TREND MICRO | txOne networks

2.0 TXOne StellarOne
管理者ガイド
for StellarProtect (Legacy Mode)

※注意事項

複数年契約について

- お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。
- 複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。
- 各製品のサポート提供期間は以下の Web サイトからご確認いただけます。
  https://success.trendmicro.com/jp/solution/000207383

法人向け製品のサポートについて

- 法人向け製品のサポートの一部または全部の内容、範囲または条件は、トレンドマイクロの裁量により随時変更される場合があります。
- 法人向け製品のサポートの提供におけるトレンドマイクロの義務は、法人向け製品サポートに関する合理的な努力を行うことに限られるものとします。

P/N: APEM29595_JP2303

プライバシーと個人データの収集に関する規定

トレンドマイクロ製品の一部の機能は、お客さまの製品の利用状況や検出にかかわる情報を収集してトレンドマイクロおよび TXOne Netwoks 社に送信します。この情報は一定の管轄区域内および特定の法令等において個人データとみなされることがあります。トレンドマイクロによるこのデータの収集を停止するには、お客さまが関連機能を無効にする必要があります。

TXOne StellarOne for StellarProtect (Legacy Mode) により収集されるデータの種類と各機能によるデータの収集を無効にする手順については、次の Web サイトを参照してください。

https://www.go-tm.jp/data-collection-disclosure

https://www.txone.com/privacy-policy

重要

データ収集の無効化やデータの削除により、製品、サービス、または機能の利用に影響が発生する場合があります。TXOne StellarOne for StellarProtect (Legacy Mode) における無効化の影響をご確認の上、無効化はお客さまの責任で行っていただくようお願いいたします。

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシー (Global Privacy Notice) に従って、お客さまのデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

目次

はじめに

この管理者ガイドでは、TXOne StellarOne について紹介するとともに、製品管理のあらゆる側面について説明します。

対象読者

TXOne StellarOne のドキュメントは、エージェントのインストールを含めた StellarOne 管理担当者を対象としています。これらのユーザがネットワークとサーバ管理に関する高度な知識を備えていることを前提としています。

ドキュメントの表記規則

次の表は、TXOne StellarOne のドキュメントで使用されている表記規則を示しています。

表 1.　ドキュメントの表記規則

表記	説明
 **注意**	設定上の注意
 **ヒント**	推奨事項
 **重要**	避けるべき操作や設定についての注意
 **警告!**	使用上の重要事項

用語

次の表は、TXOne StellarOne のドキュメントで使用されている用語を示しています。

用語	説明
サーバ	StellarOne のサーバプログラムです。
サーバコンピュータ	StellarOne サーバがインストールされているホストです。
エージェント	StellarProtect (Legacy Mode) クライアントプログラムを実行しているホストです。
管理対象エージェント 管理下のエージェント	StellarOne サーバプログラムが認識している、StellarProtect (Legacy Mode) クライアントプログラムを実行しているホストです。
対象エージェント	StellarOne の管理対象エージェントをインストールするホストです。
管理者 (または StellarOne 管理者)	StellarOne サーバを管理している人物です。
管理サーバ画面	StellarOne の設定や管理対象エージェントを設定して管理するユーザインタフェースです。
CLI	コマンドラインインタフェース
ライセンスの アクティベーション	StellarOne サーバのインストールの種類と、アプリケーションの使用許諾期間が含まれます。
エージェントの インストールフォルダ	StellarProtect (Legacy Mode) エージェントのファイルが含まれるホスト上のフォルダです。インストール時に初期設定を使用すると、インストールフォルダは次の場所になります。 "C:\Program Files\TXOne\StellarProtect (Legacy Mode)"

第 1 章

本製品の概要

概要

TXOne StellarOne は、レガシーシステム向けの TXOne StellarProtect (Legacy Mode) とモダナイズされたシステム向けの TXOne StellarProtect の両方の管理を効率化するように設計された集中管理コンソールです。このマニュアルでは、主に TXOne StellarProtect (Legacy Mode) を管理する方法について説明します。シンプルかつメンテナンス不要なソリューションである TXOne StellarProtect (Legacy Mode) は、特定用途向けのコンピュータをロックダウンして保護することによりセキュリティ上の脅威から企業を守り、高い生産性を実現します。

TXOne StellarOne について

TXOne StellarOne は、StellarProtect (Legacy Mode) エージェントのインストール、ステータス、およびイベントの集中管理を実現します。たとえば管理者は、エージェントの許可リストを作成したりアプリケーション制御を変更したりできます。

サーバの機能と特徴

TXOne StellarOne には、次の機能と特徴があります。

機能	特徴
ダッシュボード	管理サーバ画面のダッシュボードには、監視下の StellarProtect (Legacy Mode) エージェントについての概要情報が表示されます。 インストール済みの StellarProtect (Legacy Mode) エージェントのステータスを簡単に確認でき、指定された期間内の StellarProtect (Legacy Mode) エージェントのアクティビティについてセキュリティレポートを生成できます。
エージェントの集中管理	TXOne StellarOne では、管理者は次のタスクを実行できます。 • StellarProtect (Legacy Mode) エージェントステータスの監視 • 接続ステータスの確認 • 設定の表示 • 手動またはポリシーによるエージェントログの収集 • エージェントのアプリケーション制御の有効化または無効化 • エージェントのデバイスコントロールの有効化または無効化 • エージェントのメンテナンスモードの設定 • エージェントコンポーネントのアップデート • 許可リストの初期化 • エージェントへの Patch の配信 • 信頼するファイルおよび USB デバイスの追加
イベントの集中管理	StellarProtect (Legacy Mode) エージェントで保護されたコンピュータでは、管理者がステータスやイベントを監視し、ファイルの実行がブロックされた場合はそれに対処できます。StellarOne にはイベント管理機能があり、管理者はこれを使用して、ブロックされたファイルイベントを迅速に把握して処理を実行できます。

機能	特徴
監査	StellarOne の管理サーバ画面にアクセスするためのアカウントで実行された操作を監査することが可能です。StellarOne では各アカウントの操作をログに記録して、ログインしたユーザ、設定を変更したユーザ、イベントログを削除したユーザなどを追跡できます。

新機能

TXOne StellarOne for StellarProtect (Legacy Mode) 2.0 には、次の新機能および機能強化が含まれています。

機能	説明
自己管理グループポリシー	この新しく追加されたグループポリシーにより、現場のオペレータがエージェントのポリシー設定を独自に指定できるようになります。自己管理ステータスに切り替わったローカルエージェントは、StellarOne の管理サーバ画面のポリシー管理から外されます。
オープン API	エージェントのデータをクエリするためのオープン API が提供されています。API キーを生成して、アカウント管理のために各ユーザアカウントに対して有効期限を設定することもできます。

第 2 章

エージェント/グループ管理

StellarProtect (Legacy Mode) エージェントの管理

この章では、エージェント管理を行う管理サーバ画面の概要について説明します。

[エージェント] 画面について

[エージェント] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。この画面では、StellarOne の管理サーバ画面で管理されているエージェントのリストが表示され、設定タスクを実行できます。

注意

初期設定では、[すべて] グループにすべてのエージェントが表示されます。 アイコンはグループを、 アイコンはエージェントを示します。

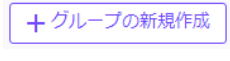
エージェントツリーを管理する

StellarOne では、エージェントツリーを編成して StellarProtect (Legacy Mode) エージェントの情報を管理できます。

タスク	詳細
エージェントグループの追加	複数エージェントの管理を容易にするため、場所、種類、または目的に応じてグループを作成します。
エージェントグループの再編成	グループを再編成します。
エージェントグループ名の変更	グループの名前を変更します。
エージェントグループの削除/ エージェントの登録解除	StellarOne の管理サーバ画面から、グループを削除するかエージェントを登録解除します。
エージェントまたは グループの検索	検索条件を追加してエージェント/グループを検索します。

グループを追加する

手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。[エージェント] 画面が表示されます。
2. [エージェント] ビューの [すべて] グループから開始します。
3. グループ名をクリックして目的の親グループに移動し、新しいグループを作成します。
4. 上部のコントロール領域で 

ボタンをクリックします。
5. [グループの新規作成] 画面が表示されます。
6. グループ名を入力し、[確認] を選択します。

注意

- グループ名は 50 文字以内で入力してください。
- レベルの最大数は 15 です。

グループ名を変更する

手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。[エージェント] 画面が表示されます。
2. 名前を変更するグループを選択します。
3. [処理] の縦 3 点リーダーのアイコン (⋮) をクリックし、[名前の変更] をクリックします。
4. [エージェントグループ名の変更] 画面が表示されます。
5. 新しい名前を入力し、[確認] をクリックします。

注意

同一レベルで同じグループ名を指定することはできません。

グループを削除する/エージェントを登録解除する

手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。[エージェント] 画面が表示されます。
2. 削除するグループまたは登録解除するエージェントを選択します。
3. [処理] の縦 3 点リーダーのアイコン (⋮) をクリックし、[削除] をクリックします。

4. [項目の削除] 確認画面が表示されます。
5. [確認] をクリックして、グループの削除またはエージェントの登録解除を行います。

> **注意**
> 空でない (グループまたは資産がある) グループは削除できません。

エージェント/グループを検索する

手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。[エージェント] 画面が表示されます。
2. ドロップダウンリストから条件を選択し、必要に応じて検索条件を追加して、特定のエージェントを検索します。

オプション	説明
名前	エージェントの名前。特定のエージェントを指定するには、エージェントの完全なホスト名またはホスト名の一部を入力します。
IP アドレス	IPv4 アドレスを入力します。
IP アドレスの範囲	IPv4 アドレスの範囲を入力します。
グループ	グループの名前。選択可能なグループを選択します。
ポリシーの継承	ポリシーの継承モード。[継承済み] または [カスタマイズ済み] を選択します。
ポリシーの配信	StellarOne からエージェントへのポリシー配信ステータス。[完了] または [実行中] を選択します。
エージェント バージョン	エージェントバージョンを入力します。

オプション	説明
前回の接続	前回の接続時間。初期設定の期間を選択するか、[カスタム] を選択して時間範囲を独自に指定します。初期設定の期間は次のとおりです。 • 1 時間以内 • 24 時間以内 • 過去 7 日間 • 過去 30 日間
製品	[StellarProtect (Legacy Mode)] または [StellarProtect] を選択します。
OS	OS を選択します。
説明	特定のエージェントをクエリするには、完全な説明または説明の一部を入力します。

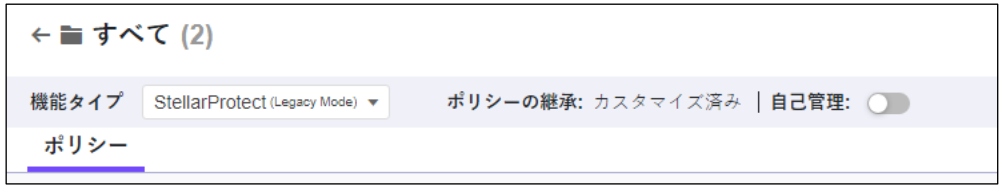
第 3 章

ポリシー管理

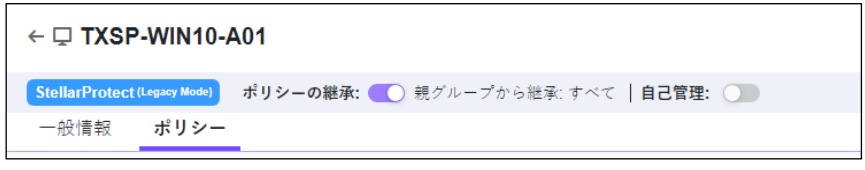
グループ/エージェントポリシーを管理する

- グループをエージェントとともに追加して、親グループから**グループポリシー**を継承することも、独自のグループポリシーをカスタマイズすることもできます。
- エージェントは、親グループからポリシーを継承する代わりに、カスタマイズした独自の**エージェントポリシー**を持つこともできます。

- エージェントを含むグループは、[製品] (StellarProtect または StellarProtect (Legacy Mode)) を切り替えると、それぞれの [ポリシー] を表示できます。

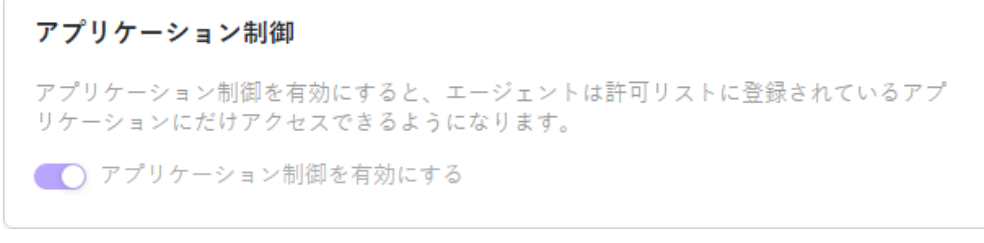


- エージェントは、タブを切り替えると、それぞれの [一般情報] と [ポリシー] を表示できます。



アプリケーション制御を設定する

アプリケーション制御を有効にすると、エージェントは許可リストに登録されているアプリケーションにだけアクセスできるようになります。許可リストの設定は [ロックダウン除外] で行います (詳細は以降のセクションを参照)。



手順

1. [エージェント] ビューで対象のエージェントまたはエージェントグループに移動します。
2. 次のいずれかの方法で [ポリシー] ビューを表示します。
   - [ポリシーの継承] リンクをクリックします。

- [処理] のポリシーアイコン ( ) をクリックします。

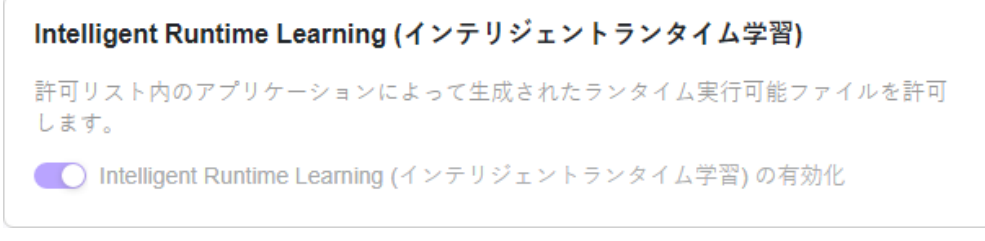
3. [ポリシー] ビューで [アプリケーション制御] ペインに移動します。
4. **スイッチ**を切り替えて、[親グループから継承] を無効にします。
5. **スイッチ**を切り替えて、アプリケーション制御を有効または無効にします。

注意

StellarProtect (Legacy Mode) エージェントの管理者は、StellarProtect (Legacy Mode) エージェントのメイン画面からアプリケーション制御のステータスを変更することもできます。

Intelligent Runtime Learning (インテリジェントランタイム学習) を設定する

Intelligent Runtime Learning (インテリジェントランタイム学習) が有効な場合、エージェントでは、信頼リストに含まれるアプリケーションによって生成されたランタイム実行ファイルが許可されます。



手順

1. [エージェント] ビューで対象のエージェントまたはエージェントグループに移動します。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
   - [ポリシーの継承] リンクをクリックします。
   - [処理] の**ポリシー**アイコン ( ) をクリックします。

3. [ポリシー] ビューで [Intelligent Runtime Learning (インテリジェントランタイム学習)] ペインに移動します。
4. スイッチを切り替えて、[親グループから継承] を無効にします。
5. **スイッチ**を切り替えて、Intelligent Runtime Learning (インテリジェントランタイム学習) を有効または無効にします。

ロックダウン除外を設定する

[ロックダウン除外] を使用すると、**アプリケーション制御**からの除外を設定できます。つまり、ブロックするよう指定されたアプリケーションのユーザ指定の設定です。ここで設定する許可リストには、[ポリシー] ビューの [ロックダウン除外] ペインにある [信頼するハッシュ値]、[信頼するデジタル証明書]、[除外パス]、および [書き込み制御] の設定が含まれます。

信頼するハッシュ値の設定

ハッシュ値を使用して、管理対象資産のアプリケーションやファイルの実行をリモートで許可できます。

ハッシュ値を計算する

信頼するハッシュ値を追加する前に、**ファイルハッシュ生成ツール**を使用してハッシュ値を計算します。

手順

1. [信頼するハッシュ値] 領域からファイルハッシュ生成ツールをダウンロードします。
2. ダウンロードしたフォルダから ***WKFileHashGen.exe*** を実行します。[ファイルハッシュ生成ツール] 画面が表示されます。
3. 次のいずれかの方法を使用してファイルを選択し、ハッシュ値を計算します。
   - フォルダまたはファイルを [ファイルハッシュ生成ツール] 画面にドラッグアンドドロップします。
   - **ドロップダウン**ボタンをクリックし、[ファイルの追加] をクリックして、追加するファイルを選択します。

- **ドロップダウン**ボタンをクリックし、[フォルダの追加] をクリックして、選択したフォルダのすべてのファイルを追加します。

[ファイルハッシュ （**SHA-1**）] 列にハッシュ値が表示されます。

4. ファイルが 1 つの場合は、項目を右クリックして [ハッシュ値のコピー] を選択します。ファイルが複数の場合は、[すべてエクスポート] をクリックしてハッシュ値のリストを生成します。

注意

すべての必要なファイルでハッシュ値を計算するには、対象アプリケーションのルートフォルダを**ファイルハッシュ生成ツール**に追加することをお勧めします。

[フォルダの追加] ボタンでは、インストーラファイル、スクリプトファイル、および PE (ポータブル実行可能) 形式のファイルのみが計算対象となることに注意してください。

信頼するハッシュ値を追加する

手順

1. [エージェント] ビューで対象のエージェントまたはエージェントグループに移動します。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
   - [ポリシーの継承] リンクをクリックします。
   - [処理] の**ポリシー**アイコン ( ) をクリックします。
3. [ポリシー] ビューの [ロックダウン除外] ペインにある [信頼するハッシュ値] に移動します。
4. ハッシュ値とメモを入力します。
5. 信頼するインストールパッケージによって作成または変更されたファイルが自動的に許可リストに追加されるようにするには、**スイッチ**を切り替えてインストーラを有効にします。
6. [追加] ボタンをクリックして、単一のハッシュ値と以前保存した設定を追加します。

注意

信頼するインストールパッケージによって作成または変更されたファイルが自動的に許可リストに追加されるようにするには、[インストーラ] 列でアプリケーションインストーラを選択します。

信頼するハッシュ値をインポートする

手順

1. [ポリシー] ビューの [ロックダウン除外] ペインにある [信頼するハッシュ値] に移動します。
2. [インポート] ボタンをクリックして、ハッシュ値をまとめて追加します。
3. 許可済みのインストーラによって作成または変更されたすべてのファイルを [許可リスト] に自動的に追加するように、[インストーラ] スイッチを切り替えて有効にします。

注意

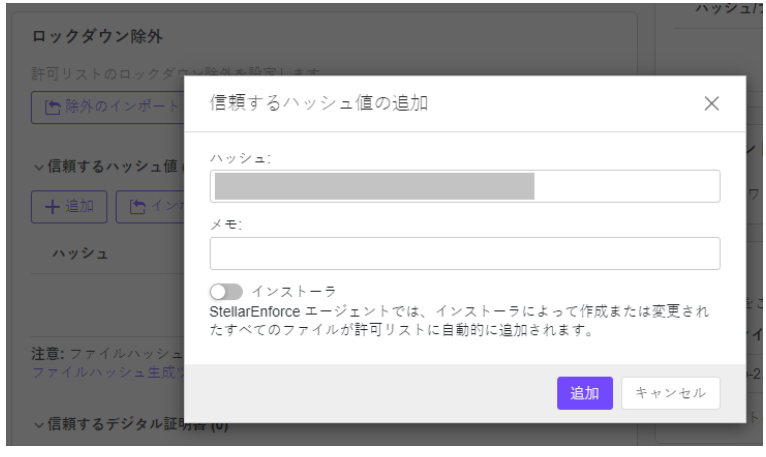
StellarOne は、インストーラフラグがマークされた信頼するハッシュ値のリストを含む.txt ファイルの一括インポート/エクスポートをサポートします。ただし、インポート/エクスポート処理により、[メモ] に含まれるタブ文字が (信頼するハッシュの配信画面で表示されるように) 空白に自動的に変換されます。

信頼するハッシュ値を編集する

手順

1. [ポリシー] ビューの [ロックダウン除外] ペインにある [信頼するハッシュ値] に移動します。
2. 編集するハッシュ値を選択します。
3. [追加] ボタンをクリックすると、[信頼するハッシュ値の追加] 画面が表示されます。

4. 編集後、[追加] ボタンをクリックして設定を保存します。

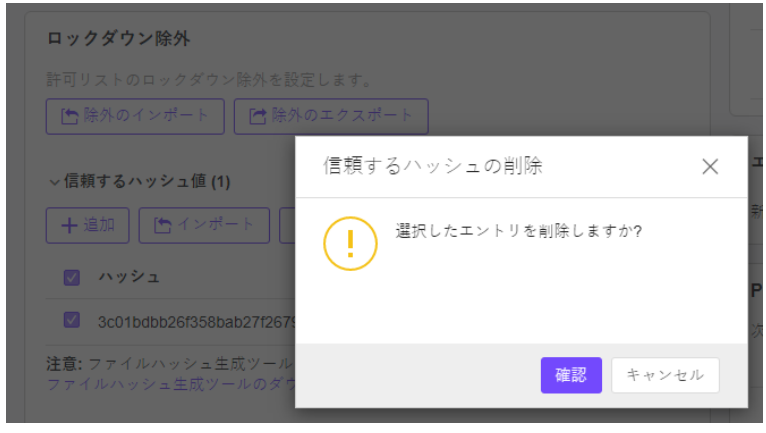


信頼するハッシュ値を削除する

手順

1. [ポリシー] ビューの [ロックダウン除外] ペインにある [信頼するハッシュ値] に移動します。
2. 削除するハッシュ値を選択します。
3. [削除] ボタンをクリックすると、確認画面が表示されます。

4. [確認] ボタンをクリックして、選択したエントリを削除します。



信頼するデジタル証明書の設定

ハッシュ値と同様に、アプリケーションベンダや組織によって作成される信頼するデジタル証明書は、StellarProtect (Legacy Mode) が信頼できるアプリケーションを識別するのに役立ちます。

信頼するデジタル証明書をインポートする

手順

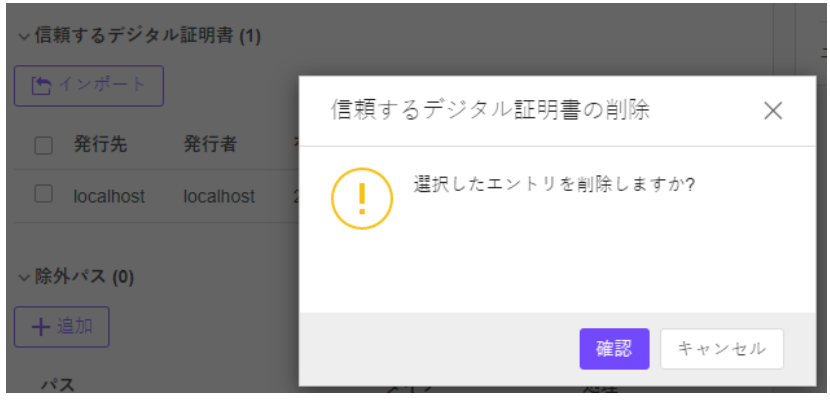
1. [エージェント] ビューで対象のエージェントまたはエージェントグループに移動します。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
   - [ポリシーの継承] リンクをクリックします。
   - [処理] のポリシーアイコン ( ) をクリックします。
3. [ポリシー] ビューの [ロックダウン除外] ペインにある [信頼するデジタル証明書] に移動します。
4. [ファイルの選択] ボタンをクリックし、追加する証明書を見つけてクリックします。
5. 許可済みのインストーラによって作成または変更されたすべてのファイルを [許可リスト] に自動的に追加するように、[インストーラ] スイッチを切り替えて有効にします。

6. [インポート] ボタンをクリックして信頼するデジタル証明書を追加し、設定を保存します。

信頼するデジタル証明書を削除する

手順

1. [ポリシー] ビューの [ロックダウン除外] ペインにある [信頼するデジタル証明書] に移動します。
2. 削除する信頼するデジタル証明書を選択します。
3. [削除] ボタンをクリックすると、[信頼するデジタル証明書の削除] 画面が表示されます。
4. [確認] ボタンをクリックして、選択したエントリを削除します。



除外パスの設定

除外パスは、ファイルまたはファイルフォルダを直接指定して、ファイルの実行を許可するために使用されます。

ファイル、フォルダ、または正規表現を除外パスとして追加する

手順

1. [エージェント] ビューで対象のエージェントまたはエージェントグループに移動します。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
   - [ポリシーの継承] リンクをクリックします。
   - [処理] のポリシーアイコン ( ) をクリックします。
3. [ポリシー] ビューの [ロックダウン除外] ペインにある [除外パス] に移動します。
4. [追加] ボタンをクリックすると、[除外パスの追加] 画面が表示されます。
5. 除外のタイプとして、**ファイル**、**フォルダ**、または**正規表現**を選択します。
6. 除外対象のファイルシステム**パス**を入力します。
7. [追加] ボタンをクリックして単一の除外パスを追加し、設定を保存します。

除外パスを編集する

手順

1. 編集する除外パスを選択します。
2. [編集] ボタンをクリックすると、[除外パスの編集] 画面が表示されます。
3. 単一の除外パスを変更したら、[編集] ボタンをクリックして設定を保存します。

除外パスを削除する

手順

1. 削除する除外パスを選択します。
2. [削除] ボタンをクリックすると、[除外パスの削除] 画面が表示されます。
3. [確認] ボタンをクリックして、選択したエントリを削除します。

書き込み制御の設定

書き込み制御により、特定のファイルまたはフォルダの内容を、不正なユーザやアプリケーションによる変更から保護できます。

書き込み制御にファイル、フォルダ、レジストリキー、またはレジストリ値を追加する

手順

1. [エージェント] ビューで対象のエージェントまたはエージェントグループに移動します。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
   - [ポリシーの継承] リンクをクリックします。
   - [処理] の**ポリシー**アイコン ( ) をクリックします。
3. [ポリシー] ビューの [ロックダウン除外] ペインにある [書き込み制御] に移動します。
4. [追加] ボタンをクリックすると、[書き込み制御の追加] 画面が表示されます。
5. 制御のタイプとして、**ファイル、フォルダ、レジストリキー**、または**レジストリ値**を選択します。
6. 書き込み制御の対象とするオブジェクトのパスを入力します。
7. [除外プロセスタイプ] を設定します。
   - すべてのユーザおよびアプリケーションからの書き込みを制限する

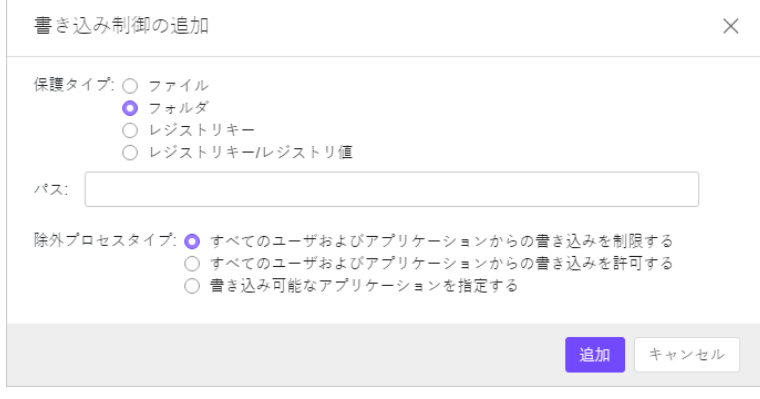
- すべてのユーザおよびアプリケーションからの書き込みを許可する
- 書き込み可能なアプリケーションを指定する

8. [追加] ボタンをクリックして設定を保存します。

書き込み制御を編集する

手順

1. [ポリシー] ビューの [ロックダウン除外] ペインにある [書き込み制御] に移動します。
2. 編集する制御のタイプを選択します。
3. [編集] ボタンをクリックして設定を保存します。



書き込み制御を削除する

手順

1. [ポリシー] ビューの [ロックダウン除外] ペインにある [書き込み制御] に移動します。
2. 削除する制御のタイプを選択します。
3. [削除] ボタンをクリックすると、[書き込み制御の削除] 画面が表示されます。
4. [確認] ボタンをクリックして、選択したエントリを削除します。

除外をインポートする

除外をインポートすることにより、ハッシュ値、信頼するデジタル証明書、除外パス、および書き込み制御の設定をグループ間で移動できます。

手順

1. [エージェント] ビューで対象のエージェントまたはエージェントグループに移動します。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
   - [ポリシーの継承] リンクをクリックします。
   - [処理] の**ポリシー**アイコン ( ) をクリックします。
3. [ポリシー] ビューの [ロックダウン除外] ペインにある [除外のインポート] ボタンに移動します。
4. [除外のインポート] ボタンをクリックすると、[除外のインポート] 画面が表示されます。
5. [ファイルの選択] ボタンをクリックし、エクスポートした設定を含むファイル (例: ***exclusion.xml***) を選択します。
6. [インポート] ボタンをクリックします。

除外をエクスポートする

手順

1. [ポリシー] ビューの [ロックダウン除外] ペインにある [除外のエクスポート] に移動します。
2. [除外のエクスポート] ボタンをクリックすると、除外設定がブラウザからダウンロードされます。

予約検索を設定する

[予約検索の設定] ペインから、検索の実行間隔、検索前のコンポーネントアップデートの設定、検索対象ファイル、検索時に実行する処理、および検索から除外するファイルを設定できます。

注意

検索機能は、Stellar 無期限版では利用できません。

予約検索

手順

1. [エージェント] ビューで対象のエージェントまたはエージェントグループに移動します。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
   - [ポリシーの継承] リンクをクリックします。
   - [処理] の**ポリシー**アイコン ( ) をクリックします。
3. [ポリシー] ビューの [予約検索の設定] ペインにある [予約] ボタンに移動します。
4. [実行間隔] ([日次]、[週次]、または [月次]) と [開始時刻] を設定します。
5. [確認] ボタンをクリックします。

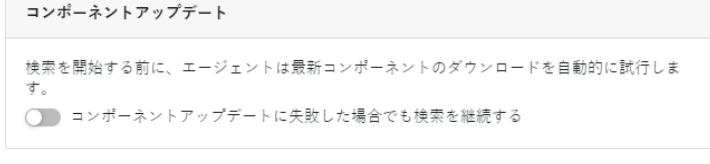
コンポーネントアップデート

手順

1. [ポリシー] ビューの [予約検索の設定] ペインにある [詳細設定] に移動します。
2. [コンポーネントアップデート] に移動します。
3. コンポーネントアップデートに失敗した場合でも検索を継続するには、該当するチェックボックスをオンにします。

注意

チェックボックスをオフにすると、検索が実行されないためコンポーネントをアップデートできません。



検索対象ファイル

手順

1. [ポリシー] ビューの [予約検索の設定] ペインにある [詳細設定] に移動します。
2. [検索対象ファイル] に移動します。
3. [すべてのローカルフォルダ] または [初期設定のフォルダ (クイック検索)] を選択するか、[特定のフォルダ] を選択して検索するフォルダのパスを入力します。
4. すべての**リムーバブルドライブ**を検索するには、[リムーバブルドライブを検索する] の横にあるチェックボックスをオンにします。
5. すべての**圧縮ファイル**を検索するには、[圧縮ファイルを検索する] の横にあるチェックボックスをオンにします。

> **注意**
>
> このチェックボックスの下で、圧縮ファイル内の検索する階層数を選択できます。

6. 特定のサイズを超えるファイルをスキップするには、[(任意の値) MB を超えるファイルをスキップする] チェックボックスをオンにし、ファイルサイズを **1**～**9999**MB の間で入力します。

検出時の処理

手順

1. [ポリシー] ビューの [予約検索の設定] ペインにある [詳細設定] に移動します。
2. [検出時の処理] に移動します。

- 事前に設定された検出時の処理を使用するには、[トレンドマイクロの推奨処理を使用する] を選択します。これは検出時の処理に詳しくない場合、または適切な処理がわからない場合に適しています。
- 結果を読み出すだけで、検出されたファイルに処理を実行しない場合は、[処理しない] を選択します。
- 対象ファイルを復元できない場合に、初期設定でそのファイルを**削除**するには、[駆除する、駆除処理に失敗した場合は削除する] を選択します。
- 対象ファイルを復元できない場合に、初期設定でそのファイルを**隔離**するには、[駆除する、駆除処理に失敗した場合は隔離する] を選択します。
- 対象ファイルを復元できない場合に、初期設定でそのファイルを**無視**するには、[駆除する、駆除処理に失敗した場合は無視する] を選択します。

検索除外

手順

1. [ポリシー] ビューの [予約検索の設定] ペインにある [検索除外] に移動します。
2. 検索から除外するファイル、フォルダ、または拡張子を指定します。
   - **フォルダ:** 検索から除外するフォルダのパスを指定します。
   - **ファイル:** 検索から除外するファイルのパスを指定します。
   - **ファイル拡張子:** 検索から除外するファイルのタイプをファイル拡張子で指定します。

デバイスコントロールを設定する

USB ドライブ、CD/DVD ドライブ、フロッピーディスクドライブやネットワークドライブなどの外部デバイスのアクセスを許可またはブロックします。除外を設定して、信頼する USB デバイスからのアクセスを許可することもできます。

デバイス情報を取得する

次のいずれかの方法で、エージェントに接続されているデバイスの情報を取得します。

- エージェントで**デバイスマネージャ**を開きます。
- エージェントで、次の項に示すコマンドを指定して ***SLCmd.exe*** を実行します。
- StellarOne の管理サーバ画面で [エージェントイベント] 画面に移動し、**エージェントイベント ID 5001** のリムーバブルデバイスの [詳細情報の表示] をクリックします。

信頼する USB デバイスのコマンド

StellarProtect (Legacy Mode) エージェントで、コマンドラインインタフェースに次の形式でコマンドを入力して、信頼する USB デバイスリストを設定します。

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

次の表は、使用可能なパラメータの省略表記一覧を示しています。

パラメータ	省略表記	用法
trustedusbdevice	tud	信頼する USB デバイスリストを管理します

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

コマンド	パラメータ	説明
show usbinfo	<drive_letter>	USB ストレージデバイスの識別子 (VID/PID/SN) を表示します たとえば、USB ストレージデバイスが D ドライブにある場合は、次のように入力します。 SLCmd.exe -p <admin_password> show usbinfo d
show trustedusbdevice		すべての信頼する USB ストレージデバイスを表示します たとえば、次のように入力します。SLCmd.exe -p <admin_password> show trustedusbdevice

コマンド	パラメータ	説明
add trustedusbdevice	[-vid <VID>] [-pid <PID>] [-sn <SN>]	指定した識別子を持つ、信頼する USB ストレージデバイスを追加します。識別子は 1 つ以上指定する必要があります。 たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add trustedusbdevice -sn 123456
remove trustedusbdevice	[-vid <VID>] [-pid <PID>] [-sn <SN>]	指定した識別子を持つ、信頼する USB ストレージデバイスを削除します。 識別子は 1 つ以上指定する必要があります。 たとえば、次のように入力します。 SLCmd.exe -p <admin_password> remove trustedusbdevice -sn 123456

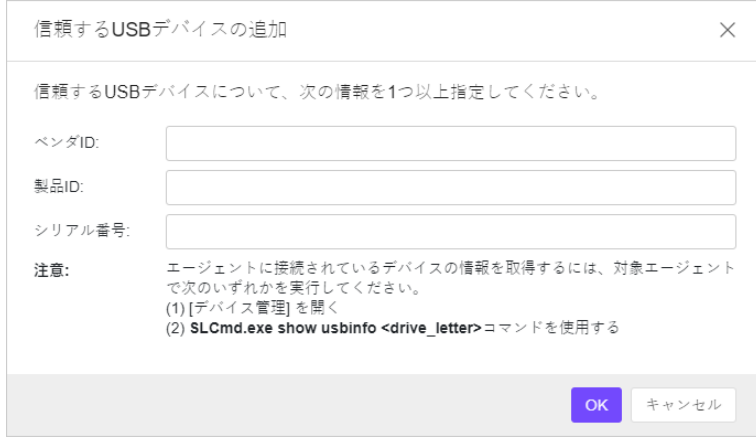
信頼する USB デバイスを追加する

デバイス情報に基づいて、管理下のエージェントへのアクセスを許可する USB ストレージデバイスを指定できます。

手順

1. [エージェント] リストで対象のエージェントまたはエージェントグループに移動します。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
   - [ポリシーの継承] リンクをクリックします。
   - [処理] の**ポリシー**アイコン ( ) をクリックします。
3. [ポリシー] ビューで [デバイスコントロール] ペインに移動します。
4. **スイッチ**を切り替えて、[ベンダ ID、シリアル番号、および製品 ID によって信頼する USB デバイスのみを許可する] を有効にします。[信頼する USB デバイスリスト] が表示されます。
5. [追加] ボタンをクリックすると、[信頼する USB デバイスの追加] 画面が表示されます。
6. 信頼する USB デバイスについて、次の情報を 1 つ以上指定し、[OK] ボタンをクリックします。
   - **ベンダ ID**
   - **製品 ID**

- **シリアル番号**



注意

エージェントにある信頼する USB デバイスのリストを表示するには、エージェントの設定をエクスポートします。エージェントにある信頼する USB デバイスのリストを手動で設定するには、SLCmd コマンドを使用してエージェントの設定をエクスポートするか、変更を行うか、アップデートした設定ファイルをインポートします。

信頼する USB デバイスを編集する

手順

1. [ポリシー] ビューで [デバイスコントロール] ペインに移動します。
2. **スイッチ**を切り替えて、[ベンダ ID、シリアル番号、および製品 ID によって信頼する USB デバイスのみを許可する] を有効にします。[信頼する USB デバイスリスト] が表示されます。
3. 編集する信頼する USB デバイスを選択します。
4. [編集] ボタンをクリックすると、確認画面が表示されます。
5. [OK] ボタンをクリックして設定を保存します。

ポリシーの設定により、信頼する USB デバイスを削除する

手順

1. [ポリシー] ビューで [デバイスコントロール] ペインに移動します。
2. **スイッチ**を切り替えて、[ベンダ ID、シリアル番号、および製品 ID によって信頼する USB デバイスのみを許可する] を有効にします。[信頼する USB デバイスリスト] が表示されます。
3. 削除する信頼する USB デバイスを選択します。
4. [削除] ボタンをクリックすると、[通知] 画面が表示されます。
5. [確認] ボタンをクリックして設定を保存します。

設定のインポートにより、信頼する USB デバイスを削除する

手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。[エージェント] 画面が表示されます。
2. 1 つ以上のエージェントを選択します。
3. [インポート/エクスポート]→[エージェントの設定のエクスポート] の順にクリックします。
4. [ステータス] で [ダウンロード] リンクをクリックし、エージェント設定ファイルをコンピュータにダウンロードします。
5. エージェント設定ファイルをテキストエディタで開き、**<DeviceException>** セクションを見つけます。

信頼する USB デバイスが追加されていない場合、空の <DeviceException> セクションが次のように表示されます。

```
<StorageDeviceBlocking Enable="no" ActionMode="1">
       <DeviceException>
              <DeviceGroup name="UserDefined"/>
       </DeviceException>
</StorageDeviceBlocking>
```

信頼する USB デバイスの 2 つのエントリが追加されている場合、<DeviceException> セクションは次のように表示されます。

```
<StorageDeviceBlocking Enable="no" ActionMode="1">
<DeviceException>
       <DeviceGroup name="UserDefined">
              <Device vid="781" pid="5151" sn="2444130A5442A4F5"/>
              <Device vid="951" pid="1666"
              sn="E03F49AEC0DDF351E913003F"/>
       </DeviceGroup>
</DeviceException>
</StorageDeviceBlocking>
```

6. 目的の信頼する USB デバイスのエントリを削除し、エージェント設定ファイルを保存します。
7. 更新したエージェント設定ファイルをインポートします。

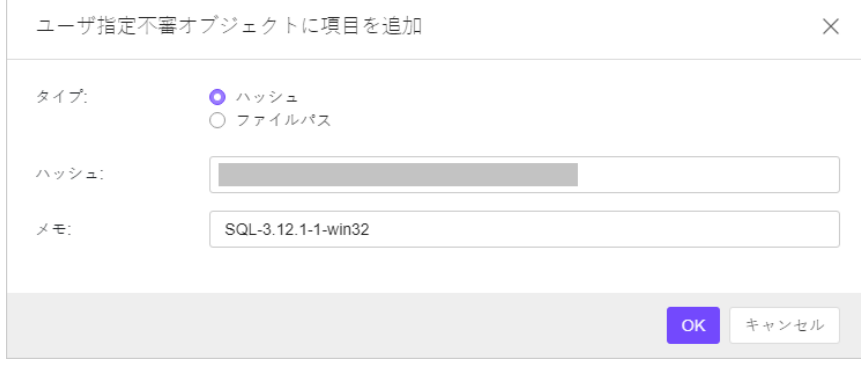
ユーザ指定不審オブジェクトを設定する

ユーザ指定不審オブジェクトを設定すると、TXOne の研究者により発見された不正プログラムからシステムを保護することができます。

ユーザ指定不審オブジェクトを追加する

手順

1. [エージェント] リストで対象のエージェントまたはエージェントグループに移動します。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
   - [ポリシーの継承] リンクをクリックします。
   - [処理] の**ポリシー**アイコン ( ) をクリックします。
3. [ポリシー] ビューで [ユーザ指定不審オブジェクト] ペインに移動します。
4. [追加] ボタンをクリックすると、[ユーザ指定不審オブジェクトに項目を追加] 画面が表示されます。
5. 変更後、[OK] ボタンをクリックして設定を保存します。



ユーザ指定不審オブジェクトを削除する

手順

1. [ポリシー] ビューで [ユーザ指定不審オブジェクト] ペインに移動します。
2. 削除するハッシュ/ファイルパスを選択します。
3. [削除] ボタンをクリックすると、確認画面が表示されます。

4. [確認] ボタンをクリックして、選択した項目を削除します。

エージェントのパスワードを設定する

StellarOne の管理サーバ画面を使用して、StellarProtect (Legacy Mode) エージェントのパスワードをリモートで更新します。新しいパスワードの作成に古いエージェントのパスワードは必要ありません。

手順

1. [エージェント] リストで対象のエージェントまたはエージェントグループに移動します。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
   - [ポリシーの継承] リンクをクリックします。
   - [処理] の**ポリシー**アイコン ( ) をクリックします。
3. [ポリシー] ビューで [エージェントのパスワード] ペインに移動します。
4. [新しいパスワード] と [パスワードの確認] を入力します。
5. [保存] ボタンをクリックして設定を保存します。

注意

この機能を利用できるのは、管理者またはオペレータの権限を持つユーザだけです。管理者またはオペレータの権限を持つユーザは、エージェント管理者のパスワードをリモートで変更できます。

Patch を設定する

手順

1. [エージェント] リストで対象のエージェントまたはエージェントグループに移動します。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
   - [ポリシーの継承] リンクをクリックします。
   - [処理] の**ポリシー**アイコン ( ) をクリックします。
3. [ポリシー] ビューで [Patch] ペインに移動します。
4. 適用する Patch の横にあるチェックボックスをオンにします (複数可)。
5. [アップデート] リンクをクリックして、新しい Patch をインポートします。
6. リンクをクリックして、[ダウンロード/アップデート] 画面に移動します。
7. [確認] ボタンをクリックして設定を保存します。

注意

Patch のバージョンが現在のエージェントのバージョンよりも低い場合は、その Patch を適用しないでください。ステータスは非同期のままとなり、他のポリシーも配信されません。20 分待てば、他のポリシーがエージェントに適用可能になります。

第 4 章

エージェントの保護とアップデート

メンテナンスモードを設定する

エージェントでアップデートを実行するには、メンテナンスモードを設定します。これにより、StellarProtect (Legacy Mode) がすべてのファイルの実行を許可し、作成、実行、または変更されたすべてのファイルを許可リストに追加する期間を定義できます。

> たとえば、Mozilla Firefox をインストールまたはアップデートする必要がある場合は、メンテナンスモードを有効にしてインストールまたはアップデートを許可し、さらに処理中に作成または修正されたファイルを許可リストに追加します。

セキュリティ強化のため、メンテナンス期間後は**ファイルの検索**を有効にして**検出時の処理**を選択できます。

重要

メンテナンスモードを使用する前に、必要なアップデートを次のサポート対象プラットフォームに適用してください。

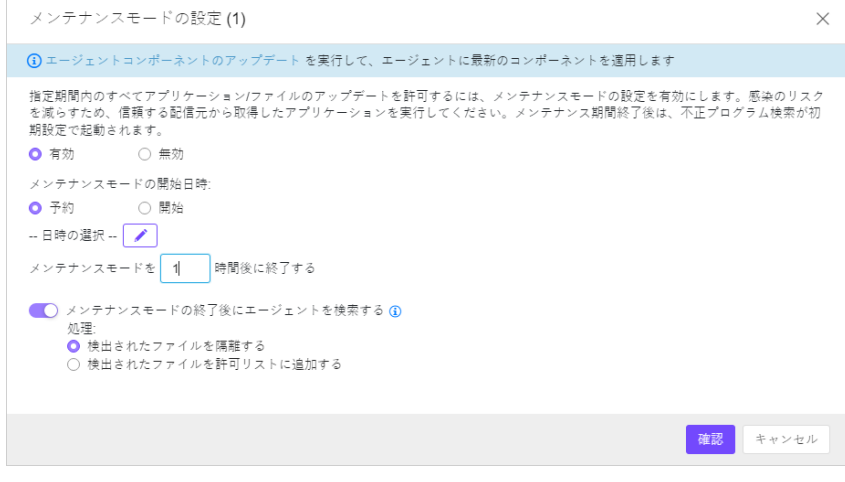
- Windows 2000 Service Pack 4 の場合、Microsoft Update カタログの Web サイトから更新プログラム KB891861 を適用します。
- Windows XP SP1 の場合、Windows XP SP2 にアップグレードします。

注意

- 感染のリスクを減らすため、メンテナンス期間中は、信頼する配信元から取得したアプリケーションのみをエージェント上で実行してください。
- エージェントでは、一度に 1 つの予約されたメンテナンス期間を開始できます。新しいメンテナンス期間を設定すると、まだ開始されていない既存のメンテナンスの予約が上書きされます。
- メンテナンスモードを終了しようとしているときにエージェントを再起動すると、StellarProtect (Legacy Mode) がキュー内のファイルを許可リストに追加できなくなります。
- メンテナンス期間中、エージェントの Patch のアップデートは実行できません。
- メンテナンスモードが有効な場合、StellarProtect (Legacy Mode) では、メンテナンス期間中にエージェントの再起動を必要とする Windows Update がサポートされません。
- メンテナンス期間中にネットワークフォルダにファイルを配信するインストーラを実行するには、StellarProtect (Legacy Mode) にネットワークフォルダに対するアクセス権限が必要です。
- メンテナンスモードでは Microsoft Windows Visual Studio デバッガはサポートされないことに注意してください。

手順

1. [エージェント] ビューで対象のエージェントまたはエージェントグループに移動します。
2. 横にあるチェックボックスをオンにして、エージェント (またはグループ) を 1 つ以上選択します。
3. [エージェント] 画面の上部にあるツールバーで 保護 ボタンをクリックします。
4. [メンテナンスモードの設定] オプションをクリックし、さらに [保護] メニュー画面の [確認] ボタンをクリックします。設定画面が表示されます。



5. [有効] または [無効] を選択します。
   - メンテナンスモードの設定を開始するには、[有効] をクリックします。
   - メンテナンスモードを終了するか、予約されたメンテナンス期間を中止するには、[無効] をクリックします。
6. [予約] または [開始] を選択します。
   - [予約] を選択した場合は、メンテナンス期間を指定する必要があります。
   - [メンテナンスモードの終了後にエージェントを検索する] を選択すると、StellarProtect (Legacy Mode) はメンテナンス期間終了後にエージェントで脅威を検索します。
7. 目的の処理を選択します。
   - **検出されたファイルを隔離する**
   - **検出されたファイルを許可リストに追加する**

注意

StellarProtect (Legacy Mode) は、メンテナンス期間中にエージェントで作成、実行、または変更されたファイルを検索します。

8. [確認] ボタンをクリックして、選択したエージェントまたはグループに設定を配信します。
9. [コマンド配信] 画面に配信ステータスが表示されます。この画面は、[閉じる] ボタンをクリックして閉じることができます。

許可リストをアップデートする

アプリケーション制御が有効な場合は、実行したいアプリケーションを新規インストールした後、StellarProtect (Legacy Mode) エージェントの許可リストを定期的にアップデートしてください。許可リストのアップデートを実行すると、選択したエージェントの許可リストが再作成され、新たに検出されたアプリケーションがグローバルな許可リストに追加されます。

StellarProtect (Legacy Mode) でエージェントの保護を開始するには、最初に、エージェントをチェックしてシステムの正常な実行に必要なアプリケーションとファイルを確認する必要があります。StellarProtect (Legacy Mode) のアプリケーション制御が有効な場合は、許可リストに含まれるアプリケーションのみを実行できます。

許可リストを設定した後は、メンテナンスモードを有効にすることで新しいプログラムも追加できるようになり、新しいファイルまたは変更済みのファイルが許可リストに追加されます。

手順

1. [エージェント] リストで対象のエージェントまたはエージェントグループに移動します。
2. 横にあるチェックボックスをオンにして、エージェント (またはグループ) を 1 つ以上選択します。
3. [エージェント] 画面の上部にあるツールバーで 保護 ボタンをクリックします。
4. [許可リストのアップデート] オプションをクリックし、さらに [保護] メニュー画面の [確認] ボタンをクリックします。確認画面が表示されます。
5. [OK] ボタンをクリックして許可リストをアップデートします。

注意

アップデート中はエージェントを再起動したりシャットダウンしたりしないでください。アップデートプロセスの完了には 30 分以上かかることがあります。

検索開始を設定する

選択したエージェントで手動検索を開始し、検索を設定して、1 つまたは複数の StellarProtect (Legacy Mode) の対象エージェントに配信できます。

検索開始を実行する

感染が疑われる 1 つ以上のエージェントに対して検索開始を実行できます。

手順

1. [エージェント] リストで対象のエージェントまたはエージェントグループに移動します。
2. 横にあるチェックボックスをオンにして、エージェント (またはグループ) を 1 つ以上選択します。
3. [エージェント] 画面の上部にあるツールバーで 保護 ボタンをクリックします。
4. [検索開始] オプションをクリックし、さらに [保護] メニュー画面の [確認] ボタンをクリックします。確認画面が表示されます。
5. 検索の設定後、[OK] ボタンをクリックして検索開始を実行します。

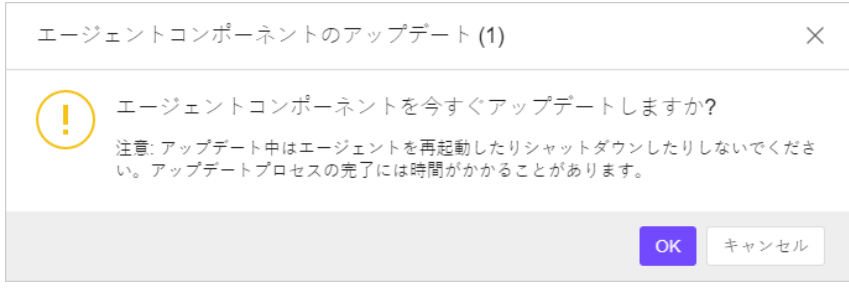
サーバから選択した StellarProtect (Legacy Mode) エージェントに通知が送信されます。検索のステータスについてログを確認できます。

エージェントコンポーネントのアップデート

選択したエージェントに対して、StellarOne からエージェントコンポーネントのアップデートプロセスを開始できます。エージェントは、最新のコンポーネントアップデートをダウンロードします。エージェントコンポーネントを定期的にアップデートすることで、最新のセキュリティリスクからエージェントを保護できます。

手順

1. [エージェント] 表で対象のエージェントまたはエージェントグループに移動します。
2. 横にあるチェックボックスをオンにして、エージェント (またはグループ) を 1 つ以上選択します。
3. [エージェント] 画面の上部にあるツールバーで アップデート ボタンをクリックします。
4. [エージェントコンポーネントのアップデート] オプションをクリックし、さらに [アップデート] メニュー画面の [確認] ボタンをクリックします。確認画面が表示されます。
5. [OK] ボタンをクリックしてエージェントコンポーネントをアップデートします。



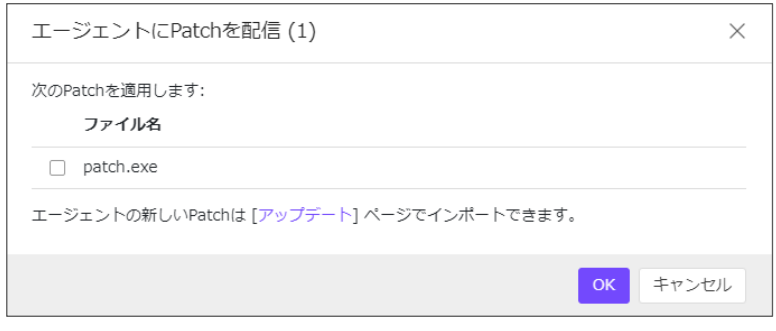
エージェントに Patch を配信する

StellarOne を使用して、アップロードした Patch ファイルを選択した StellarProtect (Legacy Mode) エージェントに配信することで、管理サーバ画面からリモートでエージェントをアップグレードできます。

手順

1. [エージェント] リストで対象のエージェントまたはエージェントグループに移動します。
2. 横にあるチェックボックスをオンにして、エージェント (またはグループ) を 1 つ以上選択します。
3. [エージェント] 画面の上部にあるツールバーで アップデート ボタンをクリックします。
4. [エージェントに Patch を配信] オプションをクリックし、さらに [アップデート] メニュー画面の [確認] ボタンをクリックします。確認画面が表示されます。

5. 設定後、[OK] ボタンをクリックします。



アップロードプロセスの完了を待ちます。StellarOne でファイルの有効性が検証されると、選択したエージェントに Patch ファイルが配信されます。

注意

Windows 7 SP1 以前のバージョンでは、StellarProtect (Legacy Mode) 1.0 エージェントへの Patch のリモート配信はサポートされません。

接続を確認する

選択した StellarProtect (Legacy Mode) エージェントの接続ステータスを確認します。

手順

1. [エージェント] リストで対象のエージェントまたはエージェントグループに移動します。
2. 横にあるチェックボックスをオンにして、エージェント (またはグループ) を 1 つ以上選択します。
3. [エージェント] 画面の上部にあるツールバーで アップデート ボタンをクリックします。
4. [接続の確認] オプションをクリックし、さらに [確認] ボタンをクリックします。画面が表示されます。
5. [ステータス] または [製品] の基準を選択して、接続ステータスを確認します。

注意

- StellarOne サーバに接続できないエージェントを特定したら、接続されていないエージェントのネットワーク接続を確認することをお勧めします。
- 初期設定では、エージェントは StellarOne の管理サーバ画面と **20** 分ごとに自動同期されます。

イベントログを収集する

ログにはエージェントのアクティビティに関する情報が含まれています。イベントログを収集することで、StellarOne のデータベースを更新し、選択したエージェント情報を最新の状態にすることができます。

手順

1. [エージェント] リストで対象のエージェントに移動します。
2. 横にあるチェックボックスをオンにして、エージェントを 1 つ以上選択します。
3. [エージェント] 画面の上部にあるツールバーで アップデート ボタンをクリックします。
4. [イベントログの収集] オプションをクリックし、さらに [確認] ボタンをクリックします。

ログとステータスが StellarProtect (Legacy Mode) エージェントから StellarOne に正常に送信されると、[前回の接続] 列に表示される日付と時刻が更新されます。

注意

ユーザは次のログの情報レベル (Setup.ini) を有効にして、エージェントのアクティビティに関する情報を含める必要があります。

```
[EventLog]
Enable = 1
Level_WarningLog = 1
Level_InformationLog = 1
```

第 5 章

エージェントの設定のインポート/エクスポート

以下の機能はエージェントレベル専用です。ユーザがリストから任意のグループを選択する際、この機能は無効化されています。

エージェントの設定をエクスポートする

StellarOne の管理サーバ画面からエージェントの設定と許可リストをエクスポートしてダウンロードすることにより、それらをリモートで取得できます。

エージェントの設定をエクスポートする

手順

1. [エージェント] リストで対象のエージェントまたはエージェントグループに移動します。
2. 横にあるチェックボックスをオンにして、対象のエージェントを選択します。
3. [エージェント] 画面の上部にあるツールバーで インポート/エクスポート ボタンをクリックします。
4. [エージェントの設定のエクスポート] オプションをクリックし、さらに [インポート/エクスポート] メニュー画面の [確認] ボタンをクリックします。画面が表示されます。

5. [ダウンロード] リンクをクリックして、エージェントの設定ファイルをダウンロードします。[詳細] ポップアップ画面で進行状況を確認できます。

許可リストをエクスポートする

手順

1. [エージェント] リストで対象のエージェントまたはエージェントグループに移動します。
2. 横にあるチェックボックスをオンにして、対象のエージェントを選択します。
3. [エージェント] 画面の上部にあるツールバーで インポート/エクスポート ボタンをクリックします。

4. [許可リストのエクスポート] オプションをクリックし、さらに [インポート/エクスポート] メニュー画面の [確認] ボタンをクリックします。画面が表示されます。

5. [ダウンロード] リンクをクリックして、許可リストファイルをダウンロードします。[詳細] ポップアップ画面で進行状況を確認できます。

エージェントの設定をインポートする

StellarOne の管理サーバ画面から、新しいエージェントの設定をリモートで適用できます。この機能により次のことが可能になります。

- エージェントの設定をリモートで上書きする
- 許可リストをリモートで上書きする

カスタマイズしたエージェントの設定ファイルまたは許可リストを必ず最初に準備してください。

- エージェントの設定ファイルまたは許可リストをエクスポートしてダウンロードします。
- ダウンロードしたファイルをカスタマイズします。

正常にインポートするため、インポートするファイルが次の要件を満たしていることを確認します。

- 許可リストの場合、ファイルが CSV 形式で UTF-8 エンコーディングを使用している
- サポートされるファイルの最大サイズは **20MB**
- エージェントの設定ファイルの場合、ファイルが XML 形式で、サポートされるファイルの最大サイズは **1MB**

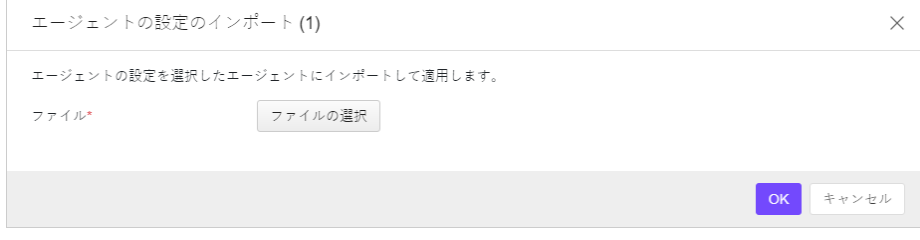
エージェントの設定をインポートする

手順

1. [エージェント] リストで対象のエージェントまたはエージェントグループに移動します。
2. 横にあるチェックボックスをオンにして、対象のエージェントを選択します。
3. [エージェント] 画面の上部にあるツールバーで インポート/エクスポート ボタンをクリックします。

4. [エージェントの設定のインポート] オプションをクリックし、さらに [インポート/エクスポート] メニュー画面の [確認] ボタンをクリックします。画面が表示されます。

5. [ファイルの選択] をクリックしてファイルを選択し、[OK] ボタンをクリックして設定のインポートを開始します。



許可リストをインポートする

手順

1. [エージェント] リストで対象のエージェントまたはエージェントグループに移動します。
2. 横にあるチェックボックスをオンにして、対象のエージェントを選択します。
3. [エージェント] 画面の上部にあるツールバーで インポート/エクスポート ボタンをクリックします。

4. [許可リストのインポート] オプションをクリックし、さらに [インポート/エクスポート] メニュー画面の [確認] ボタンをクリックします。画面が表示されます。

5. [ファイルの選択] をクリックしてファイルを選択し、[OK] ボタンをクリックして許可リストのインポートを開始します。

注意

[既存アプリケーションの信頼するハッシュ値を更新します。] スイッチは、(許可リスト内の) 既存の信頼するハッシュ値を上書きする場合に使用します。

エージェントの処理

タグを編集する

エージェントの識別と検索に役立つタグを編集できます。タグを編集するには、次の手順に従います。

- 各エージェントの [処理] メニューから
- [編成] ボタンの [タグの編集] から

手順

1. [エージェント] 画面に移動します。
2. 横にあるチェックボックスをオンにして、エージェントを 1 つ以上選択します。
3. [処理] にある [さらに処理を表示] アイコンをクリックします。
4. [タグの編集] をクリックし、内容を入力または変更します。
5. [確認] ボタンをクリックします。

移動する

複数エージェントの管理を容易にするため、場所、種類、または目的に応じてエージェントをグループ化します。

- 各エージェントの [処理] メニューから
- [編成] ボタンの [タグの編集] から

手順

1. [エージェント] 画面に移動します。
2. 横にあるチェックボックスをオンにして、エージェントを 1 つ以上選択します。
3. [処理] にある [さらに処理を表示] アイコンをクリックします。
4. [移動] をクリックし、対象の**グループ名**を選択します。

5. [確認] ボタンをクリックします。

削除する

StellarOne サーバからエージェントを削除します。

エージェントの StellarOne からの削除は、エージェントのアンインストール時に試行されます。ただし、StellarProtect (Legacy Mode) が StellarOne に接続されていなければエージェントを削除することはできません。

エージェントを環境から削除する前にアンインストールできない場合、そのエージェントが [エージェント] 画面に表示されたままになることがあります。今後 StellarOne で管理しないエージェントを監視対象エージェントのリストから削除するには、[削除] 機能を使用します。

手順

1. [エージェント] 画面に移動します。
2. 横にあるチェックボックスをオンにして、エージェントを 1 つ以上選択します。
3. [処理] にある [さらに処理を表示] アイコンをクリックします。
4. [削除] をクリックし、対象のグループ名を選択します。
5. [確認] ボタンをクリックして、選択した項目を削除します。リストからエージェントが削除されます。

注意

監視対象エージェントのリストからエージェントを削除しても、既存のエージェントイベントログは削除されません。

第 6 章

StellarProtect (Legacy Mode) の監視

StellarProtect (Legacy Mode) の監視

この章では、StellarOne の管理サーバ画面の監視方法の概要について説明します。

ダッシュボードについて

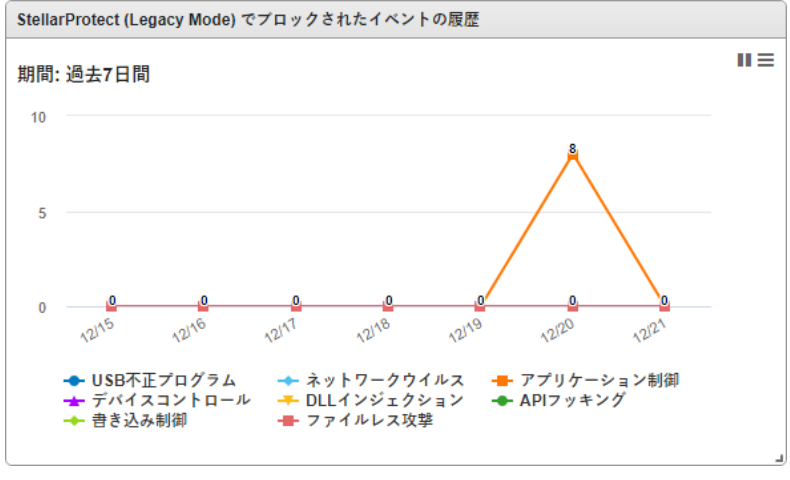
[ダッシュボード] では、[概要] タブに表示される情報を使用してイベントを監視します。このタブは、ユーザ指定のタブがない場合に初期設定で [ダッシュボード] に追加されます。

[概要] タブと [システム] タブに含まれる初期設定のウィジェットには、[ブロックされたイベントの履歴]、[イベントをブロックしたエージェントの上位]、[CPU 使用率]、[メモリ使用率]、および [ディスク使用率] があります。

ブロックされたイベントの履歴

このウィジェットには、指定した期間内にブロックされたイベントの概要が表示されます。初期設定で、このウィジェットは [ダッシュボード] の [イベントの概要] タブに表示されます。表示アイコンをクリックすると、データが円グラフまたは折れ線グラフで表示されます。

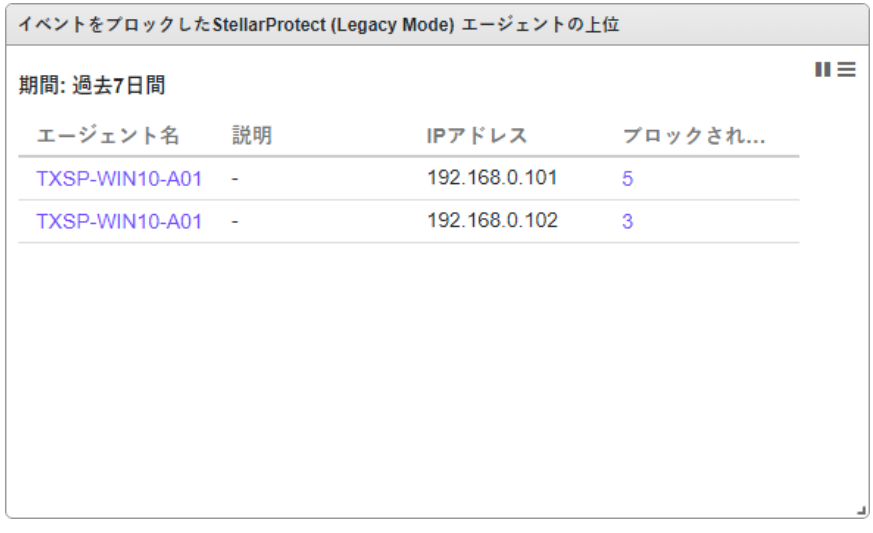
- 指定した期間内のイベントデータのみを表示するには、[期間] のドロップダウンを使用します。
- グラフ下に並ぶカテゴリをクリックすると、そのイベントのデータが表示または非表示になります。
- グラフの値をクリックすると、ブロックされたイベントの詳細が表示されます。



ブロック件数が上位のエージェント

このウィジェットには、ブロック件数が上位のエージェントが表示されます。初期設定で、このウィジェットは [ダッシュボード] の [イベントの概要] タブに表示されます。

列	説明
エージェント名	エージェントの名前
説明	エージェントに割り当てられたタグ
IP アドレス	エージェントの IP アドレス
ブロックされたイベント	エージェントでブロックされたイベントの合計数



[ブロックされたイベント] 列の値をクリックすると、そのイベントの詳細が表示されます。指定した期間内のイベントデータのみを表示するには、[期間] のドロップダウンを使用します。表示するイベント数を指定するには、[ウィジェット設定] ダイアログを開き、[表示するイベント] の値を選択します。

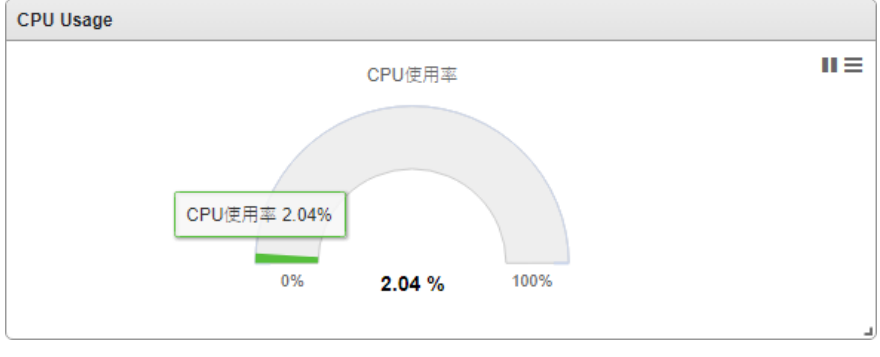
ブロックされた件数が上位のファイル

このウィジェットには、ブロック件数が上位のファイルのリストが表示されます。初期設定ではダッシュボードに表示されません。

列	説明
ファイル名	ブロックされたファイルの名前
ファイルハッシュ	ブロックされたファイルの SHA-1 ハッシュ
エージェント	当該ファイルのブロックイベントを報告したエージェントの数
ブロックされたイベント	当該ファイルについて報告されたブロックイベントの合計数

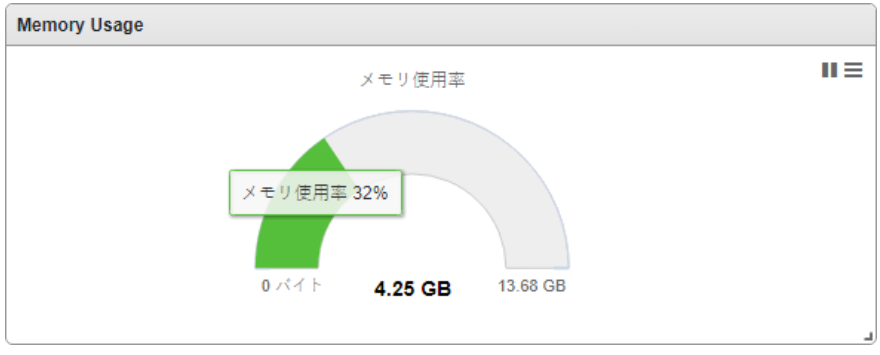
CPU 使用率

このウィジェットには、CPU の使用率情報が表示されます。



メモリ使用率

このウィジェットには、メモリの使用率情報が表示されます。



ディスク使用率

このウィジェットには、ディスクの使用率情報が表示されます。

ウィジェットを追加する

タブに追加できるウィジェットの数は、タブのレイアウトに応じて異なります。

タブに含まれるウィジェットが最大数に達した場合は、ウィジェットをタブから削除するか、追加するウィジェットに対して新しいタブを作成する必要があります。

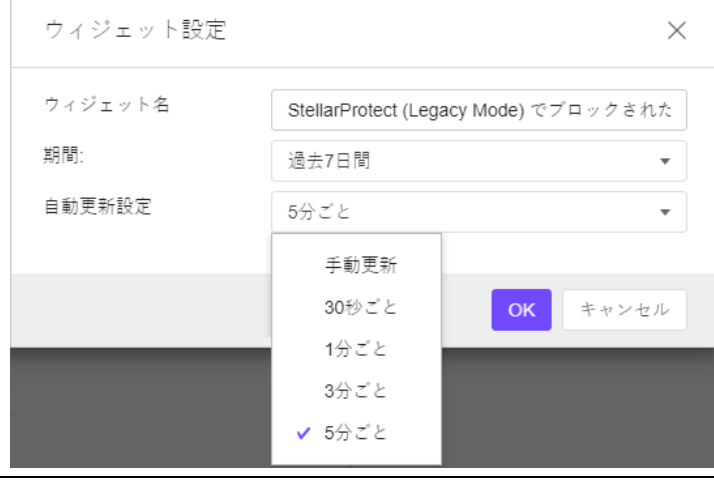
手順

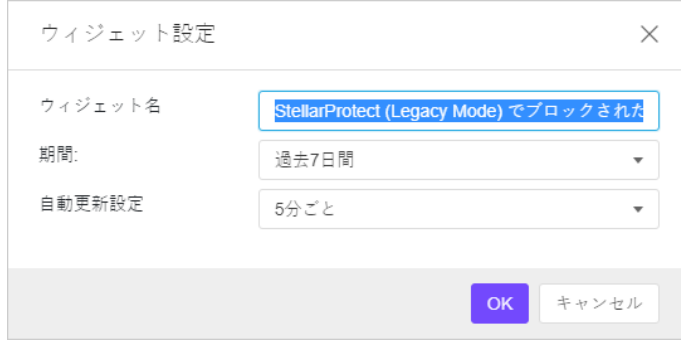
1. 管理サーバ画面の上部にあるナビゲーションで [ダッシュボード] を選択します。
2. ダッシュボードで、ウィジェットを追加するタブ ([概要] または [システム]) を選択します。
3. [ウィジェットの追加] をクリックして画面を表示します。

4. 現在のタブに追加するウィジェットを 1 つ以上選択し、[追加] をクリックします。

ウィジェットを使用する

各ウィジェットで次のタスクを実行します。

タスク	手順
ウィジェットの移動	ウィジェット上部のタイトルバーをクリックしたままドラッグして、タブ内の任意の場所に移動します。
ウィジェットのサイズ変更	ウィジェットの端をドラッグしてサイズを変更します。
ウィジェットデータの表示更新	最初は [ウィジェット設定] で [自動更新設定] を指定します (初期設定値は [5 分ごと])。 
ウィジェット名の変更	1. ウィジェットの上部にある [その他のオプション] アイコンをクリックします。 2. [ウィジェット設定] を選択します。[ウィジェット設定] 画面が表示されます。 3. わかりやすい**ウィジェット名**を入力します。

タスク	手順
	
ウィジェットを閉じる	1. ウィジェットの上部にある [その他のオプション] アイコンをクリックします。 2. [ウィジェットの削除] を選択します。 
期間の設定	指定した期間のデータを表示します (初期設定値は [過去 7 日間])。 

[エージェントイベント] 画面について

[エージェントイベント] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで、[ログ]→[エージェントイベント] の順に選択します。この画面には、StellarOne の管理下のエージェントの許可リストにないアプリケーションに関するイベントのリストが表示されます。

StellarProtect (Legacy Mode) は、「機能の状態」に基づいて、次の表のイベントに対応した処理を行い、ログを生成します。イベントログには、許可リストにないファイルと実行された処理に関する、管理下のエージェントからの情報が含まれます。

イベント	機能の状態	StellarProtect (Legacy Mode) の処理
エージェントの許可リストにないファイルが動作しようとしたり、エージェントに変更を加えようとしたりする	ロックダウンが無効	ファイルの動作を許可します
	ロックダウンが有効	ファイルをブロックし、ユーザ処理を求めるプロンプトを表示します
ストレージデバイス (CD/DVD ドライブ、フロッピーディスク、または USB デバイス) がエージェントにアクセスしようとする	デバイスコントロールが無効	デバイスのアクセスを許可します
	デバイスコントロールが有効	(デバイスの種類がリムーバルデバイスの場合) デバイスのアクセスを拒否し、ユーザ処理を求めるプロンプトを表示します

次の表は、イベントに対するユーザ処理を示しています。

ユーザ処理	説明
許可リストに追加	検出されたタイミングではファイルの実行を防いだり USB デバイスのエンドポイントへのアクセスを拒否したりしますが、ファイルまたは USB デバイスをエージェントの許可リストに追加します。これにより、以降の検出についてファイルの実行または USB デバイスのアクセスが許可されるようになります。
無視	ファイルの実行は防ぎますが、ファイルの移動や変更は行いません。
隔離	ファイルの実行を防ぎ、後で分析するためにファイルを隔離します。
削除	ファイルの実行を防ぎ、ファイルを削除します。

エージェントイベントログをクエリする

クエリを実行すると、表示されるエージェントイベントログのリストが更新されます。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [ログ]→[エージェントイベント] の順に選択します。[エージェントイベント] 画面が表示されます。
2. 期間でフィルタするには、初期設定が [過去 30 日間] である [期間] のドロップダウンをクリックして、期間を選択します。次のいずれかを実行します。
   - リストされる期間をクリックします。
   - [カスタム] をクリックし、期間を指定して [検索] をクリックします。
3. [エージェント名]、[エージェントグループ]、[IP アドレス]、[IP アドレスの範囲]、[タグ]、[イベントのタイプ]、[重大度]、[変更監視]、[ブロックされたファイル]、または [不正プログラム検出] でフィルタするには、検索バーの左側にあるドロップダウンをクリックして条件を指定します。
   - エージェント名: 探しているエージェントの名前を指定します。
   - エージェントグループ: 探しているグループの名前を指定します。
   - IPアドレス: 探しているエージェントのIPアドレスを指定します。
   - IPアドレスの範囲: エージェントを検索するIPアドレスの範囲を指定します。
   - タグ: エージェントに割り当てられたタグを指定します。
   - イベントのタイプ: 特定のイベントを選択し、[適用] をクリックします。
   - 重大度: イベントレベルとして [情報] または [警告] を選択します。
   - 変更監視: [ファイルまたはフォルダ] または [レジストリキーまたはレジストリ値] を選択し、[検索] をクリックします。[ファイルまたはフォルダ] 検索では、文字列の部分一致がサポートされます。
   - ブロックされたファイル: [ファイル名] または [ファイルハッシュ (SHA-1)] を選択し、[検索] をクリックします。[ファイル名] 検索では、文字列の部分一致がサポートされます。
   - 不正プログラム検出: [すべての検出]、[失敗した処理]、[駆除されました]、[隔離されました]、[削除されました]、[無視されました]、または [ロールバックされました] を選択します。

4. 選択したフィルタに一致するエントリのみが表に表示されます。

エージェントイベントをエクスポートする

選択したエージェントのイベントログエントリに関するデータを **CSV** ファイル形式で保存します。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [ログ]→[エージェントイベント] の順に選択します。[エージェントイベント] 画面が表示されます。
2. 情報をエクスポートするエージェントログエントリをリストから選択します。
   - すべてのエントリをエクスポートするには、右上にある [すべてエクスポート] をクリックします。
   - 選択したエントリのみをエクスポートするには、エクスポートするエントリを選択し、左上にある [選択内容のエクスポート] ボタンをクリックします。
3. ファイルを保存します。

[サーバイベント] 画面について

[サーバイベント] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで、[ログ]→[サーバイベント] の順に選択します。

この画面には、StellarProtect、StellarProtect (Legacy Mode)、および StellarOne の監査対象 StellarOne ユーザアカウントのアクティビティのログが表示されます。

注意

サーバイベントログには、StellarOne のユーザアカウントとポリシーにより実行された処理について収集された情報が含まれます。

サーバイベントログをクエリする

クエリを実行すると、表示されるサーバイベントログのリストが更新されます。

手順

1. 管理サーバ画面の上部にあるナビゲーションで、[ログ]→[サーバイベント] の順に選択します。[サーバイベント] 画面が表示されます。
2. [サーバイベント] のドロップダウンリストをクリックします。検索条件のリストが表示されます。
3. 目的の検索条件を選択します。選択した条件に応じた検索フィールドが表示されます。
4. 選択した条件に応じた手順を実行します。

オプション	説明
期間	次のいずれかを実行します。 • リストから期間を選択します。 • 期間をカスタマイズして指定します。 a. リストの [カスタム範囲] を選択します。 b. カスタマイズする期間を指定します。 c. [適用] をクリックします。
ユーザ ID	特定のユーザによりログに記録されたすべてのイベントを表示します。
エージェント名	エージェントのホスト名 (最初の数文字またはすべて) を入力し、[検索] をクリックします。
グループ名	特定のグループによりログに記録されたすべてのイベントを表示します。
イベントのタイプ	特定のイベントを選択します。

サーバイベントログのリストに検索結果が表示されます。

サーバイベントログをエクスポートする

選択したサーバのイベントログエントリに関するデータを CSV ファイル形式で保存します。

手順

1. 管理サーバ画面の上部にあるナビゲーションで、[ログ]→[サーバイベント] の順に選択します。[サーバイベント] 画面が表示されます。
2. 情報をエクスポートするサーバログエントリをリストから選択します。
   - すべてのエントリをエクスポートするには、[すべてエクスポート] アイコンをクリックします。
   - 選択したエントリのみをエクスポートするには、エクスポートするエントリを選択し、[選択内容のエクスポート] をクリックします。
3. ファイルを保存します。

[システムログ] 画面について

[システムログ] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで、[ログ]→[システムログ] の順に選択します。この画面には、調整可能な StellarOne の管理サーバ画面の設定のログが表示されます。

サーバログをクエリする

クエリを実行すると、表示されるサーバイベントログのリストが更新されます。

手順

1. 管理サーバ画面の上部にあるナビゲーションで、[ログ]→[システムログ] の順に選択します。[システムログ] 画面が表示されます。
2. 目的の検索条件を選択します。選択した条件に応じた検索フィールドが表示されます。
3. 選択した条件に応じた手順を実行します。

オプション	説明
期間	次のいずれかを実行します。 • リストから期間を選択します。 • 期間をカスタマイズして指定します。 a. リストの [カスタム] を選択します。 b. カスタマイズする期間を指定します。 c. [検索] をクリックします。
重大度	次のいずれかの条件を選択して、[検索] をクリックします。 • 緊急 • アラート • 重大 • エラー • 警告 • 注意 • 情報 • デバッグ

システムログのリストに検索結果が表示されます。

システムログをエクスポートする

選択したサーバのイベントログエントリに関するデータを CSV ファイル形式で保存します。

手順

1. 管理サーバ画面の上部にあるナビゲーションで、[ログ]→[システムログ] の順に選択します。[システムログ] 画面が表示されます。
2. 情報をエクスポートするシステムログエントリをリストから選択します。
   - すべてのエントリをエクスポートするには、[すべてエクスポート] アイコンをクリックします。
   - 選択したエントリのみをエクスポートするには、エクスポートするエントリを選択し、[選択内容のエクスポート] をクリックします。

[監査ログ] 画面について

[監査ログ] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで、[ログ]→[監査ログ] の順に選択します。この画面には、StellarOne の監査ログが表示されます。

監査ログをクエリする

クエリを実行すると、表示されるサーバイベントログのリストが更新されます。

手順

1. 管理サーバ画面の上部にあるナビゲーションで、[ログ]→[監査ログ] の順に選択します。[監査ログ] 画面が表示されます。
2. 目的の検索条件を選択します。選択した条件に応じた検索フィールドが表示されます。
3. 選択した条件に応じた手順を実行します。

オプション	説明
期間	

オプション	説明
	次のいずれかを実行します。 • リストから期間を選択します。 • 期間をカスタマイズして指定します。 a. リストの [カスタム] を選択します。 b. カスタマイズする期間を指定します。 c. [検索] をクリックします。
ユーザ ID	ユーザ ID を入力し、[検索] をクリックします。
クライアント IP	クライアント IP 番号を入力し、[検索] をクリックします。
重大度	次のいずれかの条件を選択して、[検索] をクリックします。  • 緊急 • アラート • 重大 • エラー • 警告 • 注意 • 情報 • デバッグ

監査ログのリストに検索結果が表示されます。

監査ログをエクスポートする

選択したサーバのイベントログエントリに関するデータを CSV ファイル形式で保存します。

手順

1. 管理サーバ画面の上部にあるナビゲーションで、[ログ]→[監査ログ] の順に選択します。[監査ログ] 画面が表示されます。
2. 情報をエクスポートするシステムログエントリをリストから選択します。
   - すべてのエントリをエクスポートするには、[すべてエクスポート] をクリックします。
   - 選択したエントリのみをエクスポートするには、エクスポートするエントリを選択し、[選択内容のエクスポート] をクリックします。

第 7 章

管理設定

この章では、TXOne StellarOne の管理設定の概要について説明します。

[アカウント管理] 画面について

[アカウント管理] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで [管理]→[アカウント管理] の順に選択します。

この画面は、StellarOne の管理サーバ画面にアクセスするためのアカウントの管理に使用します。TXOne StellarOne の管理サーバ画面にアクセスするためのアカウントには、次の権限があります。

アカウントの種類	権限
管理者 (フルコントロール)	a. StellarOne 管理: システム設定を行うための権限です。 b. グループ管理: グループを作成、移動、または削除するための権限です。 c. アカウント管理: StellarOne アカウントを管理するための権限です。 d. ポリシー設定: USB コントロールや Intelligent Runtime Learning (インテリジェントランタイム学習) など、エージェントのポリシーを定義するための権限です。
オペレータ (資産コントロール)	a. グループ管理: グループを作成、移動、または削除するための権限です。 b. ポリシー設定: USB コントロールや Intelligent Runtime Learning (インテリジェントランタイム学習) など、エージェントのポリシーを定義するための権限です。
閲覧者 (読み取りのみ)	a. [ダッシュボード]、[ポリシー設定]、[エージェントイベント] の読み取りのみです。 b. エージェントインストーラパッケージをダウンロードできます。 c. 自身のアカウントのパスワードを変更します。

サーバアカウントの概要

TXOne StellarOne では、管理サーバ画面にアクセスするためのアカウントにいくつかの権限と制限を適用できます。これらのアカウントを使用して StellarOne を設定し、StellarProtect (Legacy Mode) エージェントを監視または管理できます。次の表は、一般的な StellarOne のタスクと、その実行に必要なアカウントの権限を示しています。

タスク	許可される権限		
	管理者	オペレータ	閲覧者
ダッシュボード	V	V	V
アプリケーション制御の設定	V	V	
メンテナンスモードの設定	V	V	
デバイスコントロールの設定	V	V	
信頼するファイルの追加	V	V	
信頼する USB デバイスの追加	V	V	
検索開始	V	V	
許可リストのアップデート	V	V	
エージェントコンポーネントのアップデート	V	V	
エージェントに Patch を配信	V	V	
接続の確認	V	V	V
イベントログの収集	V	V	
インポート/エクスポート (許可リスト/エージェントの設定)	V	V	
編成 (タグの編集/移動/削除)	V	V	
グループポリシーの設定	V	V	
グローバルポリシーの設定	V	V	
エージェントイベントログの監視	V	V	V
サーバイベントログの監視	V	V	

タスク	許可される権限		
	管理者	オペレータ	閲覧者
システムログの監視	V	V	
監査ログの監視	V	V	
アカウント管理	V		
シングルサインオン	V		
システム時間	V	V	
Syslog 転送	V	V	
ログの削除	V	V	
レポートの予約	V	V	V
通知設定	V	V	V
SMTP 設定	V	V	
プロキシ設定	V	V	
ダウンロード/アップデート	V	V	V
ファームウェア	V		
SSL 証明書	V		
ライセンス管理	V	V	

アカウントを追加する

手順

1. 管理者アカウントを使用して管理サーバ画面にログオンします。(ここに入力する情報は、大文字と小文字が区別されることに注意してください)
2. 管理サーバ画面の上部にあるナビゲーションで [管理]→[アカウント管理] の順に選択します。[アカウント管理] 画面が表示されます。
3. [ユーザの追加] ボタンをクリックすると、[ユーザアカウントの追加] 画面が表示されます。
4. [認証ソース] を指定します ([ローカル] または [SMAL ID プロバイダ])。
   a. **ローカル**ユーザを追加するには、[ID] と [名前] を指定します (ここに入力する情報は、大文字と小文字が区別されることに注意してください)。
   b. **SAML ID プロバイダ**ユーザを追加するには、[SAML アカウントのマッピング用メール] と [名前] を指定します (ここに入力する情報は、大文字と小文字が区別されることに注意してください)。

5. [ロール] にアカウントの権限として [管理者]、[オペレータ]、または [閲覧者] (初期設定) を指定します。

a. **ローカル**ユーザの場合、[ローカルパスワード] を指定し、再入力します。

6. [グループコントロール] に、対象アカウントがアクセスするグループコントロールを指定します。

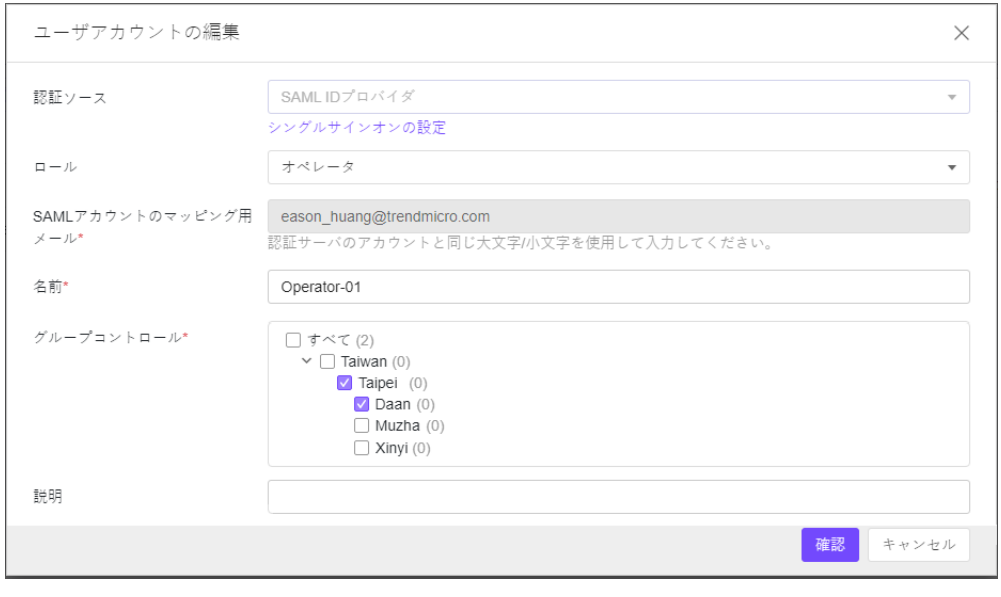
7. 必要に応じて、アカウントの [説明] を入力します。

8. [確認] ボタンをクリックすると、対象のユーザアカウントが作成されます。

アカウントを編集する

手順

1. **管理者**ロールを持つアカウントを使用して、管理サーバ画面にログオンします (ここに入力する情報は、大文字と小文字が区別されることに注意してください)。
2. 管理サーバ画面の上部にあるナビゲーションで [管理]→[アカウント管理] の順に選択します。[アカウント管理] 画面が表示されます。
3. [処理] の**編集**アイコンをクリックすると、[ユーザアカウントの編集] 画面が表示されます。
   - **ローカル**ユーザの場合、アカウントの [ロール]、[名前]、[ローカルパスワード]、[グループコントロール]、[説明] を指定できます。
   - **SAML IDプロバイダ**ユーザの場合、アカウントの [ロール]、[名前]、[グループコントロール]、[説明] を指定できます。
4. [確認] をクリックします。

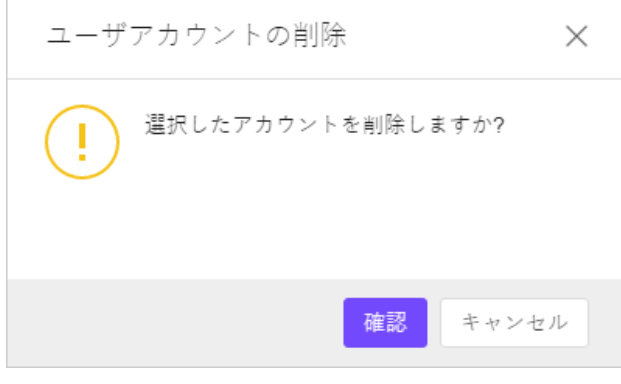


アカウントを削除する

手順

1. 管理者アカウントを使用して管理サーバ画面にログオンします。(ここに入力する情報は、大文字と小文字が区別されることに注意してください)
2. 管理サーバ画面の上部にあるナビゲーションで [管理]→[アカウント管理] の順に選択します。[アカウント管理] 画面が表示されます。
3. 削除するアカウントを選択します。**(初期設定**の **admin** だけは削除できません)

4. **削除**アイコンをクリックすると、[ユーザアカウントの削除] 画面が表示されます。



5. [確認] ボタンをクリックすると、対象のユーザアカウントがリストから削除されます。

API キーの生成

API キーを生成し、オープン API を使用してエージェントのデータをクエリできます。各ユーザアカウントに対して API キーの有効期限を設定することで、アカウント管理の効率性が向上します。

手順

1. 管理者アカウントを使用して管理サーバ画面にログオンします。(ここに入力する情報は、大文字と小文字が区別されることに注意してください)
2. 管理サーバ画面の上部にあるナビゲーションで [管理]→[アカウント管理] の順に選択します。[アカウント管理] 画面が表示されます。
3. [ユーザ] タブで、変更するユーザ ID を見つけ、画面右側の [操作] の下にある三点リーダーメニューに移動します。
4. 三点リーダーをクリックし、[API キーの生成] オプションを選択します。
5. [API キーの生成] 画面が表示されます。日付選択機能をクリックし、表示されるカレンダーで有効期限を選択します。[確認] をクリックします。
6. API キーが生成されます。クリップボードをクリックし、生成された API キーをコピーします。

重要

次の手順へ進む前に、コピーした API キーのバックアップを必ず作成してください。セキュリティ上の理由から、この API キーは再度表示されません。

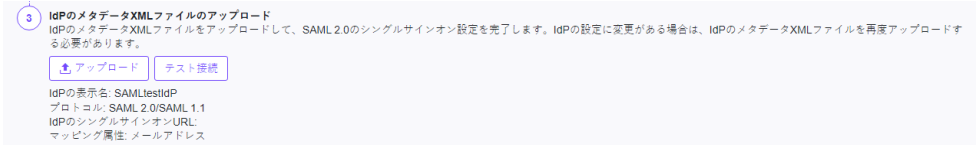
---

7. [OK] をクリックします。

シングルサインオン

手順

1. 管理者アカウントを使用して管理サーバ画面にログオンします。(ここに入力する情報は、大文字と小文字が区別されることに注意してください)
2. 管理サーバ画面の上部にあるナビゲーションで [管理]→[シングルサインオン] の順に選択します。
3. [ダウンロード] ボタンをクリックして、StellarOne のメタデータ XML ファイルをダウンロードします。
4. StellarOne の XML ファイルを IdP にアップロードしてから、IdP のメタデータ XML ファイルをダウンロードします。
5. [アップロード] ボタンをクリックして IdP のメタデータ XML ファイルを StellarOne の管理サーバ画面にアップロードし、SAML 2.0 のシングルサインオン設定を完了します。IdP の設定に変更がある場合は、IdP のメタデータ XML ファイルを再度アップロードする必要があります。



6. IdP のメタデータ XML ファイルがアップロードされると、[テスト接続] ボタンが表示されます。
7. [テスト接続] ボタンをクリックして、StellarOne への接続をテストします。

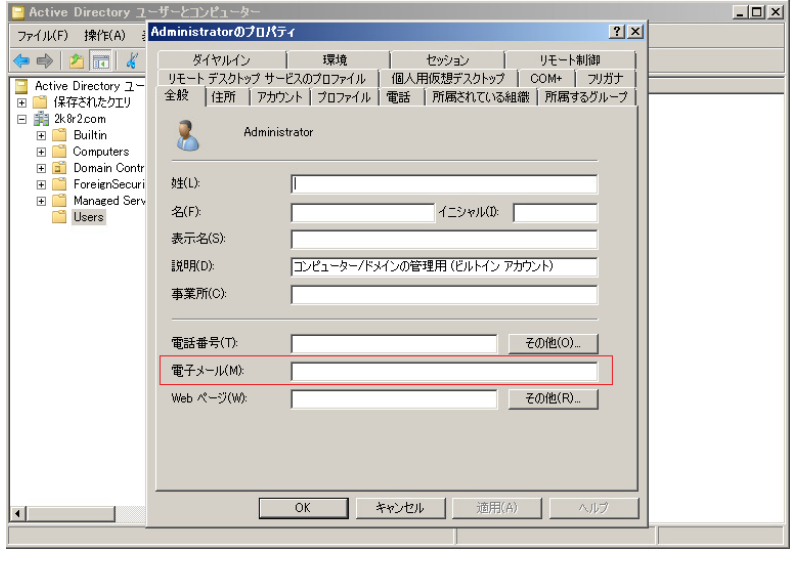
注意

SAML 設定の完了後、無効なログオンを示すエラーメッセージが表示されることがあります。シングルサインオンの問題の解決を参照して、IdP サーバでのメールアドレスの設定、および IdP サーバと StellarOne サーバのシステム時間の同期について確認してください。

シングルサインオンの問題の解決

手順

1. IdP サーバの [Active Directory ユーザーとコンピューター] で [Users] フォルダを開きます。
2. シングルサインオンに使用するユーザアカウントを右クリックし、[プロパティ]→[全般] の順に移動します。
3. [電子メール] を確認します。ここに入力されているメールアドレスが、StellarOne の管理サーバ画面にアクセスするためのアカウントのメールアドレスと一致することを確認します。

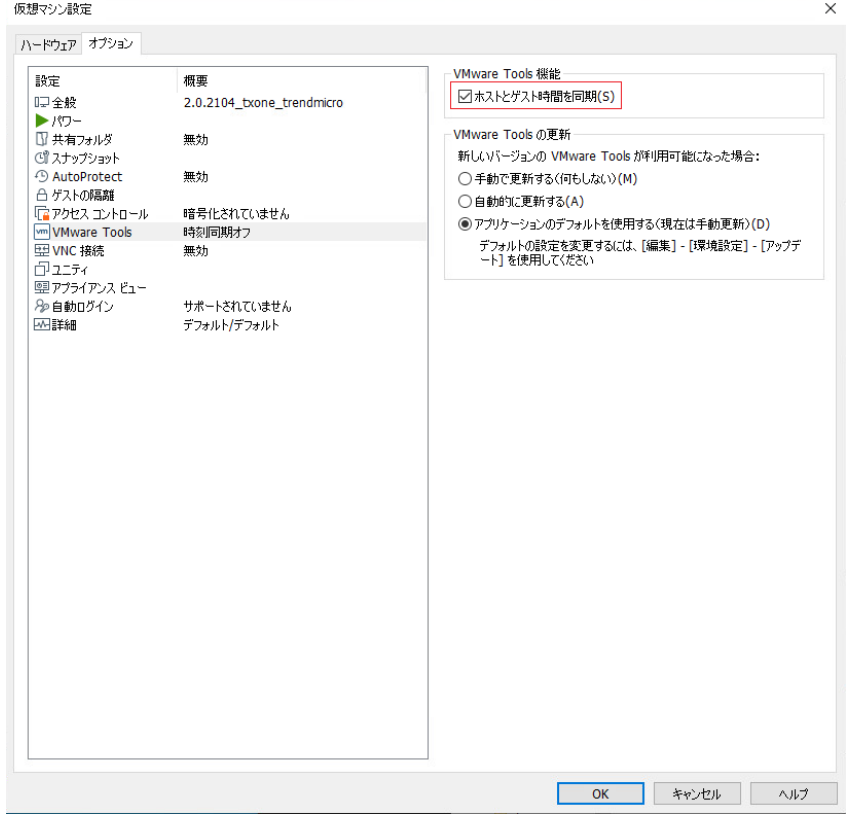


4. IdP サーバと StellarOne サーバのシステム時間が同期することを確認します。時間を同期するための推奨される設定手順は次のとおりです。

   a. IdP サーバの時間が StellarOne 仮想マシンを実行するホスト PC と同期するようにします。

   b. StellarOne の仮想マシン設定を開きます。[オプション]→[VMware Tools] の順に移動します。

   c. [ホストとゲスト時間を同期] チェックボックスをオンにして、[OK] をクリックします。



システム時間

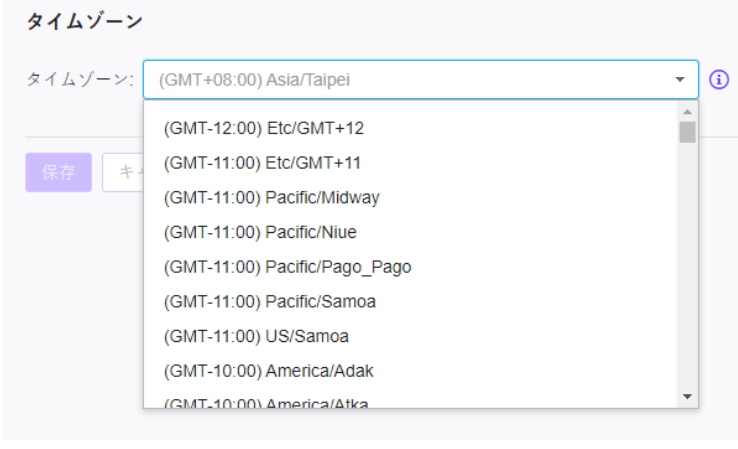
システム時間設定を変更するには、[管理]→[システム時間] の順に選択します。

日付と時刻

[期間] ドロップダウンボタンを使用し、特定のシステム時間を選択します。

タイムゾーン

ドロップダウンを使用し、特定のシステムタイムゾーンを選択します。



Syslog 転送

サーバとエージェントのイベントログを外部 syslog サーバに転送することで、他のデバイスでの管理および監視が可能になります。TXOne StellarOne の管理サーバ画面では、ログが Common Event Format (CEF) 形式で転送されます。お使いの Syslog サーバが Common Event Format (CEF) 形式をサポートしていることを確認してください。

手順

1. [管理]→[Syslog 転送] の順に選択します。
2. [ログを Syslog サーバに転送する (CEF のみ)] を有効にします。

3. Syslog サーバのプロトコル、サーバアドレス、およびポート番号を指定します。

Syslog 形式

CEF キー	説明	値
Header (logVer)	CEF 形式のバージョン	CEF: 0
Header (vendor)	デバイスのベンダ	例: TXOne Networks
Header (pname)	デバイスの製品	例: StellarOne、StellarProtect (Legacy Mode)
Header (pver)	デバイスのバージョン	例: 1.2.0171
Header (eventid)	デバイスのイベントクラス ID	例: 2509、6005
Header (eventName)	名前	例: エージェントイベント、サーバイベント、管理サーバ画面ログ
Header (severity)	重大度	例: 4
rt	ログに記録された日時	例: Apr 02 2022 13:31:51 GMT+00:00

CEF キー	説明	値
msg	イベント ID のマッピングされたメッセージ	例: ファイルのアクセスがブロックされました。ファイルが許可リストに存在しません
dvchost	コンピュータ名	例: ローカルホスト
dvc	IP アドレス	例: 192.168.154.137
cs1Label	詳細なイベントメッセージ	詳細なイベントメッセージ
cs1	イベント ID のマッピングされた詳細なメッセージ	例: ファイルのアクセスがブロックされました: C:\\Documents and Settings\\Administrator\\Local Settings\\Temp\\is-D5V0T.tmp\\is-H7K4O.tmp 不正プログラムが検出されました: 隔離。ファイルパス: C:\\eicar\\EICAR_TEST_FILE.exe
cs2Label	クライアント OS	クライアント OS
cs2	OS の説明	例: Microsoft Windows 7 Enterprise Edition Service Pack 1 build 7601, 64-bit
cs3Label	クライアントの説明	クライアントの説明
cs3	説明	-
suser	ログインユーザ	例: PC1688\\Administrator
act	処理の種類	例: ACTION_TYPE_BLOCKED
fileHash	SHA1	例: 2201589AA3ED709B3665E4FF979E10C6AD5137FC
filePath	ファイルパス	例: C:\\Documents and Settings\\Administrator\\Local Settings\\Temp\\is-D5V0T.tmp\\is-H7K4O.tmp
fileCreateTime	ファイル作成日時	例: 04 02 2022 14:00:21

CEF キー	説明	値
fileModificationTime	ファイル変更日時	例: 04 02 2022 14:00:21
logGuid	ログの GUID	例: F43500BB-1F8A-4589-A292-144A9DA343AA、{56B7345A-B6D3-4BBB-A515-4AFFAE04092F}
ServerIP	サーバの IP アドレス	例: 10.8.145.157

例:

メッセージ: CEF:0|TXOne Networks|StellarProtect (Legacy Mode)|1.2.0171|2509|エージェントイベント|4|rt=Apr 02 2022 14:09:29 GMT+00:00 msg=ファイルのアクセスがブロックされました。ファイルが許可リストに存在しません dvchost=PC1688 dvc=192.168.154.137 logGuid={CEFD0E54-7693-4B3F-9DDA-3E6F40A9384E} cs1Label=詳細なイベントメッセージ cs1=ファイルのアクセスがブロックされました: C:\\eicar\\EICAR_TEST_FILE.gz.vbs cs2Label=クライアント OS cs2=Windows XP Professional Service Pack 3 build 2600, 32-bit cs3Label=クライアントの説明 cs3= suser=PC1688\\Administrator act=ACTION_TYPE_BLOCKED fileHash=7dd27fab1f11084e984b631a614a5120c8e25598 filePath=C:\\eicar\\EICAR_TEST_FILE.gz.vbs fileCreateTime=09 13 2007 23:57:52 fileModificationTime=09 13 2007 23:57:52

ログの削除設定

古いログを削除して、StellarOne で使用しているデータベースのサイズを削減します。

今すぐ削除

手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理]→[ログの削除] の順に選択します。[ログの削除] 画面が表示されます。
2. 削除するログの種類を指定します。
   - すべてのログ

- システムログ、監査ログ、エージェントイベント、またはサーバイベント

3. **経過期間**にイベントログエントリを保持する最長期間を指定します。
   - 無期限
   - 1か月、2か月、3か月、6か月、12か月、18か月、24か月、36か月、48か月、60か月
4. **最大保持数**に保持するイベントエントリの最大件数を指定します。
   - 0件
   - 10,000件、50,000件、100,000件、500,000件、1,000,000件、5,000,000件、10,000,000件
5. [今すぐ削除] ボタンをクリックすると、イベントログが削除されます。

自動削除

1 日に 1 回の自動削除を設定するには、次の設定を使用します。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理]→[ログの削除] の順に選択します。[ログの削除] 画面が表示されます。
2. 削除するログの種類を指定します。
   - システムログ
   - 監査ログ
   - エージェントイベント
   - サーバイベント

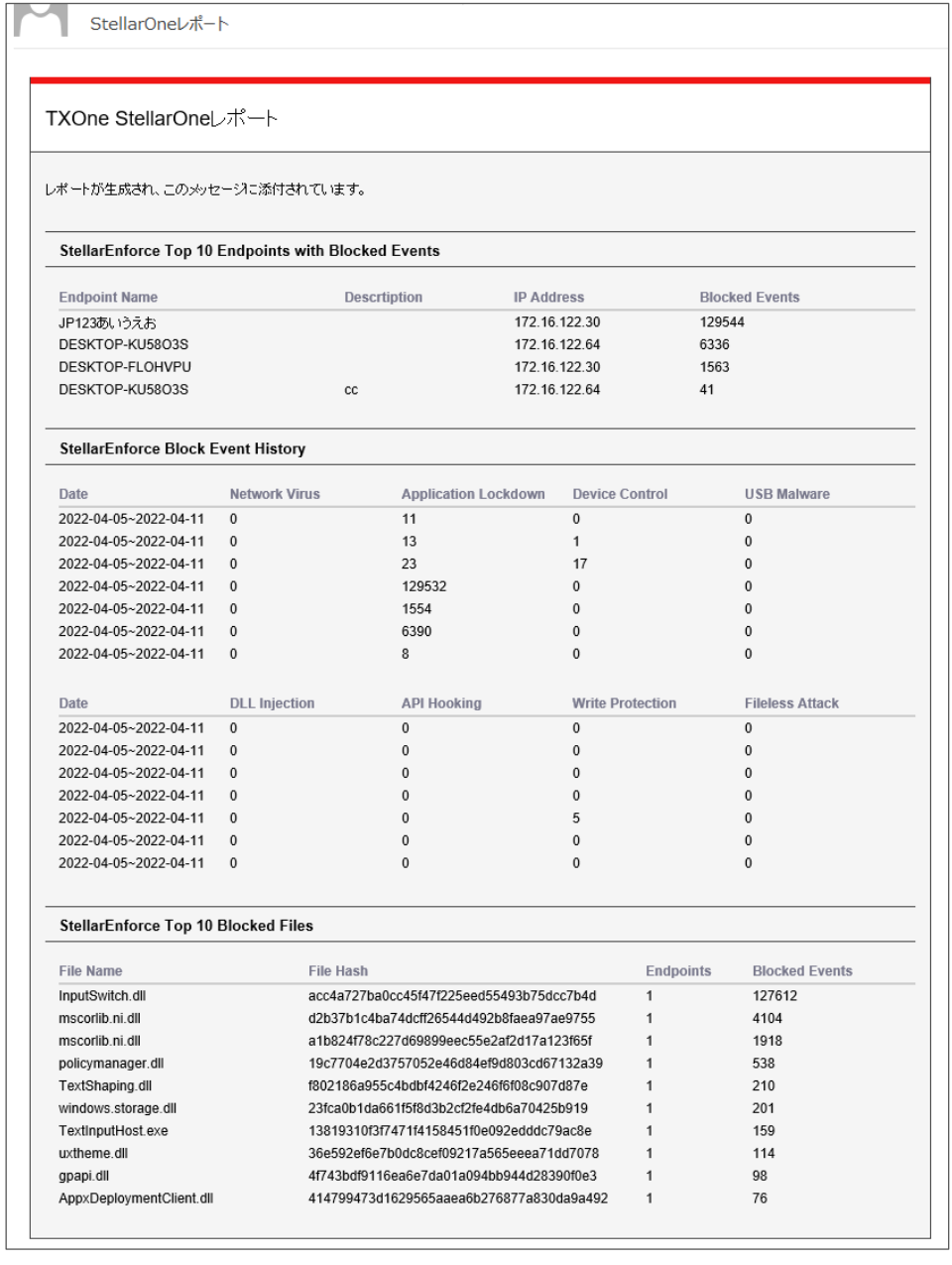
3. **経過期間**にイベントログエントリを保持する最長期間を指定します。
    - 無期限
    - 1か月、2か月、3か月、6か月、12か月、18か月、24か月、36か月、48か月、60か月
4. **最大保持数**に保持するイベントエントリの最大件数を指定します。
    - 10,000件
    - 50,000件
    - 100,000件
    - 500,000件
    - 1,000,000件
    - 5,000,000件
    - 10,000,000件
5. [保存] ボタンをクリックします。

予約レポートの設定

[管理]→[予約レポート] にある [予約レポート] 画面には、ユーザ指定のスケジュールで自動的に生成されるすべてのレポートのリストが表示されます。この画面を使用して、これまでに設定した予約レポートや受信者に関する基本情報を表示したり、予約レポートを有効および無効にしたりすることができます。

次の表は、[予約レポート] 画面で実行できるタスクを示しています。

タスク	説明
予約レポートの送信	[予約レポートの送信] チェックボックスをオンにして、予約レポートを有効にします (初期設定は無効)。
レポート内容	イベントのタイプ: • StellarProtect (Legacy Mode) でブロックされたイベントの履歴 • イベントをブロックした StellarProtect (Legacy Mode) エージェントの上位 10 件 • StellarProtect (Legacy Mode) でブロックされたファイルの上位 10 件 期間: • 過去 7 日間 • 過去 14 日間 • 過去 30 日間 • 過去 3 か月 • 過去 6 か月
予約	予約レポートの頻度と開始時刻を日、週、または月単位で設定します。  **注意** 指定した日付が存在しない月は予約タスクがスキップされます。タスクを定期的に実行するには、29 日、30 日、または 31 日を指定しないことをお勧めします。
受信者	レポートの受信者を指定するには有効なメールアドレスが必要です。



StellarOneレポート

TXOne StellarOneレポート

レポートが生成され、このメッセージに添付されています。

StellarEnforce Top 10 Endpoints with Blocked Events

Endpoint Name	Descrtiption	IP Address	Blocked Events
JP123あいうえお		172.16.122.30	129544
DESKTOP-KU58O3S		172.16.122.64	6336
DESKTOP-FLOHVPU		172.16.122.30	1563
DESKTOP-KU58O3S	cc	172.16.122.64	41

StellarEnforce Block Event History

Date	Network Virus	Application Lockdown	Device Control	USB Malware
2022-04-05~2022-04-11	0	11	0	0
2022-04-05~2022-04-11	0	13	1	0
2022-04-05~2022-04-11	0	23	17	0
2022-04-05~2022-04-11	0	129532	0	0
2022-04-05~2022-04-11	0	1554	0	0
2022-04-05~2022-04-11	0	6390	0	0
2022-04-05~2022-04-11	0	8	0	0

Date	DLL Injection	API Hooking	Write Protection	Fileless Attack
2022-04-05~2022-04-11	0	0	0	0
2022-04-05~2022-04-11	0	0	0	0
2022-04-05~2022-04-11	0	0	0	0
2022-04-05~2022-04-11	0	0	0	0
2022-04-05~2022-04-11	0	0	5	0
2022-04-05~2022-04-11	0	0	0	0
2022-04-05~2022-04-11	0	0	0	0

StellarEnforce Top 10 Blocked Files

File Name	File Hash	Endpoints	Blocked Events
InputSwitch.dll	acc4a727ba0cc45f47f225eed55493b75dcc7b4d	1	127612
mscorlib.ni.dll	d2b37b1c4ba74dcff26544d492b8faea97ae9755	1	4104
mscorlib.ni.dll	a1b824f78c227d69899eec55e2af2d17a123f65f	1	1918
policymanager.dll	19c7704e2d3757052e46d84ef9d803cd67132a39	1	538
TextShaping.dll	f802186a955c4bdbf4246f2e246f6f08c907d87e	1	210
windows.storage.dll	23fca0b1da661f5f8d3b2cf2fe4db6a70425b919	1	201
TextInputHost.exe	13819310f3f7471f4158451f0e092edddc79ac8e	1	159
uxtheme.dll	36e592ef6e7b0dc8cef09217a565eeea71dd7078	1	114
gpapi.dll	4f743bdf9116ea6e7da01a094bb944d28390f0e3	1	98
AppxDeploymentClient.dll	414799473d1629565aaea6b276877a830da9a492	1	76

通知設定

[メール通知] にメールを入力します。画面を保存する際、他の設定と一緒にメールも保存されます。

1. 最初に [管理]→[SMTP 設定] の順に選択して、SMTP サーバの設定を指定します。
2. 通知設定を変更するには、[管理]→[通知] の順に選択します。
3. [通知] には次のセクションがあります。
    - 警告レベルのエージェントイベント (初期設定は無効)
    - 大規模感染 (初期設定は無効)
    - メール通知

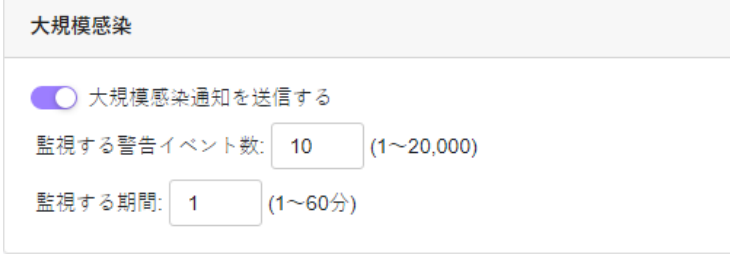
警告レベルのエージェントイベント

[警告レベルのエージェントイベント] の下にあるスイッチが**オン**の場合、「**警告**」を引き起こすイベントが発生するとメールで通知が送信されます。

大規模感染

[大規模感染] の下にあるスイッチが**オン**の場合、指定した期間内に指定した数を超える未処理の警告メッセージが発生すると、メールで通知が送信されます。

大規模感染が発生したと見なす監視するイベント数 (1～20,000) と、その数を計測する期間 (1～60分) を設定できます。



SMTP 設定

この画面には、通知や予約レポートを送信するための SMTP サーバの設定を指定できます。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理]→[SMTP 設定] の順に選択します。[SMTP 設定] 画面が表示されます。
2. [サーバアドレス]、[ポート]、および [送信者] を指定します。
3. SMTP サーバで認証が必要な場合は、[SMTP サーバの認証を設定する] を選択します。
4. StellarOne からテストメールを送信するには、[テストメールの送信] ボタンをクリックします。
5. [保存] ボタンをクリックします。

プロキシ設定

[StellarOne のインターネットプロキシ設定]、[StellarOne からエージェントへの通信プロキシ設定]、および [エージェントから StellarOne への通信プロキシ設定] の 3 つのプロキシ設定があります。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理]→[プロキシ] の順に選択します。
2. 次のプロキシ設定を指定します。
   - StellarOneのインターネットプロキシ設定
   - StellarOneからエージェントへの通信プロキシ設定
   - エージェントからStellarOneへの通信プロキシ設定
3. アップデートのためのプロキシ設定を行うには、次の手順を実行します。

   (1) プロトコルとして [HTTPS] または [HTTP] を選択します。

   注意

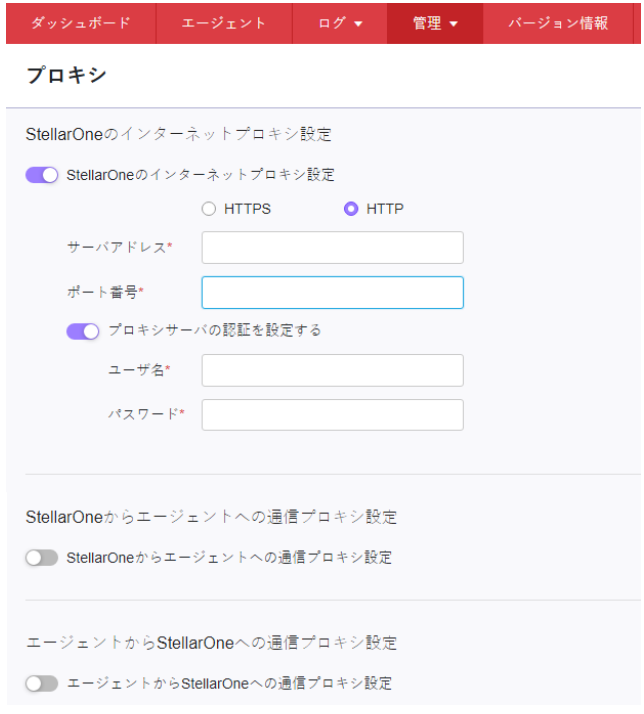
   [エージェントから StellarOne への通信プロキシ設定] について、StellarProtect (Legacy Mode) では現在 HTTPS プロキシがサポートされていないため、接続先が HTTPS サーバの場合は、接続に HTTP プロキシを使用してください。

   (2) [サーバアドレス] で、プロキシサーバの IPv4 アドレスか FQDN を指定します。

   (3) [ポート] を指定します。

   (4) プロキシサーバで認証が必要な場合は、[プロキシサーバ認証] を選択して資格情報を指定します。

   (5) [保存] をクリックします。



ヒント

StellarProtect (Legacy Mode) にリクエストを送信するために StellarOne で使用するプロキシ設定を行うには、次の手順を実行します。

StellarOne からエージェントへの通信プロキシ設定:

エージェントインストーラパッケージで使用する設定ファイルにプロキシ情報を追加します。プロキシ設定を保存します。これにより、エージェントパッケージを再パックする際に、保存した設定が含まれるようになります。

エージェントから StellarOne への通信プロキシ設定:

StellarProtect (Legacy Mode) の管理者ガイドを参照し、ローカルの StellarProtect (Legacy Mode) エージェントで **SLCmd.exe** コマンドラインインタフェースツールを使用します。

ダウンロード/アップデート設定

StellarOne および StellarProtect (Legacy Mode) のダウンロード/アップデートを管理するには、管理サーバ画面の上部にあるナビゲーションで [管理]→[ダウンロード/アップデート] の順に選択します。

ここには [StellarOne] と [StellarProtect (Legacy Mode)] の 2 つのタブがあります。

次の表は、この画面の [StellarOne] タブで実行するタスクを示しています。

機能	説明
検索コンポーネント	[アップデート] をクリックすると、最新のコンポーネントをダウンロードできます。ここにはパターンファイルとエンジンのすべてのバージョンがリストされています。
検索コンポーネントのアップデートスケジュール	コンポーネントの予約アップデートの頻度と時刻を [日次]、[週次]、または [月次] のいずれかに設定し、その曜日または日付と [開始時刻] を指定します。
検索コンポーネントのアップデート元 (StellarOne)	アップデートサーバを指定するか、トレンドマイクロのアップデートサーバから直接アップデートをダウンロードします。
検索コンポーネントのアップデート元 (エージェント)	アップデートサーバを指定することも、StellarOne から直接ダウンロードすることもできます。

次の表は、この画面の [StellarProtect (Legacy Mode)] タブで実行するタスクを示しています。

機能	説明
StellarProtect (Legacy Mode) エージェントインストーラパッケージの準備	• 最新のエージェントインストーラパッケージをダウンロードします。エージェントコンポーネントのアップデート元やプロキシ設定を変更したり、最新のコンポーネントにアップデートしたりすることもできます。 • Group.ini ファイルをダウンロードしてインストーラパッケージに追加します。これにより、StellarOne の管理サーバ画面を介して StellarProtect (Legacy Mode) エージェントを特定グループに直接登録できるようになります。詳細については、グループのマッピングを参照してください。
Patch	ここでは、[インポート] ボタンをクリックして Patch を手動でインポートするか、[削除] をクリックして StellarProtect (Legacy Mode) の Patch を削除できます。

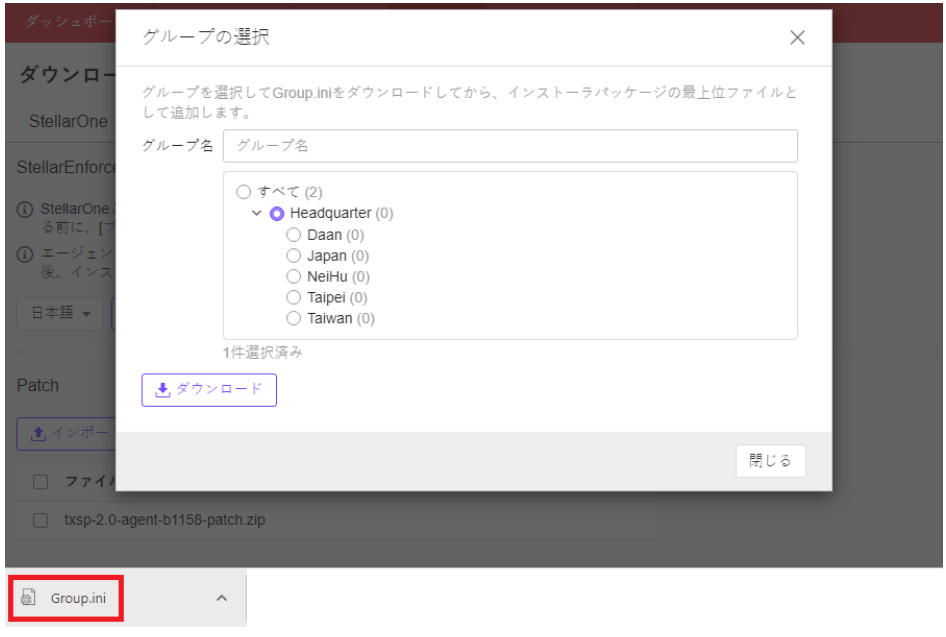
グループのマッピング

手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理]→[ダウンロード/アップデート] の順に選択します。
2. [StellarProtect (Legacy Mode)] タブを選択します。
3. インストーラパッケージをダウンロードした後、[Group.ini のダウンロード] をクリックします。

4. StellarProtect (Legacy Mode) エージェントのグループを選択し、[ダウンロード] をクリックします。Group.ini という名前のファイルがダウンロードされます。この Group.ini ファイルを、エージェントのインストーラパッケージの最上位ファイルとして配置します。

5. 対象のエージェントでインストールを実行します。インストール時、エージェントが StellarOne の管理サーバ画面に接続されていることを確認してください。

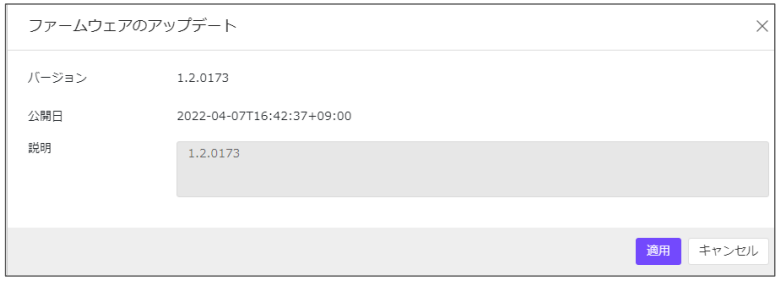


6. StellarOne の管理サーバ画面と StellarProtect (Legacy Mode) のメイン画面で、エージェントが登録されたことを確認できます。

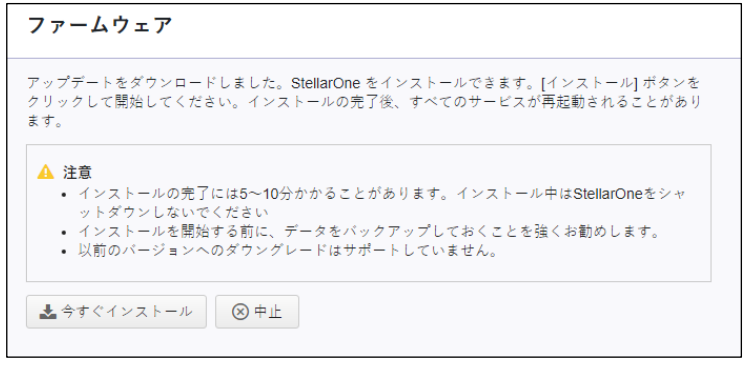
ファームウェア

手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理]→[ファームウェア] の順に選択します。
2. [インポート] をクリックして、ファームウェアの Patch ファイルを指定します (例: `acus.fw_2.0.1137.acf`)。
   - [バージョン] に、StellarOneの現在のビルドバージョンが表示されます。
   - [公開日] と [説明] には、StellarOneのPatchファイルの現在の情報が表示されます。



3. [ファームウェアのアップデート] 画面が表示されたら、[適用] をクリックして、Patch を StellarOne に適用します。
4. 通知の説明を確認します。
5. [今すぐインストール] をクリックしてアップデートを実行するか、[中止] をクリックしてアップデートを停止します。



SSL 証明書

手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理]→[SSL 証明書] の順に選択します。
2. 目的の [証明書のインポート] を選択します。
3. 証明書をインポートするには、仮想インスタンスを再起動する必要があります。
   (1) [証明書] の横にある [ファイルの選択...] ドロップダウンを使用して、インポートする証明書を選択します。
   (2) [秘密鍵] の横にある [ファイルの選択...] ドロップダウンを使用して、目的の秘密鍵を選択します。
   (3) [パスフレーズ] を指定します (任意)。

4. [インポートして再起動] をクリックします (StellarOne の管理サーバ画面が再ロードされます)。

ライセンス管理

[ライセンス管理] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで [管理]→[ライセンス] の順に選択します。この画面には、次の詳細事項が表示されます。

項目	説明
ライセンス エディション	StellarProtect (Legacy Mode) および StellarProtect の現在のライセンスエディションを表示します。
ライセンス種別	製品版: 正式に承認されたバージョン。 体験版: 使用機能が制限されたバージョン。 無期限: 永久使用可能で製品サポート終了までテクニカルサポートを提供。
シート数	StellarOne に現在登録されているエージェント数と、StellarOne に登録可能なエージェントの合計数を指定します。

項目	説明
ステータス	有効: 既存のライセンスは有効です。 有効期限終了: 既存のライセンスは古くなっています。 **注意** ウイルスの脅威からデバイスを保護するため、ただちにライセンスを更新することをお勧めします。
有効期限	StellarOne と StellarProtect (Legacy Mode) エージェントの機能が利用できる期限の日付が表示されます。(製品サポートは StellarEnforce のサポート終了期限まで提供します。)
アクティベーションコード	アクティベーションコードが表示されます
最終更新日	アクティベーションコードの前回の更新日が表示されます
詳細	リンクをクリックすると、ライセンスの詳細についてオンラインヘルプが表示されます。

アクティベーションコードを変更する

手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理]→[ライセンス] の順に選択します。[ライセンス管理] 画面が表示されます。
2. [アクティベーションコードの入力] ボタンをクリックします。
3. 新しいアクティベーションコードを入力して、StellarOne の管理サーバ画面で更新を実行します。

注意

[ライセンスの更新] ボタンをクリックして、製品ライセンスを更新します。TXOne の製品ライセンスサーバへの接続が必要になります。

第 8 章

ログの説明の参照情報

この章では、管理に関する追加情報について説明します。この章の内容は次のとおりです。

- StellarProtect (Legacy Mode) エージェントのイベントログの説明
- StellarProtect (Legacy Mode) エージェントのエラーコードの説明
- StellarOneサーバのイベントログの説明

エージェントのイベントログの説明

イベント ID	タスクカテゴリ	レベル	ログの説明
1000	システム	情報	サービスが開始されました。
1001	システム	警告	サービスが停止されました。
1002	システム	情報	アプリケーション制御が有効になりました。
1003	システム	警告	アプリケーション制御が無効になりました。
1004	システム	情報	無効化されました。
1005	システム	情報	管理者パスワードが変更されました。
1006	システム	情報	制限付きユーザのパスワードが変更されました。
1007	システム	情報	制限付きユーザのアカウントが有効になりました。
1008	システム	情報	制限付きユーザのアカウントが無効になりました。
1009	システム	情報	製品が有効になりました。
1010	システム	情報	製品が無効になりました。
1011	システム	警告	ライセンスの有効期限が終了しています。猶予期間が有効になりました。
1012	システム	警告	ライセンスの有効期限が終了しています。猶予期間が終了しました。
1013	システム	情報	製品の設定のインポートを開始しました: %path%
1014	システム	情報	製品の設定のインポートが完了しました: %path%
1015	システム	情報	製品の設定のエクスポート先: %path%
1016	システム	情報	USB 不正プログラム対策が [許可] に設定されました。
1017	システム	情報	USB 不正プログラム対策が [ブロック] に設定されました。
1018	システム	情報	USB 不正プログラム対策が有効になりました。
1019	システム	警告	USB 不正プログラム対策が無効になりました。
1020	システム	情報	ネットワークウイルス対策が [許可] に設定されました。

イベント ID	タスクカテゴリ	レベル	ログの説明
1021	システム	情報	ネットワークウイルス対策が [ブロック] に設定されました。
1022	システム	情報	ネットワークウイルス対策が有効になりました。
1023	システム	警告	ネットワークウイルス対策が無効になりました。
1025	システム	情報	メモリのランダム化が有効になりました。
1026	システム	警告	メモリのランダム化が無効になりました。
1027	システム	情報	API フッキング対策が [許可] に設定されました。
1028	システム	情報	API フッキング対策が [ブロック] に設定されました。
1029	システム	情報	API フッキング対策が有効になりました。
1030	システム	警告	API フッキング対策が無効になりました。
1031	システム	情報	DLL インジェクション対策が [許可] に設定されました。
1032	システム	情報	DLL インジェクション対策が [ブロック] に設定されました。
1033	システム	情報	DLL インジェクション対策が有効になりました。
1034	システム	警告	DLL インジェクション対策が無効になりました。
1035	システム	情報	事前指定による許可リスト自動更新が有効になりました。
1036	システム	情報	事前指定による許可リスト自動更新が無効になりました。
1037	システム	情報	DLL/ドライバ制御が有効になりました。
1038	システム	警告	DLL/ドライバ制御が無効になりました。
1039	システム	情報	スクリプト制御が有効になりました。
1040	システム	警告	スクリプト制御が無効になりました。
1041	システム	情報	スクリプトが追加されました。 [詳細] ファイル拡張子: %extension% インタープリタ: %interpreter%

イベント ID	タスクカテゴリ	レベル	ログの説明
1042	システム	情報	スクリプトが削除されました。 [詳細] ファイル拡張子: %extension% インタープリタ: %interpreter%
1044	システム	情報	除外パスが有効になりました。
1045	システム	情報	除外パスが無効になりました。
1047	システム	情報	信頼するデジタル証明書が有効になりました。
1048	システム	情報	信頼するデジタル証明書が無効になりました。
1049	システム	情報	書き込み制御が有効になりました。
1050	システム	警告	書き込み制御が無効になりました。
1051	システム	情報	書き込み制御が [許可] に設定されました。
1052	システム	情報	書き込み制御が [ブロック] に設定されました。
1055	システム	情報	書き込み制御リストに追加されたファイル。 パス: %path%
1056	システム	情報	書き込み制御リストから削除されたファイル。 パス: %path%
1057	システム	情報	書き込み制御の除外リストに追加されたファイル。 パス: %path% プロセス: %process%
1058	システム	情報	書き込み制御の除外リストから削除されたファイル。 パス: %path% プロセス: %process%
1059	システム	情報	書き込み制御リストに追加されたフォルダ。 パス: %path% 範囲: %scope%
1060	システム	情報	書き込み制御リストから削除されたフォルダ。 パス: %path% 範囲: %scope%

イベント ID	タスクカテゴリ	レベル	ログの説明
1061	システム	情報	書き込み制御の除外リストに追加されたフォルダ。 パス: %path% 範囲: %scope% プロセス: %process%
1062	システム	情報	書き込み制御の除外リストから削除されたフォルダ。 パス: %path% 範囲: %scope% プロセス: %process%
1063	システム	情報	書き込み制御リストに追加されたレジストリ値。 レジストリキー: %regkey% レジストリ値の名前: %regvalue%
1064	システム	情報	書き込み制御リストから削除されたレジストリ値。 レジストリキー: %regkey% レジストリ値の名前: %regvalue%
1065	システム	情報	書き込み制御の除外リストに追加されたレジストリ値。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% プロセス: %process%
1066	システム	情報	書き込み制御の除外リストから削除されたレジストリ値。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% プロセス: %process%
1067	システム	情報	書き込み制御リストに追加されたレジストリキー。 パス: %regkey% 範囲: %scope%
1068	システム	情報	書き込み制御リストから削除されたレジストリキー。 パス: %regkey% 範囲: %scope%
1069	システム	情報	書き込み制御の除外リストに追加されたレジストリキー。 パス: %regkey% 範囲: %scope% プロセス: %process%

イベント ID	タスクカテゴリ	レベル	ログの説明
1070	システム	情報	書き込み制御の除外リストから削除されたレジストリキー。 パス: %regkey% 範囲: %scope% プロセス: %process%
1071	システム	情報	カスタム処理が [無視] に設定されました。
1072	システム	情報	カスタム処理が [隔離] に設定されました。
1073	システム	情報	カスタム処理が [Intelligent Manager で確認する] に設定されました
1074	システム	情報	隔離ファイルが復元されました。 [詳細] 元の場所: %path% ソース: %source%
1075	システム	情報	隔離ファイルは削除されました。 [詳細] 元の場所: %path% ソース: %source%
1076	システム	情報	変更監視が有効になりました。
1077	システム	情報	変更監視が無効になりました。
1078	システム	情報	Root Cause Analysis レポートに失敗しました。 [詳細] パス: %path%
1079	システム	情報	管理サーバの証明書のインポート先: %path%
1080	システム	情報	管理サーバの証明書のエクスポート先: %path%
1081	システム	情報	集中管理モードの設定のインポート先: %path%
1082	システム	情報	集中管理モードの設定のエクスポート先: %path%
1083	システム	情報	集中管理モードが有効になりました。
1084	システム	情報	集中管理モードが無効になりました。
1085	システム	情報	書き込み制御が有効の場合、書き込み制御リストと許可リストが対象に含まれます。

イベント ID	タスクカテゴリ	レベル	ログの説明
1086	システム	警告	書き込み制御が有効の場合、書き込み制御リストのみが対象になります。
1088	システム	情報	Windows Update サポートが有効になりました。
1089	システム	情報	Windows Update サポートが無効になりました。
1094	システム	情報	TXOne StellarProtect (Legacy Mode) がアップデートされました。 適用されたファイル: %file_name%
1096	システム	情報	信頼するハッシュリストが有効になりました。
1097	システム	情報	信頼するハッシュリストが無効になりました。
1099	システム	情報	ストレージデバイスのアクセスが [許可] に設定されました
1100	システム	情報	ストレージデバイスのアクセスが [ブロック] に設定されました
1101	システム	情報	ストレージデバイスのブロックが有効になりました
1102	システム	警告	ストレージデバイスのブロックが無効になりました
1103	システム	情報	イベントログの設定が変更されました。 [詳細] Windows イベントログ: %ON|off% レベル: 警告ログ: %ON|off% 情報ログ: %ON|off% システムログ: %ON|off% 除外パスログ: %ON|off% 書き込み制御ログ: %ON|off% リストログ: %ON|off% 許可されたアクセスのログ: Dll ドライバログ: %ON|off% アップデートプログラムのログ: %ON|off% 除外パスログ: %ON|off% 信頼するデジタル証明書のログ: %ON|off% 信頼するハッシュのログ: %ON|off% 書き込み制御ログ: %ON|off% ブロックされたアクセスのログ: %ON|off% USB 不正プログラム対策ログ: %ON|off% 実行防止対策のログ: %ON|off% ネットワークウイルス対策のログ: %ON|off%

イベント ID	タスクカテゴリ	レベル	ログの説明
			変更監視ログ ファイル作成ログ: %ON|off% ファイル変更ログ: %ON|off% ファイル削除ログ: %ON|off% ファイル名変更ログ: %ON|off% RegValue 変更ログ: %ON|off% RegValue 削除ログ: %ON|off% RegKey 作成ログ: %ON|off% RegKey 削除ログ: %ON|off% RegKey 名前変更ログ: %ON|off% デバイスコントロールのログ: %ON|off% デバッグログ: %ON|off%
1104	システム	警告	このバージョンの Windows ではメモリのランダム化は使用できません。
1105	システム	情報	ファイルのブロック通知が有効になりました。
1106	システム	情報	ファイルのブロック通知が無効になりました。
1107	システム	情報	管理者パスワードがリモートで変更されました。
1111	システム	情報	ファイルレス攻撃対策が有効になりました。
1112	システム	警告	ファイルレス攻撃対策が無効になりました。
1500	リスト	情報	許可リスト自動更新が開始されました。
1501	リスト	情報	許可リスト自動更新が停止されました。
1502	リスト	情報	許可リストのインポートを開始しました: %path%
1503	リスト	情報	許可リストのインポートが完了しました: %path%
1504	リスト	情報	許可リストのエクスポート先: %path%
1505	リスト	情報	許可リストに追加されました: %path%
1506	リスト	情報	許可済みインストーラまたはアップデートプログラムのリストに追加されました: %path%
1507	リスト	情報	許可リストから削除されました: %path%
1508	リスト	情報	許可済みインストーラまたはアップデートプログラムのリストから削除されました: %path%
1509	リスト	情報	許可リストがアップデートされました: %path%

イベント ID	タスクカテゴリ	レベル	ログの説明
1510	リスト	情報	許可済みインストーラまたはアップデートプログラムのリストがアップデートされました: %path%
1511	リスト	警告	許可リストに対して追加またはアップデートを実行できませんでした: %path%
1512	リスト	警告	許可済みインストーラまたはアップデートプログラムのリストに対して追加またはアップデートを実行できません: %path%
1513	システム	情報	除外パスリストに追加されました。 [詳細] 種類: %exceptionpathtype% パス: %exceptionpath%
1514	システム	情報	除外パスリストから削除されました。 [詳細] 種類: %exceptionpathtype% パス: %exceptionpath%
1515	システム	情報	信頼するデジタル証明書リストに追加されました。 [詳細] ラベル: %label% ハッシュ: %hashvalue% 種類: %type% 件名: %subject% 発行者: %issuer%
1516	システム	情報	信頼するデジタル証明書リストから削除されました。 [詳細] ラベル: %label% ハッシュ: %hashvalue% 種類: %type% 件名: %subject% 発行者: %issuer%

イベント ID	タスクカテゴリ	レベル	ログの説明
1517	システム	情報	信頼するハッシュリストに追加されました。%n [詳細] ラベル: %label% ハッシュ: %hashvalue% 種類: %type% 許可リストに追加: %yes|no% パス: %path% メモ: %note%
1518	システム	情報	信頼するハッシュリストから削除されました。%n [詳細] ラベル: %label% ハッシュ: %hashvalue% 種類: %type% 許可リストに追加: %yes|no% パス: %path% メモ: %note%
1519	リスト	情報	許可リストからリモートで削除されました: %path%
1520	リスト	警告	%1 でファイルの列挙中に予期しないエラーが発生したため、許可リストを作成できません。%n エラーコード: %2 %n
1521	システム	情報	ファイルレス攻撃対策の除外を追加しました。 [詳細] ラベル: %label% 対象プロセス: %process_name% 引数: %arguments% %regex_flag% 親プロセス 1 のパス: %path% 親プロセス 2 のパス: %path% 親プロセス 3 のパス: %path% 親プロセス 4 のパス: %path%
1522	システム	情報	ファイルレス攻撃対策の除外を削除しました。 [詳細] ラベル: %label% 対象プロセス: %process_name% 引数: %arguments% %regex_flag% 親プロセス 1 のパス: %path% 親プロセス 2 のパス: %path% 親プロセス 3 のパス: %path% 親プロセス 4 のパス: %path%

イベント ID	タスクカテゴリ	レベル	ログの説明
1523	システム	情報	メンテナンスモードを開始しました
1524	システム	情報	メンテナンスモードを終了しています
1525	システム	情報	メンテナンスモードを終了しました
1526	リスト	情報	メンテナンスモードで許可リストに追加されました。 パス: %1 ハッシュ: %2
1527	リスト	情報	メンテナンスモードで許可リストがアップデートされました。 パス: %1 ハッシュ: %2
2000	許可されたアクセス	情報	ファイルのアクセスが許可されました: %path% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode% リスト: %list%
2001	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode% ファイルハッシュが許可されました: %hash%
2002	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% 許可リストの確認中にファイルパスを取得できません。 [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2003	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% 許可リストの確認中にハッシュを計算できません。 [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%

イベント ID	タスクカテゴリ	レベル	ログの説明
2004	許可された アクセス	警告	ファイルのアクセスが許可されました: %path% プロセスを監視するための通知を取得できません。
2005	許可された アクセス	警告	ファイルのアクセスが許可されました: %path% プロセスを例外リスト以外に追加できません。
2006	許可された アクセス	情報	ファイルのアクセスが許可されました: %path% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2007	許可された アクセス	警告	ファイルのアクセスが許可されました: %path% 除外パスリストの確認中にエラーが発生しました。 [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2008	許可された アクセス	警告	ファイルのアクセスが許可されました: %path% 信頼するデジタル証明書リストの確認中にエラーが発生しました。 [詳細] パス: %path% アクセスユーザ: %username% モード: s%mode%
2011	許可された アクセス	情報	レジストリのアクセスが許可されました。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2012	許可された アクセス	情報	レジストリのアクセスが許可されました。 レジストリキー: %regkey% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%

イベント ID	タスクカテゴリ	レベル	ログの説明
2013	許可された アクセス	情報	除外リストによってファイル/フォルダの変更が許可されました: %path% [詳細] パス: アクセスユーザ: %username% モード: %mode%
2015	許可された アクセス	情報	除外リストによってレジストリ値の変更が許可されました。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2016	許可された アクセス	情報	除外リストによってレジストリキーの変更が許可されました。 レジストリキー: %regkey% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2017	許可された アクセス	警告	ファイル/フォルダの変更が許可されました: %path% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2019	許可された アクセス	警告	レジストリ値の変更が許可されました。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%

イベント ID	タスクカテゴリ	レベル	ログの説明
2020	許可された アクセス	警告	レジストリキーの変更が許可されました。 レジストリキー: %regkey% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2021	許可された アクセス	警告	ファイルのアクセスが許可されました: %path% 信頼するハッシュリストの確認中にエラーが発生しました。 [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2022	許可された アクセス	警告	ファイルレス攻撃対策によりプロセスが許可されました: %path% %argument% [詳細] アクセスユーザ: %username% 親プロセス 1 のパス: %path% 親プロセス 2 のパス: %path% 親プロセス 3 のパス: %path% 親プロセス 4 のパス: %path% モード: アプリケーション制御が無効の状態 理由: %reason%
2503	ブロックされた アクセス	警告	ファイル/フォルダの変更がブロックされました: %path% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2505	ブロックされた アクセス	警告	レジストリ値の変更がブロックされました。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%

イベント ID	タスクカテゴリ	レベル	ログの説明
2506	ブロックされたアクセス	警告	レジストリキーの変更がブロックされました。 レジストリキー: %regkey% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2507	ブロックされたアクセス	情報	指定した処理が実行されました: %path% [詳細] 操作: %action% ソース: %source%
2508	ブロックされたアクセス	警告	指定された処理の実行に失敗しました: %path% [詳細] 操作: %action% ソース: %source%
2509	ブロックされたアクセス	警告	ファイルのアクセスがブロックされました: %path% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode% 理由: 許可リスト内に存在しません。 ファイルハッシュがブロックされました: %hash%
2510	ブロックされたアクセス	警告	ファイルのアクセスがブロックされました: %path% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode% 理由: 計算されたハッシュ値が、保存されている値と一致しません。 ファイルハッシュがブロックされました: %hash%
2511	ブロックされたアクセス	情報	ファイル/フォルダの変更がブロックされました: %path% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%

イベント ID	タスクカテゴリ	レベル	ログの説明
2512	ブロックされたアクセス	警告	レジストリ値の変更がブロックされました。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% [詳細] パス: %path% アクセスユーザ: %username% 注意 イベント ID 2512 は、サービス作成対策機能を有効にすることに起因します。
2513	ブロックされたアクセス	警告	ファイルレス攻撃対策によりプロセスがブロックされました: %path% %argument% [詳細] アクセスユーザ: %username% 親プロセス 1 のパス: %path% 親プロセス 2 のパス: %path% 親プロセス 3 のパス: %path% 親プロセス 4 のパス: %path% モード: アプリケーション制御が有効の状態 理由: %reason%
2514	ブロックされたアクセス	警告	ファイルのアクセスがブロックされました: %BLOCKED_FILE_PATH% [詳細] パス: %PARENT_PROCESS_PATH% アクセスユーザ: %USER_NAME% 理由: ブロックされたファイルは、大文字と小文字を区別する属性が有効になっているフォルダ内にあります。
3000	USB 不正プログラム対策	警告	デバイスのアクセスが許可されました: %path% [詳細] パス: %path% アクセスユーザ: %username% デバイスタイプ: %type%
3001	USB 不正プログラム対策	警告	デバイスのアクセスがブロックされました: %path% [詳細] パス: %path% アクセスユーザ: %username% デバイスタイプ: %type%

イベント ID	タスクカテゴリ	レベル	ログの説明
3500	ネットワークウイルス対策	警告	ネットワークウイルスが許可されました: %name% [詳細] プロトコル: TCP 送信元 IP アドレス: %ip_address% 送信元ポート: %port% 送信先 IP アドレス: %ip_address% 送信先ポート: 80
3501	ネットワークウイルス対策	警告	ネットワークウイルスがブロックされました: %name% [詳細] プロトコル: TCP 送信元 IP アドレス: %ip_address% 送信元ポート: %port% 送信先 IP アドレス: %ip_address% 送信先ポート: 80
4000	プロセス保護イベント	警告	API フッキング/DLL インジェクションが許可されました: %path% [詳細] パス: %path% ユーザ: %username%
4001	プロセス保護イベント	警告	API フッキング/DLL インジェクションがブロックされました: %path% [詳細] パス: %path% ユーザ: %username%
4002	プロセス保護イベント	警告	API フッキング対策が許可されました: %path% [詳細] パス: %path% ユーザ: %username%
4003	プロセス保護イベント	警告	API フッキング対策がブロックされました: %path% [詳細] パス: %path% ユーザ: %username%
4004	プロセス保護イベント	警告	DLL インジェクションが許可されました: %path% [詳細] パス: %path% ユーザ: %username%

イベント ID	タスクカテゴリ	レベル	ログの説明
4005	プロセス保護イベント	警告	DLL インジェクションがブロックされました: %path% [詳細] パス: %path% ユーザ: %username%
4500	システム内の変更	情報	作成されたファイル/フォルダ: %path% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
4501	システム内の変更	情報	変更されたファイル: %path% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
4502	システム内の変更	情報	削除されたファイル/フォルダ: %path% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
4503	システム内の変更	情報	名前が変更されたファイル/フォルダ: %path% 新しいパス: %path% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
4504	システム内の変更	情報	変更されたレジストリ値: レジストリキー: %regkey% レジストリ値の名前: %regvalue% レジストリ値の種類: %regvaluetype% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%

イベント ID	タスクカテゴリ	レベル	ログの説明
4505	システム内の変更	情報	削除されたレジストリ値: レジストリキー: %regkey% レジストリ値の名前: %regvalue% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
4506	システム内の変更	情報	作成されたレジストリキー: レジストリキー: %regkey% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
4507	システム内の変更	情報	削除されたレジストリキー: レジストリキー: %regkey% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
4508	システム内の変更	情報	名前が変更されたレジストリキー: レジストリキー: %regkey% 新しいレジストリキー: %regkey% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
5000	デバイスコントロール	警告	ストレージデバイスのアクセスが許可されました: %PATH% [詳細] パス: %PATH% アクセスユーザ: %USERNAME% デバイスタイプ: %TYPE% %DEVICEINFO%
5001	デバイスコントロール	警告	ストレージデバイスのアクセスがブロックされました: %PATH% [詳細] パス: %PATH% アクセスユーザ: %USERNAME% デバイスタイプ: %TYPE% %DEVICEINFO%

イベント ID	タスクカテゴリ	レベル	ログの説明
6000	システム	情報	%Result% [詳細] アップデート元: %SERVER% [元のバージョン] ウイルスパターンファイル: %VERSION% スパイウェアパターンファイル: %VERSION% デジタル署名パターンファイル: %VERSION% プログラム検査パターンファイル: %VERSION% ダメージクリーンナップテンプレート: %VERSION% ダメージクリーンナップエンジン設定: %VERSION% ウイルス検索エンジン: %VERSION% ダメージクリーンナップエンジン: %VERSION% 検索サービス: %VERSION% [最新バージョン] ウイルスパターンファイル: %VERSION% スパイウェアパターンファイル: %VERSION% デジタル署名パターンファイル: %VERSION% プログラム検査パターンファイル: %VERSION% ダメージクリーンナップ テンプレート: %VERSION% ダメージクリーンナップエンジン設定: %VERSION% ウイルス検索エンジン: %VERSION% ダメージクリーンナップエンジン: %VERSION% 検索サービス: %VERSION%
6001	システム	警告	アップデートに失敗しました: %ERROR_MSG% (%ERROR_CODE%) [詳細] アップデート元: %SERVER% [元のバージョン] ウイルスパターンファイル: %VERSION% スパイウェアパターンファイル: %VERSION% デジタル署名パターンファイル: %VERSION% プログラム検査パターンファイル: %VERSION% ダメージクリーンナップテンプレート: %VERSION% ダメージクリーンナップエンジン設定: %VERSION% ウイルス検索エンジン: %VERSION% ダメージクリーンナップエンジン: %VERSION% 検索サービス: %VERSION% [最新バージョン] ウイルスパターンファイル: %VERSION%

イベント ID	タスクカテゴリ	レベル	ログの説明
			スパイウェアパターンファイル: %VERSION% デジタル署名パターンファイル: %VERSION% プログラム検査パターンファイル: %VERSION% ダメージクリーンナップテンプレート: %VERSION% ダメージクリーンナップエンジン設定: %VERSION% ウイルス検索エンジン: %VERSION% ダメージクリーンナップエンジン: %VERSION% 検索サービス: %VERSION%
6002	システム	情報	不正プログラム検索を開始しました: %SCAN_TYPE% [詳細] 検索するファイル: %SCAN_FOLDER_TYPE% 検索されたフォルダ: %PATHS% 除外されたパス: %PATHS% 除外されたファイル: %PATHS% 除外された拡張子: %PATHS% [コンポーネント] ウイルスパターンファイル: %VERSION% スパイウェアパターンファイル: %VERSION% デジタル署名パターンファイル: %VERSION% プログラム検査パターンファイル: %VERSION% ダメージクリーンナップテンプレート: %VERSION% ダメージクリーンナップエンジン設定: %VERSION% ウイルス検索エンジン: %VERSION% ダメージクリーンナップエンジン: %VERSION% 検索サービス: %VERSION%
6003	システム	情報	不正プログラム検索が完了しました: %SCAN_TYPE% 感染ファイル数: %NUM% [詳細] 検索するファイル: %SCAN_FOLDER_TYPE% 検索されたフォルダ: %PATHS% 除外されたパス: %PATHS% 除外されたファイル: %PATHS% 除外された拡張子: %PATHS% 開始日時: %DATE_TIME% 終了日時: %DATE_TIME% 検索ファイル数: %NUM% 感染ファイル数: %NUM% 駆除されたファイル数: %NUM% 再起動後に駆除されたファイル数: %NUM%

イベント ID	タスクカテゴリ	レベル	ログの説明
			[コンポーネント] ウイルスパターンファイル: %VERSION% スパイウェアパターンファイル: %VERSION% デジタル署名パターンファイル: %VERSION% プログラム検査パターンファイル: %VERSION% ダメージクリーンナップテンプレート: %VERSION% ダメージクリーンナップエンジン設定: %VERSION% ウイルス検索エンジン: %VERSION% ダメージクリーンナップエンジン: %VERSION% 検索サービス: %VERSION%
6004	システム	警告	不正プログラム検索は完了していません: %SCAN_TYPE% %ERROR% [詳細] 検索するファイル: %SCAN_FOLDER_TYPE% 検索されたフォルダ: %PATHS% 除外されたパス: %PATHS% 除外されたファイル: %PATHS% 除外された拡張子: %PATHS% 開始日時: %DATE_TIME% 終了日時: %DATE_TIME% 検索ファイル数: %NUM% 感染ファイル数: %NUM% 駆除されたファイル数: %NUM% 再起動後に駆除されたファイル数: %NUM% [コンポーネント] ウイルスパターンファイル: %VERSION% スパイウェアパターンファイル: %VERSION% デジタル署名パターンファイル: %VERSION% プログラム検査パターンファイル: %VERSION% ダメージクリーンナップテンプレート: %VERSION% ダメージクリーンナップエンジン設定: %VERSION% ウイルス検索エンジン: %VERSION% ダメージクリーンナップエンジン: %VERSION% 検索サービス: %VERSION%

イベント ID	タスクカテゴリ	レベル	ログの説明
6005	システム	情報	不正プログラムが検出されました: %ACTION% ファイルパス: %PATH% [詳細] 再起動が必要: %NEED_REBOOT% [検索結果] 脅威の種類: %TYPE% 脅威の名前: %NAME% [コンポーネント] ウイルスパターンファイル: %VERSION% スパイウェアパターンファイル: %VERSION% デジタル署名パターンファイル: %VERSION% プログラム検査パターンファイル: %VERSION% ダメージクリーンナップテンプレート: %VERSION% ダメージクリーンナップエンジン設定: %VERSION% ウイルス検索エンジン: %VERSION% ダメージクリーンナップエンジン: %VERSION% 検索サービス: %VERSION%
6006	システム	警告	不正プログラムが検出されました。検出時の処理を実行できません: %PATH% [詳細] 1 次処理: %1ST_ACTION% 2 次処理: %2ND_ACTION% 脅威の種類: %TYPE% 脅威の名前: %NAME% [コンポーネント] ウイルスパターンファイル: %VERSION% スパイウェアパターンファイル: %VERSION% デジタル署名パターンファイル: %VERSION% プログラム検査パターンファイル: %VERSION% ダメージクリーンナップテンプレート: %VERSION% ダメージクリーンナップエンジン設定: %VERSION% ウイルス検索エンジン: %VERSION% ダメージクリーンナップエンジン: %VERSION% 検索サービス: s%VERSION%

イベント ID	タスクカテゴリ	レベル	ログの説明
6007	メンテナンスモード	警告	メンテナンスモードで不正プログラムが検出されました (ファイルの隔離に成功): %PATH% [詳細] コンポーネントのバージョン: ウイルスパターンファイル: %VERSION% スパイウェアパターンファイル: %VERSION% デジタル署名パターンファイル: %VERSION% プログラム検査パターンファイル: %VERSION% ダメージクリーンナップテンプレート: %VERSION% ダメージクリーンナップエンジン設定: %VERSION% ウイルス検索エンジン: %VERSION% ダメージクリーンナップエンジン: %VERSION% 検索サービス: %VERSION%
6008	メンテナンスモード	警告	メンテナンスモードで不正プログラムが検出されました (ファイルの隔離に失敗): %PATH% [詳細] コンポーネントのバージョン: ウイルスパターンファイル: %VERSION% スパイウェアパターンファイル: %VERSION% デジタル署名パターンファイル: %VERSION% プログラム検査パターンファイル: %VERSION% ダメージクリーンナップテンプレート: %VERSION% ダメージクリーンナップエンジン設定: %VERSION% ウイルス検索エンジン: %VERSION% ダメージクリーンナップエンジン: %VERSION% 検索サービス: %VERSION%
6009	メンテナンスモード	警告	メンテナンスモードで不正プログラムが検出されました: %PATH% [詳細] コンポーネントのバージョン: ウイルスパターンファイル: %VERSION% スパイウェアパターンファイル: %VERSION% デジタル署名パターンファイル: %VERSION% プログラム検査パターンファイル: %VERSION% ダメージクリーンナップテンプレート: %VERSION% ダメージクリーンナップエンジン設定: %VERSION% ウイルス検索エンジン: %VERSION% ダメージクリーンナップエンジン: %VERSION% 検索サービス: %VERSION%

イベント ID	タスクカテゴリ	レベル	ログの説明
7000	システム	情報	グループポリシーが適用されました [詳細] 古いグループ名: %GROUP NAME% 古いポリシーバージョン: %VERSION% 新しいグループ名: %GROUP NAME% 新しいポリシーバージョン: %VERSION%
7001	システム	警告	グループポリシーを同期できません [詳細] 古いグループ名: %GROUP NAME% 古いポリシーバージョン: %VERSION% 新しいグループ名: %GROUP NAME% 新しいポリシーバージョン: %VERSION% 理由: %Reason%

エージェントのエラーコードの説明

このリストでは、TXOne StellarProtect (Legacy Mode) エージェントで使用されるさまざまなエラーコードについて説明します。

エラーコードの説明 (StellarProtect (Legacy Mode))

コード	説明
0x00040200	操作に成功しました。
0x80040201	操作に失敗しました。
0x80040202	操作に失敗しました。
0x00040202	一部のみ操作に成功しました。
0x00040203	要求された機能はインストールされていません。
0x80040203	要求された機能はサポートされていません。
0x80040204	無効な引数です。
0x80040205	無効なステータスです。
0x80040206	メモリが不足しています。
0x80040207	ビジー状態です。要求は無視されました。
0x00040208	やりなおしてください。(通常はタスクの実行時間が長すぎる場合に出力されます)
0x80040208	システムにより予約済み。(未使用)
0x80040209	ファイルパスが長すぎます。
0x0004020a	システムにより予約済み。(未使用)
0x8004020b	システムにより予約済み。(未使用)
0x0004020c	システムにより予約済み。(未使用)
0x0004020d	システムにより予約済み。(未使用)
0x8004020d	システムにより予約済み。(未使用)
0x0004020e	再起動が必要です。

コード	説明
0x8004020e	予期しないエラーのため再起動が必要です。
0x0004020f	タスクの実行が許可されました。
0x8004020f	許可が拒否されました。
0x00040210	システムにより予約済み。(未使用)
0x80040210	無効または予期しないサービスモードです。
0x00040211	システムにより予約済み。(未使用)
0x80040211	要求されたタスクは現在のステータスでは許可されていません。ライセンスを確認してください。
0x00040212	システムにより予約済み。(未使用)
0x00040213	システムにより予約済み。(未使用)
0x80040213	パスワードが一致しません。
0x00040214	システムにより予約済み。(未使用)
0x80040214	システムにより予約済み。(未使用)
0x00040215	見つかりません。
0x80040215	「必要ですが見つかりません。」
0x80040216	認証がロックされています。
0x80040217	パスワードの長さが無効です。
0x80040218	パスワードに無効な文字が含まれています。
0x00040219	パスワードが重複しています。管理者と制限付きユーザのパスワードは同一にできません。
0x80040220	システムにより予約済み。(未使用)
0x80040221	システムにより予約済み。(未使用)
0x80040222	システムにより予約済み。(未使用)
0x80040223	ファイルが見つかりません (予想どおりでエラーではありません)。
0x80040224	システムにより予約済み。(未使用)
0x80040225	システムにより予約済み。(未使用)

コード	説明
0x80040240	ライブラリが見つかりません。
0x80040241	ライブラリ関数で無効なライブラリステータスまたは予期しないエラーが発生しました。
0x80040260	システムにより予約済み。(未使用)
0x80040261	システムにより予約済み。(未使用)
0x80040262	システムにより予約済み。(未使用)
0x80040263	システムにより予約済み。(未使用)
0x80040264	システムにより予約済み。(未使用)
0x00040265	システムにより予約済み。(未使用)
0x80040265	システムにより予約済み。(未使用)
0x80040270	システムにより予約済み。(未使用)
0x80040271	システムにより予約済み。(未使用)
0x80040272	システムにより予約済み。(未使用)
0x80040273	システムにより予約済み。(未使用)
0x80040274	システムにより予約済み。(未使用)
0x80040275	システムにより予約済み。(未使用)
0x80040280	アクティベーションコードが無効です。
0x80040281	アクティベーションコードの形式が正しくありません。

サーバのイベントログの説明

[サーバイベント] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで、[ログ]→[サーバイベント] の順に選択します。

サーバのイベントログの説明 (StellarProtect (Legacy Mode))

イベント ID	サーバイベント	説明
1001	コンソールにログオン	管理サーバ画面にログオンしました。
1002	コンソールからログオフ	管理サーバ画面からログオフしました。
1003	セッションタイムアウト	管理サーバ画面のセッションがタイムアウトしました。アカウント「%user_name%」は自動的にログオフしました。
1011	レポートを送信できません	予約レポートを%email_address%に送信できません。
1012	通知を送信できません	通知を%email_address%に送信できません。
2001	アカウントの作成	Intelligent Manager アカウント「%user_name%」を作成しました。
2002	アカウントの削除	Intelligent Manager アカウント「%user_name%」を削除しました。
2003	アカウントの変更	Intelligent Manager アカウント「%user_name%」%field_name%を変更しました。

イベント ID	サーバイベント	説明
3001	エージェントイベントログの削除 -自動	エージェントイベントログの自動削除。
3002	エージェントイベントログの削除 -手動	エージェントイベントログの手動削除。
3003	エージェントイベントログのバックアップ	エージェントイベントログの自動バックアップ。 パス: %filepath%
3004	サーバイベントログの削除 - 自動	サーバイベントログの自動削除。
3005	サーバイベントログの削除 - 手動	サーバイベントログの手動削除。
3006	サーバイベントログのバックアップ	サーバイベントログの自動バックアップ。 パス: %filepath%
4001	許可されていないブロックされたファイルの処理	エージェントに要求を送信しました (ブロックされたファイルを許可リストに追加する)。 ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1) エージェントに要求を送信しました (ブロックされたファイルを削除する)。 ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1) エージェントに要求を送信しました (ブロックされたファイルを無視する)。 ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1) エージェントに要求を送信しました (ファイルを隔離する)。 ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1) エージェントに要求を送信しました (隔離されたファイルを復元する)。 ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1)

イベント ID	サーバイベント	説明
4004	隔離された 不正ファイルの解除	エージェントに要求を送信しました (隔離されたファイルを復元する)。 ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1)
4005	隔離された 不正ファイルの削除	エージェントに要求を送信しました (隔離されたファイルを削除する)。 ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1)
4006	許可されていない ファイルレス攻撃の処理	エージェントに要求を送信しました (ブロックされたプロセスチェーンとコマンド引数の組み合わせを追加する)。 プロセスチェーン: %process_name% コマンド引数: %parameter% エージェントに要求を送信しました (ブロックされたプロセスチェーンとコマンド引数の組み合わせを無視する)。 プロセスチェーン: %process_name% コマンド引数: %parameter%
5001	アプリケーション制御を 有効化	エージェントのアプリケーション制御を有効化しました。
5002	アプリケーション制御を 無効化	エージェントのアプリケーション制御を無効化しました。
5011	信頼するファイルの ハッシュを追加しました	エージェントに信頼するファイルのハッシュを 1 個追加しました。エージェントに信頼するファイルのハッシュを%num%個追加しました。
5013	許可されたファイルの 削除	指定された項目をエージェントの許可リストから SLtasks.exe を使用して削除しました。
5021	ストレージデバイスの アクセスをブロック	エージェントでストレージデバイスのアクセスをブロックしました。
5023	ストレージデバイスの アクセスを許可	エージェントでストレージデバイスのアクセスを許可しました。
5025	信頼する USB デバイスの 追加	選択したエージェントに信頼する USB デバイスを追加しました
5601	エージェントの設定の エクスポート	ファイル (%file_desc%) を%endpoint_name%からエクスポートしました。

イベント ID	サーバイベント	説明
5602	エージェントの設定のインポート	ファイル (%file_desc%) をエージェントにインポートしました。
5800	エージェントの管理者パスワードの変更	エージェントのパスワードを変更しました。
5700	不正プログラムの検索	エージェントで不正プログラム検索を実行しました。
5701	エージェントコンポーネントのアップデート	エージェントコンポーネントをアップデートしました。
5900	エージェントの許可リストの更新	エージェントの許可リストを更新しました。
6001	エージェントに Patch を配信	エージェントに Patch を配信します。 Patch 名: %patch_name%
6101	エージェントの移動	エージェントが新しい Intelligent Manager サーバに移動されました
6201	メンテナンスモードを有効にしました	エージェントのメンテナンスモードを有効にしました。
6202	メンテナンスモードを無効にしました	エージェントのメンテナンスモードを無効にしました。
6301	グループポリシーの配信	グループポリシーを配信します。 バージョン: %version%
6302	ODC サーバに接続できません	ODC サーバに接続できません。
6401	Intelligent Runtime Learning (インテリジェントランタイム学習) の設定	Intelligent Runtime Learning (インテリジェントランタイム学習) を設定します。 バージョン: %policy_version%
6402	エージェントのパスワードの設定	エージェントのパスワードを設定します。 バージョン: %policy_version%
6403	予約検索の設定	予約検索を設定します。 バージョン: %policy_version%
6404	ユーザ指定不審オブジェクトの設定	ユーザ指定不審オブジェクトを設定します。 バージョン: %policy_version%

イベント ID	サーバイベント	説明
6405	エージェントの Patch の設定	エージェントの Patch を設定します。バージョン: %policy_version%

サーバのイベントログの説明 (StellarOne)

イベント ID	説明
45313	検索コンポーネントのアップデート開始
45314	検索コンポーネント [%s] のアップデートジョブが開始されました
45315	検索コンポーネントの予約アップデートを有効にする
45316	検索コンポーネントの予約アップデートを無効にする
45317	StellarOne の検索コンポーネントのアップデート元を変更する
45318	エージェントの検索コンポーネントのアップデート元を変更する
45319	検索コンポーネント [%s] のアップデートに成功しました
45320	検索コンポーネント [%s] のアップデートに成功しましたが複製は必要ありませんでした
45321	内部エラーにより検索コンポーネント [%s] のアップデートに失敗しました
45322	ネットワークに接続できなかったため検索コンポーネント [%s] のアップデートに失敗しました
45323	ポリシーのカスタマイズ
45324	[%s] からのポリシーの継承

第 9 章

テクニカルサポート

TXOne Networks 製品のサポートは、TXOne Networks とトレンドマイクロが相互に行います。すべての製品サポート情報は、TXOne とトレンドマイクロのエンジニアを介して提供されます。

この章では、トラブルシューティング、TXOne およびトレンドマイクロへの問い合わせ、不審コンテンツの送信、およびその他のリソースについて説明します。

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

https://success.trendmicro.com/jp/technical-support

脅威データベース

現在、不正プログラムの多くは、コンピュータのセキュリティプロトコルを回避するために、2 つ以上の技術を組み合わせた複合型脅威で構成されています。トレンドマイクロは、カスタマイズされた防御戦略を策定した製品で、この複雑な不正プログラムに対抗します。脅威データベースは、既知の不正プログラム、スパム、悪意のある URL、および既知の脆弱性など、さまざまな混合型脅威の名前や兆候を包括的に提供します。

詳細については、https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/をご覧ください。

- 現在アクティブまたは「in the Wild」と呼ばれている生きた不正プログラムと悪意のあるモバイルコード
- これまでの Web 攻撃の記録を記載した、相関性のある脅威の情報ページ
- 対象となる攻撃やセキュリティの脅威に関するオンライン勧告
- Web 攻撃およびオンラインのトレンド情報
- 不正プログラムの週次レポート

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「製品サポートガイド」または「スタンダードサポートサービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話またはお問い合わせ Web フォームをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポートサービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービス継続を希望される場合は契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意

サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出/駆除できない場合などに、感染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「脅威データベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

https://success.trendmicro.com/jp/virus-and-threat-help

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

メールレピュテーションについて

スパムメールやフィッシングメールなどの送信元を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

ファイルレピュテーションについて

不正プログラムなどのファイル情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Web レピュテーションについて

不正な Web サイトや URL などの情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

製品やドキュメントの最新版は、次の Web ページからダウンロードできます。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

注意

サービス製品、販売代理店経由での販売製品、または異なる提供形態をとる製品など、一部対象外の製品があります。

脅威解析・サポートセンターTrendLabs (トレンドラボ)

TrendLabs (トレンドラボ) は、フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 か所の各国拠点と連携してソリューションを提供しています。

世界中から選び抜かれた 1,000 名以上のスタッフで 24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。

文書番号: APEM29595_JP2303