



CHAPTER 3

Cisco ISE 3300 シリーズ アプライアンスの設定

この章では、Cisco Identity Services Engine (ISE) 3300 シリーズ アプライアンスの初期設定を実行する方法について説明します。内容は次のとおりです。

- 「Cisco ISE 3300 シリーズ アプライアンスを設定する前に」(P.3-1)
- 「セットアッププログラムのパラメータについて」(P.3-3)
- 「Cisco ISE 3300 シリーズ ハードウェア アプライアンスの設定」(P.3-5)
- 「設定プロセスの確認」(P.3-10)



(注)

Cisco ISE 3300 シリーズ アプライアンスで Cisco ISE ソフトウェアの設定を試みる前に、この章の設定の前提条件を確認する必要があります。

Cisco ISE 3300 シリーズ アプライアンスを設定する前に

Cisco ISE 3300 シリーズ アプライアンスには、Cisco Application Deployment Engine (ADE) リリース 2.0 オペレーティング システム (ADE-OS) および Cisco ISE リリース 1.1 ソフトウェアがあらかじめインストールされています。Cisco ADE-OS と Cisco ISE ソフトウェアは、専用の Cisco ISE アプライアンス (Cisco ISE 3300 シリーズ) にあらかじめインストールされています。また、このリリースでは VMware サーバにインストールすることもできます。

手順を進める前に、各アプライアンスまたは VMware インスタンスの以下のすべてのコンフィギュレーションの設定を特定していることを確認します。

- ホスト名
- ギガビット イーサネット 0 (eth0) インターフェイスの IP アドレス
- ネットマスク
- デフォルト ゲートウェイ
- DNS ドメイン
- プライマリ ネーム サーバ
- プライマリ ネットワーク タイム プロトコル (NTP) サーバ
- システム時間帯

- ユーザ名 (CLI 管理ユーザのユーザ名)
- パスワード (CLI 管理ユーザのパスワード)
- データベース管理者のパスワードおよびデータベース ユーザのパスワード (ワンタイム エントリのみ)

CLI 管理ユーザと Web ベース管理ユーザの権限の違いの詳細については、「[CLI 管理ユーザと Web ベース管理ユーザの admin 権限の違い](#)」(P.3-2) を参照してください。

CLI 管理ユーザと Web ベース管理ユーザの admin 権限の違い

Cisco ISE セットアップ プログラムを使用して設定したユーザ名およびパスワードは、Cisco ISE CLI および Cisco ISE Web インターフェイスでの管理アクセスでの使用を意図しています。Cisco ISE CLI にアクセスできる管理者を CLI 管理ユーザといいます。デフォルトでは、CLI 管理ユーザのユーザ名は **admin**、パスワードはセットアップ プロセスでユーザが定義したパスワードです。デフォルトのパスワードはありません。

CLI 管理ユーザのユーザ名、およびセットアップ プロセスで定義したパスワードを使用して、Cisco ISE Web インターフェイスに最初にアクセスできます。Web ベース **admin** のデフォルトのユーザ名およびパスワードはありません。

CLI 管理ユーザは、Cisco ISE の Web ベースの管理ユーザ データベースにコピーされます。最初の CLI 管理ユーザのみが Web ベースの管理ユーザとしてコピーされます。両方の管理ロールで同じユーザ名とパスワードを使用できるように、CLI と Web ベースの管理ユーザ ストアは同期を保持する必要があります。

追加の Web ベースの管理ユーザはユーザ インターフェイスから追加できます。さらに詳細については、『[Cisco Identity Services Engine User Guide, Release 1.1](#)』の「Configuring Cisco ISE Administrators」を参照してください。

Cisco ISE CLI 管理ユーザは、Cisco ISE Web ベースの管理ユーザとは異なる権限と機能を持ち、追加のタスクを実行できます。

CLI 管理ユーザおよび Web ベース管理ユーザによって実行されるタスク

CLI 管理ユーザおよび Web ベース管理ユーザは、次の Cisco ISE システム関連タスクを実行できます。

- Cisco ISE アプリケーション データをバックアップする。
- Cisco ISE アプライアンス上でシステム、アプリケーション、または診断ログを表示する。
- Cisco ISE ソフトウェア パッチ、メンテナンス リリース、およびアップグレードを適用する。
- NTP サーバ コンフィギュレーションを設定する。

CLI 管理ユーザによってのみ実行されるタスク

CLI 管理ユーザのみが、次の Cisco ISE システム関連タスクを実行できます。

- Cisco ISE アプリケーション ソフトウェアを起動および停止する。
- Cisco ISE アプライアンスをリロードまたはシャットダウンする。
- ロックアウトした場合、Web ベースの管理ユーザをリセットする。詳細については、「[管理者のロックアウトによるパスワードの無効化](#)」(P.6-15) を参照してください。

Cisco ISE CLI にアクセスするユーザのみを明示的に作成し、CLI 管理ユーザの資格情報を保護することを推奨します。



(注)

Cisco ISE ユーザ インターフェイスを使用して作成された Web ベース管理ユーザは、Cisco ISE CLI に自動的にログインできません。これらの権限を持つように明示的に作成された CLI 管理ユーザのみが、Cisco ISE CLI にアクセスできます。

詳細については、「[Web ブラウザを使用した Cisco ISE へのアクセス](#)」(P.6-7) を参照してください。

他の CLI 管理ユーザを作成するには、まず CLI 管理ユーザとして Cisco ISE CLI にログインし、次のタスクを実行します。

- ステップ 1** セットアッププロセスで作成した CLI 管理ユーザ名とパスワードを使用してログインします。
- ステップ 2** コンフィギュレーション モードを開始します。
- ステップ 3** `username` コマンドを実行します。



(注)

詳細については、『[Cisco Identity Services Engine CLI Reference Guide, Release 1.0.4](#)』を参照してください。

セットアッププログラムのパラメータについて

Cisco ISE セットアッププログラムを実行して Cisco ISE ソフトウェアを設定する場合、対話形式の CLI が起動し、システムの設定に必要なパラメータの入力を求めるプロンプトが表示されます (表 3-1 を参照)。サポートされるハードウェア アプライアンスへの接続を確立してセットアッププログラムを実行する方法は、いくつかあります。

- ハードウェア アプライアンスへのネットワークベースのコンソール接続を使用する。
- アプライアンスの背面パネルへのローカル シリアル コンソール ケーブル接続を使用する。
- アプライアンスへのローカル キーボードおよびビデオ (VGA) 接続を使用する。

これらの方法により、アプライアンス管理者の資格情報の最初のセットを作成する初期ネットワークを設定できます。セットアッププログラムの使用は一度だけ実行する設定作業です。



(注)

次の手順は、推奨手順に従って、サポートされているアプライアンスを適切にインストール、接続、および電源投入していることを前提としています。VMware サーバの設定については、「[Cisco Identity Services Engine ISE ソフトウェア DVD を使用した VMware システムの設定](#)」(P.4-12) を参照してください。

■ セットアッププログラムのパラメータについて

表 3-1 セットアップ用の Identity Services Engine ネットワーク設定パラメータ

プロンプト	説明	例
ホスト名 (Hostname)	19 文字以下にする必要があります。有効な文字は、英数字 (A ~ Z, a ~ z, 0 ~ 9) とハイフン (-) で、最初の文字はアルファベット文字でなければなりません。	isebeta1
(eth0) イーサネット インターフェイス アドレス (eth0) Ethernet interface address)	ギガビット イーサネット 0 (eth0) インターフェイスの有効な IPv4 アドレスでなければなりません。	10.12.13.14
ネットマスク (Netmask)	有効な IPv4 ネットマスクでなければなりません。	255.255.255.0
デフォルト ゲート ウェイ (Default gateway)	デフォルト ゲートウェイの有効な IPv4 アドレスでなければなりません。	10.12.13.1
DNS ドメイン名 (DNS domain name)	IP アドレスは入力できません。有効な文字は、ASCII 文字、数値、ハイフン (-)、およびピリオド (.) です。	mycompany.com
プライマリ ネーム サーバ (Primary name server)	プライマリ ネーム サーバの有効な IPv4 アドレスでなければなりません。	10.15.20.25
別のネーム サーバ の追加/編集 (Add/Edit another name server)	追加のネーム サーバの有効な IPv4 アドレスでなければなりません。	(オプション) 複数のネーム サーバを設定できます。これを行 うには、 y を入力して続行し ます。
プライマリ NTP サーバ (Primary NTP server)	NTP サーバの有効な IPv4 アドレスまたはホスト名でなければなりません。	clock.nist.gov
別の NTP サーバの 追加/編集 (Add/Edit another NTP server)	有効な NTP ドメインでなければなりません。	(オプション) 複数の NTP サー バを設定できます。これを行 うには、 y を入力して続行しま す。
システム時間帯 (System Time Zone)	有効な時間帯でなければなりません。詳細については、『 Cisco Identity Services Engine CLI Reference Guide, Release 1.0.4 』に記載されている Cisco ISE がサポートする時間帯のリストを参照してください。たとえば、太平洋標準時 (PST) の場合は、PST8PDT (または UTC-8 時間) です。 (注) このハイパーリンクで参照される時間帯は、最も頻繁に使用される時間帯です。サポートされている時間帯のすべてのリストについては、Cisco ISE CLI から show timezones コマンドを実行できます。	UTC (デフォルト)
ユーザ名	Cisco ISE システムへの CLI アクセスに使用される管理者ユーザ名を特定します。デフォルト (admin) を使用しない場合は、新しいユーザ名を作成する必要があります。ユーザ名は 3 ~ 8 文字で、有効な英数字 (A ~ Z, a ~ z, 0 ~ 9) で構成されている必要があります。	admin (デフォルト)

表 3-1 セットアップ用の Identity Services Engine ネットワーク設定パラメータ (続き)

プロンプト	説明	例
パスワード	Cisco ISE システムへの CLI アクセスに使用される管理者パスワードを特定します。このパスワードは作成する必要があります (デフォルトはありません)。パスワードは最低 6 文字で、小文字 (a ~ z)、大文字 (A ~ Z)、数字 (0 ~ 9) がそれぞれ 1 つ以上含まれている必要があります。	MyIseYP@@ss
データベース管理者のパスワード (Database Administrator Password)	Cisco ISE データベースのシステム レベルのパスワードを特定します。このパスワードは作成する必要があります (デフォルトはありません)。パスワードは最低 11 文字で、小文字 (a ~ z)、大文字 (A ~ Z)、数字 (0 ~ 9) がそれぞれ 1 つ以上含まれている必要があります。使用可能な文字のリストには、アンダースコア (_) およびポンド (#) キーも含まれます。 (注) 分散環境のすべてのノードに同じパスワードが必要であるため、必ず同じエントリを使用してすべてのノードを設定してください。このパスワードの設定後、Cisco ISE はこれを「内部的に」使用します。つまり、システムのログイン時にこのパスワードを入力する必要はありません。	ISE4adbp_ss
データベースユーザのパスワード (Database User Password)	Cisco ISE データベースのアクセス レベルのパスワードを特定します。このパスワードは作成する必要があります (デフォルトはありません)。パスワードは最低 11 文字で、小文字 (a ~ z)、大文字 (A ~ Z)、数字 (0 ~ 9) がそれぞれ 1 つ以上含まれている必要があります。使用可能な文字のリストには、アンダースコア (_) およびポンド (#) キーも含まれます。 (注) 分散環境のすべてのノードに同じパスワードが必要であるため、必ず同じエントリを使用してすべてのノードを設定してください。このパスワードの設定後、Cisco ISE はこれを「内部的に」使用します。つまり、システムのログイン時にこのパスワードを入力する必要はありません。	ISE5udbp#ss



(注)

Web ベースの管理者のユーザ名およびパスワードの詳細については、「[Web ブラウザを使用した設定の確認](#)」(P.6-10) を参照してください。

VMware サーバに Cisco ISE ソフトウェアをインストールしている場合は、Cisco ISE は初期セットアップ中に VMware ツールもインストールおよび設定します。Cisco ISE は VMware ツールバージョン 8.3.2 をインストールします。VMware ツールが正しくインストールされたことを確認するには、「[VMware ツールのインストールの確認](#)」(P.6-12) を参照してください。

Cisco ISE 3300 シリーズ ハードウェア アプライアンスの設定

この項では、サポートされているハードウェア アプライアンス用に Cisco ISE 3300 シリーズ ソフトウェアを設定するための Cisco ISE セットアップ プログラムの実行について説明します。

セットアッププログラムを使用して Cisco ISE 3300 シリーズ アプライアンスを設定するには、次の手順を実行します。

- ステップ 1** キーボードと VGA モニタを Cisco ISE 3300 シリーズ アプライアンスに接続します。
- ステップ 2** 電源コードが Cisco ISE 3300 シリーズに接続されており、アプライアンスがオンであることを確認します。



(注) Cisco ISE ソフトウェアはすでにアプライアンスにあらかじめインストールされています。Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx) DVD を挿入しないでください。DVD は、アプライアンスのイメージ再適用の実行、または CLI パスワードのリカバリの目的にのみ提供されています。

約 2 分で、次のプロンプトが表示されます。これはブート シーケンスが完了したことを意味します。

Please type 'setup' to configure the appliance

- ステップ 3** プロンプトで、**setup** と入力し、セットアッププログラムを起動します。ネットワーキング パラメータおよび最初の資格情報の入力を求めるプロンプトが表示されます。次に、セットアッププログラムとデフォルト プロンプトの例を示します。



(注) Cisco ISE アプライアンスは、UTC 時間帯を使用して内部的に時間を追跡します。特定の時間帯が不明の場合は、Cisco ISE アプライアンスがある都市、地域、または国に基づいて入力します。時間帯の例については、表 3-2、表 3-3、および表 3-4 の表を参照してください。インストール中に、セットアップによりこの設定を求めるプロンプトが表示された時に、希望する時間帯（デフォルトは UTC）を設定することをお勧めします。



注意

インストール後に Cisco ISE アプライアンス上で時間帯を変更すると、そのノード上で Cisco ISE アプリケーションを使用できなくなります。時間帯の変更による影響の詳細については、『Cisco Identity Services Engine CLI Reference Guide, Release 1.0.4』の付録 A の「clock time zone」を参照してください。

```
Enter hostname[: ise-server-1
Enter IP address[: 10.1.1.10
Enter Netmask[: 255.255.255.0
Enter IP default gateway[: 172.10.10.10
Enter default DNS domain[: cisco.com
Enter Primary nameserver[: 200.150.200.150
Add/Edit another nameserver? Y/N: n
Enter primary NTP domain[: clock.cisco.com
Add/Edit another NTP domain? Y/N: n
Enter system time zone[: UTC
Enter username [admin]: admin
Enter password:
Enter password again:
Bringing up the network interface...
Pinging the gateway...
Pinging the primary nameserver...
Do not use `Ctrl-C' from this point on...
```

```

Virtual machine detected, configuring VMware tools...
Appliance is configured
Installing applications...
Installing ISE...
Application bundle (ise) installed successfully

===Initial Setup for Application: ise===

Welcome to the ISE initial setup. The purpose of this setup is to provision the
internal ISE database. This setup requires you to create database administrator
password and also create a database user password.

Please follow the prompts below to create the database administrator password.

Enter new database admin password:
Confirm new database admin password:
Successfully created database administrator password.

Please follow the prompts below to create the database user password.

Enter new database user password:
Confirm new database user password:
Successfully created database user password.
Running database cloning script...

Generating configuration...
Rebooting...

Welcome to the ISE initial setup. The purpose of this setup is to provision the
internal database. This setup is non-interactive and will take roughly 15
minutes to complete. Please be patient.

Running database cloning script...
Running database network config assistant tool...
Extracting ISE database contents...
Starting ISE database processes...

...

```



(注) 「Virtual machine detected, configuring VMware tools...」メッセージは、Cisco ISE が仮想マシンにインストールされている場合のみ表示されます。このメッセージは、Cisco ISE が物理マシンにインストールされている場合は表示されません。

ステップ 4

Cisco ISE ソフトウェアの設定後、Cisco ISE システムは自動的にリブートします。Cisco ISE CLI にログインし直すには、セットアップ時に設定した CLI 管理ユーザの資格情報を入力する必要があります。

Cisco ISE のリブート後、新しいデータベース管理者およびデータベース ユーザのパスワードの入力および確認を求めるプロンプトが表示されます。(分散環境のすべてのノードに同じパスワードが必要であるため、必ず同じエントリを使用してすべてのノードを設定してください)。このプロンプトが表示されます。

```

Welcome to the ISE initial setup. The purpose of this setup is to
provision the internal database. This setup requires you to create
a database administrator password and also create a database user password.

```

```

Please follow the prompts below to create the database administrator password.

```



```
Enter new database admin password:
Confirm new database admin password:
Successfully created database administrator password.
```

Please follow the prompts below to create the database user password.

```
Enter new database user password:
Confirm new database user password:
Successfully created database user password.
```

```
Running database cloning script...
Running database network config assistant tool...
Extracting ISE database contents...
Starting ISE database processes...
```

...

- ステップ 5** Cisco ISE CLI シェルにログインし直したら、次の CLI コマンドを実行して、Cisco ISE アプリケーションプロセスのステータスを確認することができます。

```
ise-server/admin# show application status ise

ISE Database listener is running, PID: 4845
ISE Database is running, number of processes: 27
ISE Application Server is running, PID: 6344
ISE M&T Session Database is running, PID: 4502
ISE M&T Log Collector is running, PID: 6652
ISE M&T Log Processor is running, PID: 6738
ISE M&T Alert Process is running, PID: 6542
ise-server/admin#
```

- ステップ 6** Cisco ISE アプリケーション サーバが実行中であることを確認した後、次のサポートされている Web ブラウザのいずれかを使用して Cisco ISE ユーザ インターフェイスにログインできます ([「Web ブラウザを使用した Cisco ISE へのアクセス」 \(P.6-7\)](#) を参照)。

Web ブラウザを使用して Cisco ISE ユーザ インターフェイスにログインするには、アドレス フィールドに次のように入力します。

```
https://<your-ise-hostname or IP address>/admin/
```

ここで、「your-ise-hostname or IP address」はセットアップ時に Cisco ISE 3300 シリーズ アプライアンスに対して設定したホスト名または IP アドレスを表します。

- ステップ 7** Cisco ISE のログイン ウィンドウで、Cisco ISE ユーザ インターフェイスにアクセスするための Web ベース admin ログイン資格情報 (ユーザ名およびパスワード) を求めるプロンプトが表示されます。CLI 管理ユーザのユーザ名、およびセットアッププロセスで定義したパスワードを使用して、Cisco ISE Web インターフェイスに最初にアクセスできます。

Cisco ISE ユーザ インターフェイスにログインしたら、続いて、デバイス、ユーザ ストア、ポリシー、およびその他のコンポーネントを設定できます。

Cisco ISE ユーザ インターフェイスへの Web ベースのアクセスに使用するユーザ名とパスワードの資格情報は、Cisco ISE CLI インターフェイスへのアクセス用にセットアップ時に作成した CLI 管理ユーザの資格情報と同じではありません。これらの 2 種類の管理ユーザの違いの説明については、[「CLI 管](#)

「[理ユーザーと Web ベース管理ユーザーの admin 権限の違い](#)」(P.3-2) を参照してください。

サポートされている時間帯

この項では、欧州、米国およびカナダ、オーストラリア、アジアの共通の UTC 時間帯の詳細を 3 つの表で示しています。



(注)

時間帯の形式は、POSIX または System V です。POSIX 時間帯形式の構文は America/Los_Angeles、一方、System V 時間帯の構文は PST8PDT のようになります。

- 欧州、米国およびカナダの時間帯については、[表 3-2](#) を参照してください。
- オーストラリアの時間帯については、[表 3-3](#) を参照してください。
- アジアの時間帯については、[表 3-4](#) を参照してください。

表 3-2 共通の時間帯

略語または名前	時間帯名
欧州	
GMT、GMT0、GMT-0、GMT+0、UTC、Greenwich、Universal、Zulu	グリニッジ標準時 (UTC)
GB	英国
GB-Eire、Eire	アイルランド
WET	西ヨーロッパ時間 (UTC)
CET	中央ヨーロッパ標準時 (UTC + 1 時間)
EET	東ヨーロッパ時間 (UTC + 2 時間)
米国およびカナダ	
EST、EST5EDT	東部標準時、UTC - 5 時間
CST、CST6CDT	中央標準時、UTC - 6 時間
MST、MST7MDT	山岳部標準時、UTC - 7 時間
PST、PST8PDT	太平洋標準時、UTC - 8 時間
HST	ハワイ標準時、UTC - 10 時間

表 3-3 オーストラリアの時間帯

オーストラリア¹			
ACT ²	Adelaide	Brisbane	Broken_Hill
Canberra	Currie	Darwin	Hobart
Lord_Howe	Lindeman	LHI ³	Melbourne
North	NSW ⁴	Perth	Queensland
South	Sydney	Tasmania	Victoria
West	Yancowinna		

1. 国と都市をスラッシュ (/) で区切って入力します (例: Australia/Currie)。
2. ACT = Australian Capital Territory (オーストラリア首都特別地域)
3. LHI = Lord Howe Island (ロード・ハウ諸島)
4. NSW = New South Wales (ニュー サウス ウェールズ)

表 3-4 アジアの時間帯

アジア ¹			
Aden ²	Almaty	Amman	Anadyr
Aqtau	Aqtobe	Ashgabat	Ashkhabad
Baghdad	Bahrain	Baku	Bangkok
Beirut	Bishkek	Brunei	Kolkata
Choibalsan	Chongqing	Columbo	Damascus
Dhakar	Dili	Dubai	Dushanbe
Gaza	Harbin	Hong_Kong	Hovd
Irkutsk	Istanbul	Jakarta	Jayapura
Jerusalem	Kabul	Kamchatka	Karachi
Kashgar	Katmandu	Kuala_Lumpur	Kuching
Kuwait	Krasnoyarsk		

1. アジアの時間帯には、東アジア、南アジア、東南アジア、西アジア、および中央アジアがあります。
2. 地域と都市または国をスラッシュ (/) で区切って入力します (例: Asia/Aden)。



(注)

Cisco ISE CLI **show timezones** コマンドを使用すると、追加の時間帯を使用できます。この CLI コマンドを実行すると、使用可能なすべての時間帯が表示されます。ネットワークの場所に最適な時間帯を選択します。

設定プロセスの確認

設定プロセスが正しく完了したことを確認するには、次の 2 つの方法のいずれかを使用して Cisco ISE 3300 シリーズ アプライアンスにログインします。

- Web ブラウザ
- Cisco ISE CLI



(注)

インストール後の設定の確認を実行するには、第 6 章「インストール後のタスクの実行」を参照してください。