Cisco Smart Software Manager オンプレミス リリースノート

バージョン 8 リリース 202006

リリース日：2020/06/12

Smart Software Manager オンプレミスは、Cisco Smart Software Manager（software.cisco.com）と連携して機能するオンプレミス アセット マネージャです。これにより、スマートライセンス対応の製品インスタンスを、cisco.com でホストされている Cisco Smart Software Manager に直接接続せずに、お客様が製品およびライセンスをオンプレミスで管理できます。

シスコソフトウェアリリースの検索

IP アドレスの後にポート番号を入力して、Web ブラウザ経由で Cisco Smart Software Manager オンプレミスにアクセスします。

たとえば、IP アドレスが 172.16.0.1 の場合は、次のように入力します。

https://172.16.0.1:8443/admin

管理者ポータルにログインすると、[システムヘルス（System Health）] セクションに、実行中の Cisco Smart Software Manager オンプレミスソフトウェアのリリースが表示されます。

「Smart Software Manager サテライト」という製品名を検索して、https://software.cisco.com/download/home からイメージをダウンロードします。Smart Software Manager サテライトのダウンロードページで、[すべてのリリース（All Release）] を展開し、[最新リリース（Latest Release）] を選択します。バージョン 8 ビルド 202006 を見つけます。緑色の .iso イメージにカーソルを合わせると、関連するすべてのドキュメントへのリンクがポップアップで表示されます。

米国本社
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

最新の シスコソフトウェアリリースのダウンロード

「**Smart Software Manager サテライト**」という製品名を検索して、https://software.cisco.com/download/home からイメージをダウンロードします。Smart Software Manager サテライトのダウンロードページで、[すべてのリリース（All Release）] を展開し、[最新リリース（Latest Release）] を選択します。バージョン 8 ビルド 202006 を見つけます。緑色の .iso イメージにカーソルを合わせると、関連するすべてのドキュメントへのリンクがポップアップで表示されます。

バージョン 7 より前のシステムのアップグレード

バージョン 8（SSM オンプレミス）より前の SSMS システムにパッチを適用したりアップグレードしたりする場合は、『Smart Software Manager オンプレミス インストール ガイド』の「付録 2」を参照してください。バージョン 7 より前のシステムのアップグレード。

高可用性（HA）クラスタのアップグレード

高可用性（HA）クラスタのアップグレード手順の詳細については、『Cisco Smart Software オンプレミス 8 インストールガイド』の「付録 5：高可用性（HA）クラスタバージョン 8 のアップグレード」を参照してください。

Cisco SSM オンプレミスリリース

バージョン 8 リリース 202006 の機能の使用方法については、『Cisco Smart Software オンプレミスユーザガイド』を参照してください。「シスコソフトウェアリリースの検索」セクションをご覧ください。

バージョン 8 リリース 202006

このリリースでは、このリリースで予定されていた新機能が追加されています。さらに、重大度 1 と重大度 2 が修正され、脆弱性とエクスポージャーも解決済みです。

新機能

バージョン 8 ビルド 202006 には、次の新機能があります。

- **最大 30 万台のデバイスの製品サポート**

  SSM オンプレミスは、複数のアカウントにまたがって 10 万 ～ 30 万台のデバイスをサポートできます（各アカウントにつき、使用するライセンス数にかかわらず最大 25,000 台の製品をサポート）。30 万台の製品の場合、最大 2 時間かかることに注意してください。

- **トークンの寿命を延長**

  トークンの寿命を最長で 27 年（9999 日）に設定するためのキャパシティを提供します。

- **FIPS 140-2 準拠**

  連邦情報処理標準（FIPS）パブリケーション 140-2 は、情報テクノロジー製品の暗号化モジュールの最小セキュリティ要件を定義する、米国政府標準規格です。FIPS 14-2 認定により、連邦政府のお客様が STIG プロファイルを使用して SSM オンプレミスを導入する際に、FIPS に準拠することができます。

- **同時ユーザのセッション数制限**

  UI とオンプレミスシェルの両方に対して、最大同時ユーザログイン数を制限する STIG セキュリティ設定と機能をサポートします。

- **複数の NTP サーバと、NTP サーバによる認証を使用可能**

  SSM オンプレミスは、認証に Chrony を使用するバックアップ NTP サーバを設定するための追加のキャパシティを提供します。SSM オンプレミスで 2 つの NTP サーバの設定がサポートされることで、1 台目のサーバが応答しなくなった場合に 2 台目のサーバをフォールバックとして機能させることができます。

- **ローカリゼーション機能の強化によりフランス語に対応**

  SSM オンプレミスではローカリゼーション機能を強化し、フランス語に対応しています。

- **プロキシサーバでお客様の証明書を使用可能**

  プロキシサーバでお客様の証明書を使用できるように機能を強化し、プロキシサーバで使用される CA をアップロードできるようになりました。

- **エンドポイント レポート モデル（ERM）の互換性**

  エンドポイント レポート モデルは、ワイヤレス LAN コントローラのバージョン 16.12.1 以降をサポートする特定のコントローラに対するライセンスの二重カウントを軽減するために使用される、スマートライセンスの追加 API です。

バージョン 8 リリース 202006 に含まれる以前のリリースからの重要な修正

- オンプレミス 7-202001 で、プロキシが HTTPS で機能しない（https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvt13065）
- ログアウト後に同期クレデンシャルがクリアされる（https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs94939）
- デバイスの HA スイッチオーバーが失敗する（https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs91758）
- ライセンス不足の重複レコードがイベントログに表示される（https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs78783）

- オンプレミス 7.2 のライセンスページで、HSEC ライセンスの製品詳細情報が不足している（https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs70622）
- 通信が 90 日間ない場合でも、製品からライセンスが解放されない（https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvo04458）
- 強制登録をしても、ライセンスの使用がクリーンアップされない（https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvt03959）
- サードパーティの認証ユーザが、ベアラートークンを生成できない（https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvt35383）
- Chrome でオンプレミスにアクセスできない https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvt27571
- お客様が UI 証明書用の脆弱な暗号証明書をアップロードすると、GUI が使用できなくなる https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvt95777
- Smart Software Manager オンプレミス 7 で、一貫性のないライセンスが表示される https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvt89461
- FP4110 の登録時に有効期限の設定に失敗する https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvt29523
- オンプレミスバージョン 7-201907、または 7-201907 からそれ以降のバージョンへのアップグレードで、不一致がカウントされる https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvu22739
- Syslog サーバに誤設定がある場合、製品の登録が失敗する https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvu32429

解決済みの共通脆弱性

バージョン 8 リリース 202006 では、次の CentOS セキュリティの脆弱性が解決されています。

クリティカル

CESA-2020:0374、CESA-2020:0839、CESA-2020:1016：（CVE-2019-14895、CVE-2019-14901、CVE-2019-14898、CVE-2019-17133、CVE-2019-17666、CVE-2019-19338、CVE-2019-11487、CVE-2018-20169、CVE-2019-12382、CVE-2019-15221、CVE-2019-13233、CVE-2019-11884、CVE-2019-15916、CVE-2019-16746、CVE-2019-9503、CVE 2018-7191、CVE-2019-10207、CVE-2019-13648、CVE-2019-10639、CVE-2019-3901、CVE-2019-10638、CVE-2017-17807、CVE-2015-9289、CVE-2019-18660、CVE-2019-14283、CVE-2018-19985、CVE-2019-11190）

高

CESA-2020:1113：（CVE-2019-9924）

CESA-2020:1011：（CVE-2015-2716）

CESA-2020:1138：（CVE-2018-18751）

CESA-2020:1180：（CVE-2019-13133、CVE-2019-14981、CVE-2019-11472、CVE-2019-13297、CVE-2019-14980、CVE-2019-11470、CVE-2019-13295、CVE-2019-11597、CVE-2019-13135、CVE-2019-13454、CVE-2019-13134、CVE-2018-10805、CVE-2019-11598、CVE-2018-10804、CVE-2018-16749、CVE-2017-11166、CVE-2018-11656、CVE-2019-17540、CVE-2018-13153、CVE-2017-18273、CVE-2019-7397、CVE-2019-7398、CVE-2019-13301、CVE-2019-17541、CVE-2019-13300、CVE-2019-12975、CVE-2019-13306、CVE-2019-12976、CVE-2019-13305、CVE-2019-13304、CVE-2019-12974、CVE-2019-12979、CVE-2019-13309、CVE-2017-18271、CVE-2019-12978、CVE-2019-13307、CVE-2017-12805、CVE-2017-12806、CVE-2018-12599、CVE-2018-10177、CVE-2018-16750、CVE-2018-8804、CVE-2019-15139、CVE-2019-13311、CVE-2019-13310、CVE-2019-16708、CVE-2019-16709、CVE-2018-12600、CVE-2018-9133、CVE-2018-16328、CVE-2019-15140、CVE-2019-15141、CVE-2018-18544、CVE-2019-7175、CVE-2017-18251、CVE-2019-16710、CVE-2017-18252、CVE-2019-16711、CVE-2018-20467、CVE-2019-16712、CVE-2017-18254、CVE 2019-10131、CVE-2019-10650、CVE-2019-9956、CVE-2019-16713、CVE-2019-19948、CVE-2019-19949、CVE-2018-15607、CVE-2017-1000476、CVE-2018-14437、CVE-2018-14434、CVE-2018-14436、CVE-2018-14435）

CESA-2020:1000：（CVE-2019-17042、CVE-2019-17041）

中

CESA-2020:1080：（CVE-2019-3890、CVE-2018-15587）

CESA-2020:1176：（CVE-2017-6519）

CESA-2020:1061：（CVE-2019-6465、CVE-2019-6477、CVE-2018-5745）

CESA-2020:1050：（CVE-2018-4180、CVE-2018-4181、CVE-2018-4700）

CESA-2020:1020：（CVE-2019-5436）

CESA-2020:1022：（CVE-2018-10360）

CESA-2020:0897：（CVE-2020-10531）

CESA-2020:1189：（CVE-2019-12779）

CESA-2020:1021：（CVE-2019-3820）

CESA-2020:1081：（CVE-2018-18066）

CESA-2020:1131：（CVE-2018-20852、CVE-2019-16056）

CESA-2020:0227：（CVE-2019-13734）

CESA-2020:0540：（CVE-2019-18634）

CESA-2020:1181：（CVE-2019-13232）

CESA-2020:1084：（CVE-20191-0197、CVE-2019-10218）

低

CESA-2020:1135：（CVE-2018-1116）

追加のコンテナの更新

CVE-2014-1912、CVE-2011-1521、CVE-2012-0845、CVE-2012-1150、CVE-2011-4940、CVE-2015-7981

CVE-2019-547

CVE-2020-5249、CVE-2020-5247、CVE-2019-16770

CVE-2019-10193、CVE-2019-10192、CVE-2018-11219、CVE-2018-12326、CVE-2018-11218

CVE-2014-10077

CVE-2019-8331、CVE-2018-20676、CVE-2018-20677、CVE-2018-1404、CVE-2016-10735

バージョン 7 リリース 202001

このリリースでは、このリリースで予定されていた新機能が追加されています。さらに、脆弱性の解決、重大度 1 と重大度 2 の修正、および以前のリリースからの重要な修正も含まれています。

新機能

バージョン 7 ビルド 202001 には、次の新機能があります。

このリリースには新機能はありません。

バージョン 7 リリース 202001 で修正済みの重大度 1 および重大度 2

- インストールごとに固有の DB パスワード（HA/バックエンド）（https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs42156）
- コンプライアンス違反を示すライセンス（https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs43179）
- SmartTransport を使用したエクスポート制御が機能しない（https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs40521）
- Firepower でトークンを使用できない https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs47442
- オンプレミス 7-201910 で、改行デリミタなしでトークンが生成される https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs56822
- オンプレミス 7.2 のライセンスページで、HSEC ライセンス製品の詳細情報が不足している https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs70622

解決済みの共通脆弱性

バージョン 7 リリース 202001 では、次の CentOS セキュリティの脆弱性が解決されています。

CESA-2019:3834（CVE-2019-11135、CVE-2018-12207、CVE-2019-0154）

CESA-2019:3872（CVE-2019-0155）

CESA-2019:3976（CVE-2018-19519）

CESA-2019:4326（CVE-2019-18397）

CESA-2019:3979（CVE-2019-14821、CVE-2019-15239）

CESA-2019:4190（CVE-2019-11729、CVE-2019-11745）

CVE-2019-5420
CVE-2019-5419
CVE-2019-5418
CVE-2019-16770

CVE-2019:10193

CVE-2019-10192

CVE-2018-12326

バージョン 7 ビルド 202001 に含まれる、以前のリリースからの重要な修正

CSCvr17188：IPv6 を無効にしても IPv6 が無効化されない

CSCvs40521：EC で SmartTransport をサポートしない

CSCvs47442：Firepower でトークンを使用できない

CSCvs17220：SSM オンプレミスのホスト共通名が、アップグレード後にリセットされる

CSCvr13793：SSM オンプレミスの HTTP のセキュリティヘッダーが欠落している

CSCvs40226：ハードコーディングされたクレデンシャルを使用して設定した CSSM オンプレミスデータベースへの、予期しない読み取り/書き込みアクセス

CSCvr51499：ライセンス階層内の同期のたびにライセンス使用数が増加する

バージョン 7 リリース 201910

このリリースでは、このリリースで予定されていた新機能が追加されています。さらに、脆弱性の解決、重大度 1 と重大度 2 の修正も含まれています。

新機能

バージョン 7 ビルド 201910 には、次の新機能があります。

- **SHA256 署名キー**

  SHA256 署名キーの追加により、パッチセキュリティが強化されました。

- **セキュア LDAP**

  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。ホスト、ポート、bind dn、パスワードの設定が誤っている場合にエラーメッセージを表示することで、適切な設定を強制し、セキュリティを保証します。

- **ADFS：OAuth ADFS**

  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ています。

- **Active Directory**（OAUTH2）：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ています。

  この機能により、LDAP グループのインポートに Active Directory のサポートも追加されます。

- **ブラウザ証明書管理**：ユーザのブラウザ証明書とフレームワークをインストールします。

  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**：パスワード強度の設定、およびパスワードのリセット/回復のワークフロー

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。

- **アカウント管理**：アカウントのロックアウト/管理設定

  不正ログインが特定の回数試行された場合に、アカウントをロックすることができます。システム管理者はそのアカウントのパスワードをリセットできます。

注： このリリースで自動ロック機能が正常に機能するためには、**セカンダリ認証**が設定されている必要があります。

- **製品インスタンスエンジン（PIE）とオンプレミスの統合**

  Tomcat コンテナを Typhan コンテナに置き換えたことで、パフォーマンスと拡張性が向上しています。このアーキテクチャの変更により、将来の拡張が可能なインフラが整備されました。以下の PIE インスタンスのサポートを参照してください。

- **製品インスタンスエンジン（PIE）によるスマートトランスポートのサポート**

  SSM オンプレミスではサポートを拡張し、スマートトランスポートのメッセージを受信するためのエンドポイントを提供することで、スマートに対応できるようになりました。

- **製品インスタンスエンジン（PIE）の登録**

  基本的な製品インスタンスの登録（認可なし）

- **製品インスタンスエンジン（PIE）のサードパーティライセンス**

  この機能により、サードパーティ（Nuance、APNS）に対してライセンスが提供されるため、サードパーティはスマートライセンスを使用して製品を登録できます。そのためには、権限付与タグを設定して「getKeys」要求を作成し、すべての情報を検証する必要があります。

- **セキュリティウィジェットの強化**

  この機能により、セキュリティウィジェット機能が強化され、証明書（「ブラウザ証明書管理」を参照）とパスワードの強化（「パスワード管理」を参照）が可能になります。

- **ハードウェアの最小ディスク容量要件**

  アップグレードされた最小ディスク要件は 100 GB です。

- **製品インスタンスの最大キャパシティの増加**

  製品インスタンスの最大キャパシティが 50,000（アカウントごとの製品インスタンスの最大キャパシティは 25,000）にアップグレードされました。

バージョン 7 リリース 201910 で修正された重大度 1 および 重大度 2

- 要求の通信が失敗した場合、ライセンスが 1 つではなく 4 つインストールされる（https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvq99678）
- HA オンプレミスのデータベース レプリケーションが破損している（https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs17939）

解決済みの共通脆弱性

バージョン 7 リリース 201910 では、次の CentOS セキュリティの脆弱性が解決されています。

- CESA:2019:2091（CVE-2018-16866、CVE-2018-16888、CVE-2018-15686）
- CESA:2019:2197（CVE-2019-9516、CVE-2019-9511、CVE-2019-9513）
- CESA:2019:2027（CVE-2018-18520、CVE-2018-18310、CVE-2018-16062、CVE-2019-7150、CVE-2018-16402、CVE-2018-16403、CVE-2019-7664、CVE-2019-7665、CVE-2018-18521、CVE-2019-7149）
- CESA:2019:2829（CVE-2019-14835、CVE-2019-7222、CVE-2019-3460、CVE-2019-3882、CVE-2019-5489、CVE-2019-11810、CVE-2019-11599、CVE-2019-11833、CVE-2019-3900、CVE-2018-14625、CVE-2018-8087、CVE-2018-16885、CVE-2018-7755、CVE-2018-9516、CVE-2018-9517、CVE-2018-13094、CVE-2018-13095、CVE-2018-15594、CVE-2018-13053、CVE-2018-13093、CVE-2018-18281、CVE-2018-10853、CVE-2019-3459、CVE-2018-9363、CVE-2018-14734、CVE-2018-16658）
- CESA:2019-3055（CVE-2019-3846、CVE-2018-20856、CVE-2019-10126、CVE-2019-9506）
- CESA:2019:2077（CVE-2018-12327）
- CESA: 2019:2046（CVE-2018-19788）
- CESA: 2019:2057（CVE-2018-5741）
- CESA: 2019:2075（CVE-2018-12641、CVE-2018-12697、CVE-2018-1000876）
- CESA: 2019:2181（CVE-2018-16842）
- CESA: 2019:2060（CVE-2019-6470）
- CESA: 2019:2118（CVE-2016-10739）
- CESA: 2019:2047（CVE-2018-14348）
- CESA: 2019:2049（CVE-2018-18585、CVE-2018-18584）
- CESA: 2019:1884（CVE-2019-3862）
- CESA: 2019:2136（CVE-2019-3858、CVE-2019-3861）
- CESA: 2019:2237（CVE-2018-0495、CVE-2018-12404）
- CESA: 2019:2033（CVE-2018-6952、CVE-2016-10713）
- CESA: 2019-2964（CVE-2018-20969、CVE-2019-13638）
- CESA: 2019:2189（CVE-2018-1122）
- CESA: 2019:2030（CVE-2019-9740、CVE-2018-14647、CVE-2019-5010、CVE-2019-9948、CVE-2019-9947）

- CESA: 2019:2110（CVE-2018-16881）
- CESA: 2019:2099（CVE-2019-3880）
- CESA: 2019:2159（CVE-2018-18384）
- CESA: 2019:3197（CVE-2019-1428）
- CESA: 2019:3197（CVE-2019-1428）
- runc（CVE-2019-5736）
- nginx（CVE-2019-9516、CVE-2019-9511、CVE-2019-9513）

バージョン 7 ビルド 201907

新機能

バージョン 7 には次の新機能があります。

- サテライトからオンプレミスへのリブランド

  「SSM サテライト Enhanced Edition」という名称が出現する箇所はすべて、「SSM オンプレミス」に変更されます。
- 連邦政府基準の STIG に準拠した OS：

  STIG 準拠の OS を、CentOS 7 で実行可能なアプリケーションとして出荷します。

  STIG への準拠が必要なお客様が導入および使用できる、SSM オンプレミスのインストールオプションを提供します。
- セキュリティ：

  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。
- 移行スクリプト：

  サテライト 4.x/5.x ～ 6.3 をサポートする移行スクリプト。

  6.3 にアップグレード後、7 のパッチを使用してオンプレミス 7 にアップグレードしてください。
- プラットフォームの健全性：

  管理者ロールで、管理者ポータルからユーザに関する情報を編集できます。

  PAK ファイルライセンスをスマートライセンスに変換するプロセスでのエラー処理が改善されました。
- ローカリゼーション：

  UI のすべてのテキストを、日本語、中国語、韓国語にローカライズしました。

- 高可用性

  アクティブ/スタンバイの高可用性向けの、一般利用可能なリリースです。

  高可用性は、仮想マシン（VM）または物理サーバを二重化して使用することで、ライセンス運用を保護します。これにより、冗長サーバが提供され、ネットワークの可用性が向上します。この機能は、SSM オンプレミス VM の一方をアクティブプロセッサとして設定し、もう一方の VM をスタンバイとして指定した後、これらの VM 間で重要なステート情報を同期します。2 つの VM の初回同期後、高可用性は VM 間のステート情報をダイナミックに維持します。

- ライセンス階層

  拡張 SL ライセンスモデルにより、上位のライセンスを使用して、複数の下位のライセンスを満たすことができます。

  下位階層のライセンスを、上位階層の複数の親によって満たせるようにするサポートが追加されました。

- スマートトランスポートのサポート

  選択された製品で使用される新しい通信エンドポイントを提供します。スマートトランスポートの新しいエンドポイントは、https://< IP アドレス >/SmartTransport です。

解決済みの共通脆弱性

バージョン 7 201907 では、次の CentOS セキュリティの脆弱性が解決されています。

- CESA-2019:1481
- CESA-2019:1235
- CESA-2019:1294
- CESA-2019:1619
- CESA-2019:1587

バージョン 7 リリース 201907 の既知の問題

次の表に、バージョン 7 リリース 201907 における既知の、未解決の問題およびバグをすべて記載します。

1	Firefox での読み込みエラー	CSCvm64119

バージョン 7 リリース 201910 の既知の問題

次の表に、バージョン 7 リリース 201910 における既知の、未解決の問題およびバグをすべて記載します。

1	部分同期では、ライセンス数が減少しない場合があります。不一致を修正するには、完全同期を実行する必要があります。	CSCvr92319
2	CUCM ID の更新失敗：このリリースでは、バージョンが 3.0.13 未満の Java エージェントを使用する製品との互換性の問題があります。該当する製品のリストを以下に示します。 • Cisco Emergency Responder（CER）：Java 2.1.6 • Cisco HyperFlex Systems：Java 1.3.2 • Cisco IoT Field Network Director（FND）：（リリース番号なし） • Cisco Policy Suite（CPS）：Java 1.2 • Cisco SON スイート：Java 1.3.6 • Cisco Webex Meeting Server（CWMS）：Java 2.1.4 • Cisco Wide Area Application Services（WAAS/vWAAS）：2.0.6 • Cisco Unity Connection：Java 2.1.6 • Cisco Unity Express Virtual（vCUE）：Java 2.0.10 • CloudCenter Suite：Java 2.1.4 • Data Center Network Manager（DCNM）：Java 2.1 • Edge and Fog Module（EFM）: Java 2.0.13 • Evolved Programmable Network Manager（EPN-M）：Java 1.2 • Identity Services Engine（ISE）：Java 1.2	CSCvs39279

	• 産業用ネットワーキングディレクタ（IND）：Java 1.2 • Prime Collaboration Provisioning（PCP）Java 1.3.6 • Prime Infrastructure：Java 1.1 • Prime Infrastructure Operations Center Java：（リリース番号なし） • Session Management Edition（SME）：Java 2.1.6 • Stealthwatch Learning Network（SLN）Java 1.2 • Unified Communications Manager（CUCM）Java 2.1.6 • Video Surveillance Manager（VSM）Java jret1.8-11.9.0_192-fcs.x86_64 • Cisco Unified SIP Proxy（CUSP）Java 1.0 および Java 2.0.9	

バージョン 7 リリース 202001 の既知の問題

次の表に、バージョン 7 リリース 202001 における既知の、未解決の問題およびバグをすべて記載します。

1	ユーザウィジェットの AD ユーザにユーザ名が表示されない	CSCvs44010
2	SSO 認証トークンが、スケジュールされた同期の 30 日後に期限切れになっているように見える	CSCvs64165

確立された回避策

製品の互換性

TLS 1.0 を使用する製品をお使いのお客様は、HTTPS を使用して登録できません。サテライト EE への登録には HTTP を使用する必要があります。これは、InfoSec で TLS 1.0 を使用できないことに起因します。これには 1.5 より前のスマートエージェントが該当します。

DNS 回避策

DNS がキックスタートで正しく設定されていない場合、**管理**ワークスペースの [ネットワーク設定（Network Settings）] からは修正できません。SSM サテライトには、**nmtui** というテキストベースの設定ツールが含まれています。このツールを使用して、ネットワーク インターフェイスの設定を編集し、誤った DNS エントリを持つインターフェイスの IP アドレスを修正できます。

DNS を変更するには、次の手順を実行します。

1. SUDO 権限で **nmtui** を実行します。

   ```
   $ sudo nmtui
   ```

   nmtui の代わりに、次のようにネットワークスクリプトをインターフェイスごとに直接編集することもできます。

   ```
   $ sudo vi /etc/sysconfig/network-scripts/ifcfg-ens3
   ```

2. DNS1 = "" のプロパティを正しい DNS IP アドレスに変更します。
3. ネットワークサービスを再起動して、NetworkManager が新しい /etc/resolv_conf を強制的に書き出すようにします。

   ```
   $ sudo systemctl restart network
   ```

4. ケルベロスサービスを再起動して、Atlantis のシステムデータベースを更新します。

   ```
   $ sudo systemctl restart cerberus
   ```

5. SSM サテライトは、LibCurl が DNS エントリを再解決する必要があることを明示的に示していないため、Atlantis を再起動する必要があります。

   ```
   $ sudo systemctl restart satellite
   ```

TAC によるサポート

有効なシスコサービス契約の対象となるお客様、パートナー、リセラー、ディストリビュータであれば、受賞歴を誇る無休のテクニカルサポートサービスをオンラインや電話でご利用いただけます。お客様のニーズを満たすために、TAC ではさまざまなサポートオプションを提供しています。

製品とサービスに関するケースのオープン

次の手順に従って、SSM オンプレミスの製品または問題を登録するためのサポートチケットを開きます。

注： シスコサポートへお問い合わせの際は、リクエストをスムーズに処理するため、Cisco.com のユーザ ID、契約番号、および製品のシリアル番号をあらかじめご用意ください。

ステップ	アクション
ステップ 1	https://mycase.cloudapps.cisco.com/case にアクセスします。
ステップ 2	Support Case Manager の Web ページで、デフォルト設定をすべてそのままにし、ページの左側を下にスクロールして、[新規ケースのオープン（Open New Case）] をクリックします。[サービスオプション（Services Options）] ポップアップが画面の左側に表示されます。
ステップ 3	[製品とサービス（Products and Services）] を選択します。
ステップ 4	タブ画面の右側のセクションで、[ケースのオープン（Open Case）] をクリックします。
ステップ 5	[リクエストタイプ（Request Type）] が [診断および解決（Diagnose and Fix）] に設定されていることを確認し、画面を下にスクロールして [バイパス条件（Bypass Entitlement）] フィールドに移動します。
ステップ 6	[バイパス条件（Bypass Entitlement）] フィールドで、ドロップダウンリストから [ソフトウェアライセンスの問題（Software Licensing Issue）] を選択します。
ステップ 7	[次へ（Next）] をクリックします。
ステップ 8	問題の説明画面で、重大度レベルとして [質問（Ask a Question）] を選択します。
ステップ 9	[タイトル（Title）]、[説明（Description）]、およびすべての**関連情報**を入力します。

ステップ 10	入力した情報を確認し、[ケースの送信（Submit Case）] をクリックします。これで、クエリが送信されました。

ソフトウェアライセンスの問題に関するケースのオープン

CSSM ライセンス（software.cisco.com）のケースを開くには、次の手順に従います。

注： シスコサポートへお問い合わせの際は、リクエストをスムーズに処理するため、Cisco.com のユーザ ID、契約番号、および製品のシリアル番号をあらかじめご用意ください。

ステップ	アクション
ステップ 1	https://mycase.cloudapps.cisco.com/case にアクセスします。
ステップ 2	Support Case Manager の Web ページで、デフォルト設定をすべてそのままにし、ページの左側を下にスクロールして、[新規ケースのオープン（Open New Case）] をクリックします。[サービスオプション（Services Options）] ポップアップが画面の左側に表示されます。
ステップ 3	[ソフトウェアライセンス（Software Licensing）] を選択します。
ステップ 4	下にスクロールして、ニーズに合った [カテゴリ（Category）] を選択します。
ステップ 5	[ケースのオープン（Open Case）] をクリックします。
ステップ 7	[タイトル（Title）] と [説明（Description）] を入力し、オプションフィールドに**すべての関連情報**を入力します。 **注：**画面の右側にあるチャット画面を使用して**チャット**を開始することもできます。
ステップ 8	入力した情報を確認し、[ケースの送信（Submit Case）] をクリックします。これで、ライセンスクエリが送信されました。

スマート ソフトウェア ライセンス（software.cisco.com）

Smart Software Manager にアクセスして、スマートライセンスを追跡および管理します。

- [スマートライセンスに変換（Convert to Smart Licensing）]で、PAK ベースのライセンスをスマートライセンスに変換できます（該当する場合）。

スマートアカウント

Cisco Software Central の [管理（Administration）]セクションに移動して、既存のスマートアカウントを管理するか、選択肢から新しいアカウントを選択して要求します。

- 自分の会社のアカウントにアクセスするには、[既存のスマートアカウントへのアクセスを要求（Request Access to an Existing Smart Account）] に移動します。
- トレーニングとドキュメントについては、こちらをクリックしてください。

エンタープライズライセンス契約（ELA）

ELA Workspace にアクセスし、ELA からライセンスを管理します。

その他のセルフサービスのライセンス機能も利用できます。ハウツービデオやその他の資料については、ヘルプページを参照してください。

緊急のリクエストについては、電話でお問い合わせください。

ケースを更新するには、添付ファイルや更新情報を attach@cisco.com に送信します。その際、電子メールの件名に**ケース番号**を記載してください。エンジニアに電子メールを送信する際に、宛先に licensing@cisco.com を**含めない**でください。