システムアクセスとセキュリティの管理

ここでは、次の内容について説明します。

証明書の管理

証明書とは

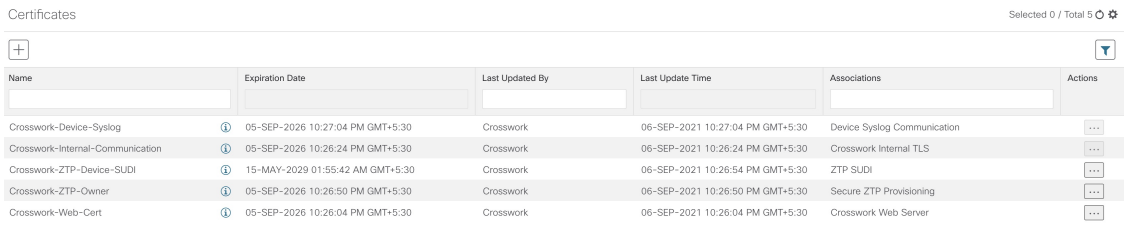
証明書は、個人、サーバー、会社、または別のエンティティを識別し、そのエンティティを公開キーに関連付ける電子文書です。公開キーを使用して証明書を作成すると、一致する秘密キーも生成されます。TLS では、公開キーはエンティティに送信されるデータの暗号化に使用され、秘密キーは復号に使用されます。証明書は、発行者または「親」証明書（認証局）によって、つまり、親の秘密キーによって署名されます。証明書は自己署名することもできます。TLS の交換では、証明書の発行者の有効性を確認するために証明書の階層が使用されます。この階層は信頼チェーンと呼ばれ、ルート CA 証明書（自己署名）、場合によっては複数レベルの中間 CA 証明書、およびサーバー（またはクライアント）証明書（エンドエンティティ）の 3 つのタイプで構成されます。中間証明書は、サーバー証明書を CA のルート証明書にリンクし、追加のセキュリティ層を提供する「信頼のリンク」として機能します。ルート証明書の秘密キーから開始し、信頼チェーン内の各証明書の秘密キーは、最終エンティティ証明書に最終的に署名するまで、チェーン内の次の証明書に署名して発行します。エンドエンティティ証明書は、チェーン内の最後の証明書であり、クライアント証明書またはサーバー証明書として使用されます。これらのプロトコルの詳細については、「X.509 証明書 （43 ページ）」と「HTTPS （43 ページ）」を参照してください。

Crosswork での証明書の使用方法

Crosswork アプリケーションとデバイス間の通信やさまざまな Crosswork コンポーネント間の通信は、TLS プロトコルを使用して保護されます。TLS は X.509 証明書を使用して安全にデバイスを認証し、データを暗号化して送信元から接続先までその整合性を確保します。Crosswork は、生成された証明書とクライアントがアップロードした証明書を組み合わせて使用します。アップロードされた証明書は、認証局（CA）から購入するか、自己署名することができます。たとえば、Cisco Crosswork VM がホストする Web サーバーとクライアントブラウザベースのユーザーインターフェイスは、TLS 経由で交換される Crosswork によって生成された X.509 証明書を使用して相互に通信します。

Crosswork Cert Manager は、分散フレームワーク内の複数のマイクロサービスおよびサービスのプロキシであり、すべての Crosswork 証明書を管理します。証明書管理 の UI（**[管理（Administration）] > [証明書管理（Certificate Management）]**）を使用すると、証明書を表示、アップロード、および変更できます。次の図に、Cisco Crosswork が提供するデフォルトの証明書を示します。

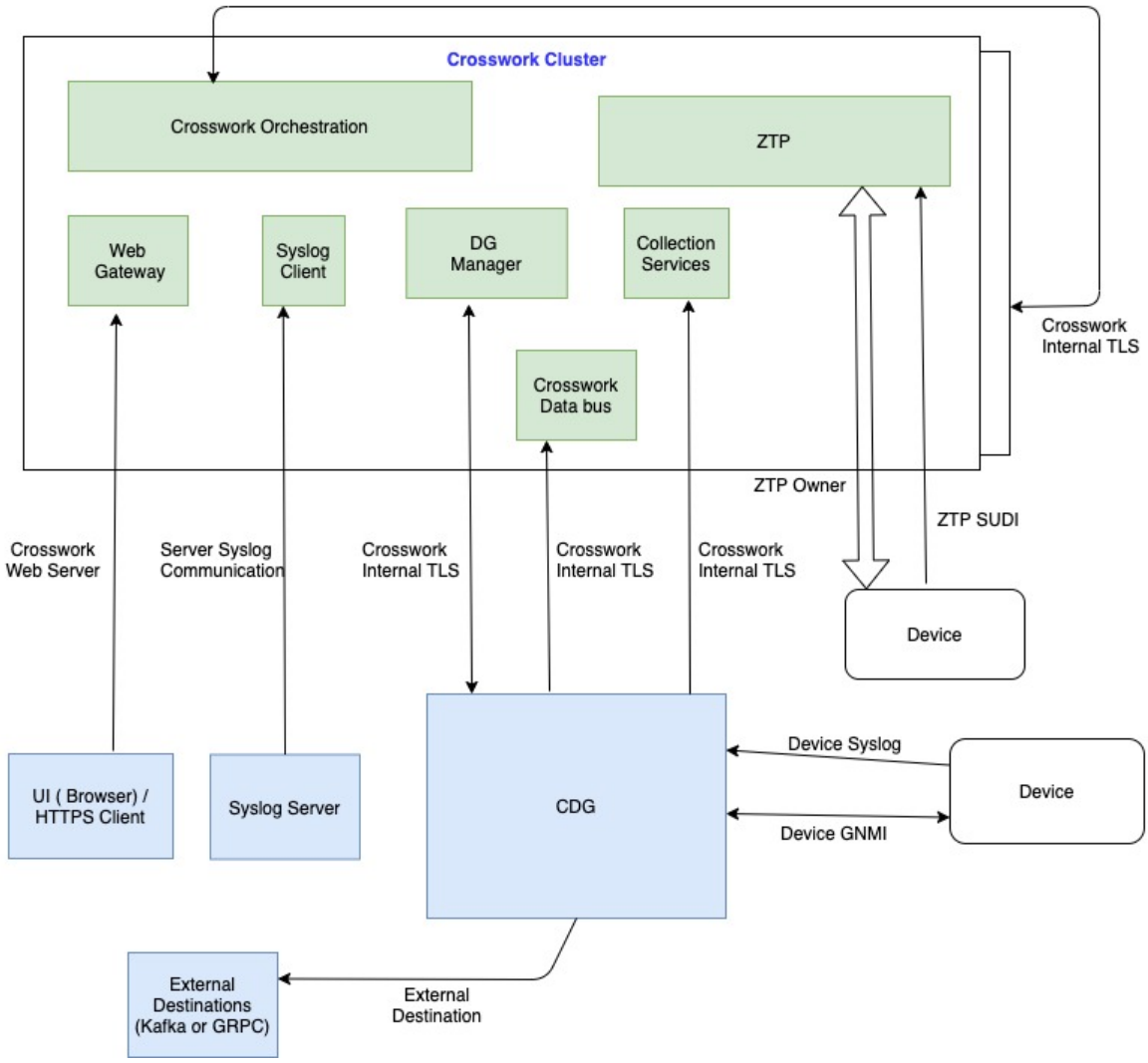
図 *1:* 証明書管理の *UI*



証明書のタイプと使用方法

次の図に、Crosswork がさまざまな通信チャネルで証明書を使用する方法を示します。

図 *2 : Cisco Crosswork* の証明書



これらの証明書は、次の表に示すように、使用例に応じて異なるプロパティを持つさまざまなロールに分類されます。

ロール	UI 名	説明	サーバー	クライアント	許可される操作	デフォルトの有効期限	許可される有効期限
Crosswork（CW）内部 TLS	CW 内部通信（CW- Internal-Communication）	• Crosswork によって生成および提供されます。 • この信頼チェーンは、UI（サーバーとクライアントリーフ証明書を含む）で使用でき、初期化時に Crosswork によって作成されます。これらは、Crosswork と CDG 間のプロセス間通信と内部 Crosswork コンポーネント間の通信に使用されます。 • 相互認証とサーバー認証を許可します。	CW	• CDG • CW	ダウンロード	5 年	—
CW Web サーバー	CW Web 証明書（CW-Web-Certificate） サーバー認証	• Crosswork によって生成および提供されます。 • ユーザーブラウザと Crosswork 間の通信を提供します。 • サーバー認証を許可します。	CW Web サーバー	ユーザーブラウザまたは API クライアント	• アップロード • ダウンロード	5 年	30 日 ～ 5 年

ロール	UI 名	説明	サーバー	クライアント	許可される操作	デフォルトの有効期限	許可される有効期限
ZTP SUDI	CW ZTP デバイスの SUDI（CW-ZTP-Device-SUDI）	• Crosswork の一部として提供される公開シスコ証明書。 • ZTP アプリケーションとデバイス間の ZTP プロトコル通信チャネルを提供します。 • サーバー認証を許可します。	CW ZTP	Device	• アップロード • ダウンロード	100 日	30 日 ～ ユーザー定義
セキュア ZTP プロビジョニング	CW ZTP 所有者（CW-ZTP-Owner）	• Crosswork によって生成および提供されます。 • ZTP によってデバイスに転送され、暗号化の第 2 層に使用されます。	CW ZTP	Device	• アップロード • ダウンロード	5	30 日 ～ ユーザー定義
デバイスの Syslog	CW デバイスの Syslog（CW-Device-Syslog）	• Crosswork によって生成および提供されます。 • デバイスと CDG 間の Syslog テレメトリ通信を提供します。 • サーバー認証を許可します。	CDG	Device	ダウンロード	5 年	—

ロール	UI 名	説明	サーバー	クライアント	許可される操作	デフォルトの有効期限	許可される有効期限
デバイス gNMI 通信	—	デバイスと CDG 間の GNMI テレメトリ通信を提供します。	CDG	Device	• アップロード • ダウンロード	N/A	30 日 ～ ユーザー定義
サーバーの Syslog	N/A	• Crosswork から外部 Syslog サーバーへの syslog イベントとログを許可します。 • サーバー認証を許可します。	外部 Syslog サーバー	Crosswork	• アップロード （注） 異なるサーバーに関連付けられた複数の証明書をアップロードできます。 • ダウンロード	—	30 ～ ユーザー定義

ロール	UI 名	説明	サーバー	クライアント	許可される操作	デフォルトの有効期限	許可される有効期限
外部接続先	—	CDG から外部接続先（Kafka または GRPC）にテレメトリデータをエクスポートします。	外部接続先（Kafka または GRPC）	CDG	• アップロード （注） • ダウンロード	— 異なる接続先に関連付けられた複数の証明書をアップロードできます。	30 ～ ユーザー定義

Crosswork には 2 つのカテゴリロールがあります。

- 信頼チェーンのみをアップロードまたはダウンロードできるロール
- 信頼チェーンと中間証明書およびキーの両方のアップロードまたはダウンロードを許可するロール

新しい証明書の追加

次のロールの証明書を追加できます。

- [外部接続先（External Destination）]：このロール用にアップロードした証明書は、CDG と外部接続先（Kafka サーバーなど）間の通信を保護するために使用されます。相互認証を有効にするには、CDG と外部サーバーの両方に共通する **CA 証明書信頼チェーン**をアップロードします。この信頼チェーンには、ルート CA 証明書と任意の数のオプションの中間 CA 証明書が含まれています。チェーンの最後の中間証明書とそれに対応する秘密キーは、**中間キー**、**中間証明書**、およびオプションで**パスフレーズ**（中間キーの生成に使用した場合）を使用して UI に個別にアップロードされます。Crosswork は、外部接続先に接続する CDG のこの中間キーを使用して、クライアント証明書を内部的に作成します。接続先（Kafka など）のサーバー証明書の信頼は、同じルート CA 証明書から取得する必要があります。
- [Syslogサーバー通信（Syslog Server Communication）]：ユーザーは Syslog サーバー証明書の信頼チェーンをアップロードします。この信頼チェーンは、Syslog サーバーを認証するために Crosswork で使用されます。この信頼チェーンがアップロードされ、Crosswork 内に伝達されると、ユーザーは syslog サーバーを追加して（**[管理（Administration）]** > **[設定（Settings）]** > **[Syslog サーバー設定（Syslog Server Configuration）]**）、証明書を関連付けて TLS を有効にできます。詳細については、「Syslog サーバーの設定 （47 ページ）」を参照してください。
- [デバイスgNMI通信（Devices gNMI communication）]：ユーザーは、接続しているデバイスを認証するために CDG で使用される信頼チェーンのバンドルをアップロードします。この信頼チェーンとデバイス gNMI 証明書もデバイスで設定する必要があります。アップロードする信頼チェーンファイルには、ネットワーク内のすべてのデバイスが接続できるように、必要に応じて信頼証明書の階層を複数含めることができます。詳細については、「gNMI 証明書の設定」を参照してください。
- [セキュアLDAP通信（Secure LDAP Communication）]：ユーザーは、セキュア LDAP 証明書の信頼チェーンをアップロードします。この信頼チェーンは、LDAP サーバーを認証するために Crosswork で使用されます。この信頼チェーンがアップロードされて Crosswork 内に伝播されると、ユーザーは LDAP サーバーを追加し（LDAP サーバーの管理 （40 ページ） を参照）、証明書を関連付けることができます。

（注） Cisco Crosswork は、Web 証明書を直接受信しません。中間 CA と中間キーを受け入れて新しい Web 証明書を作成し、Web ゲートウェイに適用します。

（Cisco Crosswork 内で提供されるデフォルトの証明書を使用する代わりに）独自の ZTP（ゼロタッチプロビジョニングの概念）と Web 証明書をアップロードする場合は、[編集（Edit）] 機能を使用します（「証明書の編集」を参照）。

始める前に

- 証明書のタイプと使用方法については、「証明書のタイプと使用方法 （2 ページ）」を参照してください。
- アップロードするすべての証明書がプライバシー強化メール（PEM）形式である必要があります。簡単に移動できるように、これらの証明書がシステム内のどこにあるかに注意してください。
- アップロードする信頼チェーンファイルには同じファイル内の階層全体（ルート CA と中間証明書）が含まれている場合があります。場合によっては、同じファイルで複数のチェーンを使用することもできます。
- 中間キーは、PKCS1 形式または PKCS8 形式である必要があります。
- 外部接続先の新しい証明書を追加する前に、データ送信先を設定する必要があります。詳細については、「データ宛先の追加または編集」を参照してください。

ステップ 1 メインメニューから **[管理（Administration）] > [証明書管理（Certificate Management）]** を選択し、＋をクリックします。

ステップ 2 署名書の一意の名前を入力します。

ステップ 3 [証明書のロール（Certificate Role）] ドロップダウンメニューから、証明書を使用する目的を選択します。詳細については、「証明書の管理 （1 ページ）」を参照してください。

ステップ 4 [参照（Browse）] をクリックして証明書の信頼チェーンに移動します。

ステップ 5 外部接続先証明書の場合は、1 つ以上の接続先を選択し、CA 証明書の信頼チェーン、中間証明書、および中間キーを指定する必要があります。パスフレーズフィールドはオプションで、中間キーの作成に使用されます（該当する場合）。

ステップ 6 [保存（Save）] をクリックします。

（注） アップロードされると、Crosswork 証明書マネージャはサーバー証明書を受け入れ、検証し、生成します。検証が成功すると、アラーム（「Crosswork Web サーバーの再起動（Crosswork Web Server Restart）」）によって証明書が適用されようとしていることが示されます。証明書管理 UI は自動的にログアウトし、証明書を Web ゲートウェイに適用します。新しい証明書を確認するには、https://<crosswork_ip>:30603 の横にあるロック <Not Secure>/<secure> アイコンをクリックします。

証明書の編集

証明書を編集して、接続先を追加または削除したり、期限切れまたは誤って設定された証明書をアップロードおよび置換したりできます。ユーザー指定の証明書と、ZTP および Web 証明書を編集できます。Cisco Crosswork が提供するその他のシステム証明書は変更できず、選択できません。

また、この手順に従って証明書を「削除」して証明書を置き換えるか、または割り当てられた接続先のセキュリティを無効にする（[セキュアな通信を有効にする（Enable Secure Communication）] オプションを無効にする）こともできます（「データ宛先の追加または編集」を参照）。Cisco Crosswork システムからの証明書の永続的な削除はサポートされていません。

（注） ZTP 証明書については、「ZTP アセットの組み立てと読み込み」を参照してください。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[証明書管理（Certificate Management）]** を選択し、変更する証明書を確認します。

ステップ 2 変更する証明書で … をクリックし、[証明書の更新（Update Certificate）] を選択します。

ステップ 3 必要なオプションを更新します。

（注） CW Web サーバー証明書の更新時に、次のフィールドに関連する値を入力します。

- [Crosswork Web CA]：ルート CA 証明書と中間証明書を 1 つ以上含むか、まったく含んでいない信頼チェーンファイル（PEM 形式）。
- [Crosswork Web 中間（Crosswork Web Intermediate）]：ルート CA 証明書で署名された中間 CA 証明書。
- [Crosswork Web 中間キー（Crosswork Web Intermediate Key）]：中間 CA 証明書に関連付けられているキー。
- [Crosswork Web パスフレーズ（Crosswork Web Passphrase）]：これはオプションのフィールドです。

検証が成功すると、証明書管理 UI が自動的にログアウトし、Web ゲートウェイに証明書を適用します。

ステップ 4 [保存（Save）] をクリックします。

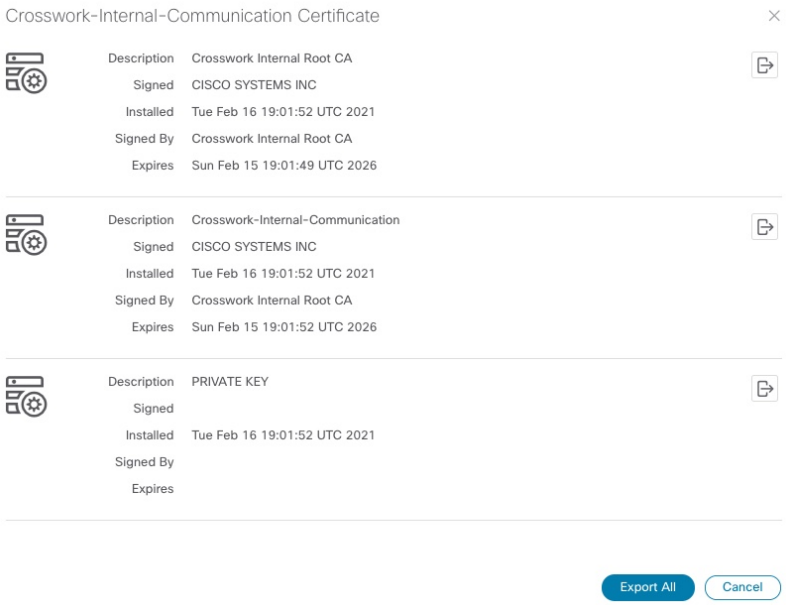
証明書のダウンロード

証明書をエクスポートするには、次の手順を実行します。

ステップ 1 メインメニューから **[管理（Administration）]** > **[証明書管理（Certificate Management）]** を選択します。

ステップ 2 ダウンロードする証明書の ⓘ をクリックします。

図 *3*:証明書のエクスポート



ステップ 3 ルート証明書、中間証明書、および秘密キーを個別にダウンロードするには、をクリックします。証明書と秘密キーすべてを一度にダウンロードするには、[すべてエクスポート（Export All）] をクリックします。

証明書の更新

証明書は、有効期限が切れるまで1年間有効です。以下の手順は、クラスタ内の各ノード（ハイブリッドとワーカー）で順番に実行する必要があります。1 つのノードで証明書を更新したら、次のノードに進む前にポッドが正常であることを確認します。

（注） 有効期限が切れる前に証明書を更新する場合は、クラスタが動作状態にあるため、メンテナンスウィンドウ中にこのアクティビティを実行することをお勧めします。

証明書を更新するには、次の手順を実行します。

ステップ 1 ノードで、コマンドを実行して root ユーザーに移動します。

```
sudo -i
```

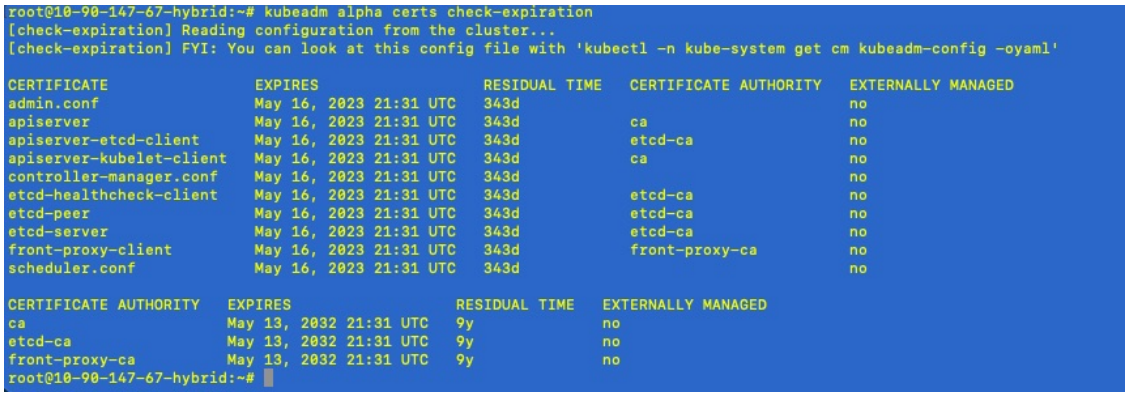
パスワードを入力するように求められます。`cw-admin` ユーザーパスワード。

ステップ 2 証明書の日付が期限切れになっているかどうかを確認します。

```
kubeadm alpha certs check-expiration
```

次の画像は、出力のサンプルです。

図 *4*:証明書の有効期限のサンプル出力



ステップ 3 証明書と conf ファイルのバックアップを作成します。

```
mkdir $HOME/Old-K8-Certs
mkdir $HOME/Old-K8-Certs/pki
cp -p /etc/kubernetes/pki/*.* $HOME/Old-K8-Certs/pki
cp -p /etc/kubernetes/*.conf $HOME/Old-K8-Certs
~#
```

ステップ 4 コマンドを実行して証明書を更新します。

```
kubeadm alpha certs renew all
```

ステップ 5 手順 2 を繰り返して、新しい証明書の作成を確認します。

ステップ 6 コマンドを実行して kubelet を再起動します。

```
systemctl stop kubelet
```

（注） 再起動はすべてのノードで発生し、更新された証明書は kubelet と kube-apiserver が再起動されるまで有効になりません。再起動時にアプリケーションからの操作を停止することをお勧めします。

kubelet を停止した後、次のプロセスを見つけます（ps -eaf | grep を使用）<process name>）：

```
kube-apiserver
controller-manager
kube-scheduler
```

それらを中止（kill -9 <pid>を使用）します。上記のプロセスを強制終了した後、以下を実行して kubelet を再起動します。

```
systemctl daemon-reload
systemctl start kubelet
```

ノードは最初に劣化状態に移行し、次にダウン状態に移行します。

（注） ノードがダウン状態に移行した後でも、syslog には引き続きトラフィックが表示される場合があります。

```
10-90-147-67-hybrid kernel: [1897091.695393] ll header: 00000000: ff ff ff ff ff ff fa
51 56 a2 9c 7c 08 0
10-90-147-67-hybrid kernel: [1897091.695414] IPv4: martian source 169.254.1.1 from
10.244.215.17, on dev calieff0340c649
10-90-147-67-hybrid kernel: [1897091.695416] ll header: 00000000: ff ff ff ff ff ff 72
e8 75 10 bb 64 08 06
```

ステップ 7 すべてのポッドが正常で実行されていることを確認します。

```
kubectl get pods -A -o wide
```

また、再起動したハイブリッドノードで実行中のポッドも検証します。

ステップ 8 証明書が更新されているかどうかを確認します。

ステップ 9 問題が引き続き発生する場合は、conf ファイルを変更します。

```
sudo kubeadm alpha kubeconfig user --org system:nodes --client-name system:node:$(hostname) >
/etc/kubernetes/kubelet.conf
```

クラスター内のノードごとに上記の手順を繰り返します。

ライセンスの管理

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンスモデルです。また、これは安全です。ユーザーがアクセスできるものを制御できます。スマートライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。PAK（製品アクティベーションキー）は不要です。
- **管理の統合**：My Cisco Entitlements（MCE）は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供するので、取得したもの、使用しているものを常に把握できます。
- **ライセンスの柔軟性**：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります（software.cisco.com）。**Cisco スマートアカウント**は、スマート対応製品のリポジトリを提供し、シスコライセンスの有効化、ライセンスの使用状況の監視、およびシスコ製品購入の追跡を可能にします。**Cisco Smart Software Manage（CSSM）**を使用すると、一元化された 1 つの Web サイトから Cisco スマートソフトウェアのすべてのライセンスを管理できます。Cisco Smart Software Manager では、ライセンスを管理するためにスマートアカウント内で複数のバーチャルアカウントを作成および管理できます。シスコライセンスの詳細については、cisco.com/go/licensingguide を参照してください。

メインメニューから **[管理（Administration）]** > **[スマートライセンスの登録（Smart Licensing Registration）]** を選択し、[スマート ソフトウェア ライセンス（Smart Software Licensing）] ウィンドウを表示します。このウィンドウを使用して、Cisco Crosswork アプリケーションの登録、トランスポート設定の編集、ライセンスの更新、アプリケーションの登録解除を行うことができます。

スマートライセンスの登録の前提条件

次が必要です。

- Cisco スマートアカウント。
- Cisco Crosswork アプリケーションの購入済みライセンス。

転送設定

トランスポート設定を構成して、Cisco Crosswork とシスコのサーバーとの通信方法を決定します。

- [直接（Direct）] : アプリケーションは Cisco Smart Software Manager（CSSM）に直接接続します。
- [トランスポートゲートウェイ（Transport Gateway）] : アプリケーションは、トランスポートゲートウェイ、またはクラウドベースのユーザーエクスペリエンスを複製してもオンプレミスのすべての通信を保持する CSSM オンプレミスオプションを介して通信します。

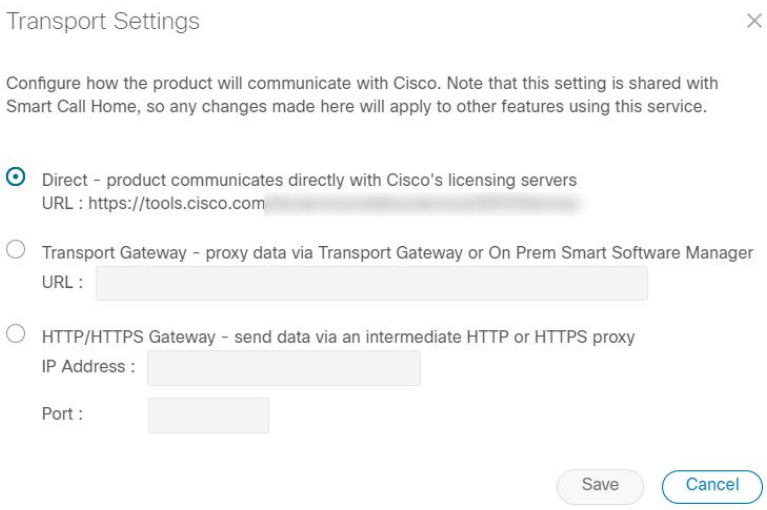
（注） CSSM オンプレミスオプションの詳細については、『Smart Software Manager guide』を参照してください。

- [HTTP/HTTPS ゲートウェイ（HTTP/HTTPS Gateway）] : アプリケーションは中間プロキシサーバーを介して接続します。これは、直接モードにのみ適用されます。

（注） トランスポート設定は、Cisco Crosswork が登録モードになっている間は変更できません。変更するには登録を解除する必要があります。

ステップ 1 [スマート ソフトウェア ライセンス（Smart Software Licensing）] ウィンドウの [トランスポート設定（Transport Settings）] に、現在選択されているトランスポートモードが表示されます。変更するには、[表示/編集（View/Edit）] をクリックします。

[トランスポート設定（Transport Settings）] ダイアログボックスが表示されます。



ステップ 2 関連するトランスポートモードを選択し、表示されたフィールドに関連するエントリを入力します。

ステップ 3 [保存（Save）] をクリックします。

Cisco Crosswork アプリケーションの登録

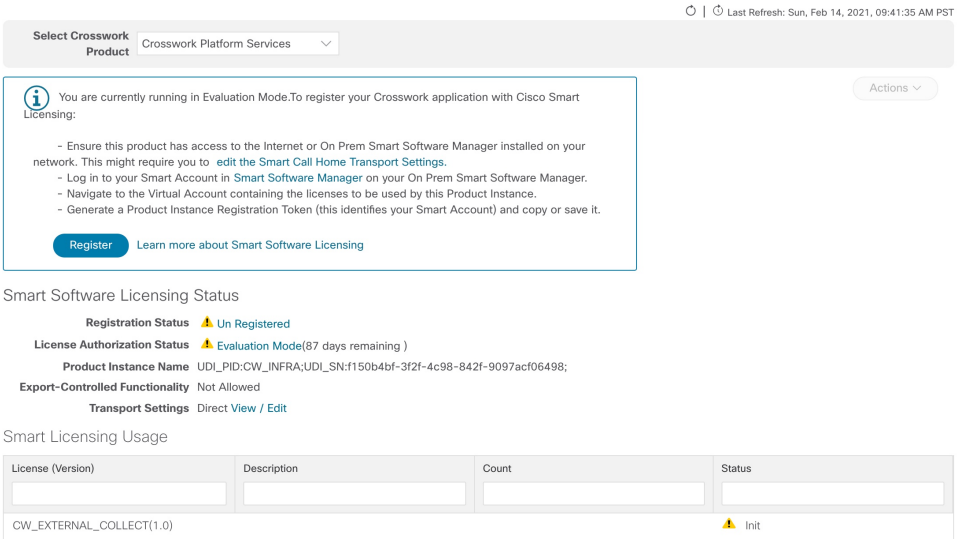
ライセンス機能を有効にするには、登録 ID トークンを使用して Cisco Crosswork アプリケーションを CSSM に登録する必要があります。登録されると、ID 証明書はスマートアカウントに安全に保存され、進行中のすべての通信に使用されます。証明書は 1 年間有効で、6 ヵ月後に自動的に更新されて継続的な運用が保証されます。

（注） 登録トークンの生成については、Smart Software Manager の Web ページで提供されているサポートリソースを参照してください。

ステップ 1 メインメニューから **[管理（Administration）]** > **[スマートライセンスの登録（Smart Licensing Registration）]** を選択し、[スマート ソフトウェア ライセンス（Smart Software Licensing）] ウィンドウを表示します。登録ステータス

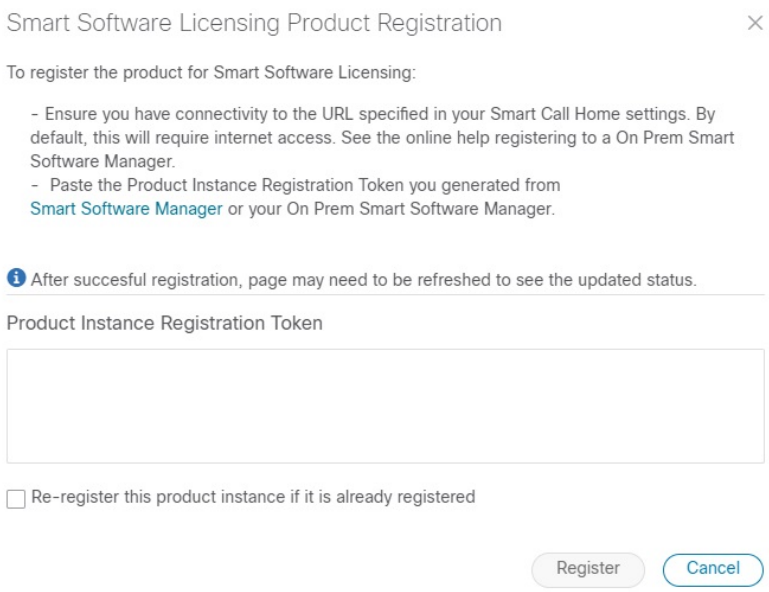
登録ステータスとライセンス認証ステータスは、それぞれ [未登録（Unregistered）] と [評価（Evaluation）] モードになります。

図 5: スマート ソフトウェア ライセンスの未登録の例



ステップ 2 [スマート ソフトウェア ライセンス（Smart Software Licensing）] ウィンドウで、[登録（Register）] をクリックします。

[スマート ソフトウェア ライセンス製品の登録（Smart Software Licensing Product Registration）] ダイアログボックスが表示されます。



ステップ 3 **[製品インスタンス登録トークン（Product Instance Registration Token）]** フィールドに、スマートアカウントから生成された登録トークンを入力します。トークン ID が正確で、有効期間内であることを確認してます。詳細については、「https://www.cisco.com/c/en_in/products/software/smart-accounts/software-licensing.html」を参照してください。

ステップ 4 （オプション）アプリケーションを再登録する場合は、[すでに登録されている場合はこの製品を再登録します（Re-register this product registration if is already registered）] チェックボックスをオンにします。

（注） バックアップ復元または災害後の復元操作の後、Cisco Crosswork VM を CSSM に手動で再登録する必要があります。これは、復元操作で使用されるバックアップの取得中にすでに登録されている Cisco Crosswork VM の場合に適用されます。

ステップ 5 [登録（Register）] をクリックします。登録の処理には数分かかる場合があります。成功すると、「製品登録が正常に完了しました（Product Registration completed successfully）」というメッセージが表示されます。

登録ステータスとライセンス認証ステータスは、それぞれ [登録済み（Registered）] と [承認済み（Authorized）] に更新されます。

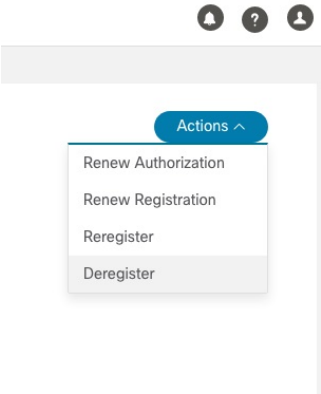
（注）
- 登録エラー（「通信送信エラー」や「ライセンスクラウドからの無効な応答」など）が発生した場合は、しばらく待ってから登録を再試行してください。複数回試行してもエラーが続く場合は、シスコ カスタマー エクスペリエンス チームにお問い合わせください。
- 登録中に通信タイムアウトエラーが発生した場合は、エラーダイアログボックスで [OK] をクリックすると、アプリケーションが登録を再試行します。
- 場合によっては、登録が成功した後に更新されたステータスを表示するには、ページを手動で更新する必要があります。

ライセンスアクションの手動での実行

Cisco Crosswork の場合、登録および認証の更新はデフォルトで自動的に有効になっています。ただし、アプリケーションとシスコサーバー間の通信障害が発生した場合は、これらのアクションを手動で開始できます。[アクション（Actions）] ドロップダウンボタンを使用して、アプリケーションを手動で更新、再登録、および登録解除できます。

（注） Cisco Optimization Engine スマートライセンスの場合、ノードカウントは、デバイスの最初のオンボーディング中、およびライセンスの登録と資格付与中に追跡されます。ノード数の変更は、GMT の 24 時間ごとにスマートライセンスサーバーと同期されます。待機しない場合は、アプリケーションライセンスを再登録して、ノード数をすぐに更新できます。

ステップ 1 [スマートライセンス（Smart License）] ウィンドウで、[アクション（Actions）] ドロップダウンボタンをクリックし、次のクイックアクションに関連するオプションを選択します。



a) **[アクション（Actions）] > [認証の更新（Renew Authorization）]**：30 日の終わりに自動更新サービスが失敗した場合に手動で認証を更新します。

b) **[アクション（Actions）]>[登録の更新（Renew Registration）]**：6 か月の終わりに自動更新サービスが失敗した場合に手動で登録を更新します。

c) **[アクション（Actions）] > [再登録（Re-register）]**：登録トークンの期限切れなどの理由で、アプリケーションを再登録します。

d) **[アクション（Actions）] > [登録解除（De-register）]**：トランスポート設定を変更する必要があるなどの場合に、アプリケーションの登録を解除します。

（注） 登録が解除されると、アプリケーションは [評価（Evaluation）] モード（評価期間がある場合）または [評価期限切れ（Evaluation Expired）] モードに移行します。詳細については、ライセンス認証ステータス （18 ページ）を参照してください。

ステップ 2 選択したアクションが正常に実行されます。

ライセンス認証ステータス

Cisco Crosswork アプリケーションの登録ステータスに基づいて、次のライセンス認証ステータスが表示されます。

表 *1:* ライセンス認証ステータス

登録ステータス	ライセンス認証ステータス	説明
未登録	評価モード（Evaluation mode）	アプリケーションのライセンス機能を自由に使用できる 90 日の評価期間。この状態は、アプリケーションを初めて使用するときに開始されます。
	評価期限切れ（Evaluation Expired）	評価期間の終了時にアプリケーションが正常に登録されませんでした。この状態の間、アプリケーション機能は無効になります。アプリケーションを使用し続けるには、登録する必要があります。
	登録期限切れ（Registered Expires）	アプリケーションは、アイデンティティ証明書の有効期限が切れる前に CSSM に接続できず、未登録状態に戻りました。残りの評価期間がある場合、アプリケーションは再開します。この段階では、アプリケーションを再登録するために新しい登録 ID トークンが必要です。
登録済み	承認済み（準拠）（Authorized (In Compliance)）	アプリケーションは、予約済みのライセンス機能の使用を完全に許可されています。認証は 30 日ごとに自動的に更新されます。
	コンプライアンス違反（Out of Compliance）	アプリケーションの現在の機能を使用するために予約できる十分なライセンスが関連付けられたバーチャルアカウントにありません。アプリケーションを引き続き使用するには、トークンに登録されている権限/使用制限を更新する必要があります。
	認証が期限切れ（Authorization Expired）	アプリケーションが 90 日以上 CSSM と通信できず、認証の有効期限が切れています。

ユーザーの管理

ベストプラクティスとして、管理者はすべてのユーザーに対して個別のアカウントを作成する必要があります。Cisco Crosswork を使用するユーザーのリストを準備します。ユーザー名と予備パスワードを決定し、それらのユーザープロファイルを作成します。ユーザーアカウントの作成時に、ユーザーがアクセスできる機能を決定するためのユーザーロールを割り当てます。「admin」以外のユーザーロールを使用する場合は、ユーザーを追加する前にユーザーロールを作成します（「ユーザーロールの作成 （23 ページ）」を参照）。

ステップ 1 メインメニューから、**[管理（Administration）] > [ユーザーとロール（Users and Roles）] > [ユーザー（Users）]** タブを選択します。このウィンドウから、新しいユーザーの追加、既存のユーザーの設定の編集、およびユーザーの削除を行うことができます。

ステップ 2 新しいユーザーを追加するには、次の手順を実行します

a) ＋をクリックして必要なユーザーの詳細を入力します。

b) [保存（Save）] をクリックします。

ステップ 3 ユーザーを編集するには、次の手順を実行します。

a) ユーザーの横にあるチェックボックスをクリックし、✎をクリックします。

b) 変更を加えたら、[保存（Save）] をクリックします。

ステップ 4 ユーザーを削除するには、次の手順を実行します。

a) ユーザーの横にあるチェックボックスをクリックし、🗑をクリックします。

b) [削除の確認（Confirm Deletion）] ウィンドウで、[削除（Delete）] をクリックします。

ステップ 5 ユーザーの監査ログを表示するには、次の手順を実行します：

a) [アクション（Actions）] 列の下の ⋯ アイコンをクリックし、[監査ログ（Audit Log）] を選択します。

選択したユーザー名の [監査ログ（Audit Log）] 画面が表示されます。監査ログの詳細については、「View Audit Log」を参照してください。

インストール時に作成された管理ユーザー

インストール時に、Crossworkは2つの特別な管理IDを作成します。

1. ユーザー名が**`cw-admin`**で、デフォルトのパスワードが**`admin`**の**仮想マシン管理者**。データセンター管理者はこのIDを使用してログインし、Crossworkサーバーをホストしている VM をトラブルシューティングします。
2. ユーザー名が **`admin`** でデフォルトのパスワードが **`admin`** の **Cisco Crosswork 管理者**。製品管理者は、このIDを使用してログインし、ユーザーインターフェイスを設定し、新しいユーザーIDの作成などの特別な操作を実行します。

両方の管理ユーザーIDのデフォルトパスワードは、最初に使用するときに変更する必要があります。次の方法を使用して、Cisco Crossworkの管理者パスワードを変更することもできます。

- 管理者ユーザーとしてログインし、管理者ユーザーパスワードを編集します。
- `admin(config)# username admin <password>` と入力します。

ユーザーロール、機能カテゴリ、および権限

[ロール（Roles）] ウィンドウでは、適切な権限を持つユーザーがカスタムユーザーロールを定義できます。デフォルトの *admin* ロールと同様に、カスタムユーザーロールは次の要素で構成されます。

- 「Operator」や「admin」などの一意の名前。
- 選択した、名前付きの 1 つ以上の機能カテゴリ。そのロールを持つユーザーが、API によって制御されている特定の Cisco Crosswork 機能を実行するために必要なその API にアクセスできるかどうかを制御します。
- 選択した 1 つ以上の権限。そのロールを持つユーザーが機能カテゴリ内で実行できる操作の範囲を制御します。

ユーザーロールが機能カテゴリにアクセスできるようにするには、そのカテゴリとその基盤となる API が選択済みであることがそのロールの [ロール（Roles）] ページに表示されている必要があります。機能カテゴリが未選択としてユーザーロールに表示されている場合、このロールが割り当てられているユーザーは、その機能領域にアクセスすることはできません。

一部の機能カテゴリは、1 つのカテゴリ名で複数の API をグループ化します。たとえば、「AAA」カテゴリは、パスワードの変更、リモート認証サーバーの統合、およびユーザーとロールの管理の API へのアクセスを制御します。このタイプのカテゴリでは、一部の API を選択しないままにして、それら API へのアクセスを拒否する一方で、他の API を選択してカテゴリ内のそれらの API へのアクセスを提供することができます。たとえば、自身のパスワードを変更できても、リモート AAA サーバーのインストールを統合するための設定を表示または変更できない、または新しいユーザーとロールを作成できない「オペレータ」ロールを作成する場合は、「AAA」というカテゴリ名を設定し、[リモート認証サーバー統合 API（Remote Authentication Server Integration API）] チェックボックスと [ユーザーおよびロール管理 API（Users and Role Management API）] チェックボックスをオフにします。

選択したカテゴリの各ロールについて、[ロール（Roles）] ページでは、基盤となる各機能 API に対する権限を定義することもできます。

- [読み取り（Read）] 権限では、ユーザーはその API によって制御されているオブジェクトを表示および操作できますが、オブジェクトの変更や削除はできません。
- [書き込み（Write）] 権限では、ユーザーはその API によって制御されているオブジェクトを表示および変更できますが、削除はできません。
- [削除（Delete）] 権限では、その API によって制御されているオブジェクトに対する削除権限がユーザーロールに付与されます。削除権限は、Crosswork プラットフォームとそのアプリケーションによって設定された基本的な制限を上書きしないことに注意してください。

必要に応じて権限を混在させることもできます。

- ユーザーアクセス用の API を選択する場合は、その API に少なくとも「読み取り」権限を付与する必要があります。

- ユーザーアクセス用の API を選択すると、Cisco Crosswork はそのユーザーがその API に対するすべての権限を持つことを想定し、自動的に 3 つの権限すべてを選択します。
- [読み取り（Read）] を含むすべての権限をオフにすると、Cisco Crosswork は API へのアクセスを拒否すると想定し、選択が解除されます。

ベスト プラクティス：

カスタムユーザーロールを作成する場合は、次のベストプラクティスに従うことをお勧めします。

- Crosswork の展開全体のメンテナンスと管理のための管理を明示的に担当する管理者ユーザーのロールでの [削除（Delete）] 権限を制限します。
- すべての Cisco Crosswork API を使用する開発者のロールには、管理者ユーザーと同じ権限が必要です。
- Cisco Crosswork を使用してネットワークの管理に積極的に関与しているユーザーには、少なくとも [読み取り（Read）] 権限と [書き込み（Write）] 権限をロールに適用します。
- システムアーキテクトまたはプランナーとしての業務に役立つ Cisco Crosswork データのみを表示する必要があるユーザーには、ロールへの読み取り専用アクセス権を付与します。

次の表に、作成を検討する必要があるカスタムユーザーロールの例を示します。

表 *2:* カスタムユーザーロールの例

ロール	説明	カテゴリ/API	権限
オペレータ	アクティブネットワーク マネージャ。KPIアラートに応じてプレイブックをトリガーします。	すべて	読み取り、書き込み
モニター	アラートのみをモニターします	Health Insights、インベントリ、トポロジ	読み取り専用
API インテグレータ	すべて	すべて	すべて

（注） 管理者ロールには読み取り、書き込み、および削除の権限を含める必要があり、読み取り/書き込みロールには読み取りと書き込みの両方の権限を含める必要があります。ゼロタッチプロビジョニング機能を使用するには、すべての ZTP API にアクセスする必要があります。

ユーザーロールの作成

管理者権限を持つローカルユーザーは、必要に応じて新しいユーザーを作成できます（「ユーザーの管理 （19 ページ）」を参照）。

この方法で作成されたユーザーは、割り当てたユーザーロールに関連付けられている機能またはタスクのみを実行できます。

ローカル **admin** ロールは、すべての機能へのアクセスを可能にします。インストール時に作成され、変更または削除することはできません。ただし、その権限は新しいローカルユーザーに割り当てることができます。ローカルユーザーのみがユーザーロールを作成または更新できます。 TACACS ユーザーはそれらの操作を実行できません。

新しいユーザーロールを作成するには、次の手順を実行します。

ステップ 1 メインメニューから、**[管理（Administration）]**>**[ユーザーとロール（Users and Roles）]**>**[ロール（Roles）]** タブを選択します。

[ロール（Roles）] ウィンドウの左側には [ロール（Roles）] テーブル、右側には対応する [管理（admin）] テーブルがあり、選択したロールのユーザー権限のグループが表示されます。

ステップ 2 [ロール（Roles）] テーブルで、＋をクリックしてテーブルに新しいロールエントリを表示します。

ステップ 3 新しいロールに一意の名前を入力します。

ステップ 4 ユーザーロールの権限設定を定義します。

a) このロールを持つユーザーがアクセスできるすべての API のチェックボックスをオンにします。API は、対応するアプリケーションに基づいて論理的にグループ化されます。

b) API ごとに、適切なチェックボックスをオンにして、ユーザーロールに [読み取り（Read）]、[書き込み（Write）]、および [削除（Delete）] の権限があるかどうかを定義します。API グループ全体（AAA など）を選択することもできます。グループ内のすべての API が選択され、これらの API には [読み取り（Read）]、[書き込み（Write）]、および [削除（Delete）] の権限が事前に選択されています。

ステップ 5 [保存 (Save)] をクリックして、新しいロールを作成します。

新しいユーザーロールを 1 つ以上のユーザー ID に割り当てるには、ユーザー ID の [ロール（Role）] の設定を編集します（「ユーザーロールの編集 （24 ページ）」を参照）。

ユーザーロールの複製

既存のユーザーロールの複製は、新しいユーザーロールの作成と同じですが、権限を設定する必要はありません。必要に応じて、複製されたユーザーロールに元のユーザーロールのすべての権限を継承させることができます。

ユーザーロールの複製は、多数の新しいユーザーロールをすばやく作成して割り当てるための便利な方法です。次の手順に従って、既存のロールを複数回複製できます。複製されたユーザーロールの権限の定義はオプションの手順です。複製されたロールに新しい名前を付ける必要があるだけです。必要に応じて、ユーザーグループに実行するロールを示す名前を割り当て

ることができます。次に、そのユーザーグループのユーザー ID を編集して、新しいロールを割り当てます（「ユーザーの管理 （19ページ）」を参照）。後で、ロール自体を編集してユーザーに必要な権限を付与できます（「ユーザーロールの編集 （24 ページ）」を参照）。

ステップ 1 メインメニューから、**[管理（Administration）]>[ユーザーとロール（Users and Roles）]>[ロール（Roles）]** タブを選択します。

ステップ 2 既存のロールをクリックします。

ステップ 3 をクリックして、元のロールのすべての権限を持つ新しい重複エントリを [ロール（Roles）] テーブルに作成します。

ステップ 4 複製したロールに一意の名前を入力します。

ステップ 5 （オプション）ロールの設定を定義します。

a) 複製したロールがアクセスできるすべての API のチェックボックスをオンにします。

b) 各 API について、適切なチェックボックスをオンにして、クローンロールに [読み取り（Read）]、[書き込み（Write）]、および [削除（Delete）] の権限があるかどうかを定義します。API グループ全体（AAA など）を選択することもできます。グループ内のすべての API が選択され、これらの API には [読み取り（Read）]、[書き込み（Write）]、および [削除（Delete）] の権限が事前に選択されています。

ステップ 6 [保存 (Save)] をクリックして、新たに複製したロールを作成します。

ユーザーロールの編集

管理者権限を持つユーザーは、デフォルトの **admin** ロール以外のユーザーロールの権限をすばやく変更できます。

ステップ 1 メインメニューから、**[管理（Administration）]>[ユーザーとロール（Users and Roles）]>[ロール（Roles）]** タブを選択します。

ステップ 2 [ロール（Roles）] テーブルで、既存のロールをクリックして選択します。右側の [管理者（Admin）] テーブルに、選択したロールの権限設定が表示されます。

ステップ 3 ロールの設定を定義します。

a) ロールがアクセスできるすべての API のチェックボックスをオンにします。

b) API ごとに、適切なチェックボックスをオンにして、ロールに [読み取り（Read）]、[書き込み（Write）]、および [削除（Delete）] の権限があるかどうかを定義します。API グループ全体（AAA など）を選択することもできます。グループ内のすべての API が選択され、これらの API には [読み取り（Read）]、[書き込み（Write）]、および [削除（Delete）] の権限が事前に選択されています。

ステップ 4 完了したら、[保存（Save）] をクリックします。

ユーザーロールの削除

管理者権限を持つユーザーは、デフォルトの**admin**ユーザーロールではないユーザーロール、または現在ユーザー ID に割り当てられていないユーザーロールを削除できます。1 つ以上のユーザー ID に現在割り当てられているロールを削除する場合は、それらのユーザー ID を編集して別のユーザーロールに割り当てる必要があります。

ステップ 1 メインメニューから、**[管理（Administration）]**>**[ユーザーとロール（Users and Roles）]**>**[ロール（Roles）]** タブを選択します。

ステップ 2 削除するロールをクリックします。

ステップ 3 をクリックします。

ステップ 4 [削除（Delete）] をクリックして、ユーザーロールの削除を確定します。

ロール権限のカテゴリ

[ロール（Roles）] ウィンドウでは、適切な権限を持つユーザーがカスタムユーザーロールを定義できます。

次の表は、Cisco Crosswork のさまざまなロール権限カテゴリの概要です。

表 *3:* ロール権限のカテゴリ

カテゴリ	ロール権限	説明
AAA	パスワード変更 API	パスワードを管理する権限を提供します。読み取りおよび書き込みアクセス許可は、デフォルトで自動的に有効になります。削除アクセス許可は、パスワード変更操作には適用されません（パスワードは削除できません。変更のみが可能です）。
	リモート認証サーバー統合 API	Crossworkでリモート認証サーバー構成を管理する権限を提供します。構成を表示/読み取るには読み取りアクセス許可が必要です。また、外部認証サーバー（LDAP、TACACS など）の構成を Crosswork に追加/更新するには、書き込みアクセス許可が必要です。削除アクセス許可は、これらの API には適用されません。
	ユーザーとロールの管理 API	ユーザー、ロール、セッション、およびパスワードポリシーを管理する権限を提供します。サポートされている操作には、「新しいユーザー/ロールの作成」、「ユーザー/ロールの更新」、「ユーザー/ロールの削除」、「ユーザー/ロールのタスク詳細の更新」、「セッション管理（アイドル タイムアウト、最大セッション..）」が含まれます。 "、"パスワード ポリシーの更新"、"パスワード ツールチップのヘルプ テキストの取得"、"アクティブなセッションの取得" など。 読み取りアクセス許可ではコンテンツを表示でき、書き込みアクセス許可では作成と更新ができ、削除アクセス許可ではユーザーまたはロールを削除できます。
アラーム	アラーム API	アラームを管理できます。 読み取りアクセス許可により、要求基準に従ってイベント/アラームを取得し、Syslog 宛先のリストを取得し、トラップ宛先のリストを取得できます。 書き込みアクセス許可により、アラームが発生または確認されたときの応答の設定、イベントの作成/発生、イベント情報マニフェストの更新、およびアラームへのメモの追加を行うことができます。 削除アクセス許可により、REST宛先、Syslog宛先、およびトラップ宛先を削除できます。

カテゴリ	ロール権限	説明
自動保証 DSS インスタンス	データストアサービスの管理者設定	管理者は、データストアストレージ情報（読み取りアクセス許可）を表示し、外部ストレージ（書き込みアクセス許可）の診断テストを実行できます。
	データストアサービス API	長期保存のために外部ストレージを使用したり、サービスメトリクスデータをアーカイブするために Service Assurance が使用する外部データストアを管理したりできます。 読み取りアクセス許可により、ストレージプロバイダー情報の取得、ストレージ統計の確認などを行うことができます。 書き込みアクセス許可により、ローカル CW データストアを外部ストレージと同期し、診断を実行できます。 削除アクセス許可により、外部ストレージプロバイダーを削除できます。

カテゴリ	ロール権限	説明
Crosswork Network Controller	CAT FP 展開マネージャ API	関数パックのアップロードと展開を管理できます。 読み取りアクセス許可により、パッケージ、ファイル、および展開情報のリストを取得できます。 書き込みアクセス許可により、パッケージ/関数パック/ファイルをアップロード/展開/展開解除できます。 削除アクセス許可は、これらの API には適用されません。
	CAT インベントリ RESTCONF API	North Bound Interface（NBI）CAT サービスインベントリデータ用の RESTCONF インターフェイス（CAT から外部コンシューマーへ）。 読み取りアクセス許可では CAT からサービス情報を取得でき、書き込みアクセス許可ではオペレーション API を呼び出して CAT からサービス情報を取得できます。削除アクセス許可は、これらの API には適用されません。
	CAT ISTP REST API	システム使用のみ。 CAT UI/ISTP が機能するには、読み取り/書き込みアクセス許可が必須です。削除アクセス許可は、これらの API には適用されません。
	CAT サービスオーバーレイ API	主にオーバーレイの問題を調査するために使用されます。読み取りアクセス許可のみが適用されます。
	CAT UI API	CAT UI がすべての NSO サービスとリソースを取得できるようにする必須の API。 読み取りアクセス許可を使用すると、すべてのサービス情報を取得して表示できます。書き込みアクセス許可を使用すると、サービス保証情報をコミットできます。削除アクセス許可は、これらの API には適用されません。
	NSO コネクタ API	サービスの再同期、完全な再同期、ログレベルの変更、およびサービスの HA ステータスを返すことができます。 読み取りアクセス許可ではサービスのステータスを確認できますが、他のすべての操作には書き込みアクセス許可が必要です。削除アクセス許可は、これらの API には適用されません。
	OAM サービス API	N/A

カテゴリ	ロール権限	説明
変更自動化	管理 API	ジョブスケジューリングの管理、ログイン情報の上書きの管理、および Playbook 実行のためのユーザーロールの構成を行うための管理制御を提供します。 読み取りアクセス許可ではステータスを確認して情報を取得でき、書き込みアクセス許可では変更を行うことができます。削除アクセス許可は、これらの API には適用されません。
	アプリケーション API	変更自動化タスクを管理できます（たとえば、Playbook 実行のスケジュール、Playbook の実行、Playbook ジョブの更新、Playbook 実行ステータスの確認、Playbook ジョブセットの詳細の確認、サポートされている YANG モジュールの一覧表示など）。 読み取りアクセス許可では、該当する情報を表示できます（たとえば、ジョブステータスの確認、ジョブの詳細の取得など）。一方、書き込みアクセス許可は、Playbook ジョブのスケジューリング/実行に必要です。削除アクセス許可は、これらの API には適用されません。
	プレイブック API	プレイブックを管理できます。 読み取りアクセス許可により、プレイブック、パラメータ、およびポリシー仕様を取得できます。 書き込みアクセス許可により、プレイブックのインポート/エクスポート、および生成が可能になります。 削除アクセス許可により、プレイブックを削除できます。
	Play API	プレイを管理できます。 読み取りアクセス許可ではプレイを取得または表示でき、書き込みアクセス許可ではプレイを作成、更新、またはインポートできます。削除アクセス許可により、プレイを削除できます。

カテゴリ	ロール権限	説明
コレクションインフラ	コレクション API	収集ジョブを管理するための API のアクセス許可。 読み取り/書き込み/削除アクセス許可に基づいて、収集ジョブの表示、新しい収集ジョブ（外部）の作成/更新、または既存の収集ジョブの削除を行うことができます。システム収集ジョブ（Crosswork 消費のために内部で設定されたデータ収集）は、これらのアクセス許可に関係なく変更できません（管理者のみに許可されます）。ただし、読み取りアクセス許可を持つユーザーは、システム収集ジョブを含むすべての収集ジョブの詳細を表示できます。 ほとんどのユーザーにとって、デバイス/センサーパスレベルごとの収集ジョブの詳細（要求とステータス）と実際のデータ収集ステータス/メトリックを表示できるため、読み取り専用のアクセス許可で十分です。
	データ ゲートウェイ マネージャ API	宛先、データゲートウェイ、カスタムパッケージなどでCRUD操作を実行するアクセス許可。 読み取りアクセス許可ではデータを表示でき、書き込みアクセス許可ではデータの追加/更新/削除ができます。
Crosswork 最適化エンジン	OPTIMA 分析 API	Crosswork Optimization Engine で分析を管理できます。 読み取りアクセス許可では履歴データを表示/エクスポートでき、書き込みアクセス許可では Traffic Engineering Dashboard の設定を変更できます。
	最適化エンジン UI API	SR ポリシー、RSVP トンネル、LCM、BWoPT、BWoD、およびプレビューポリシーを管理できます。 読み取りアクセス許可により、展開されたポリシー、設定、ルート、LCM ドメイン構成/データ、サービスオーバーレイデータ、パスクエリ、ダッシュボードメトリックなどを表示できます。 書き込みアクセス許可により、LCM、BWoD、BWoptの設定、ポリシーの展開、CNC/COE管理ポリシーのプレビューなどを行うことができます。 削除アクセス許可により、SR ポリシー、RSVP トンネルの削除、アフィニティマッピングの削除、LCM ドメインの削除を行うことができます。

カテゴリ	ロール権限	説明
Crosswork Optimization Engine v2	最適化エンジン RESTCONF API v2	Crosswork Optimization Engine で RESTCONF インターフェイスのアクセス許可をカスタマイズできます。 読み取りアクセス許可により、L2およびL3トポロジの詳細、およびセグメントルーティングポリシーの詳細を取得できま 書き込みアクセス許可により、ポリシールートのフェッチ、SR ポリシーのプロビジョニング/変更/削除/プレビュー、および LCM 構成の管理を行うことができます。 削除アクセス許可は、これらの API には適用されません。
データゲートウェイのグローバル設定	データ ゲートウェイ グローバル パラメータ API	CDG には特定のパラメータがあり、展開内のすべての CDG でグローバルに変更できます。 読み取りアクセス許可ではデータを表示できますが、データをリセット/更新するには書き込みアクセス許可が必要です。
	Data Gateway グローバルリソースリセット API	グローバルパラメータに対して行われた更新をリセットできます。 読み取りアクセス許可ではデータを表示できますが、書き込みアクセス許可はデータをリセット/更新します。
	Data Gateway グローバルリソース更新 API	グローバルパラメータを更新できます。 読み取りアクセス許可ではデータを表示できますが、書き込みアクセス許可はデータを更新します。
データゲートウェイのトラブルシューティング	データ ゲートウェイ再起動 API	Crosswork Data Gateway（CDG）を再起動します。 書き込みアクセス許可では、CDG を再起動できます。
	データゲートウェイ Showtech API	CDG の showtech ログを生成してダウンロードします 読み取りアクセス許可により showtech を表示でき、書き込みアクセス許可により showtech が生成されます。 書き込みアクセス許可により、showtech を生成できます
Health Insights	Health Insights API	Heath Insights の KPI を管理できます。 書き込みアクセス許可では、すべての KPI、KPI プロファイル、ジョブの詳細、アラートなどを表示できます。 書き込みアクセス許可により、KPI および KPI プロファイルの作成または更新、KPI プロファイルの有効化/無効化、KPI とプレイブックのリンクなどを行うことができます。 削除アクセス許可により、カスタム KPI および KPI プロファイルを削除できます。

カテゴリ	ロール権限	説明
アイコンサーバー	ICON サーバー API	トポロジおよび最適化のユースケースを対象としたインターフェイス/IP データ収集の収集設定を更新できます。
インベントリ	インベントリ API	インベントリ管理ができます。 読み取りアクセス許可により、次のことができます。 • ノードのリスト、ノードのログイン情報、およびデータベース内のノードの数を取得します。 • HA プール、DG 登録、仮想データゲートウェイ、およびインベントリジョブ情報のリストを取得します。 • ポリシー、プロバイダー、およびタグのリストを取得します。 書き込みアクセス許可では、次のことができます。 • 仮想データゲートウェイプールへのデバイスマッピングを更新します。 • 要求されたノードをロック/ロック解除します。 • ノードからタグの関連付けを削除します。部分的な割り当て解除はサポートしていません。 • 一連のデバイスへの入力データを更新します。 • プロバイダーのオンボーディングの API エンドポイントを設定します。 削除アクセス許可により、次のことができます。 • ログイン情報プロファイルとノードの一括削除を実行します。 • 削除操作用の CSV をアップロードします。 • HA プール、データゲートウェイの登録、および仮想データゲートウェイを削除します。 • ポリシー、プロバイダー、およびタグを削除します。

カテゴリ	ロール権限	説明
プラットフォーム	プラットフォーム API	読み取りアクセス許可により、サーバーステータス、クラスタノード情報、アプリケーション ヘルス ステータス、収集ジョブステータス、証明書情報、バックアップおよび復元ジョブステータスなどを取得できます。 書き込みアクセス許可では、次のことができます。 • xFTP サーバーのイネーブル化/ディセーブル化 • クラスタの管理（ログインバナーの設定、マイクロサービスの再起動など） • クラスタリソースの再調整 • ノードの管理（クラスタインベントリのエクスポート、VM の追加、VM 構成の適用、クラスタからの VM の削除など） • 証明書の管理（トラストストアと中間キーストアのエクスポート、証明書の作成または更新、Web サーバーの構成など） • 通常/データのみのバックアップおよび復元操作を実行します。 • アプリケーションの管理（アクティブ化、非アクティブ化、アンインストール、パッケージの追加など） 削除アクセス許可により、VM（ID で識別される）を削除したり、ソフトウェアリポジトリからアプリケーションを削除したりできます。
	分散キャッシュ API	読み取りアクセス許可により、トラブルシューティングのためにキャッシュ統計を取得できます。
	API のグループ化	グループ化管理とトポロジグループの選択ツリー。 読み取りアクセス許可ではトポロジUIを表示でき、書き込みアクセス許可ではグループの作成/更新ができます。グループ管理ページからグループを削除するには、削除アクセス許可が必要です。
	API を見る	トポロジーでのビュー管理。 読み取りアクセス許可ではビューを表示でき、書き込みアクセス許可ではビューを作成/更新でき、削除アクセス許可では削除機能が有効になります。

カテゴリ	ロール権限	説明
トポロジ	地理 API	オフラインマップの地理サービスを提供します。 読み取りアクセス許可はオフラインモードで Geo Map を使用でき、書き込みアクセス許可では Geo Map ファイルをアップロードでき、削除アクセス許可は設定で地図ファイルを削除できます。
	トポロジ API	トポロジページ、設定、またはトポロジ視覚化フレームワークを使用するその他のページを管理できます。 トポロジの視覚化には、読み取りアクセス許可が必須です。書き込みアクセス許可ではトポロジ設定を更新でき、削除アクセス許可ではトポロジリンクがダウンした場合に削除できます。
プロキシ	Crosswork プロキシ API	NSO Restconf NBI の CNC プロキシ API を管理するアクセス許可。 読み取りアクセス許可は NSO REST conf NBI のすべての GET 要求を許可し、書き込みアクセス許可は POST/PUT/PATCH 操作を許可し、削除アクセス許可はすべての削除 API を有効にします。
SWIM	SWIM NB API	SWIM リポジトリにイメージをアップロードし、デバイスに配布してインストールできます。 読み取りアクセス許可を使用すると、SWIM リポジトリからすべてのイメージを一覧表示したり、デバイスからのイメージ情報を表示したり、SWIM ジョブの詳細を確認したりできます。書き込みアクセス許可により、インストール関連のすべての操作をアップロード/配布し、実行することができます。削除アクセス許可により、コピーした画像をデバイスから削除できます。 変更自動化でソフトウェアのインストール/アンインストール Playbook を実行するには、書き込み/削除アクセス許可が必要です。

カテゴリ	ロール権限	説明
Service Health	アーカイバ API	読み取りアクセス許可により、次のことができます。 • 特定のサービスに履歴データが存在するかどうかを確認します。 • 特定のサービスの履歴タイムラインシリーズを取得します。 • 選択したサービスのタイムスタンプのサービスグラフを取得します。 • サービスメトリックデータを取得する 書き込み/削除アクセス許可は、これらの API には適用されません。
	保証グラフマネージャ API	読み取りアクセス許可により、次のことができます。 • サービスの詳細を取得します。 • 影響を受けるサービスのリストを取得します。 • 一致するサブサービス（トランスポートまたはデバイスのみ）のリストを取得します。 書き込み/削除アクセス許可は、これらの API には適用されません。
	ヒューリスティック パッケージ マネージャ API	ヒューリスティック パッケージ管理のアクセス許可と、サービスアシュアランスのプラグインと構成プロファイルを管理するためのアクセス許可。 読み込みアクセス許可により、ヒューリスティック パッケージのエクスポート、ヒューリスティック パッケージの詳細（ルール、プロファイル、サブサービス、メトリクス、プラグイン）のクエリ、および保証オプションのクエリが可能になります。 書き込みアクセス許可により、ヒューリスティック パッケージをインポートし、すべての作成/更新操作を実行できます。 削減アクセス許可により、削除操作を実行できます（たとえば、RuleClass、MetricClass などを削除します）。

カテゴリ	ロール権限	説明
ゼロタッチ プロビジョニング	CW コンフィギュレーション サービス API	読み取りアクセス許可により、次のことができます。 • ZTP 構成リポジトリに保存されているすべての day-0 構成ファイルを一覧表示します。 • ZTP 構成リポジトリに保存されている 0 日目の構成ファイルの数を取得します。 • ZTP 構成リポジトリから day-0 構成ファイルをダウンロードします。 • CW ZTP リポジトリに保存されている Day-0 構成ファイルに関連付けられた情報に基づいて、すべてのデバイスファミリ/デバイスバージョンとデバイスプラットフォームを一覧表示します。 書き込みアクセス許可では、次のことができます。 • 0 日目の構成ファイルまたはスクリプトを ZTP 構成リポジトリにアップロードします。 • ZTP 設定リポジトリに保存されている特定の 0 日目の設定ファイルに関連するメタデータを一覧表示/更新します 削除アクセス許可により、ZTP 構成リポジトリにアップロードされた構成ファイルとスクリプトを削除できます。
	CW イメージ サービス API	読み取りアクセス許可により、次のことができます。 • ZTP イメージリポジトリに保存されているすべてのデバイスイメージファイルを一覧表示します。 • CW ZTP リポジトリに保存されているイメージファイルに関連付けられているすべてのデバイスプラットフォーム/ファミリ名を一覧表示します。 • ID でデバイスイメージファイルをダウンロードします。 書き込みアクセス許可により、ZTP イメージリポジトリに保存されている特定のイメージファイルに関連付けられた関連メタデータを更新できます。 削除アクセス許可により、ZTP イメージリポジトリにアップロードされたイメージファイルを削除できます。
	CW ZTP サービス API	

カテゴリ	ロール権限	説明
		ZTP デバイスとプロファイルを管理できます。Crosswork に追加/更新/削除します。 読み取りアクセス許可により、ZTP デバイス、シリアル番号/OV、プロファイル、サンプルデータ CSV を取得し、ZTP デバイス、プロファイルを一覧表示し、ZTP デバイスとメタデータをエクスポートできます。 削除アクセス許可により、ZTPデバイス、シリアル番号/OV、プロファイルを追加し、ZTP デバイスの属性を追加/更新できます。 削除アクセス許可により、ZTP デバイス、プロファイル、シリアル番号/所有権証明書を削除できます。
CW-CLMS	共通ライセンス管理サービス（CLMS）API	Crosswork でライセンス登録を管理するための API のアクセス許可。 読み取りアクセス許可により、スマートライセンス設定、登録ステータス、およびライセンス使用状況を表示できますが、書き込みアクセス許可は、ライセンスの登録、再登録、登録解除、更新などのスマートライセンス設定を変更するために必要です。

アクティブセッションの管理

管理者は、Cisco Crosswork UI でアクティブなセッションを監視および管理し、次のアクションを実行できます。

- ユーザーセッションの終了
- 監査ログの表示

（注）
- 終了するアクセス許可を持つ管理者以外のユーザーは、自分のセッションを終了できます。
- 読み取りアクセス許可を持つ管理者以外のユーザーは、セッションの監査ログのみを収集できます。
- 読み取りアクセス許可がない管理者以外のユーザーは、[アクティブセッション（Active Sessions）] ウィンドウを表示できません。

ステップ 1 メインメニューから、**[管理（Administration）] > [ユーザーとロール（Users and Roles）] > [アクティブセッション（Active Sessions）]**の順に選択します。

[アクティブセッション（Active Sessions）] タブには、Cisco Crosswork のすべてのアクティブセッションが、ユーザー名、ログイン時間、ログイン方法などの詳細とともに表示されます。

ステップ 2 ユーザーセッションを終了するには、[アクション（Actions）] 列の下の アイコンをクリックし、[セッションの終了（Terminate Session）] を選択します。アクションを確認するためのダイアログボックスが表示されます。[終了（Terminate）] を選択し、セッションを終了します。

（注） セッションを終了するときは注意することをお勧めします。セッションが終了したユーザーは、事前に警告を受け取ることはなく、保存されていない作業は失われます。

ステップ 3 ユーザーの監査ログを表示するには、[アクション（Actions）] 列の下にある アイコンをクリックし、[監査ログ（Audit Log）] を選択します。

選択したユーザー名の [監査ログ（Audit Log）] 画面が表示されます。監査ログの詳細については、「View Audit Log」を参照してください。

ユーザー認証の設定（TACACS+ と LDAP）

Cisco Crosswork は、ローカルユーザーのサポートに加えて、TACACS+ サーバーと LDAP サーバーとの統合により TACACS+ と LDAP のユーザーをサポートします。統合プロセスには次の手順があります。

- TACACS+ と LDAP サーバーを設定します。
- TACACS+ と LDAP のユーザーが参照するロールを作成します。
- AAA 設定を設定します。

（注）

- AAA サーバーページは、すべてのサーバーが 1 回の要求で更新される一括更新モードで動作します。サーバーの削除に関連するアクセス許可を持つユーザーのみに「リモート認証サーバーの統合 API」の書き込みアクセス許可を付与することをお勧めします。
- 読み取りと書き込みのアクセス許可のみを持つ（「削除」アクセス許可のない）ユーザーは、削除操作が「書き込み」アクセス許可の一部であるため、Cisco Crosswork から AAA サーバーの詳細を削除できます。詳細については、ユーザーロールの作成 （23 ページ）を参照してください。
- AAA サーバーに変更を加えるとき（作成/編集/削除）、変更するたびに数分間待つことをお勧めします。十分な間隔を空けて頻繁に AAA を変更すると、外部ログインが失敗する可能性があります。
- Cisco Crosswork は、最大 5 台の外部サーバーの構成をサポートします。

TACACS+ サーバーの管理

Crosswork は、TACACS+ サーバーを使用してユーザーを認証することをサポートしています。

注意 この項の手順に従って操作を行うと、Crosswork のユーザーインターフェイスへのすべての新しいログインに影響することに注意してください。セッションの中断を最小限に抑えるために、すべての TACACS+ の変更を 1 回のセッションで実行し、送信することをお勧めします。

始める前に

Cisco Crosswork と同じものを設定する前に、TACACS+ サーバーで必要なユーザーロールを作成する必要があります。Crosswork を Cisco ISE（Identity Service Engine）などのアプリケーションと統合して、TACACS+ プロトコルを使用して認証することができます。このサービスを利用するには、Cisco ISE で Crosswork をクライアントとして設定する必要があります。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。
https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0/b_ISE_admin_30_device_admin.html

ステップ 1 メインメニューから、**[管理（Administration）]** > **[AAA]** > **[サーバー（Servers）]** > **[TACACS+]** タブを選択します。このウィンドウからは、新し TACACS+ サーバーの追加、設定の編集、および削除を行うことができます。

ステップ 2 **新しい TACACS+ サーバーを追加するには、次の手順を実行します**：

a) ＋アイコンをクリックします。

b) 必要な TACACS+ サーバー情報を入力します。

（注）
- 一意の優先順位値を指定し、認証要求に優先順位を割り当てることができます。
- Crossworkが外部認証サーバーと通信するには、このページで入力する[共有秘密（Shared Secret）]パラメータが、TACACS+サーバーで設定されている共有秘密の値と一致する必要があります。

c) 認証タイプを選択します。
- PAP：パスワードベースの認証は、2つのエンティティが1つのパスワードを事前に共有し、そのパスワードを認証の基準に使用するプロトコルです。
- CHAP：チャレンジハンドシェイク認証プロトコルでは、クライアントとサーバーの両方がプレーンテキストの秘密キーを認識しており、その秘密キーは絶対にネットワーク上に送信されないことが必要になります。CHAPは、パスワード認証プロトコル（PAP）より優れたセキュリティを提供します。

d) 関連するすべての詳細を入力したら、[追加（Add）]をクリックします。

（注） [ポリシーID（Policy ID）]フィールドは、TACACS+サーバーで作成したユーザーロールに対応します。必要なユーザーロールを作成する前にTACACS+ユーザーとしてCisco Crossworkにログインしようとすると、「キーが認証されていません。一致するポリシーがありません（Key not authorized: no matching policy）」というエラーメッセージが表示されます。この場合は、ブラウザを閉じます。ローカル管理者ユーザーとしてログインし、TACACS+サーバーで不足しているユーザーロールを作成し、TACACS+ユーザーログイン情報を使用してCrossworkにログインし直します。

e) [すべての変更を保存（Save All Changes）]をクリックします。変更を更新するためのサーバーの再起動に関する警告メッセージが表示されます。[変更の保存（Save Changes）]をクリックして確認します。

ステップ3 TACACS+ サーバーを編集するには、次の手順を実行します：

a) TACACS+ サーバーの横にあるチェックボックスをクリックし、をクリックします。
b) 変更を加えた後、[更新（Update）]をクリックします。

ステップ4 TACACS+ サーバーを削除するには、次の手順を実行します：

a) TACACS+ サーバーの横にあるチェックボックスをクリックし、  をクリックします。[サーバー IP アドレスの削除（Delete server-IP-address）]ダイアログボックスが開きます。
b) [削除（Delete）]をクリックして確認します。

LDAP サーバーの管理

Lightweight Directory Access Protocol（LDAP）は、ディレクトリ情報にアクセスして管理するために使用されるサーバープロトコルです。Crossworkは、LDAPサーバー（OpenLDAP、Active Directory、およびセキュアLDAP）を使用してユーザーを認証することをサポートしています。

IP ネットワーク経由でディレクトリを管理し、データ転送用の単純な文字列形式を使用して TCP/IP 上で直接実行します。

セキュア LDAP プロトコルを使用するには、LDAP サーバーを追加する前にセキュア LDAP 通信証明書を追加する必要があります。証明書の追加の詳細については、新しい証明書の追加（8 ページ） を参照してください。

注意 この項の手順に従って操作を行うと、Crosswork のユーザーインターフェイスへのすべての新しいログインに影響することに注意してください。セッションの中断を最小限に抑えるために、すべての LDAP サーバーの変更を 1 回のセッションで実行し、送信することをお勧めします。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[AAA]** > **[サーバー（Servers）]** > **[LDAP]** タブを選択します。このウィンドウを使用して、新しい LDAP サーバーの追加、設定の編集、および削除を行うことができます。

ステップ 2 **新しい LDAP サーバーを追加するには、次の手順を実行します**：

a) ＋アイコンをクリックします。

b) 必要な LDAP サーバーの詳細を入力します。

（注）
- TACACS+ サーバーと同様に、一意の優先順位値を指定し、認証要求に優先順位を割り当てることができます。
- セキュア LDAP サーバーを追加するには、[セキュア接続（Secure Connection）] トグルボタンを有効にして、関連するセキュア LDAP 証明書を [証明書（Certificate）] ドロップダウンリストから選択します。
- [ポリシーID（Policy ID）] フィールドは、 LDAP サーバーで作成したユーザーロールに対応します。必要なユーザーロールを作成する前に LDAP ユーザーとして Cisco Crosswork にログインしようとすると、「ログインに失敗しました。ポリシーが見つかりません。ネットワーク管理者にお問い合わせください。」というエラーメッセージが表示されます。このエラーを回避するには、Crosswork で新しい LDAP サーバーを設定する前に、LDAP サーバーで関連するユーザーロールを作成してください。

c) [Add] をクリックします。

d) [すべての変更を保存（Save All Changes）] をクリックします。変更を更新するためのサーバーの再起動に関する警告メッセージが表示されます。[変更の保存（Save Changes）] をクリックして確認します。

ステップ 3 **LDAP サーバーを編集するには、次の手順を実行します**：

a) LDAP サーバーの横にあるチェックボックスをクリックし、✎をクリックします。

b) 変更を加えた後、[更新（Update）] をクリックします。

ステップ 4 **LDAP サーバーを削除するには、次の手順を実行します**：

a) LDAP サーバーの横にあるチェックボックスをクリックし、 をクリックします。
b) [削除（Delete）] をクリックして確認します。

AAA サーバー設定を設定

関連する AAA アクセス許可を持つユーザーは、AAA 設定を設定できます。

ステップ 1 メインメニューから、**[管理（Administration）] > [AAA] > [設定（Settings]** の順に選択します。

ステップ 2 [ローカルへのフォールバック（Fallback to Local）] に関連する設定を選択します。デフォルトでは、Crossworkはローカルデータベース認証よりも外部認証サーバーを優先します。

（注） 管理者ユーザーは常にローカルで認証されます。

ステップ 3 [アイドル状態のユーザをすべてログアウトする間隔（Logout All Idle Users After）] フィールドの関連する値を選択します。 指定された制限を超えてアイドル状態のままになっているユーザーは、自動的にログアウトされます。

（注） デフォルトのタイムアウト値は30分です。タイムアウト値を調整すると、ページが更新されて変更が適用されます。

ステップ 4 [並列セッション数（Number of Parallel Sessions）] に関連する値を入力します。

（注） Crossworkは、同時使用ユーザーに対して5～200の並列セッションセッションをサポートします。並列セッション数を超えると、Crosswork へのログイン時にエラーが表示されます。

ステップ 5 [ローカルパスワードポリシー（Local Password Policy）] に関連する設定を選択します。特定のパスワード設定はデフォルトで有効になっており、無効にすることはできません（たとえば、最初のログイン時にパスワードを変更する）。

（注） パスワードポリシーの変更は、ユーザーが次にパスワードを変更したときにのみ適用されます。ログイン時に、既存のパスワードのコンプライアンスはチェックされません。

（注） [ローカルパスワードポリシー（Local Password Policy）] を使用すると、管理者は、ユーザーがCisco Crossworkからロックアウトされるまでのログイン試行の失敗回数とロックアウト期間を設定できます。待機時間が経過すると、ユーザーは正しいログイン情報でログインを試行することができます。

セキュリティ強化の概要

セキュリティを強化するには、次のコンポーネントがセキュリティメカニズムを最適化できるように調整する必要があります。

- Cisco Crosswork インフラストラクチャ
- Cisco Crosswork ストレージ システム（ローカルまたは外部）

Cisco Crosswork セキュリティを強化するには、次のタスクを実行する必要があります。

- 非セキュア ポートと未使用ポートのシャットダウン
- ネットワーク ファイアウォールの設定
- 必要に応じた Cisco Crosswork インフラストラクチャの強化

主な情報源として、シスコの担当者が各展開環境に固有のサーバー強化ガイダンスをご提供しますが、この項に示す手順に従って Cisco Crosswork を保護することもできます。

認証スロットリング

Cisco Crosswork は、パスワードの推測やその他の関連する不正使用のシナリオを回避するために、ログイン試行の失敗後にログイン試行を抑制します。ユーザー名のログイン試行が失敗すると、そのユーザー名のすべての認証試行が 3 秒間ブロックされます。スロットリングは、TACACS、LDAP、デフォルトのローカル認証など、サポートされているすべての認証方式に適用できます。

主要なセキュリティ概念

Cisco Crosswork 製品のセキュリティの最適化を目指す管理者は、次のセキュリティ概念をよく理解しておく必要があります。

HTTPS

Hypertext Transfer Protocol Secure（HTTPS）では、チャネルを介して送信されるデータの暗号化に、セキュア ソケット レイヤ（SSL） またはその後続の標準規格である Transport Layer Security（TLS）が使用されます。SSL で複数の脆弱性が見つかったため、Cisco Crosswork では現在 TLS のみがサポートされています。

（注） TLS は大まかに SSL と呼ばれることが多いため、本ガイドでもこの表記に従います。

SSL は、プライバシー、認証、およびデータ整合性を組み合わせることで、クライアントとサーバーの間のデータ転送を保護します。これらのセキュリティメカニズムを有効にするために、SSL は証明書、秘密キー/公開キー交換ペア、および Diffie-Hellman 鍵共有パラメータを使用します。

X.509 証明書

X.509 証明書と秘密キー/公開キーの ペアは、ユーザー認証と通信パートナーのアイデンティティ検証に使用されるデジタル識別の一種です。VeriSign や Thawte などの認証局（CA）は、

エンティティ（サーバーまたはクライアント）を識別するための証明書を発行します。クライアントまたはサーバー証明書には、発行認証局の名前とデジタル署名、シリアル番号、証明書が発行されたクライアントまたはサーバーの名前、公開キー、および証明書の有効期限が含まれます。CA は、1 つ以上の署名証明書を使用して SSL 証明書を作成します。各署名証明書には、CA 署名の作成に使用される照合秘密キーがあります。CA は署名付き証明書（公開キーが埋め込まている）を簡単に入手できるようにしているため、誰でもその証明書を使用して、SSL 証明書が実際に特定の CA によって署名されたことを確認できます。

一般に、ハイ アベイラビリティ（HA）と非 HA の両方の環境で証明書を設定するには、次の手順が必要です。

1. サーバーの ID 証明書を生成する。
2. サーバーに ID 証明書をインストールする。
3. 対応するルート証明書をクライアントまたはブラウザにインストールする。

実行する必要がある具体的なタスクは、ご利用の環境によって異なります。

次の点に注意してください。

- サーバーの開始/停止シーケンシングは、HA 環境で慎重に行う必要があります。
- 仮想 IP アドレスが設定されている非 HA 環境では、より複雑な証明書要求プロセスを完了する必要があります。

1 方向 SSL 認証

これは、クライアントが適切なサーバー（中間サーバーではなく）に接続していることを保証する必要がある場合に使用される認証方法で、オンライン バンキングの Web サイトなどのパブリック リソースに適しています。認証は、クライアントがサーバー上のリソースへのアクセスを要求したときに開始されます。リソースが存在するサーバーは、そのアイデンティティを証明するために、サーバー証明書（別名 SSL 証明書または x.509 証明書）をクライアントに送信します。クライアントは受信したサーバー証明書を、クライアントまたはブラウザにインストールする必要がある別の信頼できるオブジェクト（サーバー ルート証明書）と照合して検証します。サーバーの検証後、暗号化された（つまりセキュアな）通信チャネルが確立されます。ここで、Cisco Crosswork サーバーによって HTML 形式の有効なユーザー名とパスワードの入力が求められます。SSL 接続が確立された後にユーザー クレデンシャルを入力すると、未認証の第三者による傍受を防ぐことができます。最終的に、ユーザー名とパスワードが受け入れられた後、サーバー上に存在するリソースへのアクセスが許可されます。

（注） クライアントは複数のサーバーとやり取りするために、複数のサーバー証明書を格納する必要がある場合があります。

クライアントにルート証明書をインストールする必要があるかどうかを判断するには、ブラウザの URL フィールドでロック アイコンを探します。通常このアイコンが表示される場合は、必要なルート証明書がすでにインストール済みであることを示します。多くの場合、これはより大きいいずれかの認証局（CA）によって署名されたサーバー証明書に該当します。一般的なブラウザではこれらの CA からのルート証明書が含まれているからです。

クライアントがサーバー証明書に署名した CA を認識しない場合は、接続がセキュリティで保護されていないことを意味します。これは必ずしも大きな問題ではなく、接続するサーバーの ID が検証されていないことを示しているだけです。この時点で、次の 2 つの操作のいずれかを実行できます。1 つは必要なルート証明書をクライアントまたはブラウザにインストールできます。ブラウザの URL フィールドにロック アイコンが表示された場合は、証明書が正常にインストールされたことを意味します。もう 1 つは、クライアントに自己署名証明書をインストールできることです。信頼できる CA によって署名されたルート証明書とは異なり、自己署名証明書は作成者である個人またはエンティティによって署名されます。自己署名証明書を使用して暗号化チャネルを作成できますが、接続するサーバーの ID が検証されていないため、固有のリスクが伴うことを理解しておいてください。

非セキュアなポートおよびサービスの無効化

一般的なポリシーとして、不要なポートを無効にする必要があります。まず、どのポートが有効になっているかを確認した後、Cisco Crosswork の通常の機能を妨げることなく安全に無効化できるポートを判別する必要があります。これを行うには、開いているポートのリストを表示し、Cisco Crosswork で必要なポートのリストと比較します。

開いているすべてのリスニングポートのリストを表示するには、次の手順を実行します。

ステップ 1 Linux CLI 管理者ユーザーとしてログインし、**netstat -aln** コマンドを入力します。
netstat -aln コマンドは、現在開いている（有効化されている）サーバーの TCP/UDP ポート、システムで使用している他のサービスのステータス、およびその他のセキュリティ関連の設定情報を表示します。このコマンドは、次のような出力を返します。

```
[root@vm ~]# netstat -aln
Active Internet connections (servers and established)
Proto  Recv-Q   Send-Q   Local Address            Foreign Address         State
```

```
tcp    0      0      0.0.0.0:111             0.0.0.0:*               LISTEN
tcp    0      0      127.0.0.1:8080          0.0.0.0:*               LISTEN
tcp    0      0      0.0.0.0:22              0.0.0.0:*               LISTEN
tcp    0      0      127.0.0.1:25            0.0.0.0:*               LISTEN
tcp    0      0      127.0.0.1:10248         0.0.0.0:*               LISTEN
tcp    0      0      127.0.0.1:10249         0.0.0.0:*               LISTEN
tcp    0      0      192.168.125.114:40764   192.168.125.114:2379    ESTABLISHED
tcp    0      0      192.168.125.114:48714   192.168.125.114:10250   CLOSE_WAIT
tcp    0      0      192.168.125.114:40798   192.168.125.114:2379    ESTABLISHED
tcp    0      0      127.0.0.1:33392         127.0.0.1:8080          TIME_WAIT
tcp    0      0      192.168.125.114:40814   192.168.125.114:2379    ESTABLISHED
tcp    0      0      192.168.125.114:40780   192.168.125.114:2379    ESTABLISHED
tcp    0      0      127.0.0.1:8080          127.0.0.1:44276         ESTABLISHED
tcp    0      0      192.168.125.114:40836   192.168.125.114:2379    ESTABLISHED
tcp    0      0      192.168.125.114:40768   192.168.125.114:2379    ESTABLISHED
tcp    0      0      127.0.0.1:59434         127.0.0.1:8080          ESTABLISHED
tcp    0      0      192.168.125.114:40818   192.168.125.114:2379    ESTABLISHED
tcp    0      0      192.168.125.114:22      192.168.125.1:45837     ESTABLISHED
tcp    0      0      127.0.0.1:8080          127.0.0.1:48174         ESTABLISHED
tcp    0      0      127.0.0.1:49150         127.0.0.1:8080          ESTABLISHED
tcp    0      0      192.168.125.114:40816   192.168.125.114:2379    ESTABLISHED
tcp    0      0      192.168.125.114:55444   192.168.125.114:2379    ESTABLISHED
```

ステップ 2 ※ Cisco Crosswork で使用されているポートのテーブルを確認し、ポートがそのテーブルにリストされているかどうかを確認します。この表を参考にすると、どのサービスがポートを使用しているか、およびどのサービスが不要で、安全に無効化できるかを判別できます。この場合の「安全」とは、製品に悪影響を及ぼさずにポートを安全に無効化できることを意味します。

（注） ポートまたはサービスを無効化する必要があるかどうかが不明の場合は、Cisco の担当者にお問い合わせください。

ステップ 3 ネットワーク内にファイアウォールがある場合、Cisco Crosswork の動作に必要なトラフィックのみを許可するようにファイアウォールを設定します。

ストレージの強化

データベース、バックアップ サーバーなど、Cisco Crosswork のインストールに含めるすべてのストレージ要素を保護することをお勧めします。

- 外部ストレージを使用している場合は、ストレージのベンダーとシスコの担当者にお問い合わせください。
- 内部ストレージを使用している場合は、シスコの担当者にお問い合わせください。
- Cisco Crosswork をアンインストールまたは削除する場合は、センシティブ データを含む可能性があるすべての VM 関連ファイルがデジタルで破棄（単に削除されるのではなく）されていることを確認してください。詳細については、シスコの担当者にお問い合わせください。

システム設定の構成

管理者ユーザーは、次のシステム設定を構成できます。

Syslog サーバーの設定

Crosswork では、外部 syslog コンシューマは次を行うことができます。

- Crosswork に登録し、システムイベントを syslog として受信する。
- syslog として転送するイベントの種類をコンシューマごとに定義およびフィルタ処理する。
- syslog がコンシューマに転送されるレートを定義する。

（注） Syslog TLS サーバー証明書が追加されたら、5 分から 10 分待ってから、syslog サーバーを構成します。

始める前に

Syslog TLS サーバー証明書をアップロードしたことを確認してください。詳細については、新しい証明書の追加 （8 ページ）を参照してください。

ステップ 1 メインメニューから、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** タブを選択します。

ステップ 2 [サーバー（Server）] で、[Syslog 設定（Syslog Configuration）] オプションをクリックします。

ステップ 3 ＋をクリックします。

ステップ 4 Syslog 設定の詳細を入力します。詳細については、各オプションの横にある ? をクリックしてください。

[条件（Criteria）] オプションを使用して、syslog として転送するイベントの種類と範囲を定義します。例：**(EventSeverity<2 or EventSeverity>=5) and OriginAppId=capp-infra and EventCategory=1**

この式では、イベントがインフラストラクチャ プラットフォームから発信され、カテゴリがシステムで、シビラティ（重大度）が 2 未満または 5 以上の場合にのみイベントが syslog として送信されます。

注意 式は自由形式であり、検証されません。

ステップ 5 [保存（Save）] をクリックします。

トラップサーバーを設定

[設定（Settings）] ウィンドウからトラップサーバーを管理するには、以下の手順に従います。

ステップ 1 メインメニューから、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** タブを選択します。

ステップ 2 [サーバー（Server）] で、[サーバーのトラップ（Trap servers）] オプションをクリックします。

ステップ 3 ＋ をクリックします。

ステップ 4 トラップサーバーの詳細を入力します。詳細については、各オプションの横にある ⓘ をクリックしてください。

[条件（Criteria）] オプションを使用して、トラップとして転送するイベントの種類と範囲を定義します。

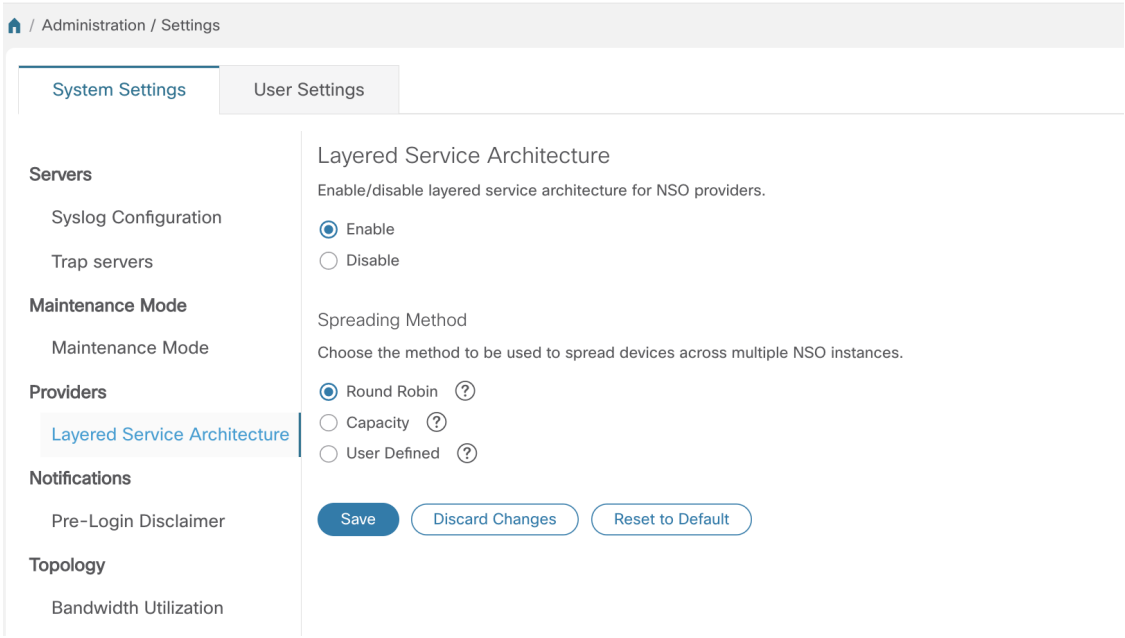
イベントの発生に使用される属性の詳細については、[イベントとアラームの例（Events and Alarms examples）] をクリックしてください。

ステップ 5 関連するすべての情報を入力したら、[追加（Add）] をクリックします。

階層化されたサービスアーキテクチャ（LSA）を有効にする

この手順は、Cisco NSO LSA 展開を選択して、メモリとプロビジョニング スループットを向上させるために任意の多くのデバイスノードを追加することを選択した場合にのみ適用されます。

ステップ 1 メインメニューから、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [階層化されたサービスアーキテクチャ（Layered Service Architecture）]** を選択します。



ステップ 2 [有効（Enable）] を選択します。

ステップ 3 複数の NSO インスタンスにデバイスを分散する方法を選択します。

- [ラウンドロビン（Round Robin）]：デバイスを周期的に RFS ノードに均等に配布します（たとえば、デバイス 1 から RFS1、デバイス 2 から RFS2 など）。
- [容量（Capacity）]：デバイスの数は、その合計容量に基づいて各 RFS インスタンスに割り当てられます。
- [ユーザー定義（User Defined）]：デバイスは、デバイス設定でデバイスに指定された NSO プロバイダーに割り当てられます。詳細については、UI を使用したデバイスの追加を参照してください。

ステップ 4 [保存（Save）] をクリックします。

（注） 設定を保存すると、すべての NSO プロバイダーを削除せずに設定を無効にすることはできません。

ログイン前の免責事項の設定

多くの組織では、ユーザーがログインする前に、システムが免責事項メッセージをバナーに表示することを求めています。システムを使用する際に承認済みのユーザーには義務をバナーで通知したり、未承認のユーザーには警告をバナーに表示することがあります。Crosswork ユーザーに対してこのようなバナーを有効にし、必要に応じて免責事項メッセージをカスタマイズできます。

ステップ 1 メインメニューから、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** タブを選択します。

ステップ 2 [通知（Notifications）] で、[ログイン前の免責事項（Pre-Login Disclaimer）] オプションをクリックします。

ステップ 3 免責事項を有効にし、バナーをカスタマイズするには、次の手順を実行します。

a) [有効（Enabled）] チェックボックスをオンにします。

b) 必要に応じて、バナーの [タイトル（Title）]、[アイコン（Icon）]、および [免責事項のテキスト（Disclaimer Text）] をカスタマイズします。

c) オプション：免責事項の編集中に、次のことを実行できます。

[プレビュー（Preview）] をクリックすると、Crossworkログインプロンプトの前に表示される変更を確認できます。

[変更の破棄（Discard Changes）] をクリックすると、最後に保存したバージョンのバナーに戻ります。

[リセット（Reset）] をクリックすると、バナーが元のデフォルトのバージョンに戻ります。

d) 変更が完了したら、[保存（Save）] をクリックして変更を保存し、すべてのユーザーにカスタム免責事項を表示できるようにします。

ステップ 4 免責事項の表示をオフにするには、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ログイン前の免責事項（Pre-Login Disclaimer）]** を選択し、[有効（Enabled）] チェックボックスをオフにします。

ファイルサーバー設定の管理

Cisco Crossworkは、セキュアなファイル転送サービスを必要とするCrossworkアプリケーションにそれらのサービス（FTP と SFTP）を提供します。デフォルトでは無効です。

（注） この機能は現在、EPNMアプリケーションでのみサポートされています。有効化のシナリオの詳細については、EPNM のユーザーマニュアルを参照してください。

ステップ 1 FTP サーバーを有効化するには、次の手順を実行します。

a) メインメニューから、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ファイルサーバー（File Servers）]** を選択します。

b) [FTP] で、[有効化（Enable）] オプションボタンを選択します。

c) [保存（Save）] をクリックして設定を保存します。

ステップ 2 SFTP サーバーを有効にするには、次の手順を実行します。

a) メインメニューから、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ファイルサーバー（File Servers）]** を選択します。

b) [サーバーアップロードの有効化（Enable Server Upload）] スライダを [オン（On）] の位置にドラッグします。

注意 SFTP は、外部から Cisco Crosswork ストレージへの書き込みアクセスを許可するアップロードオプションをサポートしています。アップロードを有効にする際は注意が必要です。また、不要になったらすぐに無効にする必要があります。

c) [保存（Save）] をクリックして設定を保存します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。