Connected Threat Defense Step by Step設定ガイド(IMSVA)

トレンドマイクロ株式会社

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro InterScan WebManager SCC、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Securing Your Journey to the Cloud、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDIオプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポート プレミアム、Airサポート、Connected Threat Defense、ライトプリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、およびTrend Micro Policy-based Security Orchestrationは、トレンドマイクロ株式会社の登録商標です。
Copyright © 2018 Trend Micro Incorporated. All rights reserved.

製品名の表記について

本ドキュメントにおいては製品名等は以下のように表記します。

- Connected Threat Defense ・・・「CTD」
- Trend Micro Deep Discovery Analyzer ・・・「DDAN」
- Trend Micro Control Manager ・・・「TMCM」
- InterScan Messaging Security Virtual Appliance ・・・「IMSVA」
- Smart Protection Server ・・・「SPS」
- Trend Micro Deep Discovery Inspector ・・・「DDI」
- 不審オブジェクト[Suspicious Object] ・・・「SO」

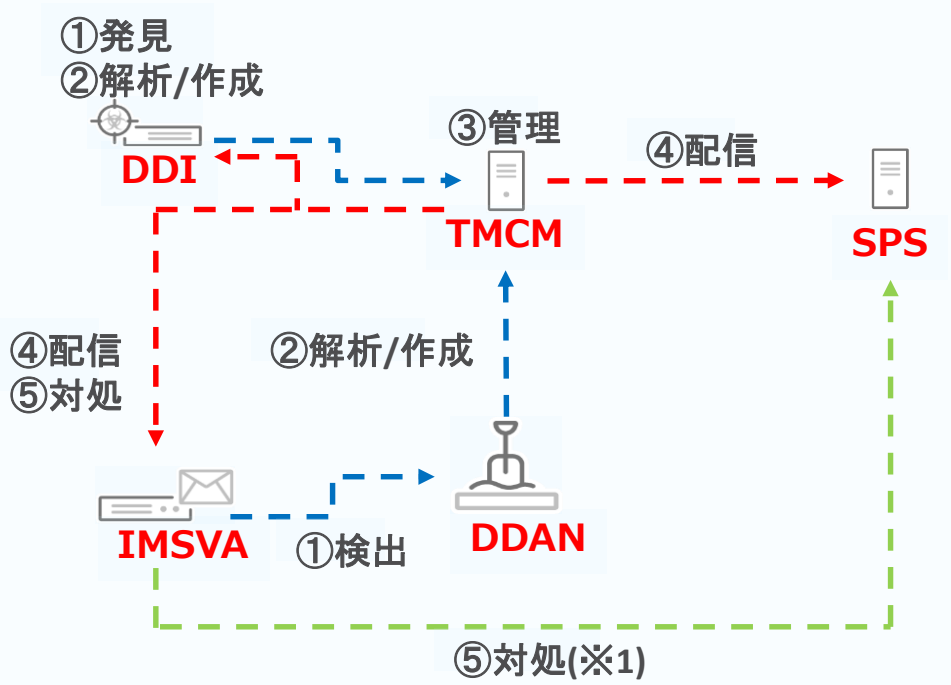
Copyright © 2018 Trend Micro Incorporated. All rights reserved.

本ドキュメントの目的

本ドキュメントはIMSVAを中心としたCTDの設定に特化した資料となります。
CTDの製品間連携の設定をする必要があり、手順は複雑になりがちです。その手順をStep by Stepで解説し、順番通りに設定すればCTDに必要な連携設定は完了します。
また、各画面におけるパラメータの解説はしておりませんので、必要に応じて各製品の管理者ガイド等を参照ください。

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

連携構成図



※1　不審オブジェクト(URL)の検出には、統合SPSまたはスタンドアロンSPSを参照します。
※2　DDIは必須コンポーネントで無いため、利用されていない環境では以降の設定は割愛ください。

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

目次

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP0 事前準備

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP0-1 DDANのAPIキーを取得する

1. DDANのWEBコンソールへアクセスします
https://[DDAN IP or FQDN]/pages/login.php
2. ログインします
3. [ヘルプ] – [バージョン情報] をクリックします
4. 以下の情報(APIキー)を控えます(以降、※1と記載)

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP0-2 TMCMのサービスURLとAPIキーを取得する

1. TMCMのWEBコンソールへアクセスします
https://[TMCM IP or FQDN]/webapp/login.aspx
2. ログインします
3. [運用管理] – [不審オブジェクト] – [配信設定] をクリックします
4. 以下の情報(サービスURL、APIキー)を控えます(以降、※2と記載)

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP1 TMCM-DDANを連携する

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP1-1 DDANをTMCMへ登録する

1. TMCMのWEBコンソールへアクセスします
https://[TMCM IP or FQDN]/webapp/login.aspx
2. ログインします
3. [運用管理] – [管理下のサーバ] をクリックします
4. [サーバの種類]からDeep Discovery Analyzer を選択します
5. [追加]をクリックします

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP1-1 DDANをTMCMへ登録する

6. 以下のパラメータを入力し、[保存]をクリックします

プロキシサーバを介してアクセスする必要がある場合はチェックする

※[管理管理] – [設定] – [プロキシ設定] を事前に設定する必要あり

DDAN WEBコンソールのURLを入力

TMCM上での表示名を入力(任意)

DDAN WEBコンソールのログイン情報を入力

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP1-1 DDANをTMCMへ登録する

7. TMCMに登録されたことを確認します

日時が表示されていれば正常に登録が完了している

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP2 TMCM-DDIを連携する

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP2-1 DDIをTMCMへ登録する

1. DDIのWEBコンソールへアクセスします

https://[DDI IP or FQDN]/

2. ログインします
3. [管理] – [統合製品/サービス] – [Control Manager] をクリックします

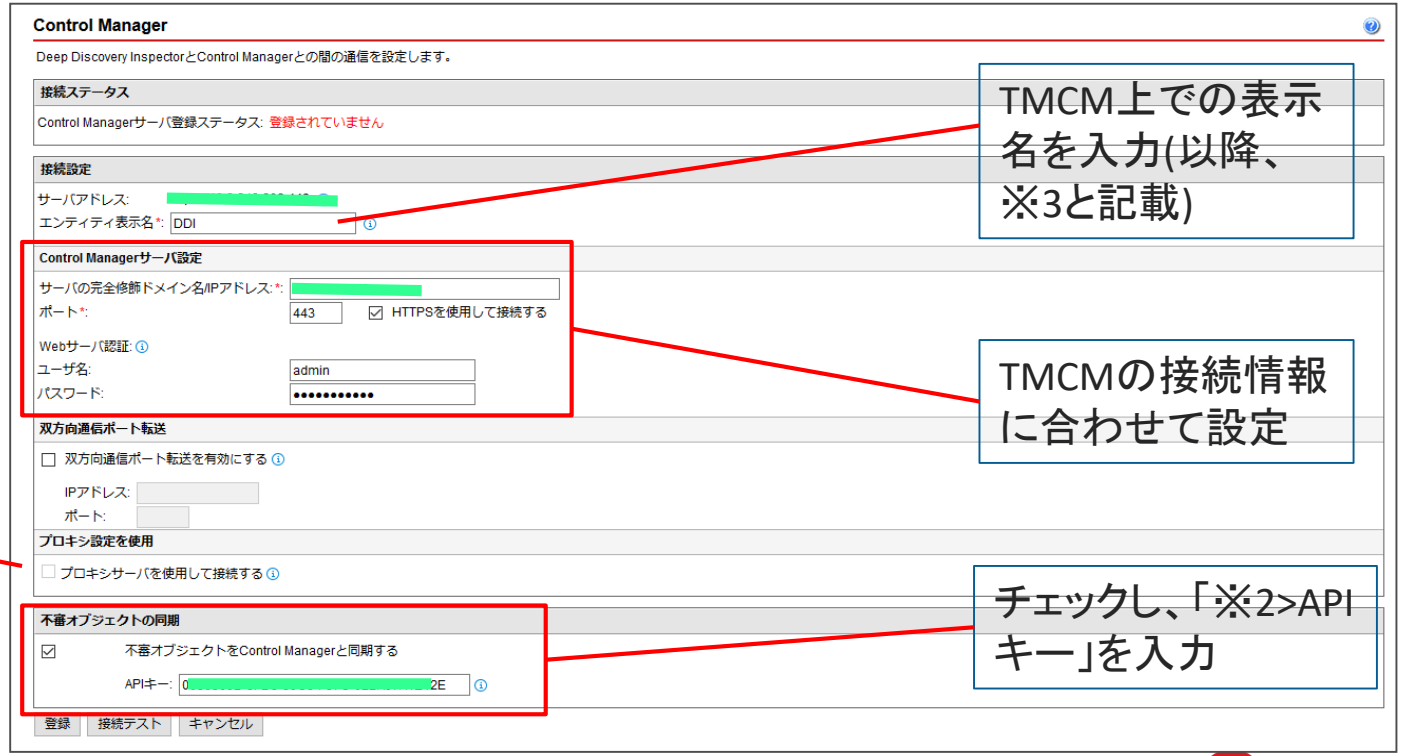
Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP2-1 DDIをTMCMへ登録する

4. 以下のパラメータを入力し、登録をクリックします

プロキシサーバを介してアクセスする必要がある場合はチェックする

※[管理] – [システム設定] – [プロキシ] を事前に設定する必要あり



TMCM上での表示名を入力(以降、※3と記載)

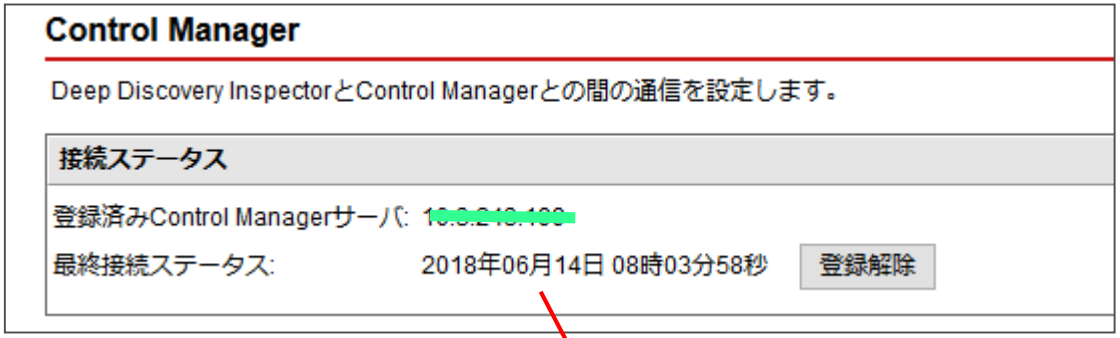
TMCMの接続情報に合わせて設定

チェックし、「※2>APIキー」を入力

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP2-1 DDIをTMCMへ登録する

5. TMCMに登録されたことを確認する



日時が表示されていれば正常に登録が完了している

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP2-2 DDIがTMCMへ登録されたことを確認する

1. TMCMのWEBコンソールへアクセスします
https://[TMCM IP or FQDN]/webapp/login.aspx
2. ログインします
3. [ディレクトリ] – [製品] をクリックします
4. ディレクトリツリーを展開します
5. ディレクトリツリー下に「※3」が登録されていることを確認します

※3の表示を確認し、緑アイコンが表示されていれば正常に登録が完了している

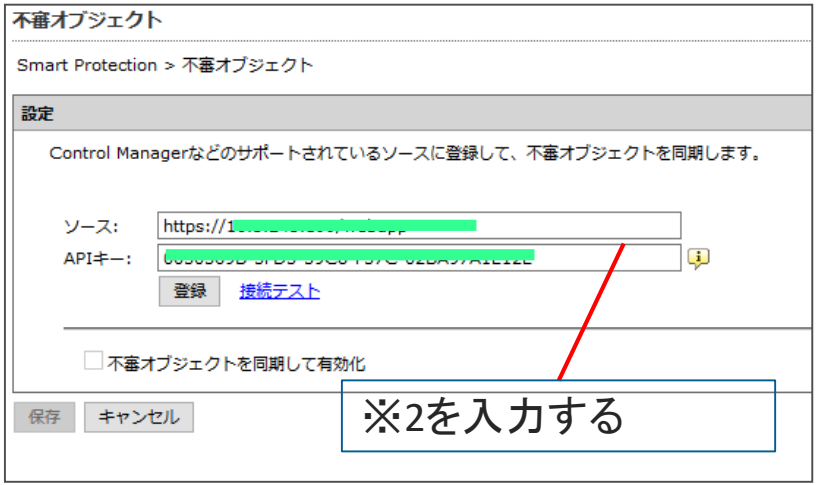
Copyright © 2018 Trend Micro Incorporated. All rights reserved.

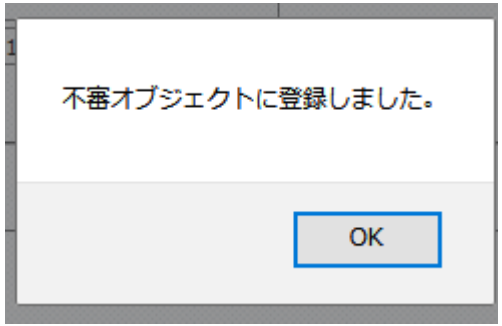
STEP3 TMCM-SPSを連携する

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP3-1 SPS-TMCMを連携する

1. SPSのWEBコンソールへアクセスします
https://[SPS IP or FQDN]:4343/console.imss
2. ログインします
3. [Smart Protection] – [不審オブジェクト] をクリックします
4. 以下の左画面へパラメータを入力し、保存をクリックします。
5. 成功時には以下右画面が表示されるのでOKをクリックします。

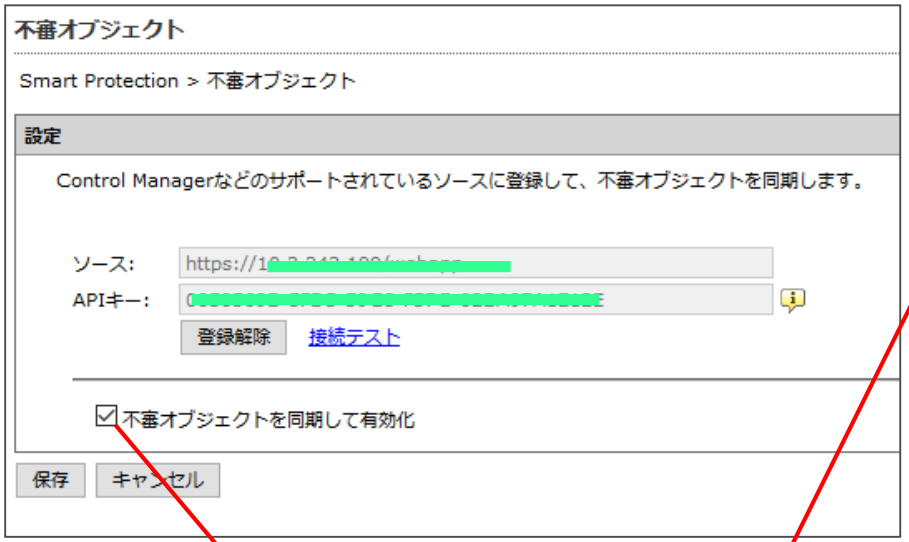


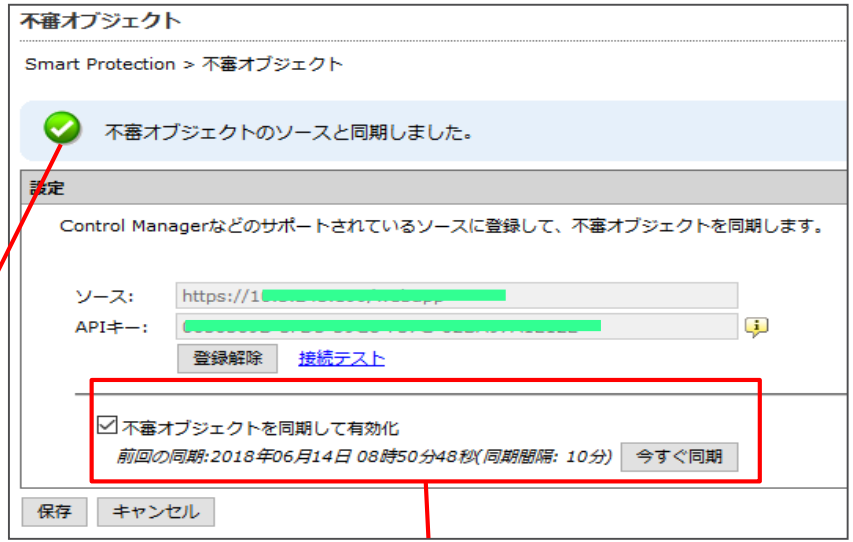


Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP3-1 SPS-TMCMを連携する

6. 以下の左画面へ設定をし、保存をクリックします
7. 以下の右画面にて連携状態の確認をします





チェックする

緑アイコンで成功しています

ボタンをクリックすると同期の日時が更新されます

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP4 IMSVA-SPSを連携する

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

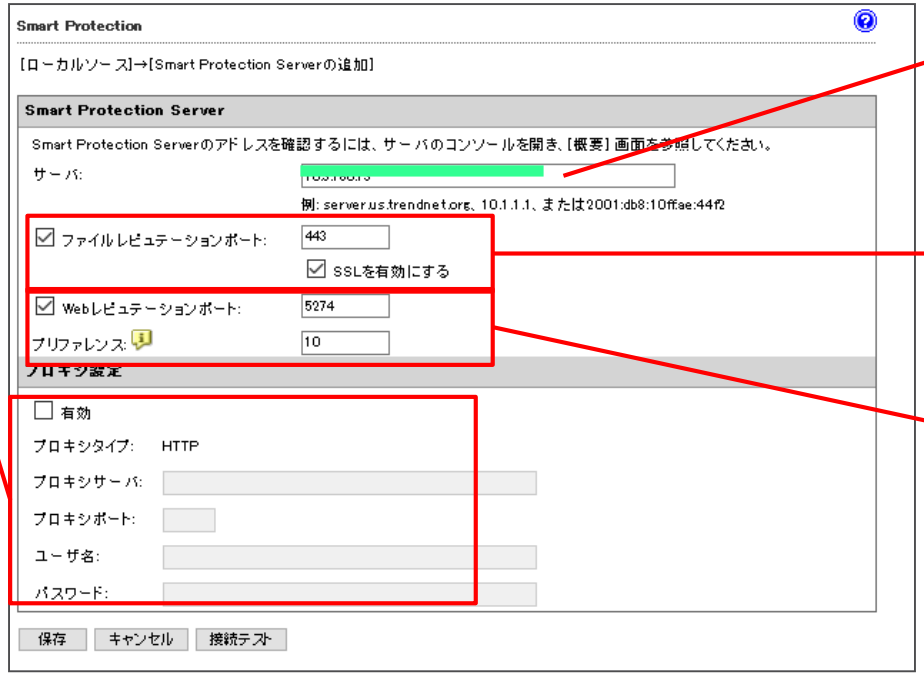
STEP4-1 IMSVAにSPSを登録します

1. IMSVAのWEBコンソールへアクセスします
https://[IMSVA IP or FQDN]:8445/console.imss
2. ログインします
3. [ポリシー] – [Smart Protection] – [ローカルソース] をクリックします
4. 追加をクリックします

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP4-1 IMSVAにSPSを登録します

5. 以下のパラメータを設定し、保存をクリックします



プロキシサーバを介してアクセスする必要がある場合はチェックする

SPSのIP or FQDNを設定する

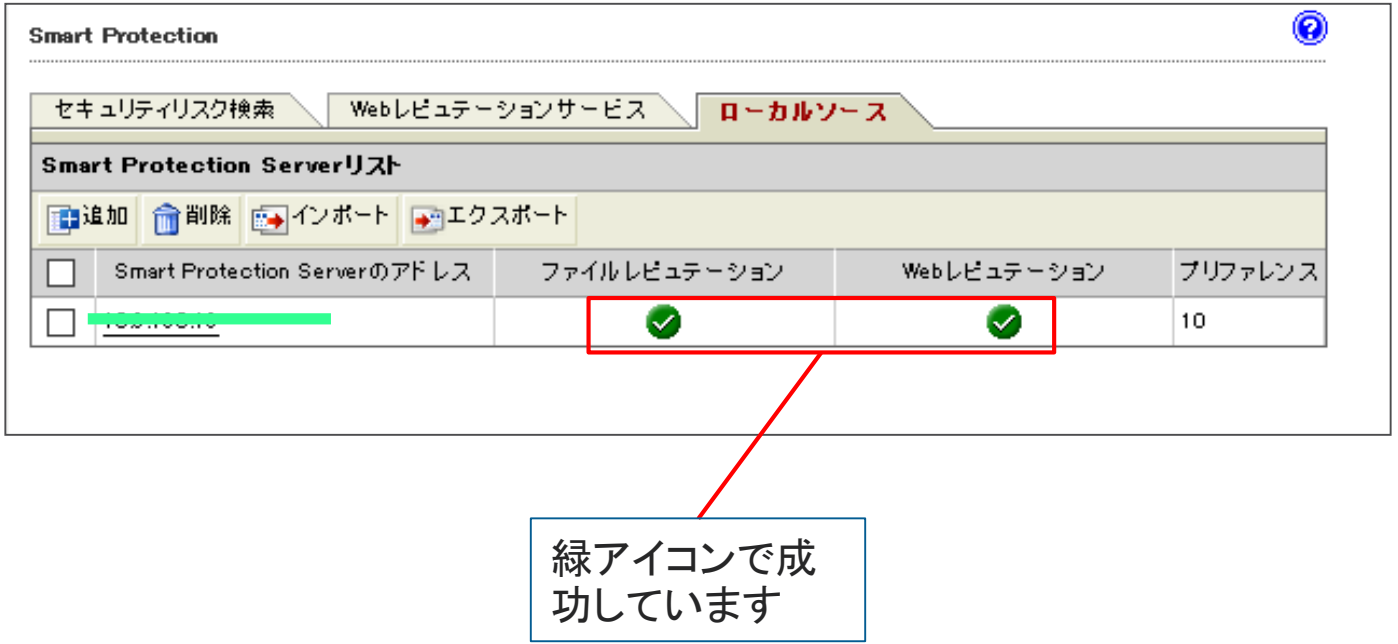
SPS側の設定に沿って設定ください

SPS側の設定に沿って設定ください

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP4-1 IMSVAにSPSを登録します

6. 正常に登録出来たことを確認します

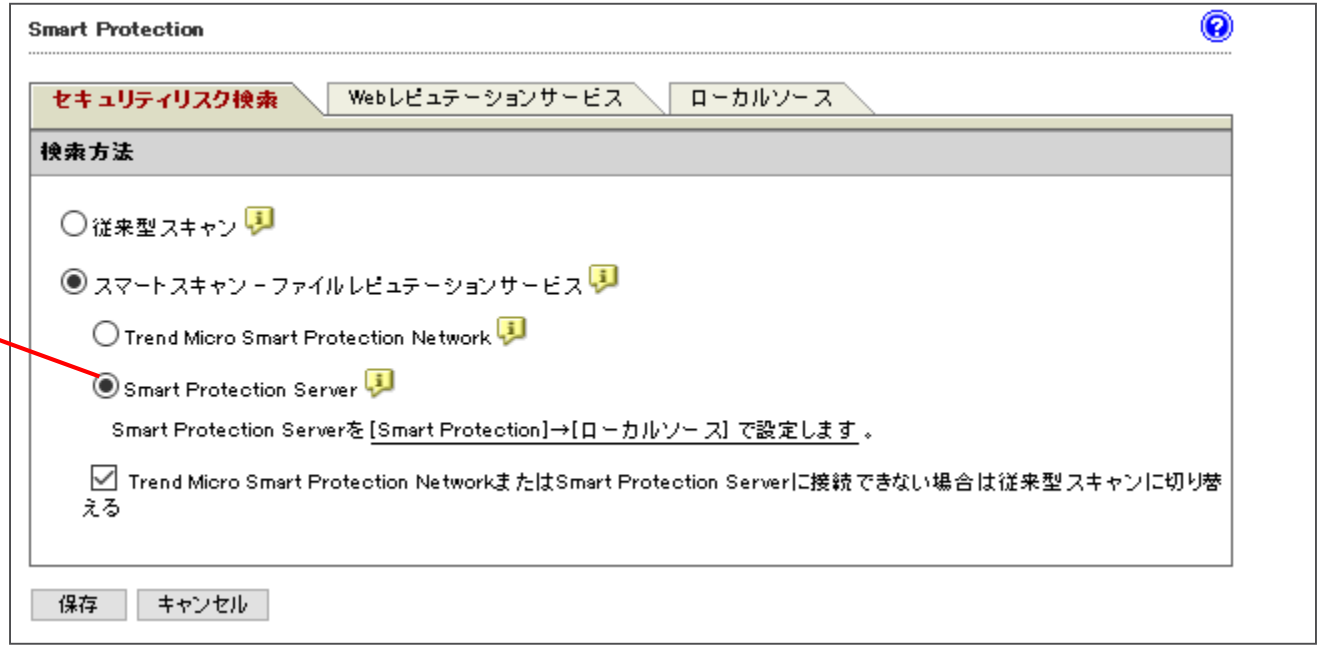


Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP4-2 ファイルレピュテーションを設定する

1. [ポリシー] – [Smart Protection] – [セキュリティリスク検索] をクリックします
2. 以下のパラメータを設定し、保存をクリックします

こちらを選択し、STEP4-1で設定した、SPSを指定します

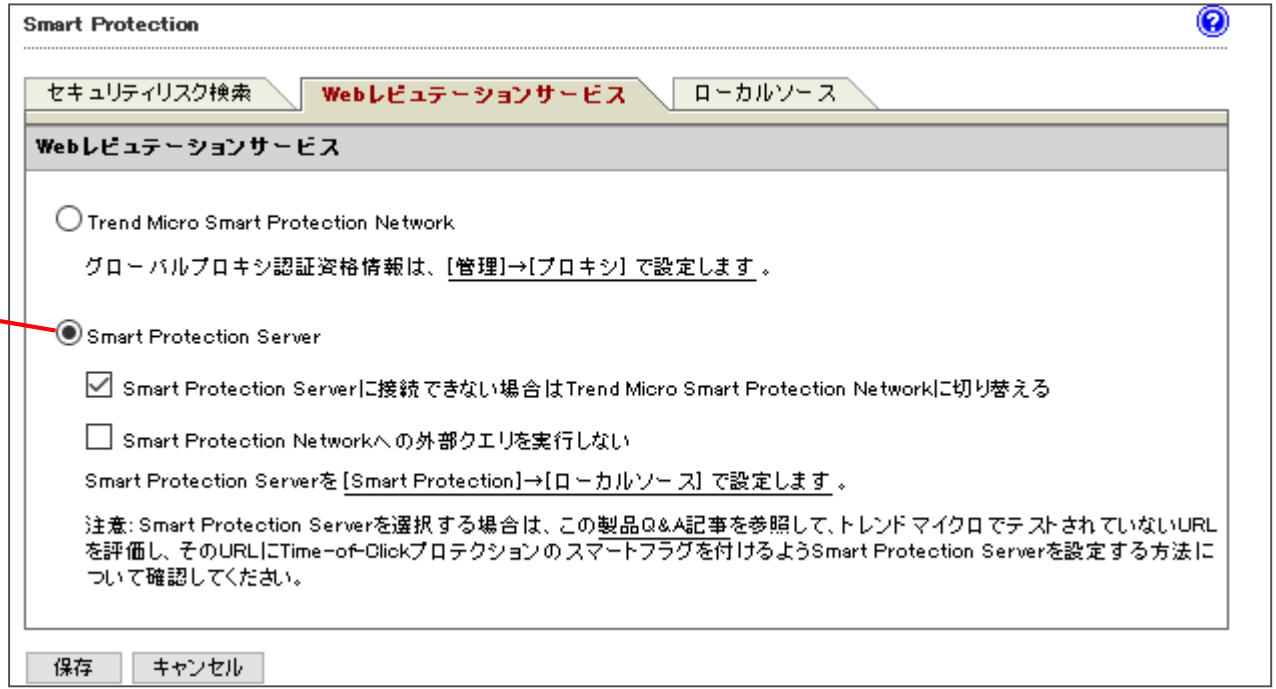


Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP4-3 Webレピュテーションを設定する

1. [ポリシー] – [Smart Protection] – [Webレピュテーション] をクリックします
2. 以下のパラメータを設定し、保存をクリックします

こちらを選択し、STEP4-1で設定した、SPSを指定します



Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP5 TMCM-IMSVAを連携する

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP5-1 IMSVAをTMCMへ登録する

1. IMSVAのWEBコンソールへアクセスします
https://[IMSVA IP or FQDN]:8445/console.imss
2. ログインします
3. [管理] – [管理 > IMSVA設定] – [接続] – [Control Managerサーバ] をクリックします

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP5-1 IMSVAをTMCMへ登録する

4. 以下のパラメータを設定し、保存をクリックします

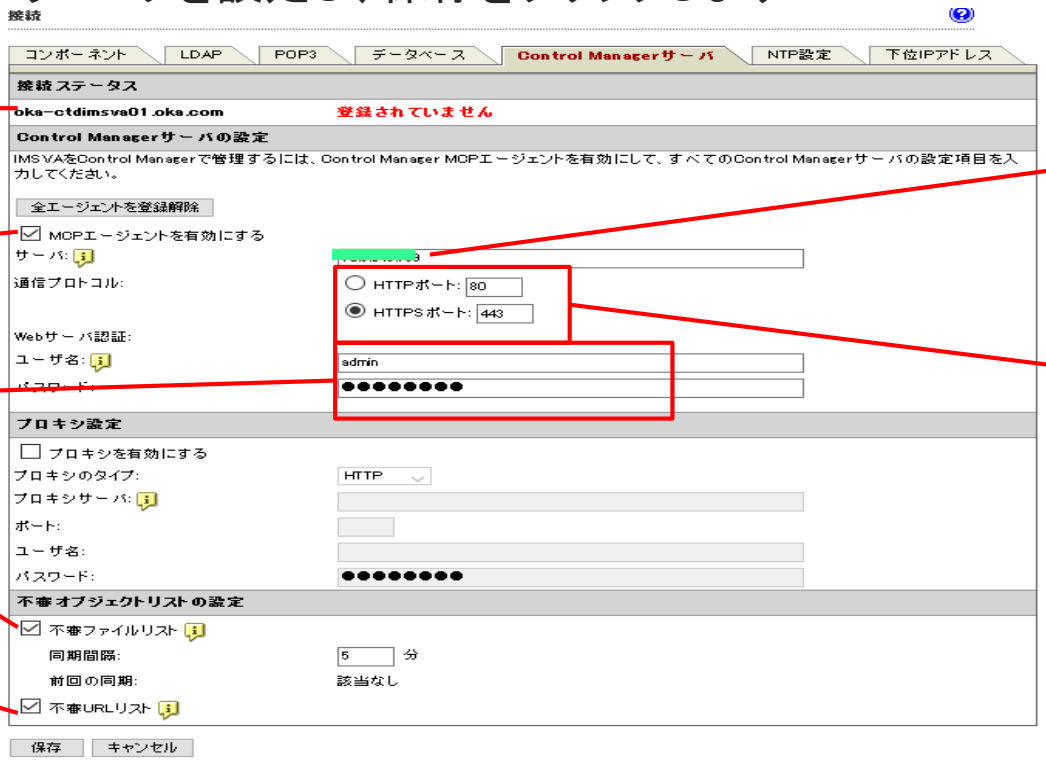
TMCM上の表示名(以降、※4と記載)

チェックする

認証が必要であれば設定します

チェックする

チェックする



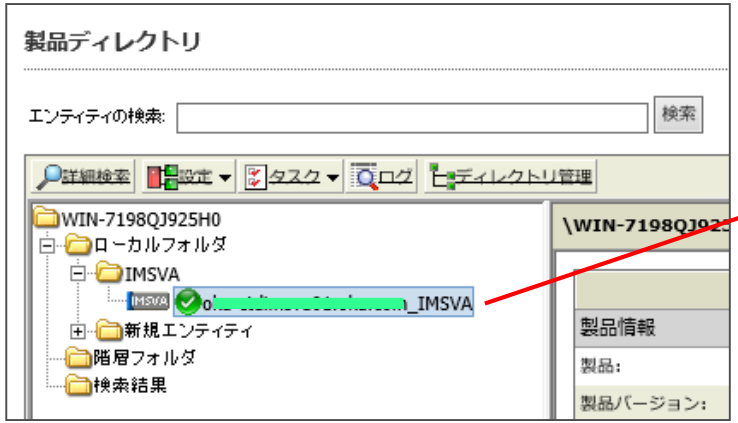
TMCMのIP or FQDNを記載する

プロトコル及びポート番号を指定します

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP5-2 IMSVAがTMCMへ登録されたことを確認する

1. TMCMのWEBコンソールへアクセスします
https://[TMCM IP or FQDN]/webapp/login.aspx
2. ログインします
3. [ディレクトリ] – [製品] をクリックします
4. ディレクトリツリーを展開します
5. ディレクトリツリー下に「※4」が登録されていることを確認します

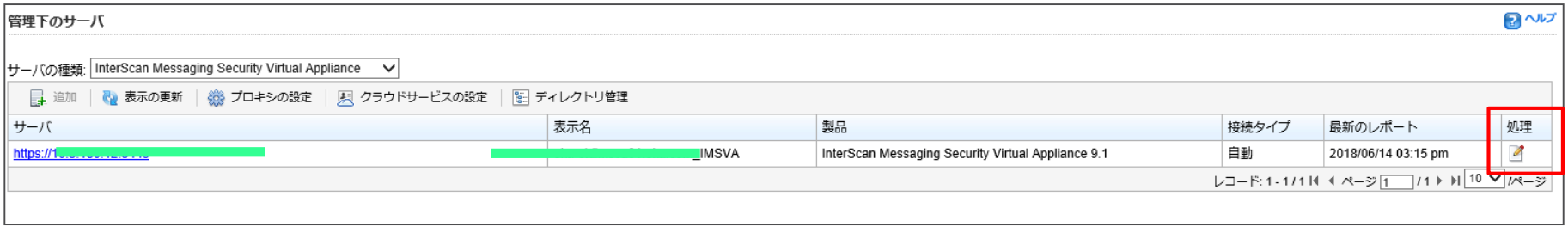


※4の表示を確認し、緑アイコンが表示されていれば正常に登録が完了している

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP5-3 TMCM上のIMSVA情報にログイン情報を登録する

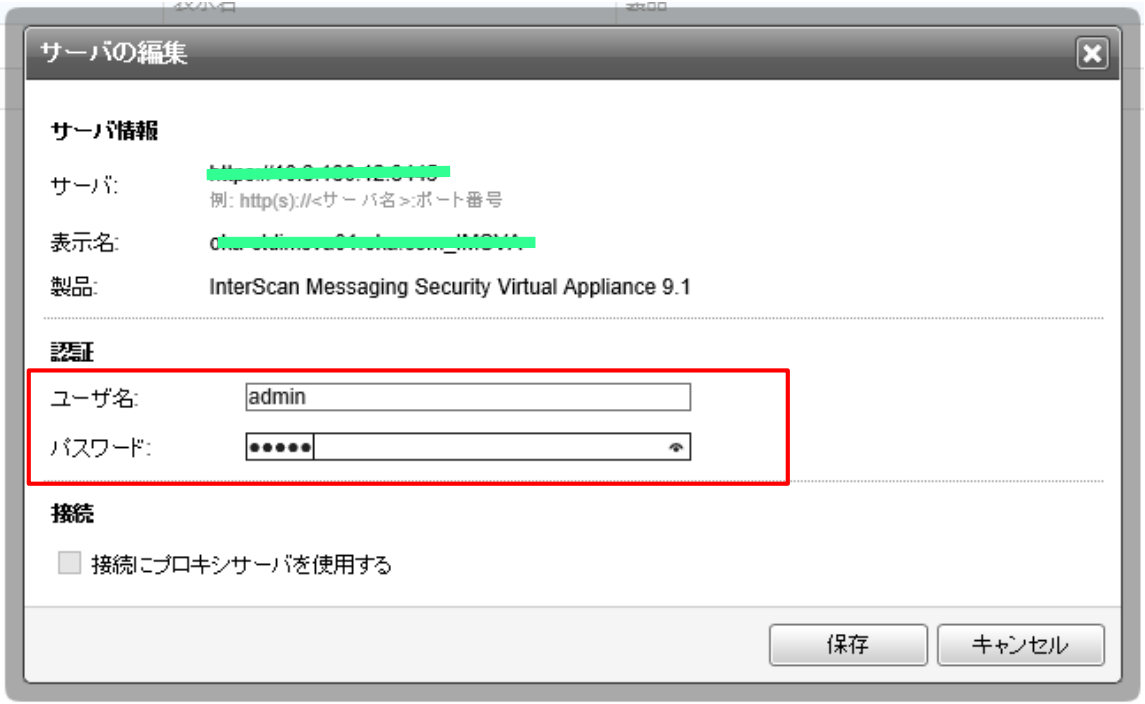
1. TMCMのWEBコンソールへアクセスします
https://[TMCM IP or FQDN]/webapp/login.aspx
2. ログインします
3. [運用管理] – [管理下にサーバ] をクリックします
4. [サーバの種類] からInterScan Messaging Security Virtual Appliance を選択します
5. 「※4」の登録を確認後、処理をクリックします



Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP5-3 TMCM上のIMSVA情報にログイン情報を登録する

6. IMSVAのWEBコンソールの認証情報を設定し、保存をクリックします



Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP6 IMSVA-DDANを連携する

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP6-1 IMSVAへDDANを登録する

1. IMSVAのWEBコンソールへアクセスします
https://[IMSVA IP or FQDN]:8445/console.imss
2. ログインします
3. [管理] – [ポリシー] – [仮想アナライザ] – [サーバ管理] をクリックします
4. [追加] をクリックします
5. パラメータを設定し、保存をクリックします。

チェックする

DDAN IP or FQDNを記載する

※1を記載する

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP6-2 仮想アナライザへの送信設定をする

1. IMSVAのWEBコンソールへアクセスします
https://[IMSVA IP or FQDN]:8445/console.imss
2. ログインします
3. [管理] – [ポリシー] – [仮想アナライザ] – [仮想アナライザ設定]をクリックします

チェックする

DDAN IP or FQDNを記載する

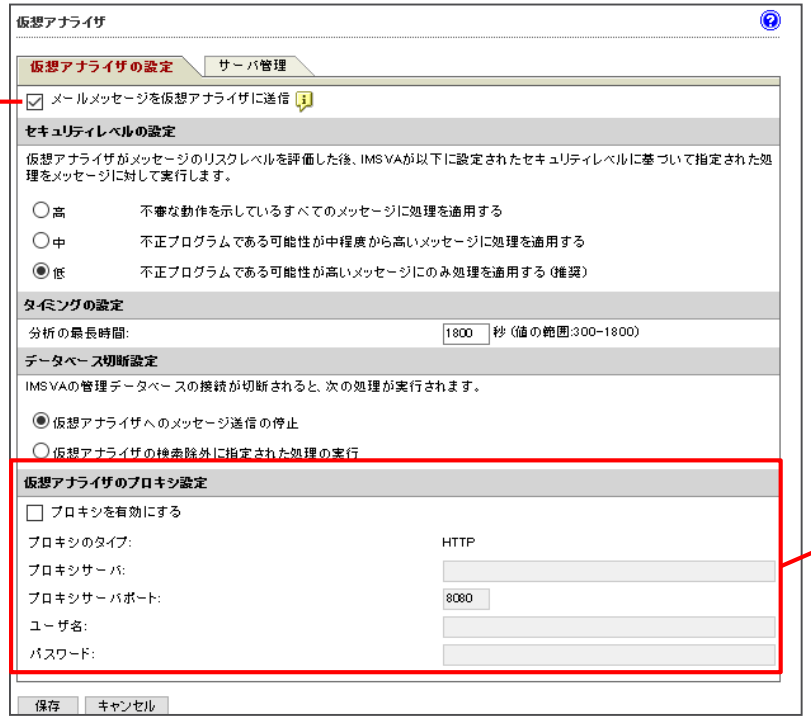
※1を記載する

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

STEP6-2 仮想アナライザへの送信設定をする

4. パラメータを設定し、保存をクリックします。

チェックする



プロキシサーバを介してアクセスする必要がある場合はチェックする

※[管理] – [プロキシ] を事前に設定する必要あり

Copyright © 2018 Trend Micro Incorporated. All rights reserved.