Management Center Virtual 初期設定

この章では、Management Center Virtual アプライアンスの導入後に実行する必要がある初期セットアッププロセスについて説明します。

Management CenterCLI（バージョン 6.5 以降）を使用した初期セットアップ

Management Center Virtual を展開した後、初期セットアップのためにアプライアンスコンソールにアクセスできます。Web インターフェイスを使用する代わりに、CLI を使用して初期設定を実行できます。初期構成ウィザードを完了させ、信頼できる管理ネットワークで通信するように新しいアプライアンスを設定する必要があります。ウィザードでは、エンドユーザーライセンス契約（EULA）に同意し、管理者パスワードを変更する必要があります。

始める前に

- Management Center Virtual が管理ネットワーク上で通信するために必要な次の情報があることを確認してください。
  - IPv4 管理 IP アドレス

    Management Center インターフェイスは、DHCP によって割り当てられた IPv4 アドレスを受け入れるように事前設定されています。DHCP が Management Center MAC アドレスに割り当てるように設定されている IP アドレスを確認するには、システム管理者に問い合わせてください。DHCP が使用できないシナリオでは、Management Center インターフェイスは IPv4 アドレス 192.168.45.45 を使用します。
  - ネットワークマスクとデフォルトゲートウェイ（DHCP を使用しない場合）。

ステップ 1 **admin** アカウントのユーザー名に **admin** を、パスワードに **Admin123** を使用して、コンソールで Management Center Virtual にログインします。パスワードでは、大文字と小文字が区別されることに注意してください。

ステップ 2 プロンプトが表示されたら、Enter を押してエンドユーザーライセンス契約（EULA）を表示します。

ステップ 3 EULA を確認します。プロンプトが表示されたら、**yes**、**YES** を入力するか、Enter を押して EULA に同意します。

重要 EULA に同意せずに続行することはできません。**yes**、**YES**、または Enter 以外で応答すると、ログアウトされます。

ステップ 4 システムのセキュリティやプライバシーを確保するために、Management Center に初めてログインするときは、**admin** のパスワードを変更する必要があります。新しいパスワードの入力を求めるプロンプトが表示されたら、表示された制限に従って新しいパスワードを入力し、確認のプロンプトが表示されたら同じパスワードを再度入力します。

（注） Management Center では、パスワードをパスワード クラッキング ディクショナリと照合して、英語の辞書に載っている多くの単語だけでなく、一般的なパスワードハッキング技術で簡単に解読できるその他の文字列についてもチェックします。たとえば、「abcdefg」や「passw0rd」などのパスワードは初期設定スクリプトによって拒否される場合があります。

（注） 初期設定プロセスの完了時に、2 つの **admin** アカウント（Web アクセス用と CLI アクセス用）のパスワードは同じ値に設定されます。これは、ご使用のバージョンの『Cisco Secure Firewall Management Center アドミニストレーション ガイド』に記載されている強力なパスワードの要件に準拠しています。その後、いずれかの **admin** アカウントのパスワードを変更すると、パスワードは同じではなくなり、Web インターフェイスの **admin** アカウントから強力なパスワード要件を削除できます。

ステップ 5 プロンプトに応答して、ネットワーク設定を行います。

セットアッププロンプトに従う際に、複数の選択肢がある質問では、選択肢が **(y/n)** のように括弧で囲まれて示されます。デフォルト値は、**[y]** のように大カッコ内に列挙されます。プロンプトに応答する場合は、次の点に注意してください。

- Enter を押して、デフォルトを受け入れます。
- ホスト名に関しては、完全修飾ドメイン名（<hostname>.<domain>）またはホスト名を入力します。このフィールドは必須です。
- DHCP を使用する場合は、割り当てられたアドレスが変更されないように、DHCP 予約を使用する必要があります。DHCP アドレスが変更されると、Management Center ネットワーク設定が同期しなくなるため、デバイスの登録は失敗します。DHCP アドレスの変更から回復するには、Management Center に接続し（ホスト名または新しい IP アドレスを使用）、**システム**（⚙）> **[構成（Configuration）]** > [管理インターフェイス（Management Interfaces）] の順に選択してネットワークをリセットします。
- IPv4 を手動で設定することを選択した場合、IPv4 アドレス、ネットマスク、およびデフォルトゲートウェイの入力が求められます。

- DNS サーバーの設定はオプションです。DNS サーバーを指定しない場合は **none** を入力します。それ以外の場合は、1 つまたは 2 つの DNS サーバーに IPv4 アドレスを指定します。2 つのアドレスを指定する場合は、カンマで区切ります。（3 つ以上の DNS サーバーを指定した場合、システムは追加のエントリを無視します）Management Center にインターネットアクセスがない場合は、ローカルネットワークを出て DNS を使用できません。

  （注） 評価ライセンスを使用している場合、この時点での DNS の指定はオプションですが、展開の際に永続ライセンスを使用するには DNS が必要です。

- ネットワークから到達可能な少なくとも 1 つの NTP サーバーの完全修飾ドメイン名または IP アドレスを入力する必要があります。（DHCP を使用していない場合は、NTP サーバーの FQDN を指定できません）2 つのサーバー（プライマリとセカンダリ）を指定できます。情報はカンマで区切ります。（3 つ以上の DNS サーバーを指定した場合、システムは追加のエントリを無視します）Management Center からインターネットにアクセスできない場合は、ローカルネットワークを出て NTP サーバーを使用できません。

例：

```
Enter a hostname or fully qualified domain name for this system [firepower]: fmc
Configure IPv4 via DHCP or manually? (dhcp/manual) [DHCP]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.0.66
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.224
Enter the IPv4 default gateway for the management interface [ ]: 10.10.0.65
Enter a comma-separated list of DNS servers or 'none' [CiscoUmbrella]: 208.67.222.222,208.67.220.220
Enter a comma-separated list of NTP servers [0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org]:
```

ステップ 6 システムによって、設定の選択内容の概要が表示されます。入力した設定を確認してください。

例：

```
Hostname:                           fmc
IPv4 configured via:                manual configuration
Management interface IPv4 address:  10.10.0.66
Management interface IPv4 netmask:  255.255.255.224
Management interface IPv4 gateway:  10.10.0.65
DNS servers:                        208.67.222.222,208.67.220.220
NTP servers:                        0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org
```

ステップ 7 最後のプロンプトで設定を確認することができます。

- 設定が正しい場合は、**y** を入力して **Enter** を押し、設定を承認して続行します。
- 設定が間違っている場合は、 **n** を入力し **Enter** を押します。ホスト名で始まる情報を再入力するように求められます。

例：

```
Are these settings correct? (y/n) y
If your networking information has changed, you will need to reconnect.

Updated network configuration.
```

ステップ 8 設定を承認したら、**exit** と入力して Management Center CLI を終了します。

次のタスク

- 設定したネットワーク情報を使用して Management Center Virtual の Web インターフェイスに接続できます。
- 初期設定プロセスの一環として、Management Center で自動的に設定される週次メンテナンスアクティビティを確認します。このアクティビティは、システムを最新の状態に保ち、データをバックアップする目的で設計されています。バージョン 6.5 以降の自動初期設定の確認 （8 ページ）を参照してください。
- ご使用のバージョンの Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド の説明に従い、Web インターフェイスを使用して初期セットアップを完了した後で、IPv6 アドレッシング用に Management Center を設定できます。

Web インターフェイスを使用したプラットフォームの初期設定（バージョン 6.5 以降）

を展開した後、Management Center Virtualアプライアンスの Web インターフェイスで HTTPS を使用して初期設定を実行できます。

Management Center の Web インターフェイスへの初回ログイン時に、初期設定ウィザードが Management Center に表示され、アプライアンスの基本設定をすばやく簡単に実行できます。このウィザードは、次の 3 つの画面と 1 つのポップアップ ダイアログ ボックスで構成されています。

- 最初の画面では、**admin** ユーザーのパスワードをデフォルト値の **Admin123** から変更するよう求められます。
- 2 番目の画面では、シスコ エンドユーザー ライセンス契約（EULA）が表示されます。アプライアンスを使用するには、この内容に同意する必要があります。
- 3 番目の画面では、アプライアンス管理インターフェイスのネットワーク設定を変更できます。このページには現在の設定があらかじめ入力されており、必要に応じて変更できます。
- この画面で入力した値については、ウィザードによる検証が実行されて、次の点が確認されます。
  - 構文の正確性
  - 入力値の互換性（たとえば、IPアドレスやゲートウェイに互換性があるか、またFQDNを使用して NTP サーバーが指定されている場合は設定された DNS に互換性があるか）

- Management Center Virtual と DNS サーバーおよび NTP サーバーとの間のネットワーク接続

これらのテストの結果はリアルタイムで画面上に表示されます。したがって、必要な修正を行い、設定の妥当性をテストしてから、画面の下部にある [終了（Finish）] をクリックできます。NTP および DNS 接続テストは非ブロッキングです。ウィザードが接続テストを完了する前に [終了（Finish）] をクリックすることもできます。[終了（Finish）] をクリックした後に接続の問題が見つかった場合は、このウィザードで設定を変更することはできませんが、初期設定の完了後に Web インターフェイスを使用してその接続を設定できます。

Management Center Virtual とブラウザとの間の既存の接続を切断することになる設定値を入力した場合、接続テストは実行されません。この場合、DNS または NTP の接続ステータス情報はウィザードに表示されません。

- 3 つのウィザード画面に続いて、ポップアップ ダイアログ ボックスが表示され、必要に応じてスマートライセンスをすばやく簡単に設定できます。

初期設定ウィザードと [スマートライセンス（Smart Licensing）] ダイアログの終了後、[デバイス管理（Device Management）] ページが表示されます。ご使用のバージョンの Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド で「Device Management」を参照してください。

始める前に

- Management Center が管理ネットワーク上で通信するために必要な次の情報があることを確認してください。
  - IPv4 管理 IP アドレス

    Management Center インターフェイスは、DHCP によって割り当てられた IPv4 アドレスを受け入れるように事前設定されています。DHCP が Management Center MAC アドレスに割り当てるように設定されている IP アドレスを確認するには、システム管理者に問い合わせてください。DHCP が使用できないシナリオでは、Management Center インターフェイスは IPv4 アドレス 192.168.45.45 を使用します。
  - ネットワークマスクとデフォルトゲートウェイ（DHCP を使用しない場合）。
- DHCP を使用していない場合は、次のネットワーク設定を使用して、ローカルコンピュータを設定します。
  - IP アドレス：192.168.45.2
  - ネットマスク：255.255.255.0
  - デフォルト ゲートウェイ：192.168.45.1

  このコンピュータの他のネットワーク接続をすべて無効にします。

ステップ 1 Web ブラウザを使用して、 Management Center Virtual の IP アドレス：https://<Firepower Management Center-IP> に移動します。

ログイン ページが表示されます。

ステップ 2 管理者アカウントのユーザー名に **admin** を、パスワードに **Admin123** を使用して Management Center Virtual にログインします（パスワードでは大文字と小文字が区別されます）。

ステップ 3 [パスワードの変更（Change Password）] 画面で、次のようにします。

a) （オプション）この画面の使用中にパスワードが表示されるようにするには、[パスワードの表示（Show password）] チェックボックスをオンにします。

b) （オプション）[パスワードの生成（Generate Password）] ボタンをクリックして、表示されている条件に準拠するパスワードを自動的に作成します（生成されたパスワードは非ニーモニックです。このオプションを選択する場合は、パスワードをメモしてください）。

c) 任意のパスワードを設定するには、[新しいパスワード（New Password）] テキストボックスと [パスワードの確認（Confirm Password）] テキストボックスに新しいパスワードを入力します。

パスワードは、ダイアログに示された条件を満たす必要があります。

（注） Management Center では、パスワードをパスワード クラッキング ディクショナリと照合して、英語の辞書に載っている多くの単語だけでなく、一般的なパスワードハッキング技術で簡単に解読できるその他の文字列についてもチェックします。たとえば、「abcdefg」や「passw0rd」などのパスワードは初期設定スクリプトによって拒否される場合があります。

（注） 初期設定プロセスが完了すると、システムは 2 つの **admin** アカウント（1 つは Web アクセス用、もう 1 つは CLI アクセス用）のパスワードを同じ値に設定します。パスワードは、ご使用のバージョンの Cisco Secure Firewall Management Center アドミニストレーション ガイド に記載されている強力なパスワード要件に準拠している必要があります。その後、いずれかの **admin** アカウントのパスワードを変更すると、パスワードは同じではなくなり、Web インターフェイスの **admin** アカウントから強力なパスワード要件を削除できます。

d) [次へ（Next）] をクリックします。

[パスワードの変更（Change Password）] 画面で [次へ（Next）] をクリックし、**admin** の新しいパスワードが承認されると、残りのウィザードの手順が完了していなくても、Web インターフェイスと CLI の両方の **admin** アカウントでそのパスワードが有効になります。

ステップ 4 [ユーザー契約（User Agreement）] 画面では、EULA を読み、[同意する（Accept）] をクリックし続行します。

[同意しない（Decline）] をクリックすると、Management Center Virtual からログアウトされます。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [ネットワークの設定の変更（Change Network Settings）] 画面では次を実行します。

a) [完全修飾ドメイン名（Fully Qualified Domain Name）] を入力します。デフォルト値が表示される場合、ネットワーク設定に対応していれば、それを使用できます。あるいは、完全修飾ドメイン名（シンタックス：`<hostname>.<domain>`）またはホスト名を入力します。

b) [IPv4の設定（Configure IPv4）] オプションでブートプロトコルとして、[DHCPの使用（Using DHCP）] または [スタティック/手動の使用（Using Static/Manual）] を選択します。

DHCP を使用する場合は、割り当てられたアドレスが変更されないように、DHCP 予約を使用する必要があります。DHCP アドレスが変更されると、Management Center ネットワーク設定が同期しなくなるため、デバイスの登録は失敗します。DHCP アドレスの変更から回復するには、Management Center に接続し（ホスト名または新しい IP アドレスを使用）、**システム**（⚙）>**[構成（Configuration）]**>[管理インターフェイス（Management Interfaces）] の順に選択してネットワークをリセットします。

c) [IPv4アドレス（IPv4 Address）] に表示されている値を使用するか（値が表示されている場合）、新しい値を入力できます。ドット付き 10 進法形式を使用します（192.168.45.45 など）。

（注） 初期設定中にIPアドレスを変更した場合は、新しいネットワーク情報を使用してManagement Center に再接続する必要があります。

d) [ネットワークマスク（Network Mask）] に表示されている値を使用するか（値が表示されている場合）、または新しい値を入力できます。ドット付き 10 進法形式を使用します（255.255.0.0 など）。

（注） 初期設定中にネットワークマスクを変更した場合は、新しいネットワーク情報を使用して Management Center に再接続する必要があります。

e) [ゲートウェイ（Gateway）] に表示されている値を使用するか（値が表示されている場合）、または新しいデフォルトゲートウェイを入力できます。ドット付き 10 進法形式を使用します（192.168.0.1 など）。

（注） 初期設定中にゲートウェイアドレスを変更した場合は、新しいネットワーク情報を使用して、Management Center への再接続が必要になる場合があります。

f) （オプション）[DNSグループ（DNS Group）] の場合は、デフォルト値の [Cisco Umbrella DNS] を使用します。

DNS 設定を変更するには、ドロップダウンリストから [カスタムDNSサーバー（Custom DNS Servers）] を選択し、[プライマリDNS（Primary DNS）] と [セカンダリDNS（Secondary DNS）] の IPv4 アドレスを入力します。Management Center にインターネットアクセスがない場合は、ローカルネットワークの外部で DNS を使用することはできません。ドロップダウンリストから [カスタムDNSサーバー（Custom DNS Servers）] を選択し、[プライマリDNS（Primary DNS）] フィールドと [セカンダリDNS（Secondary DNS）] フィールドを空白のままにして、DNS サーバーを設定しません。

（注） IP アドレスではなく FQDN を使用して NTP サーバーを指定する場合は、この時点で DNS を指定する必要があります。評価ライセンスを使用している場合、DNS はオプションですが、展開の際に永続ライセンスを使用するには DNS が必要です。

g) [NTPグループサーバー（NTP Group Servers）] の場合は、デフォルト値の [デフォルトNTPサーバー（Default NTP Servers）] を受け入れることができます。この場合は、システムでは **0.sourcefire.pool.ntp.org** がプライマリ NTP サーバーとして使用され、**1.sourcefire.pool.ntp.org** がセカンダリ NTP サーバーとして使用されます。

他の NTP サーバーを設定するには、ドロップダウンリストから [カスタムNTPグループサーバー（Custom NTP Group Servers）] を選択し、ネットワークから到達可能な 1 台または 2 台の NTP サーバーの FQDN または IP アドレスを入力します。Management Center からインターネットにアクセスできない場合は、ローカルネットワークを出て NTP サーバーを使用できません。

（注） 初期設定中にネットワーク設定を変更する場合は、新しいネットワーク情報を使用して Management Center に再接続する必要があります。

ステップ 7 [終了（Finish）] をクリックします。

ウィザードでは、この画面で入力した値の検証を実行して、構文の正確性、入力した値の互換性、Management Center と DNS および NTP サーバー間のネットワーク接続を確認します。[終了（Finish）] をクリックした後に接続の問題が見つかった場合は、このウィザードで設定を変更することはできませんが、初期設定の完了後に Management Center Web インターフェイスを使用してその接続を設定できます。

次のタスク

- スマートライセンシングを迅速かつ簡単にセットアップできるポップアップ ダイアログ ボックスが表示されます。このダイアログボックスの使用は任意です。スマートライセンスについて十分な知識があり、Management Center Virtual で 脅威に対する防御 を管理する場合は、このダイアログを使用してください。それ以外の場合は、このダイアログを閉じて、ご使用のバージョンの Cisco Secure Firewall Management Center アドミニストレーション ガイド で「Licensing」を参照してください。
- 初期設定プロセスの一環として、Management Center で自動的に設定される週次メンテナンスアクティビティを確認します。このアクティビティは、システムを最新の状態に保ち、データをバックアップする目的で設計されています。バージョン 6.5 以降の自動初期設定の確認 （8 ページ）を参照してください。
- 初期設定ウィザードと [スマートライセンス（Smart Licensing）] ダイアログの終了後、[デバイス管理（Device Management）] ページが表示されます。ご使用のバージョンの Cisco Firepower Management Center コンフィギュレーション ガイド [英語] を参照してください。
- ご使用のバージョンの Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド の説明に従い、Web インターフェイスを使用して初期セットアップを完了した後で、IPv6 アドレッシング用に Management Center を設定できます。

バージョン 6.5 以降の自動初期設定の確認

初期設定の一環として（初期設定ウィザードまたは CLI のどちらで実行しても）、Management Center によって、メンテナンスタスクが自動的に設定され、システムが最新の状態に保たれるとともに、データがバックアップされます。

タスクは UTC でスケジュールされるため、いつ現地で実行されるかは、日付と場所によって異なります。また、タスクは UTC でスケジュールされるため、サマータイムなど、所在地で実施される場合がある季節調整に合わせて調節されることもありません。このような影響を受ける場合、スケジュールされたタスクは、現地時間を基準とすると、夏期では冬期の場合よりも 1 時間「遅れて」実行されることになります。

（注） 自動スケジュール設定を検証し、Management Center がスケジュールを正しく確立し、必要に応じて調整しているかを確認することを強くお勧めします。

- 週次 GeoDB 更新

  Management Center では、毎週、ランダムに選択された時刻に行われるように、GeoDB の更新が自動的にスケジュールされます。Web インターフェイスのメッセージ センターを使用して、この更新のステータスを確認できます。この自動更新の設定は、Web インターフェイスの **[システム（System）]** > **[更新（Updates）]** > **[地理位置情報の更新（Geolocation Updates）]** > [位置情報の定期的な更新（Recurring Geolocation Updates）] で確認できます。システムが更新を設定できず、Management Center からインターネットに接続できる場合は、ご使用のバージョンの Cisco Secure Firewall Management Center アドミニストレーション ガイド の説明に従って、通常の GeoDB 更新を設定することを推奨します。

- Management Center の週次ソフトウェアアップデート

  Management Center では、Management Center およびその管理対象デバイスの最新ソフトウェアをダウンロードするための週次タスクが自動的にスケジュールされます。このタスクは、UTC で日曜日の午前 2 ～ 3 時の間に行われるようにスケジュールされます。したがって、日付と場所に応じて、現地時間では、土曜日の午後から日曜日の午後の範囲内のいずれかの時間帯に行われることになります。Web インターフェイスのメッセージ センターを使用して、このタスクのステータスを確認できます。このタスクの設定は、Web インターフェイスの **[システム（System）]** > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** で確認できます。タスクのスケジューリングに失敗するが、Management Center がインターネットにアクセスできる場合は、ご使用のバージョンの Cisco Secure Firewall Management Center アドミニストレーション ガイド の説明に従って、ソフトウェアの更新をダウンロードする定期タスクをスケジュールすることを推奨します。

  このタスクでは、アプライアンスで現在実行されているバージョンに対するソフトウェア パッチおよびホットフィックスをダウンロードするだけです。このタスクでダウンロードされた更新プログラムのインストールは、別に行う必要があります。詳細については、Cisco Management Center アップグレードガイド [英語] を参照してください。

- 週次の Management Center 設定バックアップ

  Management Center では、ローカルに保存された設定のみのバックアップを実行するための週次タスクが自動的にスケジュールされます。このタスクは、UTC で月曜日の午前 2 時に行われるようにスケジュールされます。したがって、日付と場所に応じて、現地時間では、日曜日の午後から月曜日の午後の範囲内のいずれかの時間帯に行われることになります。Web インターフェイスのメッセージ センターを使用して、このタスクのステータスを確認できます。このタスクの設定は、Web インターフェイスの **[システム（System）]** > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** で確認できます。タスクのスケジューリングに失敗する場合は、ご使用のバージョン Cisco Secure Firewall Management Center アドミニストレーション ガイド の説明に従って、バックアップを実行する定期タスクをスケジュールすることを推奨します。

- 脆弱性データベースの更新

Management Center バージョン 6.6+ では、 シスコのサポートサイトから最新の脆弱性データベース（VDB）の更新ファイルがダウンロードおよびインストールされます。これは 1 回限りの操作です。Web インターフェイスのメッセージ センターを使用して、この更新のステータスを確認できます。システムを最新の状態に保つために、Management Center がインターネットにアクセスできる場合は、ご使用のバージョンの Cisco Secure Firewall Management Center アドミニストレーション ガイド の説明に従って、自動の定期 VDB 更新のダウンロードとインストールを実行するタスクをスケジュールすることを推奨します。

- 侵入ルールの更新

  Management Center のバージョン 6.6+ では、 侵入ルールがシスコのサポートサイトから自動的に日次更新されるように設定されます。影響を受けるポリシーが Management Center で次に展開される際、該当する管理対象デバイスに対して自動侵入ルールの更新が展開されます。Web インターフェイスのメッセージ センターを使用して、このタスクのステータスを確認できます。このタスクの設定は、Web インターフェイスの **[システム（System）] > [更新（Updates）] > [ルールの更新（Rule Updates）]** で確認できます。更新の設定に失敗するが、Management Center がインターネットにアクセスできる場合は、ご使用のバージョンの Cisco Secure Firewall Management Center アドミニストレーション ガイド の説明に従って、通常の侵入ルールの更新を設定することを推奨します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。