TRITON Unified Security Center ヘルプ

Websense® TRITON Unified Security Center

v7.7

Published 2012
Printed in the United States of America and Ireland.

商標について

目次

1 使用開始にあたって

TRITON Unified Security Center は、Websense セキュリティ ソフトウェアの全般的設定、ポリシー管理およびレポート機能のための集中的グラフィカル インターフェースを提供するブラウザ ベースのコンソールです。

TRITON コンソールは、ご使用のサブスクリプションによって、以下のようなモジュールの 1 つまたはいくつかを含んでいます。

- **TRITON – Web Security** は種々の統合デバイス（プロキシ サーバー、ファイアウォール、ルーター、キャッシング アプライアンスなど）とともに動作し、これによってユーザーはインターネット アクセス ポリシーを作成し、モニターし、適用することができます。
- **TRITON – Data Security** は、組織の周辺および内部における情報漏洩とデータ喪失から組織を保護します。
- **TRITON – Email Security** は、電子メールによるマルウェア、スパム、その他の望ましくないコンテンツの脅威から組織を保護します。

ご使用のサブスクリプションに TRITON Mobile Security が含まれている場合、TRITON コンソールには Mobile Security ポータルへのリンクも用意されています。これはモバイル デバイスの脅威からの保護とデータ損失の防止を管理するために使用するクラウド ベースのコンソールです。

TRITON コンソールへのログオン

TRITON コンソールは、ご使用の Websense ソフトウェア モジュールのソフトウェア構成と設定を管理するための集中化された設定インタフェースです。このウェブ ベースのツールは、以下のような完全にサポートされるブラウザで動作します。

- Microsoft Internet Explorer 8 、,9 、および 10

> **ご注意**
> Internet Explorer を使用している場合は、Enhanced Security Configuration がオフになっていることを確認してください。
>
> また、Internet Explorer 8 を使用している場合は、Compatibility View はサポートされていません。

- Mozilla Firefox 4.x 、 5.x 、および 6.x
- Google Chrome 13 以上

TRITON コンソールは他のブラウザからでも起動できますが、このアプリケーションのすべての機能を利用し、適切に表示ためには、サポートされているブラウザを使用してください。

> **ご注意**
> TRITON コンソール上の一部のアニメーションは、ブラウザの設定に依存します。アニメーションを適切に表示するためには、Internet Explorer で、**[Tools (ツール)]** > **[Internet Options (インターネット オプション)]** > **[Advanced (詳細)]** > **[Multimedia (マルチメディア)]** > **[Play animation in webpages (ウェブページのアニメーションを再生する)]** オプションを選択します。

TRITON コンソールを起動するには、次のいずれかを実行します。

- Windows コンピュータ上で **[Start (スタート)]** >**[Programs (プログラム)]** > **[Websense]** へ進み、**[TRITON] [Unified Security Center]** を選択します。
- インストール時にデスクトップ上に置かれている TRITON Unified Security Center のショートカットをダブルクリックします。
- ネットワーク上のコンピュータ上でサポートされているブラウザを開き、以下のように入力します。

  ```
  https://<IP_address_or_hostname>:9443/triton/
  ```

  "IP address or hostname" の部分に TRITON コンピュータの実際の IP アドレスまたはホスト名を入力します。IP アドレスの使用をお勧めします – 特に、リモート コンピュータから TRITON を起動する場合。

インストールが完了した時、デフォルト ユーザ、**admin** が TRITON コンソールのすべてのモジュールに対して完全な管理アクセス権を持ちます。このアカウントの削除はできず、そのユーザ名は変更できません。admin パスワードはインストール時に設定されます。

ログオン ページで、**ユーザ名** と **パスワード**を入力し、**[Log On (ログオン)]** をクリックします。組織が二要素認証を使用している場合は、*二要素認証によるログオン* の項を参照してください。

> **ご注意**
> TRITON コンソールで作成したローカル ユーザ名を使用していて、そのユーザ名とパスワードがネットワーク アカウントのユーザ名とパスワードと一致する場合、ローカル アカウントが優先されます。

リモート コンピュータから TRITON コンソールに接続できない場合は、ファイアウォールがそのポートでの通信を許可するようにしてください。

二要素認証によるログオン

二要素認証を使用している場合、通常はログオン ページは表示されません。その代わり、TRITON コンソール URL にアクセスすると:

1. コンソールは、クライアント証明書がインストールされているかどうかを検出します。
2. 組織による定義されている二要素認証を入力します。
3. 認証が成功すると、TRITON コンソールはクライアント証明書を受け取り、それがアップロードされているルート CA 証明書の署名と一致するかどうかを調べます。
4. 署名が一致すれば、TRITON コンソールは、ユーザーが TRITON コンソールにアップロードした、またはユーザー ディレクトリからインポートされた証明書と完全に一致するかどうかを調べます。
5. 一致が確認されると、コンソールへのログオンが完了します。

証明書の一致が確認されない場合のログオン プロセスは、前もって設定されているフォールバック オプションによって異なります。

- 属性マッチングは、クライアント証明書がユーザー ディレクトリ中の特定の LDAP 属性と一致するプロパティを含んでいるかどうかを調べます。
- 証明書の一致と属性マッチングが失敗した場合は、パスワード認証が有効化されます。

いずれのオプションも利用できない場合、一致する証明書なしにログオンすることはできません。

すべての管理者アカウントが二要素認証を使用するように設定されていて、管理者にクライアント証明書がないか、または証明書の一致に失敗する場合でも、以下のようにして TRITON コンソールにログオンできます。

1. TRITON Management Server コンピュータでブラウザを開きます。Remote Desktop Connection を使用して、そのコンピュータにアクセスできます。
2. URL、https://127.0.0.1:9443/triton (または https://localhost:9443/triton) にアクセスします。
3. **admin** ユーザ名およびパスワードを使用して、ログオンします。

ここで、他の管理者アカウントにフォールバックを提供する二要素認証オプションを設定することができます。*証明書認証の構成*, 27 ページを参照してください。

セキュリティ証明書アラート

TRITON コンソールとのセキュアなブラウザ ベースの通信のために、SSL 接続 が使用されます。この接続は、Websense, Inc. が発行するセキュリティ証明書を使用します。対応しているブラウザは Websense, Inc. を既知の Certificate Authority として認識しないので、新しいブラウザから TRITON コンソールを最初に起動するとき証明書エラーが表示されます。このエラーを

避けるためには、ブラウザ内にその証明書をインストールするか、またはその証明書を「今後も受け入れる」ように設定します。その方法については、Websense Technical Library を参照してください。

セキュリティ証明書が受け入れられると、TRITON Unified Security Center ログオン ページがブラウザのウィンドウに表示されます。

ご注意
Internet Explorer を使用している場合、その証明書を受け入れてからも証明書エラーが表示されます。このエラー メッセージを消去するには、ブラウザをいったん閉じて、再度開きます。

Windows 7 の考慮事項

Windows 7 オペレーティングシステムを使用している場合は、管理者としてブラウザを開いて、ActiveX コントロールを許可しなければなりません。

1. ブラウザ アプリケーションを右クリックし、**[Run as administrator（管理者として実行）]** を選択します。
2. TRITON コンソールにログオンし、上の説明のようにセキュリティ証明書を受け入れます。

Adobe Flash Player

Data Security、Web Security および Email Security ダッシュボードを使用するには Adobe Flash Player v8 以上が必要です。TRITON コンソールの他のすべての機能は Flash なしで動作します。Flash Player がインストールされていない場合、ログオン時にインストールを要求されます。表示されるリンクをクリックし、Adobe ダウンロード センターから Flash Player をダウンロードします。

タイムアウト

TRITON コンソール セッションは、ユーザー インタフェースでの最後のアクション（ページの移動のためのクリック、情報の入力、変更のキャッシング、変更の保存など）から 30 分を経過した時に終了します。セッション終了の 5 分前に警告メッセージが表示されます。

- キャッシュされていない、または保存されていない変更がある場合、セッション終了時にその変更は失われます。必ず変更を定期的に保存および配備してください。
- 同じブラウザ ウィンドウの複数のタブで TRITON コンソールが開かれている場合、すべてのインスタンスで同じセッションが共有されます。いずれかのタブでセッションがタイムアウトすると、セッションはすべてのタブでタイムアウトします。
- 同じコンピュータの複数のブラウザ ウィンドウで TRITON コンソールが開かれている場合、デフォルトではすべてのインスタンスで同じセッションが共有されます。

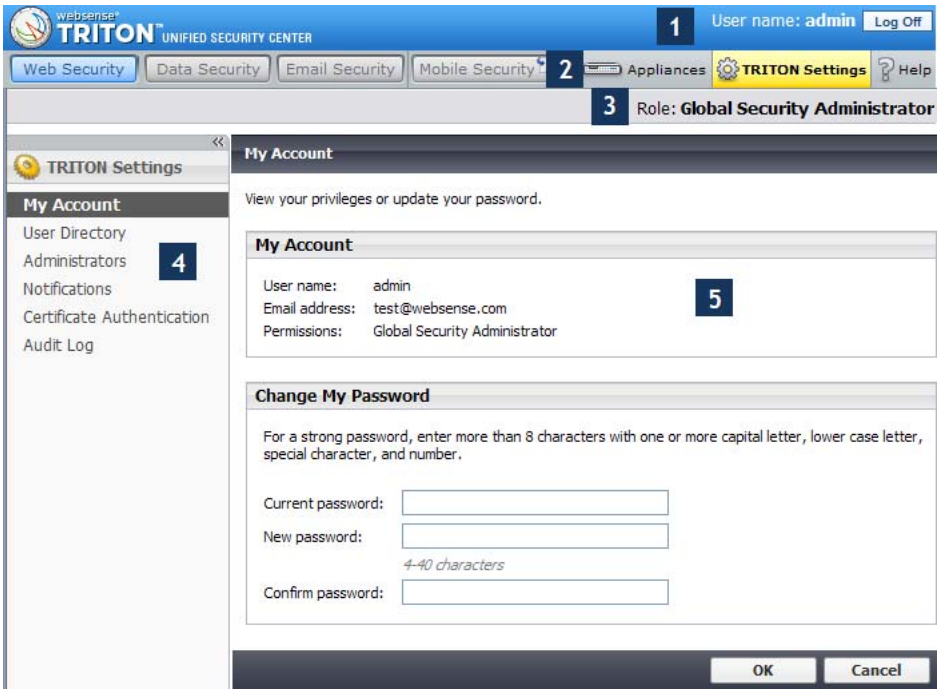
いずれかのウィンドウでセッションがタイムアウトすると、セッションはすべてのウィンドウでタイムアウトします。

- 以下のような場合には、セッションを共有しない複数の TRITON インスタンスを開くことができます。その場合、いずれかのウィンドウがタイムアウトしても、他のウィンドウへの影響はありません。
  - [File] > [New Session] コマンドを使って、新しい Internet Explorer 8 または 9 のウィンドウを開きます。
  - Internet Explorer を使って TRITON コンソールとの接続を開き、次に Firefox または Chrome を使って別の接続を開きます。

TRITON コンソールからログオフせずにブラウザを閉じるか、または TRITON コンソールにアクセスするために使用しているリモート コンピュータが突然にシャットダウンすると、ユーザは一時的にロックアウトされます。Websense ソフトウェアは、通常、この問題を約 2 分以内に検出し、中断されたセッションを終了し、ユーザが再度ログオンできるようになります。.

TRITON コンソールでのナビゲーション

TRITON Settings インタフェースには 5 つのメイン エリアがあります:



1. バナー
2. TRITON ツールバー
3. モジュール ツールバー
4. ナビゲーション ペイン
5. コンテンツ ペイン

バナーには以下の情報が示されます。

- 現在の **ログオン アカウント**
- 管理者セッションを終了するときに使用する **[Log Off(ログオフ)]** ボタン。

TRITON ツールバー はどのモジュールがアクティブかを示し、このツールバーから他の TRITON モジュールを起動することができます。また、**[Help(ヘルプ)]**、チュートリアル、Technical Library、その他の有益な情報にアクセスすることもできます。

TRITON コンソールにログオンすると、最後にアクセスしたモジュールがアクティブになり、TRITON ツールバー上でそのモジュールのボタンが黄色になります。インストールされているが、現在アクティブでないモジュールのボタンは青色になり、インストールされていないモジュールのボタンはグレイ表示になります。

モジュール ツールバーには、現在アクティブなモジュールの情報とそのオプションが示されます。TRITON 設定またはアプライアンスを構成するとき、ここに TRITON 管理者許可が表示されます。

ナビゲーション ペインには、現在選択されている TRITON モジュールまたは TRITON 設定オプションに使用できるナビゲーション オプションがあります。**コンテンツ ペイン** は、ナビゲーション ペインでの選択によって異なります。

個々のモジュールの詳細については、以下の項目を参照してください:

- TRITON – Data Security ヘルプ
- TRITON – Email Security ヘルプ
- TRITON – Web Security ヘルプ

MyWebsense ポータルによるアカウントの管理

Websense, Inc. のカスタマ ポータル www.mywebsense.com では、ご使用の Websense ソフトウェアの製品更新、パッチおよびホットフィックス、製品ニュース、評価、テクニカル サポート情報ソースなどにアクセスできます。

アカウントを作成すると、アカウントはお客様の Websense サブスクリプション キーに関連付けられます。これによって、ご使用の

組織の複数のユーザーのために、同じサブスクリプション キーに関連付けられた MyWebsense ログオンを作成することができます。

Websense テクニカル サポート

Websense ソフトウェアおよびサービスに関する下記のような技術情報に support.websense.com で 1 日 24 時間いつでもアクセスできます:

- 最新のリリース情報
- 検索可能な Websense Knowledge Base
- サポート フォーラム
- サポート ウェビナー
- "show-me" チュートリアル
- 製品マニュアル
- よくある質問に対する回答
- カスタマがよく遭遇する問題
- 詳細な技術ペーパー

その他の質問については、このページの上部にある [Contact Support] タブをクリックしてください。

緊急の問題の場合は、下記のいずれかのオフィスに電話してください。最初に対応可能な技術者に転送されます。この技術者がお客様を支援します。

緊急でない場合は、ask.websense.com のオンライン **Support Request Portal** を利用してください。

速やかな電話応答のために、MyWebsense の「 Profile 」セクションにある **サポート アカウント ID** を利用することができます。

地域	連絡先情報
北米	+1-858-458-2940
フランス	最寄の Websense の販売店に連絡してください。最寄の Websense の販売店が不明の場合 : +33 (0) 1 5732 3227
ドイツ	最寄の Websense の販売店に連絡してください。最寄の Websense の販売店が不明の場合 : +49 (0) 69 517 09347
英国	最寄の Websense の販売店に連絡してください。最寄の Websense の販売店が不明の場合 : +44 (0) 20 3024 4401
その他のヨーロッパ	最寄の Websense の販売店に連絡してください。最寄の Websense の販売店が不明の場合 : +44 (0) 20 3024 4401
中東	最寄の Websense の販売店に連絡してください。最寄の Websense の販売店が不明の場合 : +44 (0) 20 3024 4401
アフリカ	最寄の Websense の販売店に連絡してください。最寄の Websense の販売店が不明の場合 : +44 (0) 20 3024 4401
オーストラリア / ニュージーランド	最寄の Websense の販売店に連絡してください。最寄の Websense の販売店が不明の場合 : +61 (0) 2 9414 0033
アジア	最寄の Websense の販売店に連絡してください。最寄の Websense の販売店が不明の場合 : +86 (10) 5884 4200
ラテン アメリカおよびカリブ地域	+1-858-458-2940

電話でのサポートの場合、次の準備が必要です。

- Websense のライセンス キー
- Websense 管理コンソールへのアクセス
- レポーティング ツールを実行しているコンピュータとデータベース サーバーへのアクセス
- ネットワークのアーキテクチャに精通しているか、専門家に連絡できること

2 TRITON 設定の構成

TRITON Unified Security Center は、中央管理コンソールによるウェブ、データおよび電子メール セキュリティ設定、ポリシー、レポーティングなどの管理を支援します。

この集中的管理を支援するために、グローバル セキュリティ管理者（デフォルトの **admin** アカウントを含む）は、**TRITON Settings** を使用して以下のような権限を持つ管理者アカウントの作成および設定することができます。

- すべての TRITON モジュールへの完全な管理アクセス
- 1 つの 1 つの TRITON モジュールへの完全な管理アクセス
- 1 つ以上の TRITON モジュールへの制限付きアクセス（例えば、レポーティングだけのアクセス）

管理者について, 13 ページを参照してください。

ご注意
TRITON 設定を変更すると、その変更が他の TRITON モジュールへ伝わるのに 30~90 秒かかります。たとえば、TRITON – Data Security の管理者を作成すると、その管理者が Data Security モジュールで表示されるのに 1 ～ 2 分かかります。

また、TRITON Settings を使用して、以下のこともできます：

- アカウント情報の表示とパスワードの変更。*アカウント情報の表示*, 10 ページを参照してください。
- ディレクトリ サービスへの接続のセットアップして、管理者がそのネットワーク アカウントにより TRITON コンソールへログオンできるようにする。*ユーザー ディレクトリ情報の設定*, 10 ページを参照してください。
- SMTP サーバーへの接続の構成して、管理者が TRITON コンソールへのアクセスを認められたり、そのアカウントが変更されたとき、電子メール通知を受け取れるようにする。また、これにより管理者はパスワードリセットを要求できるようになります。*電子メール通知の設定*, 25 ページを参照してください。
- 管理者用の二要素認証の構成。*証明書認証の構成*, 26 ページを参照してください。

- 管理者による TRITON Settings. へのログオン試行とその変更の監査。*監査ログ*, 30 ページを参照してください。

アカウント情報の表示

「 **TRITON Settings** 」>「 **My Account** 」ページを使用して、アカウントの許可情報を表示し、Help 情報表示のための優先言語を選択します。

TRITON コンソールのためのローカル ユーザ名とパスワードを割り当てられている場合、このページでそのパスワードを変更することもできます。

ネットワーク資格情報を入力して TRITON コンソールにログオンした場合、パスワード変更はネットワーク ディレクトリ サービスを通じて処理されます。問題があれば、システム管理者に連絡してください。

ご使用のアカウント に割り当てられている許可がこのページのツールバーに表示されます:

- グローバル セキュリティ管理者は、サブスクリプションに含まれるすべてのモジュールのすべての TRITON コンソール設定とすべてのポリシー、レポーティングおよび構成の設定への完全なアクセス権を持ちます。*グローバル セキュリティ管理者*, 13 ページを参照してください。
- グローバル セキュリティー管理者の権限を持っていない場合は、アクセスおよび管理できる TRITON モジュールがリストされます。

パスワードを変更するには以下の手順を実行します:

1. **現在のパスワード**を入力します。
2. **新しいパスワード**を入力し、確認のためにもう一度入力します。
   - パスワードは 4 ～ 40 文字で指定してください。
   - 強いパスワード、つまり 8 文字以上で、大文字、小文字、数字および特殊文字 (ハイフン、下線、空白など) をそれぞれ 1 文字以上含むパスワードの使用を推奨します■次のセグメントと統合。
3. **[OK]** をクリックして、変更を保存します。

Help の優先言語として英語以外の言語を選択するには、**[Language (言語)]** ドロップダウン リストで適切なエントリーを選択します。すべての Help ページがすべての言語で利用できるわけではないので、ご注意ください。特定の Help ページが選択言語で利用できないとき、英語のページが表示されます。

ユーザー ディレクトリ情報の設定

「 **TRITON Settings** 」>「 **User Directory (ユーザー ディレクトリ)** 」ページを使用して、ネットワーク アカウントを使用する管理者のためのディレクトリ通信を構成します。すべての管理ユーザの認証に同じディレクトリを使用しなければなりません。

- ユーザー ディレクトリは、ネットワークのユーザーとリソースに関する情報を格納します。
- 管理者がそのネットワーク アカウントを使用して TRITON Unified Security Center にログオンできるようにするには、ユーザー ディレクトリから情報を取得できるように TRITON コンソールを構成しなければなりません。

> **ご注意**
> 管理者のためのユーザー ディレクトリの構成は、エンド ユーザーのためのディレクトリ サービスの構成とは別に行われます。エンド ユーザー ディレクトリ サービスの構成は、個々の TRITON モジュールの内部でセットアップします。

TRITON コンソールは、以下の LDAP (Lightweight Directory Access Protocol) ディレクトリと通信することができます:

- Windows Active Directory (ネイティブ・モード)
- Novell eDirectory
- Oracle Directory Service
- Lotus Notes/Domino

このコンソールは他の汎用 LDAP ベース ディレクトリとも通信することができます。

以下のことにご注意ください:

- 重複するユーザ名は、LDAP ベース ディレクトリ サービスではサポートされていません。同一のユーザ名が複数のドメインで使用されないようにしてください。
- Windows Active Directory または Oracle Directory Service を使用する場合、パスワードが空白のユーザー名はサポートされません。すべてのユーザーにパスワードが割り当てられていることを確認してください。

管理者がネットワーク アカウントによって TRITON コンソールにログオンできるようにするには、以下の手順を実行します。

1. **[User directory server]** リストでユーザー ディレクトリを選択します。.
2. ディレクトリ サーバーを指定するために **IP アドレスまたはホスト名**を入力します。
3. Websense ソフトウェアがディレクトリとの通信で使用する**ポート** を入力します。
4. Websense ソフトウェアがディレクトリからユーザー名とパス情報を取得するために使用する管理者アカウントの**ユーザー識別名** と **パスワード**を指定します。
   - このアカウントはディレクトリからのクエリーおよび読み取りを実行できる必要がありますが、ディレクトリを変更できる必要はなく、またドメイン管理者である必要もありません。

- **[User distinguished name (ユーザー識別名)]** フィールドにアカウントの詳細を単一の文字列として入力します。"CN=user, DC=domain" の形式を利用でき、また、組織が Active Directory を使用している場合は "domain¥username" の形式を利用することもできます。

5. **[Test Connection (接続テスト)]** クリックして、指定された IP アドレスまたは名前およびポート番号にディレクトリが存在し、指定のアカウントがそのディレクトリと接続できることを確認します。
6. TRITON コンソールがユーザー情報の検索のために使用する**ルート ネーミング コンテクスト**を入力します。これは汎用 LDAP ディレクトリ、Lotus Notes/Domino および Oracle Directory Service では必須であり、Active Directory および Novell eDirectory では任意です。値を入力する場合、それは組織のドメインで有効なコンテクストでなければなりません。**[Root naming context (ルート ネーミング コンテクスト)]** フィールドが空白であれば、Websense ソフトウェアはディレクトリ サービスの最高レベルから検索を始めます。

> **ご注意**
> 複数のドメインで同じユーザ名を使用しないでください。Websense ソフトウェアが 1 人のユーザーについて重複したアカウント名を検出した場合、そのユーザーの透過的識別ができなくなります。

7. LDAP スキーマがネストされたグループを含んでいる場合は、**[Perform additional nested group search (別のネストされたグループ検索の実行)]** をオンにします。
8. ディレクトリ サービスとの通信を暗号化するには、**[Use SSL encryption (SSL 暗号化の使用)]** をオンにします。
9. ディレクトリ サービスが LDAP 参照を使用している場合は、Websense ソフトウェアがその参照に従うかどうかについて指示します。
10. [Generic Directory (汎用ディレクトリ)] を選択している場合は、以下のように設定します:
    - **Email attribute**: LDAP エントリ中のユーザーの電子メール アドレスを検出するために使用する属性名。デフォルトは **mail** です。
    - **User logon ID attribute**: LDAP エントリ中のユーザーのログオン ID を検出するために使用する属性名。
    - **User logon filter**: ログオン時にユーザーの詳細情報を検索する場合に適用するフィルタ。この文字列は **%uid** トークンを含んでいなければなりません。このトークンは、ログオン時にユーザーが入力したユーザー名と置き換わります。
    - **User lookup filter**:「 Add Network Account (ネットワーク アカウントの追加)」ページにインポートするユーザーを検出するために使用するフィルタ。このフィールドに **%query** をプレースホルダとして入力し、次に、「 Add Network Account 」ページで **[Refine search (検索の絞込み)]** をクリックして、ネットワーク ユーザーを見つけるための新しいコンテクストを入力します。

- **Group object class**（オプション）: グループを表す LDAP オブジェクト クラス。デフォルトは **group** です。
- **Group Properties**: ディレクトリ スキーマが memberOf 属性を使用するかどうかを指定します。memberOf 属性を使用する場合は、ユーザーが属しているグループの参照のために使用される属性を **[Group attribute（グループ属性）]** フィールドに入力します。

  そうでない場合は、特定のユーザーを含むグループの解決のために使用するクエリーを **[User group filter（ユーザー グループ フィルタ）]** フィールドに入力します。**%dn** を入力することができ、これはユーザーの DN によって置き換えられます。

11. **[OK]** をクリックします。

> **ご注意**
> 後日、ユーザー ディレクトリ設定を変更する場合は、そのユーザー ディレクトリ サーバーの正確なミラーリングを指定しておかなければ、既存の管理者は無効になります。新しいサーバーがミラーでなければ、新しいユーザーと既存のユーザーを区別できなくなる可能性があります。

管理者について

管理者は TRITON コンソールにアクセスし、1 つまたは複数のセキュリティ ソリューションの構成、ポリシーの管理、レポートの作成、またはこれらのタスクの組み合わせを実行することができます。利用できる許可は管理者のタイプによって異なります。

- グローバル セキュリティ管理者は、利用できるすべての TRITON モジュールへの完全なアクセスおよび管理権限を持ちます。*グローバル セキュリティ管理者*, 13 ページを参照してください。
- 他のタイプの管理者は、TRITON モジュールへの限定的なアクセス権限を持ちます。管理者には、同じアカウントで 1 つまたは複数の TRITON モジュールを管理または監査する権限が与えられます。*TRITON 管理者*, 14 ページを参照してください。

管理者の識別はネットワーク ログオン資格情報によって行うことができ、また TRITON コンソールへのアクセスに専用のアカウントを作成することができます。*ネットワーク アカウントの追加*, 19 ページ および *ローカル アカウントの追加*, 17 ページを参照してください。

グローバル セキュリティ管理者

デフォルトの Global Security Administrator ロールがインストール時に作成され、デフォルトのユーザー **admin** にこのロールが割り当てられます。インストール時に設定された パスワードで最初にログオンしたとき、TRITON コンソ

ールのすべての構成設定への完全な管理者アクセスが許可され、また、サブスクリプションに含まれるモジュールに対する以下の許可も付与されます。

- **TRITON – Web Security:** 無制限の許可を持つ Super Administrator（スーパー管理者）ロールに追加されます。
- **TRITON – Data Security:** Super Administrator 許可の割り当て。
- **TRITON – Email Security:**Super Administrator 許可の割り当て。

また、TRITON コンソールのこのインスタンスに登録されているすべてのアプライアンスの管理と透過的ログオンのための完全な許可も割り当てられます。

個別の TRITON モジュール内でグローバル セキュリティ管理者に与えられている許可は変更できません。

admin アカウントは Super Administrator ロールの管理者リストには表示されません。これは削除できず、許可の変更もできません。

必要に応じて、さらにグローバル セキュリティ管理者を追加することができます。複数のグローバル セキュリティ管理者を作成することによって、プライマリ グローバル セキュリティ管理者が不在の時に、別の管理者がすべての Websense ポリシーおよび構成設定にアクセスできるようになります。

TRITON 管理者

TRITON 管理者には 1 つ以上の TRITON モジュール（Web Security、Data Security、Email Security）へのアクセス権が与えられます。管理者には、Mobile Security ポータル、

管理者に 1 つ以上のモジュールへの**アクセス**権限または**アクセスおよびアカウント管理**権限を割り当てることができます。個別のモジュールについて管理者に割り当てられる 権限は、そのモジュールで管理者がどのように構成されているかによって異なります。デフォルトでは、以下のような許可が割り当てられます。

- TRITON – Web Security
  - **アクセス**:管理者はどのロールにも追加されず、「Status（ステータス）」>「Dashboard and Status（ダッシュボードとステータス）」>「Alerts（アラート）」ページにアクセスできるだけです。
  - **アクセスおよびアカウント管理**管理者は、無制限の許可を持つ Super Administrator ロールに追加されます。

  TRITON – Web Security では、管理者許可の変更は**「Policy Management（ポリシー管理）」>「Delegated Administration（指定済み管理）」**ページで行なうことができます。
- TRITON – Data Security

- **すべてのオプション**:管理者は Default（デフォルト）アクセス ロールを割り当てられ、「 Incidents & Reports（インシデントとレポート）」、「 Today（今日）」、「 My Settings（私の設定）」の各ページにアクセスできます。

TRITON – Data Security では、管理者許可の変更は「 **Settings（設定）**」>「 **General（一般）**」>「 **Authorization（認可）**」>「 **Administrators** 」ページと「 **Settings** 」>「 **General** 」>「 **Authorization** 」>「 **Roles（ロール）**」ページで行なうことができます。

- TRITON – Email Security
  - **アクセス**:管理者はデフォルトの Reporting 許可を割り当てられます。
  - **アクセスおよびアカウント管理**管理者は、デフォルトで Super Administrator 許可を割り当てられます。

  TRITON – Email Security では、管理者許可の変更は「 **Settings** 」>「 **General** 」>「 **Administrator Accounts（管理者アカウント）**」ページで行うことができます。

アプライアンスについて、管理者に TRITON コンソールに登録されているアプライアンスへの**完全アクセス**または**制限付きアクセス**を割り当てることができます。

- 完全アクセスが割り当てられていれば、管理者はアプライアンスの登録および登録削除を行うことができ、また TRITON コンソールから直接にアプライアンスにアクセスできます。Access is via single sign-on if configured (see *既存のアプライアンスをシングル サインオンに設定する*, 36 ページ).
- 制限付きアクセスが割り当てられている場合、管理者はアプライアンスにアクセスできますが、アプライアンスの登録および登録削除を行うことはできません。アクセスはすべてのアプライアンス（あとで追加されたものも含む）に対して、または特に選択されたアプライアンスに対して許可できます。

アカウント管理許可を持つ管理者はまた、割り当てられている許可の制限内で、TRITON コンソール内の他の管理者を編集および削除することもできます。

Administrators who log on to the TRITON console with a ローカルユーザー アカウントを使って TRITON コンソールにログオンする管理者は、自分の TRITON パスワード を変更することもできます（ *アカウント情報の表示*, 10 ページを参照してください）。

共有管理者アカウントが構成されたあとは、いずれかの TRITON モジュール（たとえば TRITON – Web Security）にログオンした管理者は、再びログオンすることなしに、TRITON ツールバーを使用して別のモジュール (Data Security または Email Security) に切り換えることができます。

TRITON コンソールへのアクセスの有効化

「 **TRITON Settings** 」>「 **Administrators** 」ページを使用して、管理者が TRITON コンソールにアクセスするために使用するアカウントを作成および管理します。

> **ご注意**
> このページを利用できるのは、グローバル セキュリティ管理者と、1 つ以上の TRITON モジュールを管理する権限を持っている管理者だけです。

Websense ウェブ、電子メールおよびデータ セキュリティの各ソリューションの組み合わせを含む配備では、管理者アカウントに利用可能な TRITON モジュールへの個別または一括のアクセス権限を与えることができます。

[User Name] 列の横の [Type] 列に各管理者アカウントのタイプが表示されます:

- **Local accounts (ローカル アカウント)** は、その TRITON コンソール内での使用のために特別に作成されます。
- **Network accounts (ネットワーク アカウント)** は、サポートされているディレクトリ サービスからの、TRITON コンソールへのアクセス権を付与されているアカウントです (*電子メール通知の設定*, 25 ページを参照してください)。

アカウントを追加するには、[Add Local Account (ローカル アカウントの追加)] または [Add Network Account (ネットワーク アカウントの追加)] をクリックします (*ローカル アカウントの追加*, 17 ページ および *ネットワーク アカウントの追加*, 19 ページを参照してください)。

このページ上の管理者アカウントの名前の隣に感嘆符のアイコンがあるときは、以下のいずれか (または両方) の場合です。

- そのアカウントに、関連付けられた電子メール アドレスがない。したがって管理者はパスワード変更または許可の更新についての通知を受け取ることができません。管理者の詳細情報を編集して、電子メール アドレスを追加してください。
- 管理者権限が Websense Data Security バージョン 7.5 と Websense Web Security Gateway バージョン 7.5 からインポートされ、TRITON コンソール内で統一されたものである。

  たとえば、バージョン 7.5 で Data Security Super Administrator 許可と Web Security Full Reporting 許可を持つ管理者が、以下のような許可を持つ TRITON コンソールにインポートされるようなケースです。

  - Data Security: アクセスおよびアカウント管理許可
  - Web Security: アクセスのみ
  - Email Security: アクセスなし

  管理者アカウントを編集し、割り当てられている許可を確認するか、または変更してください。そうしないと、管理者はログオンできません。

1 つ以上の TRITON モジュールを管理する許可がある TRITON 管理者としてこのページを表示している場合は、そのモジュールの管理者アカウントだけを管理および削除することができます。

グローバル セキュリティ管理者は任意の既存アカウントを管理および削除することができます。アカウントを削除するには、そのアカウント名の横のチェックボックスをオンにし、**[Delete]** をクリックします。

重要
管理者アカウントを削除すると、その管理者によって実行されたアクションは Data Security インシデント履歴に表示されなくなります。管理者アクションを保存する場合には、アカウントを削除せず、その管理者ロールを TRITON- Data Security に制限することを推奨します。

ローカル アカウントの追加

関連項目

- *TRITON コンソールへのアクセスの有効化*, 16 ページ
- *ネットワーク アカウントの追加*, 19 ページ
- *ローカル アカウントの編集*, 21 ページ

「 TRITON Settings 」>「 Administrators 」>「 Add Local Account（ローカル アカウントの追加）」 ページを使用して、Websense ユーザー アカウントを追加します。

1. 固有の **ユーザー名** を 50 文字以内で入力してください。
   - 名前は名前は 1～50 文字でなければならず、また、以下の文字を含むことはできません。
     `* < > ' ? { } ~ ! $ % & @ # . " | \ & + = ? / ; : , ^ ( )`
   - ユーザー名にはスペースとダッシュを含めることができます。
2. そのユーザーの有効な **電子メール アドレス** を入力します。

   この電子メール アドレスは、新しい管理者にアカウント情報を送信するために使用します。
3. このユーザーの **パスワード**（4～255 文字）を入力し、確認のためにもう一度入力します。

   強いパスワード、つまり 8 文字以上で、大文字、小文字、数字および特殊文字（ハイフン、下線、空白など）をそれぞれ 1 文字以上含むパスワードの使用を推奨します。
   - 大文字
   - 小文字

- 数字
- 特殊文字（ハイフン、アンダーライン、ブランク等）

> **ご注意**
> 「TRITON Settings」>「Certificate Authentication（証明書認証）」ページで二要素認証が有効化されていて、パスワード認証が無効化されている場合、ローカル アカウントではパスワード ログオンを利用できません。

4. 「TRITON Settings」>「Certificate Authentication」ページで二要素認証が有効化されている場合：
   a. [Certificate Authentication（証明書認証）] をクリックします。
   b. このアカウントの管理者認証で使用する証明書が置かれている場所を参照します。
   c. [Upload Certificate] をクリックします。

   詳細については、*証明書認証の構成*, 26 ページを参照してください。
5. TRITON コンソールとサブスクリプションのすべてのモジュールおよびアプライアンスの全体にわたる完全な許可を持つ管理者を作成するには、[Global Security Administrator] を選択します。

> **ご注意**
> グローバル セキュリティ管理者だけが他のグローバル セキュリティ管理者を作成できます。

6. 新しい管理者にアカウント情報とアクセス手順を電子メールで送信するには、[Notify administrator of the new account via email（新しいアカウントについて管理者に電子メールで通知する）] をオンにします。

   管理者に電子メールを送信するには、「Notifications（通知）」ページで SMTP 詳細を設定しなければなりません。「Notifications」ページ上で電子メール メッセージのコンテンツをカスタマイズすることもできます（*電子メール通知の設定*, 25 ページ を を参照してください）。
7. 管理者が TRITON コンソールに最初にログオンしたときにアカウント パスワードを変更することを要求するには、「Force administrator to create a new password at logon（ログオン時に管理者に新しいパスワードを作成させる）」をオンにします。
8. このアカウントがグローバル セキュリティ管理者でない場合、[Module Access Permissions（モジュールのアクセス許可）] で新しい管理者に割り当てる許可を選択します。
   - 利用できるオプション（Web Security、Data Security、Email Security）のそれぞれについて設定を選択し、新しい管理者に 1 つ以上の TRITON モジュールを管理する許可を割り当てます。利用できるオプションは、サブスクリプションに含まれるモジュールによって異なります。

それぞれのモジュールについて、新しい管理者にどのアクセス許可を割り当てるかを選択します。

- このモジュールへのアクセスを許可しない
- このモジュールへのアクセスのみ
- このモジュールへのアクセスと、このモジュールで他の管理者を管理する権限の両方

詳細については、*TRITON 管理者*, 14 ページを参照してください。

ご注意
アクセス許可を割り当てることができるのは、管理権限を持つ TRITON モジュールに対してだけです。

- 配備に 1 つ以上のアプライアンスが含まれている場合、管理者に以下のどれかを割り当てることができます。
  - アプライアンスへのアクセスを許可しない
  - すべてのアプライアンスへの完全なアクセス
  - アプライアンスへの制限付きアクセス

  制限付きアクセスを選択する場合、管理者にすべてのアプライアンスへのアクセスを許可するか、特定のアプライアンスへのアクセスのみを許可するかを指定してください。

9. 変更を完了したとき、[OK] をクリックします。

ネットワーク アカウントの追加

関連項目

- *電子メール通知の設定*, 25 ページ
- *ローカル アカウントの追加*, 17 ページ
- *ネットワーク アカウントの編集*, 23 ページ

「 TRITON Settings 」>「 Administrators 」>「 Add Network Account（ネットワーク アカウントの追加）」 ページを使用して、サポートされているディレクトリ サービスで TRITON 管理者として定義されるユーザーを追加します。

TRITON 管理者として追加するアカウントを見つけるために、[Search] フィールドに検索キーワードを入力します。アステリスク ワイルドカード (*) を検索で使用することもできます。

デフォルトでは、この検索コンテクストは「 Directory Service 」ページからのデフォルト ドメイン コンテクストです（*電子メール通知の設定*, 25 ページを参照してください）。このコンテクストを編集するには、[Refine search（検索の絞り込み）] をクリックし、表示されるフィールドに新しい検索コンテクストを入力します。[Restore default（デフォルトの復元）] をクリックすると、デフォルトのコンテクストに戻ることができます。

Active Directory を使用している場合、ユーザーについて、選択されているコンテクストの Email 、Login Name（ログイン名）および Display Name（表示名）フィールドを検索します。Novell eDirectory 、Oracle Directory Service または Lotus Notes/Domino を使用している場合、ユーザーについて Email 、Display Name 、Username （ユーザー名）および Common Name（共通名：CN）フィールドを検索します。すべてのディレクトリ サービスで、グループについて CN フィールドを検索します。

検索結果では、指定されたキーワードと一致するユーザーとグループの両方がリストされ、ネットワーク アカウントのユーザー名と電子メール アドレスの両方が表示されます。ユーザーまたはグループを管理者として追加するには、そのアカウント名の横のチェックボックスをオンにし、次に、右向き矢印（>）をクリックして、アカウントを選択されているアカウントのリストに追加します。

選択されているアカウントのリストからユーザーを削除するには、そのアカウント名の横のチェックボックスをオンにし、次に左向き矢印（<）をクリックします。

「 TRITON Settings 」>「 Certificate Authentication 」ページで二要素認証が有効化されている場合は（*証明書認証の構成*, 26 ページ）、**[Certificate Authentication]** をクリックして、TRITON コンソールのログオン時に選択されている管理者の認証のために使用する証明書をアップロードまたはインポートします。

- **[Import from LDAP (LDAP からインポート)]** をクリックすると、ユーザーディレクトリから証明書がインポートされます。
- **[Upload Certificate]** をクリックすると、証明書の場所に移動し、その証明書がアップロードされます。

証明書が正常にインポートまたはアップロードされると、証明書名、失効日、発行元およびソース情報が現在のページの「 Certificate Authentication 」領域に表示されます。

選択されているアカウントのリストに 1 つ以上のアカウントを追加したあと、**[Notify administrator of the new account via email（管理者に新しいアカウントを電子メールで通知する）]** を設定するかどうかを指定します。管理者に電子メールを送信するには、「 Notifications（通知）」ページで SMTP 詳細を設定しなければなりません。「 Notifications 」ページ上で電子メール メッセージのコンテンツをカスタマイズすることもできます（電子メール通知の設定、23 ページ を参照してください）。

次に、新しい管理者に付与するアクセス許可を選択します。

- TRITON コンソールとサブスクリプションのすべてのモジュールおよびアプライアンスの全体にわたる完全な許可を持つ管理者を作成するには **[Global Security Administrator]** を選択します。

> **ご注意**
> グローバル セキュリティ管理者だけが他のグローバル セキュリティ管理者を作成できます。

- アカウントがグローバル セキュリティ管理者でないときは、**[Module Access Permissions]** で新しい管理者に割り当てる許可を選択します。
  - 利用できるオプション (**Web Security** 、**Data Security** 、**Email Security**) のそれぞれについて設定を選択し、新しい管理者に 1 つ以上の TRITON モジュールを管理する許可を割り当てます。利用できるオプションは、サブスクリプションに含まれるモジュールによって異なります。

    それぞれのモジュールについて、新しい管理者にどのアクセス許可を割り当てるかを選択します。
    - このモジュールへのアクセスを許可しない
    - このモジュールへのアクセスのみ
    - このモジュールへのアクセスと、このモジュールで他の管理者を管理する権限の両方

    詳細については、*TRITON 管理者*, 14 ページ を参照してください。

    ご注意
    アクセス許可を割り当てることができるのは、管理権限を持つ TRITON モジュールに対してだけです。

  - サブスクリプションに 1 つ以上のアプライアンスが含まれている場合、新しい管理者に下記のどのアクセス許可を割り当てるかを選択します。
  - 配備に 1 つ以上のアプライアンスが含まれている場合、管理者に以下のどれかを割り当てることができます。
    - アプライアンスへのアクセスを許可しない
    - すべてのアプライアンスへの完全なアクセス
    - アプライアンスへの制限付きアクセス

    制限付きアクセスを選択する場合、管理者にすべてのアプライアンスへのアクセスを許可するか、特定のアプライアンスへのアクセスのみを許可するかを指定してください。

管理者アカウントの選択を完了したとき、**[OK]** をクリックします。

ローカル アカウントの編集

「 TRITON Settings 」>「 Administrators 」>「 Edit Local Account (ローカル アカウントの編集) 」 ページを使用して、既存の Websense ユーザー アカウントを編集します。

1. **ユーザー名**を変更するには、固有の名前を 50 文字以内で入力します。
   - 名前は 1～50 文字でなければならず、また、以下の文字を含むことはできません。

     `* < > ' { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,`
   - ユーザー名にはスペースとダッシュを含めることができます。

2. 管理者の**電子メール アドレス**を変更するには、そのユーザーの有効なアドレスを入力します。

   この電子メール アドレスは、この管理者にアカウント情報を送信するために使用します。

3. 管理者の**パスワード**をリセットするには、パスワード (4～255 文字) を入力し、確認のためにもう一度入力します。

   強いパスワード、つまり 8 文字以上で、大文字、小文字、数字および特殊文字 (ハイフン、下線、空白など) をそれぞれ 1 文字以上含むパスワードの使用を推奨します。

   - 大文字
   - 小文字
   - 数字
   - 特殊文字 (ハイフン、下線、空白など)

   ご注意
   「 TRITON Settings 」>「 Certificate Authentication (**証明書認証**) 」ページで二要素認証が有効化されていて、パスワード認証が無効化されている場合、ローカル アカウントではパスワード ログオンを利用できません。

4. 「 TRITON Settings 」>「 Certificate Authentication 」ページで二要素認証が有効化されている場合 :

   a. [Certificate Authentication (**証明書認証**)] をクリックします。

   b. TRITON コンソールへのログオン時に管理者が認証するために使用する証明書が置かれている場所を参照します。

   c. [Upload Certificate] をクリックします。

   詳細については、*証明書認証の構成*, 26 ページを参照してください。

5. TRITON コンソールとサブスクリプションのすべてのモジュールおよびアプライアンスの全体にわたる完全な許可を管理者に付与するには、[Global Security Administrator] を選択します。

   ご注意
   グローバル セキュリティ管理者だけが他のグローバル セキュリティ管理者を作成できます。

6. この管理者にアカウント変更の通知を電子メールで送信するには、[Notify administrator of the account change via email (**アカウント変更について管理者に電子メールで通知する**)] をオンにします。

7. 管理者が次に TRITON コンソールにログオンしたときにアカウント パスワードを変更することを要求するには、[Force administrator to create a new password at logon] をオンにします。

8. これがグローバル セキュリティ管理者アカウントでない場合、**[Module Access Permissions]** オプションを使用して、その管理者に割り当てる許可を更新します。
   - 利用できるオプション (**Web Security**、**Data Security**、**Email Security**) のそれぞれについて設定を選択し、管理者に 1 つ以上の TRITON モジュールを管理する許可を割り当てます。利用できるオプションは、サブスクリプションに含まれるモジュールによって異なります。

     それぞれのモジュールについて、管理者にどのアクセス許可を割り当てるかを選択します。
     - このモジュールへのアクセスを許可しない
     - このモジュールへのアクセスのみ
     - このモジュールへのアクセスと、このモジュールで他の管理者を管理する権限の両方

     For more information see *TRITON 管理者*, 14 ページ.

     ご注意
     アクセス許可を割り当てることができるのは、管理権限を持つ TRITON モジュールに対してだけです。

   - 配備に 1 つ以上のアプライアンスが含まれている場合、管理者に以下のどれかを割り当てることができます。
     - アプライアンスへのアクセスを許可しない
     - すべてのアプライアンスへの完全なアクセス
     - アプライアンスへの制限付きアクセス

     制限付きアクセスを選択する場合、管理者にすべてのアプライアンスへのアクセスを許可するか、特定のアプライアンスへのアクセスのみを許可するかを指定してください。
9. 変更を完了したとき、**[OK]** をクリックします。

ネットワーク アカウントの編集

「 TRITON Settings 」>「 Administrators 」>「 Edit Network Account (ネットワーク アカウントの編集) 」 ページを使用して、既存のネットワークアカウントのアクセスおよび認証許可を編集します。

「 TRITON Settings 」>「 Certificate Authentication 」ページで二要素認証が有効化されている場合は (*証明書認証の構成*, 26 ページを参照してください)、**[Certificate Authentication]** をクリックして、TRITON コンソールへのログオン時に管理者の認証のために使用する証明書をアップロードまたはインポートします。

- **[Import from LDAP (LDAP からインポート)]** をクリックすると、ユーザーディレクトリから証明書がインポートされます。
- **[Upload Certificate]** をクリックすると、証明書の場所に移動し、その証明書がアップロードされます。

証明書が正常にインポートまたはアップロードされると、証明書名、失効日、発行元およびソース情報が現在のページの「 Certificate Authentication 」領域に表示されます。**[Import New from LDAP (LDAP から新規インポート)]** をクリックすると、ユーザー ディレクトリから新しい証明書がインポートされ、既存の証明書と置き換わります。

[Remove Certificate (証明書の削除)] をクリックすると、このネットワーク アカウントから証明書が削除されます。証明書を削除すると、このネットワーク アカウントは二要素認証を使用できなくなります。

ネットワーク アカウントのアクセス許可を変更するには、以下の手順を実行します。

- 管理者に TRITON コンソールとサブスクリプションのすべてのモジュールおよびアプライアンスの全体にわたる完全な許可を割り当てるには、**[Global Security Administrator]** を選択します。

  ご注意
  グローバル セキュリティ管理者だけが他のグローバル セキュリティ管理者を作成できます。

- これがグローバル セキュリティ管理者アカウントでない場合、**[Module Access Permissions]** オプションを使用して、その管理者に割り当てる許可を更新します。
  - 利用できるオプション (**Web Security** 、**Data Security** 、**Email Security**) のそれぞれについて設定を選択し、管理者に 1 つ以上の TRITON モジュールを管理する許可を割り当てます。利用できるオプションは、サブスクリプションに含まれるモジュールによって異なります。

    それぞれのモジュールについて、管理者にどのアクセス許可を割り当てるかを選択します。
    - このモジュールへのアクセスを許可しない
    - このモジュールへのアクセスのみ
    - このモジュールへのアクセスと、このモジュールで他の管理者を管理する権限の両方

    詳細については、*TRITON 管理者*, 14 ページを参照してください。

    ご注意
    アクセス許可を割り当てることができるのは、管理権限を持つ TRITON モジュールに対してだけです。

  - 配備に 1 つ以上のアプライアンスが含まれている場合、管理者に以下のどれかを割り当てることができます。
    - アプライアンスへのアクセスを許可しない
    - すべてのアプライアンスへの完全なアクセス
    - アプライアンスへの制限付きアクセス

制限付きアクセスを選択する場合、管理者にすべてのアプライアンスへのアクセスを許可するか、特定のアプライアンスへのアクセスのみを許可するかを指定してください。

管理者許可の編集を完了したとき、[OK] をクリックします。

電子メール通知の設定

「 TRITON Settings 」>「 Notifications 」 ページを使用して、TRITON コンソールからのすべての電子メール通知で使用する SMTP サーバーをセットアップし、管理者に送信する電子メール通知のメッセージを構成します。

ご注意
このページを表示し、編集できるのはグローバル セキュリティ管理者だけです。

最初に、SMTP サーバーとの接続を確立し、電子メール通知を送信できるようにします。

1. SMTP サーバー コンピュータの **IP アドレスまたはホスト名**と**ポート**を入力します。
2. 通知で使用する **送信者電子メール アドレス**を入力します。
3. 電子メールの「 From 」アドレスに表示する**送信者名**を入力します。これは管理者にその電子メールが TRITON コンソールと関連していることを知らせるのに便利です。

次に、管理者通知に使用するテンプレートを検討します。以下の 3 種類のテンプレートが用意されています。

- **New Account (新しいアカウント)**:管理者に新しい TRITON アカウントを通知します。このテンプレートは、通常、新しいログオン名およびパスワードとその管理者に割り当てられている許可の一覧を含んでいます。
- **Edit Account (アカウントの編集)**: 管理者に TRITON アカウントの変更を通知します。これは、通常、変更される可能性があり、その管理者に知らせる必要がある情報 (ログオン名、パスワード、許可など) を含んでいます。
- **Forgot Your Password (パスワードをお忘れですか？)** :TRITON ログオン ページで "Forgot Your Password" リンクをクリックした管理者に対して、そのパスワードがリセットされたことを確認します。これは、通常、一時的パスワードとそのパスワードの有効期限についての情報を含んでいます。

各テンプレートは、デフォルトのテキスト (そのまま使用するか変更することができる) といくつかの利用可能な変数を含んでいます。電子メールが管理者に送信されるとき、これらの変数はユーザー固有のデータまたはシステムの他の部分で設定されている値に置き換えられます。変数は常にパーセント記号で囲まれています (例 %Username%)。

通知メッセージを変更するには、以下の手順を実行します。

1. 電子メール通知テンプレートのいずれかのタブを選択します。New Account 、Edit Account 、Forgot Your Password 。
2. 電子メール メッセージの適切な件名ヘッダーを入力します。たとえば、新しいアカウントのヘッダーとして "Welcome to Websense TRITON (ようこそ Websense TRITON へ)" や "Your new TRITON console account (新しい TRITON コンソール アカウントです)" などを使用できます。
3. メッセージ本文を適切に変更します。変数を追加するには、**[Insert Variable (変数の挿入)]** をクリックし、ドロップダウン リストから選択します。

変数	説明
%TRITON URL%	TRITON コンソールにアクセスするために使用する URL 。
%Username%	管理者の TRITON ユーザー名。
%Password%	管理者の TRITON パスワード。 これは、"Forgot Your Password" リンクを使用した管理者に割り当てられる一時的パスワードである場合もあります。このパスワードの有効期間は 30 分であり、管理者がこの期間内にログオンしたとき、新しいパスワードの入力を求められます。
%Permissions%	管理者に割り当てられる許可。

ご注意
デフォルトの通知テキストの全部または一部を利用する場合、変数はデフォルト メッセージの末尾にだけ含めることができます。

4. いつでもデフォルトの通知テキストに戻ることができます。そのためには **[Restore Default (デフォルトの復元)]** をクリックし、次に確認のために **[OK]** をクリックします。

証明書認証の構成

「 TRITON Settings 」>「 Certificate Authentication 」ページで、管理者ログオンでの二要素認証の使用を管理します。

ご注意
このページにアクセスできるのはグローバル セキュリティ管理者のみです。

二要素認証では、管理者は TRITON コンソールへのログオン時に 2 つの形式の ID を提供しなければなりません（*証明書認証の仕組み*, 28 ページを参照してください）。

TRITON 管理者に他の Websense 管理コンソール (Appliance Manager と Content Gateway Manager) へのシングル サインオン アクセスを許可することができます。この機能を二要素認証で利用する方法:

- **Appliance Manager**:Content Gateway Manager のパスワード認証を無効化します*既存のアプライアンスをシングル サインオンに設定する*, 36 ページを参照してください）。**Manager**:Content Gateway Manager のパスワード認証を無効化します (Content Gateway Help の「 Configuring Content Gateway for two-factor authentication 」を参照してください）。

TRITON コンソール証明書認証を設定するには、以下の手順を実行します。

1. **[Authenticate administrators using two-factor authentication (二要素認証による管理者の認証)]** をオンにします。
2. 属性マッチングを有効化するために、**[Use attribute matching as a fallback method (属性マッチングをフォールバック方法として使用)]** をオンにし、これをすべての管理者に適用するか、TRITON コンソールに証明書がない管理者にのみ適用するかを選択します。

   マッチングに使用する属性を構成するために、[Configure Attribute Matching (属性マッチングの構成)] をクリックし、次に *属性マッチングのセットアップ*, 29 ページを参照してください。
3. ユーザー ディレクトリからネットワーク管理者の証明書をインポートするために、**[Import Administrator Certificates (管理者証明書のインポート)]** をクリックします。

   証明書が正常にインポートされると、完了メッセージがページの上部に表示されます。いずれかの証明書が正常にインポートされなかった場合、「 TRITON Settings 」>「 Administrators 」>「 Edit Network Account 」ページ上で個々のネットワーク管理者の証明書をアップロードすることができます。
4. **[Root Certificates (ルート証明書)]** の下の **[Add]** をクリックして、署名確認のためのルート証明書を追加します。二要素認証が機能するためには、TRITON コンソールに 1 つ以上のルート証明書がなければなりません。
5. ルート証明書ファイルが置かれている場所を参照し、**[Upload Certificate (証明書のアップロード)]** をクリックします。
6. ルート証明書を追加または変更したときは必ず、新しいマスタ証明書ファイルを作成し、そのファイルを Websense TRITON Web Server サービスにコピーしなければなりません。
   [Create Master Certificate File (マスター証明書ファイルの作成)] をクリックして新しいファイルを作成し、次に、詳細について *マスター証明書ファイルの配備*, 29 ページを参照してください。

7. パスワード認証をフォールバック方法として有効にするために、**[Allow password authentication to log on to the TRITON console (TRITON コンソールへのログオンでパスワード認証を許可)]** をオンにし、これをすべての管理者に適用するか、TRITON コンソールに証明書がない管理者にのみ適用するかを選択します。

> **ご注意**
> インストール時に作成された **admin** アカウントは、常に TRITON Management Server コンピュータからパスワード方式の認証によりログオンすることができます。

8. **[OK]** をクリックします。

証明書認証の仕組み

「 Certificate Authentication 」ページで二要素認証を有効化したとき、管理者が TRITON コンソール URL にアクセスする際のログオン プロセスは以下のようになります。

- TRITON コンソールは、クライアント証明書がインストールされているかどうかを検出します。複数の証明書が利用できる場合、管理者はコンソールへのアクセスを許可する証明書を選択するよう求められます。
- 管理者は、組織によって定義されている二要素認証資格情報を提供します。たとえば、Common Access Card (CAC) とカード リーダーを使用する場合があります。
- 認証が成功すると、TRITON コンソールはクライアント証明書を受け取り、それがアップロードされているルート CA 証明書の署名と一致するかどうかを調べます。署名が一致すれば、TRITON コンソールは、ユーザーが TRITON コンソールにアップロードした、またはユーザー ディレクトリからインポートされた証明書と完全に一致するかどうかを調べます。一致が確認された場合、その二要素認証資格情報と関連付けられている管理者はコンソールにログオンされます。
- 一致する証明書が見つからず、属性マッチングがフォールバック方法として設定されている場合、クライアント証明書がユーザー ディレクトリ内の特定の LDAP 属性と一致するプロパティを含んでいるかどうかがチェックされます。一致が確認された場合、その二要素認証資格情報と関連付けられている管理者はコンソールにログオンされます。

構成されているすべての証明書および属性マッチングが失敗した場合、または管理者にクライアント証明書がない場合、パスワード認証をフォールバック オプションとして許可することができます。パスワード認証が無効化されている場合は、証明書の一致が確認できない管理者はログオンできません。

マスター証明書ファイルの配備

証明書認証のルート証明書を変更したあとで新しいマスター証明書ファイル作成するとき、その新しいファイルで Websense TRITON Web Server サービスを更新しなければなりません。そのために以下の手順を実行します。

1. TRITON Unified Security Center がインストールされているディレクトリ（デフォルトでは **C:¥Program Files (X86)¥Websense**）に移動し、**EIP Infra** ディレクトリにアクセスします。
2. スクリプト ファイル **replace_2fa_certificate.bat** を実行します。

このスクリプト ファイルは作成した新しいマスター証明書ファイルを Websense TRITON Web Server サービスにコピーし、次にこのサービスを再起動します。

属性マッチングのセットアップ

「 TRITON Settings 」>「 Certificate Authentication 」>「 Configure Attribute Matching 」 ページを使用して、提供された証明書の中のプロパティとマッチングする管理者 LDAP プロパティを定義します。

1. **[Administrator Property]** の下で、管理者の証明書とのマッチングに使用するプロパティをユーザー ディレクトリから選択します。これは以下のいずれかから選択できます。
   - 管理者の**電子メール アドレス**（ローカル アカウントとネットワーク アカウント）
   - **LDAP 識別名**（ネットワーク アカウントのみ）
   - **ユーザー名**（ローカル アカウントとネットワーク アカウント）
   - **カスタム LDAP フィールド**（ネットワーク アカウントのみ）

   ご注意
   汎用 LDAP ユーザー ディレクトリを使用する場合は、カスタム フィールドを指定しなければなりません。

2. カスタム LDAP フィールドを定義した場合、**[Verify Administrator Property（管理者のプロパティの確認）]** をクリックして、そのプロパティがユーザー ディレクトリにあることを確認します。どのネットワーク管理者アカウントに対して確認するかを選択します。

   ご注意
   [Verify Administrator Property] を利用できるのは、TRITON コンソールでユーザー ディレクトリを構成していて、少なくとも 1 つのネットワーク管理者アカウントをセットアップしている場合のみです。

このページの設定を保存したとき、TRITON コンソール内のすべての該当するアカウント（ネットワーク アカウントのみ、またはローカル アカウントとネットワーク アカウント）のカスタム プロパティがインポートされます。後にこのフィールドの変更が必要になった場合、**[Update Property（プロパティの更新）]** をクリックして、新しい属性マッチング値をインポートします。

3. **[Certificate Property（証明書プロパティ）]** で、管理者ログオン証明書の中から、定義した LDAP プロパティとマッチングするプロパティを選択します：
   - subjectAltName フィールドの電子メール（RFC822）属性。ユーザー ディレクトリの中の管理者電子メール アドレスとマッチングする場合にこれを選択します。
   - 件名識別名。これはこの証明書に関連付けられているエンティティを定義します。
   - 特定の Certification Authority（証明機関：CA）によって発行された各証明書の固有のシリアル番号。
4. **[OK]** をクリックします。

   選択したプロパティが、**「TRITON Settings」>「Certificate Authentication」** ページの「Certificate Matching（証明書マッチグ）」領域に表示されます。

監査ログ

「TRITON Settings」>「Audit Log（監査ログ）」 ページを使用して、システムで管理者が実行したアクションを表示します。

> **ご注意**
> このページにアクセスできるのはグローバル セキュリティ管理者のみです。

デフォルトでは、表示されるアクションは日付と時刻によってソートされます。フィルタを使用している場合は、表示されているアクションの数がリストの上部に表示されます。

列	説明
ID	アクションの ID 番号。**[Find ID（ID の検索）]** フィールドで ID 番号を入力し、**[Find（検索）]**. をクリックすることによって Audit Log アクションにすばやくジャンプできます。
日付と時刻	アクションが行われた日付と時刻。
管理者	TRITON コンソールでそのアクションを開始した管理者の名前とユーザー名。

列	説明
ロール	管理者のロール。
実行されたアクション	アクションの詳細。この列には、システムによって書き込まれる変数が表示されることがあります（例: ログオンのユーザー名）。

3 アプライアンスへのアクセス

Websense, Inc. は、Web および電子メールのトラフィックおよびコンテンツの分析のために最適化されたオペレーティング システムを備えたセキュリティ アプライアンスを提供しています。アプライアンス ベースのソリューションを購入された場合には、TRITON コンソールで種々のアプライアンスの詳細を表示し、それらのアプライアンスに容易にアクセスすることができます。

アプライアンスの管理

「Appliances（アプライアンス）」>「Manage Appliances（アプライアンスの管理）」ページを使用して、TRITON コンソールに登録され（関連付けられ）ている Websense アプライアンスをチェックし、追加アプライアンスを登録し、アプライアンスの登録を削除します。

登録されているそれぞれのアプライアンスについて、下記の情報が表示されます。

- アプライアンス上の C インターフェースの IP アドレス
- アプライアンスのホスト名
- セキュリティ モード:Web Security、Email Security、または Web Security と Email Security
- ポリシー ソース モード(Web Security を含むアプライアンスのみ):完全なポリシー ソース、ユーザー ディレクトリおよびフィルタリング、またはフィルタリングのみ
- 説明(Appliance Manager の「System（システム）」ページで編集できます）
- Websense のソフトウェア バージョン（例、7.7.0）
- ハードウェア プラットフォーム（例、V5000、V10000 G2）

アプライアンスの IP アドレスの横の矢印をクリックすると、アプライアンス情報が展開され、その詳細が表示されます。**[Expand All（すべてを展開）]** および **[Collapse All（すべてを非表示）]** ボタンを使用して、すべてのアプライアンス情報を展開するか、非表示にします。

アプライアンスの詳細の中に Single Sign-On（シングル サインオン）ボタンが表示されている場合、追加のログオン資格情報を提供することなしにそのアプライアンスにアクセスすることができます。

TRITON コンソールに新しいアプライアンスを追加するとき、そのアプライアンスをシングル サインオンに設定することができます。既存のアプライアンス（たとえば以前のバージョンからアップグレードされたアプライアンス）をシングル サインオンに設定することができます。*既存のアプライアンスをシングル サインオンに設定する*, 36 ページを参照してください。

シングル サインオンなしに TRITON コンソールからアプライアンスに直接にアクセスできますが、別にログオン資格情報を入力しなければなりません。*アプライアンスへのログオン*, 37 ページを参照してください。

アプライアンスの登録

新しい アプライアンスを登録するには、以下の手順を実行します。

1. **[Register Appliance（アプライアンスの登録）]** をクリックします。
2. アプライアンス上のネットワーク インターフェース C の IP アドレスを入力します。
3. この TRITON コンソールからアプライアンスへのシングル サインオンを設定するには、**[Enable single sign-on from the TRITON console（TRITON コンソールからのシングル サインオンを有効にする）]** をオンにします。
4. アプライアンスへのアクセスのための管理者パスワードを入力します。
5. このアプライアンスに対するシングル サインオン許可を持っている TRITON 管理者を指定し、**[User Permissions（ユーザー許可）]** をクリックします。
6. 管理者にシングル サインオン許可を付与するために、利用可能ユーザーのリストの中のユーザー名のチェックボックスをオンにし、次に右向き矢印（>）をクリックして、管理者をアクセス リストの中の Users に追加します。

   ご注意
   グローバル セキュリティ管理者とアプライアンスへの完全なアクセス権限を持っている管理者は、アクセス リストの中の Users でグレイ表示されます。なぜなら、デフォルトでシングル サインオン アクセスを許可されており、それを変更できないからです。

7. **[Save]** をクリックします。

   正常に完了した場合、アプライアンスが TRITON コンソールに追加されたことを確認する [Appliance Details（アプライアンス詳細）] ポップアップが表示され、アプライアンスから取得される情報が表示されます。

   アプライアンスをシングル サインオンに設定できるのは、1 つの TRITON Management Server からのみです。別の TRITON インスタンスがすでにアプライアンスに対するシングル サインオンを登録している場合、エラー メッセージが表示されます。**[Transfer registration（登録の転送）]** をクリックして、ご使用の TRITON コンソールにシングル サインオンを転送するか、または **[Register without Single Sign-On（シングル サイン**

オンなしで登録)] をクリックしてそのアプライアンスを登録し、他の TRITON Management Server 上のシングル サインオン設定をそのままにしておきます。

8. さらにアプライアンスを追加するには、[**Add Another Appliance (別のアプライアンスの追加)**] をクリックし、上記のステップ 2 ～ 7 を繰り返します。アプライアンスの追加が完了したとき、[**Done (完了)**] をクリックします。

TRITON コンソールがユーザーによって入力された IP アドレスに接続できない場合は、以下のことを確認してください。

- The IP address you entered is the correct one for the appliance?s C interface
- アプライアンスとアプライアンス マネージャの両方が実行していること
- TRITON コンソール コンピュータ上のシステム クロックとアプライアンス上のクロックの差が 1 分未満であること

アプライアンスの情報を更新するには、アプライアンス情報を展開し、[**Refresh Details (詳細の更新)**] をクリックします。このページのすべてのアプライアンス情報を更新するには、[**Refresh All Appliances (すべてのアプライアンスの更新)**] をクリックします。

アプライアンスをリストから削除するには、アプライアンス情報を展開し、[**Unregister (登録削除)**] をクリックし、次に、確認のために [**Yes (はい)**] をクリックします。

アプライアンスの詳細の編集

アプライアンスの IP アドレスを編集するには、以下の手順を実行します。

1. 現在のアプライアンス IP アドレスの横の矢印をクリックして、アプライアンス情報を展開します。
2. 現在の IP アドレスの右側のアイコンをクリックします。
3. アプライアンス上のネットワーク インターフェース C の新しい IP アドレスを入力します。
4. [**Save**] をクリックします。

TRITON コンソールがユーザーによって入力された IP アドレスに接続できない場合は、以下のことを確認してください。

- 入力した IP アドレスがアプライアンスの C インターフェースに対応していること
- アプライアンスとアプライアンス マネージャの両方が実行していること
- TRITON コンソール コンピュータ上のシステム クロックとアプライアンス上のクロックの差が 1 分未満であること

シングル サインオンでアプライアンスにアクセスできる管理者のリストを変更するには、以下の手順を実行します。

1. 現在のアプライアンス IP アドレスの横の矢印をクリックして、アプライアンス情報を展開します。
2. アプライアンス情報ペインの右上隅の「シングル サインオン ユーザー許可の編集」アイコンをクリックします。
3. 管理者にシングル サインオン許可を付与するために、利用可能ユーザーのリストの中のユーザー名のチェックボックスをオンにし、次に右向き矢印 (>) をクリックして、管理者をアクセス リストの中の Users に追加します。
4. 管理者からシングル サインオン許可を除去するために、アクセス リストの中の Users のユーザー名の横のチェックボックスをオンにし、次に右向き矢印 (<) をクリックして、管理者を利用可能なユーザーのリストに追加します。

ご注意
グローバル セキュリティ管理者とアプライアンスへの完全なアクセス権限を持っている管理者は、アクセス リストの中の Users でグレイ表示されます。なぜなら、デフォルトでシングル サインオン アクセスを許可されており、それを変更できないからです。

5. **[Save]** をクリックします。

既存のアプライアンスをシングル サインオンに設定する

1. 編集するアプライアンスについて **[Configure single sign-on (シングル サインオンの構成)]** をクリックします。
2. **[Enable single sign-on from the TRITON console]** をオンにします。
3. アプライアンスへのアクセスのための管理者パスワードを入力します。
4. このアプライアンスに対するシングル サインオン許可を持っている TRITON 管理者を指定し、**[User Permissions (ユーザー許可)]** をクリックします。
5. 管理者にシングル サインオン許可を付与するために、利用可能ユーザーのリストの中のユーザー名のチェックボックスをオンにし、次に右向き矢印 (>) をクリックして、管理者をアクセス リストの中の Users に追加します。

ご注意
グローバル セキュリティ管理者とアプライアンスへの完全なアクセス権限を持っている管理者は、アクセス リストの中の Users でグレイ表示されます。なぜなら、デフォルトでシングル サインオン アクセスを許可されており、それを変更できないからです。

6. **[Save]** をクリックします。

アプライアンスをシングル サインオンに設定できるのは、1 つの TRITON Management Server からのみです。別の TRITON インスタンスがすでにアプライアンスに対するシングル サインオンを登録している場合、エラー メッセージが表示されます。**[Transfer registration (登録の転送)]** をクリックして、ご使用の TRITON コンソールにシングル サインオンを転送するか、または **[Register without Single Sign-On (シングル サインオンなしで登録)]** をクリックしてそのアプライアンスを登録し、他の TRITON Management Server 上のシングル サインオン設定をそのままにしておきます。

アプライアンスへのログオン

この TRITON コンソールからのシングル サインオンが設定されていないアプライアンスについては、そのアプライアンスの IP アドレスをクリックして、新しいブラウザでログオン ページを開きます。

4 TRITON データのバックアップと復元

TRITON Unified Security Center の設定とシステム データを TRITON Management Server コンピュータ上でバックアップし、必要に応じて前の設定に戻すことができます。バックアップ プロセスにより保存されたデータを使用して、アップグレード後に Websense 設定情報をインポートすることができ、また、設定情報を別の TRITON Management Server コンピュータに転送することもできます。

重要
設定をバックアップまたは復元する前に、すべての管理者が TRITON Unified Security Center からログオフしていることを確認してください。

バックアップ プロセスでは、下記の情報を保存します。

- TRITON Settings Database に保存されているグローバル設定およびインフラストラクチャ情報（管理者データおよびアプライアンス データを含む）。
- TRITON ブラウザ コンポーネントへのアクセスのために必要な証明書ファイル。

バックアップ プロセスでは、下記の処理を実行します。

1. 即時バックアップを開始するか（*即時バックアップの実行*, 41 ページを参照してください）、またはバックアップ スケジュールを定義します（*TRITON インフラストラクチャ バックアップのスケジューリング*, 40 ページ を参照してください）。
   - バックアップはいつでも手動で開始できます。
   - デフォルトではバックアップ ファイルは **C:¥EIPBackup** ディレクトリに保存されます。バックアップ ファイルの場所を変更するには、*バックアップ設定の変更*, 42 ページを参照してください。
2. バックアップ プロセスは、コンピュータ上のすべての Websense コンポーネントをチェックし、バックアップするデータを収集し、EIPBackup ディレクトリに下記の形式の新しいフォルダを作成します。

   ```
   mm-dd-yyyy-hh-mm-ss-PP
   ```

   このフォーマットはバックアップの日付と時刻を表します。以下はその例です。

```
02-10-2011-10-45-30-PM
```

各バックアップ フォルダにはいくつかのファイルが入っています。以下はその例です。

- EIP.db: 標準 PostgreSQL バックアップ ファイル。
- httpd-data.txt: 埋め込みの証明書情報と暗号化キーが入っています。
- backup.txt: バックアップが正常に終了した場合に作成されます。
- DataBackup.log: バックアップ中に生成された情報を含む詳細ログ ファイルです。

These files should be part of your organization?s regular backup procedures.

バックアップが正常に完了したことを確認するには、**C:¥Program Files (X86)¥Websense¥EIP Infra** ディレクトリに移動し、Notepad などのテキスト エディタで **EIPBackup.log** ファイルを開きます。ログ情報は以下のようになっているはずです。

```
2/15/2011 2:27:42 AM --- Backing up to:C:\EIPBackup\2-15-2011-2-27-42-AM
2/15/2011 2:27:42 AM --- Backing Up Certificates ...
2/15/2011 2:27:42 AM --- Backing Up PostgreSQL ...
2/15/2011 2:27:42 AM *** BACKUP FINISHED ***
```

各 TRITON モジュールには、そのモジュール システム設定のための独自のバックアップおよび復元プロセスがあります。

- TRITON – Data Security については、TRITON – Data Security Help 中の システムのバックアップ を参照してください。
- TRITON – Email Security については、TRITON – Email Security ヘルプ中の管理サーバー設定のバックアップと復元 を参照してください。
- TRITON – Web Security については、TRITON – Web Security ヘルプの Websense データのバックアップと復元 を参照してください。.

TRITON – Web Security バックアップと同時に TRITON インフラストラクチャ バックアップを実行することをお勧めします。*TRITON インフラストラクチャと TRITON – Web Security のバックアップの同期化*, 44 ページを参照してください。

TRITON インフラストラクチャ バックアップのスケジューリング

TRITON Unified Security Center のインストール時に、バックアップのためのスケジュール設定されたタスクが作成されています。デフォルトでは、このタスクは無効化されています。

Websense 管理者にバックアップ スケジュールを通知することによって、管理者がバックアップ プロセス中に TRITON Unified Security Center からログオフしているように指示します。

すべてのバックアップは「ホット」であり、システム動作を妨げません。しかし、バックアップはシステムの負荷が大きくない時間帯にスケジュール設定しておくことを推奨します。

Windows Server 2008 上でバックアップをスケジュールするには、以下の手順を実行します。

1. TRITON Management Server 上で「**Start**」>「**Administrative Tools**」>「**Task Scheduler**」へ移動します。
2. [Task Scheduler] ウィンドウで **[Task Scheduler Library]** を選択します。
3. **[Triton Backup (TRITON バックアップ)]** タスクを右クリックし、**[Enable (有効化)]** を選択します。
4. もう一度 **[Triton Backup]** を右クリックし、**[Properties (プロパティ)]** 選択します。
5. **[Triggers (トリガ)]** タブを選択します。
6. **[Edit (編集)]** をクリックし、スケジュールを適切に編集します。デフォルトでは、このタスクは毎週土曜日深夜 (24 時) に実行するように設定されています。
7. **[OK]** を 2 度クリックします。
8. 要求された場合、TRITON Management Server コンピュータにアクセスするための管理者パスワードを入力し、タスクの変更を確認してください。

即時バックアップの実行

手動バックアップを実行する前に、すべての管理者が TRITON Unified Security Center からログアウトしていることを確認します。

即時バックアップを起動するには、以下の手順を実行します。

1. TRITON Management Server 上で「**Start**」>「**Administrative Tools**」>「**Task Scheduler**」へ移動します。
2. [Task Scheduler] ウィンドウで **[Task Scheduler Library]** を選択します。
3. **[Triton Backup]** タスクが無効化されている場合、このタスクを右クリックして **[Enable]** を選択します。
4. **[Triton Backup]** タスクを右クリックし、**[Run (実行)]** を選択します。

TRITON インフラストラクチャ バックアップ データの復元

TRITON Infrastructure Modify ウィザードから復元動作を開始できます。すべての管理者が TRITON Unified Security Center からログオフしていることを確認します。

復元プロセスを開始する前に TRITON Unified Security Center サービスを停止することをお勧めします。

TRITON インフラストラクチャ データを復元するには、以下の手順を実行します。

1. TRITON Management Server 上で「 **Start** 」>「 **Administrative Tools** 」>「 **Services (サービス)** 」へ移動します。
2. **[Websense TRITON Unified Security Center]** サービスを右クリックして、**[Stop]** を選択します。
3. Windows の［コントロール パネル］を開き、**[プログラム]**>**[プログラムと機能]** を選択します。
4. **[Websense TRITON Infrastructure]** を選択します。
5. **[アンインストールと変更]** をクリックします。
6. TRITON Infrastructure の追加、削除または変更を選択するよう求められたとき、**[変更]** を選択します。
7. **[Restore Data from Backup (バックアップからデータの復元)]** 画面が表示されるまで **[Next (次へ)]** をクリックします。
8. **[Use backup data (バックアップ データの使用)]** を選択し、次に **[Browse (参照)]** をクリックして、バックアップ フォルダを見つけます。
9. 復元プロセスが開始するまで **[Next]** をクリックします。
10. **[Finish (終了)]** をクリックして、復元ウィザードを終了します。
11. Services ウィンドウに戻り、**[Refresh]** をクリックします。Websense TRITON Unified Security Center サービスが再起動しない場合は、**[Start]** をクリックします。

復元プロセスが完了すると、復元のために使用された日付スタンプのバックアップ フォルダに **DataRestore.log** という名前のファイルが作成されます。

バックアップ設定の変更

初めてバックアップを実行するとき、それぞれのバックアップ ファイルのセットを保存するための日付スタンプ フォルダを格納する **EIPBackup** ディレクトリが作成されます。デフォルトでは、このディレクトリは C:¥ に作成されます。この場所を変更することができ、また、バックアップ ディレクトリに何回分のバックアップを保存するかを指定することができます。

バックアップ ファイルに関する設定を変更するには、以下の手順を実行します:

1. TRITON Management Server 上で **C:¥Program Files (X86)¥Websense¥EIP Infra** ディレクトリに移動します。
2. Notepad などのテキスト エディタで **EIPBackup.xml** を開きます。.

   このファイルは以下のようなパラメータが含まれます。

パラメータ	説明
NUM_OF_COPIES	バックアップ ディレクトリに格納されるバックアップの世代数。デフォルトは 5 です。
PATH	EIPBackup ディレクトリを保存する場所。デフォルトは C:¥ です。
DOMAIN	これは <PATH> パラメータがリモート コンピュータにアクセスするように設定されていて、その場所への書き込みアクセスのために domain¥user の形式の資格証明書を提供しなければならない場合にのみ必要とされます。パスがローカル コンピュータ上に設定されているか、または <USER_NAME> で資格証明書を入力した場合は、このフィールドを空白にしておきます。
USER_NAME	これは <PATH> パラメータがリモート コンピュータにアクセスするように設定されていて、その場所への書き込みアクセスのためにユーザー名を入力しなければならない場合にのみ必要とされます。パスがローカル コンピュータ上に設定されているか、または <DOMAIN> で資格証明書を入力した場合は、このフィールドを空白にしておきます。
PASSWORD	これは <PATH> パラメータがリモート コンピュータにアクセスするように設定されていて、<DOMAIN> または <USER_NAME> で資格証明書を入力した場合にのみ必要とされます。パスワードはプレーン テキストとして格納されます。

3. <NUM_OF_COPIES> パラメータを編集して、保存するバックアップの世代数を指定します。この数に到達したあと、次のバックアップを実行するとき、最も古いバックアップが削除されます。
4. <PATH> パラメータを編集して、バックアップ ファイルを保存する場所を設定します。この場所はバックアップ プロセスでは作成されませんから、事前に作成しておく必要があります。たとえば、このパラメータを TRITON Management Server コンピュータ上の下記の場所に設定します。

   ```
   <PATH>D:\TRITON\Backups</PATH>
   ```

   この場合、バックアップ ファイルは D:¥TRITON¥Backups¥EIPBackup に格納されます。

   また、下記のように、ネットワーク上の別のコンピュータ上の場所に設定することもできます。

   ```
   <PATH>//server01/backups</PATH>
   ```

この場合には、<USER_NAME>、<DOMAIN> または <PASSWORD> パラメータでリモート コンピュータへのアクセスのための資格証明書を入力しなければならない場合があります。この方法はお勧めできません。なぜなら、パスワードがプレーン テキストとして格納され、他のユーザーによるアクセスが可能になるからです。代わりに、資格証明書なしで書き込みアクセスを許可されている場所にバックアップを格納することをお勧めします。

ご注意
バックアップ ファイルの場所を変更した場合、古いバックアップ ファイルは新しい場所からのみ削除されます。前に設定されていた場所のバックアップ ファイルの管理は手動で行ってください。

5. 変更が完了したとき、ファイルを保存します。変更は次回のバックアップ実行時から有効になります。

TRITON インフラストラクチャと TRITON – Web Security のバックアップの同期化

TRITON – Web Security モジュールを使用している場合、管理者情報(許可、およびローカル管理者のパスワードを含む)は TRITON Settings Database と TRITON – Web Security Policy Database の両方に格納されます。これは「**TRITON Settings**」>「**Administrators**」ページで定義されている管理者に対して、TRITON – Web Security でロールを割り当てることができ、ロール内で異なる権限を割り当てることができるからです。

この情報の同期を確保するために、TRITON – Web Security と TRITON インフラストラクチャは必ず同時にバックアップし、同時に復元してください。このセクションでは先に TRITON インフラストラクチャのバックアップを実行し、次に TRITON – Web Security のバックアップを実行しますが、両方のバックアップ中に TRITON Unified Security Center で変更が行われないかぎり、バックアップの順序はどちらでもかまいません。

TRITON – Web Security と TRITON Infrastructure のバックアップを手動で同時に実行するには、以下の手順を実行します:

1. *即時バックアップの実行*, 41 ページ の指示に従います。
2. コマンド プロンプトを開き、Websense **bin** ディレクトリ(デフォルトでは C:¥Program Files (X86)¥Websense¥Web Security¥bin) に移動します。
3. 次のコマンドを入力します:

   ```
   wsbackup -b -d <directory>
   ```

   この場合、*directory* は TRITON – Web Security バックアップ アーカイブの保存先ディレクトリです。

TRITON – Web Security と TRITON Infrastructure の同時バックアップのスケジュールを設定するには、バックアップが常に同時に行われるようにスケジュール時刻と頻度を設定します。*TRITON インフラストラクチャ バックアップのスケジューリング*, 40 ページ の指示に従い、次に TRITON – Web Security Help の？バックアップのスケジューリング？を参照してください。

TRITON – Web Security と TRITON Infrastructure を同時に復元するには、以下の手順を実行します。

1. TRITON Management Server 上で「 **Start** 」>「 **Administrative Tools** 」>「 **Services（サービス）** 」へ移動します。
2. **[Websense TRITON Unified Security Center]** サービスを右クリックして、**[Stop]** を選択します。
3. **[Websense TRITON – Web Security]** サービスを右クリックして、**Stop** を選択します。
4. *TRITON インフラストラクチャ バックアップ データの復元*, 42 ページの TRITON Infrastructure 復元プロセスに従います。
5. TRITON – Web Security ヘルプの ?Websense データの復元？の説明に従って、バックアップ ユーティリティを復元モードで実行します。指定するバックアップ ファイルの日付が TRITON インフラストラクチャ バックアップ ファイルの日付と同じであることを確認してください。
6. Services ウィンドウに戻り、**[Refresh]** をクリックします。TRITON – Web Security サービスが再起動しない場合は、**[Start]** をクリックします。

索引