial Setup** (CounterACT 初期セットアップ) プロンプトが表示されます。**Enter** を押して続行します。

5. **Select CounterACT Installation Type** (CounterACT インストールのタイプを選択) メニューが開きます。1を入力し、**Enter** を押して標準CounterACT アプライアンスをインストールします。セットアップが開始されます。これには少し時間がかかる場合があります。

6. プロンプトの **Enter Machine Description**（マシンの説明を入力してください）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** を押します。以下が表示されます。

```
>>>>>> Set Administrator Password （管理者パスワードの設定） <<<<<<
This password is used to log in as 'root' to the machine Operating System and as 'admin' to the CounterACT Console.（このパスワードは、マシンのオペレーティング・システムに「root」として、また、CounterACT コンソールに「admin」としてログインするために使用します。）
The password should be between 6 and 15 characters long and should contain at least one non-alphabetic character.（パスワードの長さは6〜15文字とし、アルファベット以外の文字を少なくとも1文字使用してください。）
Administrator password : （管理者パスワード:）
```

7. **Set Administrator Password**（管理者パスワードの設定）プロンプトで、使用するパスワードとなる文字列を入力し（文字列は画面に表示されません）、**Enter** を押します。パスワード確認のためのプロンプトが表示されます。パスワードは 6 -15文字の長さとし、少なくともアルファベット以外の文字を1文字使用することが必要です。
   アプライアンスには *root* として、コンソールには *admin* としてログインします。
8. **Set Host Name**（ホスト名設定）プロンプトで、ホスト名を入力し、**Enter** を押します。ホスト名はコンソールにログインする際に使用でき、コンソールに表示されて、表示している CounterACT アプライアンスを識別するために役に立ちます。
9. **Configure Network Settings**（ネットワークの設定）画面が表示され、一連の設定パラメーターの入力を要求するプロンプトが表示されます。各プロンプトに対して値を入力し、**Enter** を押して、先に進みます。
   - CounterACT コンポーネントは管理インターフェースを通して通信します。リストされる管理インターフェースの数は、アプライアンスのモデルによって異なります。
   - **Management IP address（管理 IP アドレス）は、**CounterACT コンポーネントがそれを通して通信するインターフェースのアドレスです。CounterACT コンポーネントの間の通信に使用されるインターフェースがタギングされたポートに接続される場合のみ、このインターフェースに 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、各々のアドレスの間をスペースで区切ってください。これにより一番中側の DNS サーバーが外部および内部のアドレスを解決しますが、外部解決用 DNS サーバーを含めることが必要になる場合があります。アプライアンスによって実行されるほぼすべての DNS クエリは、内部アドレスのためですが、外部DNS サーバーが最後にリストされていることが必要です。
10. **Setup Summary**（セットアップ・サマリー）画面が表示されます。全般的接続試験の実施、再設定、または、セットアップ完了のためのプロンプトが表示されます。
    D を入力してセットアップを完了します。

ライセンス

インストール後に、CounterACT 販売店から提供された初期デモ・ライセンスをインストールする必要があります。ライセンスは初期コンソール・セットアップの間にインストールされます。初期デモ・ライセンスは、特定の日数の間有効です。この期間が終了する前に、恒久ライセンスをインストールする必要があります。期限が切れる日付は、電子メールで連絡されます。また、期限が切れる日付とライセンスの状況は、コンソールの [Appliances/Devices（アプライアンス/デバイス）] ペインに表示されます。

恒久ライセンス受領後、ライセンスは ForeScout ライセンス・サーバーにより毎日検証されます。ライセンスの警告や違反は、[Device Details（デバイス詳細）] ペインに表示されます。

1か月間検証できないライセンスは無効となります。ライセンスに関する詳細は、『CounterACT Installation Guide（CounterACT インストール・ガイド）』を参照してください。

ネットワーク接続要件

少なくとも1台の CounterACT デバイス（アプライアンスまたは EnterpriseManager）がインターネットにアクセスできることが必要です。この接続は、CounterACT ライセンスの、ForeScout ライセンス・サーバーによる検証のために使用されます。

1か月間認証できないライセンスは無効となります。CounterACT は警告電子メールを1日1回送信して、サーバーとの通信にエラーがある旨を示します。

5. リモート管理

iDRAC のセットアップ

デル・リモート・アクセス・コントローラー（iDRAC）は、LAN またはインターネット経由で、CounterACT アプライアンス/Enterprise Manager への、場所や 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。このモジュールを使用して、KVM へのアクセス、電源オン/オフ/リセット、トラブルシューティングの実行、および、メンテナンス作業が実施できます。

iDRAC モジュールを使用するには、以下の作業を実行します。

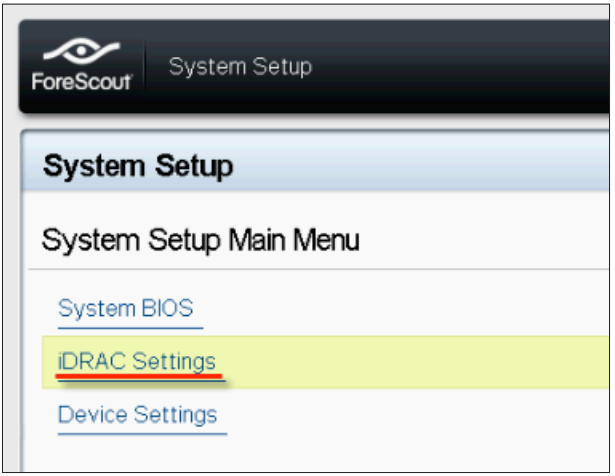
- *iDRAC モジュールの有効化と設定*
- *モジュールのネットワークへの接続*
- *iDRAC へのログイン*

iDRAC モジュールの有効化と設定

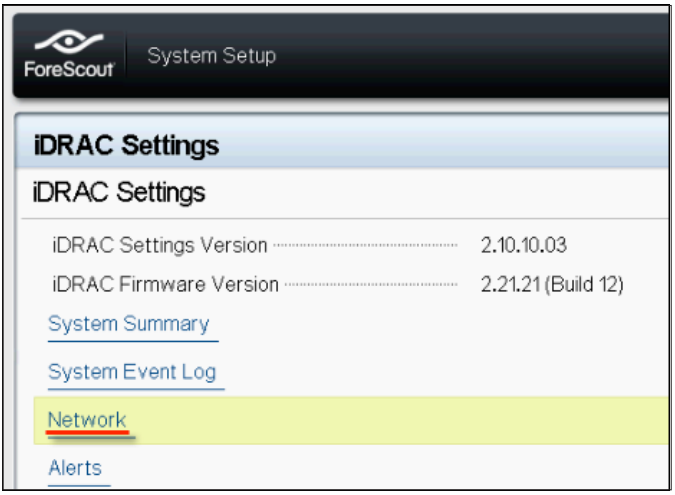
iDRACの設定を変更して、CounterACT デバイスへのリモート・アクセスを可能にします。このセクションは、CounterACT との使用に必要な基本統合設定を説明します。

iDRAC を設定する方法

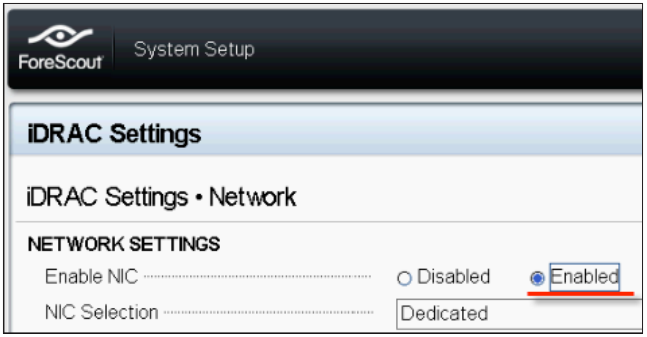
1. 管理するシステムの電源をオンにします。
2. 起動時の自己診断テスト（POST）中に「F2」キーを押します。
3. [System Setup Main Menu（システム設定メイン・メニュー）] ページで、**[iDRAC Settings（iDRAC 設定）]** を選択します。



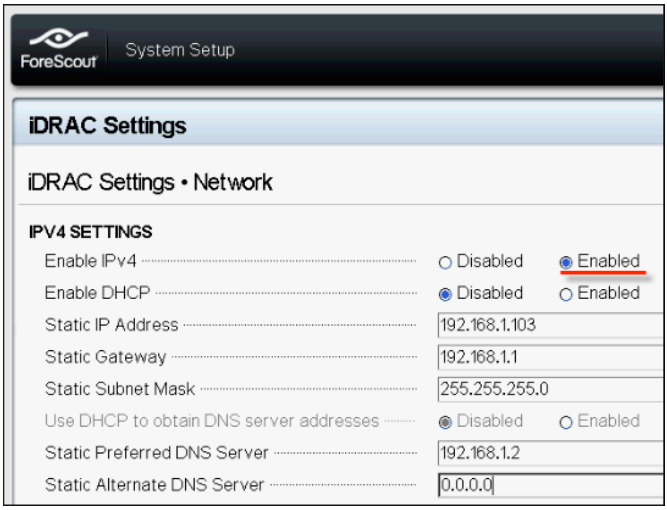
4. ［iDRAC Settings（iDRAC 設定）］ページで **［Network（ネットワーク）］**を選択します。



5. ネットワークを以下の通り設定します。
   - ***Network Settings*（ネットワーク設定）。［Enable NIC（NIC 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。



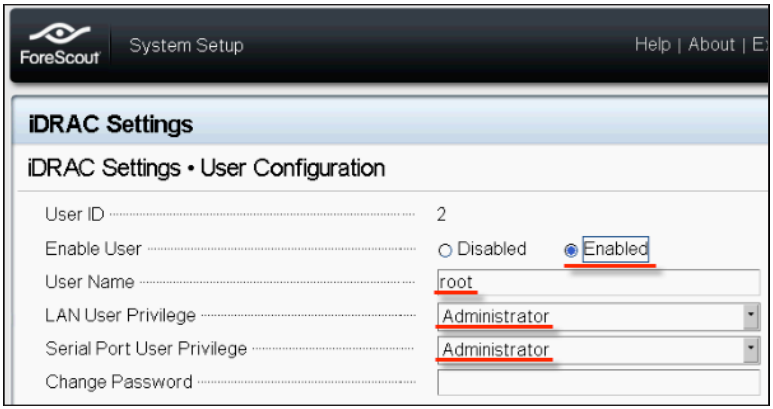
   - ***Common Settings*（共通設定）。［DNS DRAC Name（DNS DRAC 名）］**フィールドで、動的 **DNS** を更新できます（任意）。
   - ***IPV4 Settings*（*IPv4* 設定）**。［**Enable IPv4（IPv4 有効化）**］フィールドが［**Enabled（有効）**］に設定されていることを確認します。［**Enable DHCP（DHCP 有効化）**］フィールドを［**Enabled（有効）**］に設定して、動的 **IP** アドレス設定を使用するか、［**Disabled（無効）**］に設定して静的 **IP** アドレス設定を使用します。有効にすると、DHCP により IP アドレス、ゲートウェイ、および、サブネット・マスクが、自動的に **iDRAC7** に割り当てられます。無効にする場合には、［**Static IP Address（静的 IP アドレス）**］、［**Static Gateway（静的ゲートウェイ）**］および［**Static SubnetMask（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. 次の [User Configuration（ユーザー設定）] フィールドを設定します。
   - **[*Enable User*（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。
   - **[*User Name*（ユーザー名）]**。ユーザー名を入力します。
   - **[*LAN User Privilege*（*LAN* ユーザー権限）]** および **[*Serial Port User Privilege*（シリアル・ポート・ユーザー権限）]**。管理者の権限レベルを設定します。
   - **[Change Password（パスワード変更）]**。ユーザーのログイン用パスワードを設定します。



9. **[Back（戻る）]** を選択し、次に **[Finish（終了）]** を選択します。変更された設定を確認します。ネットワーク設定が保存され、システムが再起動します。

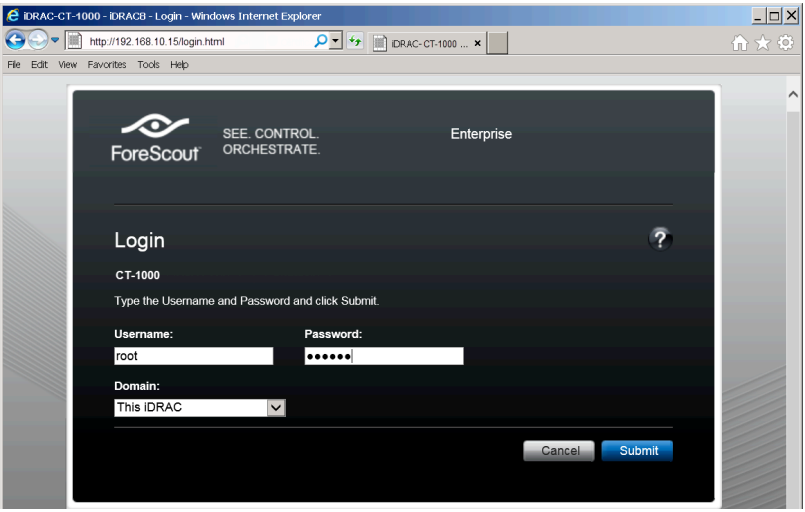
モジュールのネットワークへの接続

iDRAC はイーサネット・ネットワークに接続されます。これは通常、管理ネットワークに接続されます。次の画像は、CT-1000 アプライアンスの背面パネルの、iDRAC ポート位置を示します。

iDRAC のログイン

iDRAC にログインする方法

1. **[iDRAC Settings（iDRAC 設定）] > [Network（ネットワーク）]** を選択して、設定した **IP** アドレスまたはドメイン名を参照します。



2. iDRAC システム・セットアップの［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 に関する詳細は、iDRAC ユーザーズガイドを参照してください。

デフォルトのログイン情報は必ず更新してください。

6. 接続の検証

管理インターフェース接続の検証

管理インターフェース接続のテストを行うために、アプライアンスにログインして、次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 （管理インターフェースのステータス）
Pinging default gateway information （デフォルト・ゲートウェイ情報の ping）
Ping statistics （ping の統計）
Performing Name Resolution Test （名前解決テストの実行）
Test summary （テスト・サマリー）
```

スイッチ/アプライアンス間接続の検証

データ・センターでの作業を終了する前に、スイッチがアプライアンスに正しく接続されていることを検証します。これを行うために、fstool ifcount コマンドを、アプライアンスから、検出された各のインターフェースに対して実行します。

```
fstool ifcount eth0 eth1 eth2
```

（各インターフェースをスペースで区切ります。）

ツールは、指定されたインターフェース上のネットワーク・トラフィックを連続して表示します。インターフェースごと、または VLAN ごとの2つのモードで実行されます。このモードは表示から変更できます。次の各トラフィック・カテゴリーの、秒あたりの合計ビットとパーセンテージが表示されます。

- 監視インターフェースは、主にミラーリングされたトラフィックを調べます—90%以上。
- レスポンス・インターフェースは、主にブロードキャスト・トラフィックを調べます。
- 監視インターフェースおよびレスポンス・インターフェースは、どちらも、予想される VLAN を調べます。

コマンド・オプション

v – VLAN モードで表示
I – インターフェース・モードで表示
P – 前を表示
N – 次を表示
q – 表示を終了

VLAN モード:

```
update=[4]      [eth3: 14 vlans]
Interface/Vlan  Total   Broadcast  Mirrored  *To my MAC  *From my MAC
eth3.untagged   4Mbps   0.2%       99.8%     0.0%        0.0%
eth3.1          9Mbps   0.0%       100.0%    0.0%        0.0%
eth3.2          3Mbps   0.1%       99.9%     0.0%        0.0%
eth3.4          542bps  100.0%     0.0%      0.0%        0.0%
eth3.20         1Kbps   100.0%     0.0%      0.0%        0.0%
Show [v]lans [i]nterfaces <-[p]rev [n]ext->     [q]uit
```

インターフェース・モード

```
update=[31]     [eth0: 32 vlans] [eth1: 1 vlans]
Interface       Total   Broadcast  Mirrored  *To my MAC  *From my MAC
eth0            3Kbps   42.3%      0.0%      14.1%       43.7%
eth1            475bps  0.0%       100.0%    0.0%        0.0%
```

*To my MAC — 宛先のMAC はアプライアンスの MAC。

*From my MAC — このアプライアンスにより送信されるトラフィック（発信元 MAC はアプライアンスの MAC。宛先にはブロードキャストまたはユニキャストが可能）

トラフィックが何も見えない場合は、インターフェースが稼動していることを確認してください。アプライアンスで次のコマンドを使用します。

`ifconfig [interface name] up`

Ping テストの実施

アプライアンスからネットワーク・デスクトップ宛てに ping テストを実行して、接続を確認します。

テストを実行する方法

1. アプライアンスにログインします。
2. 次のコマンドを実行します。**`Ping [network desktop IP]`**
   デフォルトでは、アプライアンス自体は ping には応答しません。

7. CounterACT コンソールの設定

CounterACT コンソールのインストール

CounterACT コンソールは、アプライアンスによって検出されたアクティビティを表示、追跡、分析する、中心的な管理アプリケーションです。NAC、脅威防御、ファイアウォール、および、その他のポリシーを、コンソールから定義できます。詳細は『CounterACT Console User Manual（CounterACT コンソール・ユーザー・マニュアル）』を参照してください。

CounterACT Consoleアプリケーションソフトウェアをホストするには、マシンが必要です。最小ハードウェア要件は以下の通りです。

- 非専用マシンの場合は以下を実行できるもの
  - Windows XP、Windows VistaまたはWindows 7
  - Windows Server 2003またはServer 2008
  - Linux
- Pentium 3,1 GHz
- メモリ 2 GB
- ディスクの空き領域 1 GB

コンソールのインストール実行には、次の2つの方法があります。

アプライアンスに内蔵されたインストール・ソフトウェアを使用。

1. コンソール・コンピューターからブラウザー・ウィンドウを開きます。
2. ブラウザーのアドレス行に次のアドレスを入力します。
   `http://<Appliance ip>/install`
   この際の`<Appliance ip>` はこのアプライアンスの `IP` アドレスです。
   ブラウザーがコンソールのインストール・ウィンドウを表示します。
3. 画面上の指示に従います。

CounterACT CD-ROM からインストール

1. CounterACT CD-ROM を DVD ドライブに挿入します。
2. **`ManagementSetup.htm`** ファイルを、ブラウザーを使用して CD-ROMから開きます。
3. 画面上の指示に従います。

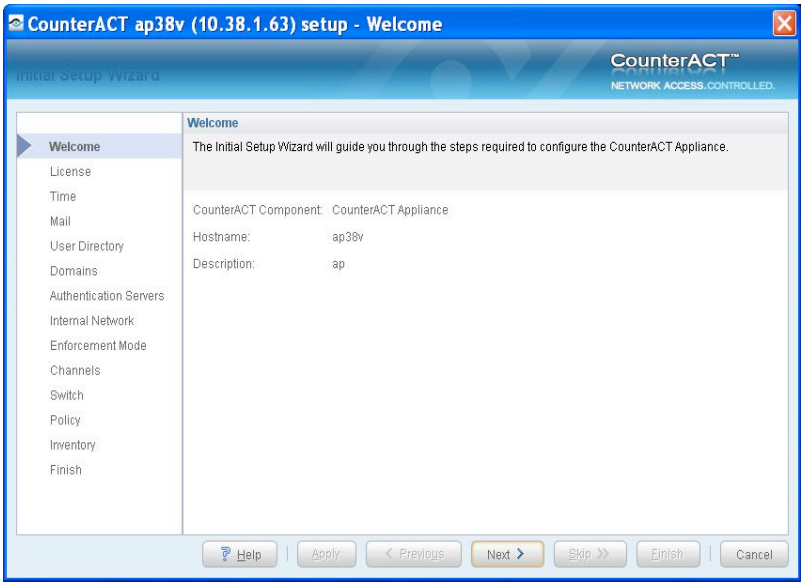
ログイン

インストールが完了したら、CounterACT コンソールにログインできます。

1. 作成したショートカット位置から、CounterACT アイコンを選択します。
2. アプライアンスの IP アドレスまたはホスト名を、**[IP/Name (IP/名前)]** フィールドに入力します。
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。

初期セットアップの実行

初めてログインすると、Initial Setup Wizard（初期セットアップ・ウィザード）が表示されます。ウィザードにより、CounterACT を起動するための重要な設定ステップがガイドされ、素早く効率的に稼働することができます。



初期セットアップを始める前に

ウィザードを実行する前に、以下の情報を用意します。

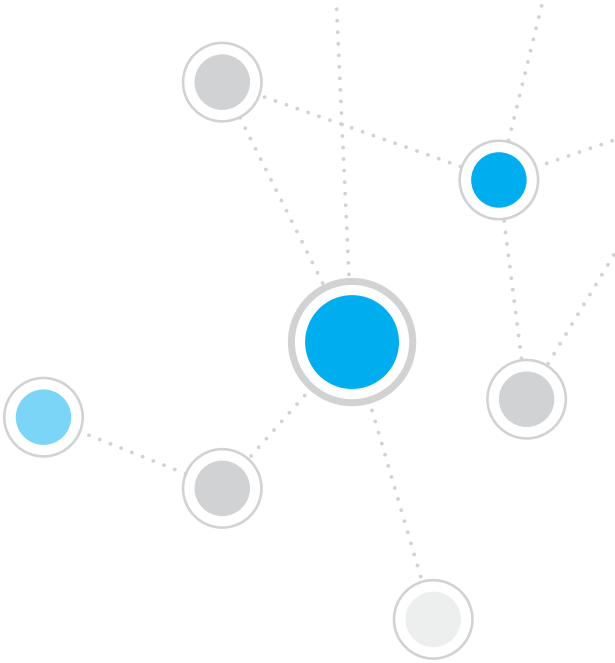
情報	値
□ 組織で使用する NTP サーバーのアドレス（オプション）。	
□ 内部メール中継 IP アドレス。アプライアンスからの SMTP トラフィックが許可されていない場合に、CounterACTからの電子メールの配信を可能にします（オプション）。	
□ CounterACT 管理者の電子メール・アドレス。	
□ データ・センターで定義された、監視・インターフェースおよびレスポンス・インターフェースの割り当て。	
□ DHCP のないセグメントまたは VLANには、監視インターフェースが直接接続されるネットワーク・セグメントまたは VLAN、および、このような各 VLAN で CounterACT により使用される固定 IP アドレス。この情報は、Enterprise Manager セットアップには必要ありません。	
□ アプライアンスが保護する IP アドレスの範囲（未使用アドレスを含むすべての内部アドレス）。	
□ ユーザー・ディレクトリー・アカウント情報、および、ユーザー・ディレクトリー・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、ドメイン資格情報。	
□ 認証サーバー。CounterACT でどのネットワーク・ホストが正常に認証されたかを分析するため。	
□ コア・スイッチの IP アドレス、ベンダー、および SNMP パラメーター。	

ウィザード使用に関する詳細は、『*CounterACT Console User Manual*（*CounterACT* コンソール・ユーザー・マニュアル）』、または、オンライン・ヘルプを参照してください。

連絡先情報

ForeScout のテクニカル・サポートに関しては、support@forescout.com 宛てに電子メールで、または、以下の電話番号までお問い合わせください。

- フリーダイヤル（米国）: 1 866 377-8771
- 米国外からの電話: 1 408 213-3191
- サポート: 1 708 237-6591
- Fax: 1 408 371-2284



ForeScout

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

フリー・ダイアル（米国） 1 866 377-8771
米国外からの電話 1 408 213-3191
サポート 1 708 237-6591
Fax 1 408 371-2284

400-00020-01