Users

ここでは、次の内容について説明します。

ユーザーアクセスの管理

NxF はセキュリティのレイヤーを追加し、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。CWM では NxF を介してユーザーアクセスを管理できます。

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 : NxF* ドロワの設定

a) 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) 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/user` 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。

a) [アクティブ有効（Active enabled）]：ユーザーは CWM にログインできます。
b) [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。
c) [ロック有効（Locked enabled）]：ユーザーの削除を防止します。
d) [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 : NxF 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。

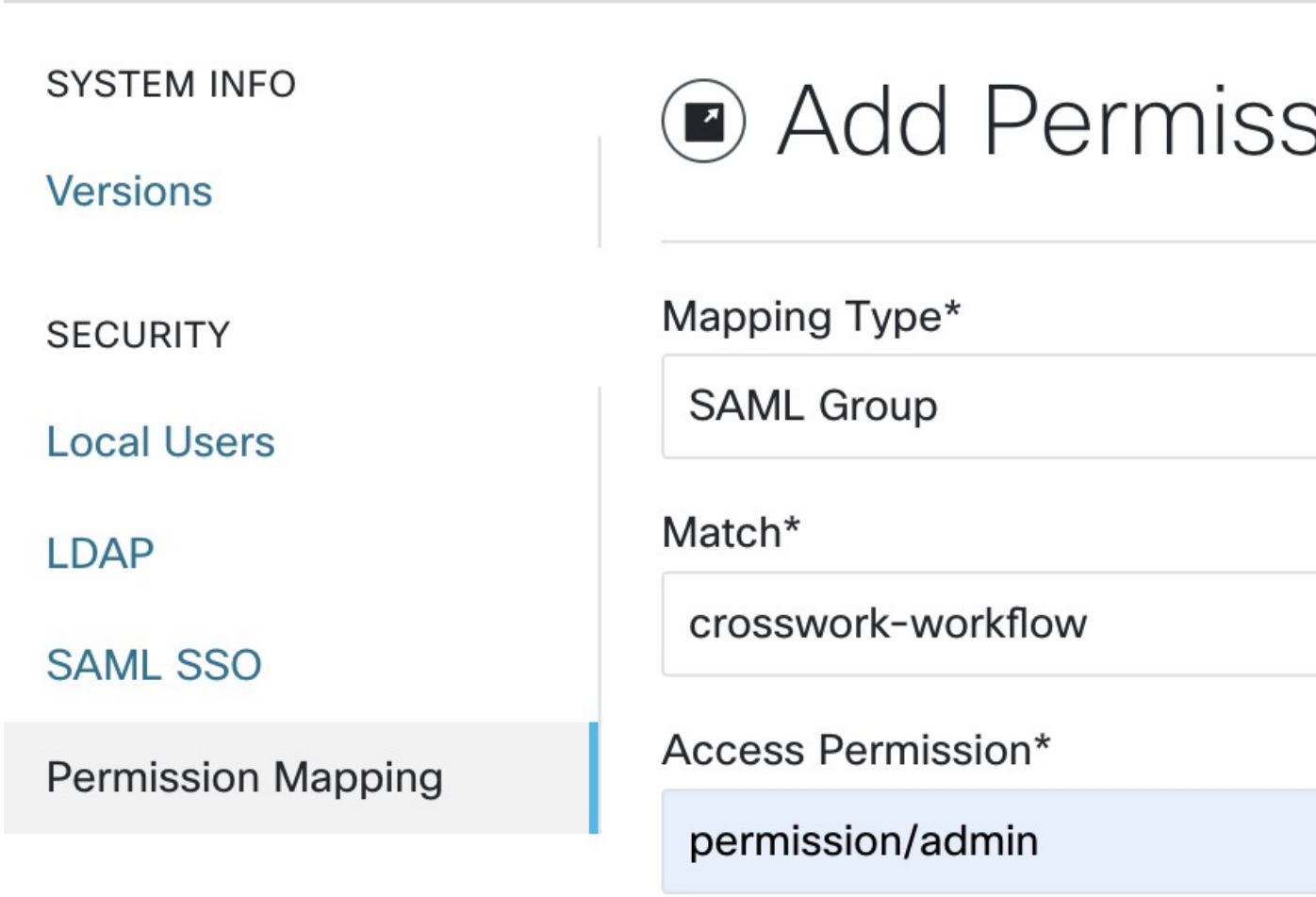
ステップ 1 CWM で、左端のナビゲーションメニューに移動します。

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 : NxF* の権限マッピング



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。