



管理タスクの管理

この章は次のトピックで構成されています。

- [証明書の管理](#) (1 ページ)
- [ユーザーの管理](#) (7 ページ)
- [ユーザー認証の設定 \(TACACS+、LDAP および RADIUS\)](#) (16 ページ)
- [システムとアプリケーションの正常性のモニター](#) (26 ページ)
- [バックアップの管理](#) (31 ページ)
- [システムおよびネットワークアラームの表示](#) (35 ページ)
- [監査ログの表示](#) (35 ページ)
- [ログイン前の免責事項の設定](#) (36 ページ)
- [メンテナンスモード設定の管理](#) (37 ページ)
- [ネットワークアクセス設定の更新](#) (38 ページ)
- [コレクタ機能の更新](#) (39 ページ)
- [エージングの構成](#) (40 ページ)
- [アーカイブされたプランファイルの消去の設定](#) (40 ページ)
- [スタティックルートの設定](#) (41 ページ)

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。

Cisco Crosswork Planningでの証明書の使用方法

Cisco Crosswork とデバイス間の通信やさまざまな Cisco 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。

証明書管理ウィンドウ（[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 Planning が提供するデフォルトの証明書を示します。

図 1: 証明書管理ウィンドウ

Name	Expiration date	Last updated by	Last updated time	Associations	Actions
Crosswork-Device-Syslog	14-Jul-2034 07:37:43 PM IST	Crosswork	16-Jul-2024 07:37:43 PM IST	Device syslog communication	...
Crosswork-Internal-Communication	15-Jul-2029 07:37:09 PM IST	Crosswork	16-Jul-2024 07:37:09 PM IST	Crosswork internal TLS	...
Crosswork-Web-Cert	15-Jul-2029 07:35:57 PM IST	Crosswork	16-Jul-2024 07:35:57 PM IST	Crosswork web server	...

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 内部 TLS	Crosswork Internal Communication	<ul style="list-style-type: none"> • 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 証明書 (Crosswork-Web-Cert) サーバー認証	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 \(19 ページ\)](#) 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。

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)

Cisco Crosswork Planning 7.0 には、[セキュアLDAP通信 (Secure LDAP communication)] オプションのみを適用できます。

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、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)

Crosswork 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

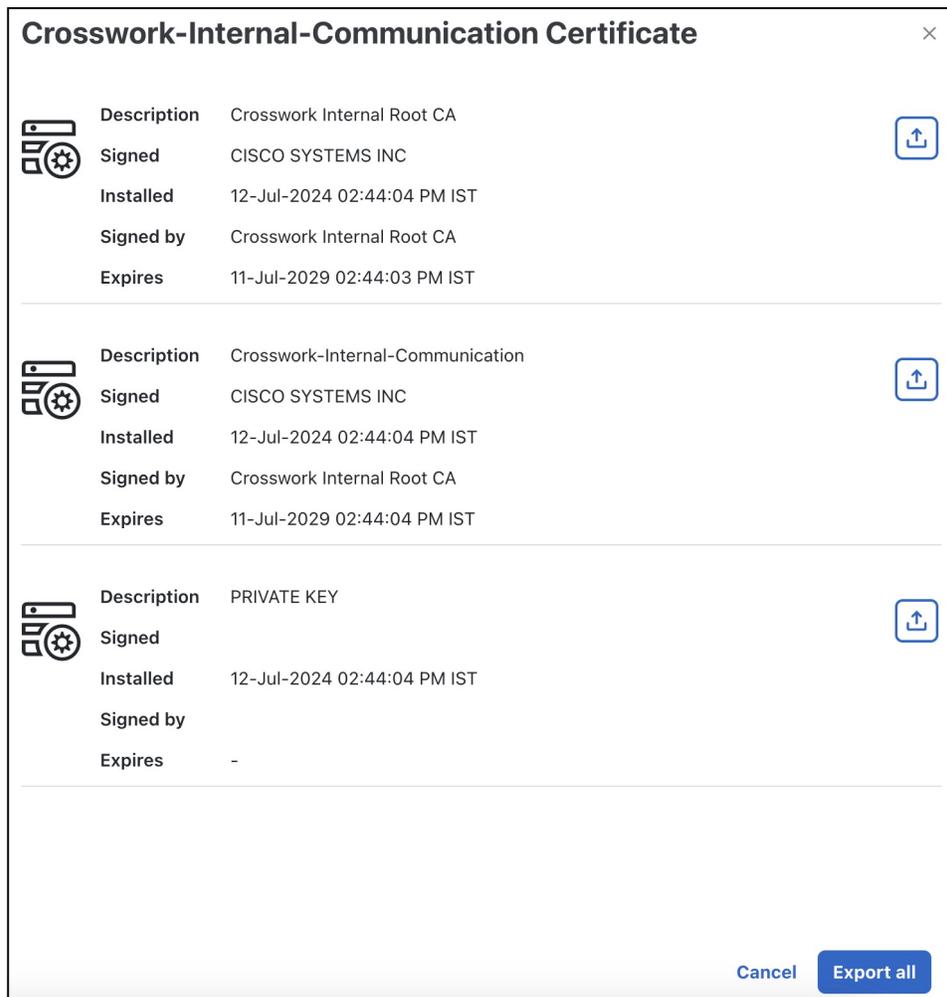
証明書をエクスポートするには、次の手順を実行します。

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。

図 2: 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。

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（「[ユーザーロールの作成（10 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
-  をクリックして必要なユーザーの詳細を入力します。
 - [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。
- 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。
 - 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。
- 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。
 - [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。
- [アクション (Actions)] 列の下での  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（35 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。

- 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 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、Cisco 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。

- Cisco 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 \(7 ページ\)](#)」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。

- 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。
- 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 \(11 ページ\)](#)」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（7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（11ページ）](#)」を参照）。

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的な名前を入力します。
- 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。
- 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。
 - 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 (Administrative Operations)	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、Cisco Crosswork Planning 7.0 で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	<p>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。</p> <p>書き込みアクセス許可では、次のことができます。</p> <ul style="list-style-type: none"> • 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） <p>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。</p>
	API を見る	<p>Cisco Crosswork Planning Design でのビューの管理。</p> <p>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。</p>

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せん。
 - 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 \(35 ページ\)](#)」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。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 \(24 ページ\)](#) 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 \(10 ページ\)](#) 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。



注意

この項の手順に従って操作を行うと、Cisco Crosswork Planning 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。

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（スタンダードアロンまたは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+] タブを選択します。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：

- ➕ アイコンをクリックします。
- 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	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 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。
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。
[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。

フィールド	説明
サービス	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	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、「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。
[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。
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	TACACS+ の認証タイプを選択します。 <ul style="list-style-type: none"> • 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	LDAP ハンドラの名前。

フィールド	説明
[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	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	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。
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 ID (Principal 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。

フィールド	説明
ポリシー 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 Crosswork 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 サーバーに関連するユーザーロールを作成してください。
接続タイムアウト	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、次の手順を実行します：

- 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、次の手順を実行します：

- 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 メインメニューから、[管理 (Administration)]>[AAA]>[サーバー (Servers)]>[RADIUS] タブを選択します。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	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	IPv4DNS 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	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	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。

フィールド	説明
ポリシー 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時、「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。
[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。
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。 <ul style="list-style-type: none"> • 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 \(16 ページ\)](#) 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。



注目

- Cisco Crosswork Planning を再インストールするときは、Cisco Crosswork Planning 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 Planning 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。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) [アイデンティティプロバイダー (Identity 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の名前を入力します。

- [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。

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 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。

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 [並列セッションの数 (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の数 (Number of Parallel sessions per user)] フィールドに関連する値を入力します。

(注)

Cisco Crosswork Planning は、次の数の並列セッションをサポートします。

- 同時ユーザーに対して 5 ~ 400 の並列セッション。並列セッション数を超えると、Cisco Crosswork Planning へのログイン時にエラーが表示されます。
- ユーザー 1 人当たりの同時セッションに対して、1 ~ 400 の並列セッション。

ステップ 5 監査とアカウントिंग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モニター

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モニター

[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 3:[Crossworkの正常性 (Crosswork Health)]タブ

Component	Status	Microservices	Health Indicators	Recommendation
Platform Infrastructure	Healthy	23	23 Green, 0 Red, 0 Yellow	None
Crosswork Planning Infrastructure	Healthy	2	2 Green, 0 Red, 0 Yellow	None
Design	Healthy	6	6 Green, 0 Red, 0 Yellow	None
Collector	Healthy	8	8 Green, 0 Red, 0 Yellow	None

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 4:[マイクロサービス (Microservices)]タブ

Status	Name	Up time	Recommendation	Description	Actions
Healthy	cw-ipsec	15d 17h 21m 12s	None		...
Healthy	nats	15d 17h 16m 17s	None		...
Healthy	robot-orch	15d 17h 15m 19s	None		...
Healthy	robot-ui	15d 16h 57m 20s	None		...
Healthy	cas	15d 16h 57m 54s	None		...
Healthy	docker-registry	15d 17h 2m 2s	None		...
Healthy	cw-data-retention-service	15d 16h 59m 48s	None		...
Healthy	cw-fault-alarm-rest-service	15d 17h 0m 3s	None		...
Healthy	cw-views-service	15d 16h 59m 35s	None		...
Healthy	cw-fault-alarm-processing-service	15d 16h 59m 18s	None		...
Healthy	cw-distributed-cache	15d 17h 1m 15s	None		...

[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。

また、Cisco Crosswork アプリケーションまたは Cisco Crosswork Platform Showtech サービスログをすべてダウンロードし、[アプリケーションの詳細 (Application Details)] ウィンドウからインストール関連の操作を実行することもできます。上部にある ... > [アプリケーションの詳細の表示 (View application details)] をクリックして、[アプリケーションの詳細 (Application Details)] ウィンドウを開きます。

システム正常性の確認の例

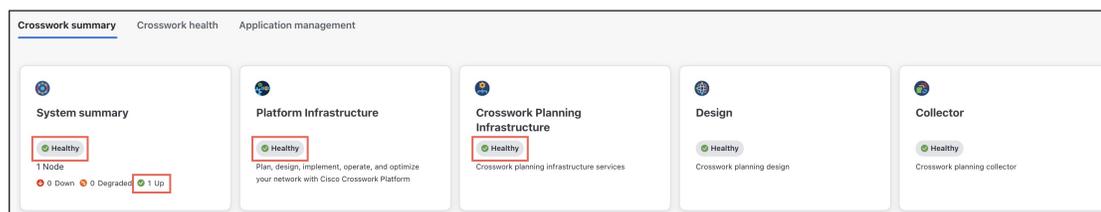
この例では、さまざまなウィンドウや、正常な Crosswork システムで確認すべき領域を検討します。

手順

ステップ 1 システム全体の正常性を確認します。

- 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。
- 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。

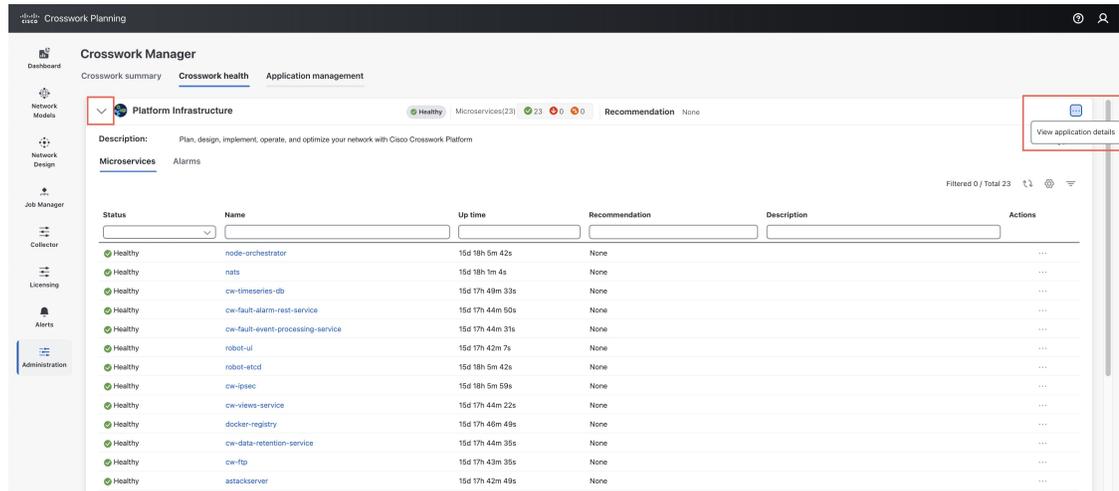
図 5: [Crosswork の概要 (Crosswork Summary)]



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。

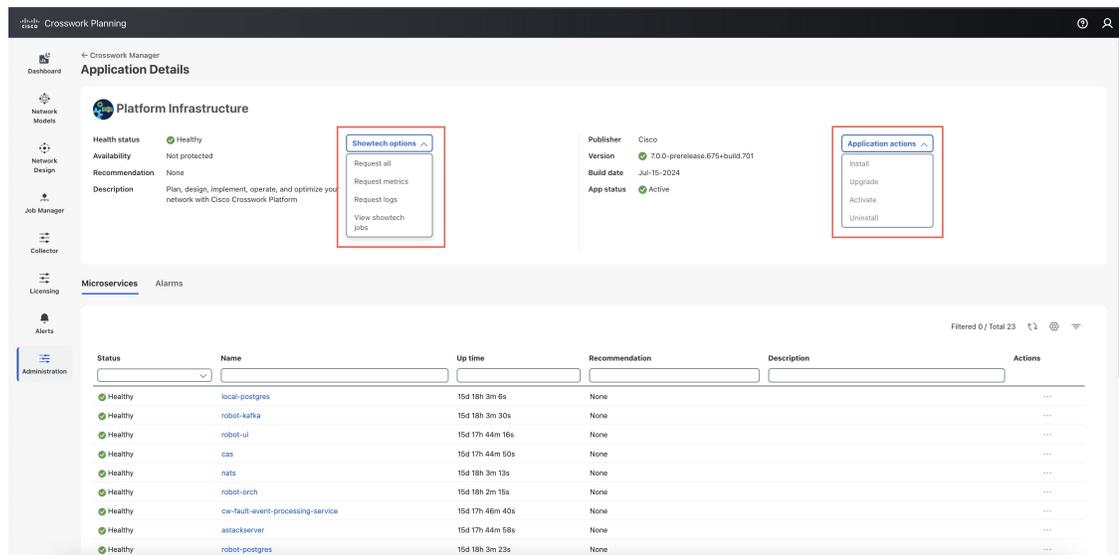
- a) [Crosswork の正常性 (Crosswork Health)] タブをクリックします。
- b) [Crossworkプラットフォームインフラストラクチャ (Crosswork Platform Infrastructure)] の行を展開し、**...** をクリックして [アプリケーション詳細を表示 (View application details)] を選択します。

図 6: [Crosswork の正常性 (Crosswork Health)]



- c) [アプリケーションの詳細 (Application Details)] ウィンドウから、マイクロサービスの詳細をチェックおよび確認し、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。

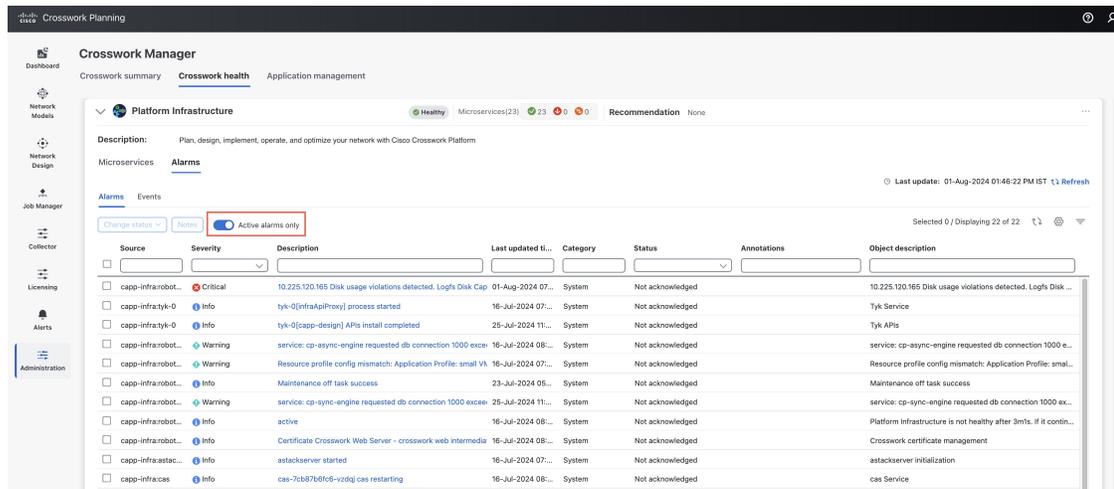
図 7: アプリケーションの詳細 (Application Details)



ステップ3 マイクロサービスに関連するアラーム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。

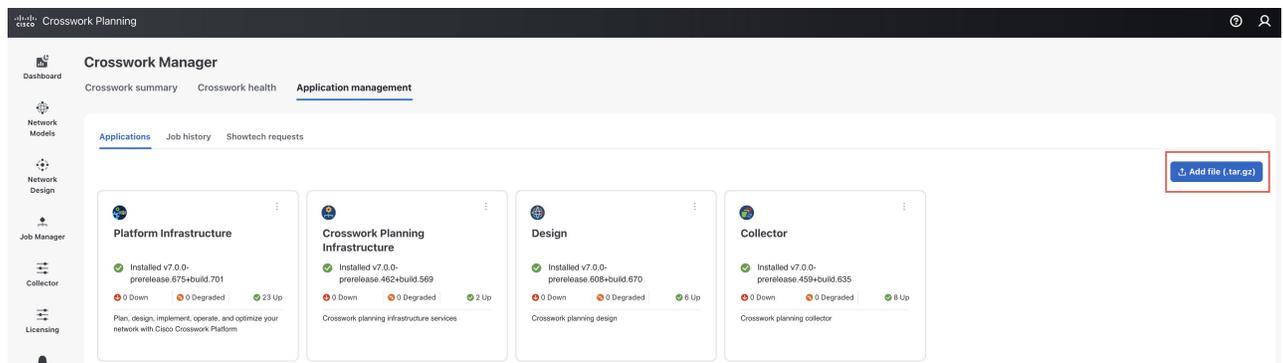
図 8: アラーム



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) メインメニューから、[管理 (Administration)] > [Crosswork Manager] > [アプリケーション管理 (Application Management)] タブを選択し、[アプリケーション (Applications)] をクリックします。このウィンドウには、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。[ファイル (.tar.gz) の追加 (Add File (.tar.gz))] をクリックして、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 9: [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、 Cisco Crosswork Planning バックアップと復元の管理 (32 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 (災害後の Cisco Crosswork Planning の復元 (34 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、 災害後の Cisco Crosswork Planning の復元 (34 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)] (注) このオプションは、Cisco Crosswork Planning 7.0 ではサポートされていません。	

Cisco Crosswork Planning バックアップと復元の管理

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。
 - Crosswork 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。

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。

- 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。
- [接続先 (Destination)] をクリックして、[接続先の追加 (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) 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)]>[データのバックアップ (Data backup)]をクリックして、宛先サーバーの詳細が事前に入力された [データのバックアップ (Data Backup)]ダイアログボックスを表示します。
- 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) マイクロサービスの問題があっても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。
- 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 (Remote path)]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)]をクリックして、Cisco Crosswork Planningにバックアップを完了するのに十分な空きリソースがあることを確認します。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。
- 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 (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。

[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。

- 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：[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。

(注)

アップロードは、認証情報が正しくない、宛先ディレクトリが無効、サーバーのスペースが不足しているなど、複数の問題が原因で失敗することがあります。[バックアップのアップロード (Upload backup)]ボタンをクリックする前に、問題を調査して修正します (たとえば、古いバックアップをクリーンアップしてスペースを解放するか、[宛先 (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)。

災害後の Cisco Crosswork Planning の復元

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 7.0 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。

データのディザスタリカバリを実行する場合は、次の点に注意してください。

- [災害後のデータ復元 (Data Disaster Restore)] を実行する前に、(データバックアップを作成したときに) 古い Cisco Crosswork Planning サーバーに存在していた正確なバージョンのアプリケーションを新しい Cisco Crosswork Planning サーバーにインストールして使用できるように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、復元ジョブが失敗する可能性があります。
- 新しい Cisco Crosswork Planning サーバーは、バックアップの作成時に使用したのと同じ Cisco Crosswork Planning のソフトウェアイメージを使用する必要があります。異なるバージョンのソフトウェアを使用して作成されたバックアップを使用してサーバーを復元することはできません。
- 災害が発生する前のシステムの状態を回復できるように、バックアップを最新の状態に保ちます。復元操作では、バックアップが作成されたときにインストールされていたすべてのアプリケーションを復元します。前回のバックアップ以降に追加の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スマートライセンス登録は、災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。

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。このファイルは通常は作成した最新のバックアップファイルです。Cisco Crosswork Planning のバックアップファイル名の形式は次のとおりです。

```
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

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。

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。

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。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。

- [有効 (Enable)] チェックボックスをオンにします。
- 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。
- (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。
- (オプション) 免責事項の編集に、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、行った変更が Cisco Crosswork Planning ログインプロンプトの前にどのように表示されるのかを確認できます。

[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)] を選択し、[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設定の更新

[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)] > [収集の設定 (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設定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 メインメニューから、[管理 (Administration)] > [設定 (Settings)] > [システム設定 (System settings)] > [収集の設定 (Collection settings)] > [コレクタ機能 (Collector capability)] を選択します。

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。

コレクタ機能設定のダウンロード

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。

エージングの構成

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、再検出する必要があります。消失したこれらの要素がネットワークから完全に削除されるまで Cisco Crosswork Planning がこれらの要素を保持する期間を設定するには、次の手順を実行します。



注意 設定する前に、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。

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)] > [収集の設定 (Collection Settings)] > [ページ遅延 (Purge delay)] を選択します。

ステップ 2 [有効 (Enable)] チェックボックスをオンにして、エージングを有効にします。

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 port)] : L3 ポートが非アクティブになった後に、ネットワーク内で保持する必要がある期間を入力します。
- [L3ノード (L3 node)] : L3 ノードが非アクティブになった後に、ネットワーク内で保持する必要がある期間を入力します。
- [L3回路 (L3 circuit)] : L3 回路が非アクティブになった後に、ネットワーク内で保持する必要がある期間を入力します。

(注)

[L3ノード (L3 node)] の値は [L3ポート (L3 port)] の値以上である必要があります。すなわち、[L3ポート (L3 port)] の値は [L3回路 (L3 circuit)] の値以上である必要があります。

アーカイブされたプランファイルの消去の設定

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)] > [収集の設定 (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の設定

スタティックルートは、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。

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。

Routes				
	IP address	Subnet mask	Static route status	Actions
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
<input type="checkbox"/>	10.10.10.0	24	Success	

- 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。