管理タスクの管理

証明書を管理する

証明書とは？

証明書は、個人、サーバー、会社などのエンティティを識別し、公開キーにリンクする電子文書です。証明書の作成時、公開キーと一致する秘密キーの両方が生成されます。TLS プロトコルでは、公開キーがデータを暗号化し、秘密キーが復号化します。

証明書は、「親」証明書として機能する発行者（多くの場合、認証局（CA））によって署名されます。このプロセスは自己署名することもできます。TLS の交換では、証明書の信頼チェーンにより発行者の有効性が確認されます。このチェーンには、自己署名ルート CA 証明書、複数の中間 CA 証明書、およびエンドエンティティ証明書の 3 種類のエンティティが含まれます。中間証明書が、サーバー証明書をルート CA に接続するため、セキュリティが強化されます。ルート証明書の秘密キーから始めて、チェーン内の各証明書が次の証明書に署名して発行し、サーバーまたはクライアントの認証に使用されるエンドエンティティ証明書で終わります。

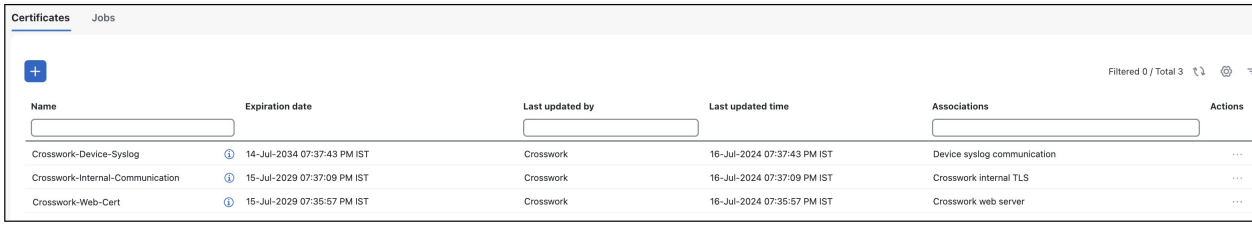
Cisco Crosswork Planning の証明書

Cisco Crosswork Planning は、TLS プロトコルを使用して、デバイスとコンポーネント間をセキュアに通信します。TLS は X.509 証明書を使用してデバイスを認証し、データを暗号化し、その完全性を確保します。システムでは、生成された証明書とクライアントによってアップロードされた証明書の組み合わせが使用されます。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、システムの VM でホストされる Web サーバーとクライアント ブラウザ インターフェイスは、セキュアな通信のために TLS 経由で交換されるシステム生成の X.509 証明書を使用します。

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（Certificate Managemen）] ページ**[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。

図 1 : [証明書管理（Certificate management）] ページ （2 ページ） は、Cisco Crosswork Planning が提供するデフォルトの証明書を表示しています。

図 *1 : [*証明書管理（*Certificate management***）*] ページ***



証明書のタイプと使用方法

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	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 内部 TLS	Crosswork-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。 • 相互認証とサーバー認証を許可します。	Crosswork	Crosswork	ダウンロード	5 年	—
Crosswork Web サーバー	Crosswork-Web-Cert 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。	Crosswork 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
Crosswork デバイス Syslog	Crosswork-Device-Syslog	• Crosswork によって生成および提供されます。 • サーバー認証を許可します。		Device	ダウンロード	5 年	—

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。

- **[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 （22 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 Planning 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。

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。

手順

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。

（注）
[セキュアLDAP通信（Secure LDAP communication）] オプションのみが Cisco Crosswork Planning に該当します。

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 [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。

手順

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 証明書を更新するには、次の手順を実行します。

a) **[アクション（Actions）]** 列で、変更する証明書の [⋯] をクリックし、**[証明書を更新（Update certificate）]** を選択します。

b) 更新する証明書に基づいて、フィールドに適切な値を入力します。詳細については、フィールドの横にある ⓘ アイコンをクリックします。

c) [保存（Save）] をクリックして、変更内容を保存します。

ステップ 3 Web 証明書のクライアント証明書認証を有効にするには、次の手順を実行します。

a) **[アクション（Actions）]** 列で、変更する Crosswork web 証明書の [⋯] をクリックし、**[クライアント証明書認証を構成（Configure client certificate authentication）]** を選択します。

[クライアント証明書認証を構成（Configure client certificate authentication）] ページが表示されます。

b) [有効（Enable）] チェックボックスをオンにします。

[証明書のスキーマ（Certificate schema）] と [OCSP] の設定が表示されます。

[OCSP] 設定はデフォルトで有効になっていますが、必要に応じて無効にすることができます。有効にした場合、オンライン証明書ステータスプロトコル（OCSP）を使用して、証明書の失効ステータスを確認できます。

c) [証明書のスキーマ（Certificate schema）] の値を選択します。

- **[自動（Automatic）]**：代替サブジェクト名領域でユーザープリンシパル名（UPN）を検索します。UPNが見つからない場合、システムは共通名の値を使用します。これはデフォルトの選択肢です。
- **[手動（Manual）]**：ユーザー アイデンティティ ソースと指定された正規表現に基づいて、サブジェクト領域でユーザー名を検索します。

d) （オプション） [OCSP] の値を選択します。

- **[自動（Automatic）]**：証明書からレスポンダ URL を抽出し、それを使用して OCSP 検証を実行します。
- **[手動（Manual）]**：OCSP レスポンダ URL を指定する必要があります。

e) [保存（Save）] をクリックして、変更内容を保存します。

ステップ 4 1 ステップで証明書を更新してクライアント認証を設定するには、次の手順を実行します。

a) 変更する Crosswork Web 証明書で [⋯] をクリックし、**[証明書の更新とクライアント認証の構成（Update Certificate and Configure Client Authentication）]** を選択します。

[証明書の更新とクライアント認証の構成（Update Certificate and Configure Client Authentication）] ページが表示されます。

（注）
証明書を更新してクライアント認証を設定する複合オプションを選択すると、Crosswork サーバーの再起動中のダウンタイムが最小限に抑えられます。これは、これらのアクションを個別に実行した場合は再起動が 2 回発生するのに対し、この複合オプションでは再起動が 1 回しか発生しないためです。

b) ステップ 2 とステップ 3 の指示に従ってデータを入力します。

c) [保存（Save）] をクリックして、変更内容を保存します。

証明書のダウンロード

証明書をダウンロードするには、次の手順を実行します。

手順

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。

ステップ 3 ルート証明書と中間証明書を個別にダウンロードするには、証明書の横にある [⬇] をクリックします。証明書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。

証明書署名要求を使用した Web 証明書の更新

Cisco Crosswork Planning は、中間認証局（CA）証明書をインポートすることで Web 証明書を更新できます。バージョン 7.0.1 以降では、証明書署名要求（CSR）による Web 証明書の更新もサポートされています。

このアプローチにより、Cisco Crosswork Planning の外部に秘密キーを公開することなく、エンタープライズまたは商用 CA によって署名された証明書を取得できます。

始める前に

- 証明書を更新すると、クライアント認証に使用される既存の証明書信頼チェーンが破壊される可能性があるため、慎重に操作を進めてください。
- このプロセスでは Crossworkサーバーを再起動する必要があるため、完了するまで数分かかります。
- クライアント認証を有効にするには、AAA モードをローカルに設定します。

手順

ステップ 1 メインメニューで、**[管理（Administration）]** > **[証明書管理（Certificate Management）]** の順に選択します。

ステップ 2 Web 証明書（`Crosswork-Web-Cert`）の [⋯] をクリックして、**[証明書を更新（Update certificate）]** を選択します。

[証明書の更新方法（Certificate Update Method）] ページが表示されます。

ステップ 3 CSR を作成して、認証局（CA）に送信します。

a) **[証明書署名要求（CSR）を作成（Create a certificate signing request (CSR)）]** ラジオボタン、**[証明書を更新（Update certificate）]** の順に選択します。

[証明書署名要求（CSR）（Certificate Signing Request (CSR)）] ページが表示されます。。

b) **[CSR の作成（Create CSR）]** をクリックします。

[証明書署名要求（CSR）を作成（Create Certificate Signing Request (CSR)）] ページが表示されます。

c) 指定されたフィールドに、関連する値を入力します。詳細については、フィールドの横にあるⓘアイコンをクリックします。次のフィールドは必須です。

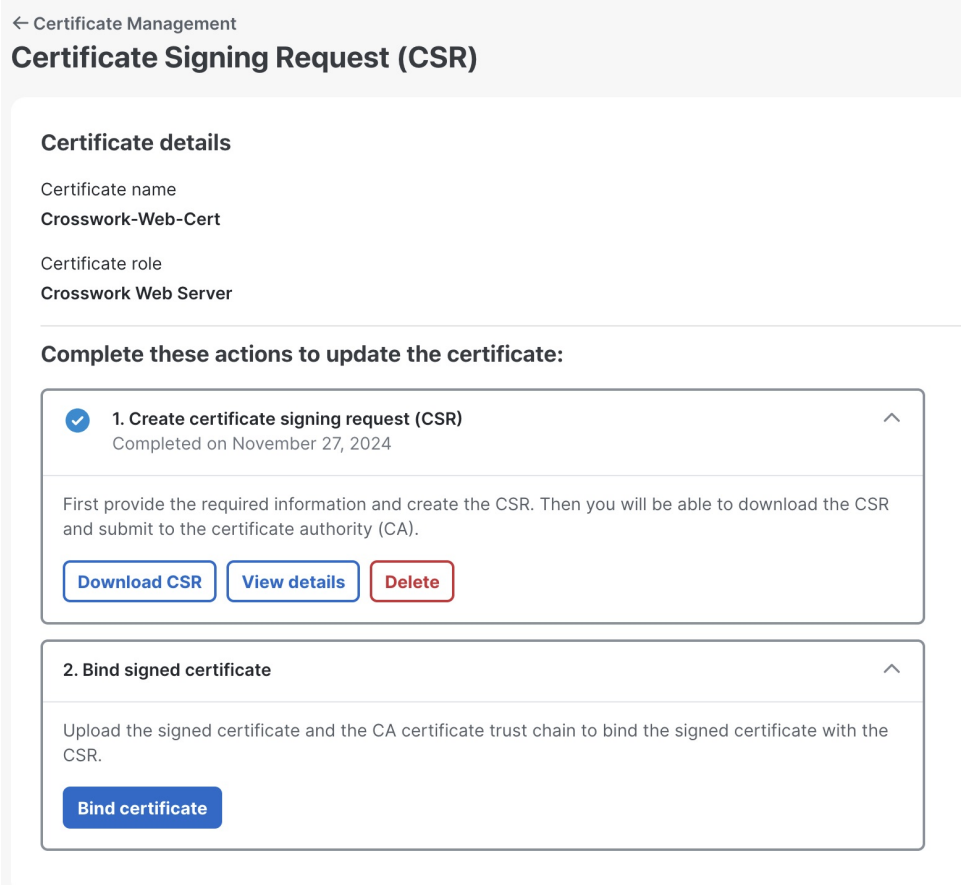
- **[共通名（CN）（Common name (CN)）]**：デフォルトでは、これはサーバーの完全修飾ドメイン名（FQDN）ですが、サーバーを識別する任意の一意の名前にすることができます。64 文字まで使用できます。
- **[IPアドレス（IP address）]**：これは、このデプロイメントで使用される Crosswork VIPアドレスです。追加の IP アドレスは、証明書の検証に必要な場合にのみ追加する必要があります。

- **[キータイプ（Key Type）]**：オプションは、[RSA] と [ECDSA] です。デフォルト値は、[RSA] です。
- **[キーのサイズ（ビット単位（Key Size (in bits)）]**：オプションは [2048]、[3072]、および [4096] です。デフォルト値は、[2048] です。
- **[キーダイジェスト（Key Digest）]**：オプションは、[SHA-256]、[SHA-384]、[SHA-224]、および [SHA-512] です。デフォルト値は、[SHA-256] です。

d) **[CSRを作成（Create CSR）]** をクリックして、アクションを完了します。

ステップ 4 CSR を生成したら、**[ダウンロード（Download）]** をクリックして、CSR をダウンロードして使用し、CA からの署名済み証明書を取得します。

図 *2 : [*証明書署名要求（*CSR*）（*Certificate Signing Request (CSR)*）*]* ページ

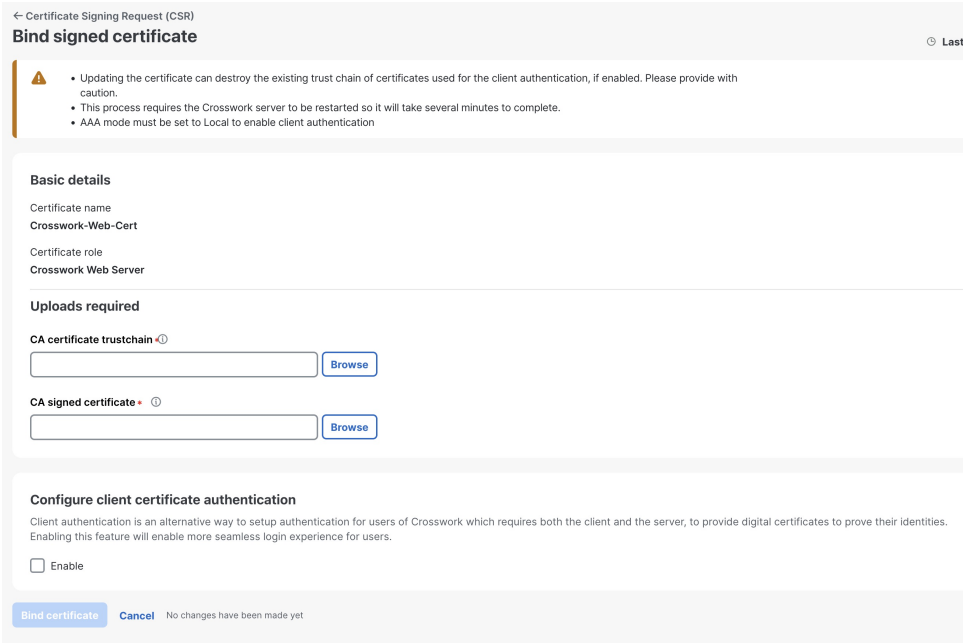


ステップ 5 CA 署名付き証明書と CA 証明書信頼チェーンをアプリケーションして、証明書をバインドします。

a) **[証明書署名要求（CSR）（Certificate Signing Request (CSR)）]** ウィンドウで、**[証明書をバインド（Bind certificate）]** をクリックします。

[署名付き証明書をバインド（Bind signed certificate）] ウィンドウが表示されます。

図 *3:* 署名付き証明書のバインド



b) 表示されたフィールドに関連データをアップロードします。詳細については、フィールドの横にある ⓘ アイコンをクリックします。

- **[CA証明書信頼チェーン（CA certificate trustchain）]**：これは、CA から取得した Web サーバー証明書の証明書信頼チェーンです。
- **[CAあ署名済み証明書（CA signed certificate）]**：これは、CA から取得した Web サーバーの最終的な署名済み証明書です。

c) （オプション）**[有効（Enable）]** チェックボックスをクリックして、クライアント証明書認証を構成します。

d) **[証明書をバインド（Bind certificate）]** をクリックして、操作を完了します。

バインドアクションが完了すると、Web 証明書がアップロードされ、新しい Web 証明書で Tyk が再起動されます。

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 Planning 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 ロールの作成 （12 ページ）」を参照）。

手順

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。詳細については、「監査ログの表示 （44 ページ）」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、Cisco Crosswork Planning 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。

ユーザーロール、関数カテゴリ、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、API の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データのみを表示する必要があるユーザーのロールには、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 *1:* 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	アクティブなネットワーク管理者	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	Cisco Crosswork Planning Design および Collector	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。

ユーザ 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 （9 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、RADIUS および LDAP 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。

手順

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 [グローバルAPI権限（Global API Permissions）] 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化が表示されます。

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 ユーザロールの権限設定を定義するには、[グローバルAPI権限（Global API Permissions）] タブを選択し、次の手順を実行します。

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 （14 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 （9 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 （14 ページ）」を参照）。

（注） 一部のAPI権限はシステム管理者ロールで事前に定義されており、複製されたロールでも変更されません。たとえば、システム管理者ロールには、**Alarms & Events API** 向けのデフォルトの **[読み取り（Read）]** および **[書き込み（Write）]** 権限があります。これらの権限は、元の管理者ロールと複製された管理者ロールの両方に対して構成することはできません。

ユーザーロールを複製するには、次の手順を実行します。

手順

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。

ユーザーロールを編集するには、次の手順を実行します。

手順

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 左側の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 [グローバルAPI権限（Global API Permissions）] タブに、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。

ユーザーロールを削除するには、次の手順を実行します。

手順

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。

グローバル API 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。

次の表は、Cisco Crosswork Planning のさまざまな**グローバル API 権限**の概要です。

表 *2:* グローバル *API* 権限のカテゴリ

カテゴリ	グローバル API 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	Cisco Crosswork Planning 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 Cisco Crosswork Planning 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）」、「パスワードポリシーの更新」、「パスワードのツールチップヘルプテキストの取得」、「アクティブなセッションの取得」などが含まれます。 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。
管理操作	診断情報 API	
アラームおよびイベント	アラームおよびイベント API	システムアラームを管理できます。 （注） Cisco Crosswork Planning アプリケーションに関連付けられているアラームとイベントは、サポートされていません。
Crosswork Planning		

カテゴリ	グローバル API 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、Cisco Crosswork Planning 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 • ノード情報の管理（ログインバナーの設定、マイクロサービスの再起動など） • 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。
	API を見る	Cisco Crosswork Planning Design でのビューの管理。 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。

アクティブ セッションの管理

管理者は、Cisco Crosswork Planning 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

注目

- 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。

手順

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）]** タブを選択します。

[アクティブセッション（Active sessions）] タブには、Cisco Crosswork Planning 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。

（注）
[送信元IP（Source IP）] 列は、[監査のために送信元IPを有効にします（Enable source IP for auditing）] チェックボックスをオンにして、Cisco Crosswork Planning に再ログインした場合にのみ表示されます。このオプションは、**[管理（Administration）]** > **[AAA]** > **[設定（Settings）]** ページの [送信元IP（Source IP）] セクションにあります。

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、[終了（Terminate）] 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。

注目
- 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。
- セッションが終了したユーザーには、次のエラーメッセージが表示されます。「セッションが終了しました。もう一度ログインし直してください（`Your session has ended. Log into the system again to continue`）」。

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、「監査ログの表示 （44 ページ）」を参照してください。

ユーザー認証の設定（TACACS+、LDAP および RADIUS）

Cisco Crosswork Planning は、ローカルユーザーのサポートに加えて、TACACS+、LDAP、および RADIUS サーバーとの統合により、TACACS+、LDAP、および RADIUS ユーザーをサポートします。

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、すべての外部サーバーの認証の変更を 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。

統合プロセスには、次の手順があります。

- TACACS+、LDAP、および RADIUS サーバーを設定します。
- TACACS+、LDAP、および RADIUS 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。
- TACACS+、LDAP、および RADIUS ユーザーの認証にシングルサインオン（SSO）を有効にすることもできます。詳細については、シングルサインオン（SSO）の有効化（28 ページ）を参照してください。

（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承認を持つユーザーのみに Remote Authentication Servers Integration 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 ロールの作成 （12 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。

TACACS+ サーバーの管理

Cisco Crosswork Planning 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。

Crosswork をスタンドアロンサーバー（(open TACACS+）、または 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。

始める前に

- Cisco Crosswork Planning で AAA サーバーを設定する前に、TACACS+ サーバー（スタンドアロンまたは Cisco ISE）で関連パラメータ（ユーザーロール、デバイスアクセスグループ属性、共有秘密形式、共有秘密値）を設定します。Cisco ISE での手順の詳細については、最新バージョンの『Cisco Identity Services Engine Administrator Guide』を参照してください。

手順

ステップ 1 メインメニューから、**[管理（Administration）]** > > **[AAA]** > > **[サーバー（Servers）]** > > **[TACACS+]** タブの順に選択します。このウィンドウからは、新しい TACACS+ サーバーの追加、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。

表 *3 : TACACS+* フィールドの説明

フィールド	説明
[認証順序（Authentication order）]	一意の優先順位値を指定して認証要求に優先順位を割り当てます。順序は 10 ～ 99 の間の任意の数値です。10 未満はシステムで予約済みです。 デフォルトでは 10 が選択されます。
[IP アドレス（IP address）]	TACACS+ サーバーの IP アドレスを入力します（IP アドレスが選択されている場合）。
[DNS 名（DNS name）]	DNS 名を入力します（DNS 名を選択した場合）。IPv4 DNS 名のみがサポートされています。
[ポート（Port）]	デフォルトの TACACS+ ポート番号は 49 です。
[共有秘密形式（Shared secret format）]	アクティブな TACACS+ サーバーの共有秘密。ASCII または 16 進数を選択します。

フィールド	説明
[共有秘密（Shared secret）]/[共有秘密の確認（Confirm shared secret）]	アクティブな TACACS+ サーバーのプレーンテキストの共有秘密。入力したテキストの形式は、選択した形式（ASCII または 16 進数）と一致する必要があります。 Crosswork が外部認証サーバーと通信するには、この画面で入力する [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。
[サービス（Service）]	アクセスしようとしているサービスの値を入力します。たとえば、「raccess」です。 このフィールドは、スタンドアロン TACACS+ の場合にのみ検証されます。Cisco ISE の場合は、ジャンク値を入力できます。フィールドを空白のままにしないでください。
[ポリシーID（Policy ID）]	TACACS+ サーバーで作成したユーザーロールを入力します。 （注） 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 Planning 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 Cisco Crosswork Planning にログインし直します。
[Device Access Group属性（Device access group attribute）]	Device Access Group 属性値は、（ISE/スタンドアロン）TACACS+ サーバー属性でデバイスアクセスグループに使用されるキーに基づいています。これらの値は、1 つまたは複数のカンマで区切られたエントリにすることができます。 TACACS+ のコンテキストでは、Device Access Group 属性は、通常、TACACS+ サーバーがネットワークデバイスに送り返すカスタム属性または承認属性です。この属性により、認証されたユーザに適用されるネットワークデバイスのグループ、またはデバイスのアクセスポリシーのレベルを指定します。Device Access Group 属性は、ポリシー ID と同期して動作し、デバイス間でのユーザー権限を定義します。
[再送信タイムアウト（Retransmit timeout）]	タイムアウトの値を入力します。最大タイムアウトは 30 秒です。
[再試行（Retries）]	許可される認証の再試行回数を指定します。

フィールド	説明
認証タイプ	TACACS+ の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。

詳細については、このトピックの最後にある例を参照してください。

c) 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。
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、確定します。

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。Cisco Crosswork Planning は、ユーザーを認証するための LDAP サーバー（OpenLDAP、Active Directory、およびセキュア LDAP）の使用をサポートします。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（4 ページ） を参照してください。

始める前に

- Cisco Crosswork Planning で AAA サーバーを設定する前に、LDAP サーバーで関連パラメータ（バインド DN、ポリシーベース DN、ポリシー ID など）を設定します。

手順

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、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。

表 *4 : LDAP* フィールドの説明

フィールド	説明
[認証順序（Authentication order）]	一意の優先順位値を指定して認証要求に優先順位を割り当てます。順序は 10 ～ 99 の間の任意の数値です。10 未満はシステムで予約済みです。 デフォルトでは 10 が選択されます。
[名前（Name）]	LDAP ハンドラの名前。
[IPアドレス/ホスト名（IP address/ Host name）]	LDAP サーバーの IP アドレスまたはホスト名
[セキュア接続（Secure connection）]	SSL 通信を介して LDAP サーバーに接続する場合は、[セキュア接続（Secure Connection）] トグルボタンをオンにします。オンにする場合は、[証明書（Certificate）] ドロップダウンリストからセキュア LDAP 証明書を選択します。 （注） セキュア LDAP サーバーを設定する前に、[証明書の管理（Certificate Management）] 画面にセキュア LDAP 証明書を追加する必要があります。 このフィールドは、デフォルトでは無効です。
[ポート（Port）]	デフォルトの LDAP ポート番号は 389 です。セキュア接続 SSL が有効になっている場合は、デフォルトの LDAP ポート番号は 636 です。
バインド DN（Bind DN）	データベースへのログインアクセスの詳細を入力します。バインド DN により、ユーザーは LDAP サーバーにログインできます。
[バインドログイン情報（Bind credential）]/[バインドログイン情報の確認（Confirm bind credential）]	LDAP サーバーにログインするためのユーザー名とパスワード。

フィールド	説明
ベース DN（Base DN）	ベースDNは、LDAPサーバーがディレクトリ内のユーザー認証を検索するために使用する開始点です。
[ユーザーフィルタ（User filter）]	ユーザー検索のフィルタ。
[DNの形式（DN Format）]	ベース DN でユーザーを識別するために使用される形式。
[プリンシパル l ID（Principal l ID）]	この値は、特定のユーザー名が編成されている LDAP サーバー ユーザー プロファイル内の UID 属性を表します。
[ポリシーベースDN（Policy BaseDN）]	この値は、ディレクトリ内のユーザーロールのロールマッピングを表します。
[ポリシーマップ属性（Policy map attribute）]	これは、ポリシーベース DN でユーザーを識別するのに役立ちます。 この値は、LDAP サーバー属性の `userFilter` パラメータにマッピングされます。
[ポリシーID（Policy ID）]	[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。 （注） 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 Crossworks Planning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、Cisco Crosswork Planning 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。
[Device Access Group属性（Device access group attribute）]	Device Access Group 属性値は、LDAP サーバー属性でデバイスアクセスグループに使用されるキーに基づいています。これらの値は、1つまたは複数のカンマで区切られたエントリにすることができます。 LDAP のコンテキストでは、Device Access Group 属性は、通常、LDAP サーバーがネットワークデバイスに送り返すカスタム属性または承認属性です。この属性により、認証されたユーザに適用されるネットワークデバイスのグループ、またはデバイスのアクセスポリシーのレベルを指定します。Device Access Group 属性は、ポリシー ID と同期して動作し、デバイス間でのユーザー権限を定義します。
[接続タイムアウト（Connection timeout）]	タイムアウトの値を入力します。最大タイムアウトは 30 秒です。

詳細については、このトピックの最後にある例を参照してください。

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**：

a) LDAP サーバーを選択して、  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**：

a) LDAP サーバーを選択して、  をクリックします。
b) [削除（Delete）] をクリックして確認します。

RADIUS サーバーの管理

Crosswork は、RADIUS（Remote Authentication Dial-In User Service）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。Crosswork を Cisco ISE（Identity Service Engine）などのアプリケーションと統合して、RADIUS プロトコルを使用して認証することもできます。

始める前に

- TACACS+ サーバーと同様に、Cisco Crosswork Planning で AAA サーバーを設定する前に、RADIUS サーバーで関連パラメータ（ユーザーロール、デバイスアクセスグループ属性、共有秘密形式、共有秘密値）を設定する必要があります。Cisco ISE での手順の詳細については、最新バージョンの『Cisco Identity Services Engine Administrator Guide』を参照してください。

手順

ステップ 1 メインメニューで、**[管理（Administration）] > [AAA] > [サーバー（Servers）] > [RADIUS]** タブの順に選択します。このウィンドウからは、新しい RADIUS サーバーの追加、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 RADIUS サーバーを追加するには**：

a)  アイコンをクリックします。
b) 必要な RADIUS サーバー情報を入力します。

表 *5 : RADIUS* フィールドの説明

フィールド	説明
[認証順序（Authentication order）]	一意の優先順位値を指定して認証要求に優先順位を割り当てます。順序は 10 ～ 99 の間の任意の数値です。10 未満はシステムで予約済みです。 デフォルトでは 10 が選択されます。
[IP アドレス（IP address）]	RADIUS サーバーの IP アドレスを入力します（IP アドレスが選択されている場合）。
[DNS 名（DNS name）]	IPv4 DNS名のみがサポートされています（DNS名が選択されている場合）。
[ポート（Port）]	デフォルトの RADIUS ポート番号は 1645 です。
[共有秘密形式（Shared secret format）]	アクティブな RADIUS サーバーの共有秘密。ASCII または 16 進数を選択します。
[共有秘密（Shared secret）]/[共有秘密の確認（Confirm shared secret）]	アクティブな RADIUS サーバーのプレーンテキストの共有秘密。入力したテキストの形式は、選択した形式（ASCII または 16 進数）と一致する必要があります。 Cisco Crosswork Planning が外部認証サーバーと通信するには、この画面で入力する [共有秘密（Shared Secret）] パラメータが、RADIUS 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。
[サービス（Service）]	アクセスしようとしているサービスの値を入力します。たとえば、「raccess」です。
[ポリシーID（Policy ID）]	[ポリシーID（Policy Id）] フィールドは、RADIUS サーバーで作成したユーザーロールに対応します。 （注） 必要なユーザーロールを作成する前に RADIUS ユーザーとして Cisco Crosswork Planning 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、RADIUS サーバーで不足しているユーザーロールを作成し、RADIUS ユーザーログイン情報を使用して Cisco Crosswork Planning にログインし直します。

フィールド	説明
[Device Access Group属性（Device access group attribute）]	Device Access Group 属性値は、RADIUS サーバー属性でデバイスアクセスグループに使用されるキーに基づいています。これらの値は、1つまたは複数のカンマで区切られたエントリにすることができます。 RADIUS のコンテキストでは、Device Access Group 属性は、通常、RADIUS サーバーがネットワークデバイスに送り返すカスタム属性または承認属性です。この属性により、認証されたユーザに適用されるネットワークデバイスのグループ、またはデバイスのアクセスポリシーのレベルを指定します。Device Access Group 属性は、ポリシー ID と同期して動作し、デバイス間でのユーザー権限を定義します。
[再送信タイムアウト（Retransmit timeout）]	タイムアウトの値を入力します。最大タイムアウトは 30 秒です。
[再試行（Retries）]	許可される認証の再試行回数を指定します。
認証タイプ	RADIUS の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。

RADIUS の設定は TACACS+ と非常によく似ているため、詳細については、TACACS+ サーバーの管理 （19 ページ）の詳細な例を参照してください。

c) 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。
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、確定します。

ステップ 3 RADIUS サーバーを編集するには：

a) RADIUS 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 RADIUS サーバーを削除するには：

a) RADIUS 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。

シングルサインオン（SSO）の有効化

シングルサインオン（SSO）は、単一の ID とパスワードを使用して、関連するが独立したソフトウェアシステムのいずれかにログインできる認証方法です。これにより、一度ログインすると、認証要素を再入力することなくサービスにアクセスできます。Cisco Crossworkはアイデンティティプロバイダー（IDP）として機能し、信頼するサービスプロバイダーに認証サポートを提供します。TACACS+、LDAP、および RADIUS ユーザーの認証に SSO を有効にすることもできます。

Crossworkは SSO 相互起動をサポートしており、サービスプロバイダーとのナビゲーションを容易にします。設定が完了すると、ウィンドウの右上隅にある起動アイコン（ ）を使用して URL を起動できます。

注目

- Crossworkを再インストールまたは移行するときは、Crossworkからの最新の IDP メタデータがサービス プロバイダー アプリケーションに対して更新されていることを確認する必要があります。これを行わないと、メタデータ情報が一致しないため、認証が失敗します。
- 初めてログインするユーザーは、パスワードを強制的に変更する前に別のユーザー名の使用に切り替えることはできません。唯一の回避策は、管理者がセッションを終了することです。

（注） Central Authentication Service（CAS）ポッドが再起動中または実行されていない場合、Cisco Crossworkプランニング ログインページは表示されません。

始める前に

[管理（Administration）] > **[AAA]** > **[設定（Settings）]** ページで [監査のために送信元IPを有効にします（Enable source IP for auditing）] チェックボックスがオンになっていることを確認します。

手順

ステップ 1 メインメニューから、**[管理（Administration）]** > **[AAA]** > **[SSO]** の順に選択します。[アイデンティティプロバイダー（Identity Provider）] ウィンドウが表示されます。このウィンドウを使用して、サービスプロバイダーの追加、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 **新しいサービスプロバイダーを追加するには**、次のことを行います。

a) アイコンをクリックします。

b) [サービスプロバイダー（Service Provider）] ウィンドウで、次のフィールドに値を入力します。

- [名前（Name）]：サービス プロバイダー エンティティの名前を入力します。

  （注）
  URL を指定すると、[アイデンティティプロバイダー（Identity Provider）] ウィンドウの [サービス名（Service name）] 列のエントリがハイパーリンクになります。

- [評価順序（Evaluation Order）]：サービス定義が考慮される順序を示す一意の番号を入力します。
- [メタデータ（Metadata）]：フィールドをクリックするか、[参照（Browse）] をクリックして、SAML クライアントの展開を説明するメタデータ XML ドキュメントに移動します。ここにサービスプロバイダーの URL を入力して、相互起動を行うことができます。

ステップ 3 [追加（Add）] をクリックして、サービスプロバイダーの追加を終了します。

ステップ 4 [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、確定します。

設定を保存した後、統合サービス プロバイダー アプリケーションに初めてログインすると、アプリケーションは Cisco Crosswork サーバーにリダイレクトされます。Crosswork 認証情報を提供すると、サービスプロバイダー アプリケーションは自動的にログインします。以降のすべてのアプリケーションログインでは、認証の詳細を入力する必要はありません。

ステップ 5 **サービスプロバイダーを編集するには**、次のことを行います。

a) サービスプロバイダ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。必要に応じて、[評価順序（Evaluation Order）] と [メタデータ（Metadata）] の値を更新できます。
b) 変更を加えた後、[更新（Update）] をクリックします。

ステップ 6 **サービスプロバイダーを削除するには**、次のことを行います。

a) サービスプロバイダ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 設定の構成

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。

手順

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、Cisco Crosswork Planning 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ー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）]** フィールドと **[ユーザー1人当たりの並列セッション数（Number of Parallel sessions per user）]** フィールドに関連する値を入力します。

（注）
Crossworkは、同時接続ユーザーに対して5～200の並列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。

（注）
Crossworkは、50 ～ 400 件の同時 NBI セッションをサポートします。

ステップ 5 監査とアカウンティングのためにユーザーの IP アドレス（送信元 IP）をログに記録するには、[監査のために送信元IPを有効にします（Enable source IP for auditing）] チェックボックスをオンにします。デフォルトでは、このチェックボックスは無効になっています。このオプションを有効にしてCisco Crosswork Planningに再ログインすると、[監査ログ（Audit Log）] ページと [アクティブセッション（Active Sessions）] ページに [送信元IP（Source IP）] 列が表示されます。

ステップ 6 [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 Planning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。

システムとアプリケーションの正常性の監視

Cisco Crossworkプラットフォームは、マイクロサービスで構成されるアーキテクチャ上に構築されます。これらのマイクロサービスの性質上、Crossworkシステム内のさまざまなサービスには依存関係があります。すべてのサービスが稼働している場合、システムとアプリケーションは正常と見なされます。1つ以上のサービスがダウンしている場合、正常性は[Degraded（低下）]と見なされます。すべてのサービスがダウンしている場合、正常性のステータスは[ダウン（Down）] です。

メインメニューから [管理（Administration）] > [Crosswork Manager] を選択して、[Crossworkの概要（Crosswork summary）] ウィンドウと [Crossworkの正常性（Crosswork health）] ウィンドウにアクセスします。各ウィンドウには、システムとアプリケーションの正常性をモニターするためのさまざまなビューがあります。また、このウィンドウでは、Cisco Crosswork、プラットフォームインフラストラクチャ、およびインストールされているアプリケーションの問題を特定、診断、および修正するために使用できるツールと情報が、シスコ カスタマー エクスペリエンス アカウント チームからのサポートとガイダンスとともに提供されます。

両方のウィンドウで同じタイプの情報にアクセスできますが、各サマリーとビューの目的は異なります。

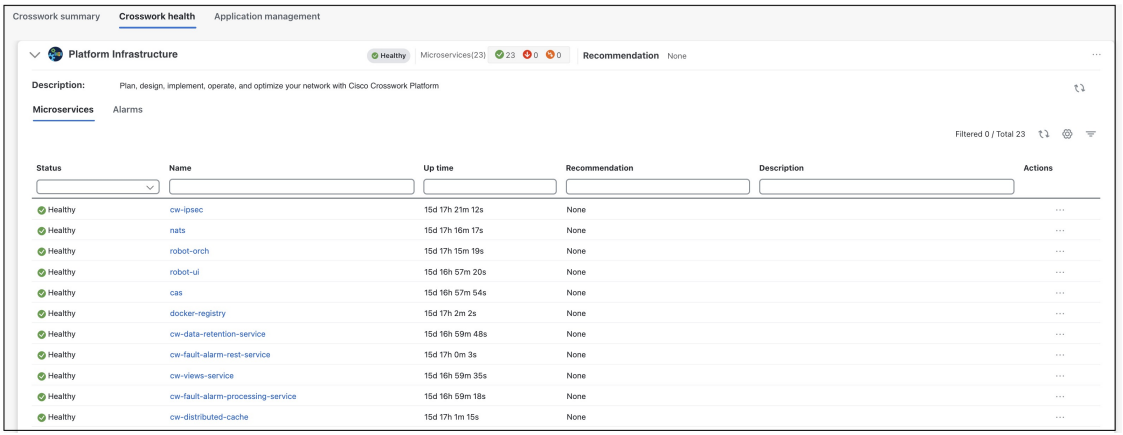
プラットフォームインフラストラクチャとアプリケーション正常性の監視

[Crossworkの正常性（Crosswork Health）] ウィンドウ（**[管理（Administration）]** > **[Crosswork Manager]** > **[Crossworkの正常性（Crosswork Health）]** タブ）には、Cisco Crosswork プラットフォーム インフラストラクチャとインストールされているアプリケーションの正常性の概要と、マイクロサービスステータスの詳細が表示されます。

図 *4 : [Crosswork* 正常性（*Crosswork health*）*]* タブ

このウィンドウ内で、アプリケーションの行を展開して、マイクロサービスとアラームの情報を表示します。

図 *5 : [*マイクロサービス（*Microservices*）*]* タブ



[マイクロサービス（Microservices）] タブで、次の手順を実行します。

- マイクロサービス名をクリックして、マイクロサービスのリストと、該当する場合は関連付けられているマイクロサービスのリストを表示します。
- ⋯ をクリックして再起動するか、マイクロサービスごとにShowtechデータとログを取得します。

（注） Showtech ログは、アプリケーションごとに個別に収集する必要があります。

[アラーム（Alarms）] タブから、次の操作を実行できます。

- アクティブなアラームをフィルタリングします。
- アラームの詳細をドリルダウンするには、アラームの説明をクリックします。
- アラームの状態変更（確認、未確認、クリア）
- アラームへメモを追加します。
- 製品内のイベントのリストを表示します。
- 各イベントの相関アラームを表示します。

システム正常性チェック例

この例では、さまざまなウィンドウや、正常な Crosswork システムで確認すべき領域を検討します。

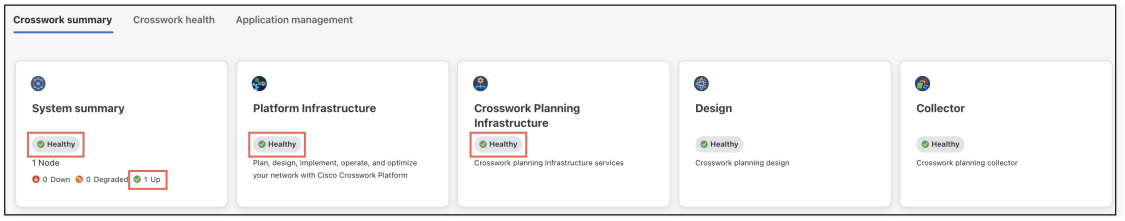
手順

ステップ 1 システム全体の正常性を確認します。

a) メインメニューから、**[管理（Administration）] > [Crosswork Manager] > [Crossworkの概要（Crosswork summary）]** タブを選択します。

b) すべてのノードが動作状態（[アップ（Up）]）であり、[システム概要（System Summary）]、[プラットフォーム インフラストラクチャ（Platform Infrastructure）]、および [Crosswork Planningインフラストラクチャ（Crosswork Planning Infrastructure）] が正常であることを確認します。

図 *6 : [Crosswork* の概要（*Crosswork Summary*）*]* タブ

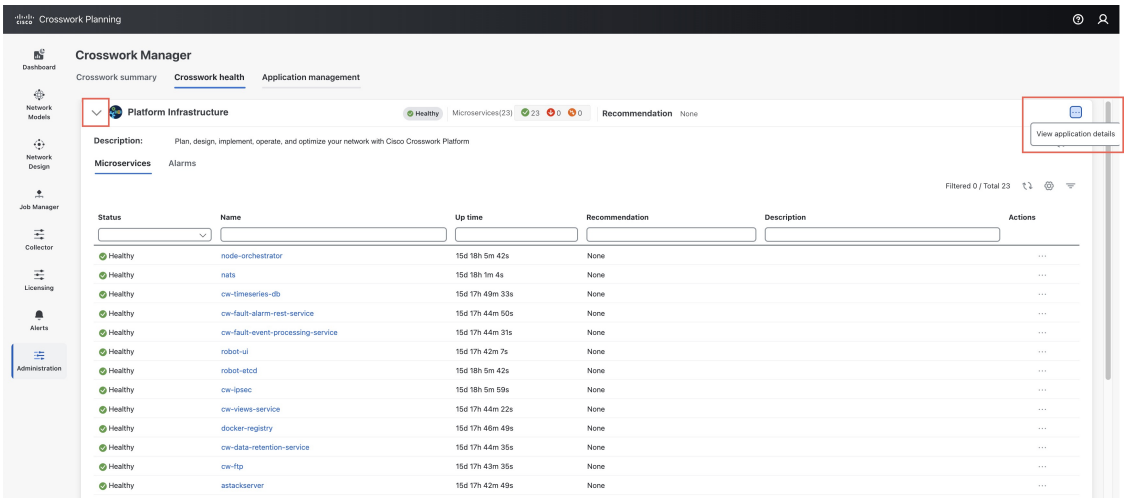


ステップ 2 Crosswork プラットフォーム インフラストラクチャの一部として実行されているマイクロサービスに関する詳細情報を確認および表示します。

a) **[Crossworkの正常性（Crosswork Health）]** タブをクリックします。

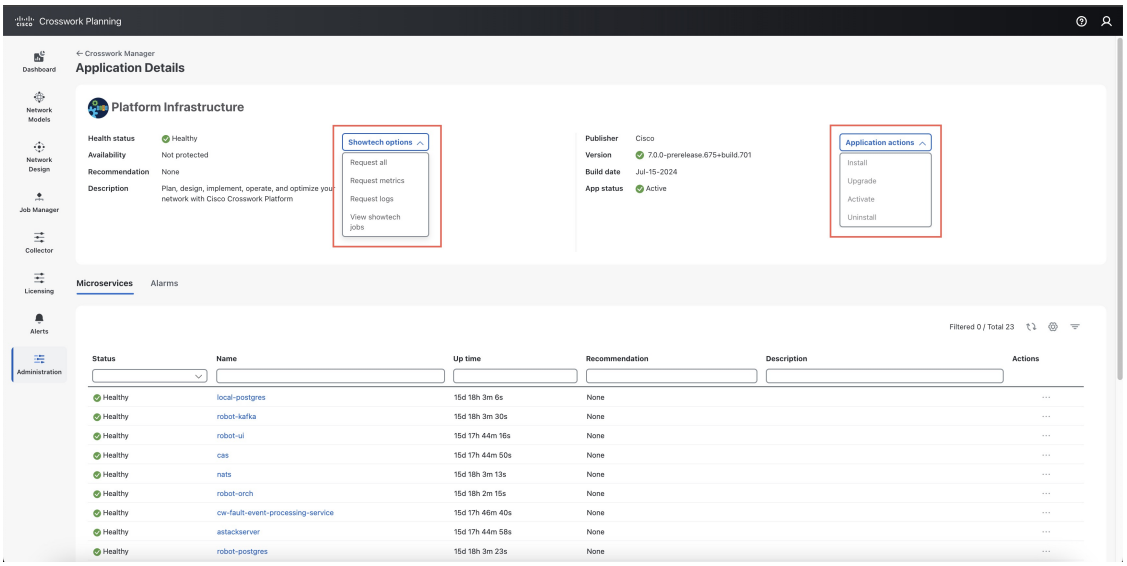
b) [Crossworkプラットフォームインフラストラクチャ（Crosswork Platform Infrastructure）] の行を展開し、 をクリックして [アプリケーション詳細を表示（View application details）] を選択します。

図 *7 : [Crosswork* 正常性（*Crosswork health*）*]* タブ



c) [アプリケーションの詳細（Application Details）] ページでは、マイクロサービスの詳細をチェックおよび見直し、マイクロサービスを再起動し、showtech 情報を収集できます。このウィンドウからインストール関連のタスクを実行することもできます。

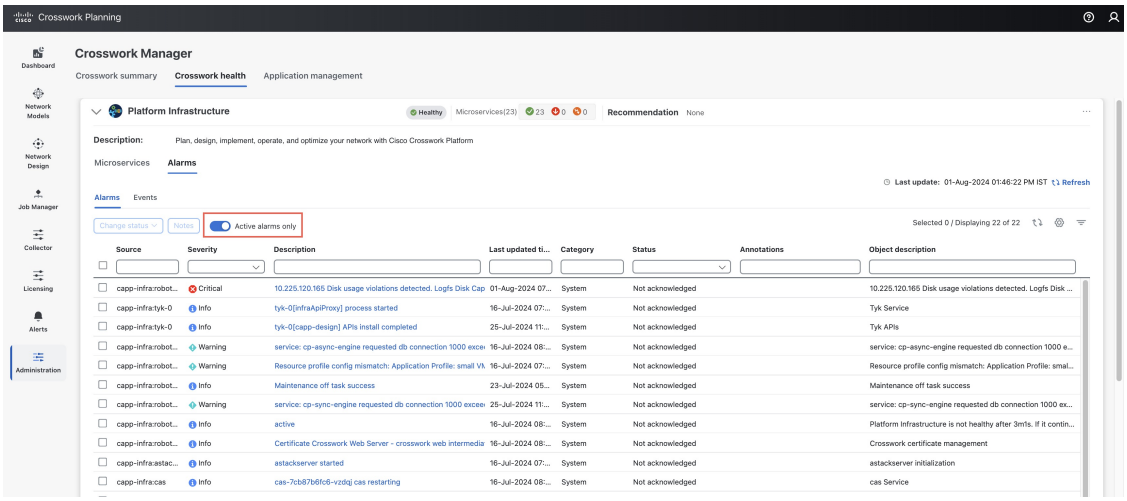
図 *8 : [*アプリケーションの詳細（***Application Details***）*]* ページ



ステップ 3 マイクロサービスに関連するアラームとイベントを確認および表示します。

a) [アラーム（Alarms）] タブをクリックします。リストには、Crosswork Platform Infrastructure のアラームのみが表示されます。アクティブなアラームのみを表示することで、リストをさらにフィルタ処理できます。

図 *9 : [*アラーム（***Alarms***）*]* タブ



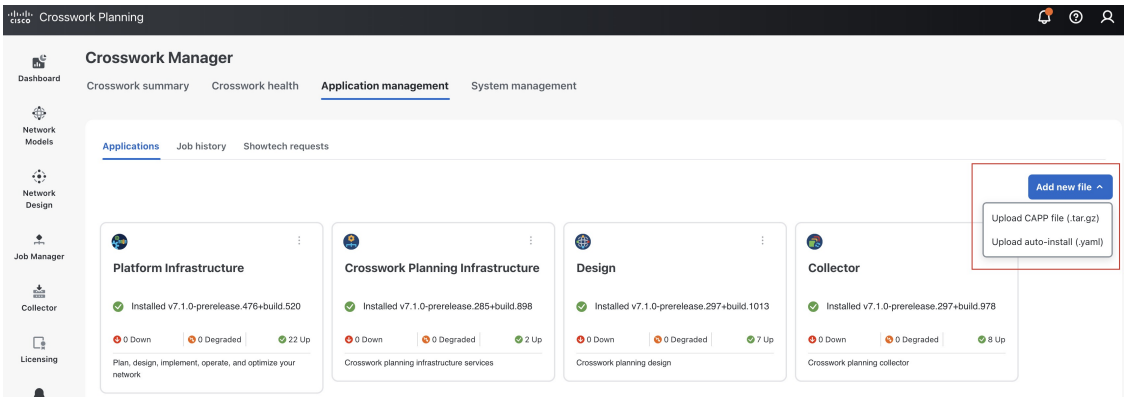
b) [イベント（Events）] タブをクリックします。リストには、すべての Crosswork Platform Infrastructure イベントおよび関連するアラームが表示されます。

ステップ 4 インストールされている Crosswork アプリケーションを表示します。

a) メインメニューで、**[管理（Administration）]**、**>[Crosswork Manager]**、**>[アプリケーション管理（Application Management）]** タブ、**[アプリケーション（Applications）]** の順に選択します。このページには、インストールされているすべてのアプリケーションが表示されます。**[新しいファイルを追加**

（**Add new file**）] をクリックして、別のアプリケーションバンドルまたは自動インストールファイルをアップロードすることで、さらにアプリケーションをインストールすることもできます。

図 *10 : [アプリケーション管理（Application Management）] ウィンドウ*



ステップ 5 ジョブのステータスを表示します。

a) [ジョブ履歴（Job History）] タブをクリックします。このウィンドウには、ジョブのステータスと、ジョブプロセスの一部として実行された一連のイベントに関する情報が表示されます。

バックアップの管理

Backup and Restore の概要

Cisco Crosswork Planning のバックアップ機能と復元機能は、データ損失を防ぎ、インストールされているアプリケーションと設定を保持します。

Cisco Crosswork Planning には、データをバックアップおよび復元するための複数のメニューオプションが用意されています。

メインメニューから、**[管理（Administration）]>[バックアップと復元（Backup and Restore）]** をクリックして、[バックアップと復元（Backup and Restore）] ウィンドウにアクセスします。

表 *6 : Backup and Restore* オプション

メニュー オプション	説明
[アクション（Actions）]>[データのバックアップ（Data backup）] （詳細については、Backup and Restore の管理 （36 ページ） を参照）	Cisco Crosswork Planning 構成データを保持します。バックアップファイルは、データの災害復旧（障害発生後に Cisco Crosswork Planning を復旧する （40 ページ））で使用して、重大な機能停止から回復することができます。
[アクション（Actions）]>[災害後のデータ復元（Data disaster restore）] （詳細については、障害発生後に Cisco Crosswork Planning を復旧する （40 ページ） を参照）	自然災害または人為的災害により Cisco Crosswork Planning サーバーの再構築が必要になった後に、Cisco Crosswork Planning 構成データを復元します。
[アクション（Actions）]>[データ移行（Data migration）]（詳細については、「バックアップと復元を使用してデータを移行する （42 ページ）」 を参照）	Cisco Crosswork Planning の古いバージョンから新しいバージョンにデータを移行します。

Backup and Restore の管理

このセクションでは、Cisco Crosswork Planning UI からデータバックアップおよび復元操作を実行する方法について説明します。

注目

- バックアップ用ターゲットマシンの構築は、このドキュメントの範囲外です。オペレータは、サーバーを配置し、サーバーのログイン情報を把握し、バックアップ用の十分なスペースを備えたターゲットディレクトリを用意する必要があります。
- Cisco Crosswork Planning はバックアップを管理しません。オペレータは、ターゲットサーバーから古いバックアップを定期的に削除して、将来のバックアップ用のスペースを確保する必要があります。
- バックアッププロセスには、十分な量のストレージスペースを備えたサーバーへの SCP アクセスが必要です。各バックアップに必要なストレージは、Cisco Crosswork Planning サーバー内のアプリケーション、およびスケールの要件によって異なります。
- バックアップまたは復元プロセスにかかる時間は、バックアップのタイプ、および Cisco Crosswork Planning サーバー内のアプリケーションによって異なります。

Cisco Crosswork Planning のバックアップの作成時または復元時は、次の手順を実行します。

- 最初のログイン時に、バックアップファイルを保存する接続先 SCP サーバーを設定します。これは1回限りのセットアップであり、バックアップを作成したり、復元操作を開始したりする前に完了する必要があります。
- バックアップ操作または復元操作は、スケジュールされているメンテナンス期間に行います。これらの操作中、ユーザーはシステムにアクセスしてはいけません。バックアップではシステムが約 10 分間オフラインになりますが、復元操作には時間がかかり、他のアプリケーションが一時停止し、データ収集ジョブに影響を与える可能性があります。
- バックアップの作成に使用したものと同じプラットフォームイメージを災害後の復元に使用します。異なるソフトウェアバージョンは、災害後の復元と互換性がありません。
- ダッシュボードを使用して、バックアップまたは復元プロセスの進行状況をモニターします。エラーや内容の誤りを防ぐために、これらのプロセス中にシステムを使用しないでください。
- 一度に実行できるバックアップまたは復元操作は 1 つだけです。
- Cisco Crosswork Planning と SCP サーバーの両方が、同じ IP 環境（たとえば、両方とも IPv6 を使用）にあることを確認します。
- バックアップサーバーの領域を確保するために、古いバックアップを削除することもできますが、これらはジョブリストに引き続き表示されます。
- より多くの変更を行うオペレータは、より頻繁に（できれば毎日）バックアップする必要がありますが、他のオペレータは、週に1回または主要なシステムのアップグレードの前にバックアップを行えば十分です。
- デフォルトでは、システムが正常であると見なされない場合、バックアップは許可されませんが、トラブルシューティングのために強制できます。

- コレクタエージェントを使用している場合は、Backup and Restore 操作後、停止状態のままになる可能性があるため、手動で再起動します。

始める前に

作業を開始する前に、次を確認してください。

- セキュアな SCP サーバーのホスト名または IP アドレスおよびポート番号。サーバーに十分なストレージがあることを確認してください。
- バックアップファイルの接続先として使用する SCP サーバー上のファイルパス。
- 接続先 SCP サーバーのリモートパスに対するファイルの読み取り/書き込み権限を持つアカウントのユーザークレデンシャル。
- インストールされているアプリケーションのビルドバージョンをメモしている。データの復元を実行する前に、それらのアプリケーションの正確なバージョンをインストールする必要があります。アプリケーションのビルドバージョンに不一致があると、データが失われ、データの復元ジョブが失敗する可能性があります。

手順

ステップ 1 **SCP バックアップサーバーを設定します。**

a) メインメニューから、**[管理（Administration）]** > **[バックアップと復元（Backup and Restore）]** を選択します。
b) **[接続先（Destination）]** をクリックして、**[接続先を編集（Edit destination）]** ドロワーパネルを表示します。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。
c) [保存（Save）] をクリックして、バックアップサーバーの詳細を確認します。

ステップ 2 **バックアップを作成します。**

a) メインメニューから、**[管理（Administration）]** > **[バックアップと復元（Backup and Restore）]** を選択します。
b) **[アクション（Actions）]** > **[データをバックアップ（Data backup）]** の順に選択し、宛先サーバーの詳細が事前に入力された **[データバックアップ（Data Backup）]** ドロワーパネルを表示します。
c) [ジョブ名（Job name）] フィールドに、バックアップに該当する名前を入力します。
d) VM またはいずれかのアプリケーションの状態が、[正常（Healthy）]状態ではない場合に、バックアップを作成する場合は、**[強制（Force）]** チェックボックスをオンにします。

（注）
[Force] オプションは、シスコ カスタマー エクスペリエンス チームに相談した後にのみ使用する必要があります。

e) 必要に応じて残りのフィールドにも入力します。

別のリモートサーバーアップロード先を指定する場合：事前に入力された**[ホスト名（Host name）]**、**[ポート（Port）]**、**[ユーザー名（Username）]**、**[パスワード（Password）]**、および**[リモートパス/ロケーション（Remote path/Location）]**フィールドを編集して、別の接続先を指定します。

f) （オプション）**[バックアップ準備の確認（Verify backup readiness）]**をクリックすると、Cisco Crosswork Planningにバックアップを完了するための十分な空きリソースがあるかを確認できます。確認が成功すると、時間がかかる動作の特性に関する警告が Cisco Crosswork Planning に表示されます。[OK] をクリックして、先へ進みます。

検証に失敗した場合は、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。

g) [バックアップ（Backup）]をクリックして、バックアップ操作を開始します。Cisco Crosswork Planningは、対応するバックアップジョブセットを作成し、それをジョブリストに追加します。[Job Details] パネルには、完了した各バックアップステップのステータスが表示されます。

h) バックアップジョブの進行状況を表示するには、**[バックアップおよび復元ジョブセット（Backup restore job sets）]**テーブルの検索フィールドにジョブの詳細（状態やジョブタイプなど）を入力します。次に、目的のジョブセットをクリックします。

[ジョブの詳細（Job Details）] パネルに、選択したジョブセットに関する情報（ジョブステータス、ジョブ名、ジョブタイプなど）が表示されます。失敗したジョブがある場合は、[Status] 列の近くにあるアイコンの上にマウスポインタを合わせると、エラーの詳細が表示されます。

（注）
バックアップ操作が完了したら、宛先 SCP サーバーディレクトリに移動し、バックアップファイルが作成されていることを確認します。このバックアップファイルは、アップグレードプロセスの後の段階で必要になります。

（注）
リストにバックアップジョブが表示されない場合は、[Backup and Restore Job Sets] テーブルを更新します。

i) リモートサーバへのアップロード中にバックアップが失敗した場合：[Job Details] パネルの [Status] アイコンのすぐ下にある [Upload backup] ボタンをクリックして、アップロードを再試行します。

（注）
SCPバックアップサーバーとの接続の問題（たとえば、ログイン情報の誤り、ディレクトリまたはディレクトリの権限の欠落、パスの欠落など）が原因でアップロードに失敗することがあります。こうした原因によることは、タスク `uploadBackupToRemote` の失敗によって示されます。このような状況が発生した場合は、SCP サーバーの詳細を確認し、誤りを修正してから再試行してください。または、[Upload backup] をクリックする前に、[Destination] ボタンを使用して、別の SCP サーバーとパスを指定できます。

ステップ 3 バックアップファイルから復元するには、次の手順を実行します。

a) メインメニューから、**[管理（Administration）]** > **[バックアップと復元（Backup and Restore）]**を選択します。

b) [バックアップおよび復元ジョブセット（Backup and Restore Job Sets）] テーブルで、復元に使用するデータバックアップファイルを選択します。[ジョブの詳細（Job Details）] パネルには、選択したバックアップ ファイルに関する情報が表示されます。

c) バックアップファイルを選択した状態で、**[ジョブの詳細（Job Details）]** パネルに表示されている **[データを復元（Data Restore）]** ボタンをクリックして、復元操作を開始します。Cisco Crosswork Planning は対応する復元ジョブセットを作成し、ジョブリストに追加します。

復元操作の進行状況を表示するには、進行状況ダッシュボードへのリンクをクリックします。

推奨事項：復元後のアクション

復元プロセスが完了したら、通常のシステム操作を再開するために、次のアクションが実行されていることを確認します。

コレクションの編集

バックアップを復元した後、**[コレクタ（Collector）]**、>**[コレクション（Collections）]** ページで、一覧されている各コレクションで、Edit collection 操作を実行します。変更を加えずにコレクションを保存します。これにより、構成データが適切に更新されます。

エージェントの再起動

復元プロセスは、データベースとファイルシステムデータのみをコピーします。復元プロセスが完了すると、すべてのエージェントが停止状態になり、Cisco Crosswork Planning UI から手動で再起動する必要があります。

- **[エージェントをセットアップ（Setup Agent）]** ページで（**[コレクタ（Collector）]**、> **[エージェント（Agents）]**）、それぞれのエージェントに対して、**[起動（Start）]オプションを使用して**、NetFlow と SR-PCE エージェントを再起動します。詳細については、エージェント設定の編集 を参照してください。
- [Traffic コレクタ（Traffic collector）] 構成ページで、**[トラフィックコレクション（Traffic collection）]** オプションを無効にしてから有効にして、トラフィックポーラーエージェントを再起動します。詳細については、トラフィック統計情報の収集 を参照してください。

スケジューラーの実行

- 「今すぐ実行」スケジューラーを使用している場合は、スケジューラーを手動で実行します。
- スケジューラーに CRON ジョブが設定されている場合、スケジューラーは CRON ジョブの設定に基づいて自動的にトリガーされます。

障害発生後に Cisco Crosswork Planning を復旧する

ディザスタリカバリは、自然災害または人為的な災害によって Cisco Crosswork Planning サーバーが破壊された後に使用する復元操作です。*Cisco Crosswork Planning 7.2* インストールガイドの手順に従って、最初に新しいサーバーを展開する必要があります。

ディザスタリカバリを実行するには、次の手順を実行します。

始める前に

- SCPバックアップサーバーから、ディザスタリカバリで使用するバックアップファイルの完全な名前を取得します。通常、これは作成した最新のバックアップファイルとなります。 Cisco Crosswork Planningバックアップファイルの名前は通常、次の形式に従います。

  `backup_JobName_CWVersion_TimeStamp.tar.gz`

  ここで、

  - *JobName* は、ユーザーが入力したバックアップジョブの名前です。
  - *CWVersion* は、バックアップされたシステムのCisco Crosswork Planningプラットフォームのバージョンです。
  - *TimeStamp* は、Cisco Crosswork Planningがバックアップファイルを作成した日時です。

  例：`backup_Wednesday_4-0_2021-02-31-12-00.tar.gz`

- データのバックアップが作成されたときに古いCisco Crosswork Planningサーバーに存在していたアプリケーションの正確なバージョンをインストールします。バージョンが一致しないと、データの損失や復元ジョブの失敗につながる可能性があります。
- バックアップの作成時に使用したものと同じ Cisco Crosswork Planning のソフトウェアイメージを使用してください。異なるソフトウェアバージョンで作成されたバックアップを使用してクラスタを復元することはできません。
- システムの状態を、災害が発生する前に存在していた状態に正確に回復できるように、バックアップを最新の状態に保ちます。前回のバックアップ以降に新しいアプリケーションやパッチをインストールした場合は、別のバックアップを作成します。
- ディザスタリカバリが失敗した場合は、シスコ カスタマー エクスペリエンスにお問い合わせください。
- Crosswork アプリケーションの Smart Licensing 登録は、障害復元操作中には復元されないため、再度登録する必要があります。

手順

ステップ 1 新たに展開したCisco Crosswork Planningサーバーのメインメニューから、**[管理（Administration）]**>**[バックアップと復元（Backup and Restore）]** を選択します。

ステップ 2 **[アクション（Actions）]** > **[災害後のデータ復元（Data disaster restore）]** をクリックして、リモートサーバーの詳細が事前に入力された [災害後のデータ復元（Data Disaster Restore）] ダイアログボックスを表示します。

ステップ 3 [バックアップファイル名（Backup file name）] フィールドに、復元するバックアップのファイル名を入力します。

ステップ 4 [復元の開始（Start restore）] をクリックして、リカバリ操作を開始します。

操作の進行状況を表示するには、進行状況ダッシュボードへのリンクをクリックします。

バックアップと復元を使用してデータを移行する

データ移行のバックアップと復元を使用することは、Cisco Crosswork Planning インストールを新しいソフトウェアバージョンにアップグレードするとき、または既存のデータを新しいインストールに移動するときの前提条件です。

データ移行バックアップを作成する場合は、次のガイドラインに従ってください。

- データ移行ファイルを格納する宛先 SCP サーバーが設定されていることを確認してください。この設定は 1 回限りのアクティビティです。
- Cisco Crosswork Planning と SCP サーバーの両方は、同じ IP 環境内に存在する必要があります。たとえば、Cisco Crosswork Planning を IPv6 経由で通信している場合は、バックアップサーバーも IPv6 で通信している必要があります。
- Cisco Crosswork Planning インストールをアップグレードする場合にのみデータ移行バックアップを作成し、スケジュールされたアップグレードウィンドウ中にのみ作成することをお勧めします。データ移行のバックアップまたは復元操作の実行中は、Cisco Crosswork Planning にアクセスしないでください。

始める前に

次を保持していることを確認します。

- セキュアな接続先 SCP サーバーのホスト名または IP アドレスおよびポート番号。
- データ移行用バックアップファイルの接続先として使用する SCP サーバー上のファイルパス。
- 接続先 SCP サーバーのリモートパスに対するファイルの読み取り/書き込み権限を持つアカウントのユーザーログイン情報。

手順

ステップ 1 **SCP バックアップサーバーを設定します。**

a) メインメニューから、**[管理（Administration）]** > **[バックアップと復元（Backup and Restore）]** を選択します。
b) **[接続先（Destination）]** をクリックして、**[接続先を追加（Add destination）]** ダイアログボックスを表示します。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。
c) [保存（Save）] をクリックして、バックアップサーバーの詳細を確認します。

ステップ 2 バックアップを作成します。

a) データを別のインストールに移行する Cisco Crosswork Planning インストールに管理者としてログインします。

b) メインメニューから、**[管理（Administration）]** > **[バックアップと復元（Backup and Restore）]** を選択します。

c) **[アクション（Actions）]** > **[データをバックアップ（Data backup）]** の順に選択し、宛先サーバーの詳細が事前に入力された **[データバックアップ（Data Backup）]** ダイアログボックスを表示します。

d) [Job Name] フィールドに、バックアップに該当する名前を入力します。

e) マイクロサービスの問題があっても、バックアップを実行する場合は、**[強制（Force）]** チェックボックスをオンにします。

f) 必要に応じて残りのフィールドにも入力します。

別のリモートサーバーアップロード先を指定する場合：事前に入力された **[ホスト名（Host name）]**、**[ポート（Port）]**、**[ユーザー名（Username）]**、**[パスワード（Password）]**、および **[リモートパス/ロケーション（Remote path/Location）]** フィールドを編集して、別の接続先を指定します。

g) **[バックアップ（Backup）]** をクリックして、バックアップ操作を開始します。Cisco Crosswork Planning は、対応するバックアップジョブ一式を作成し、それを **[ジョブ一式をバックアップしてリストア（Backup and Restore Job Sets）]** テーブルに追加します。[Job Details] パネルには、完了した各バックアップステップのステータスが表示されます。

h) バックアップジョブの進行状況を表示するには、[Backup and Restore Job Sets] テーブルの検索フィールドにジョブの詳細（ステータスやジョブタイプなど）を入力します。次に、目的のジョブセットをクリックします。

[Job Details] パネルに、選択したジョブセットに関する情報（ジョブのステータス、ジョブタイプ、開始時刻など）が表示されます。失敗したジョブがある場合は、[Status] 列の近くにあるアイコンの上にマウスポインタを合わせると、エラーの詳細が表示されます。

i) リモートサーバーへのアップロード中にバックアップが失敗した場合：[ジョブの詳細（Job Details）] パネルの [ステータス（Status）] アイコンのすぐ下にある [バックアップのアップロード（Upload backup）] ボタンをクリックして、アップロードを再試行します。

リモートサーバーの問題が原因でアップロードが失敗した場合は、[バックアップのアップロード（Upload backup）] をクリックする前に、[接続先（Destination）] ボタンを使用して別のリモートサーバーとパスを指定します。

ステップ 3 バックアップの新しいインストールへの移行（**Migrate the backup to the new installation**）

a) バックアップからデータを移行する先の Cisco Crosswork Planning インストールに管理者としてログインします。

b) メインメニューから、**[管理（Administration）]** > **[バックアップと復元（Backup and Restore）]** を選択します。

c) **[アクション（Actions）]** > **[データ移行（Data Migration）]** の順に選択し、リモートサーバーの詳細が事前に入力された **[データ移行（Data Migration）]** ダイアログボックスを表示します。

d) [バックアップファイル名（Backup file name）] フィールドに、復元するバックアップのファイル名を入力します。

e) **[移行を開始（Start Migration）]** をクリックして、データ移行操作を開始します。Cisco Crosswork Planning は、対応するデータ移行ジョブ一式を作成し、それをジョブリストに追加します。

データ移行操作の進行状況を表示するには、進行状況ダッシュボードへのリンクをクリックします。

システムおよびネットワークアラームの表示

アラームを表示するには、次のいずれかに移動します。

- メインメニューから **[アラート（Alerts）] > [アラームとイベント（Alarms and Events）]** を選択します。
- アプリケーション固有のアラームの場合は、**[管理（Administration）] > [Crosswork Manager] > [Crosswork の正常性（Crosswork Health）]** タブを選択します。いずれかのアプリケーションを展開し、[アラーム（Alarms）] タブを選択します。

  [アラーム（Alarms）] タブから、次の操作を実行できます。

  - アラームの詳細をドリルダウンするには、アラームの説明をクリックします。
  - アラームのステータスを変更します（確認、未確認、クリア）。アラームを選択し、[ステータスの変更（Change status）] ドロップダウンから必要なステータスを選択します。
  - アラームへメモを追加します。アラームを選択し、[メモ（Notes）]ボタンをクリックします。

監査ログの表示

[監査ログ（Audit Log）] ウィンドウは、次の AAA 関連のイベントを追跡します。

- ユーザーの作成、削除、更新
- ロールの作成、削除、更新
- ユーザー ログイン アクティビティ：ログイン、ログアウト、アクティブセッション最大制限によるログイン失敗、ログイン試行失敗によるアカウントロック。
- [送信元IP（Source IP）] : アクションが実行されたマシンの IP アドレス。この列は、[監査のために送信元IPを有効にします（Enable source IP for auditing）] チェックボックスをオンにして、Cisco Crosswork Planning に再ログインした場合にのみ表示されます。このチェックボックスは、**[管理（Administration）] > [AAA] > [設定（Settings）]** ページの [送信元IP（Source IP）] セクションにあります。
- ユーザーによるパスワード変更

監査ログを表示するには、次の手順を実行します。

手順

ステップ 1 メインメニューから、**[管理（Administration）]** > **[監査ログ（Audit Log）]** を選択します。

[監査ログ（Audit Log）] ウィンドウが表示されます。

ステップ 2 をクリックして、クエリに基づいて結果をフィルタリングします。

エクスポートアイコン（）を使用すると、ログをCSV形式でエクスポートできます。CSVをエクスポートする場合は、デフォルトのファイル名を使用するか、一意の名前を入力するかを選択できます。

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バナーに表示する免責事項メッセージが必要です。バナーにより、権限を持つユーザーに対してシステムを使用する際の義務を通知したり、権限を持たないユーザーに警告することができます。Cisco Crosswork Planning 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。

手順

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

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（Enable）]** 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）ユーザーがログインする前に免責事項に同意するようにユーザーに求めるには、[ユーザーの同意が必要（Require user consent）] の下の [有効（Enable）] チェックボックスをオンにします。

d) （オプション）免責事項の編集中に、次を実行できます。

- **[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。
- [デフォルトにリセット（Reset to default）] 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。

e) 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）] > [ログイン前の免責事項（Pre-Login Disclaimer）]** の順に選択し、**[有効（Enable）]** チェックボックスをオフにします。

メンテナンスモード設定の管理

メンテナンスモードでは、Cisco Crosswork Planning システムを一時的にシャットダウンする手段が提供されます。Cisco Crosswork Planning は、シャットダウン前にすべてのアプリケーションデータを同期します。システムがメンテナンスモードになるまでに数分かかる場合があります。メンテナンスモードをオフにすると、再起動します。その間は、ログインしたり、Cisco Crosswork Planning アプリケーションを使用したりできません。

⚠

注意

- メンテナンスモードを有効にする前に、Cisco Crosswork Planning システムのバックアップを作成してください。
- システムをメンテナンスモードにする予定があることを他のユーザーに通知し、ログアウトの期限を示します。メンテナンスモードの操作は、一度開始するとキャンセルできません。

手順

ステップ 1 Crosswork をメンテナンスモードにするには、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）] > [メンテナンスモード（Maintenance mode）]** を選択します。

b) [メンテナンスのオン/オフ（Turn on/off maintenance）] スライダを右、すなわちオンの位置にドラッグします。

c) システムがメンテナンスモードに移行しようとしていることを示す警告メッセージが表示されます。[続行（Continue）] をクリックして選択内容を確認します。

（注）
再起動する場合は、システムがメンテナンスモードになった後、Cisco Crosswork データベースが同期できるように 5 分間待ってから続行します。

ステップ 2 メンテナンスモードから再起動するには、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）] > [メンテナンスモード（Maintenance mode）]** を選択します。

b) [メンテナンスのオン/オフ（Turn on/off maintenance）] スライダを左、すなわちオフの位置にドラッグします。

（注）
システムをメンテナンスモードにした状態で再起動または復元を実行した場合、システムはメンテナンスモードで起動し、ポップアップウィンドウでメンテナンスモードをオフにするように求められます。プロンプトが表示されない場合（メンテナンスモード中にシステムが再起動した場合でも）、アプリケーションが正常に機能するように、メンテナンスモードのオンとオフを切り替える必要があります。

ネットワークアクセス構成の更新

[ネットワークアクセス設定（Network access configuration）] セクションでは、SNMP、ログイン、および SAM インターフェイスを介したネットワークアクセスに使用されるパラメータを指定します。これらのパラメータは、特定の要件に合うように変更できます。たとえば、必要に応じて SNMP タイムアウト値を更新できます。

⚠

注意 編集する前に、変更はグローバルに適用され、すべての収集、ジョブ、およびプランファイルに影響することに留意してください。

ネットワークアクセス設定を編集するには、次の手順を実行します。

手順

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）] > [コレクションの設定（Collection settings）] > [ネットワークアクセス設定（Network access configuration）]** を選択します。

ステップ 2 [Edit] ボタンをクリックします。必要なサービスを無効にするように設定を変更すると収集が失敗することを通知する、アラートウィンドウが表示されます。タイムアウトとその他のパラメータのみを変更する場合は、[確認（Confirm）] をクリックします。

ページが編集可能になります。

ステップ 3 要件に応じてファイルを編集します。

ステップ 4 [保存（Save）] をクリックして、変更内容を保存します。

ネットワークアクセス構成ファイルのダウンロード：

ネットワークアクセス設定ファイルをローカルマシンにダウンロードするには、  をクリックします。

コレクタ機能の更新

各コレクタのデータソースと、コレクタによってデータが入力されているテーブル/列は、[コレクタ機能（Collector capability）] ページに表示されます。Cisco Crosswork Planningでは、要件に応じてこれらの設定を更新できます。

⚠

注意 更新する前に、変更はグローバルに適用され、すべての収集、ジョブ、およびプランファイルに影響することに留意してください。

コレクタのテーブルと列の詳細は、次の形式を使用して設定されます。

Collector.table.table-name=ALL/Column list

ここで、ALLは、コレクタによってそのテーブルのすべての列にデータが入力されることを示します。コレクタによって列のサブセットのみが入力される場合は、カンマで区切られた列名のリストとして指定されます。

デフォルト設定を更新するには、次の手順を実行します。

手順

ステップ 1 メインメニューで、**[管理（Administration）] > [設定（Settings）] > [システム設定（System settings）] > [コレクションの設定（Collection settings）] > [コレクタ機能（Collector capability）]** の順に選択します。

ステップ 2 [Edit] ボタンをクリックします。

ページが編集可能になります。

ステップ 3 要件に応じて .txt ファイルを編集します。

ステップ 4 [保存（Save）] をクリックして、変更内容を保存します。

コレクタ機能構成のダウンロード

コレクタ機能の設定をローカルマシンにダウンロードするには、  をクリックします。

デフォルト設定にリセット

設定をデフォルト値にリセットするには、右上の [デフォルト設定のリセット（Reset default config）] ボタンをクリックします。

エージング設定の構成

このトピックでは、非アクティブな回路、ポート、ノード、またはリンクをシステムがネットワークから完全に削除するまで保持する期間を設定する方法について説明します。

デフォルトでは、回路、ポート、ノード、またはリンクがネットワークから消失すると、永久に削除されます。削除された項目を復元するには、その項目を再検出する必要があります。エージングを設定すると、これらの要素がシステムから消去されるまでの保持期間を制御できます。

始める前に

⚠

注意 変更はグローバルに適用され、すべてのコレクション、ジョブ、およびプランファイルに影響することに留意してください。

手順

ステップ 1 メインメニューで、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [コレクション設定（Collection Settings）] > [パージ遅延（Purge delay）]** の順に選択します。

ステップ 2 **[有効（Enable）]** チェックボックスをオンにします。

ステップ 3 該当するフィールドに値を入力します。

- **L3 ポート**：L3 ポートを非アクティブにした後、ネットワークに保持する時間を指定します。
- **L3 ノード**：L3ノードを非アクティブにした後、ネットワークに保持する時間を指定します。
- **L3 回路**：L3 回路を非アクティブにした後、ネットワークに保持する時間を指定します。

（注）
L3 ノードの値は、**L3 ポート** の値と同等かそれ以上にする必要があります。つまり、**L3 回路**の値以上にする必要があります。

ステップ 4 [保存（Save）] をクリックして変更を保存します。

システムは、非アクティブな回路、ポート、ノード、およびリンクを指定された期間保持してから、完全に削除します。

アーカイブされたプランファイル消去の設定

アーカイブされたプランファイルは、ストレージ容量を節約するために Cisco Crosswork Planning で定期的に削除されます。デフォルトでは、ファイルは 30 日間保持されます。

要件に応じて保持期間（日数）を設定するには、次の手順を実行します。

手順

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）] > [コレクションの設定（Collection settings）] > [アーカイブ消去（Archive purge）]** を選択します。

ステップ 2 [アーカイブ保持（Archive retention）] フィールドに、ファイルが削除されるまでの日数を入力します。

たとえば、このフィールドに 40 と入力すると、40 日よりも古いプランファイルが削除されます。

ステップ 3 [保存（Save）] をクリックして、変更内容を保存します。

（注） アーカイブされたプランファイルの消去を無効にするには、[有効（Enable）] チェックボックスをオフにします。無効にすると、最終的にストレージ容量を使い切ってしまうことに注意してください。

スタティック ルートを設定します。

スタティックルートは、データインターフェイス経由で異なるサブセット内のデバイスに到達するために使用されます。

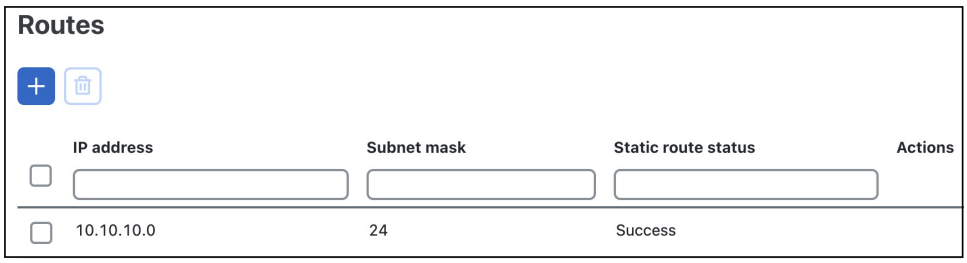
（注） スタティックルートの適用後、Crosswork シェルプロンプトで、**ip rule list** コマンドを実行すると、対応するエントリが表示されます。

スタティックルートの追加

スタティックルートを追加するには、次の手順を実行します。

手順

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）] > [デバイス接続管理（Device connectivity management）] > [ルート（Routes）]** を選択します。



ステップ 2 をクリックします。[ルートIPの追加（Add Route IP）] ウィンドウが表示されます。

ステップ 3 有効な IPv4 または IPv6 サブネットを CIDR 形式で入力します。

ステップ 4 [追加（Add）] をクリックします。

スタティック ルートの削除

スタティックルートを削除するには、次の手順を実行します。

手順

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）] > [デバイス接続管理（Device connectivity management）] > [ルート（Routes）]** を選択します。

ステップ 2 削除するスタティックルートを選択し、をクリックします。

ステップ 3 確認ウィンドウで、[削除（Delete）] をクリックします。

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。