Smart Software Manager オンプレミス クイック スタートインストールガイド

バージョン 8 リリース 202006

初版：02/16/2015
最終変更日：2020/7/1

米国本社
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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となります。

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。

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティング システムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムを適応したものです。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。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコおよびその代理店は、このマニュアルに適用できるまたは適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およびその代理店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 IP 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 およびシスコのロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧は http://www.cisco.com/jp/go/trademarks でご確認いただけます。記載されているサードパーティの商標（Java など）は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。（1110R）

The Java logo is a trademark or registered trademark of Sun Microsystems, Inc. in the U.S. or other countries

Cisco Smart Software Manager オンプレミスの導入のためのチェックリスト

SSM オンプレミスをインストールして導入する前に以下のリソースを確認してください。

1. Software.cisco.com から ISO イメージをダウンロードする。
2. １つの専用の IP アドレスの確保（HA クラスタ構成の場合は複数の IP アドレス）
3. 適切なネットマスク
4. DNS (Domain Name Server) アドレス
5. 大文字と小文字、数字、特殊文字を混合した 15 文字以上のパスワード(例えば CiscoAdmin!2345）
6. NTP サーバアドレス

更に、ハードウェア上にインストールする場合は以下のものが必要です。

7. ISO からの USB イメージ
8. 最初に USB から、次にハードディスクからブートする様に設定されたハードウェア BIOS
9. マスターブートレコードを使ってブートする様に設定されたハードウェア BIOS（レガシーBIOS モード）

Smart Software Manager オンプレミス クイック スタート インストール

NOTE: SSM オンプレミスを導入するのに必要な情報は 開始前の準備 を参照してください。

メディアをブートした後、KickStart スクリーンで SSM On-Prem ライセンスサーバソフトウェアをインストールできるようになる前に初期設定値の入力が求められます。この時の入力を完了するために以下の情報が事前に必要です。

- 使用予定のサーバのホスト名
- セキュリティプロファイル(DISA STIG Profile を推奨)
- IP アドレス情報
- ネットマスクまたはサブネットに対応するプレフィクス
- ゲートウェイ IP アドレス
- DNS サーバ IP アドレス

- SSH シェルのパスワード: 大文字と小文字、数字、特殊文字を混合した 15 文字以上のパスワード(例えば CiscoAdmin!2345）

ISO image を以下の手順でインストールします。

次の手順は、ISO イメージをインストールするための、SSM オンプレミス インストール ワークフローを示しています。

ステップ	アクション
ステップ 1	CCO から **ISO イメージ**をダウンロードします。
ステップ 2	オーケストレーション環境ごとに **ISO** を導入します。
ステップ 3	Cisco SSM オンプレミス クイック スタート インストール UI で、以下の必要情報を入力します。 • [ホスト名（Hostname）] を設定します。 • [システム分類（System Classification）] : オプションは [未分類（Unclassified）]（デフォルト）、[部外秘（Confidential）]、[秘密（Secret）]、[最高秘密（Top Secret）] です。オプションを選択すると、この分類がコンソールの [本日のメッセージ（Message of the Day）] バナーに表示されます。 • [FIPS 140-2 モード（FIPS 140-2 Mode）] : 変更不可
ステップ 4	[システムプロファイル（System Profile）] を選択します。 • [標準プロファイル（Standard Profile）] • [DISA STIG プロファイル（DISA STIG Profile）] : OS（CentOS 7.5.1804）が STIG モードに入ることができます。
ステップ 5	ネットワーク環境ごとに **IPv4** や **IPv6** のネットワーク値を入力します。必要な値は次のとおりです。 • アドレス • [ネットマスク/プレフィックス（Netmask / Prefix）] • [ゲートウェイ（Gateway）]
ステップ 6	**DNS** を設定します。
ステップ 7	[OK] をクリックします。
ネットワーク設定を入力すると、SSM オンプレミスのインストールを完了する準備が整います。ステップ 8 に進みます。	
ステップ 8	[システムパスワードの設定（Configure System Password）] のポップアップが表示されます。シェルアクセス用のセキュアな **LINUX SSH パスワード**を入力します。 **注** : これは、UI 管理者パスワードとは異なります。パスワード回復オプションがない

ステップ	アクション
	ため、このパスワードは安全な場所に保管してください。
ステップ 9	**パスワード**を再入力します。
ステップ 10	[OK] をクリックします。 これで初期セットアップは完了です。インストールが完了するまで約 **10～15** 分待ってから、アプリケーションを開きます。

注： インストール後にシステムから ISO イメージをマウント解除し、サーバをリブートすることをお勧めします。SSM オンプレミスシステムが自動的に起動します。

システムプロファイルの選択

SSM オンプレミスは 2 つのプロファイルを提供します。

- **標準プロファイル**：デフォルトの Centos シェルのプロンプトが表示され、オプションでオンプレミスコンソールを使用することもできます。このプロファイルは、通常、国防関連以外の組織に必要な標準のセキュリティ機能を提供します。その機能は次のとおりです。
  - SHA 256 署名キーが追加されたことで、パッチのセキュリティが強化されています。
  - LDAP Secure SSM オンプレミスは、TLS（トランスポート レイヤ セキュリティ）とプレーンテキストログインをサポートしています。LDAP により、ホスト、ポート、bind dn、およびパスワードの正しい設定が強制されます。これらのパラメータが正しくないか、入力されていない場合は、エラーメッセージが表示されます。
  - さらに次のようなセキュリティ機能があります。
    - インストール中にシステムパスワードを更新するように管理者に強制します。
    - 管理者パスワードをデフォルトのパスワードに戻すことを許可しません。
    - ユーザの追加/削除がイベントログに記録されるようになりました。
    - 10 分間アイドル状態になったユーザをシステムから自動的にログアウトします。

- **DISA STIG プロファイル**：シェルに SSH 接続すると、ホワイトリストに登録されたコンソールに配置されます。これにより、ルートアクセスができなくなり、オンプレミスコンソールでホワイトリストに登録されたコンソールコマンドのみを使用するように制限されます。STIP への準拠が必要な場合は、インストール時にこのセキュリティプロファイルを選択します。このプロファイルを選択することで、米国国防総省のセキュリティシステムに必要なセキュリティ機能が有効になります。さらに、このプロファイルの選択することで有効になる機能は、セキュリティ技術導入ガイド（STIG）の標準にも準拠しています。STIG の機能は次のとおりです。
  - ブラウザの証明書管理で、ブラウザの証明書とフレームワークを有効にできます。この機能により、お客様は自分の証明書を、自分のローカルディレクトリからブラウザでインポートできます。

- パスワード管理により、ユーザはパスワードの強度とパスワードのリセット/回復ワークフローを設定できます。セキュリティウィジェットに新しく追加されたタブで、パスワードの有効期限パラメータと特定のパスワード設定を設定し、パスワードの強度を高めることができます。
- ADFS：OAuth ADFS により、OAuth Active Directory フェデレーションサービスによる LDAP のサポートが追加されます。
- Active Directory（OAUTH2）：LDAP グループのインポートについて、Active Directory によるサポートの他に、Active Directory フェデレーションサービスによるサポートが追加されます。