構成管理

この章では、初期設定後の Threat Grid アプライアンスの設定に関する追加情報について説明します。説明する項目は次のとおりです。

はじめに

Threat Grid アプライアンスの初期設定は、アプライアンスのセットアップ時に、『*Cisco Threat Grid Appliance Setup And Configuration Guide*』の説明に従って、TGSH ダイアログと OpAdmin ポータルを使用して実行します。

（注） Threat Grid 組織およびユーザアカウントは、Threat Grid Portal UI で管理します（ナビゲーションバーのログイン名の横にあるドロップダウン矢印から選択）。

TGSH ダイアログを使用したネットワーク設定

初期ネットワーク設定は、TGSH ダイアログを使用して実行します（『*Cisco Threat Grid Appliance Setup and Configuration Guide*』を参照）。このセクションでは、TGSH ダイアログの使用に関する追加情報について説明します。

TGSH ダイアログを使用したネットワークの設定

ネットワークの初期設定を変更する場合は、次の手順を実行します。

（注） DHCP を使用して IP を取得する場合は、「ネットワーク設定と DHCP」を参照してください。

ステップ 1 TGSH ダイアログにログインします。

（注） 認証が [**LDAP Only**] に設定されている場合、TGSH ダイアログにログインするには LDAP を使用する必要があります。認証モードが [**System Password or LDAP**] に設定されている場合、TGSH ダイアログのログインで許可されるのは**システム**ログインのみです。

ステップ 2 TGSH ダイアログのインターフェイスで、[CONFIG_NETWORK] を選択します。

[**Network Configuration**] コンソールが開き、現在のネットワーク設定が表示されます。

ステップ 3 必要な変更を行います（新しいエントリを入力する前に、バックスペースを押して古いエントリを削除する必要があります）。

ステップ 4 ダーティ ネットワークの [DNS Name] を空白のままにします。

ステップ 5 ネットワーク設定の更新が完了したら、Tab キーで下に移動し、[**Validate**] を選択してエントリを確認します。

エラーが発生した場合は、無効な値を修正し、もう一度 [**Validate**] を選択します。

検証が完了すると、[**Network Configuration**] ページに入力した値が表示されます。

ステップ 6 [Apply] を選択して各種設定を適用します。

行われた設定変更に関する詳細情報が表示されます。

ステップ 7 [OK] を選択します。

[**Network Configuration**] コンソールが再更新され、IP アドレスが表示されます。これで、ネットワークの設定は完了しました。

TGSH ダイアログへの再接続

TGSH ダイアログはコンソール上で開いたままになり、アプライアンスにモニタを接続するか、（CIMC が設定されている場合は）リモート KVM を使用することでアクセスできます。

TGSH ダイアログに再接続するには、ユーザ「**threatgrid**」として管理 IP アドレスに SSH 接続します。必要なパスワードは、ランダムに生成される初期パスワードであり、最初に TGSH ダイアログに表示されたパスワードか、OpAdmin 設定の最初の手順で作成した新しい管理者パス

ワードです（『*Cisco Threat Grid Appliance Setup and Configuration Guide*』を参照してください）。

リカバリモードでのネットワークの設定

リカバリモードでのネットワークの設定は、システム全体に反映されます（バージョン2.7 以降）。

- すべてのインターフェイスが起動します。
- ファイアウォールルールとポリシールーティングにより、どのプロセスがどのインターフェイスで通信するかが制限されます。

（注） ポート 19791 のサポートモードトラフィックは、3 つのインターフェイスすべての許可リストに含まれています。

リカバリモードでネットワーキングを設定するには、次の手順を実行します。

ステップ 1 Threat Grid アプライアンスを再起動してから、起動メニューで **[Recovery Mode]** を選択します。

ステップ 2 システムが起動したら、**Enter** キーを数回押して clean コマンド プロンプトを表示させます。

ステップ 3 「**netctl clean**」と入力し、次の情報を入力します。

- **[Configuration type]**：static
- **[IP Address]**：<クリーン IP アドレス>/<ネットマスク>
- **[Gateway Address]**：<クリーン ネットワーク ゲートウェイ>
- **[Routes]**：<空白>
- **[Final Question]**：「**y**」と入力

ステップ 4 **Exit** と入力して設定を適用します。

アプライアンスは、ポート 19791/tcp のクリーンインターフェイスでアウトバウンドサポート接続を開こうとします。

OpAdmin ポータルを使用した設定

初期設定および設定ウィザードについては、『Cisco Threat Grid Appliance Setup and Configuration Guide』を参照してください。新しい Threat Grid アプライアンスでは、管理者が付加的な設定を実行する必要があります。また OpAdmin の設定には、時間の経過とともに更新が必要になる場合があります。

OpAdmin ポータルは、Threat Grid アプライアンス管理者の主要な設定インターフェイスです。Threat Grid アプライアンスの管理インターフェイスで IP アドレスが設定された後に使用できる Web ポータルです。

OpAdmin ポータルは、次のような各種の Threat Grid アプライアンスの設定を決定し管理するために使用されます。

- 管理者のパスワード（OpAdmin および **threatgrid** ユーザの場合）
- Threat Grid ライセンス
- レート制限
- SMTP
- SSH
- SSL 証明書
- DNS サーバ（AMP for Endpoints プライベート クラウド統合用の DNS 設定を含む）
- NTP サーバ
- サーバ通知
- syslog メッセージおよび Threat Grid 通知のリモート サーバの設定
- CA 証明書管理（AMP for Endpoints プライベート クラウド統合用）
- LDAP 認証
- サードパーティ検出およびエンリッチメントサービス（ClamAV、OpenDNS、Titanium Cloud、VirusTotal など）

（注）

- 設定時に IP アドレスが遮断される可能性を減らすために、OpAdmin での設定の更新は 1 回のセッションで完了する必要があります。
- OpAdmin はゲートウェイエントリを検証しません。誤ったゲートウェイを入力して保存すると、OpAdmin インターフェイスにアクセスできなくなります。ネットワーク設定を管理インターフェイスで実行した場合は、コンソールを使用してネットワーク設定を修正する必要があります。管理インターフェイスがまだ有効であれば、OpAdmin で修正して再起動することによって問題を解決できます。
- Threat Grid アプライアンス（v2.7 以降）は、ホスト名としてシリアル番号を使用することにより、一部の NFS v4 サーバとの相互運用性を向上させます。

重要 OpAdmin は HTTPS を使用するため、ブラウザのアドレスバーに HTTPS を入力する必要があります。管理 IP をポイントするだけでは十分ではありません。ブラウザに次のアドレスを入力します。

https://adminIP/

または

https://adminHostname/

SSH キーの設定

SSH キーを設定すると、Threat Grid アプライアンス管理者は、SSH を使用して TGSH ダイアログ（`threatgrid@<host>`）にアクセスできるようになります。

ルートアクセスやコマンドシェルは提供されません。**[Configuration] > [SSH]**で複数のキーを追加できます。

Threat Grid アプライアンスにアクセスするための SSH 公開キーを設定すると、SSH を使用したパスワードベースの認証が無効になります（v2.7.2 以降）。そのため、2 つの SSH 認証方式は、両方ではなくどちらか一方のみが有効になります。キーベース認証を使用して SSH 接続が成功すると、TGSH ダイアログで、両方のトークンが必要なパスワードの入力を求められます。

通知用のリモート Syslog サーバの設定

電子メールでシステム通知を配信するように設定できる定期的な通知に加えて（OpAdmin の [**Configuration**] > [**Notifications**]）、syslog メッセージと Threat Grid 通知を受信するようにリモート syslog サーバを設定できます。

ステップ 1 OpAdmin ポータルにログインし、**[Configuration] > [Syslog]** をクリックします。

ステップ 2 **サーバ DNS**を入力した後、ドロップダウンリストからプロトコルを選択します（デフォルトの [TCP]、または [UDP] を選択できます）。

ステップ 3 設定を保存した後に DNS ルックアップを実行するには、[**Verification**] チェックボックスをオンにします。

ホストがその名前を解決できない場合は、エラーが出力され、（有効なホスト名を入力するまで）ホスト名は保存されません。[**Verification**] チェックボックスをオンにしなかった場合、アプライアンスは、DNS で有効な名前かどうかにかかわらず、任意の名前を受け入れます。

ステップ 4 [Save] をクリックします。

Syslog DNS を編集または削除するには、**[Configuration] > [Syslog]** を開き、変更を加えてから、[**Save**] をクリックします。

LDAP 認証の設定

Threat Grid アプライアンスは、OpAdmin ログインと TGSH ダイアログログインのための LDAP による認証と許可をサポートしています。

ドメインコントローラまたは LDAP サーバで管理されるさまざまなログイン情報を使用して、複数のアプライアンス管理者を認証できます。認証モードは、[System Password Only]、[System Password or LDAP]、[LDAP Only] のいずれかです。

3 つの LDAP プロトコル オプション、[LDAP]、[LDAPS]、[LDAP with STARTLS] があります。

次の点を考慮する必要があります。

- デュアル認証モード（**システムパスワードまたは LDAP**）は、LDAP の設定時に、Threat Grid アプライアンスから誤ってロックアウトされないようにするために必要です。

  最初から [**LDAP Only**] を選択することはできません。まずデュアルモードを実行して、動作することを確認する必要があります。初期設定後に OpAdmin からログアウトした後、LDAP ログイン情報を使用して再度ログインして [**LDAP Only**] に切り替える必要があります。

- 認証を [**LDAP Only**] に設定した場合、TGSH ダイアログにログインするには LDAP を使用する必要があります。認証モードが [**System Password or LDAP**] に設定されている場合、TGSH ダイアログのログインで許可されるのはシステムログインのみです。

- Threat Grid アプライアンスが LDAP 認証のみ（[**LDAP Only**]）に設定されている場合は、リカバリモードでパスワードをリセットして、認証モードを再設定し、システムパスワードによるログインを許可することもできます。

- メンバーシップを制限するための認証フィルタが設定されていることを確認します。

- TGSH ダイアログと OpAdmin ポータルでは、[**LDAP Only**] モードの場合にのみ LDAP ログイン情報が必要です。[**LDAP Only**] に設定されている場合、TGSH ダイアログでは、システムパスワードではなく、LDAP ユーザ/パスワードの入力のみが求められます。

- 認証が [**System Password or LDAP**] に設定されている場合、TGSH ダイアログでは、これら両方ではなく、システムパスワードのみを入力するように求められます。

- LDAP の問題をトラブルシューティングするには、リカバリモードでパスワードをリセットして LDAP を無効にします。

- SSH を使用して TGSH ダイアログにアクセスするには、[**LDAP Only**] モードの場合、LDAP ログイン情報に加えて、システムパスワードまたは設定済みの SSH キーが必要です。

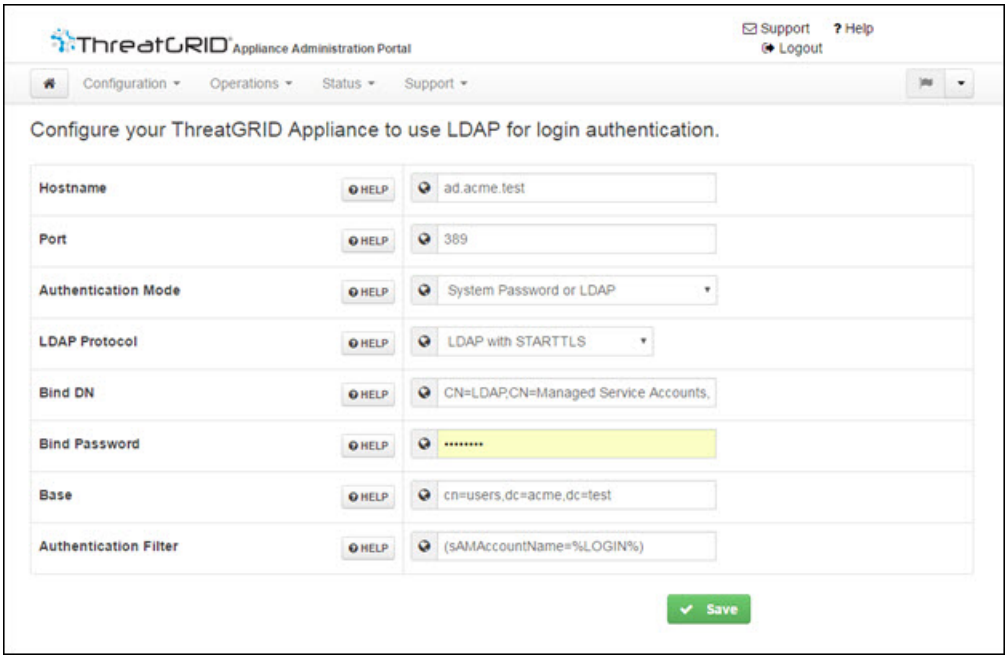
- LDAP はクリーン インターフェイスからの発信です。

OpAdmin での LDAP 認証の設定

OpAdmin ポータルで LDAP 認証を設定するには、次の手順を実行します。

ステップ 1 OpAdmin ポータルにログインし、**[Configuration] > [LDAP]** を選択して [LDAP Configuration] ページを開きます。

図 *1 : LDAP* 認証の設定



ステップ 2 ページのフィールドに入力します。各フィールドの横にある [**Help**] アイコンをクリックすると、詳細な説明と情報を表示できます。

（注） LDAP 認証を最初に設定するときは、[**System Password** or **LDAP**] を選択し、OpAdmin からログアウトしてから、LDAP ログイン情報を使用して再度ログインする必要があります。その後、[**LDAP Only**] を実装するように設定を変更できます。

ステップ 3 [Save] をクリックします。

ユーザが OpAdmin または TGSH ダイアログにログインすると、次のいずれかの画面が表示されます。

図 *2 : [LDAP Only]*

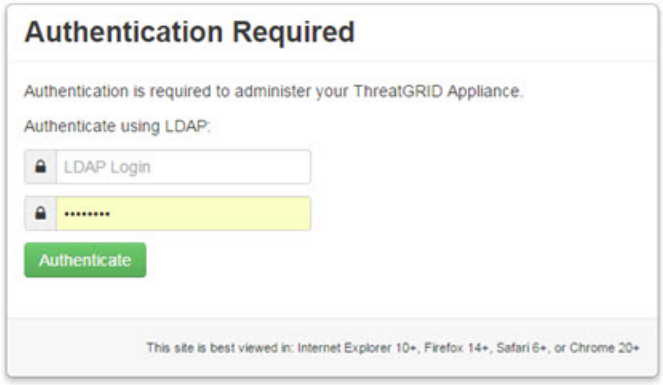
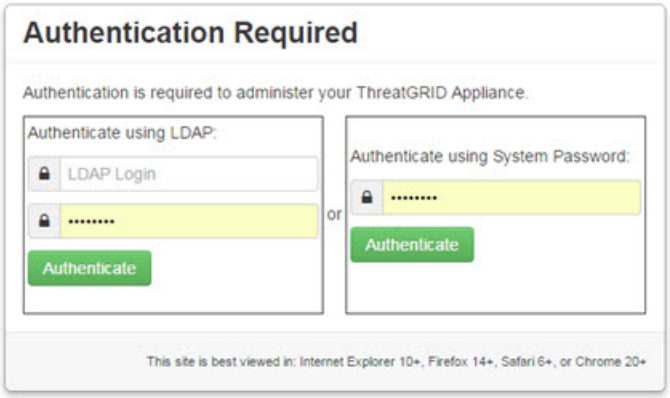


図 *3 : [System Password or LDAP]*



サードパーティ検出およびエンリッチメントサービスの設定

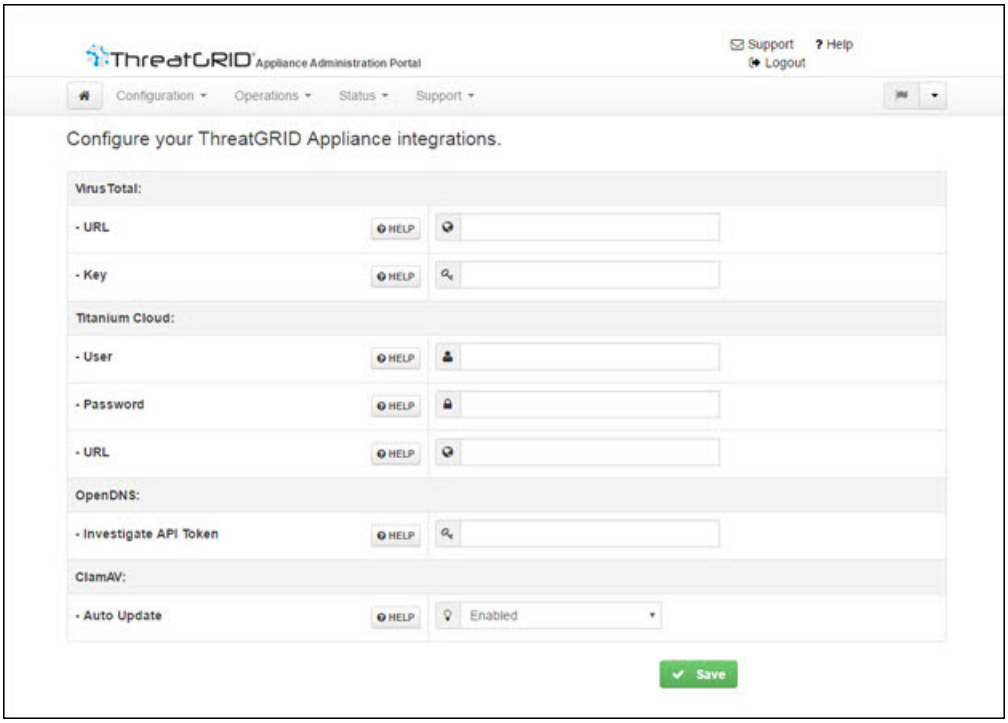
OpenDNS、TitaniumCloud、VirusTotal といった複数のサードパーティ検出およびエンリッチメントサービスとの統合を、[**Integration**] ページを使用してアプライアンスで設定できます（v2.2 以降）。

クラウド検索フェデレーション機能（v2.8 以降で使用可能）により、クラウドエンドポイントが（管理インターフェイスの [**Integrations**] ページで）設定されている場合、Threat Grid クラウドインスタンスに対して検索クエリを再実行する、ポータルアプリケーション UI のオプションが使用可能になります。

（注） OpenDNS が設定されていない場合、分析レポートの [Domains] エンティティページに **whois** 情報（UI のマスクバージョン）は表示されません。

ステップ 1 OpAdmin ポータルにログインし、**[Configuration] > [Integrations]** をクリックして [**Integrations**] ページを開きます。

図 *4* : 統合の設定



ステップ 2 必要な認証情報などの値を入力します。

（注） ClamAV シグネチャは、毎日自動的に更新できます。この署名はデフォルトで有効になっており、[**ClaimAV**] フィールドで無効にすることができます。

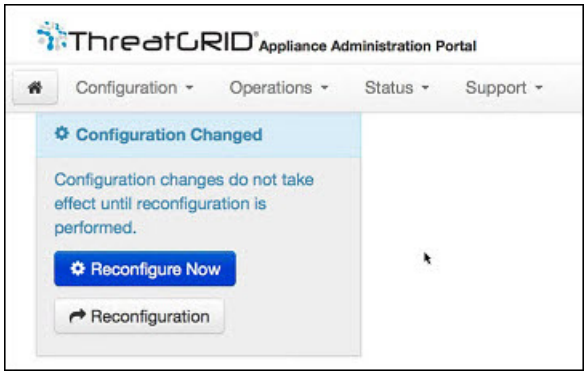
ステップ 3 **[Save]** をクリックします。

設定変更の適用

設定が変更されると、[**Configuration**] メニューの下にライトブルーの [**Configuration Changed**] アラートが表示されます。OpAdmin の設定を更新した場合、新しい設定を別の手順で保存する必要があります。

ステップ 1 [**Configuration Changed**] をクリックして、ダイアログを開きます。

図 *5:* 設定変更ダイアログ



ステップ 2 [**Reconfigure Now**] をクリックして、変更をアプライアンスに適用します。

DHCP の使用

ほとんどの Threat Grid アプライアンスユーザは、DHCP で設定されたネットワークを使用しません。ただし、DHCP を使用するように設定されたネットワークに接続している場合は、このセクションを読み、要件を理解することが重要です。

（注） アプライアンスの初期ネットワーク設定で DHCP を使用したものの、静的 IP アドレスに切り替える必要が生じた場合は、「ネットワーク設定と DHCP」を参照してください。

TGSH ダイアログには、OpAdmin ポータルインターフェイスにアクセスして設定するために必要な情報が表示されます。アプライアンスの起動後、DHCP の IP アドレスが表示されるまでに時間がかかる場合があります。

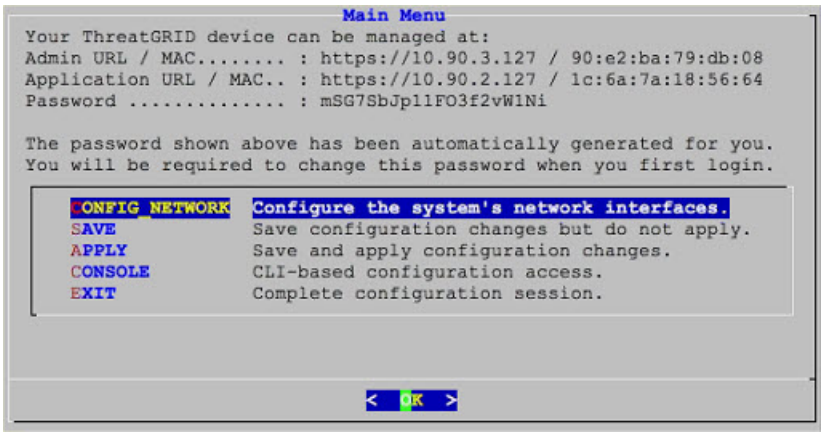
DHCP の明示的 DNS

DHCP を使用する Threat Grid アプライアンスでは、DNS を明示的に指定する必要があります。

警告 DNS サーバが明示的に指定されていないシステムのアップグレードは失敗します。

TGSH ダイアログを開き、次の情報を確認します。

図 *6 : TGSH* ダイアログ（*DHCP* を使用するように設定されたネットワークに接続済み）



- [**Admin URL**]：管理ネットワーク。OpAdmin の残りの設定作業を継続するためにこのアドレスが必要です。
- [**Application URL**]：クリーンネットワーク。OpAdmin を使用して設定を完了した後に、Threat Grid アプリケーションにアクセスするために使用するアドレスです。

  ダーティ ネットワークは表示されません。
- [**Password**]：Threat Grid アプライアンスのインストール時にランダムに生成される初期管理パスワード。後で、OpAdmin 設定プロセスの最初の手順として、このパスワードを変更する必要があります。

DHCP を永続的に使用する場合、管理 IP アドレスを静的に変更する必要がない限り、追加のネットワーク設定は必要ありません。

ネットワーク設定と DHCP

初期設定に DHCP を使用した後、3 つのネットワークすべてに関して、IP 割り当てを DHCP から固定的な静的 IP アドレスに調整する必要がある場合は、次の手順を実行します。

（注） OpAdmin はゲートウェイエントリを検証しません。誤ったゲートウェイを入力して保存すると、OpAdmin インターフェイスにアクセスできなくなります。ネットワーク設定を管理インターフェイスで実行した場合は、コンソールを使用してネットワーク設定を修正する必要があります。管理インターフェイスがまだ有効であれば、OpAdmin で修正して再起動することによって問題を解決できます。

ステップ 1 OpAdmin ポータルで、ナビゲーションウィンドウの [**Network**] をクリックします（[License] ウィンドウで **[Configuration] > [Network]** がオンになっていても、DHCP ネットワーク設定は完了していません）。

[**Network**] ページが開きます。

ステップ 2 次のフィールドに入力します。

（注） 管理ネットワークの設定は、最初の Threat Grid アプライアンスのセットアップおよび設定時に **TGSH ダイアログ**を使用して設定されています。

- [**IP Assignment**]：クリーンとダーティ両方のネットワーク インターフェイスのドロップダウンリストから [**Static**] を選択します。
- [**IP Address**]：クリーンまたはダーティ ネットワーク インターフェイスの静的 IP アドレスを入力します。
- [**Subnet Mask**]：ネットワーク インターフェイスのタイプに応じて入力されます。
- [**Validate DNA Name**]：クリーン ネットワーク インターフェイスの場合、[**Validate DNA Name**] チェックボックスをオンにして、DNS が IP アドレスに解決されていることを確認します。
- [**Primary and Secondary DNS**]：プライマリおよびセカンダリ DNS サーバの情報を入力します。

ステップ 3 [**Next（Applies Configuration**）] をクリックして、ネットワーク構成の設定を保存します。

（注） 電子メール設定は [**Email**] ページから管理され、NTP サーバは [**Date and Time**] ページで管理されます。

ステップ 4 [**Configuration Changed**] をクリックし [**Reconfigure Now**] を選択して、DHCP 設定を適用します。