



起動と実行（インストール後）

ここでは、次の内容について説明します。

- [はじめる前に（1 ページ）](#)
- [設定のワークフロー（3 ページ）](#)
- [ログインとログアウト（5 ページ）](#)

はじめる前に

Cisco Crosswork アプリケーションの使用を開始する前に、次の基本概念を理解し、計画と情報収集の手順を完了することをお勧めします。

- **ユーザーロール**：シスコでは、ロールベースのアクセス制御を使用して、ユーザーに対してそのユーザーが業務を遂行するために必要なソフトウェア機能のみに限定することをお勧めします。デフォルトでは、作成するすべての新しいユーザーに完全な管理権限が備わります。すべてのユーザーに同じ権限を付与する場合を除き、ユーザーロールのシステムを計画し、それらを作成して、作成したユーザープロファイルに割り当てる必要があります。
- **ユーザーアカウント**：ベストプラクティスとして、すべてのユーザーに個別のアカウントを作成し、システム上のユーザーアクティビティの監査レコードを作成することをお勧めします。Crosswork アプリケーションを使用するユーザーのリストを作成します。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。Crosswork は、多くの TACACS+ および LDAP サーバーとの統合もサポートしており、ユーザーの役割とアカウントを集中管理できます。詳細については、[ユーザー認証の設定（TACACS+、LDAP および RADIUS）](#) を参照してください。
- **クレデンシャルプロファイル**：Cisco Crosswork がデバイスにアクセスするか、またはプロバイダと対話するには、クレデンシャルを提示する必要があります。必要になるたびにクレデンシャルを入力する代わりに、クレデンシャルプロファイルを作成すると、この情報を安全に保存できます。プラットフォームは、アクセスプロトコルのタイプごとに一意のクレデンシャルをサポートし、複数のプロトコルとそれらに対応するクレデンシャルを 1 つのプロファイルにバンドルできます。同じクレデンシャルを使用するデバイスは、クレデンシャルプロファイルを共有できます。たとえば、特定の建物内のすべてのルータが

単一の SSH ユーザー ID とパスワードを共有する場合、Cisco Crosswork がそれらにアクセスして管理できるように単一のクレデンシャルプロファイルを作成できます。

クレデンシャルプロファイルを作成する前に、デバイスをモニターおよび管理するために使用するアクセスクレデンシャルとサポートされているプロトコルを収集する必要があります。デバイスの場合は、ユーザー ID、パスワード、および SNMP v2 の読み取り/書き込みコミュニティ文字列、SNMPv3 認証と権限タイプなどの追加データが含まれます。他のタイプのプロバイダ（NSO、SR-PCE、ストレージ、アラート、および WAE）の場合、これには常にユーザー ID、パスワード、および接続プロトコルが含まれます。これらを使用してクレデンシャルプロファイルを作成します。

- **タグ**：タグは、デバイスをグループ化するためにデバイスに添付できる単純なテキスト文字列です。Cisco Crosswork には、ネットワークデバイスのグループ化にそのまま使用できるタグの短いリストが付属しています。独自のタグを作成してさまざまな目的でデバイスを識別、検索、およびグループ化することができます。

システムの設定時に作成するカスタムタグの予備リストを計画しておくことで、最初のオンボーディング時にデバイスをグループ化するために使用できます。最初にタグの完全なリストを用意する必要はありません。後でさらに追加することもできます。ただし、使用する予定のタグはすべて、必要になる前に配置する必要があります。それ以外の場合は、手動で戻って、使用したい場所に追加する必要があります。詳細については、[Cisco NSO プロバイダの追加](#)を参照してください。

- **プロバイダ**：Cisco Crosswork アプリケーションは、設定変更、セグメントルーティングパスの計算などのさまざまなタスクに関して Cisco Network Services Orchestrator（NSO）や SR-PCE などの外部サービスに依存しています。Crosswork アプリケーション間での情報のアクセスと再利用を管理するには、外部サービスごとにプロバイダ（NSO や SR-PCE など）を設定する必要があります。プロバイダファミリーによって、プロバイダが Cisco Crosswork に提供するサービスのタイプと、そのサービスに固有のパラメータが決まります。それらのサービスタイプとパラメータを設定する必要があります。プロバイダーの設定に必要なパラメータは、使用する Crosswork アプリケーションのタイプによって異なります。プロバイダを設定する前に、各 Crosswork アプリケーションの要件を確認して収集することが重要です。詳細については、「[プロバイダファミリーについて](#)」および「[プロバイダの依存関係](#)」を参照してください。

- Cisco Network Services Orchestrator（Cisco NSO）は、すべての Cisco Crosswork アプリケーションのインストールで使用されるデフォルトのプロバイダです。そのため、Cisco NSO の IP アドレスまたはホスト名、ポート、およびプロトコル、ならびに通信するために使用するクレデンシャルを収集する必要があります（クレデンシャルプロファイルとし追加する必要があります）。
- Crosswork 最適化エンジンを使用する場合は、デバイスを検出し、ポリシー設定をデバイスに配布するために、少なくとも Cisco SR-PCE プロバイダを定義する必要があります。使用する自動オンボーディングモードとデバイス クレデンシャル プロファイルを決定する必要があります（デバイスを自動オンボーディングする場合）。詳細については、「[Cisco SR-PCE プロバイダの追加](#)」を参照してください。

- **デバイス** : UI、CSV ファイル、API、SR-PCE 検出、または ZTP を使用してデバイスをオンボーディングできます。デバイスのオンボーディング方法によって、Crosswork でデバイスを設定するために必要な情報のタイプが決まります。また、Crosswork は NSO にデバイス設定を転送できるため、NSO プロバイダのプロビジョニング方法を変更できます。詳細については、「[インベントリへのデバイスの追加](#)」を参照してください。
- **外部データ送信先** : Cisco Crosswork は Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) のコントローラとして機能します。Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) に他のデータ送信先にデータを転送させることを計画しているオペレータは、それらの接続先で必要な形式とその他の接続要件を認識しておく必要があります。詳細については、「[Cisco Crosswork Data Gateway](#)」を参照してください。
- **ラベル** : ラベルは、プレイブックを実行できるユーザーを制限するために Crosswork Change Automation で使用されます。たとえば、下位レベルのオペレータがプレイブックのチェックを実行できるようにする一方で、ラベルを使用してネットワークデバイスの設定に変更を加えるような、より複雑なプレイブックまたは影響力のあるプレイブックを実行しないようにします。
- Crosswork Health Insights を使用する場合は、**KPI (主要業績評価指標) プロファイル**を使用してネットワークの正常性をモニターします。ネットワークでのデバイスの使用方法に基づいて、固有のパフォーマンス条件を確立できます。KPI をグループ化して KPI プロファイルを形成することができます。モニターする予定のデータと、Health Insights の設定時に確立するパフォーマンス目標を把握しておくで役立ちます。
- Crosswork Service Health アプリケーションをインストールする場合は、提供されているサンプルを確認して、ネットワーク内のサービスをモニターする方法を決定する必要があります。

デバイス、クレデンシャルプロファイル、タグ、プロバイダリストをスプレッドシート形式でキャプチャし、そのスプレッドシートを CSV 形式に変換してから、使用する Crosswork アプリケーションにインポート機能を使用して一括でアップロードできます。ユーザーインターフェイスで対応する場所にある [インポート (Import)] アイコンをクリックすると、これらのリストそれぞれの CSV テンプレートにアクセスできます。エクスポート先のパスとファイル名を選択するように求められたら、[テンプレートのダウンロード (Download template)] リンクを選択します。

設定のワークフロー


Cisco Crosswork を使用するための最初の手順は、システムを使用できるように準備することです。次の表に、以下の各タスクを実行する際に役立つトピックを示します。



- (注) このワークフローは、Cisco Crosswork Data Gateway がすでにインストールされていることを前提としています。インストール手順については、最新バージョンの『*Cisco Crosswork Network Controller 5.0 Installation Guide*』を参照してください。

「はじめる前に」で説明した推奨される計画手順を実行できた場合は、このワークフローの各手順を完了するために必要なすべての情報が必要です。

表 1: Cisco Crosswork を開始する前に完了すべきタスク

手順	操作
1. デバイスが通信用とテレメトリ用に適切に設定されていることを確認します。	次のガイドラインと設定例を参照してください。 新しいデバイスのテレメトリの前提条件 Cisco NSO デバイスの設定例
2. (オプション) セットアップが Cisco NSO LSA 展開の場合は、LSA を有効にします。	階層化されたサービスアーキテクチャ (LSA) を有効にする の手順に従います。
3. クレデンシャルプロファイルを作成します。	クレデンシャルプロファイルの作成 の手順に従います。
4. プロバイダーを追加します。	プロバイダの追加 についての手順に従います。
5. プロバイダーとの通信を検証します。	プロバイダの詳細の取得 の手順を使用して、プロバイダの到達可能性を確認します。
6. タグをインポートまたは作成します。	タグをインポートするには、 タグのインポート の手順を実行します。 タグを作成するには、 タグの作成 の手順を実行します。
7. 希望する方法でデバイスをオンボーディングします。	「 インベントリへのデバイスの追加 」を参照してください。
8. Crosswork Data Gateway の設定	データを収集するための Crosswork Data Gateway の設定 の手順を実行します。
9. デバイスと Cisco Crosswork の通信を検証します。	[デバイス (Devices)] ウィンドウを確認します (「 ネットワーク デバイスの管理 」を参照)。オンボーディングしたすべてのデバイスが到達可能である必要があります。 [到達可能性の状態 (Reachability State)] が  (到達不能)、  (低下)、または  (不明) としてマークされているデバイスを調査する場合は  をクリックします。
10. (オプション) 監査のために送信元 IP を有効にします。	監査とアカウンティングのためにユーザーの IP アドレスを記録する場合は、 AAA サーバー設定を設定 を参照してください。

手順	操作
11. (オプション) 追加のユーザーアカウントとユーザーロールを作成します。	ユーザーの管理 と ユーザーロールの作成 の手順を実行します。
12. (オプション) 追加のクレデンシャルプロファイルとプロバイダーをインポートまたは作成します。	プロバイダーをインポートするには、 プロバイダーのインポート の手順を実行します。 プロバイダーを作成するには、 UIを使用したプロバイダーの追加 の手順を実行します。
13. (オプション) 要件に応じてデバイスを論理的にグループ化します。	デバイスグループの作成と変更 の手順を実行します。
14. (オプション) トポロジの表示設定を行います。	マップの表示設定の定義 と リンク帯域幅使用率の色分けしきい値の定義 の手順を実行します。

ログインとログアウト

Cisco Crosswork のユーザーインターフェイスはブラウザベースです。サポートされているブラウザのバージョンについては、『[Cisco Crosswork Network Controller 5.0 Installation Guide](#)』を参照してください。



注目

- Cisco Crosswork は、ログイン試行の失敗が繰り返された後、指定された期間、ユーザーをロックアウトします。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。ユーザーは、有効なログイン情報を入力するまでロックアウトされたままになります。ログイン試行の失敗回数とロックアウト時間は、管理者が[ローカルパスワードポリシー (Local Password Policy)] で設定します。詳細については、[AAA サーバー設定を設定](#)を参照してください。
- 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、Crosswork ログインページは表示されません。
- ユーザーが同じクライアントから (複数のタブ/ウィンドウを介して) 複数のセッションを開いており、そのセッションに対していずれかのウィンドウからログアウト/セッションの終了を実行すると、そのウィンドウにログアウト画面が表示され、他のすべてのタブ/ウィンドウに次のエラーメッセージが表示されます。「セッションは終了しました。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 1 Web ブラウザを開き、次を入力します。

`https://<Crosswork Management Network Virtual IP (IPv4)>:30603/`

または

`https://[<Crosswork Management Network Virtual IP (IPv6)>]:30603/`


（注） URL 内の IPv6 アドレスは括弧で囲む必要があります。

ブラウザから Cisco Crosswork に初めてアクセスした場合、一部のブラウザではサイトが信頼できないという警告が表示されます。この場合は、指示に従ってセキュリティ例外を追加し、サーバーから自己署名証明書をダウンロードします。これを実行すると、ブラウザはその後のすべてのログインで信頼できるサイトとして Cisco Crosswork サーバーを受け入れます。

ステップ 2 Cisco Crosswork のブラウザベースのユーザーインターフェイスにログインウィンドウが表示されます。ユーザー名とパスワードを入力します。

デフォルトの管理者ユーザー名とパスワードは **admin** です。このアカウントは、インストール時に自動的に作成されます（「インストール時に作成された管理ユーザー」を参照）。このアカウントの初期パスワードは、インストールの検証時に変更する必要があります。シスコでは、デフォルトの管理者クレデンシャルを安全に保管し、通常のログインには使用しないことを強くお勧めしています。代わりに、適切な権限を持つ新しいユーザーロールを作成し、それらのロールに新しいユーザーを割り当てます。作成するユーザーの 1 人以上に「管理者」ロールを割り当てる必要があります。

ステップ 3 [ログイン (Log In)] をクリックします。

ステップ 4 ログアウトするには、メインウィンドウの右上にある  をクリックし、[ログアウト (Log out)] を選択します。

Crosswork UI の言語を日本語に変更できます。デバイス名やサーバー名などのユーザー固有の値は、引き続き英語であることに注意してください。言語を変更するには、ログイン画面から希望の言語を選択します。

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。