管理

ここでは、次の内容について説明します。

アダプタの管理

外部ターゲットシステムと連携するには、CWM にアダプタが必要です。アダプタは、CWM API を使用して管理できます。アダプタの処理には、次の API エンドポイントを使用できます。

- `GET/adapter`：CWM アプリケーションに存在するアダプタのリストを取得します。
- `POST/adapter`：アダプタの **.tar** ファイルを CWM ストレージにアップロードします。
- `GET/adapter/{adapterId}`：CWM アプリケーションに存在する特定のアダプタの詳細を取得します。これには、アダプタで使用可能なすべてのアクティビティの一覧表示が含まれます。
- `PUT/adapter/{adapterId}`：既存のアダプタファイルを新しいアダプタバージョンで更新します。
- `DELETE/adapter/{adapterId}`：CWM アプリケーションからアダプタを削除します。
- `POST/adapter/{adapterId}/deploy`：アップロードされたアダプタファイルに基づいてシステムにアダプタを展開します。

アダプタのインストール

CWM アダプタは、**.tar** インストールファイルに含まれています。ワークフローで使用するには、事前にストレージにアップロードしてシステムに展開する必要があります。その方法について説明します。

アダプタファイルのアップロード

アダプタを展開する前に、アダプタの **.tar** ファイルを CWM ストレージにアップロードする必要があります。

ステップ 1 最新のアダプタ インストール ファイルを取得するか、独自のアダプタを作成します。

ステップ 2 CWM にログインし、左側のナビゲーションメニューから [Swagger] アイコンをクリックします。

ステップ 3 [adapters] セクションで、`POST/adapter` エンドポイントをクリックして展開します。エンドポイント内で、[試す（Try it out）] をクリックします。

ステップ 4 表示されるサブセクションで、[ファイルの選択（Choose File）] をクリックし、アダプタの **.tar** インストールファイルを選択して [アップロード（Upload）] をクリックし、[実行（Execute）] をクリックします。

サーバーの応答コードが `201` の場合、アダプタファイルは CWM データベースに正常にアップロードされています。

アダプタの展開

ステップ 1 CWM API の [アダプタ（adapters）] セクションで、`GET/adapter` エンドポイントをクリックして展開します。エンドポイント内で、[試す（Try it out）] と[実行（Execute）] をクリックします。

ステップ 2 サーバーの応答本文から、アップロードしたアダプタの `id` フィールドの値をコピーします。

ステップ 3 CWM API の [アダプタ（adapters）] セクションで、`POST/adapter/{adapterId}/deploy` エンドポイントをクリックして展開します。

ステップ 4 エンドポイント内で、[試す（Try it out）] をクリックします。[アダプタID（Adapter ID）] フィールドにアダプタ ID を貼り付けます。

ステップ 5 [createWorker] フィールドで、`createWorker` パラメータを `true` に設定できます。これにより、アダプタ ID と同じ名前のワーカーが作成されます。

ステップ 6 [実行（Execute）] をクリックします。

サーバーの応答コードが `201` の場合、アダプタプラグインは正常にインストールされています。

アダプタの削除

アダプタをストレージから完全に削除して「アンインストール」するには、次の手順を実行します。

ステップ 1 CWM API の [アダプタ（adapters）] セクションで、`GET/adapter` エンドポイントをクリックして展開します。エンドポイント内で、[試す（Try it out）] と[実行（Execute）] をクリックします。

ステップ 2 サーバーの応答本文から、アップロードしたアダプタの `id` フィールドの値をコピーします。

ステップ 3 CWM API の [アダプタ（adapters）] セクションで、`DELETE/adapter/{adapterId}` エンドポイントをクリックして展開します。

ステップ 4 エンドポイント内で、[試す（Try it out）] をクリックします。[アダプタID（Adapter ID）] フィールドにアダプタ ID を貼り付けます。

ステップ 5 [実行（Execute）] をクリックします。

ワーカーの管理

ワーカーは、ワークフロー定義とアダプタコードで定義されたアクションを実行するプロセスです。**オペレータ**ガイドで説明されているように CWM UI を使用してワーカーを管理できます。または以下で説明しているように CWM API を使用して管理できます。

ワーカーを管理するための次のアクションを使用できます。

- `GET/worker`：CWM アプリケーションに存在するワーカーのリストを取得します。
- `POST/worker`：CWM アプリケーション内に新しいワーカーを作成します。
- `GET/worker/{workerName}`：CWM アプリケーションに存在する特定のワーカーの詳細を取得します。
- `PUT/worker/{workerName}`：既存のワーカーを新しいパラメータ値で更新します。
- `DELETE/worker/{workerName}`：CWM アプリケーションからワーカーを削除します。
- `POST/worker/{workerName}/start`：アプリケーションで作成されたワーカーをアクティブにします。
- `POST/worker/{workerName}/stop`：アプリケーションで作成されたワーカーを非アクティブ化します。

ワーカーの作成

ステップ 1 CWM にログインし、左側のナビゲーションメニューから [Swagger] アイコンをクリックします。

ステップ 2 CWM API の [ワーカー（workers）] セクションで、POST/worker エンドポイントをクリックして展開します。エンドポイント内で、[試す（Try it out）] をクリックします。

ステップ 3 [ワーカーデータ（Worker data）] フィールドに、必要な値を入力します。

a) [activities]：展開されたアダプタの ID または特定のアダプタアクティビティを貼り付けます。

b) [startWorker]：`true` に設定します。

c) [workerName] : ワーカーの名前を指定します。

ステップ 4 [実行（Execute）] をクリックします。

ワーカーの開始

ステップ 1 CWM API の [ワーカー（workers）] セクションで、`POST/{workerName}/start` エンドポイントをクリックして展開します。エンドポイント内で、[試す（Try it out）] をクリックします。

ステップ 2 次の**パラメータ**のフィールドに、必要な値を入力します。

a) [開始するワーカーの名前（Name of a worker to start）] : 開始するワーカーの名前を貼り付けます。

b) [forceReload]: ワーカーを強制的に起動する場合は `true` に設定します。

ステップ 3 [実行（Execute）] をクリックします。

ワーカーの停止

ステップ 1 CWM API の [ワーカー（workers）] セクションで、`POST/{workerName}/stop` エンドポイントをクリックして展開します。エンドポイント内で、[試す（Try it out）] をクリックします。

ステップ 2 次の**パラメータ**のフィールドに、必要な値を入力します。

a) [停止するワーカーの名前（Name of a worker to stop）] : 停止するワーカーの名前を貼り付けます。

b) [forceStop]: ワーカーを強制的に停止する場合は `true` に設定します。

ステップ 3 [実行（Execute）] をクリックします。

ワークフローの管理

ワークフローインスタンスは、**オペレータ**ガイドで説明されているように CWM UI で、または CWM API を使用して管理できます。

- `POST/workflow`：CWM アプリケーション内に新しいワークフローインスタンスを作成します。
- `GET/workflow/list`：CWM アプリケーションに存在するアダプタのリストを取得します。

- `GET/workflow/{id}`：CWMアプリケーションに存在する特定のワークフローの詳細を取得します。
- `PUT/workflow/{id}`：既存のワークフローを新しいワークフロー定義で更新します。
- `DELETE/workflow/{id}`：選択したワークフローをCWMアプリケーションから削除します。

（注） ワークフローを管理するには、CWM UIを使用することが推奨されます。詳細については、オペレータガイドを参照してください。

リソースとシークレットの管理

CWMでは、アダプタは、他のシステムやアプリケーションなどの外部エンティティでアクションを実行できるようにするアクティビティを定義します。これらのエンティティは、ほとんどの場合、通常は接続と認証データを必要とするAPIを介して統合されます。CWMは、アクティビティがワークフローで使用されるときに、接続エンドポイントの詳細と認証データを実行時に渡すことができるフレームワークを提供します。したがって、ワークフローを実行するオペレータは、IPアドレス、ポート、ユーザー名、パスワードなど、これらのシステム（リソース）の詳細を知らない場合があります。

CWMは、データベース内のリソースとシークレットを安全に処理し、それぞれのIDでそれらを識別するためのフレームワークを提供します。ワークフローインスタンスを実行する場合は、リソースIDのみを渡す必要があり、残りのデータはリソースマネージャによってアダプタに送信されます。オペレータの介入やアダプタ開発者の追加開発は必要ありません。

リソースおよびシークレットのタイプ

リソースおよびシークレットのタイプは、ユーザーが作成したリソースとシークレットをタイプ別に整理するために使用される入れ物と考えることができます。タイプは特定のアダプタ内で定義され、アダプタのインストール時に自動的にシステムに追加されます。
`GET/secret/type/{type}` APIエンドポイントを使用して、特定のタイプに属するシークレットを一覧表示できます。

シークレットAPIエンドポイント

シークレットを管理するための次のアクションを使用できます。

- `GET/secret`：CWMアプリケーションに存在するシークレットのリストを取得します。
- `POST/secret`：CWMアプリケーション内に新しいシークレットを作成します。
- `GET/secret/type/{type}`：CWMアプリケーションに存在する、特定のタイプに属するシークレットを一覧表示します。

- `GET/secret/types`：CWM アプリケーションに存在するシークレットのタイプのリストを取得します。
- `GET/secret/{id}`：既存のシークレットの詳細を取得します。
- `DELETE/secret/{id}`：CWM アプリケーションからシークレットを削除します。
- `PATCH/secret/{id}`：CWMアプリケーションに存在するシークレットを新しいパラメータ値で更新します。

リソース API エンドポイント

リソースを管理するための次のアクションを使用できます。

- `GET/resource`：CWM アプリケーションに存在するリソースのリストを取得します。
- `POST/resource`：CWM アプリケーションに新しいリソースを作成します。
- `GET/resource/{resourceId}`：CWM アプリケーションに存在する特定のリソースの詳細を取得します。
- `PUT/resource/{resourceId}`：既存のリソースを新しいパラメータ値で更新します。
- `DELETE/resource/{resourceId}`：CWM アプリケーションからリソースを削除します。
- `GET/resourceType`：CWM アプリケーションに存在するリソースタイプのリストを取得します。
- `GET/resourceType/{resourceId}`：既存のリソースタイプの詳細を取得します。

シークレットの作成

ステップ 1 CWM にログインし、左側のナビゲーションメニューから [Swagger] アイコンをクリックします。

ステップ 2 CWM API の [シークレット（secrets）] セクションで、[POST /secret] エンドポイントをクリックして展開します。

ステップ 3 エンドポイント内で、[試す（Try it out）] をクリックし、[シークレット入力（Secret input）] フィールドにデータを入力します。入力の例を次に示します。

```
{
"secret": {
"username": "admin",
"password": "admin"
},
"secretId": "NSOSecret",
"secretType": "basicAuth"
}
```

ステップ 4 [実行（Execute）] をクリックします。

サーバーの応答コードが 201 の場合、シークレットは正常に作成されており、シークレットを関連付けるリソースの作成を開始できます。

リソースの作成

ステップ 1 CWM API の [リソース（resources）] セクションで、`POST /resource` エンドポイントをクリックして展開します。

ステップ 2 エンドポイント内で、[試す（Try it out）] をクリックし、[リソース入力（Resource input）] フィールドにデータを入力します。入力の例を次に示します。

```
{
    "resource": {
        "scheme": "http",
        "host": "127.0.0.1",
        "port": 8080
    },
    "resourceId": "NSOLocal",
    "resourceType": "cisco.nso.resource.v1.0.0",
    "secretId": "NSOSecret"
}
```

ステップ 3 [実行（Execute）] をクリックします。

サーバー応答コードが 201 の場合、リソースは正常に作成されています。

NxF を介したユーザーアクセス

CWM では、NextFusion（NxF）を介してユーザーアクセスと権限を管理できます。NxF はセキュリティの追加レイヤを追加し、単一認証エージェントとして機能するため、ローカル、LDAP、および SAML の各ユーザーを共有します。

ユーザー、ロールおよび権限

現在、1 つのロールと権限タイプ（管理者）のみがサポートされています。すべてのユーザーは、デフォルトで管理者権限に関連付けられています。

通常のユーザーで構成される大きなグループに CWM へのアクセスを許可するには、環境に応じて、LDAP または SAML SSO プロトコル（両方を同時に使用できます）を介したユーザー認証を設定します。

権限の範囲

管理者ロールには、CWMとそのすべての機能へのフルアクセス権があります。管理者は、ユーザーのアクセスと権限を制御できます。管理者権限を持つすべての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。

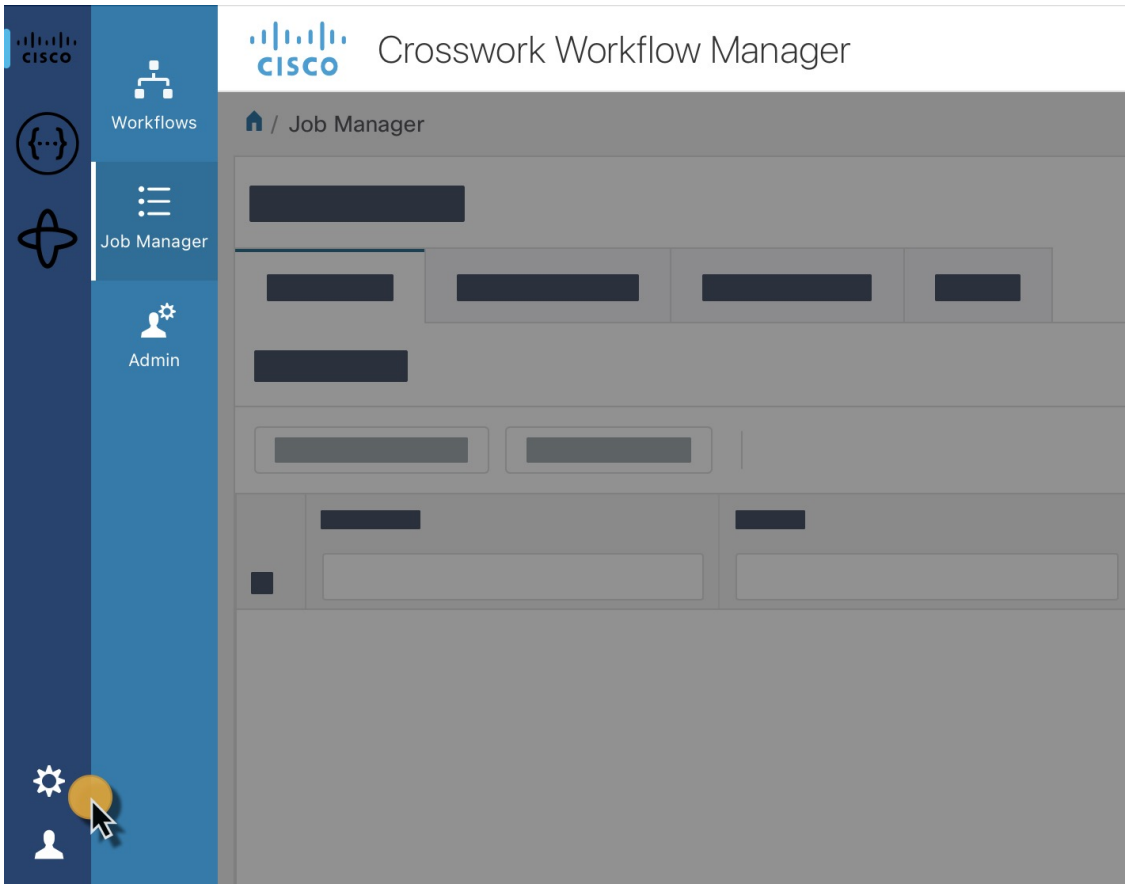
CWM 内の NxF 機能

NxF 機能は、管理者ユーザーが CWM UI の [設定（Settings）] タブから使用できます。CWM の NxF 機能にアクセスするには、次の手順を実行します。

ステップ 1 CWM で、左端のナビゲーションメニューに移動します。

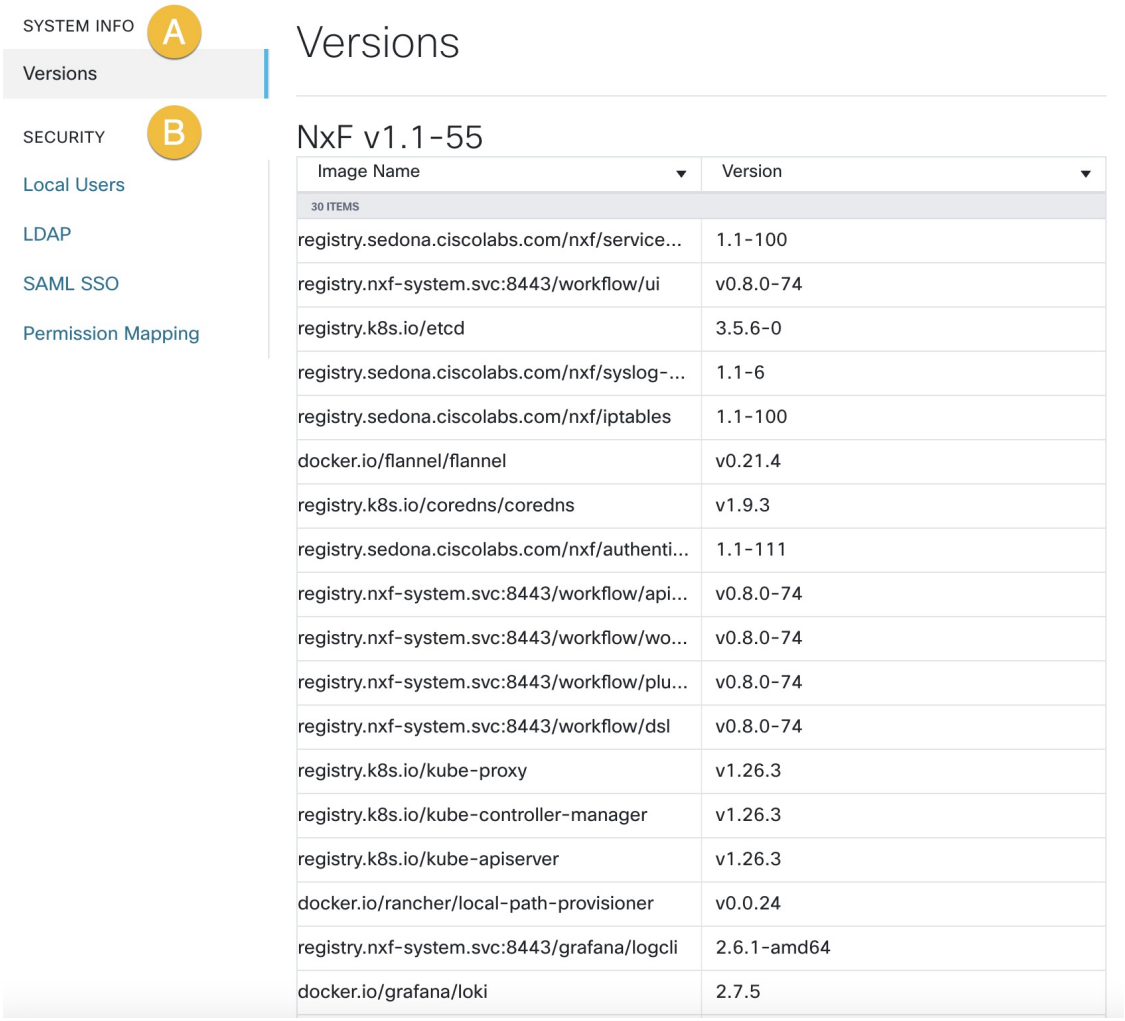
ステップ 2 [設定（Settings）] アイコン（歯車アイコン）をクリックします。

図 *1 : NxF* の設定



ステップ 3 展開されたドロワに、次の項目が表示されます。

図 *2* : 設定のドロワ



a) [システム情報（System Info）] セクションには、NxF および CWM マイクロサービスの最新バージョンに関する情報が表示されます。

b) [セキュリティ（Security）] セクションには、アクセス管理に関する次の項目が表示されます。

- [ローカルユーザー（Local Users）]：UI を介してローカルユーザーを表示、作成、および編集できます。
- [LDAP]：ユーザー認証の LDAP 設定を構成できます。
- [SAML SSO]：ユーザー認証の SAML シングルサインオン設定を構成できます。
- [権限マッピング（Permission Mapping）]：シスコ ポリシー管理ツールを使用して権限管理を操作できます。

ローカルユーザーの追加

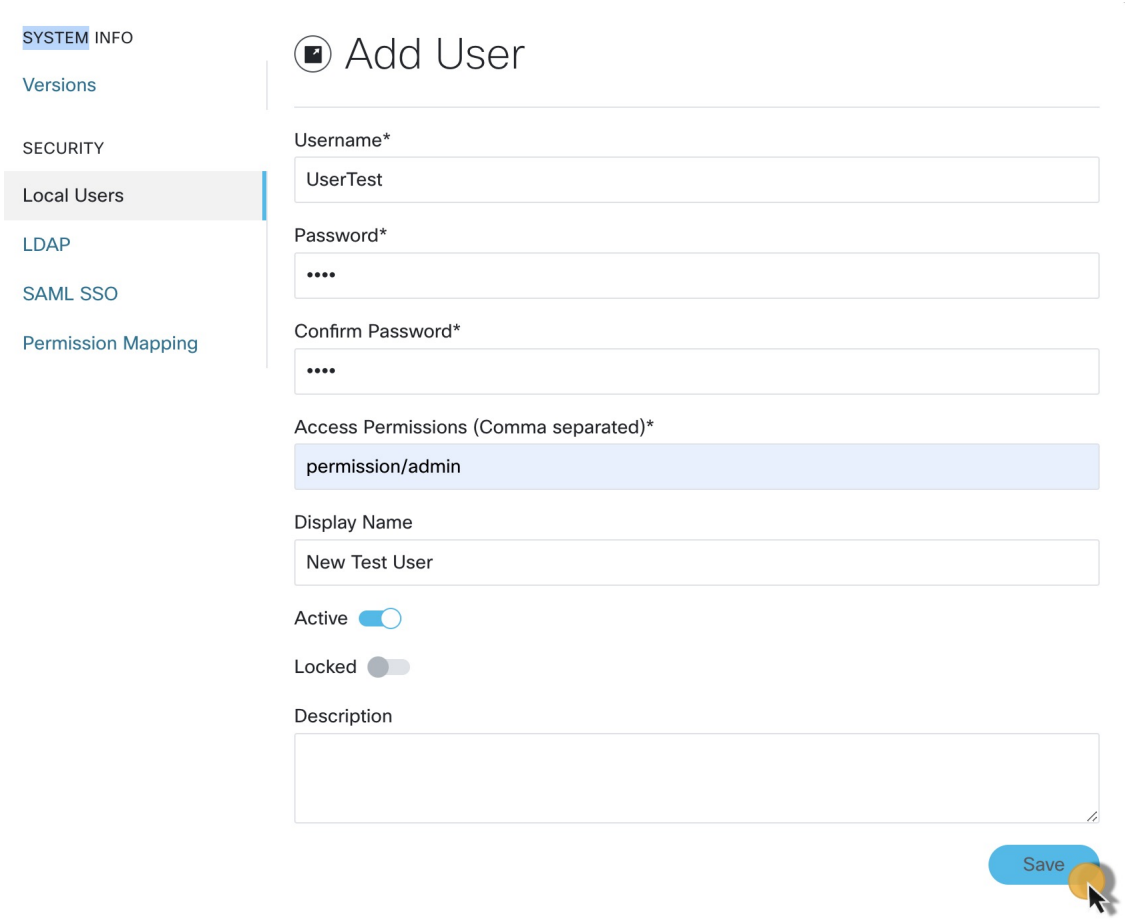
ステップ 1 CWM で、左端のナビゲーションメニューに移動します。

ステップ 2 CWM（Cisco アイコン）から [ローカルユーザー（Local Users）] タブに移動します。

ステップ 3 [追加...（Add...）] をクリックします。

ステップ 4 [ユーザーの追加（Add User）] パネルで、必須フィールド（アスタリスクでマークされているフィールド）の [ユーザー名（Username）]（CWM へのログインに使用）、[パスワード（Password）]、[パスワードの確認（Confirm Password）]、[アクセス権限（Access Permissions）]（`permission/admin` と入力）に入力します。[説明（Description）] と [表示名（Display Name）]（CWM でユーザー名の横に表示される）はオプションのフィールドです。

図 *3 : NxF* ユーザーの追加



ステップ 5 オプションボタンを使用して、ユーザーステータスを設定します。両方のオプションボタンを同時に無効または有効にできます。

- [アクティブ有効（Active enabled）]：ユーザーは CWM にログインできます。

- [アクティブ無効（Active disabled）] : ユーザーは CWM へのログインが禁止されます。
- [ロック有効（Locked enabled）] ：ユーザーの削除を防止します。
- [Lロック無効（Locked disabled）] : ユーザーの削除を許可します。

ステップ 6 [保存（Save）] をクリックします。

LDAP を介した認証の設定

CWM では、ローカルユーザーのサポートに加えて、LDAP（Lightweight Directory Access Protocol）サーバーとの統合によって LDAP ユーザーを追加できます。

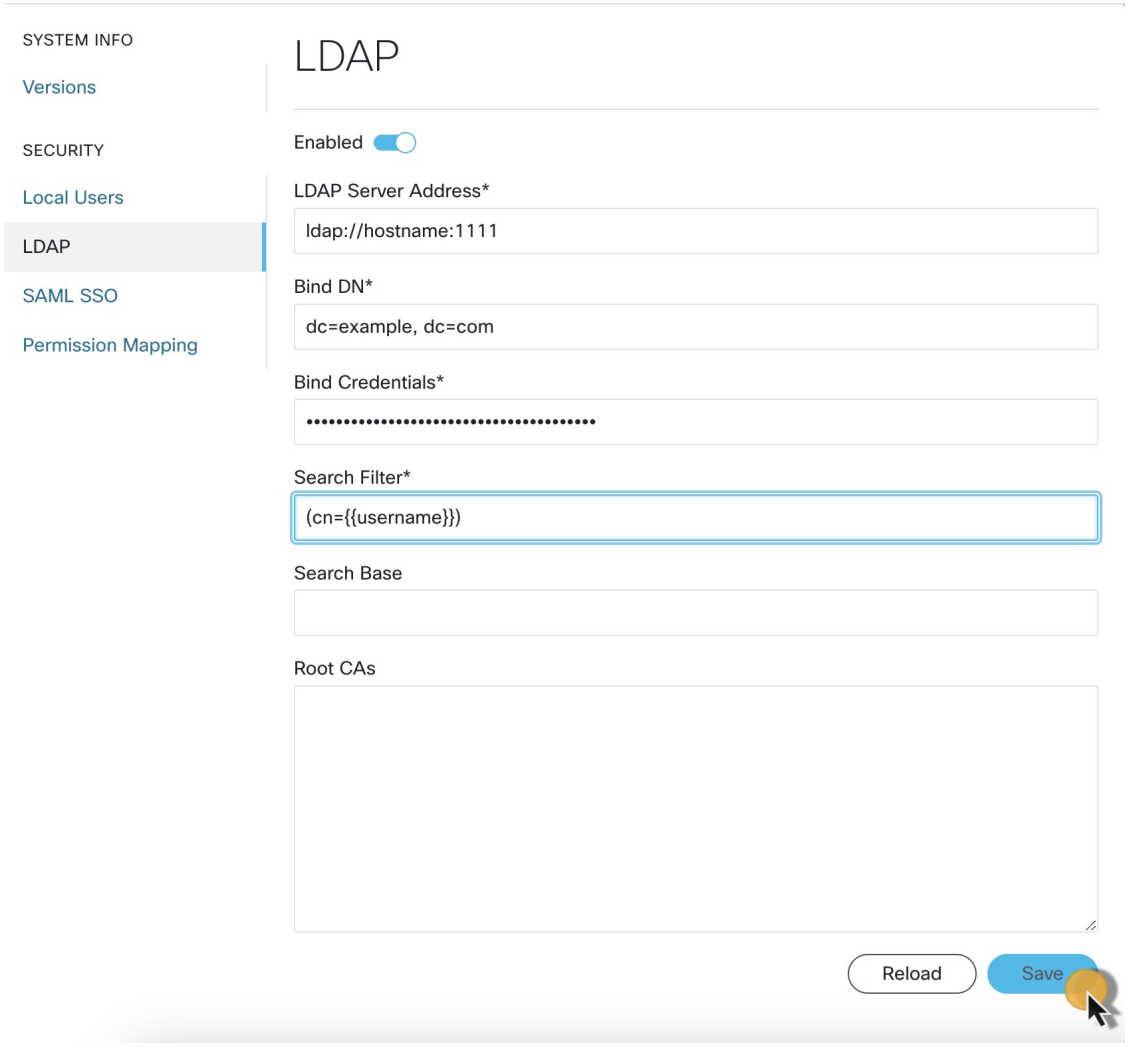
ステップ 1 CWM で、左端のナビゲーションメニューに移動します。

ステップ 2 CWM（Cisco アイコン）から、 [LDAP] タブに移動します。

ステップ 3 [有効（Enabled）] オプションボタンをクリックします。

ステップ 4 必須フィールド（アスタリスクでマークされているフィールド）の [LDAPサーバーアドレス（LDAP Server Address）]、[バインドDN（Bind DN）]、[バインドクレデンシャル（Bind Credentials）]、および [検索フィルタ（Search Filter）] に入力します。[検索ベース（Search Base）] と [ルートCA（Root CAs）] はオプションです。

図 *4 : LDAP*



ステップ 5 [保存（Save）] をクリックします。

SAML SSO を介した認証の設定

CWM は、SAML（セキュリティ アサーション マークアップ言語）プロトコルに基づいてシングルサインオンアクセスを取得するために、LDAP ユーザーと非 LDAP ユーザーの両方をサポートする SAML SSO 機能を提供します。CWM の SAML SSO は、LDAP と同時に、または LDAP なしで有効にできます。

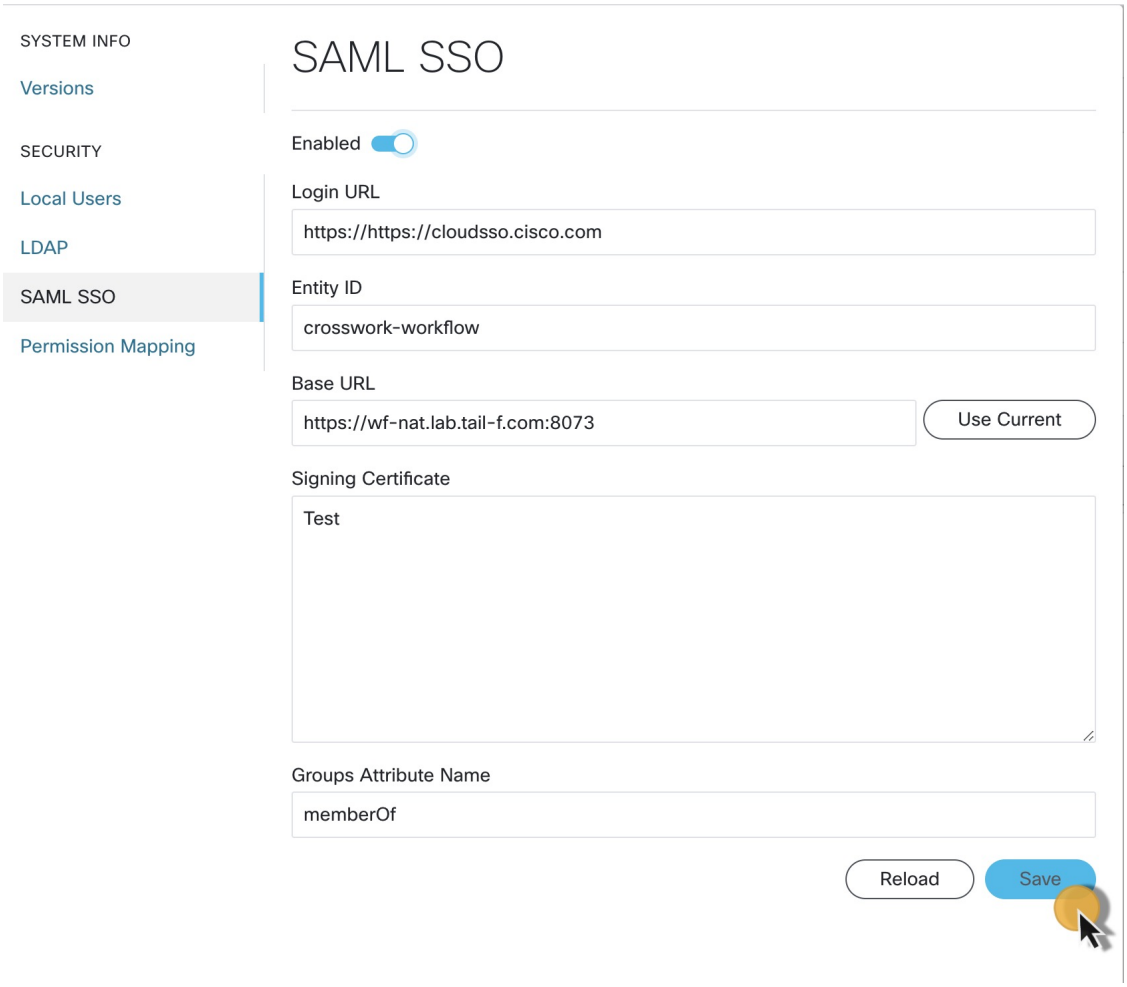
ステップ 1 CWM で、左端のナビゲーションメニューに移動します。

ステップ 2 CWM（Cisco アイコン）から [SAML SSO] タブに移動します。

ステップ 3 [有効（Enabled）] オプションボタンをクリックします。

ステップ 4 必須フィールド（[ログインURL（Login URL）]、[エンティティID（Entity ID）]、[ベースURL（Base URL）]、[署名証明書（Signing Certificate）]、および [グループ属性名（Groups Attribute Name）]）に入力します。

図 5 : NxF SAMLSSO



ステップ 5 [保存（Save）] をクリックします。

権限マッピングの設定

シスコ ポリシー管理ツール（PMT）を使用して、ユーザーのグループに特定の権限を付与できます。

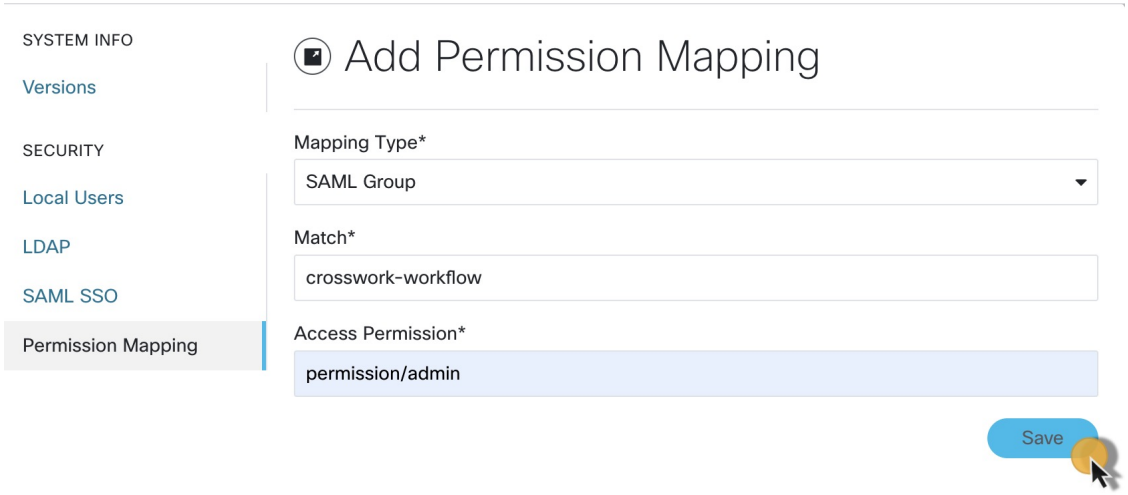
ステップ 1 CWM で、左端のナビゲーションメニューに移動します。

ステップ 2 CWM（Cisco アイコン）から [権限マッピング（Permission Mapping）] タブに移動します。

ステップ 3 [追加...（Add...）] をクリックします。.

ステップ 4 [権限マッピングの追加（Add Permission Mapping）] パネルで、ドロップダウンメニューからマッピングタイプ（SAML ユーザー、SAML グループ、LDAP ユーザー、または LDAP グループ）を選択します。

図 *6*：権限マッピング



ステップ 5 [一致（Match）] フィールドに、シスコ ポリシー管理ツールのエントリを入力します。一致は、ポリシー管理ツールの UI から [OAuthクライアント（OAuth Clients）] タブに移動して、[クライアントID（Client ID）] 列で見つけることができます。

ステップ 6 [アクセス権限（Access Permission）] フィールドに適切な権限（例：`permission/admin`）を入力します。

ステップ 7 [保存（Save）] 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。