



Cisco Identity Services Engine アップグレードガイド リリース 1.3

初版：2014年10月31日

最終更新：2014年10月31日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.



目次

はじめに v

目的 v

対象読者 vi

ガイドの構成 vi

表記法 vi

関連資料 viii

マニュアルの入手方法およびテクニカル サポート x

はじめる前に 1

Cisco ISE 1.3 でサポートされるアップグレードパス 1

アップグレード時間の計算 2

通信用に開く必要があるファイアウォールポート 2

VMware 仮想マシンの設定 3

証明書および秘密キーのエクスポート 3

リポジトリの作成およびアップグレードバンドルのコピー 3

プライマリ管理ノードからの Cisco ISE 設定および運用データのバックアップ 4

プライマリ管理ノードからのシステム ログのバックアップ 4

Active Directory および内部管理者アカウントの資格情報の取得 4

実稼働環境で使用する前のカスタム ポータル移行のラボ設定での確認 4

プロファイラ設定の記録 5

インライン ポスチャ ノード設定の記録 5

さまざまな展開タイプのアップグレード方法 7

スタンドアロンノードのアップグレード 7

アップグレードの準備 7

アップグレードの実行 8

2 ノード展開のアップグレード 10

分散展開のアップグレード 12

- アップグレードプロセスの確認 16
- リリース 1.3 でのゲスト サービスの変更 17
 - 管理者ポータルの変更 17
 - その他のポータル関連の変更 33
 - ポリシー関連の変更 35
- アップグレード後の作業 37
 - アップグレード後の作業 37
- アップグレードの障害からの回復 41
 - アップグレードの障害 42
 - アップグレードがバイナリのインストール中に失敗する 43



はじめに

- [目的, v ページ](#)
- [対象読者, vi ページ](#)
- [ガイドの構成, vi ページ](#)
- [表記法, vi ページ](#)
- [関連資料, viii ページ](#)
- [マニュアルの入手方法およびテクニカルサポート, x ページ](#)

目的

このマニュアルは、Cisco ISE アプライアンスおよび VMware 仮想マシンで Cisco Identity Services Engine (ISE) ソフトウェアをアップグレードする方法について説明します。

以前のリリースまたはメンテナンス リリースからリリース 1.3 に Cisco ISE をアップグレードできます。Cisco Secure Access Control System (ACS)、リリース 5.5 または 5.6 から、リリース 1.3 に移行することも可能です。

Cisco Secure ACS 4.x 以前のバージョン、Cisco Secure ACS 5.3 または 5.4、または Cisco Network Admission Control (NAC) アプライアンスからリリース 1.3 に移行することはできません。

Cisco Secure ACS、リリース 5.5 または 5.6 から Cisco ISE、リリース 1.3 への移行については、『*Cisco Identity Services Engine, Release 1.3 Migration Tool Guide*』を参照してください。



(注) Cisco Secure ACS、リリース 5.5 または 5.6 からのみ、Cisco ISE、リリース 1.3 に直接移行できます。Cisco Secure ACS、リリース 4.x、5.1、5.2、5.3、および 5.4 の場合は、ACS、リリース 5.5 または 5.6 にアップグレードしてから、Cisco ISE、リリース 1.3 に移行する必要があります。

対象読者

このガイドは、Cisco ISE 3300 シリーズおよび 3400 シリーズ アプライアンスまたは VMware サーバで Cisco ISE ソフトウェアをアップグレードおよび設定するネットワーク管理者、システムインテグレータ、ネットワーク配置担当者を対象としています。このアップグレードガイドを使用する準備として、ネットワーク機器およびケーブル接続を理解し、電気回路、配線、装置ラックの取り付けに関する基礎知識を得ておく必要があります。

ガイドの構成

章	説明
はじめる前に, (1 ページ)	アップグレードを開始する前に完了する必要がある準備タスクの一覧を示します。
さまざまな展開タイプのアップグレード方法, (7 ページ)	スタンドアロン、2 ノード展開および分散展開の Cisco ISE ノードをアップグレードする方法について説明します。
リリース 1.3 でのゲストサービスの変更, (17 ページ)	アップグレードする前に認識しておく必要があるゲストサービス関連のアップグレードの考慮事項と依存関係を示します。
アップグレード後の作業, (37 ページ)	アップグレード後に完了する必要があるタスクの一覧を示します。
アップグレードの障害からの回復, (41 ページ)	アップグレードの障害から回復する方法について説明します。

表記法

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control (Ctrl) キーを表します。たとえば、^D または Ctrl+D というキーの組み合わせは、Ctrl キーを押して、D キーを押すことを意味します。(キーラベルは大文字で表記されていますが、大文字と小文字の区別はありません)。
太字フォント	ユーザが入力する必要があるコマンドおよびキーワードは、太字フォントで示しています。

表記法	説明
イタリック体フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、イタリック体フォントで示しています。
<code>courier</code> フォント	システムが表示するターミナルセッションおよび情報は、 <code>courier</code> フォントで示しています。
太字の <code>courier</code> フォント	太字の <code>courier</code> フォントは、ユーザが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。
...	構文要素の後の省略記号（3つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。
	選択肢を示す縦棒は、キーワードセットまたは引数セットのいずれかの選択肢を示します。
[x y]	いずれか1つを選択できる省略可能な要素は、角カッコで囲み、選択肢を示す縦棒で区切って示しています。
{x y}	必ずいずれか1つを選択しなければならない必須要素は、波カッコで囲み、選択肢を示す縦棒で区切って示しています。
string	引用符を付けない一連の文字。stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてstringと見なされます。
<>	山カッコは、ユーザが入力しても画面に表示されないパスワードなどの文字列を示しています。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!#	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。



(注) 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。



ヒント この情報が問題の解決などに役立つ情報をであることを示しています。



注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。



ワンポイントアドバイス

時間を節約する方法です。記述されている操作を実行すると時間を節約できます。



警告

「警告」の意味です。人身事故を予防するための注意事項が記述されています。

関連資料

リリース固有のドキュメント

Cisco ISE の一般的な製品情報は、<http://www.cisco.com/go/ise> で参照することができます。エンドユーザのマニュアルは Cisco.com の <http://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html> で参照することができます。

表 1 : **Cisco Identity Services Engine** の製品マニュアル

『 <i>Release Notes for Cisco Identity Services Engine, Release 1.3</i> 』	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
『 <i>Cisco Identity Services Engine Network Component Compatibility, Release 1.3</i> 』	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
『 <i>Cisco Identity Services Engine User Guide, Release 1.3</i> 』	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
『 <i>Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.3</i> 』	

<p>『Cisco Identity Services Engine Hardware Installation Guide, Release 1.3』</p> <p>『Cisco Identity Services Engine アップグレードガイド リリース 1.3』</p> <p>『Cisco Identity Services Engine, Release 1.3 Migration Tool Guide』</p> <p>『Regulatory Compliance and Safety Information for Cisco Identity Services Engine 3400 Series Appliance and Cisco 3400 Secure Access Control System』</p>	<p>http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html</p>
<p>『Cisco Identity Services Engine CLI Reference Guide, Release 1.3』</p> <p>『Cisco Identity Services Engine API Reference Guide, Release 1.3』</p>	<p>http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html</p>
<p>『Cisco Identity Services Engine In-Box Documentation and China RoHS Pointer Card』</p>	<p>http://www.cisco.com/en/US/products/ps11640/products_documentation_roadmaps_list.html</p>

プラットフォーム固有のマニュアル

プラットフォーム固有のその他のマニュアルへのリンクは、次の場所にあります。

表 2: プラットフォーム固有のマニュアル

Cisco ISE	http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html
Cisco NAC Appliance	http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html
Cisco NAC Guest Server	http://www.cisco.com/en/US/products/ps10160/tsd_products_support_series_home.html
Cisco NAC Profiler	http://www.cisco.com/en/US/products/ps8464/tsd_products_support_series_home.html
Cisco Secure Access Control System	http://www.cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html
Cisco UCS C シリーズ サーバ	http://www.cisco.com/en/US/docs/unified_computing/ucs/overview/guide/UCS_rack_roadmap.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『What's New in Cisco Product Documentation』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

『What's New in Cisco Product Documentation』は Really Simple Syndication (RSS) フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。



第 1 章

はじめる前に

アップグレードを開始する前に、次の情報を注意深く読み、その設定（バックアップ、エクスポート、スクリーンショットの取得）を可能な限り記録してください。

- [Cisco ISE 1.3 でサポートされるアップグレードパス, 1 ページ](#)
- [アップグレード時間の計算, 2 ページ](#)
- [通信用に開く必要があるファイアウォールポート, 2 ページ](#)
- [VMware 仮想マシンの設定, 3 ページ](#)
- [証明書および秘密キーのエクスポート, 3 ページ](#)
- [リポジトリの作成およびアップグレードバンドルのコピー, 3 ページ](#)
- [プライマリ管理ノードからの Cisco ISE 設定および運用データのバックアップ, 4 ページ](#)
- [プライマリ管理ノードからのシステム ログのバックアップ, 4 ページ](#)
- [Active Directory および内部管理者アカウントの資格情報の取得, 4 ページ](#)
- [実稼働環境で使用する前のカスタム ポータル移行のラボ設定での確認, 4 ページ](#)
- [プロファイラ設定の記録, 5 ページ](#)
- [インライン ポスチャ ノード設定の記録, 5 ページ](#)

Cisco ISE 1.3 でサポートされるアップグレードパス

次のリリースはすべて、Cisco ISE、リリース 1.3 に直接アップグレードできます。

- Cisco ISE、リリース 1.2
- Cisco ISE、リリース 1.2.1

Cisco ISE、リリース 1.2 よりも前のバージョンを使用している場合、初めに 1.2 にアップグレードしてから 1.3 にアップグレードする必要があります。リリース 1.2 への移行でサポートされてい

るアップグレードパスについては、[『Release Notes for Cisco Identity Services Engine, Release 1.2.x』](#)を参照してください。

アップグレード時間の計算

アップグレード時間の計算

次の表に、Cisco ISE ノードのアップグレードの推定所要時間を示します。アップグレードにかかる実際の時間は、いくつかの要因によって異なります。実稼働ネットワークは、アップグレードプロセス中にダウンタイムなしで動作し続けます。ここに示すデータは25000名のユーザと250,000のエンドポイントの展開の場合です。

展開のタイプ	ノード ペルソナ	アップグレードにかかる時間
スタンドアロン (2000 エンドポイント)	管理、ポリシーサービス、モニタリング	1 時間 20 分
分散 (25,000 のユーザと 250,000 のエンドポイント)	セカンダリ管理	2 時間
	モニタリング	1.5 時間

アップグレードにかかる時間に影響する要因

- ネットワークのエンドポイント数
- ネットワークのユーザ数とゲスト ユーザ数
- プロファイリング サービス (イネーブルの場合)



(注) 仮想マシン上の Cisco ISE ノードのアップグレードは、物理アプライアンスのアップグレードよりも長い時間がかかる場合があります。

通信用に開く必要があるファイアウォール ポート

プライマリ管理ノードと他のノードの間にファイアウォールを導入している場合、次のポートがアップグレード前に開いている必要があります。

- TCP 1528 : プライマリ管理ノードとモニタリング ノード間の通信用。
- TCP 443 : プライマリ管理ノードとその他すべてのセカンダリ ノード間の通信用。
- TCP 12001 : グローバル クラスターのレプリケーション用。

- TCP 7800 および 7802 : (ポリシー サービス ノードが ノード グループの一部である場合に限り該当) PSN グループのクラスタリング用。

Cisco ISE が使用するすべてのポートのリストについては、『*Cisco Identity Services Engine Hardware Installation Guide*』を参照してください。

VMware 仮想マシンの設定

仮想マシン (VM) 上の Cisco ISE ノードをアップグレードする場合は、リリース 1.3 へのアップグレード後に VM の電源をオフにして、ゲスト オペレーティング システムを Red Hat Enterprise Linux 6 (64 ビット) に変更し、変更後に VM の電源をオンにします。

証明書および秘密キーのエクスポート

次の項目をエクスポートすることを推奨します。

- すべてのローカル証明書 (展開内のすべてのノードから) およびその秘密キーを安全な場所にエクスポートします。証明書設定 (どのサービスに証明書が使用されたか) を記録します。
- プライマリ管理ノードの証明書ストアからすべての証明書をエクスポートします。証明書設定 (どのサービスに証明書が使用されたか) を記録します。

リポジトリの作成およびアップグレードバンドルのコピー

リポジトリを作成して、バックアップを取得してアップグレードバンドルをコピーします。パフォーマンスと信頼性を高めるために、FTP を使用することを推奨します。低速 WAN リンクを介したリポジトリを使用しないでください。

アップグレード用に、次のコマンドを使用して Cisco ISE ノードのローカル ディスクにアップグレードバンドルをコピーできます。

```
copy repository_url ise-upgradebundle-1.2.x-to-1.3.0.693.x86_64.tar.gz disk:/
```

```
例 : copy sftp://sftpserver ise-upgradebundle-1.2.x-to-1.3.0.693.x86_64.tar.gz disk:/
```

ローカル ディスクにアップグレードバンドルを置くと、アップグレード時間を短縮できます。

application upgrade prepare コマンドは、アップグレードバンドルをローカル ディスクにコピーして、これを抽出します。

プライマリ管理ノードからの Cisco ISE 設定および運用データのバックアップ

コマンドラインインターフェイス (CLI) または GUI から Cisco ISE の設定および運用データのバックアップを取得します。CLI コマンドは次のとおりです。

```
backup backup-name repository repository-name {ise-config | ise-operational} encryption-key {hash | plain} encryption-keyname
```

プライマリ管理ノードからのシステムログのバックアップ

コマンドラインインターフェイス (CLI) を使用して、プライマリ管理ノードからシステム ログのバックアップを取得します。CLI コマンドは次のとおりです。

```
backup-logs backup-name repository repository-name encryption-key { hash | plain } encryption-key name
```

Active Directory および内部管理者アカウントの資格情報の取得

外部アイデンティティ ソースとして Active Directory を使用している場合は、Active Directory 資格情報を取得して有効な内部管理者アカウントの資格情報を持っていることを確認します。アップグレード後に、Active Directory 接続が失われることがあります。この場合、管理者ポータルにログインして Cisco ISE と Active Directory を再接続するための ISE 内部管理者アカウントが必要です。

実稼働環境で使用する前のカスタムポータル移行のラボ設定での確認

Cisco ISE、リリース 1.3 は、ゲストおよび従業員に、新しい合理化されたオンボーディング エクスペリエンスと、多言語のサポートから WYSIWYG へのカスタマイゼーションに至る数多くの新機能による、新しいポータルカスタマイゼーションエクスペリエンスを提供します。リリース 1.3 にアップグレードすると、すべてのカスタム ポータルが新しい ISE 1.3 エクスペリエンスに移行します。認識すべきいくつかの考慮事項を次に示します。

- 以前のリリースの ISE で CSS と HTML を使用して行っていた基本的なルック アンド フィールのカスタマイズは、1.3 へのアップグレードプロセスによって新しいゲストおよびパーソナル デバイスのフローに移行されます。

- 基本HTMLおよびネイティブ管理ツールを使用して行われたカスタマイズは、適切に移行されます。ゲストのフローを変更するためのカスタム JavaScript を使用したカスタマイズは、適切に移行されない場合があります。ISE 1.3 管理者ポータルからこれらのポータルを再作成できます。
- リリース 1.3 に移行されたカスタム ポータルはいずれも編集できません。ロック アンド フィール、フロー、または機能を変更する場合は、新しいポータルを作成する必要があります (ISE 1.3 管理者ポータルから)。
- ISE 1.2 カスタマーは、多様なポータルのカスタマイズが可能でした。これらのカスタマイズの一部は、ISE 1.3 に予期したとおりに移行しない場合があります。新しく移行されたポータルを実稼働環境で使用する前に、ラボ設定でこれらのポータルを確認することを推奨します。
- 次の場合、ISE 1.3 はゲスト アカウントの作成に失敗します。
 - 1 ISE 1.2 のゲスト ポータルでセルフサービスを許可するように設定した
 - 2 ポータルのカスタマイズ時にタイムゾーン値をハードコードした
 - 3 カスタマイズされたポータルを、ISE 1.3 アップグレードプロセスを使用して ISE 1.3 に移行した

これは、カスタマイズされたポータル内のハードコードされたタイムゾーン値が、ISE 1.3 内のゲスト ロケーション名に一致しない可能性があるために発生します。ISE 1.2 の「タイムゾーン」は、ISE 1.3 で「ゲスト ロケーション」に名称変更されました。

回避策として、リリース 1.3 へのアップグレード後に、1.2 でハードコードしたものと同一タイムゾーンを 1.3 のゲスト ロケーションとして追加します。これを行うには、ISE 1.3 管理者ポータルから、ゲスト アクセス (Guest Access) > 設定 (Settings) > ゲスト ロケーションと SSID (Guest Locations and SSIDs) を選択して、[ロケーション名 (Location name)] テキストボックスにタイムゾーンを追加して、対応するタイムゾーンを選択し、[追加 (Add)] をクリックして設定を保存します。

プロファイラ設定の記録

プロファイラ サービスを使用する場合、管理者ポータルから、各ポリシー サーバノードのプロファイラ構成を必ず記録してください ([管理 (Administration)] > [システム (System)] > [展開 (Deployment)] > *node* > [プロファイル設定 (Profiling Configuration)])。設定をメモするか、スクリーンショットを取得できます。

インラインポスチャノード設定の記録

アップグレードは、インラインポスチャノード (IPN) に適用されません。ただし、展開に IPN が存在する場合、管理者ポータルから IPN の設定を記録する必要があります ([管理

(Administration)]>[システム (System)]>[展開 (Deployment)]><inline posture node>>[編集 (Edit)])。すべての IPN 設定をメモするか、スクリーンショットを取得します。



第 2 章

さまざまな展開タイプのアップグレード方法

次の異なるタイプの展開のアップグレードを行う方法については、この章の次のセクションを確認してください。

- スタンドアロン展開：スタンドアロン ノードのアップグレード
- 2 ノード展開：2 ノード展開のアップグレード
- 分散展開：分散展開のアップグレード
- [スタンドアロン ノードのアップグレード, 7 ページ](#)
- [2 ノード展開のアップグレード, 10 ページ](#)
- [分散展開のアップグレード, 12 ページ](#)
- [アップグレードプロセスの確認, 16 ページ](#)

スタンドアロン ノードのアップグレード

管理、ポリシーサービス、モニタリングのペルソナを担当するスタンドアロンノードの CLI から `application upgrade` コマンドを実行できます。該当するアップグレードコマンドを実行する前にリモートリポジトリから Cisco ISE ノードのローカルディスクにアップグレードバンドルをコピーして、アップグレードの時間を短縮することを推奨します。または、下に示す `application upgrade prepare` コマンドおよび `application upgrade proceed` コマンドを使用できます。

アップグレードの準備

`application upgrade prepare` コマンドを実行して、アップグレードバンドルをダウンロードしてローカルで抽出できます。このコマンドはリモートリポジトリから Cisco ISE ノードのローカルディスクにアップグレードバンドルをコピーします。

はじめる前に

先に、アップグレード前の注意事項に関する章の説明を必ず読んでください。

手順

- ステップ 1** Cisco ISE コマンドラインインターフェイス (CLI) から、**application upgrade prepare** コマンドを入力します。
このコマンドは、ローカルマシンにアップグレードバンドルをコピーし、MD5 および SHA256 チェックサムを示します。

例 :

```
ise/admin# application upgrade prepare ise-upgradebundle-1.2.x-to-1.3.0.693.x86_64.tar.gz
upgrade
Getting bundle to local machine...
md5: de9e7c83679897f792ad3e9f74879c51
sha256: e3358ca424d977af67f8bb2bb3574b3e559ce9578d2f36c44cd8ba9e6dddfefd
% Please confirm above crypto hash matches what is posted on Cisco download site.
% Continue? Y/N [Y] ?
```

- ステップ 2** Y と入力して続行します。
アップグレードパッケージが抽出されます。次のメッセージが表示されます。

例 :

```
Getting bundle to local machine...
md5: de9e7c83679897f792ad3e9f74879c51
sha256: e3358ca424d977af67f8bb2bb3574b3e559ce9578d2f36c44cd8ba9e6dddfefd
% Please confirm above crypto hash matches what is posted on Cisco download site.
% Continue? Y/N [Y] ?
```

次の作業

アップグレードを実行します。

アップグレードの実行

アップグレードの準備後に、アップグレードを実行して正常に完了する必要があります。アップグレードの実行手順 :

はじめる前に

application upgrade prepare コマンドが実行済みであり、アップグレードを実行する準備ができていることを確認します。

手順

Cisco ISE CLI から、**application upgrade proceed** コマンドを入力します。

例 :

```

ise45/admin# application upgrade proceed
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
STEP 1: Stopping ISE application...
STEP 2: Verifying files in bundle...
-Internal hash verification passed for bundle
STEP 3: Validating data before upgrade...
STEP 4: Taking backup of the configuration data...
STEP 5: Running ISE configuration DB schema upgrade...
- Running db sanity check to fix index corruption, if any...

ISE Database schema upgrade completed.
STEP 6: Running ISE configuration data upgrade...
- Data upgrade step 1/73, NSFUpgradeService(1.2.1.127)... Done in 0 seconds.
- Data upgrade step 2/73, NetworkAccessUpgrade(1.2.1.127)... Done in 0 seconds.
- Data upgrade step 3/73, GuestUpgradeService(1.2.1.146)... Done in 0 seconds.
- Data upgrade step 4/73, NetworkAccessUpgrade(1.2.1.148)... Done in 2 seconds.
- Data upgrade step 5/73, NetworkAccessUpgrade(1.2.1.150)... Done in 2 seconds.
- Data upgrade step 6/73, NSFUpgradeService(1.2.1.181)... Done in 0 seconds.
- Data upgrade step 7/73, NSFUpgradeService(1.3.0.100)... Done in 0 seconds.
- Data upgrade step 8/73, RegisterPostureTypes(1.3.0.170)... Done in 0 seconds.
- Data upgrade step 9/73, ProfilerUpgradeService(1.3.0.187)... Done in 4 seconds.
- Data upgrade step 10/73, GuestUpgradeService(1.3.0.194)... Done in 0 seconds.
- Data upgrade step 11/73, NetworkAccessUpgrade(1.3.0.200)... Done in 0 seconds.
- Data upgrade step 12/73, GuestUpgradeService(1.3.0.208)... Done in 1 seconds.
- Data upgrade step 13/73, GuestUpgradeService(1.3.0.220)... Done in 0 seconds.
- Data upgrade step 14/73, RBACUpgradeService(1.3.0.228)... Done in 14 seconds.
- Data upgrade step 15/73, NetworkAccessUpgrade(1.3.0.230)... Done in 3 seconds.
- Data upgrade step 16/73, GuestUpgradeService(1.3.0.250)... Done in 0 seconds.
- Data upgrade step 17/73, NetworkAccessUpgrade(1.3.0.250)... Done in 0 seconds.
- Data upgrade step 18/73, RBACUpgradeService(1.3.0.334)... Done in 9 seconds.
- Data upgrade step 19/73, RBACUpgradeService(1.3.0.335)... Done in 9 seconds.
- Data upgrade step 20/73, ProfilerUpgradeService(1.3.0.360)... ..Done in 143 seconds.
- Data upgrade step 21/73, ProfilerUpgradeService(1.3.0.380)... Done in 3 seconds.
- Data upgrade step 22/73, NSFUpgradeService(1.3.0.401)... Done in 0 seconds.
- Data upgrade step 23/73, NSFUpgradeService(1.3.0.406)... Done in 0 seconds.
- Data upgrade step 24/73, NSFUpgradeService(1.3.0.410)... Done in 1 seconds.
- Data upgrade step 25/73, RBACUpgradeService(1.3.0.423)... Done in 0 seconds.
- Data upgrade step 26/73, NetworkAccessUpgrade(1.3.0.424)... Done in 0 seconds.
- Data upgrade step 27/73, RBACUpgradeService(1.3.0.433)... Done in 1 seconds.
- Data upgrade step 28/73, EgressUpgradeService(1.3.0.437)... Done in 0 seconds.
- Data upgrade step 29/73, NSFUpgradeService(1.3.0.438)... Done in 0 seconds.
- Data upgrade step 30/73, NSFUpgradeService(1.3.0.439)... Done in 0 seconds.
- Data upgrade step 31/73, CdaRegistration(1.3.0.446)... Done in 1 seconds.
- Data upgrade step 32/73, RBACUpgradeService(1.3.0.452)... Done in 15 seconds.
- Data upgrade step 33/73, NetworkAccessUpgrade(1.3.0.458)... Done in 0 seconds.
- Data upgrade step 34/73, NSFUpgradeService(1.3.0.461)... Done in 0 seconds.
- Data upgrade step 35/73, CertMgmtUpgradeService(1.3.0.462)... Done in 1 seconds.
- Data upgrade step 36/73, NetworkAccessUpgrade(1.3.0.476)... Done in 0 seconds.
- Data upgrade step 37/73, TokenUpgradeService(1.3.0.500)... Done in 1 seconds.
- Data upgrade step 38/73, NSFUpgradeService(1.3.0.508)... Done in 0 seconds.
- Data upgrade step 39/73, RBACUpgradeService(1.3.0.509)... Done in 16 seconds.
- Data upgrade step 40/73, NSFUpgradeService(1.3.0.526)... Done in 0 seconds.
- Data upgrade step 41/73, NSFUpgradeService(1.3.0.531)... Done in 0 seconds.
- Data upgrade step 42/73, MDMUpgradeService(1.3.0.536)... Done in 0 seconds.
- Data upgrade step 43/73, NSFUpgradeService(1.3.0.554)... Done in 0 seconds.
- Data upgrade step 44/73, NetworkAccessUpgrade(1.3.0.561)... Done in 0 seconds.
- Data upgrade step 45/73, CertMgmtUpgradeService(1.3.0.615)... Done in 0 seconds.
- Data upgrade step 46/73, CertMgmtUpgradeService(1.3.0.616)... Done in 22 seconds.
- Data upgrade step 47/73, CertMgmtUpgradeService(1.3.0.617)... Done in 1 seconds.
- Data upgrade step 48/73, OcspserviceUpgradeRegistration(1.3.0.617)... Done in 0 seconds.
- Data upgrade step 49/73, NSFUpgradeService(1.3.0.630)... Done in 0 seconds.
- Data upgrade step 50/73, NSFUpgradeService(1.3.0.631)... Done in 0 seconds.
- Data upgrade step 51/73, CertMgmtUpgradeService(1.3.0.634)... Done in 0 seconds.
- Data upgrade step 52/73, RBACUpgradeService(1.3.0.650)... Done in 7 seconds.
- Data upgrade step 53/73, CertMgmtUpgradeService(1.3.0.653)... Done in 0 seconds.
- Data upgrade step 54/73, NodeGroupUpgradeService(1.3.0.655)... Done in 0 seconds.
- Data upgrade step 55/73, RBACUpgradeService(1.3.0.670)... Done in 4 seconds.
- Data upgrade step 56/73, ProfilerUpgradeService(1.3.0.670)... ..Done in 175 seconds.

```

```

- Data upgrade step 57/73, ProfilerUpgradeService(1.3.0.675)... Done in 0 seconds.
- Data upgrade step 58/73, NSFUpgradeService(1.3.0.676)... Done in 0 seconds.
- Data upgrade step 59/73, AuthzUpgradeService(1.3.0.676)... Done in 0 seconds.
- Data upgrade step 60/73, GuestAccessUpgradeService(1.3.0.676)... ..Done in 123 seconds.
- Data upgrade step 61/73, NSFUpgradeService(1.3.0.694)... Done in 0 seconds.
- Data upgrade step 62/73, ProvisioningRegistration(1.3.0.700)... Done in 0 seconds.
- Data upgrade step 63/73, RegisterPostureTypes(1.3.0.705)... Done in 0 seconds.
- Data upgrade step 64/73, CertMgmtUpgradeService(1.3.0.727)... Done in 0 seconds.
- Data upgrade step 65/73, CertMgmtUpgradeService(1.3.0.808)... Done in 1 seconds.
- Data upgrade step 66/73, NSFUpgradeService(1.3.0.810)... Done in 0 seconds.
- Data upgrade step 67/73, RBACUpgradeService(1.3.0.834)... Done in 18 seconds.
- Data upgrade step 68/73, ProfilerUpgradeService(1.3.0.844)... ..Done in 86 seconds.
- Data upgrade step 69/73, GuestAccessUpgradeService(1.3.0.855)... Done in 1 seconds.
- Data upgrade step 70/73, NSFUpgradeService(1.3.0.858)... Done in 0 seconds.
- Data upgrade step 71/73, NSFUpgradeService(1.3.0.861)... Done in 0 seconds.
- Data upgrade step 72/73, GuestAccessUpgradeService(1.3.0.862)... Done in 0 seconds.
- Data upgrade step 73/73, ProvisioningUpgradeService(1.3.105.181)... Done in 17 seconds.
STEP 7: Running ISE configuration data upgrade for node specific data...
STEP 8: Running ISE M&T DB upgrade...
ISE Database Mnt schema upgrade completed.

Gathering Config schema(CEPM) stats ....
Gathering Operational schema(MNT) stats ....
Stopping ISE Database processes...
% NOTICE: The appliance will reboot twice to upgrade software and ADE-OS. During this time
progress of the upgrade is visible on console. It could take up to 30 minutes for this to
complete.
Rebooting to do Identity Service Engine upgrade...

```

次の作業

[アップグレードプロセスの確認, \(16 ページ\)](#)

2 ノード展開のアップグレード

application upgrade prepare コマンドおよび application upgrade proceed コマンドを使用して、2 ノード展開をアップグレードします。手動でノードの登録を解除して、再登録する必要はありません。アップグレードソフトウェアは自動的にノードを登録解除し、新しい展開に移行します。2 ノード展開をアップグレードする場合、最初にセカンダリ管理ノード（ノード B）だけをアップグレードする必要があります。セカンダリ ノードのアップグレードを完了したら、プライマリ

ノード（ノード A）をアップグレードします。次の図に示すような展開の設定の場合、このアップグレード手順を続けることができます。

図 1: Cisco ISE リリース 1.2.x、2ノード管理展開



はじめる前に

- プライマリ管理ノードから設定および運用データのオンデマンドバックアップを手動で実行します。
- 管理ペルソナがプライマリ管理ノードでのみイネーブルである場合、アップグレードプロセスによりセカンダリ管理ノードを最初にアップグレードすることが求められるので、アップグレード手順を開始する前にセカンダリノードのペルソナをイネーブルにします。
または、2ノード展開で1つの管理ノードのみがある場合は、セカンダリノードの登録を解除します。両方のノードがスタンドアロンノードになります。両方のノードをスタンドアロンノードとしてアップグレードし、リリース 1.3 へのアップグレード後に、展開をセットアップします。
- モニタリングペルソナが1つのノードのみでイネーブルの場合、次に進む前に他のノードのモニタリングペルソナをイネーブルにします。

手順

- ステップ 1** CLI からセカンダリノード（ノード B）をアップグレードします。
アップグレードプロセスで、自動的にノード B が展開から削除され、アップグレードされます。再起動すると、ノード B はプライマリノードになります。
- ステップ 2** ノード A をアップグレードします。
アップグレードプロセスで、自動的にノード A が展開に登録され、セカンダリノードになります。
- ステップ 3** 新規の展開で、ノード A をプライマリノードに昇格させます。

アップグレードが完了した後、ノードに古いモニタリングログが含まれる場合、これらのノード上で **application configure ise** コマンドを実行し、5（データベースの統計情報の更新）を選択します。

次の作業

[アップグレードプロセスの確認](#)、(16 ページ)

分散展開のアップグレード

初めに、セカンダリ管理ノードをリリース 1.3 にアップグレードします。たとえば、次の図に示すように、1つのプライマリ管理ノード（ノードA）、1つのセカンダリ管理ノード（ノードB）、1つのインラインポスチャノード（IPN）（ノードC）、および4つのポリシーサービスノード（PSN）（ノードD、ノードE、ノードF、およびノードG）、1つのプライマリモニタリングノード（ノードH）、および1つのセカンダリモニタリングノード（ノードI）を含む展開がセットアップされている場合、次のアップグレード手順に進むことができます。



(注) アップグレードの前にノードを手動で登録解除する必要はありません。 **application upgrade prepare** コマンドおよび **application upgrade proceed** コマンドを使用して、リリース 1.3 にアップグレードします。アップグレードプロセスは自動的にノードを登録解除し、新しい展開に移行します。アップグレードの前に手動でノードの登録をキャンセルする場合は、アップグレードプロセスを開始する前に、プライマリ管理ノードのライセンスファイルがあることを確認します。手元にこのファイルがない場合（たとえば、シスコパートナーベンダーによってライセンスがインストールされた場合）、Cisco Technical Assistance Center に連絡してください。

はじめる前に

- 展開にセカンダリ管理ノードがない場合は、アップグレードプロセスを開始する前に、セカンダリ管理ノードにするポリシーサービスノードを1つ設定します。
- アップグレード前の注意事項に関する章で指定されている手順をすでに読んで完了していることを確認します。
- 全 Cisco ISE 展開をアップグレードする場合は、ドメインネームシステム（DNS）のサーバ解決（順ルックアップおよび逆ルックアップ）が必須です。そうでない場合、アップグレードは失敗します。

手順

ステップ 1 CLI からセカンダリ管理ノード（ノードB）をアップグレードします。アップグレードプロセスで、自動的にノードBが展開から登録解除され、アップグレードされます。再起動すると、ノードBは、新しい展開のプライマリノードになります。各展開でモニタ

リングノードが少なくとも1つ必要になるため、アップグレードプロセスは古い展開の該当ノードでイネーブルになっていなくても、ノードBのモニタリングペルソナをイネーブルにします。ポリシーサービスペルソナが古い展開のノードBでイネーブルであった場合、この設定は新しい展開へのアップグレード後も維持されます。

ステップ2 モニタリングノードの1つ（ノードH）を新規展開にアップグレードします。セカンダリモニタリングノードの前にプライマリモニタリングノードをアップグレードすることをお勧めします（古い展開でプライマリ管理ノードがプライマリモニタリングノードとしても動作している場合にはこれは不可能です）。プライマリモニタリングノードが起動し、新規展開からログを収集します。この詳細は、プライマリ管理ノードのダッシュボードから表示できます。

古い展開でモニタリングノードが1つだけある場合は、アップグレードする前に、古い展開のプライマリ管理ノードであるノードAのモニタリングペルソナをイネーブルにします。ノードペルソナの変更により、Cisco ISEアプリケーションが再起動します。ノードAが再起動するまで待ちます。新規展開にモニタリングノードをアップグレードすると、運用データを新しい展開に移行する必要があるために、他のノードよりも時間がかかります。

新規展開のプライマリ管理ノードであるノードBが、古い展開でイネーブルにされたモニタリングペルソナを持たない場合、モニタリングペルソナをディセーブルにします。ノードペルソナの変更により、Cisco ISEアプリケーションが再起動します。プライマリ管理ノードが起動するまで待ちます。

ステップ3 次に、ポリシーサービスノード（ノードD、E、F、およびG）をアップグレードします。複数のPSNを同時にアップグレードできますが、すべてのPSNを同時にアップグレードした場合、ネットワークでダウンタイムが発生します。

PSNがノードグループクラスタの一部である場合、PSNをPANから登録解除し、スタンドアロンノードとしてアップグレードし、新規展開のPANに登録する必要があります。

アップグレード後に、新規展開のプライマリノード（ノードB）にPSNが登録され、プライマリノード（ノードB）からのデータがすべてのPSNに複製されます。PSNではそのペルソナ、ノードグループ情報、およびプローブのプロファイリング設定が維持されます。

ステップ4 プライマリ管理ノードからIPNノード（ノードC）を登録解除します。

ステップ5 IPNノード（ノードC）を新規展開のプライマリ管理ノード（ノードB）に登録します。

ステップ6 古い展開に2番目のモニタリングノード（ノードI）がある場合、次のことを行う必要があります。

a) 古い展開のプライマリノードであるノードAのモニタリングペルソナをイネーブルにします。展開でモニタリングノードは少なくとも1つ必要です。古い展開から第2のモニタリングノードをアップグレードする前に、プライマリノード自身でこのペルソナをイネーブルにします。ノードペルソナの変更により、Cisco ISEアプリケーションが再起動します。プライマリISEノードが再起動するまで待ちます。

b) セカンダリモニタリングノード（ノードI）を古い展開から新しい展開にアップグレードします。

プライマリ管理ノード（ノードA）を除いて、他のすべてのノードが新規展開にアップグレードされている必要があります。

ステップ7 最後に、プライマリ管理ノード（ノード A）をアップグレードします。このノードは、セカンダリ管理ノードとしてアップグレードされ、新規展開に追加されます。セカンダリ管理ノード（ノード A）を新規展開のプライマリ ノードに昇格させることができます。アップグレードが完了した後、アップグレードされたモニタリング ノードに古いログが含まれる場合、**application configure ise** コマンドを実行し、該当するモニタリング ノードで 11（M&T データベースの統計情報の更新）を選択します。

図 2: アップグレード後の *Cisco ISE* 展開



正常なアップグレードの CLI トランスクリプト

次の例は、正常なセカンダリ管理ノードのアップグレードの CLI トランスクリプトです。

```
ise74/admin# application upgrade proceed
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
-Checking VM for minimum hardware requirements
STEP 1: Stopping ISE application...
STEP 2: Verifying files in bundle...
-Internal hash verification passed for bundle
STEP 3: Validating data before upgrade...
STEP 4: De-registering node from current deployment.
STEP 5: Taking backup of the configuration data...
STEP 6: Running ISE configuration DB schema upgrade...
- Running db sanity check to fix index corruption, if any...

ISE Database schema upgrade completed.
STEP 7: Running ISE configuration data upgrade...
- Data upgrade step 1/73, NSFUpgradeService(1.2.1.127)... Done in 0 seconds.
- Data upgrade step 2/73, NetworkAccessUpgrade(1.2.1.127)... Done in 0 seconds.
- Data upgrade step 3/73, GuestUpgradeService(1.2.1.146)... Done in 0 seconds.
- Data upgrade step 4/73, NetworkAccessUpgrade(1.2.1.148)... Done in 3 seconds.
- Data upgrade step 5/73, NetworkAccessUpgrade(1.2.1.150)... Done in 3 seconds.
- Data upgrade step 6/73, NSFUpgradeService(1.2.1.181)... Done in 0 seconds.
- Data upgrade step 7/73, NSFUpgradeService(1.3.0.100)... Done in 0 seconds.
- Data upgrade step 8/73, RegisterPostureTypes(1.3.0.170)... Done in 0 seconds.
- Data upgrade step 9/73, ProfilerUpgradeService(1.3.0.187)... Done in 5 seconds.
- Data upgrade step 10/73, GuestUpgradeService(1.3.0.194)... Done in 1 seconds.
- Data upgrade step 11/73, NetworkAccessUpgrade(1.3.0.200)... Done in 0 seconds.
- Data upgrade step 12/73, GuestUpgradeService(1.3.0.208)... Done in 2 seconds.
- Data upgrade step 13/73, GuestUpgradeService(1.3.0.220)... Done in 0 seconds.
- Data upgrade step 14/73, RBACUpgradeService(1.3.0.228)... Done in 24 seconds.
- Data upgrade step 15/73, NetworkAccessUpgrade(1.3.0.230)... Done in 3 seconds.
- Data upgrade step 16/73, GuestUpgradeService(1.3.0.250)... Done in 0 seconds.
- Data upgrade step 17/73, NetworkAccessUpgrade(1.3.0.250)... Done in 0 seconds.
- Data upgrade step 18/73, RBACUpgradeService(1.3.0.334)... Done in 18 seconds.
- Data upgrade step 19/73, RBACUpgradeService(1.3.0.335)... Done in 18 seconds.
- Data upgrade step 20/73, ProfilerUpgradeService(1.3.0.360)... Done in 221 seconds.
- Data upgrade step 21/73, ProfilerUpgradeService(1.3.0.380)... Done in 4 seconds.
- Data upgrade step 22/73, NSFUpgradeService(1.3.0.401)... Done in 0 seconds.
- Data upgrade step 23/73, NSFUpgradeService(1.3.0.406)... Done in 0 seconds.
- Data upgrade step 24/73, NSFUpgradeService(1.3.0.410)... Done in 1 seconds.
- Data upgrade step 25/73, RBACUpgradeService(1.3.0.423)... Done in 0 seconds.
- Data upgrade step 26/73, NetworkAccessUpgrade(1.3.0.424)... Done in 0 seconds.
- Data upgrade step 27/73, RBACUpgradeService(1.3.0.433)... Done in 2 seconds.
- Data upgrade step 28/73, EgressUpgradeService(1.3.0.437)... Done in 0 seconds.
- Data upgrade step 29/73, NSFUpgradeService(1.3.0.438)... Done in 0 seconds.
- Data upgrade step 30/73, NSFUpgradeService(1.3.0.439)... Done in 0 seconds.
```



```

- Data upgrade step 31/73, CdaRegistration(1.3.0.446)... Done in 2 seconds.
- Data upgrade step 32/73, RBACUpgradeService(1.3.0.452)... Done in 26 seconds.
- Data upgrade step 33/73, NetworkAccessUpgrade(1.3.0.458)... Done in 0 seconds.
- Data upgrade step 34/73, NSFUpgradeService(1.3.0.461)... Done in 0 seconds.
- Data upgrade step 35/73, CertMgmtUpgradeService(1.3.0.462)... Done in 2 seconds.
- Data upgrade step 36/73, NetworkAccessUpgrade(1.3.0.476)... Done in 0 seconds.
- Data upgrade step 37/73, TokenUpgradeService(1.3.0.500)... Done in 1 seconds.
- Data upgrade step 38/73, NSFUpgradeService(1.3.0.508)... Done in 0 seconds.
- Data upgrade step 39/73, RBACUpgradeService(1.3.0.509)... Done in 26 seconds.
- Data upgrade step 40/73, NSFUpgradeService(1.3.0.526)... Done in 0 seconds.
- Data upgrade step 41/73, NSFUpgradeService(1.3.0.531)... Done in 0 seconds.
- Data upgrade step 42/73, MDMUpgradeService(1.3.0.536)... Done in 0 seconds.
- Data upgrade step 43/73, NSFUpgradeService(1.3.0.554)... Done in 0 seconds.
- Data upgrade step 44/73, NetworkAccessUpgrade(1.3.0.561)... Done in 2 seconds.
- Data upgrade step 45/73, CertMgmtUpgradeService(1.3.0.615)... Done in 0 seconds.
- Data upgrade step 46/73, CertMgmtUpgradeService(1.3.0.616)... Done in 22 seconds.
- Data upgrade step 47/73, CertMgmtUpgradeService(1.3.0.617)... Done in 2 seconds.
- Data upgrade step 48/73, OcspserviceUpgradeRegistration(1.3.0.617)... Done in 0 seconds.
- Data upgrade step 49/73, NSFUpgradeService(1.3.0.630)... Done in 0 seconds.
- Data upgrade step 50/73, NSFUpgradeService(1.3.0.631)... Done in 0 seconds.
- Data upgrade step 51/73, CertMgmtUpgradeService(1.3.0.634)... Done in 0 seconds.
- Data upgrade step 52/73, RBACUpgradeService(1.3.0.650)... Done in 8 seconds.
- Data upgrade step 53/73, CertMgmtUpgradeService(1.3.0.653)... Done in 0 seconds.
- Data upgrade step 54/73, NodeGroupUpgradeService(1.3.0.655)... Done in 1 seconds.
- Data upgrade step 55/73, RBACUpgradeService(1.3.0.670)... Done in 4 seconds.
- Data upgrade step 56/73, ProfilerUpgradeService(1.3.0.670)... Done in 0 seconds.
- Data upgrade step 57/73, ProfilerUpgradeService(1.3.0.675)... Done in 315 seconds.
- Data upgrade step 58/73, NSFUpgradeService(1.3.0.676)... Done in 0 seconds.
- Data upgrade step 59/73, AuthzUpgradeService(1.3.0.676)... Done in 11 seconds.
- Data upgrade step 60/73, GuestAccessUpgradeService(1.3.0.676)... Done in 660
seconds.
- Data upgrade step 61/73, NSFUpgradeService(1.3.0.694)... Done in 0 seconds.
- Data upgrade step 62/73, ProvisioningRegistration(1.3.0.700)... Done in 0 seconds.
- Data upgrade step 63/73, RegisterPostureTypes(1.3.0.705)... Done in 0 seconds.
- Data upgrade step 64/73, CertMgmtUpgradeService(1.3.0.727)... Done in 0 seconds.
- Data upgrade step 65/73, CertMgmtUpgradeService(1.3.0.808)... Done in 1 seconds.
- Data upgrade step 66/73, NSFUpgradeService(1.3.0.810)... Done in 1 seconds.
- Data upgrade step 67/73, RBACUpgradeService(1.3.0.834)... Done in 31 seconds.
- Data upgrade step 68/73, ProfilerUpgradeService(1.3.0.844)... Done in 0 seconds.
- Data upgrade step 69/73, GuestAccessUpgradeService(1.3.0.855)... Done in 517
seconds.
- Data upgrade step 70/73, NSFUpgradeService(1.3.0.858)... Done in 3 seconds.
- Data upgrade step 71/73, NSFUpgradeService(1.3.0.861)... Done in 0 seconds.
- Data upgrade step 72/73, GuestAccessUpgradeService(1.3.0.862)... Done in 0 seconds.
- Data upgrade step 73/73, ProvisioningUpgradeService(1.3.105.181)... Done in 55 seconds.
STEP 8: Running ISE configuration data upgrade for node specific data...
STEP 9: Making this node PRIMARY of the new deployment. When other nodes are upgraded it
will be added to this deployment.
STEP 10: Running ISE M&T DB upgrade...
ISE Database Mnt schema upgrade completed.

Gathering Config schema(CEPM) stats .....
Gathering Operational schema(MNT) stats ....
Stopping ISE Database processes...
% NOTICE: The appliance will reboot twice to upgrade software and ADE-OS. During this time
progress of the upgrade is visible on console. It could take up to 30 minutes for this to
complete.
Rebooting to do Identity Service Engine upgrade...
次の例は、正常な PSN ノードのアップグレードの CLI トランスクリプトです。

ise/admin# application upgrade ise-upgradebundle-1.2.x-to-1.3.0.876.x86_64.tar.gz sftp
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes
Generating configuration...
Saved the ADE-OS running configuration to startup successfully

Getting bundle to local machine...
G
md5: 8810b57c8531c2a2b20e871014e970f0

sha256: 576d0c859866cfc424711c4a0d395e55cb87c32566de8bb074bcb57cba8ff891
% Please confirm above crypto hash matches what is posted on Cisco download site.
% Continue? Y/N [Y] ? Y
Unbundling Application Package...

```

```
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
STEP 1: Stopping ISE application...
STEP 2: Verifying files in bundle...
-Internal hash verification passed for bundle
STEP 3: Validating data before upgrade...
STEP 4: De-registering node from current deployment.
STEP 5: Taking backup of the configuration data...
STEP 6: Registering this node to primary of new deployment...
STEP 7: Downloading configuration data from primary of new deployment...
STEP 8: Importing configuration data...
STEP 9: Running ISE configuration data upgrade for node specific data...
STEP 10: Running ISE M&T DB upgrade...
ISE Database Mnt schema upgrade completed.
No gather stats needed as this is not PAP or MNT node

Stopping ISE Database processes...
% NOTICE: The appliance will reboot twice to upgrade software and ADE-OS. During this time
progress of the upgrade is visible on console. It could take up to 30 minutes for this to
complete.
Rebooting to do Identity Service Engine upgrade...
```

次の作業

[アップグレードプロセスの確認, \(16 ページ\)](#)

アップグレードプロセスの確認

アップグレードが正常に行われたかどうかを確認するには、次のいずれかを実行します。

- `ade.log` ファイルでアップグレードプロセスを確認します。 `ade.log` ファイルを表示するには、Cisco ISE CLI から次のコマンドを入力します。 **show logging system ade/ADE.log**
- **show version** コマンドを実行し、ビルドバージョンを検証します。
- すべてのサービスが実行していることを確認するために、 **show application status ise** コマンドを入力します。

構成データベースの問題でアップグレードが失敗すると、変更は自動的にロールバックされます。詳細については、第4章「Cisco ISE アップグレードの障害からの回復」の章を参照してください。



第 3 章

リリース 1.3 でのゲスト サービスの変更

ゲスト サービス管理は、リリース 1.3 で簡素化されました。設定は、管理者ポータル の [ゲスト アクセス (Guest Access)] メニュー下に集中しています。ISE 1.2 と 1.3 リリース間で Cisco ISE Web ポータルにいくつかの変更があります。この章では、リリース 1.2 から 1.3 にアップグレードする場合に認識しておく必要がある、アップグレードの考慮事項と依存関係を示します。

- [管理者ポータルの変更, 17 ページ](#)
- [その他のポータル関連の変更, 33 ページ](#)
- [ポリシー関連の変更, 35 ページ](#)

管理者ポータルの変更

次の表に、管理者ポータルの変更点、および UI ナビゲーションパスと変更情報を示します。詳細については、『*Cisco ISE Administration Guide, Release 1.3*』を参照してください。

リリース 1.2 のオブジェク ト名	リリース 1.2 の UI ナビゲー ションパス	リリース 1.3 のオブジェク ト名	リリース 1.3 の UI ナビゲー ションパス	変更情報
Language Template (言 語テンプレ ート)	[管理 (Administration)] > [Web ポー タル管理 (Web Portal Management)] > [設定 (Settings)]> [ポータル (Portal)]> [言語テン プレート (Language Template)]	言語 (Languages)	[ゲスト アク セス (Guest Access)]> [設定 (Configure)] > [ゲスト ポータル (Guest Portals)]また は [スポン サーポータル (Sponsor Portals)]> [編集 (Edit)] > [ポータル ページのカス タマイズ (Portal Page Customization)] > [言語 (Languages)]	リリース 1.3 では、各ポータルタイプで、ポータルのユーザに対するテキスト表示に使用できる、15 の言語がサポートされています。これらの言語は、個別のプロパティファイルとして使用できます。これらのファイルは、圧縮された単一の言語ファイル内にまとめてバンドルされています。 リリース 1.2 で作成されたデフォルト以外の言語は、リリース 1.3 に移行されます。ただし、リリース 1.3 で導入されたすべての新しい設定は、プロファイルのデフォルト値が英語で設定されます。これらの値が会社のポリシーと標準に従っていることを確認し、対応する言語でこれらの設定を更新する必要があります。

リリース 1.2 のオブジェクト名	リリース 1.2 の UI ナビゲーションパス	リリース 1.3 のオブジェクト名	リリース 1.3 の UI ナビゲーションパス	変更情報
デバイス登録 (Device Registration)	[管理 (Administration)]> [Web ポータル管理 (Web Portal Management)]> [設定 (Settings)]> [ゲスト (Guest)]> [マルチポータル設定 (Multi-Portal Configuration)]> [ゲストポータル (Guest Portal)]> [編集 (Edit)]> [操作 (Operations)]> [ゲストユーザにデバイス登録を許可 (Guest users should be allowed to do device registration)]	ゲストデバイス登録設定 (Guest Device Registration Settings)	[ゲストアクセス (Guest Access)]> [設定 (Configure)]> [ゲストポータル (Guest Portals)]> [作成/編集/複製 (Create/Edit/Duplicate)]> [ポータル動作とフロー設定 (Portal Behavior and Flow Settings)]> [ゲストデバイス登録設定 (Guest Device Registration Settings)]	リリース 1.3 では、ゲストデバイスの自動登録のチェックボックスがオンである場合は、デバイスは自動的にエンドポイント ID グループに追加され、ゲスト ID がそのデバイスと自動的に関連付けられます。

リリース 1.2 のオブジェク ト名	リリース 1.2 のUIナビゲー ションパス	リリース 1.3 のオブジェク ト名	リリース 1.3 のUIナビゲー ションパス	変更情報
時間プロファ イル (Time Profiles) およ びゲストロー ル (Guest Role)		ゲストタイプ (Guest Types)	[ゲストアク セス (Guest Access)]> [設定 (Configure)] > [ゲストタ イプ (Guest Types)]	

リリース 1.2 のオブジェク ト名	リリース 1.2 の UI ナビゲー ションパス	リリース 1.3 のオブジェク ト名	リリース 1.3 の UI ナビゲー ションパス	変更情報
	<p>[管理 (Administration)] > [Web ポータル管理 (Web Portal Management)] > [設定 (Settings)]> [ゲスト (Guest)]> [時間プロフィール (Time Profiles)]</p> <p>[管理 (Administration)] > [Web ポータル管理 (Web Portal Management)] > [設定 (Settings)]> [ゲスト (Guest)]> [ゲストロール設定 (Guest Roles Configuration)]</p> <p>[管理 (Administration)] > [Web ポータル管理 (Web Portal Management)] > [スポンサーグループ (Sponsor Groups)]> [スポンサーグループ (Sponsor Group)]> [ゲ</p>			<p>次のゲストタイプが、リリース 1.3 でデフォルトで使用可能です。</p> <ul style="list-style-type: none"> • 日次 (Daily) : デフォルト設定では、1 ~ 5 日間程度のネットワークアクセスが許可されます。 • 週次 (Weekly) : デフォルト設定では、2 週間のネットワークアクセスが許可されます。 • 請負業者 (Contractor) : デフォルト設定では、最長 1 年のネットワークアクセスが許可されます。 <p>リリース 1.3 のゲストタイプは、リリース 1.2 のデータ要素であるスポンサーグループ、ゲストロールおよび時間プロフィールで形成されています。これら 3 種類のデータ要素の組み合わせを使用して、リリース 1.3 ではゲストタイプが作成されます。リリース 1.2 でゲストロールが認可ポリシーで使用されている場合、対応するゲストタイプがリリース 1.3 で作成されます。</p> <p>これらのデータ要素がリリース 1.2 のポリシーで使用されていない場合は、その要素のゲストタイプは、リリース 1.3 で作成されません。</p> <p>アップグレードプロセスでは、関連付けられたアクティブゲストがない時間プロフィールは移行されません。時間プロフィールをリリース 1.3 で利用可能にする場合は (ゲストタイプ)、アップグレード前にゲストアカウントを作</p>

リリース 1.2 のオブジェク ト名	リリース 1.2 の UI ナビゲー ションパス	リリース 1.3 のオブジェク ト名	リリース 1.3 の UI ナビゲー ションパス	変更情報
	スト ロール (Guest Roles)]			成し、これを必要な時間プロファ イルに関連付け、アクティブ化する 必要があります。 (注) FromFirstLogin 時間プロ ファイルはリリース 1.3 では使用できません。こ の時間プロファイルは、 初回ログイン時に開始す るアクセス時間を許可す るために使用されていま した。1日のネットワー クアクセスを許可する代 わりに、Daily ゲスト タ イプを使用できます。
アクティブな ゲストロール (Activated Guest Role)	[管理 (Administration)] > [Web ポータ ル管理 (Web Portal Management)] > [設定 (Settings)]> [ゲスト (Guest)]> [ゲストロー ル設定 (Guest Roles Configuration)]	ゲストにゲス トポータルの バイパスを許 可する (Allow guest to bypass the Guest portal)	[ゲスト アク セス (Guest Access)]> [設定 (Configure)] > [ゲスト タ イプ (Guest Type)]> [作 成/編集 (Create / Edit)]	リリース 1.2 では、Activated Guest ID グループに属するゲストは、使 用しているデバイス上のネイティ ブ サプリカントに認証情報を提供 することで、ゲストポータルをバ イパスしてネットワークにアクセ スすることが可能です。リリース 1.3 では、[ゲストにゲストポータ ルのバイパスを許可する (Allow guest to bypass the Guest portal)] オ プション ([ゲストタイプ (Guest Type)] 設定の下) をイネーブルに して、ゲストが認証情報を有線/無 線のサプリカントまたはVPN クラ イアントに提供することで、ゲス トポータルをバイパスしネット ワークにアクセスするようになり ます。

リリース 1.2 のオブジェクト名	リリース 1.2 の UI ナビゲーションパス	リリース 1.3 のオブジェクト名	リリース 1.3 の UI ナビゲーションパス	変更情報
オプションデータ 1~5 (Optional Data 1-5)	[管理 (Administration)]>[Web ポータル管理 (Web Portal Management)]>[設定 (Settings)]>[ゲスト (Guest)]>[言語テンプレート (Language Template)]	カスタムフィールド (Custom Fields)	[ゲスト アクセス (Guest Access)]>[設定 (Configure)]>[ゲスト タイプ (Guest Type)]>[作成/編集 (Create / Edit)]	リリース 1.2 では、スポンサーは代替電子メールアドレスまたは誕生日 (オプションデータ) などのゲストの付加情報を取得することができました。リリース 1.3 では、オプションデータは、カスタムフィールドと呼ばれ、[Guest Type] 設定下に表示されます。
時間制限 (Time Restrictions)	[管理 (Administration)]>[Web ポータル管理 (Web Portal Management)]>[設定 (Settings)]>[ゲスト (Guest)]>[時間プロファイル (Time Profiles)]	最大アクセス時間 (Maximum Access Time)	[ゲスト アクセス (Guest Access)]>[設定 (Configure)]>[ゲスト タイプ (Guest Types)]>[作成/編集 (Create / Edit)]>[最大アクセス時間 (Maximum Access Time)]	リリース 1.2 では、時間制限を設定できませんが (ゲストのアクセスを許可できない時間を指定)、リリース 1.3 ではアクセス時間を設定できます (ゲストのアクセスを許可できる時間を指定)。

リリース 1.2 のオブジェク ト名	リリース 1.2 の UI ナビゲー ションパス	リリース 1.3 のオブジェク ト名	リリース 1.3 の UI ナビゲー ションパス	変更情報
デバイス登録 ポータル制限 (Device Registration Portal Limit)	[管理 (Administration)] > [Web ポータ ル管理 (Portal Management)] > [設定 (Settings)]> [ゲスト (Guest)]> [ポータル ポ リシー (Portal Policy)]	ゲストが登録 可能な最大デ バイス数 (Maximum devices guests can register)	[ゲスト アク セス (Guest Access)]> [設定 (Configure)] > [ゲスト タ イプ (Guest Type)]> [作 成/編集 (Create / Edit)]> [ロ グオン オプ ション (Login Options)]	—

リリース 1.2 のオブジェクト名	リリース 1.2 の UI ナビゲーションパス	リリース 1.3 のオブジェクト名	リリース 1.3 の UI ナビゲーションパス	変更情報
スポンサーグループ (Sponsor Groups)	[管理 (Administration)] > [Web ポータル管理 (Web Portal Management)] > [スポンサーグループ (Sponsor Groups)]	スポンサーグループ (Sponsor Groups)	[ゲスト アクセス (Guest Access)]> [設定 (Configure)] > [スポンサーグループ (Sponsor Groups)]	リリース 1.3 のスポンサーグループは次のデフォルトのスポンサーグループを含みます。 <ul style="list-style-type: none"> • ALL_ACCOUNTS • GROUP_ACCOUNTS • OWN_ACCOUNTS Active Directory を設定し、リリース 1.3 へのアップグレード後に Active Directory ドメインに結合した場合、AD 外部グループが存在します。 <p>アップグレードプロセスでは、一部のスポンサーグループが移行されません。ゲストロールの作成に使用されないスポンサーグループは移行されません。この変更の結果、リリース 1.3 へのアップグレード後に一部のスポンサー（内部データベース ユーザまたは Active Directory ユーザ）は、ログインできなくなる可能性があります。ログインが失敗したスポンサーのスポンサーグループマッピングを確認する必要があります。適切なスポンサーグループにスポンサーをマッピングします。</p>
スポンサーグループポリシー (Sponsor Group Policy)	[管理 (Administration)] > [Web ポータル管理 (Web Portal Management)] > [スポンサーグループポリシー (Sponsor Group Policy)]	—	—	1.3 から削除されました。ISE 1.3 のスポンサーグループには、ユーザおよび AD グループマッピングとこれらのユーザのアクセス許可が含まれます。

リリース 1.2 のオブジェク ト名	リリース 1.2 の UI ナビゲー ションパス	リリース 1.3 のオブジェク ト名	リリース 1.3 の UI ナビゲー ションパス	変更情報
スポンサーグループアクセス許可 (Sponsor Group Permissions)	[管理 (Administration)]> [Web ポータル管理 (Web Portal Management)]> [スポンサーグループ (Sponsor Groups)]> [スポンサーグループ (Sponsor Group)]> [認可レベル (Authorization Levels)]	スポンサーアクセス許可 (Sponsor Permissions)	[ゲストアクセス (Guest Access)]> [設定 (Configure)]> [スポンサーグループ (Sponsor Groups)]> [作成/編集 (Create / Edit)]> [スポンサーアクセス許可 (Sponsor Permissions)]	

リリース 1.2 のオブジェク ト名	リリース 1.2 の UI ナビゲー ションパス	リリース 1.3 のオブジェク ト名	リリース 1.3 の UI ナビゲー ションパス	変更情報
				<p>次のフィールドが変更されました。</p> <ul style="list-style-type: none"> • ログインを許可 (Allow Login) : リリース 1.3 で削除されました。 • 単一アカウントの作成 (Create Single Account) : リリース 1.2 の [単一アカウントの作成 (Create Single Account)] オプションは、リリース 1.3 で [既知のユーザ (Known User)] オプションに置き換わります。リリース 1.2 と同様に、リリース 1.3 では、スポンサーが複数のランダムアカウントを作成して、CSV ファイルからゲストの詳細をインポートできます。 • 電子メールの送信 (Send Email) : リリース 1.3 では、このオプションはスポンサーポータルでデフォルトで利用可能であり、すべてのスポンサーは、電子メールによってゲスト認証情報を送信できます。 • SMS 送信 (Send SMS) : リリース 1.3 では、[ゲスト認証情報の SMS 通知を送信する (Send SMS notifications with guest credentials)] オプションがあります。 • アカウント開始時間 (Account Start Time) : リリース 1.3 では、[開始日を n 日より先にできない (Start date cannot be more than n days into the future)] オプションがあります。

リリース 1.2 のオブジェク ト名	リリース 1.2 の UI ナビゲー ションパス	リリース 1.3 のオブジェク ト名	リリース 1.3 の UI ナビゲー ションパス	変更情報
				<ul style="list-style-type: none"> • アカウントの最大期間 (Maximum Duration of Account) : リリース 1.3 では、このオプションは [ゲストタイプ (Guest Type)] 設定 ([ゲスト アクセス (Guest Access)] > [設定 (Configure)] > [ゲスト タイプ (Guest Types)] > [作成/編集 (Create/Edit)] > [最大アクセス時間 (Maximum Access Time)] > [最大アカウント有効期間 (Maximum account duration)]) の下で利用可能です。 • ゲスト詳細の印刷を許可 (Allow Printing Guest Details) : リリース 1.3 では、このオプションはスポンサーポータルでデフォルトで利用可能であり、すべてのスポンサーは、ゲストの詳細を印刷できます。
タイムゾーン (Time Zone)	[管理 (Administration)] > [Web ポータル管理 (Web Portal Management)] > [設定 (Settings)] > [ゲスト (Guest)] > [時間プロファイル (Time Profiles)]	ゲストロケーション (Guest Locations)	[ゲスト アクセス (Guest Access)] > [設定 (Settings)] > [ゲストロケーションと SSID (Guest Locations and SSIDs)]	リリース 1.3 のゲストロケーションは、リリース 1.2 のゲストアカウントから取得されます。リリース 1.2 でゲストを作成する場合、ゲストのタイムゾーンを関連付けます。このタイムゾーンが、リリース 1.3 でゲストロケーションを作成するために使用され、これらの場所がそれぞれのゲストグループに関連付けられます。

リリース 1.2 のオブジェクト名	リリース 1.2 の UI ナビゲーションパス	リリース 1.3 のオブジェクト名	リリース 1.3 の UI ナビゲーションパス	変更情報
ゲストアカウント消去設定 (Guest Account Purge Settings)	[管理 (Administration)]> [Web ポータル管理 (Web Portal Management)]> [設定 (Settings)]> [一般 (General)]> [消去 (Purge)]	期限切れゲストアカウントの消去スケジュール (Schedule purge of expired guest accounts)	[ゲストアクセス (Guest Access)]> [設定 (Settings)]> [ゲストアカウント消去ポリシー (Guest Account Purge Policy)]	—
ゲストユーザー名ポリシー (Guest Username Policy)	[管理 (Administration)]> [Web ポータル管理 (Web Portal Management)]> [設定 (Settings)]> [ゲスト (Guest)]> [ユーザー名ポリシー (Username Policy)]	ゲストユーザー名ポリシー (Guest Username Policy)	[ゲストアクセス (Guest Access)]> [設定 (Settings)]> [ゲストユーザー名ポリシー (Guest Username Policy)]	アップグレード中に、ゲストユーザー名ポリシーが変更されることがあります。ゲストユーザー名ポリシーを確認し、標準に準拠していることを確認する必要があります。 リリース 1.2 のデフォルトのゲストユーザー名ポリシーに加えたすべての変更は、リリース 1.3 のカスタムポリシーとして移行されます。ゲストユーザー名でサポートされている特殊文字は、リリース 1.2 と 1.3 では異なり、サポートされている特殊文字は、カスタムエントリとして移行されます。

リリース 1.2 のオブジェクト名	リリース 1.2 の UI ナビゲーションパス	リリース 1.3 のオブジェクト名	リリース 1.3 の UI ナビゲーションパス	変更情報
ゲストパスワードポリシー (Guest Password Policy)	[管理 (Administration)]> [Web ポータル管理 (Web Portal Management)]> [設定 (Settings)]> [ゲストパスワードポリシー (Guest Password Policy)]	ゲストパスワードポリシー (Guest Password Policy)	[ゲストアクセス (Guest Access)]> [設定 (Settings)]> [ゲストパスワードポリシー (Guest Password Policy)]	アップグレード中に、ゲストパスワードポリシーが変更されることがあります。ゲストパスワードポリシーを確認し、標準に準拠していることを確認する必要があります。 リリース 1.2 のデフォルトのゲストパスワードポリシーに加えたすべての変更は、リリース 1.3 のカスタムポリシーとして移行されます。ゲストパスワードでサポートされている特殊文字は、リリース 1.2 と 1.3 では異なり、サポートされている特殊文字は、カスタムエントリとして移行されます。
SMTP サーバの設定 (SMTP Server Settings)	[管理 (Administration)]> [システム (System)]> [設定 (Settings)]> [SMTP サーバ (SMTP Server)]	ゲスト電子メール設定 (Guest Email Settings)	[ゲストアクセス (Guest Access)]> [設定 (Settings)]> [ゲスト電子メールの設定 (Guest Email Settings)] [管理 (Administration)]> [システム (System)]> [設定 (Settings)]> [SMTP サーバ (SMTP Server)]	リリース 1.2 では、SMTP サーバ設定およびゲスト電子メールでの通知設定は同じ UI ページにありました。リリース 1.3 では、SMTP サーバ設定、およびゲストへの電子メールでの通知は 2 つの異なる場所で利用可能です (リリース 1.3 の UI ナビゲーションパスを参照)。

リリース 1.2 のオブジェクト名	リリース 1.2 の UI ナビゲーションパス	リリース 1.3 のオブジェクト名	リリース 1.3 の UI ナビゲーションパス	変更情報
パーソナルデバイスポータル (Personal Devices Portals)	[管理 (Administration)] > [Web ポータル管理 (Web Portal Management)] > [設定 (Settings)]	デバイスポータルの設定 (Configure Device Portals)	[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)]	次のパーソナルデバイスのポータルが、リリース 1.3 でデフォルトで利用可能です。 <ul style="list-style-type: none"> • ブラックリストポータル • BYODポータル • クライアントプロビジョニングポータル • MDMポータル • デバイスポータル <p>リリース 1.2 でデフォルトのゲストポータルインターフェイスとポートを変更した場合、1.2 のゲストポータルに対応する新しい BYODポータルおよびクライアントプロビジョニングポータルがリリース 1.3 で作成されます。認可プロファイルも適宜更新されます。</p>
ポータルテーマ (Portal Theme)	[管理 (Administration)] > [Web ポータル管理 (Web Portal Management)] > [設定 (Settings)]> [一般 (General)]> [ポータルテーマ (Portal Theme)]	ポータルテーマ (Portal Theme)	[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > [ポータル (Portal)]> [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)]	リリース 1.3 では、ポータルのテーマをカスタマイズし、加えた変更を保存する前に表示できます。

リリース 1.2 のオブジェク ト名	リリース 1.2 のUIナビゲー ションパス	リリース 1.3 のオブジェク ト名	リリース 1.3 のUIナビゲー ションパス	変更情報
モバイルに最 適化されたゲ ストポータル (Mobile Optimized Guest Portal)	[管理 (Administration)] > [Web ポータ ル管理 (Web Portal Management)] > [設定 (Settings)]> [ゲスト (Guest)]> [マルチポータ ル設定 (Mutli-Portal Configuration)] > [編集 (Edit)]> [操作 (Operations)] > [モバイル ポータルをイ ネーブルにす る (Enable Mobile Portal)]	—	—	すべてのポータルは、デフォルト でモバイル用に最適化されていま す。使用されているデバイスのタ イプに応じて、モバイルバージョ ンまたはデスクトップバージョン が使用されます。

リリース 1.2 のオブジェクト名	リリース 1.2 の UI ナビゲーションパス	リリース 1.3 のオブジェクト名	リリース 1.3 の UI ナビゲーションパス	変更情報
SMS テキストメッセージ通知 (SMS Text Message Notification)	[管理 (Administration)]>[Web ポータル管理 (Web Portal Management)]>[設定 (Settings)]>[スポンサー (Sponsor)]>[言語テンプレート (Language Template)]	SMS ゲートウェイ設定 (SMS Gateway Settings)	[管理 (Administration)]>[システム (System)]>[設定 (Settings)]>[SMS ゲートウェイ (SMS Gateway)]	リリース 1.3 の SMS ゲートウェイによって、次のことが可能になります。 <ul style="list-style-type: none"> スポンサーが、ゲストのログイン資格情報およびパスワードリセット方法が含まれた SMS 通知を手動でゲストに送信します。 ゲストが、自分自身の登録に成功した後、自分のログイン資格情報が含まれた SMS 通知を自動的に受信します。 ゲストが、自分のゲストアカウントが失効する前に実行するアクションを示す SMS 通知を自動的に受信します。

その他のポータル関連の変更

アップグレード中、すべての Cisco ISE ポータルは、リリース 1.3 に移行されます。

- デフォルトのポータル：リリース 1.3 に移行後にデフォルトのポータルの編集および変更が可能です（ゲスト、スポンサー、デバイスなど）。リリース 1.3 で新たに導入されたすべてのポータル設定がデフォルト値に設定されます。デフォルトポータルのポート、使用可能なインターフェイス、およびポータルテーマの設定は、アップグレード中に維持されます。
- ゲストおよびパーソナルデバイス用のカスタムポータル：Cisco ISE、リリース 1.3 は、ゲストおよび従業員に、新しい合理化されたオンボーディングエクスペリエンスと、多言語のサポートから WYSIWYG へのカスタマイゼーションに至る数多くの新機能による、新しいポータルカスタマイゼーションエクスペリエンスを提供します。リリース 1.3 にアップグレードすると、すべてのカスタムポータルが新しい ISE 1.3 エクスペリエンスに移行します。認識すべきいくつかの考慮事項を次に示します。
 - 以前のリリースの ISE で CSS と HTML を使用して行っていた基本的なルック アンド フィールドのカスタマイズは、1.3 へのアップグレードプロセスによって新しいゲストおよびパーソナルデバイスのフローに移行されます。
 - 基本 HTML およびネイティブ管理ツールを使用して行われたカスタマイズは、適切に移行されます。ゲストのフローを変更するためのカスタム JavaScript を使用したカスタ

マイズは、適切に移行されない場合があります。ISE 1.3 管理者ポータルからこれらのポータルを再作成できます。

- リリース 1.3 に移行されたカスタム ポータルはいずれも編集できません。ロック アンドフィールド、フロー、または機能を変更する場合は、新しいポータルを作成する必要があります (ISE 1.3 管理者ポータルから)。
- ISE 1.2 カスタマーは、多様なポータルのカスタマイズが可能でした。これらのカスタマイズの一部は、ISE 1.3 に予期したとおりに移行しない場合があります。新しく移行されたポータルを実稼働環境で使用する前に、ラボ設定でこれらのポータルを確認することを推奨します。
- 次の場合、ISE 1.3 はゲスト アカウントの作成に失敗します。
 - 1 ISE 1.2 のゲスト ポータルでセルフサービスを許可するように設定した
 - 2 ポータルのカスタマイズ時にタイムゾーン値をハードコードした
 - 3 カスタマイズされたポータルを、ISE 1.3 アップグレードプロセスを使用して ISE 1.3 に移行した

これは、カスタマイズされたポータル内のハードコードされたタイムゾーン値が、ISE 1.3 内のゲストロケーション名に一致しない可能性があるために発生します。ISE 1.2 の「タイムゾーン」は、ISE 1.3 で「ゲストロケーション」に名称変更されました。

回避策として、リリース 1.3 へのアップグレード後に、1.2 でハードコードしたものと同一タイムゾーンを 1.3 のゲストロケーションとして追加します。これを行うには、ISE 1.3 管理者ポータルから、ゲストアクセス (Guest Access) > 設定 (Settings) > ゲストロケーションと SSID (Guest Locations and SSIDs) を選択して、[ロケーション名 (Location name)] テキストボックスにタイムゾーンを追加して、対応するタイムゾーンを選択し、[追加 (Add)] をクリックして設定を保存します。

- ゲストポータル: リリース 1.2 からのすべてのゲストポータルは、リリース 1.3 に移行され、アップグレード後に次のポータルが表示されます。相当する 1.2 ゲストポータルがない場合は、デフォルトの 1.3 ゲストポータルが作成されます。
 - リリース 1.2 の DRW ポータル: リリース 1.3 のホットスポットポータル
 - リリース 1.2 のセルフサービスなしのゲストポータル: リリース 1.3 のスポンサードゲストポータル
 - リリース 1.2 でセルフサービスがイネーブルなゲストポータル: リリース 1.3 のアカウント登録でのゲストポータル
- スポンサーポータル: リリース 1.2 では、次のスポンサーポータル設定を、[ゲストアカウントの管理 (Manage Guest Accounts)] > [設定 (My Settings)] からカスタマイズできます。言語テンプレート、ロケーション、電子メールアドレス、ゲストロール、アカウント有効期間、タイムゾーン、通知言語、およびパスワード設定。リリース 1.3 へのアップグレード後は、スポンサー電子メールアドレスのみが移行され、残りの設定は移行されません。言語設

定をカスタマイズしている場合、リリース 1.3 へのアップグレード後にスポンサー ポータルにログインすると、言語設定は維持されていません。

- BYOD ポータル：次の BYOD ポータルは、リリース 1.2 から移行されます。
 - リリース 1.2 からのデバイス ポータル
 - BYOD 関連の設定があるゲスト ポータル

次のデフォルト BYOD ポータルは、リリース 1.3 にアップグレードした後に作成されます（これらのポータルは、リリース 1.2 では使用できませんでした）。

- デフォルト ブラックリスト ポータル
- デフォルト BYOD ポータル
- クライアント プロビジョニング ポータル：デフォルトのクライアント プロビジョニング (CP) ポータルは、リリース 1.3 にアップグレードしたときに作成されます。

新規 ISE ゲストおよびパーソナル デバイス機能、および管理エクスペリエンスの詳細については、『Cisco Identity Services Engine Admin Guide, Release 1.3』を参照してください。

ポリシー関連の変更

次のポリシーおよびポリシー要素の変更、および強化が、リリース 1.3 で導入されました。

- スポンサー グループ ポリシー：スポンサー グループ ポリシーは Release 1.3 から削除されました。リリース 1.3 のスポンサー グループには、ユーザおよび AD グループ マッピングに加えこれらのユーザのアクセス許可が含まれます。
- 認可プロファイル：リダイレクト URL は 1.3 形式に従ってフォーマットされます。たとえば、ホットスポット ポータルの URL リダイレクトは、
`https://ip:port/guestportal/gateway?sessionID=SessionIDValue&portal=PortalID&action=cwa&type=drw` となります。
- 認可ポリシー：新しい ID グループ（ゲストタイプの ID グループ）を認可ポリシーで使用できます。



第 4 章

アップグレード後の作業

展開のアップグレード後に、この章にリストされているタスクを実行します。

- [アップグレード後の作業, 37 ページ](#)

アップグレード後の作業

次のタスクの詳細については、『*Cisco Identity Services Engine Administrator Guide, Release 1.3*』を参照してください。

- 仮想マシン (VM) 上の Cisco ISE ノードをアップグレードする場合は、VM の電源をオフにして、ゲストオペレーティングシステムを Red Hat Enterprise Linux 6 (64 ビット) に変更し、変更後に VM の電源をオンにします。
- アップグレード後、Cisco ISE リリース 1.3 管理者ポータルにアクセスする前に、ブラウザのキャッシュをクリアしていることを確認し、ブラウザを閉じて、新しいブラウザセッションを開きます。サポート対象のブラウザは次のとおりです。
 - Mozilla Firefox バージョン 31.x ESR、32.x、および 33.x
 - Microsoft Internet Explorer 10.x および 11.x

クライアントブラウザを実行しているシステムに、Adobe Flash Player 11.2.0.0 以降がインストールされている必要があります。

Cisco ISE 管理者ポータルを表示してより良いユーザエクスペリエンスを得るために必要な最小画面解像度は、1280 x 800 ピクセルです。

- Active Directory への外部アイデンティティソースと接続が失われたときに Active Directory を使用する場合は、Active Directory とすべての Cisco ISE ノードを再度結合します。再結合した後に、外部アイデンティティソースのコールフローを実行して、確実に接続します。
 - アップグレード後に、Active Directory 管理者アカウントを使用して Cisco ISE ユーザーインターフェイスにログインした場合、アップグレード時に Active Directory の結合が失わ

れるため、ログインが失敗します。Cisco ISE にログインし、Active Directory と結合するには、内部管理者アカウントを使用する必要があります。

- アップグレード前に Cisco ISE への管理アクセスに対して証明書ベースの認証をイネーブルにしている ([管理 (Administration)] > [管理者アクセス (Admin Access)])、Active Directory をアイデンティティソースとして使用している場合、アップグレード時に Active Directory 結合が失われるため、アップグレード後に ISE ログインページを起動できません。この問題が発生した場合、次のコマンドを使用して、Cisco ISE CLI から、セーフモードで ISE アプリケーションを起動します。

application start ise safe

このコマンドにより、Cisco ISE ノードはセーフモードで起動します。

- 1 内部管理者アカウントを使用して Cisco ISE ユーザーインターフェイスにログインします。
- 2 Cisco ISE と Active Directory の結合

- プライマリ管理ノードから Cisco ISE CA 証明書およびキーのバックアップを取得し、セカンダリ管理ノードで復元します。これにより、PAN に障害が発生し、セカンダリ管理ノードを PAN に昇格する場合に、セカンダリ管理ノードが外部 PKI ルート CA または下位 CA として動作するようになります。
- 分散展開を 1.2 から 1.3 にアップグレードした後に、次の両方の条件が満たされた場合は、プライマリ管理ノードのルート CA 証明書は信頼できる証明書ストアに追加されません。
 - セカンダリ管理ノード (1.2 展開のプライマリ管理ノード) は 1.3 展開でプライマリ管理ノードに昇格されている
 - セッションサービスはセカンダリノードでディセーブルになっている

これにより、次のエラーで認証が失敗する可能性があります。

- Unknown CA in chain during a BYOD flow
- OCSP unknown error during a BYOD flow

これらのメッセージは、失敗した認証の [ライブ ログ (Live Logs)] ページの [詳細 (More Details)] リンクをクリックすると表示されます。

回避策として、展開をアップグレードし、1.3 展開で PAN になるようにセカンダリ管理ノードをプロモートした後に、管理者ポータルから新しい ISE ルート CA 証明書チェーンを作成します (管理 (Administration) > 証明書 (Certificates) > 証明書署名要求 (Certificate Signing Requests) > ISE ルート CA 証明書チェーンの置換 (Replace ISE Root CA certificate chain) を選択)。

- 外部アイデンティティソースとして RSA SecurID サーバを使用する場合は、RSA のノード秘密をリセットします。
- アップグレードプロセスでは、ポリシー サービス ノード グループ設定が保持されます。Cisco ISE リリース 1.3 はノードグループ間の通信にマルチキャストアドレスを使用させ

ん。1.3 へのアップグレード後、ノードグループは移行されますが、マルチキャストアドレスは適用されなくなったため、ノードグループページに表示されません。

- ポスチャサービスをイネーブルにした場合は、アップグレード後にプライマリ管理ノードからポスチャの更新を実行します。
- SNMP の設定で、手動で [元のポリシー サービス ノード (Originating Policy Services Node)] の値を設定した場合、この設定はアップグレード中に失われます。この値を再設定します。
- アップグレード後にプロファイラ フィード サービス更新して、最新 OUI がインストールされているようにします。
- クライアント プロビジョニング ポリシーで使用されているネイティブのサブリカント プロファイルをチェックして、ワイヤレス SSID が正しいことを確認します。iOS デバイスの場合、接続対象ネットワークが非表示の場合は、[iOS の設定 (iOS Settings)] エリアで [ターゲット ネットワーク 非表示時にイネーブルにする (Enable if target network is hidden)] チェック ボックスをオンにします。
- ログインが失敗したスポンサーのスポンサー グループ マッピングを確認します。適切なスポンサー グループにスポンサーをマッピングします。アップグレードプロセスによってすべてのスポンサー グループが移行されるわけではないため、一部のスポンサーがスポンサーポータルにログインできない場合があります。
- アップグレードプロセスでは、デフォルトのポータル (ゲスト、スポンサー、デバイスなど) およびカスタム ポータルが移行されます。これらのポータルが使用する、ポートおよび使用可能インターフェイスの設定は、アップグレード中に維持されます。デフォルトのポータルを編集できますが、カスタム ポータルは読み取り専用です。必要としないデフォルトのポータルは、削除できます。
- (パーソナル デバイスにのみ適用) デバイスを特定のデバイス グループに静的に割り当てている場合、リリース 1.3 にアップグレードした後に、必ず BYOD ポータル設定を更新し ([管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [BYOD (BYOD)] > [編集 (Edit)])、[エンドポイント ID グループ (Endpoint identity group)] フィールドで適切なデバイスグループを選択します。そうしないと、アップグレード後に、デバイスがネットワークに接続するときに、デバイスはデフォルトの RegisteredDevices グループに割り当てられます。認可ポリシー規則はこのデバイス グループの変更に伴って更新されないため、要求は正常に処理されません。
- エンドポイントの削除ポリシー設定 ([管理 (Administration)] > [ID の管理 (Identity Management)] > [設定 (Settings)] > [エンドポイントの削除 (Endpoint Purge)]) を確認します。
- ゲストのユーザ名、パスワード、および削除ポリシーを確認します ([ゲストアクセス (Guest Access)] > [設定 (Settings)]) 。
- 電子メール設定、お気に入りレポート、データ削除設定を再設定します。
- ゲスト関連ワークフロー用の認可ポリシーを確認し、ポリシー条件で 사용되는ゲストグループを更新します。

- ワイヤレス LAN コントローラのゲスト ローカル Web 認証の設定を更新します。Web リダイレクト外部サーバ URL を、`https://<ip>:<port>/portal/PortalSetup.action?portal=<portalId>` に置き換える必要があります。[ポータルの設定とカスタマイズ (Portal Settings and Customization)] ページで [ポータルテスト URL (Portal test URL)] をクリックして、この URL を取得します ([ゲストアクセス (Guest Access)] > [設定 (Configure)] > [ポータル (Portal)] > [作成/編集 (Create/Edit)] > [ポータルの設定とカスタマイズ (Portal Settings and Customization)])。
- 必要とする特定のアラームのしきい値またはフィルタを確認します。すべてのアラームは、アップグレード後にデフォルトでイネーブルになります。
- 必要に応じてレポートをカスタマイズします。古い展開でレポートをカスタマイズした場合は、加えた変更が、アップグレードプロセスによって上書きされます。



第 5 章

アップグレードの障害からの回復

この章では、アップグレードの障害からの回復時に必要な作業について説明します。

アップグレードソフトウェアは、いくつかの検証を実行します。アップグレードで障害が発生した場合は、画面に表示される指示に従い、回復してリリース 1.3 へのアップグレードを成功させます。

また、アップグレードで、セカンダリ管理ノードを最初にアップグレードするなど、ノードのアップグレード順序に従わないために障害が発生することがあります。このエラーが発生した場合、このガイドに記載されているアップグレード順序に従って展開をアップグレードできます。

まれに、イメージを再作成し、新規インストールを実行して、データを復元することが必要になる場合があります。アップグレードを開始する前に、Cisco ISE の設定およびモニタリングデータのバックアップが存在することが重要です。構成データベースの障害発生時に自動的に変更のロールバックが試みられますが、構成データおよびモニタリングデータをバックアップしておくことが重要です。



(注) モニタリングデータベースの問題により発生したアップグレードの障害は、自動的にロールバックされません。システムのイメージを手動で再作成し、Cisco ISE、リリース 1.3 をインストールしてから、設定データおよびモニタリングデータを復元する必要があります。

- [アップグレードの障害, 42 ページ](#)
- [アップグレードがバイナリのインストール中に失敗する, 43 ページ](#)

アップグレードの障害

アップグレード中、構成データベーススキーマとデータアップグレードの障害は自動的にロールバックされます。アプライアンスは、最後の既知の正常な状態に戻ります。この場合、次のメッセージがコンソールとログに表示されます。

```
% Warning: The node has been reverted back to its pre-upgrade state.
error: %post(CSCOcpm-os-1.2.0-899.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical
Assistance Center for support.
```

アップグレードの障害を修復し、ノードを元の状態に戻す必要がある場合は、コンソールに次のメッセージが表示されます。

```
% Warning: Do the following steps to revert node to its pre-upgrade state."
error: %post(CSCOcpm-os-1.2.0-899.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical
Assistance Center for support.
```

実際のアップグレードの障害ではない検証エラーが発生した場合は、次のメッセージが表示されます。たとえばセカンダリ PAN のアップグレードの前に PSN をアップグレードしようとする、このエラーが表示されることがあります。このエラーが発生した場合は、このドキュメントで説明されているアップグレードを実行します。

```
STEP 1: Stopping ISE application...
% Warning: Cannot upgrade this node until the standby PAP node is upgraded and running. If
standbyPAP is already upgraded
and reachable ensure that this node is in SYNC from current Primary UI.
Starting application after rollback...
```

```
% Warning: The node has been reverted back to its pre-upgrade state.
error: %post(CSCOcpm-os-1.2.0-899.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical
Assistance Center for support.
```

ADE-OS またはアプリケーションのバイナリ アップグレードが失敗した場合は、リブート後に CLI から **show application status ise** コマンドを実行すると、次のメッセージが表示されます。

```
% WARNING: An Identity Services Engine upgrade had failed. Please consult logs. You have
to reimage and restore
to previous version
```

その他のタイプのすべての障害（アップグレードのキャンセル、コンソールセッションの切断、電源障害など）の場合、元のノードでイネーブルにしていたペルソナに応じて、設定と運用のバックアップイメージを再作成し、復元する必要があります。ノードのイメージを再作成する場合は、イメージを再作成する前に、失敗の原因を確認するために、**backup-logs** CLI コマンドを実行し、リモートリポジトリ内にサポートバンドルを格納することによって、サポートバンドルを生成します。

アップグレードに失敗した場合、アップグレードを再試行する前に、次の操作を実行してください。

- ログを分析します。エラーがないかアプリケーションバンドルを検査します。
- 生成したアプリケーションバンドルを Cisco Technical Assistance Center (TAC) に送信して、問題を特定および解決します。



- (注) SSH 経由でログインし、**show application status ise** コマンドを使用することで、アップグレードの進行状況を表示できます。次のメッセージが表示されます。「%NOTICE: Identity Services Engine upgrade is in progress...」

アップグレードがバイナリのインストール中に失敗する

問題 アプリケーション バイナリのアップグレードはデータベースのアップグレード後に発生します。バイナリのアップグレードで障害が発生すると、コンソールと ADE.log に次のメッセージが表示されます。

% Application install/upgrade failed with system removing the corrupted install

解決法 ロールバックまたは回復を行う前に、**backup-logs** コマンドを使用してアプリケーションバンドルを生成し、リモートリポジトリにアプリケーションバンドルを配置します。

解決法 ロールバックするには、以前の ISO イメージを使用して Cisco ISE アプライアンスのイメージを再作成し、バックアップファイルからデータを復元します。アップグレードを再試行するには、毎回新しいアップグレードバンドルが必要です。

- **解決法** ログを分析します。エラーがないかアプリケーションバンドルを検査します。
- **解決法** 生成したアプリケーションバンドルを Cisco Technical Assistance Center (TAC) に送信して、問題を特定および解決します。

■ アップグレードがバイナリのインストール中に失敗する