設定

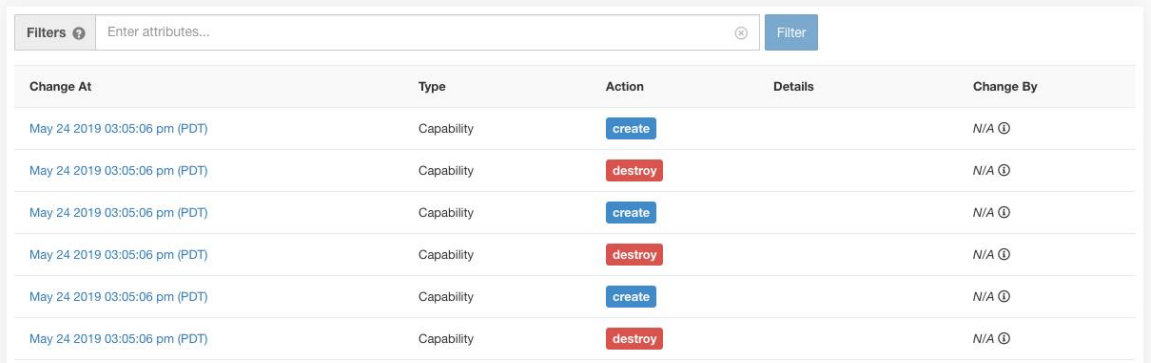
使用できるシステムレベルの設定は、ロールによって異なります。たとえば、[サイト管理者（Site Admin）] および [カスタマーサポートユーザー（Customer Support user）] ロールを持つユーザーのみが、[ユーザー（Users）] オプションを表示できます。

- ログの変更 （1 ページ）
- 収集ルール （3 ページ）
- コレクタ （4 ページ）
- 会社 （5 ページ）
- アイドルセッション （27 ページ）
- 設定 （27 ページ）
- ロール （30 ページ）
- スコープ （43 ページ）
- テナント （44 ページ）
- ユーザ（Users） （47 ページ）

ログの変更

サイト管理者は、ウィンドウの左側にあるナビゲーションバーの [管理（Manage）] メニューの下にある [変更ログ（Change Log）] ページにアクセスできます。このページには、Cisco Secure Workload で行われた最新の変更内容がすべて表示されます。

図 *1 : [*変更ログ（***Change Log***）*]* ページ

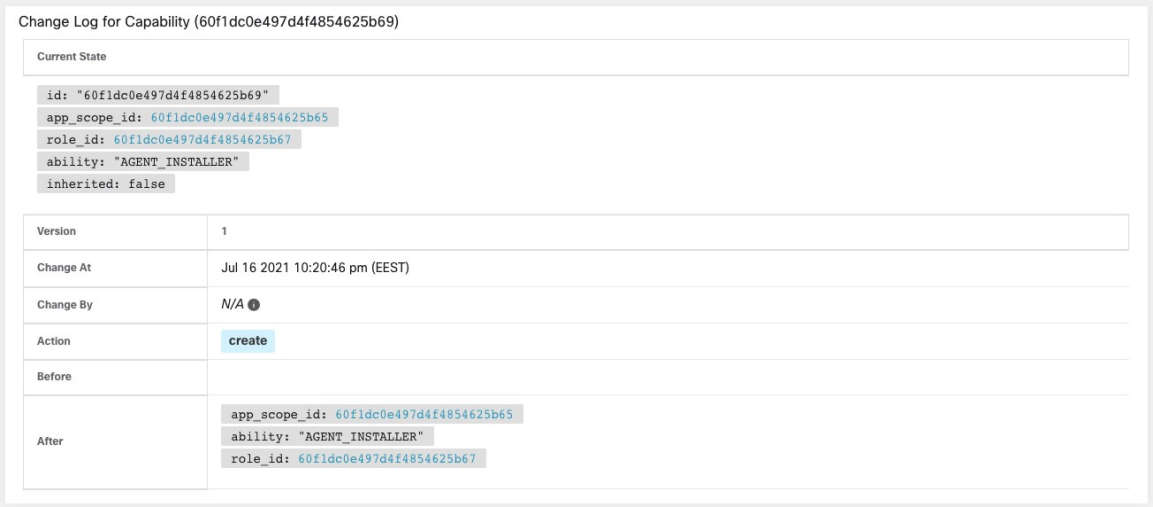


各変更ログエントリの詳細は、[変更日時（Change At）]列のリンクをクリックすると表示できます。このページには、変更されたフィールドの変更前と変更後のスナップショットが、[変更前（Before）] と [変更後（After）] に表示されます。フィールドには技術名が含まれる場合があります。Secure Workload 全体を通して見たときに、他の場所でどのような使われ方をしているのかを理解するには、何らかの解釈が必要になります。

図 *2 : [*変更ログ詳細（***Change Log Details***）*]* ページ

エンティティの変更に関する完全なリストは、右上隅にある [この<エンティティタイプ>の完全なログ（Full log for this <entity type>）] というタイトルのボタンをクリックすると表示できます。このページには、各変更の詳細が表示されます。また、エンティティの現在の状態に関する情報がある場合は、[現在の状態（Current State）] に表示されます。

図 *3:* エンティティの完全な変更ログ



収集ルール

サイト管理者と**カスタマーサポートユーザー**は、ウィンドウの左側にあるナビゲーションバーの [管理（Manage）] メニューから [収集ルール（Collection Rules）] ページにアクセスできます。このページには、Cisco Secure Workload エージェントを実行しているスイッチで使用される VRF 別のハードウェア収集ルールがすべて表示されます。各 VRF ごとにテーブルの行があります。

スイッチへの適用

スイッチのハードウェアバージョンによっては、複数の VRF のルールをサポートしていない場合があります。この場合は、1 つの VRF でのみ [スイッチに適用（Apply to Switches）] チェックボックスをオンにして、この VRF の下にあるすべてのルールを定義してください。スイッチが複数の VRF のルールをサポートしている場合は、監視するすべての VRF で [スイッチに適用（Apply to Switches）] チェックボックスをオンにします。

ルール

VRF の [編集（Edit）] ボタンをクリックして、その収集ルールを変更します。デフォルトでは、すべての VRF は 2 つのデフォルトのキャッチオールルールによって設定されます。1 つは IPv4 (`0.0.0.0/0 INCLUDE`) 用で、もう 1 つは IPv6 (`::/0 INCLUDE`) 用です。これらのデフォルトルールは削除できますが、慎重に行ってください。

さらなる包含ルールと除外ルールを追加できます。有効なサブネットを入力し、包含または除外を選択して、[ルールの追加（Add Rule）] をクリックします。これらのルールの優先度は、ドラッグアンドドロップで調整できます。リスト内のルールをクリックしたままドラッグして、順序を調整するだけです。

変更がスイッチに反映されるまでに数分かかる場合があります。VRF リストに戻るには、右上隅の [戻る（Back）] ボタンをクリックします。

優先順位

収集ルールは、優先順位の降順に並べられます。優先順位を決定するために、最長プレフィックスの一致は行われません。最初に表示されるルールは、後続のすべてのルールよりも優先されます。例：

1. 1.1.0.0/16 INCLUDE
2. 1.0.0.0/8 EXCLUDE
3. 0.0.0.0/0 INCLUDE

上記の例では、サブネット 1.1.0.0/16 を除いて、サブネット 1.0.0.0/8 に属するすべてのアドレスが除外されています。

順序を変更した別の例：

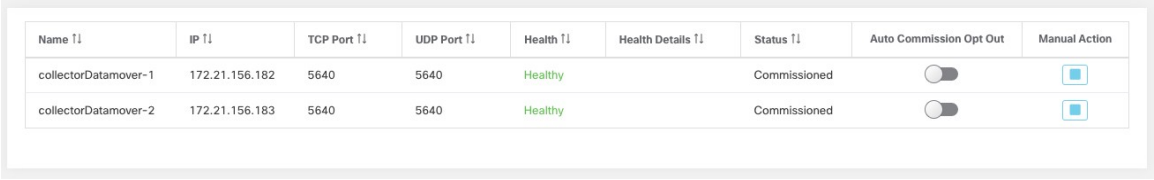
1. 1.0.0.0/8 EXCLUDE
2. 1.1.0.0/16 INCLUDE
3. 0.0.0.0/0 INCLUDE

上記の例では、サブネット1.0.0.0/8に属するすべてのアドレスが除外されています。ルール番号2は、サブネットに対してすでに高次のルールが定義されているため、ここでは実行されません。

コレクタ

サイト管理者と**カスタマーサポートのユーザー**は、ウィンドウの左側にあるナビゲーションバーの [プラットフォーム（Platform）] メニューの下にある [コレクタ（Collectors）] ページにアクセスできます。このページには、現在構成されているすべてのコレクタが表示されます。Cisco Secure Workload エージェントは、コミッションされたコレクタにフローデータを送信するため、コミッションされたすべてのコレクタが利用可能であることが重要です。デフォルトでは、すべてのコレクタは定期的に正常性をチェックされ、正常性に基づいてコミッションまたはデコミッションされます。[自動コミッションのオプトアウト（Auto Commission Opt Out）] トグルを使用して、この自動化されたプロセスからオプトアウトできます。このトグルをオンにすると、右端の列の下にある [再生（Play）] アイコンと [停止（Stop）] アイコンを使用して、コミッションとデコミッションができます。

図 *4 :* [コレクタ（*Collectors*）] ページ



会社

次のように、企業全体（Secure Workload クラスタごと）の構成を設定できます。

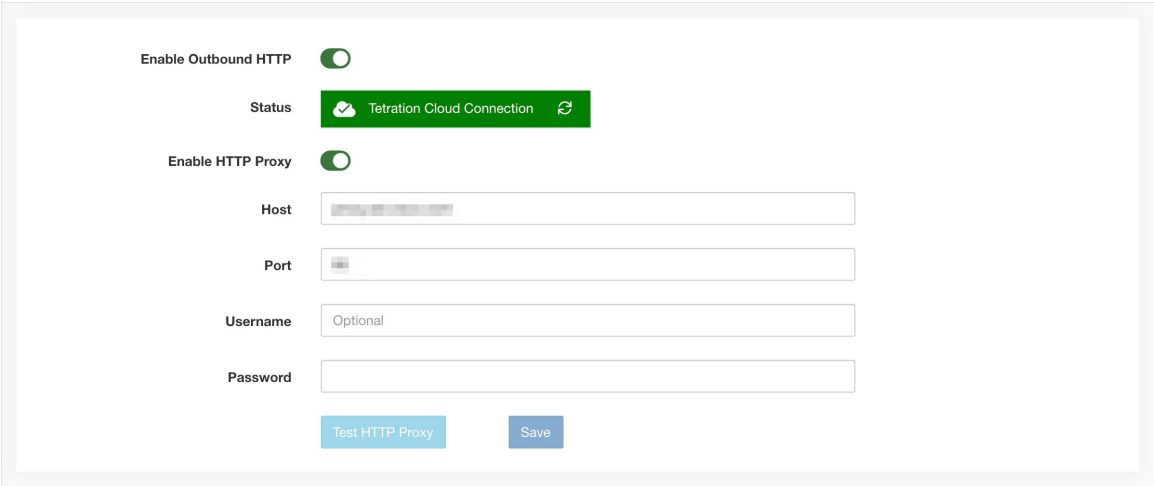
アウトバウンド HTTP 接続

Cisco Cloud から最新の脅威インテリジェンス データセットが取得されるようにするには、アウトバウンド HTTP 接続をセットアップすることを強く推奨します。

警告 エンタープライズ アウトバウンド HTTP リクエストでは、HTTP プロキシの設定に加えて、エンタープライズ ファイアウォール アウトバウンド ルールから **periscope.tetrationcloud.com** および **uas.tetrationcloud.com** へのトラフィックを許可する必要がある場合があります。以下を参照してください。

periscope.tetrationcloud.com への TLS 接続は、既知の脆弱性を識別するために脅威インテリジェンスデータを転送するために使用されます。したがって、Cisco Secure Workload では、ドメインの X.509 証明書の署名 CA 証明書を、Secure Workload に付属の信頼できるルート CA 証明書と照合して、ドメイン名の信頼性を検証することが不可欠です。X.509 信頼チェーンを改ざんすると、機能が正常に動作しなくなります。

図 *5 :* アウトバウンド *HTTP* 接続



サイト管理者と**カスタマーサポートのユーザー**は、アウトバウンドHTTP設定にアクセスできます。左側のナビゲーションバーで、**[プラットフォーム（Platform）]**>**[アウトバウンドHTTP（Outbound HTTP）]**をクリックします。

フィールド	説明
Status	Secure Workload アプライアンスが Secure Workload Cloud にアクセスして脅威インテリジェンス データセットの更新を取得できるかどうかを示します。ステータスチェックは、更新ボタンをクリックして再トリガーできます。次の HTTP プロキシ設定を使用して、Secure Workload 展開に基づいて HTTP プロキシ設定を構成できます。
Enable HTTP Proxy	このオプションが有効になっている場合、すべての外部 HTTP 接続で HTTP プロキシが使用されます。
Host	HTTP プロキシホストアドレス
ポート（Port）	HTTP プロキシポート番号
Username	HTTP プロキシサーバーが Basic 認証を使用する場合にのみ必要です。
password	HTTP プロキシサーバーが Basic 認証を使用する場合にのみ必要です。

ログインページのメッセージ

サイト管理者と**カスタマーサポートユーザー**は、サインインページでユーザーに表示される最大 1600 文字のメッセージを入力できます。

ログインページメッセージを作成または変更するには:左側のナビゲーションバーで、**[プラットフォーム（Platform）]**> **ログインページのメッセージ（Login Page Message）** をクリックします。

セッション設定

UI ユーザー認証のアイドル セッション タイムアウトは、ここで構成できます。この構成は、アプライアンスのすべてのユーザーに適用されます。デフォルトのアイドルセッション期間は 1 時間です。アイドルセッションの継続時間は、5 分から 24 時間の範囲で設定できます。セッションタイムアウトは、この値が保存されるとすぐに、ユーザーの認証されたセッションで有効になります。

サイト管理者とカスタマーサポートユーザーは、この設定にアクセスできます。左側のナビゲーション バーで、**[管理（Manage）]** > **[セッション設定（Session Configuration）]** をクリックします。

外部認証の設定

このオプションを有効にすると、認証を外部システムに委ねることができます。認証の現在のオプションは、Lightweight Directory Access Protocol（LDAP）とシングル サインオン（SSO）です。このオプションを有効にすると、サインインするすべてのユーザーが、選択したメカニズムを使用して認証を行うようになります。特に「Use Local Authentication」オプションが有効なユーザーがいない場合は、LDAP 接続が正しく設定されていることを確認することが重要です。推奨されるアプローチは、「Use Local Authentication」オプションをオンにして、**サイト管理者**のログイン情報を持つローカル認証されたユーザーを少なくとも 1 人指定する方法です。このユーザーは、LDAP が正しく設定されていることを確認できます。接続が正常にセットアップされたら、ユーザー編集フローで [ローカル認証を使用（Use Local Authentication）] オプションをオフにして、このユーザーを外部認証に移行させることもできます。

サイト管理者は、外部接続の問題やユーザーサインインの失敗などのデバッグに役立つ付加的なデバッグメッセージを有効にできます。これは [外部認証のデバッグ（External Auth Debug）] オプションをオンにすることで有効にできます。これをオンにすると、付加的な説明ログメッセージが「external_auth_debug.log」という名前の別のログファイルに書き込まれます。デバッグが完了したら、[外部認証のデバッグ（External Auth Debug）] をオフにして、余分なログがログファイルに書き込まれないようにすることをお勧めします。

（注） 「Use Local Authentication」オプションに示されているように、ユーザーごとに有効にすることで、ユーザーは外部認証をバイパスできます。このオプションは、外部認証が有効になっている場合の警告メッセージを使用して、リンクからユーザー編集フローに移動する方法でも有効にすることができます。

連携が有効になっている場合は、SSO を使用した外部認証が推奨される認証アプローチです。

（注） 3.7.1.5 リリース以降、外部認証セッションの削除時間が 6 時間から 9 時間に延長されました。この設定は、外部認証またはオンプレミスのみに適用されます。

サイト管理者および**カスタマーサポートユーザー**は、外部認証を設定できます。左側のナビゲーションバーで、**[プラットフォーム（Platform）]** > **[外部認証（External Authentication）]** をクリックします。

図 *6*: 外部認証の設定

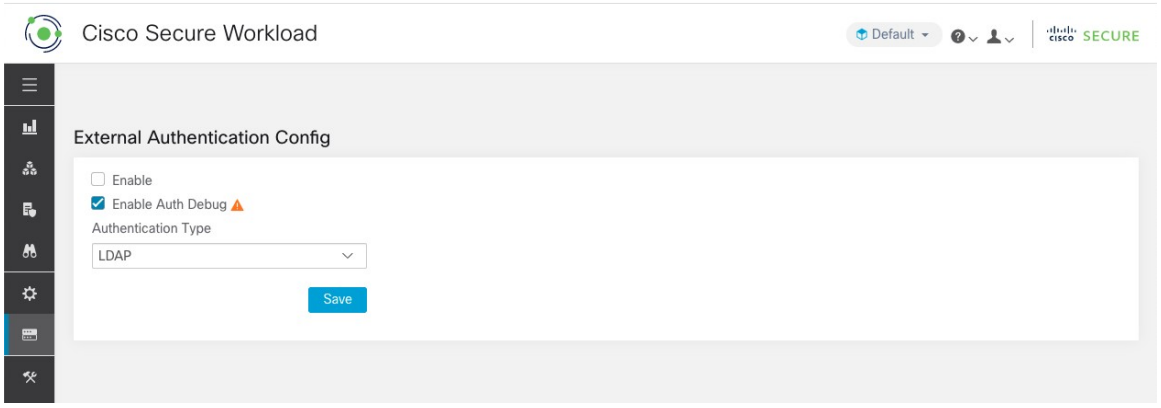


図 *7*: 外部認証の設定（続き）

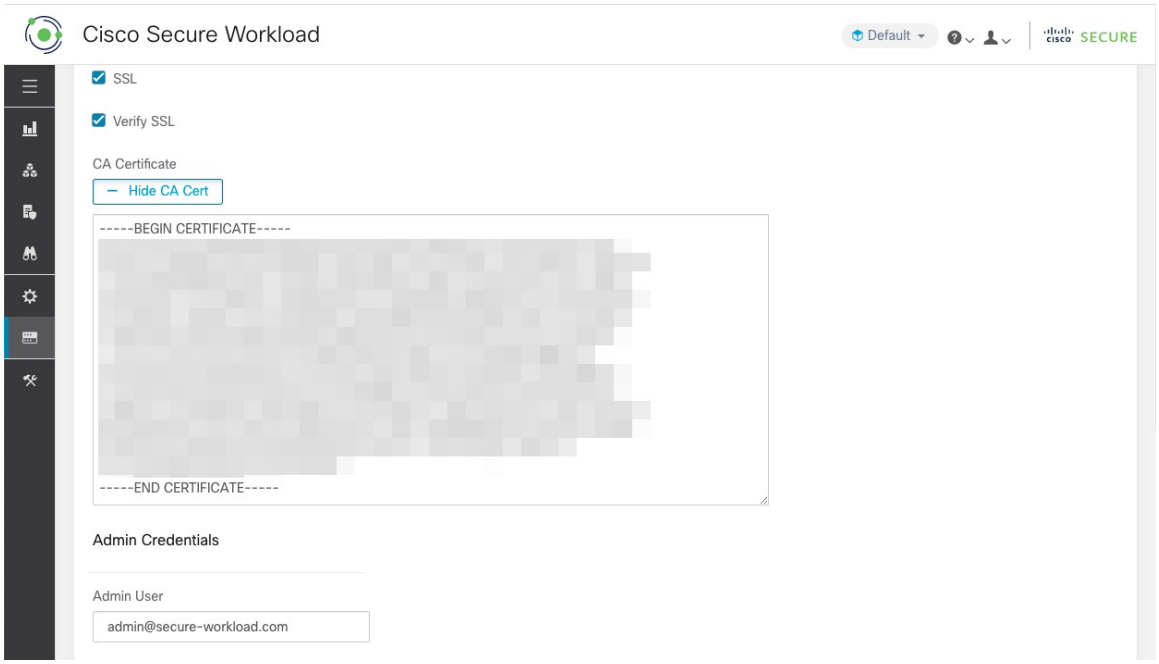


図 *8* : 外部認証の設定（続き）

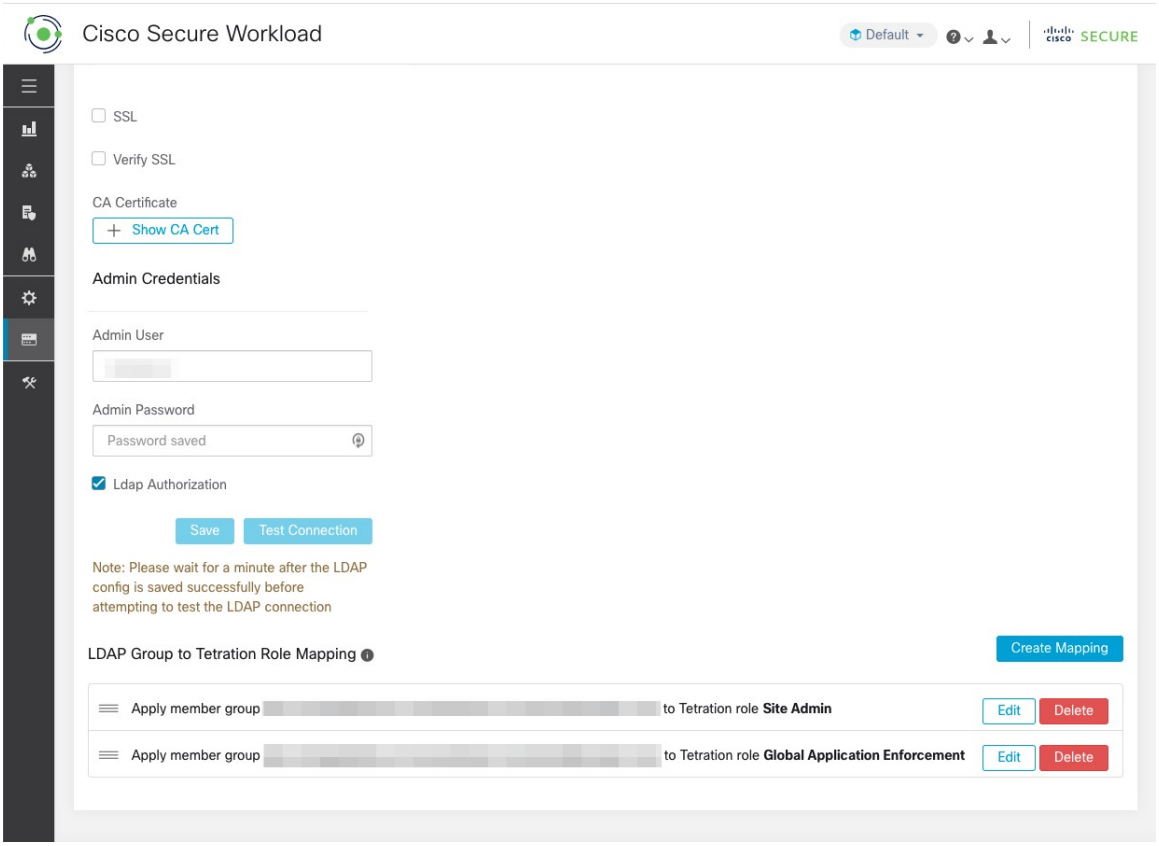
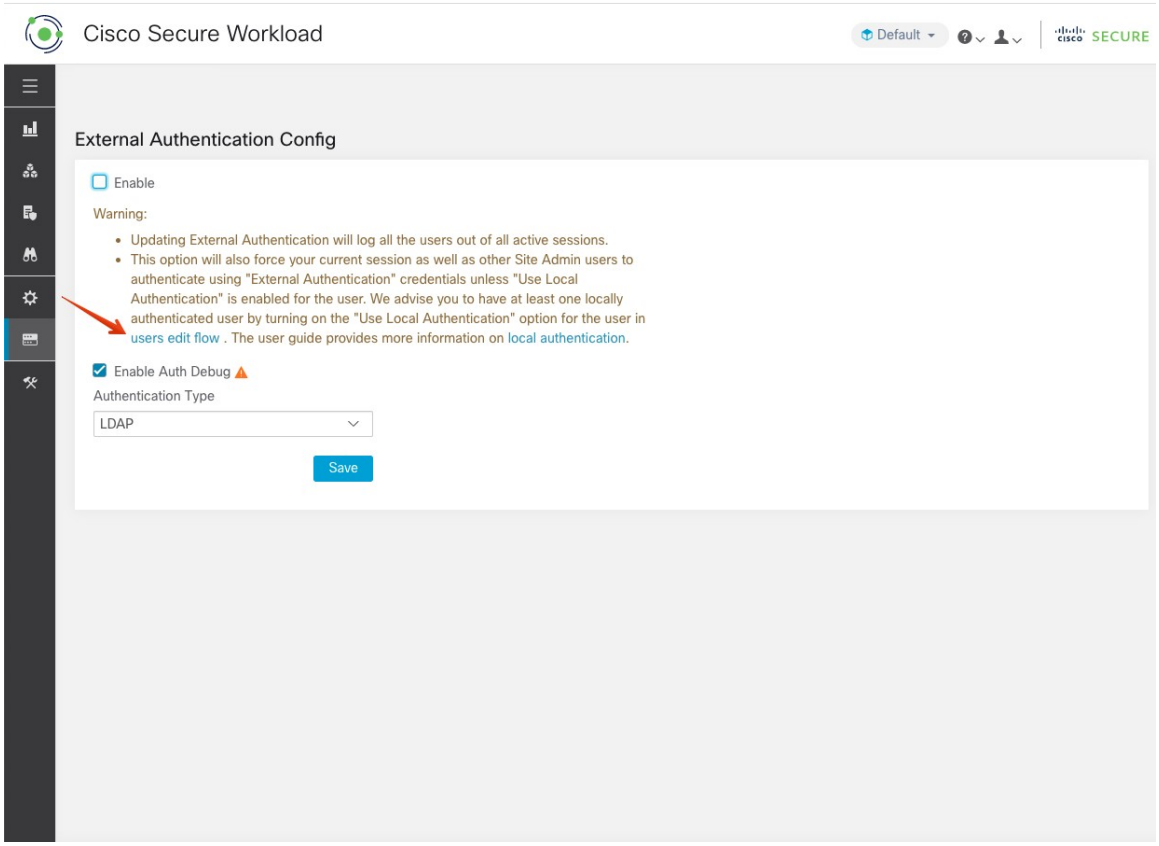


図 *9:* 外部認証に関する警告



Lightweight Directory Access Protocol（LDAP）の設定

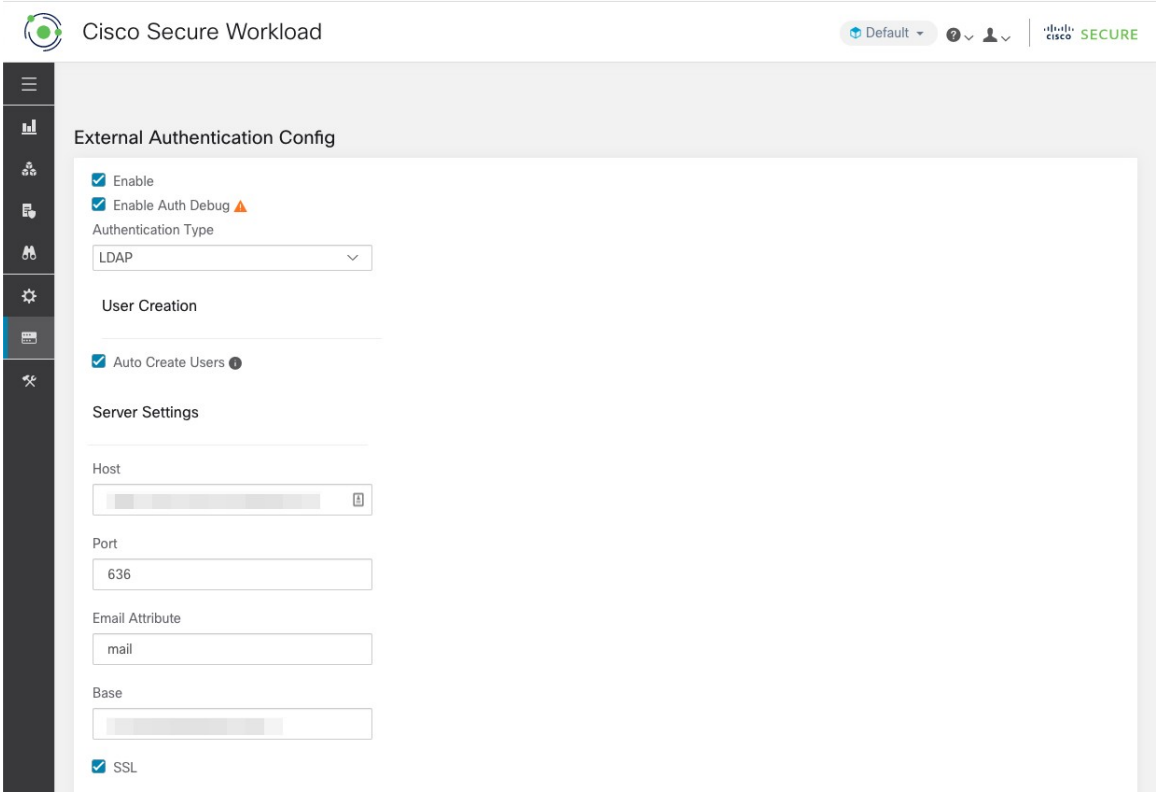
このオプションを選択すると、LDAPを使用してユーザーを認証できます。つまり、これを有効にすると、すべてのユーザーがログアウトされ、その後のサインインではLDAPの電子メールとパスワードを使用して認証されます。

「フェデレーション」が有効になっている場合、現在LDAPは認証メカニズムとして推奨されていません。

LDAPが有効になっている場合、新しいユーザーを作成するための推奨ワークフローは次のとおりです。

サイト管理者は、新しいユーザーがLDAP経由で初めてログインする前に、まず電子メールで新しいユーザーを作成し、LDAP 認証の設定（AD 認証）して適切な役割を割り当てるようにお勧めします。新しいユーザーが適切なロールなしでLDAPでログインした場合、デフォルトのロールはユーザーに割り当てられません。

図 *10 : Lightweight Directory Access Protocol*（*LDAP*）の設定



フィールド	説明
ユーザーの自動作成（Auto Create Users）	[ユーザーの自動作成（Auto Create Users）] をオンにすると、初回のログイン時に該当ユーザーが存在しない場合にユーザーが作成されます。これにより、サイト管理者は、ユーザーのログインを許可する前にユーザーを事前にプロビジョニングする必要がなくなります。Secure Workload アクセスを [ユーザー（Users）] ページで手動で作成したユーザーに制限する必要がある場合は、このオプションをオフにする必要があります。
Host	認証に使用される LDAP ホスト。
ポート（Port）	認証に使用される LDAP ポート。
メール属性（Email Attribute）	組織の電子メールを表す LDAP 属性名。
Base	ユーザーが検索される LDAP ベース DN。
SSL	暗号化を有効にして、「ldaps://」を使用します。
SSL 検証（SSL Verify）	サーバーの証明書に基づいて、完全修飾ドメイン名（FQDN）などのサーバーの SSL 属性を確認します。

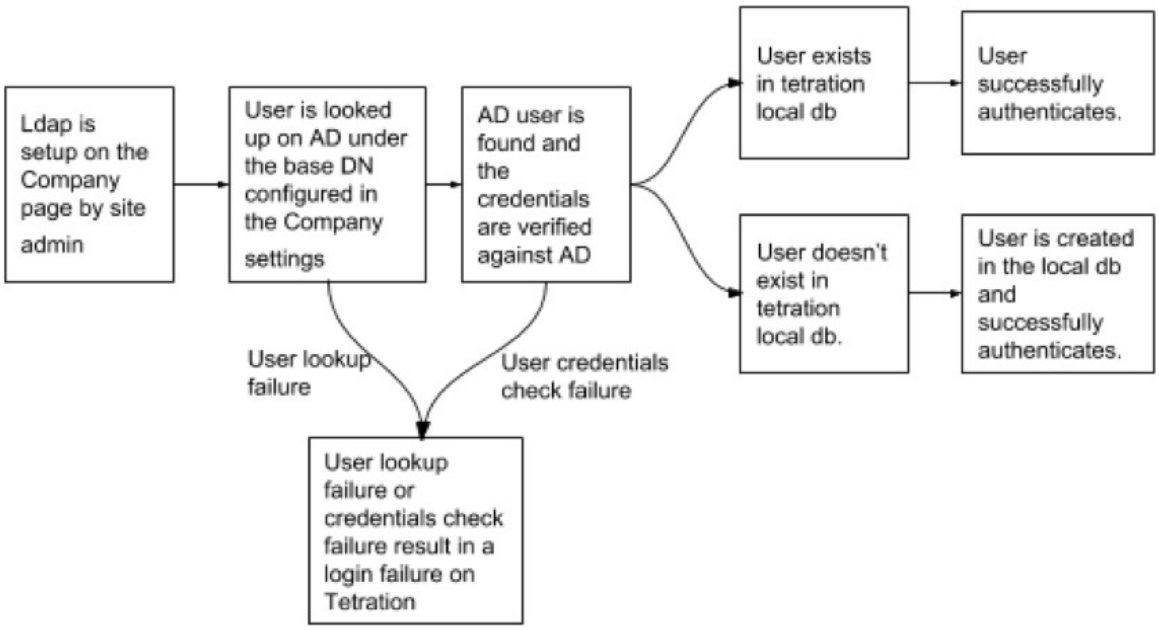
フィールド	説明
SSL認証局証明書（SSL Certificate Authority Cert）	LDAPサーバーのSSL証明書の署名証明書。サーバーの証明書チェーンを公的に検証できない場合に必要です。
管理者ユーザ（Admin User）	LDAP サーバーに対してバインドするために使用される LDAP 管理者ユーザー名（Secure Workload ユーザーではない）。例：[ユーザー]@[ドメイン] または [ドメイン]\\[ユーザー]
管理者パスワード（Admin Password）	LDAP サーバーに対してバインドするために使用される LDAP 管理者パスワード。
LDAP認証（Ldap Authorization）	LDAP認証は、「LDAP認証の設定（AD認証）」で説明されているように、有効にして構成することができます。

LDAP 構成が有効になると、「Use Local Authentication」オプションが有効になっているユーザーを除くすべてのユーザーがセッションからログアウトされます。

[保存（保存）] ボタンをクリックすると、LDAP 構成を保存できます。LDAP 構成が正常に保存された後、LDAP 接続をテストする前に 1 分間待つことをお勧めします。

[接続のテスト（Test Connection）] ボタンを使用して LDAP 構成を保存した後、LDAP 接続をテストできます。これにより、入力された管理者ログイン情報を使用してLDAPサーバーに対するバインドが試行されます。

図 *11* : 認証ワークフロー



LDAP 問題のデバッグ

LDAP 接続のテスト時にエラーが発生した場合は、次の点を確認してください。

- LDAP 管理者の資格情報が正しいかどうかを確認します。
- ホスト、ポート、SSL などの接続パラメータを確認します。
- Secure Workload UI VIP から LDAP サーバーに到達できるかどうかを確認します。
- AD サーバーが稼働しているかどうかを確認します。
- [ldapsearch] などのコマンドラインツールを接続の詳細とともに使用して、バインドできるかどうかを確認します。

ユーザーのログイン中にエラーが発生した場合は、以下を確認してください。

- ユーザーが LDAP 認証を使用する他社の Web サイトに LDAP ログイン情報でログインできるかどうかを確認します。
- 企業の LDAP 設定で指定されている「基本の」DN が正しいかどうかを確認します。[ldapsearch] などのコマンドラインツールを使用して、基本 DN に対してユーザーを検索することで実行できます。

電子メールでユーザーを検索する [ldapsearch] クエリの例：

```
ldapsearch -H "ldap://<host>:<port>" -b "<base-dn>" -D "<ldap-admin-user>" -w
<ldap->admin-password> "(mail=<users-email-address>)"
```

LDAP 認証の設定（AD 認証）

Active Directory 認証は、外部認証 LDAP 設定の [管理者資格情報（Admin Credentials）] セクションで [LDAP 認証（LDAP Authorization）] チェックボックスを有効にすることで設定できます。この設定を有効にすると、サイト管理者は、LDAP の「MemberOf」グループのマッピングを以下のセクションの Secure Workload ロールに設定する必要があります。デフォルトではこの設定がないため、Active Directory ユーザーはログインを試行する前に、1 つ以上の Secure Workload ロールを事前に設定する必要があります。

LDAP 外部認証が有効になっている場合、LDAP MemberOf グループの Secure Workload ロールへのマッピングを設定する必要があります。[マッピングの作成（Create Mapping）] を使用すると、LDAP MemberOf グループ値を Secure Workload ロールにマッピングするように設定できます。ロールドロップダウンのロールは、範囲セレクタで選択された範囲に基づいて事前に入力されています。マッピングが保存されると、すべてのユーザーは、その後のログイン時にこれらの値に基づいて承認されます。

マッピングは、並べ替え、編集、または削除ができます。マッピングへの変更は、その後のログイン時にユーザーに割り当てられたロールに反映されます。最大 50 の LDAP MemberOf グループから Secure Workload ロールへのマッピングを作成できます。

LDAP MemberOf グループ名の重複は許可されません。ただし、複数の LDAP MemberOf グループを同じロールにマッピングできます。複数のグループが同じロールにマッピングされている場合、最後のマッピングは、Secure Workload ロールに一致する LDAP MemberOf としてユーザーで保存されます。

図 *12 : Secure Workload* ロールのセットアップへの *LDAP* グループ

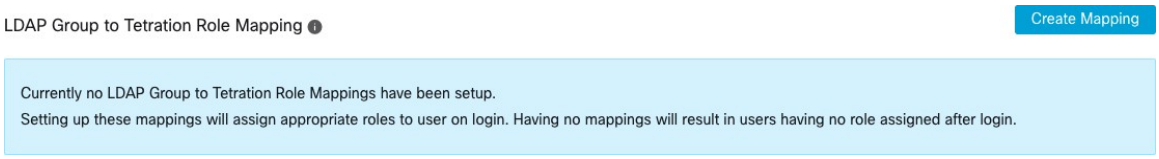
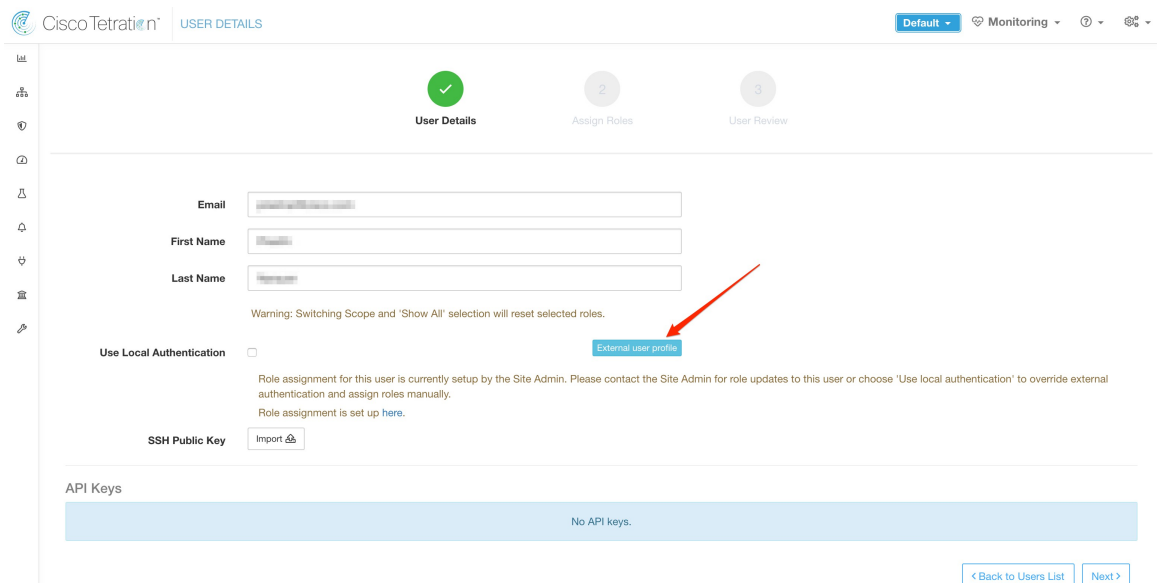


図 *13 : Secure Workload* ロールのマッピングへの *LDAP* グループ

サイト管理者ユーザーは、ユーザーが最後に成功したログインから取得した外部ユーザーの情報を利用して、上記のロールマッピングに基づいてロールの割り当てを調整できます。

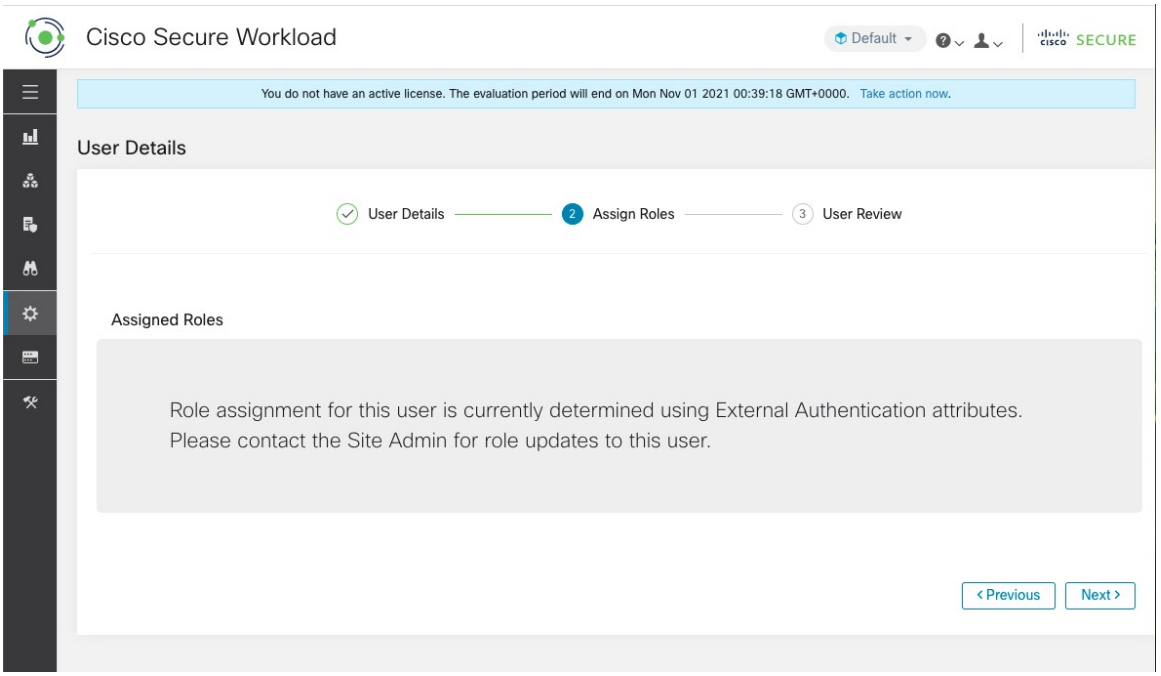
（注） 「「Use Local Authentication」オプション」オプションで示されているように、ユーザーごとに有効化すると、ユーザーは外部認証をバイパスできます。これらのユーザーは、AD 認証用に設定された認証プロセスもバイパスします。

図 *14 :* 外部ユーザー情報



認証が有効化されると、ユーザー作成フロー（新しいユーザーアカウントの追加 （48 ページ））およびユーザー編集フロー（「ユーザー アカウントの編集」）では、手動での Secure Workload ロール選択は**許可されません**。

図 *15 : [ユーザー（Users）]* ページ



Secure Workload ロールにマッピングされた LDAP MemberOf グループは、[ユーザープロファイル（User Profile）] ページに表示されます。

図 *16 : [ユーザープロファイル（User Profile）]* ページ

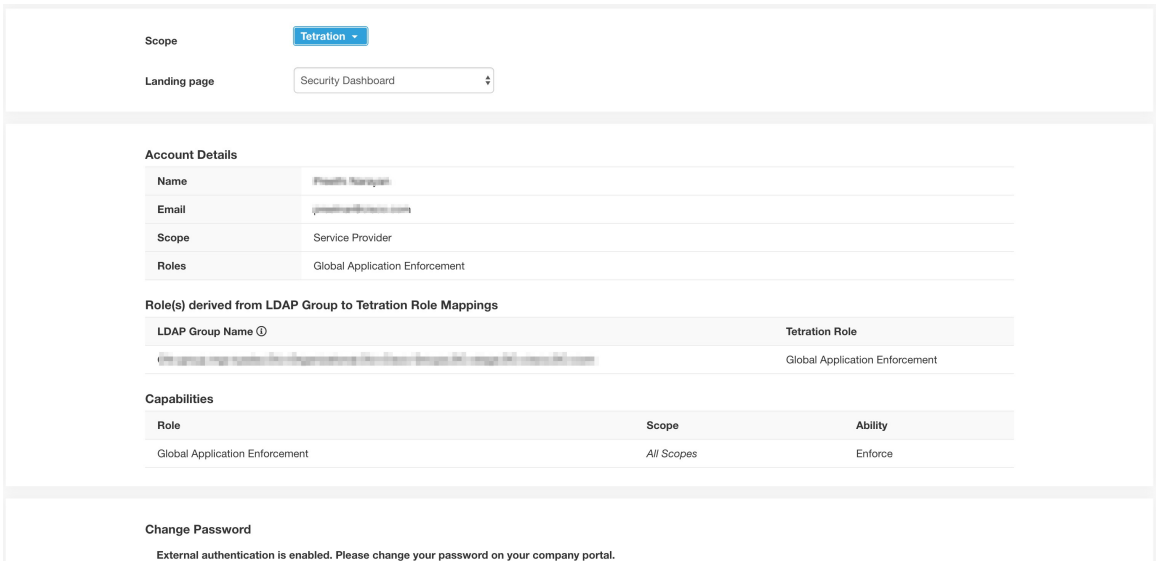
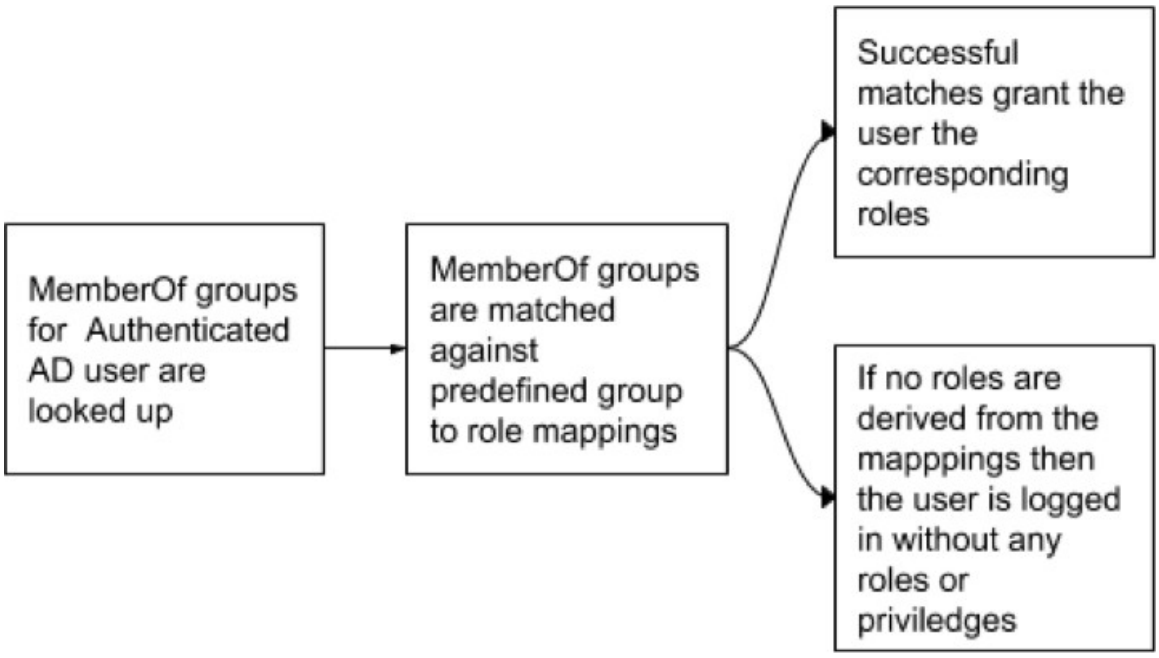


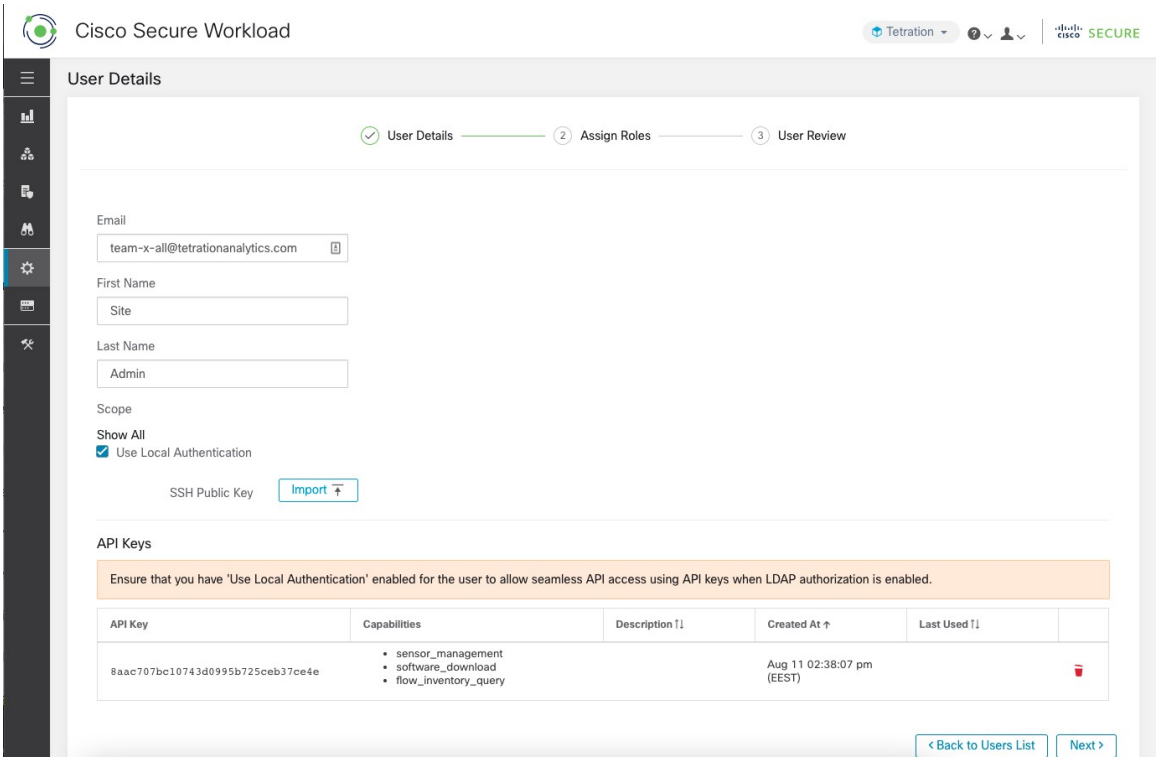
図 *17 :* 認証ワークフロー



LDAP 承認が有効な場合、ユーザーセッションが終了すると LDAP MemberOf グループから派生した Secure Workload ロールが再評価されるため、API キーを介した OpenAPI へのアクセスはシームレスに機能しなくなります。したがって、中断のない OpenAPI アクセスを保証するために、API キーを持つすべてのユーザーが 「「Use Local Authentication」オプション」を有効にすることを推奨します。

図 *18 : LDAP* 認証 *API* キーの警告

図 *19* : ユーザーページでの *LDAP* 認証 *API* キーの警告



LDAP 認証の問題のデバッグ

[外部認証（External Authentication）]、[LDAPグループからロールへのマッピング（LDAP Group to Role Mappings）] セクションで定義されたマッピングに基づいてロールがユーザーに割り当てられない場合は、ロールマッピングの設定と形式をもう一度確認してください。

- グループ文字列は文字列形式である必要があります。例：CN=group.jacpang,OU=Organizational,OU=Cisco Groups,DC=stage,DC=cisco,DC=com
- グループ名は、スペースや余分な文字が含まれず、AD に存在するものと正確に一致する必要があります。
- グループのロールマッピングは、ロールセレクタから選択する必要があります。

ユーザーロールマッピングのデバッグ手順

- 2 人のユーザーが必要です。1 人はサイト管理者（Site Admin）で、このユーザーの電子メールは AD ユーザーと同じであってはなりません。
- 以下の手順では、このユーザーを「SA ユーザー」と呼びます。
  - SA ユーザーには、前述のように、会社ページの外部認証構成でロールマッピング構成が事前に設定されています。「SA ユーザー」が [site-admin]@[ドメイン] でログインするとします。

- 「AD ユーザー」は [ad-user]@[Domain] であると仮定します。LDAP のセットアップが完了し、AD ユーザーはログインできますが、ロールを割り当てられていないと仮定します。

- AD ユーザーとして、シークレットブラウザセッションを使用してログインします。これにより、ブラウザの状態が SA ユーザーセッションから分離されます。
- SA ユーザーとしてログインし、[ユーザー（Users）] ページに移動します。
- ロールマッピングを構成する必要がある AD ユーザーの [編集（Edit）] アイコンをクリックします。
- [ユーザープロファイル（User Profile）] ページの [外部ユーザープロファイル（External User Profile）] ボタンをクリックします。
- 「memberof」セクションを含む外部認証プロファイルテーブルが表示されます。
- これは、会社ページ、[外部認証設定（External Authentication Config）]、[LDAP グループからロールへのマッピング（LDAP Group to Role Mappings）] セクションでのロールマッピングに使用できる「memberof」値の 1 つです。
- 「memberof」の行ごとの文字列全体を指定して一致させる必要があります。このロールマッピングを作成すると、同じ属性「memberof」を持つすべてのユーザーに、マップされたロールが割り当てられます。
- 新しくマップされたロールを AD ユーザーに付与するには、ユーザーはログアウトしてから再度ログインして、このマッピングプロファイルを再評価できるようにする必要があります。
- ユーザーがログインし、グループからロールへのマッピングの結果としてロールが正常に割り当てられると、一致するルールがそのユーザーの [設定（Preferences）] ページに表示されます。

シングルサインオン（SSO）の設定

このオプションを選択すると、SSO を使用してユーザーを認証できます。つまり、これを有効にすると、すべてのユーザーが認証のために ID プロバイダーのサインインページにリダイレクトされます。「Use Local Authentication」オプションが有効になっているユーザーは、サインインページで電子メールとパスワードのサインインフォームを使用して認証できます。

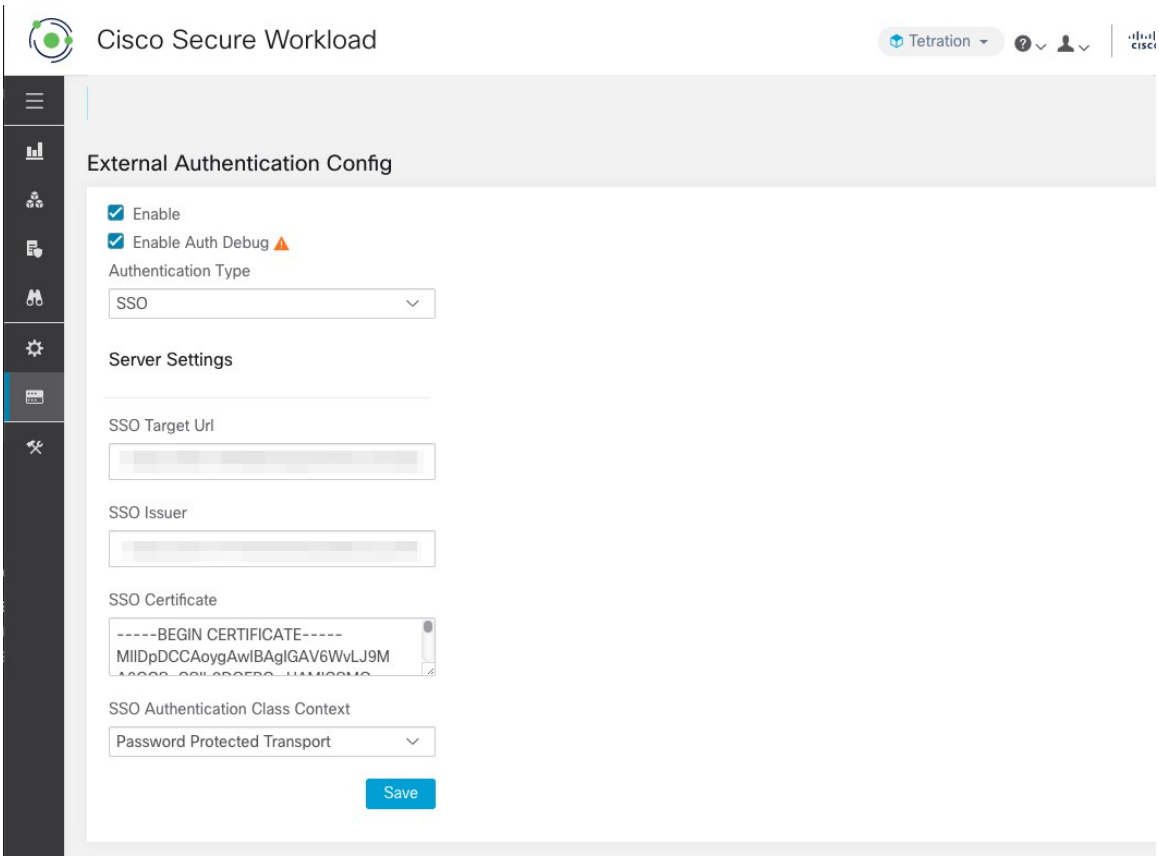
特に「Use Local Authentication」オプションが有効なユーザーがいない場合は、SSO が正しく設定されていることを確認することが重要です。推奨されるアプローチは、「Use Local Authentication」オプションをオンにして、**サイト管理者**のログイン情報を持つローカル認証されたユーザーを少なくとも 1 人指定する方法です。このユーザーは、SSO が正しく設定されていることを確認できます。接続が正常にセットアップされたら、ユーザー編集フローで [ローカル認証を使用（Use Local Authentication）] オプションをオフにして、このユーザーを外部認証に移行させることもできます。

SSOが有効になっている場合、新しいユーザーを作成するための推奨ワークフローは次のとおりです。

サイト管理者と**範囲所有者**は、新しいユーザーがSSOで初めてログインする前に、まず自分の電子メールで新しいユーザーを作成し、適切なロールと範囲を割り当てるようにお勧めします。新しいユーザーが適切なロールなしでSSOでログインした場合、デフォルトのロールはユーザーに割り当てられません。

次の表では、Secure WorkloadでSSOを設定するために設定する必要があるフィールドについて説明します。この場合のSecure Workloadは、サービスプロバイダー（SP）です。

図 *20* : シングル サインオンの設定



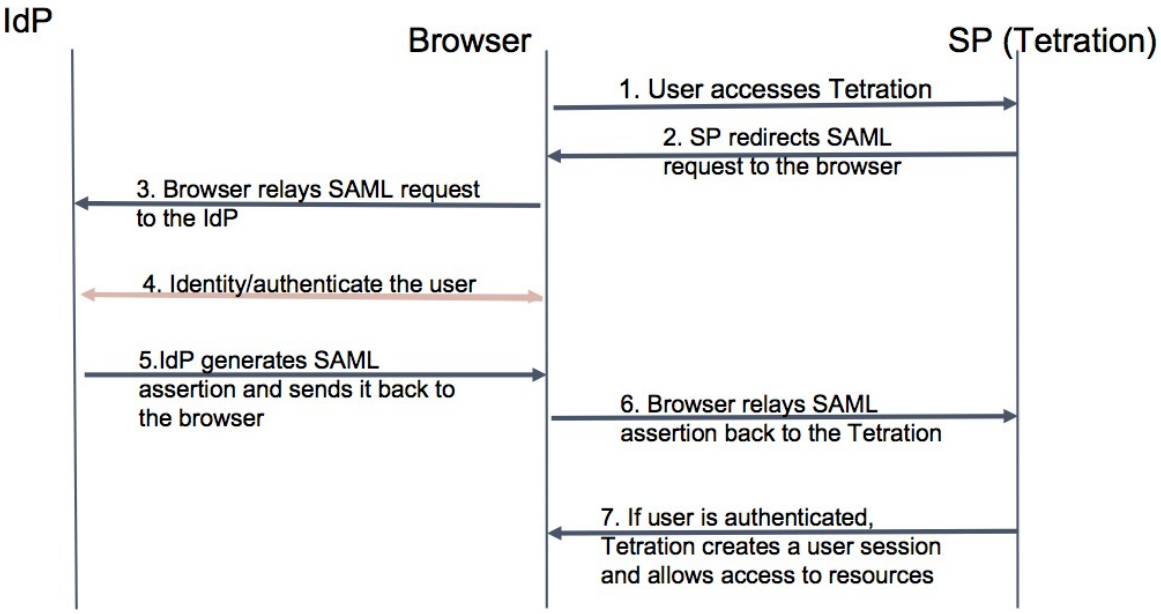
フィールド	説明
[SSOターゲットURL（SSO Target Url）]	サインインのためにユーザーがリダイレクトされるSSO IdPターゲットURL。
[SSO発行元（SSO Is-suer）]	SPのSSOエンティティID、SPを一意に識別するためのURL。これは通常、SPのメタデータです。このケースの場合： `https://<tetration-cluster-fqdn>/h4_users/saml/metadata`
[SSO証明書（SSO Certifi-cate）]	アイデンティティプロバイダー（IdP）によって提供されるSSO証明書。

フィールド	説明
[SSO AuthNコンテキスト（SSO AuthN Context）]	SAML 要求で指定された SSO AuthN コンテキストの選択肢。デフォルトのオプションは [パスワードで保護されたトランスポート（Password Protected Transport）] です。他の選択肢は、Windows および PIV ベースの認証用の [統合Windows認証（Integrated Windows Authentication）] および [X.509証明書（X.509 Certificate）] です。

SSO 設定を有効にすると、「Use Local Authentication」オプションが有効になっているユーザーを除いて、すべてのユーザーがセッションからログアウトされます。

[保存（Save）] ボタンをクリックすると、SSO 設定を保存できます。

図 *21 :* 認証ワークフロー



ID プロバイダー（IdP）に提供する情報

IdP は、認証用の SSO を設定するために Secure Workload（SP）からの情報を必要とします。次の表で、設定する必要があるフィールドについて説明します。

フィールド	説明
SSO URL（SSO Url）	SAML アサーション（IdP からの応答）を使用する認証エンドポイント（URL）。このケースの場合、次のようになります。 `https://<tetration-cluster-fqdn>/h4_users/saml/auth`
エンティティ ID（Entity Id）	これは SP のメタデータです。このケースの場合、次のようになります。 `https://<tetration-cluster-fqdn>/ h4_users/saml/metadata`

フィールド	説明
名前 ID の形式（Name ID Format）	名前 ID は電子メールアドレスです。 `'urn:oasis:names:tc:SAML:1. 1:nameid-format:emailAddress'`
属性（Attributes）	ユーザー属性は IdP から取得されます。シスコでは認証の一部としてこれらの属性を取得します。 • email • firstName • lastName 属性名が上記のとおりであることを確認してください。

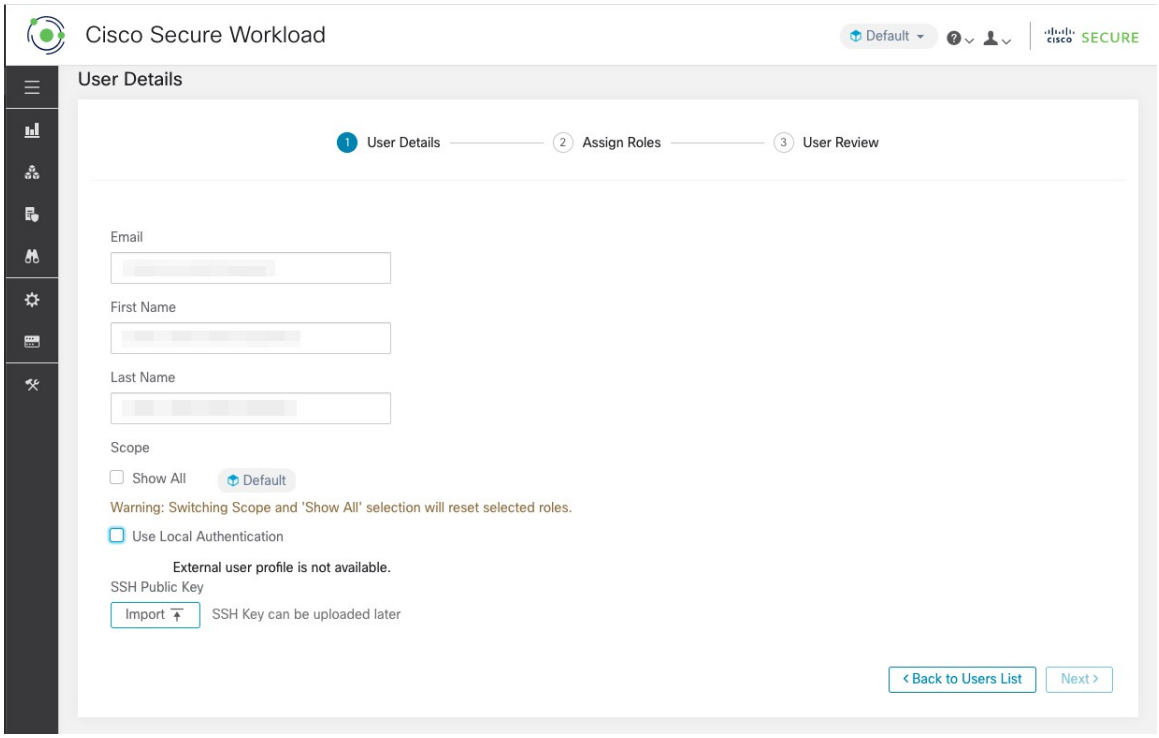
SSO の問題のデバッグ

- （サービスプロバイダーから）認証が機能することを確認できるのは設定後だけなので、SSO 構成の設定にはダウンタイムを設定します。
- 生成された IdP メタデータを確認して検証します。
- IdP と SP の間で交換されるすべての構成パラメータを確認します。
  - IdP での構成：SSO URL、対象者、名前 ID、属性など。
  - [Secure Workload Company] ページの設定：SSO ターゲット URL、SSO 発行者、および SSO 証明書。
- IdP から返されたサンプル SAML アサーションをサーバー アプリケーション ログから取得します。SAML バリデータに対して検証を行い、有効な SAML 応答であることを確認します。
- SP SSO セットアップでエラーが発生すると、IdP からエラーが生成される場合があります。ブラウザの Inspect 要素を使用すると、実行されているネットワークリクエストを確認できます。
- ユーザーのログインに問題がある場合は、Secure Workload アプリケーションへのアクセス権をそのユーザーが持っているか IdP 管理者に確認してもらいます。

「Use Local Authentication」オプション

構成がセットアップされると、サイト管理者はユーザーが外部認証を使用しないようにできます。ユーザー編集セクションの「ローカル認証を使用」フラグを有効にすると、ユーザーごとに設定できます。ユーザーに対してこのフィールドを選択すると、そのユーザーはすべてのセッションからログアウトされます。

図 *22 : Use Local Authentication*



警告 **少なくとも 1 人のユーザーがローカル認証アクセスを持っていることを確認してください。**

ユーザーの「Use Local Authentication」オプションが削除されており（つまりチェックされていない）、たまたまこのユーザーがオプションを使用した最後のユーザーだった場合、Secure Workload にサインインするためのローカル認証アクセスを持つユーザーがいなくなります。つまり、設定や接続の問題など、外部認証システムに何らかの障害が発生した場合、サインインできるユーザーがいないということになります。ローカルで認証された最後のユーザーを削除しようとすると、警告が表示されます。

外部認証を介してログインするユーザーのセッションは短くなり、セッションの有効期限が切れるとログインするように求められます。外部認証を介してログインするユーザーは、サイトでパスワードをリセットできません（勤務先の Web サイトで行う必要があります）。ただし、ユーザーに「ローカル認証を使用」フラグが設定されている場合は、パスワードのリセットが可能です。

SSL 証明書およびキー

Secure Workload UI への完全に検証可能な HTTPS アクセスを有効にするには、UI のドメイン名に固有の SSL 証明書と、SSL 証明書の公開キーと一致する RSA 秘密キーをクラスタにアップロードします。

SSL 証明書は、Secure Workload UI 仮想 IP（VIP）アドレスを参照するために使用される完全修飾ドメイン名（FQDN）の形式に応じて、2 つの方法で取得できます。Secure Workload FQDN が Tetration.cisco.com などのエンタープライズドメイン名に基づいている場合、ベースドメインを所有するエンタープライズ認証局（CA）が SSL 証明書を発行します。それ以外の場合は、信頼できる SSL 証明書ベンダーを使用して、FQDN の SSL 証明書を発行できます。

（注） Secure Workload UI はサーバー名表示（SNI）をサポートしていますが、証明書で指定されたサブジェクトの代替名（SAN）は一致しないことに注意してください。たとえば、証明書の共通名（CN）が tetration.cisco.com であり、証明書にtetration1.cisco.com の SAN が含まれている場合、ホスト名はその証明書では提供されないため、HTTPS リクエストは SNI 互換ブラウザを使用して tetration1.cisco.com のクラスタに送信されます。CN で指定されたホスト名以外のホスト名でクラスタに対して行われた HTTPS リクエストは、クラスタにインストールされているデフォルトの自己署名証明書を使用して処理されます。これらのリクエストの結果、ブラウザに警告が表示されます。

サイト管理者と**カスタマーサポートのユーザー**は、SSL 証明書を使用できます。左側のナビゲーションバーで、**[プラットフォーム（Platform）]**>**[SSL証明書（SSL Certificate）]**をクリックします。

証明書とキーをインポートするには、[新しい証明書とキーのインポート（Import New Certifcate and Key）] ボタンをクリックします。

（注） SSL 証明書と秘密キーの最初のインポートは、信頼ネットワーク接続を介してクラスタに対して実行し、トランスポート層にアクセスできる悪意のある第三者が秘密キーを傍受できないようにする必要があります。

SSL 証明書とキーについて、次の情報を入力します。

[名前（NAME）] : 証明書キーペアの任意の名前にできます。この名前は、インストールされている SSL 証明書を確認するときに役立ちます。

[X509証明書（X509 Certificate）] フィールドには、プライバシー強化メール（PEM）形式の SSL 証明書文字列を入力できます。SSL 証明書に中間 CA バンドルが必要な場合は、証明書の後に CA バンドルを連結して、Secure Workload FQDN の SSL 証明書が証明書ファイルの先頭になるようにします。

次の形式にする必要があります。

```
-----BEGIN CERTIFICATE-----

< Certificate for Secure Workload FQDN >

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

< Intermediary CA 1 content >

-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----

< Intermediary CA 2 content >

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

< Root CA content >

-----END CERTIFICATE-----
```

[RSA秘密キー（RSA Private Key）] フィールドには、前述の証明書で署名された公開キーの RSA 秘密キーを入力する必要があります。次の形式にする必要があります。

```
-----BEGIN RSA PRIVATE KEY-----

< private key data >

-----END RSA PRIVATE KEY-----
```

（注） RSA秘密キーは暗号化されていない必要があります。RSA秘密キーが暗号化されている場合、「500 内部サーバーエラー」が発生します。

インポートボタンを押すと、検証手順が実行され、証明書に署名された公開キーと秘密キーが実際にRSAキーペアであることが確認されます。検証に成功すると、証明書バンドルのSHA1ダイジェスト（SHA1 署名と作成時刻）が表示されます。

ブラウザをリロードして、Secure Workload UI への SSL 接続で新しくインポートされた SSL 証明書が使用されていることを確認します。

クラスタの設定

このセクションには、カスタマーネットワークおよび管理連絡先に関する Secure Workload クラスタの実行コンフィギュレーションが表示されます。編集可能な値は鉛筆アイコンで示されます。

（注） a. エージェント接続の強力な SSL 暗号：このオプションを有効にすると、 TLS-1.0 および TLS-1.1 プロトコルと次の暗号が、SSL ネゴシエーション中に Secure Workload クラスタによって受け入れられません。DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA

次の接続では、TLS ハンドシェイク中に強力な暗号が使用されます。

1. Secure Workload へのすべての API および UI 接続。
2. Secure Workload へのすべての可視性と適用エージェントの接続。

古い SSL ライブラリでは、このオプションがサポートされていない場合があります。

サイト管理者と**カスタマーサポートのユーザー**は、この設定にアクセスできます。左側のナビゲーションバーで、**[プラットフォーム（Platform）]**>**[クラスタ構成（Cluster Configuration）]** をクリックします。

構成の編集後、新しい構成がクラスタ全体に適用されるまでには時間がかかり、その間、特定の構成が強調表示されます。

外部 IPv6 クラスタの接続

物理 Cisco Secure Workload クラスタは、外部 IPv4 および IPv6 ネットワークの両方に接続するように設定できます。IPv4 接続は必須ですが、IPv6 接続は任意です。IPv6 接続は、一度設定すると無効化できません。クラスタの外部ネットワークの IPv6 接続は、展開またはアップグレード中にのみ有効にできます。アップグレード中に外部 IPv6 クラスタ接続を有効にする方法の詳細については、Cisco Secure Workload アップグレードガイド [英語] を参照してください。展開中に外部 IPv6 クラスタ接続を有効にする方法の詳細については、Cisco Secure Workload ハードウェア導入ガイド [英語] を参照してください。

始める前に

エージェントをデュアルスタックモード（IPv4 と IPv6 の両方をサポート）で動作させるには

前提条件

- クラスタでは IPv6 が有効になっている必要があります。
- FQDN の DNS に A および AAAA レコード（IPv4 および IPv6 用）を作成し、ドメイン名が解決されるまで待ちます。

エージェントがデュアルスタックモードで動作するように「センサーVIP FQDN」を設定する

ステップ 1 左側のナビゲーションバーから、**[プラットフォーム（Platform）]**>**[クラスタ構成（Cluster Configuration）]** を選択します。

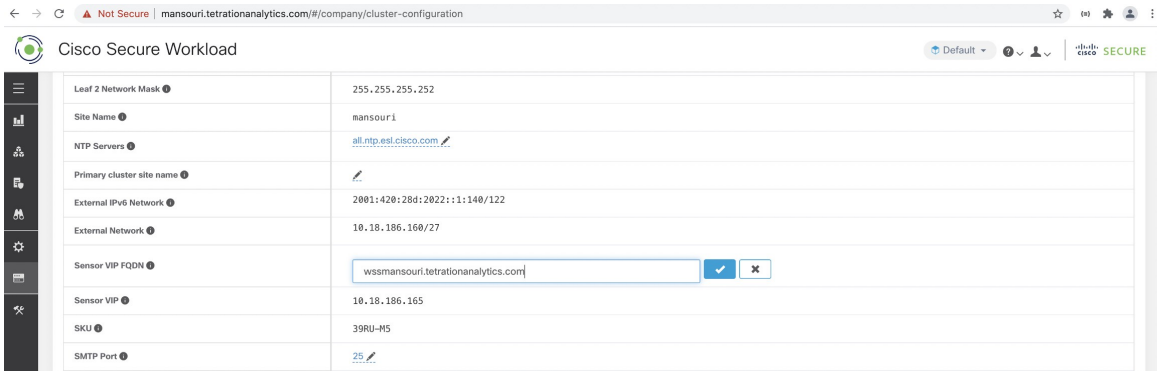
ステップ 2 [センサーIPv6 VIP（Sensor IPv6 VIP）]、[センサーVIP（Sensor VIP）]、および[センサーVIP FQDN（Sensor VIP FQDN）] フィールドを探します。[センサーIPv6 VIP（Sensor IPv6 VIP）] と [センサーVIP（Sensor VIP）] は設定されている必要があります。

ステップ 3 [センサーVIP FQDN（Sensor VIP FQDN）] が設定されていない場合は、前述の手順で作成した FQDN に設定します。設定する前に、FQDN の DNS の A レコードと AAAA レコードを解決する必要があります。

ステップ 4 [センサーVIP FQDN（Sensor VIP FQDN）] がすでに設定されている場合は、[センサーVIP FQDN（Sensor VIP FQDN）] フィールドで設定された FQDN の DNS に A レコードと AAAA レコードがあることを確認し、[センサーVIP FQDN（Sensor VIP FQDN）] フィールドをクリックして同じ値に保存し、更新されるようにします。

ステップ 5 フィールドの更新が完了すると（約 20 分後にステータスが自動的に更新されます）、エージェントは IPv4 と IPv6 の両方を介してクラスタに接続できるようになります。

ステップ 6 有効な [センサーVIP FQDN（Sensor VIP FQDN）] は 1 回だけ設定できます。



（注） AIX の IPv6 適用のサポートはありません。デュアルスタックモードの要件と制限の詳細については、Cisco Secure Workload アップグレードガイド [英語] を参照してください。

使用状況分析

シスコでは、Secure Workload ユーザーインターフェイスを改善するためにのみ使用するデータを収集しています。収集したデータは、サーバーに送信される前に一方向ハッシュによって匿名化されます。データ収集はデフォルトで有効になっており、このページで切り替えることができます。このプライバシー設定の構成可能性は、オンプレミスアプライアンスの場合はアプライアンス単位、Cisco Secure Workload SaaS の場合はテナント単位です。

サイト管理者と**カスタマーサポートのユーザー**は、使用状況分析を有効化または無効化できます。左側のナビゲーションバーで、**[管理（Manage）]** > **[使用状況分析（Usage Analytics）]**をクリックします。

アイドルセッション

このセクションでは、ローカルデータベースを使用して認証を行う場合に、ログイン試行の失敗によってユーザーアカウントがどのようにロックされるかについて説明します。

ステップ 1 電子メールアドレスとパスワードを使用したログイン試行が 5 回失敗すると、アカウントがロックされます。

（注） プロービングに対するセキュリティ対策として、ロックされたアカウントにサインインを試みた場合、ロックを示す具体的なメッセージはログインインターフェイスに表示されません。

ステップ 2 ロックアウト間隔は30分に設定されます。アカウントのロックが解除されたら、正しいパスワードを使用してログインするか、[パスワードを忘れた場合（Forgot password?）] をクリックしてパスワードの回復を開始します。

（注） 正常にサインインしたユーザーは、1 時間何も操作しないとログアウトされます。このタイムアウトは、**[管理（Manage）] > [セッション構成（Session Configuration）]** で設定します。

設定

[設定（Preferences）] ページにはアカウントの詳細が表示され、表示設定の更新、ランディングページの変更、パスワードの変更、および 2 要素認証の設定を行うことができます。

ランディングページ設定の変更

サインイン時に表示されるページを変更するには：

ステップ 1 ウィンドウの右上隅にあるユーザーアイコンをクリックし、[ユーザー設定（User preferences）] を選択します。

ステップ 2 [ランディングページ（Landing Page）] を選択します。メニューオプションを選択するとすぐに、設定が保存されます。変更を確認するには、ページの左上隅にある Secure Workload ロゴをクリックします。

パスワードの変更

ステップ 1 右上隅にあるユーザーアイコンをクリックします。

ステップ 2 [ユーザー設定（User Preferences）] をクリックします。

ステップ 3 [パスワードの変更（Change Password）] ペインで、[古いパスワード（Old Password）] フィールドに現在のパスワードを入力します。

ステップ 4 [パスワード（Password）] フィールドに新しいパスワードを入力します。

ステップ 5 [パスワードの確認（Confirm Password）] フィールドに新しいパスワードを再度入力します。

ステップ 6 変更を送信するには、[パスワード変更（Change Password）] をクリックします。

（注） **パスワードは 8 ～ 128 文字で、以下の文字記号を少なくとも 1 つ含める必要があります。**

- アルファベット小文字（a b c d. . .）
- アルファベット大文字（A B C D. . .）
- 数字（0 1 2 3 4 5 6 7 8 9）
- 特殊文字（ ! " # $ % & ’ ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ‘ { | } ~) スペースを含む

パスワードの回復

このセクションでは、パスワードを回復する方法について説明します。

始める前に

パスワードをリセットするには、まずアカウントを取得する必要があります。**サイト管理者**および**カスタマーサポートユーザー**は、新しいアカウントを追加できます。

ステップ 1 ブラウザで Cisco Secure Workload URL にアクセスし、[パスワードを忘れた場合（Forgot Password）] リンクをクリックします。[パスワードをお忘れですか?（Forgot your password?）] ダイアログが表示されます。

ステップ 2 [電子メール（Email）] フィールドに電子メールアドレスを入力します。

ステップ 3 [Reset Password] をクリックします。

パスワードのリセット手順がメールに送信されます。

（注） 電子メールベースのパスワード回復にはワンタイムパスワードを含めることができないため、二要素認証のパスワード回復手順では、Secure Workload カスタマーサポートに連絡する必要があります。

二要素認証の有効化

このセクションでは、二要素認証を有効にする方法について説明します。

ステップ 1 右上隅にあるユーザーアイコンをクリックします。

ステップ 2 [ユーザー設定（User Preferences）] をクリックします。

ステップ 3 [二要素認証（Two-Factor Authentication）] ペインで、[有効にする（Enable）] ボタンをクリックします。新しい [二要素認証（Two-Factor Authentication）] ペインが表示されます。

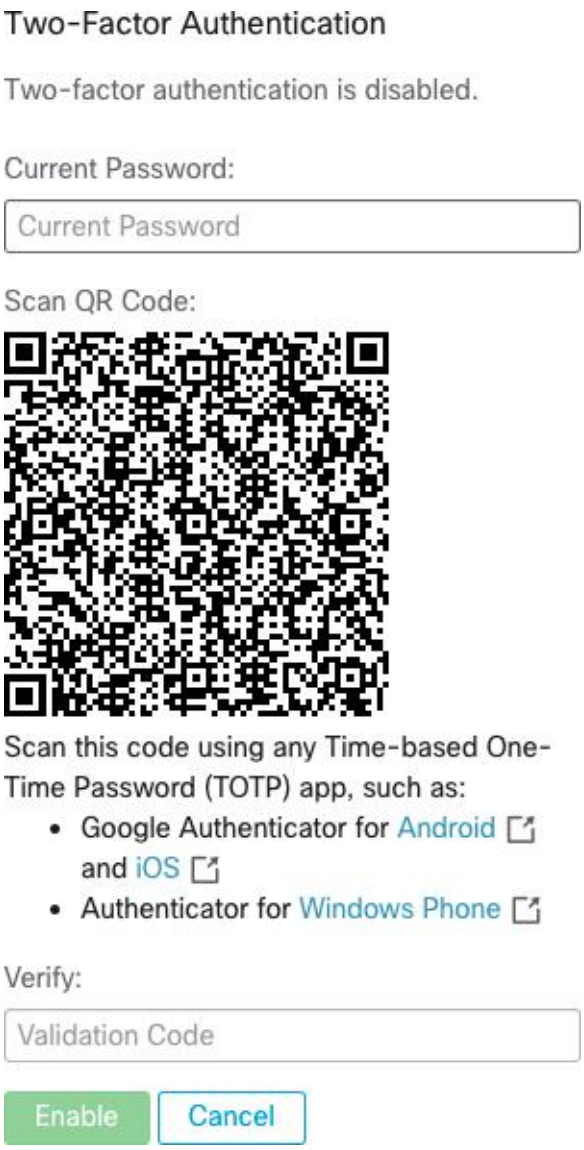
ステップ 4 パスワードを入力します。

ステップ 5 Google Authenticator（Android または iOS の場合）または Authenticator（Windows Phone の場合）などの時間ベースのワンタイムパスワード（TOTP）アプリケーションを使用して、[現在のパスワード（Current Password）] フィールドの下に表示されている QR コードをスキャンします。

ステップ 6 選択した TOTP アプリケーションによって表示される検証コードを入力します。

ステップ 7 [有効（Enable）] をクリックします。

図 *23 : [二要素認証（Two-Factor Authentication）] ペイン*



次にシステムにログインする際には、[二要素認証を使用する（Use two-factor authentication）] チェックボックスをオンにして、TOTP アプリケーションに表示される確認コードを入力してサインインする必要があります。

（注） 電子メールベースのパスワード回復にはワンタイムパスワードを含めることができないため、二要素認証のパスワード回復手順では、Secure Workload カスタマーサポートに連絡する必要があります。

二要素認証の無効化

このセクションでは、二要素認証を無効にする方法について説明します。

ステップ 1 右上隅にあるユーザーアイコンをクリックします。

ステップ 2 [ユーザー設定（User Preferences）] をクリックします。

ステップ 3 二要素認証で、[無効にする（Disable）] ボタンをクリックします。[二要素認証（Two-Factor Authentication）] ペインが表示されます。

ステップ 4 パスワードを入力します。

ステップ 5 [無効にする（Disable）] ボタンを再度クリックします。

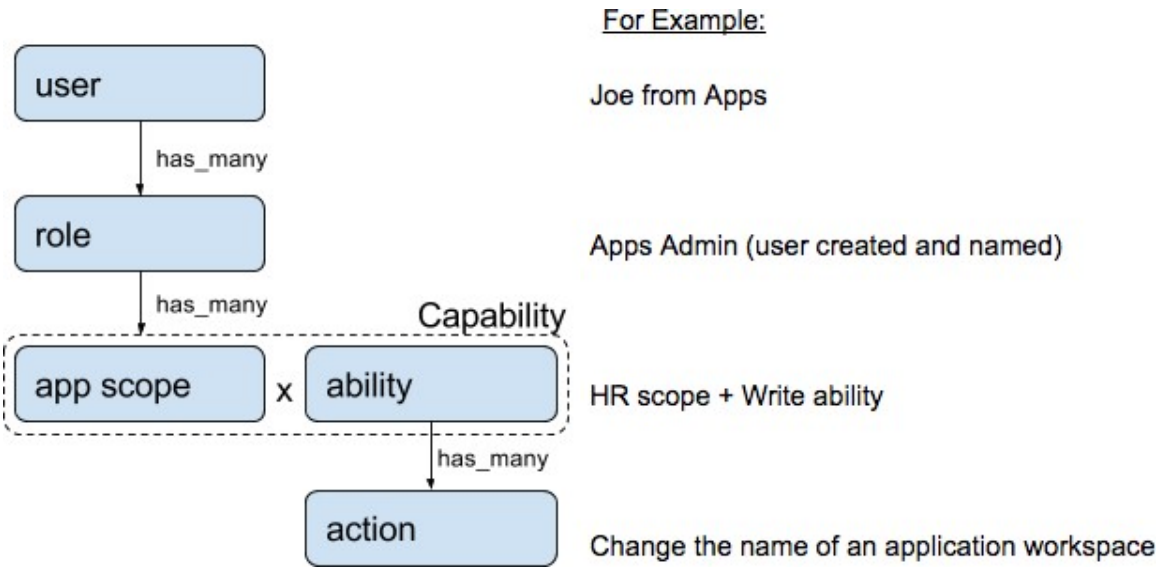
ログイン時に二要素認証コードを入力する必要はなくなりました。

ロール

ロールベースアクセスコントロール（RBAC）モデルを使用して、機能とデータへのアクセスを制限できます。

- ユーザー：Cisco Secure Workload へのログインアクセス権を持つユーザー
- ロール：ユーザーが作成した、ユーザーに割り当てることが可能な一連の機能
- 機能：範囲 + 能力のペア
- 能力：アクションの集合
- アクション：「ワークスペース名の変更」などの低レベルのユーザーアクション

図 *24 :* ロールモデル



ユーザーは、任意の数のロールを持つことができます。ロールには、任意の数の機能を含めることができます。たとえば、「HR 検索エンジニア」ロールには、可視性とコンテキストを提供する「HR 範囲での読み取り」機能と、このロールを割り当てられたエンジニアがアプリケーションに関連した特定の変更を実施できるようにする「HR 検索の実行」機能を含めることが可能です。

ロールには一連の機能が含まれ、[ユーザー（Users）]ページでユーザーに割り当てられます。ユーザーは、任意の数のロールを持つことができます。ロールには、任意の数の機能を含めることができます。

ユーザーが迅速に利用開始できるように、6 つのシステムロールが定義されています。システムロールは、**すべての範囲**（システム上の全データ）へのさまざまなレベルのアクセスを定義します。各システムロールの定義を以下に示します。

ロール	説明
エージェントインストーラ	インストール、モニター、アップグレード、変換を含むエージェントのライフサイクルを管理する機能を提供しますが、エージェントを削除したりエージェント設定プロファイルにアクセスしたりすることは**できません**。
カスタマー サポート	テクニカルサポートまたはアドバンスドサービスの場合。クラスタメンテナンス機能へのアクセスが可能です。サイト管理者と同じアクセス権が与えられますが、ユーザーを変更することは**できません**。
サイト管理者	ユーザー、エージェントなどを管理する能力を提供します。すべての機能とデータを表示および編集できます。少なくとも 1 人のサイト管理者が必要です。

ロール	説明
グローバルアプリケーション適用	すべての範囲での適用能力を提供します。
グローバルアプリケーション管理	すべての範囲での実行能力を提供します。
グローバル読み取り専用	すべての範囲での読み取り能力を提供します。

能力と機能

ロールは、範囲と能力を含む機能で構成されます。これらは、許可されるアクション、およびそれらが適用されるデータのセットを定義します。たとえば、（HR、読み取り） 機能は、「HR 範囲における読み取り能力」として解釈される必要があります。この機能により、HR 範囲とそのすべての子にアクセスできます。

能力	説明
読み取り	フロー、アプリケーション、インベントリフィルタを含むすべてのデータを読み取ります。
書き込み	アプリケーションとインベントリフィルタに変更を加えます。
実行	ポリシーの自動検出を実行し、分析のためにポリシーを公開します。
適用	指定された範囲に関連付けられたアプリケーション ワークスペースで定義されたポリシーを適用します。
オーナー	アプリケーション ワークスペースをセカンダリからプライマリに切り替えるために必要です。ユーザー アプリケーション セッションの管理、データタップの追加、視覚化データソースの作成などのデータタップ管理機能へのアクセス。

重要 能力は継承されます。たとえば、実行能力では、読み取り、書き込み、および実行アクションがすべて許可されます。

重要 能力は、範囲および範囲のすべての子に適用されます。

ロール別のメニューアクセス

ユーザーが表示および使用できるメニューは、ユーザーに割り当てられたロールによって異なります。

表 *1 : [*概要（*Overview***）*]* メニュー**

メニュー	オプション	サイト管理者	カスタマーサポート	アプリケーションのグローバル管理	グローバルに読み取り専用	アプリケーションのグローバル適用	エージェントインストーラ
[概要（Overview）]	[概要（Overview）]	○	○	○	○	○	×

表 *2 : [*整理（*Organize***）*]* メニュー**

メニュー	オプション	サイト管理者	カスタマーサポート	アプリケーションのグローバル管理	グローバルに読み取り専用	アプリケーションのグローバル適用	エージェントインストーラ
[整理（Organize）]	[範囲とインベントリ（Scopes and Inventory）]	○	○	○	○	○	×
[整理（Organize）]	[ユーザーアップロードラベル（User Uploaded Labels）]	○	○	×	×	×	×
[整理（Organize）]	[インベントリフィルタ（Inventory Filters）]	○	○	○	○	○	×

表 *3 :* [防御（*Defend*）] メニュー

メニュー	オプション	サイト管理者	カスタマーサポート	アプリケーションのグローバル管理	グローバルに読み取り専用	アプリケーションのグローバル適用	エージェントインストーラ
[防御（Defend）]	[セグメンテーション（Segmentation）]	○	○	○	○	×	×
[防御（Defend）]	[適用ステータス（Enforcement Status）]	○	○	×	×	×	×
[防御（Defend）]	[ポリシーテンプレート（Policy Templates）]	○	○	×	×	×	×
[防御（Defend）]	[フォレンジックルール（Forensic Rules）]	○	○	×	×	×	×

表 *4 :* [調査（*investigate*）] メニュー

メニュー	オプション	サイト管理者	カスタマーサポート	アプリケーションのグローバル管理	グローバルに読み取り専用	アプリケーションのグローバル適用	エージェントインストーラ
[調査（Investigate）]	[トラフィック（Traffic）]	○	○	○	○	○	×
[調査（Investigate）]	[アラート（Alerts）]	○	○	○	○	○	×
[調査（Investigate）]	[脆弱性（Vulnerabilities）]	○	○	○	○	○	×

メニュー	オプション	サイト管理者	カスタマーサポート	アプリケーションのグローバル管理	グローバルに読み取り専用	アプリケーションのグローバル適用	エージェントインストーラ
[調査（Investigate）]	[フォレンジック（Forensics）]	○	○	○	○	○	×
[調査（Investigate）]	[近隣（Neighborhood）]	○	○	○	○	○	×

表 *5 : [*管理（*Manage***）*]* メニュー**

メニュー	オプション	サイト管理者	カスタマーサポート	アプリケーションのグローバル管理	グローバルに読み取り専用	アプリケーションのグローバル適用	エージェントインストーラ
[管理（Manage）]	[エージェント（Agents）]	○	○	×	×	×	○
[管理（Manage）]	[アラート設定（Alerts Configs）]	○	○	○	○	○	×
[管理（Manage）]	[変更ログ（Change Logs）]	○	×	×	×	×	×
[管理（Manage）]	[コネクタ（Connectors）]	○	○	×	×	×	×
[管理（Manage）]	[外部オーケストレータ（External Orchestrators）]	○	○	×	×	×	×
[管理（Manage）]	[セキュアコネクタ（Secure Connector）]	○	○	×	×	×	×

メニュー	オプション	サイト管理者	カスタマーサポート	アプリケーションのグローバル管理	グローバルに読み取り専用	アプリケーションのグローバル適用	エージェントインストーラ
[管理（Manage）]	[仮想アプライアンス（Virtual Appliances）]	○	○	×	×	×	×
[管理（Manage）]	[ユーザー（Users）]	○	○	×	×	×	×
[管理（Manage）]	ロール	○	○	×	×	×	×
[管理（Manage）]	[脅威インテリジェンス（Threat Intelligence）]	○	○	×	×	×	×
[管理（Manage）]	[ライセンス（Licenses）]	○	×	×	×	×	×
[管理（Manage）]	[収集ルール（Collection Rules）]	○	○	×	×	×	×
[管理（Manage）]	[セッション設定（Session Configuration）]	○	○	×	×	×	×
[管理（Manage）]	[使用状況分析（Usage Analytics）]	○	○	×	×	×	×
[管理（Manage）]	[データタップ管理（Data Tap Admin）]	○	×	×	×	×	×

表 *6 : [*プラットフォーム（***Platform***）*]* メニュー

メニュー	オプション	サイト管理者	カスタマーサポート	アプリケーションのグローバル管理	グローバルに読み取り専用	アプリケーションのグローバル適用	エージェントインストーラ
[プラットフォーム（Platform）]	[テナント（Tenants）]	○	○	×	×	×	×
[プラットフォーム（Platform）]	[クラスタ設定（Cluster Configuration）]	○	○	×	×	×	×
[プラットフォーム（Platform）]	[アウトバウンドHTTP（Outbound HTTP）]	○	○	×	×	×	×
[プラットフォーム（Platform）]	コレクタ	○	○	×	×	×	×
[プラットフォーム（Platform）]	[外部認証（External Authentication）]	○	○	×	×	×	×
[プラットフォーム（Platform）]	[SSL証明書（SSL Certificate）]	○	○	×	×	×	×
[プラットフォーム（Platform）]	[ログインページメッセージ（Login Page Message）]	○	○	×	×	×	×
[プラットフォーム（Platform）]	[連携（Federation）]	以下を参照	以下を参照	×	×	×	×

メニュー	オプション	サイト管理者	カスタマーサポート	アプリケーションのグローバル管理	グローバルに読み取り専用	アプリケーションのグローバル適用	エージェントインストーラ
[プラットフォーム（Platform）]	[データのバックアップ（Data Backup）]	以下を参照	以下を参照	×	×	×	×
[プラットフォーム（Platform）]	[データの復元（Data Restore）]	以下を参照	以下を参照	×	×	×	×
[プラットフォーム（Platform）]	[アップグレード/再起動/シャットダウン（Upgrade/Reboot/Shutdown）]	○	○	×	×	×	×

（注）

- 連携が有効になっている場合、サイト管理者およびカスタマーサポートのロールで [連携（Federation）] オプションを使用できます。
- データのバックアップとデータの復元が有効になっている場合、サイト管理者とカスタマーサポートのロールで、[データのバックアップ（Data Backup）] と [データの復元（Data Restore）] オプションを使用できます。

表 *7 : [*トラブルシューティング（*Troubleshooting]* メニュー

メニュー	オプション	サイト管理者	カスタマーサポート	アプリケーションのグローバル管理	グローバルに読み取り専用	アプリケーションのグローバル適用	エージェントインストーラ
[トラブルシューティング（Troubleshoot）]	サービスのステータス	○	○	×	×	×	×
[トラブルシューティング（Troubleshoot）]	[クラスタのステータス（Cluster Status）]	以下を参照	以下を参照	×	×	×	×
[トラブルシューティング（Troubleshoot）]	[仮想マシン（Virtual Machine）]	○	○	×	×	×	×
[トラブルシューティング（Troubleshoot）]	[スナップショット（Snapshots）]	○	○	×	×	×	×
[トラブルシューティング（Troubleshoot）]	[メンテナンスエクスプローラ（Maintenance Explorer）]	○	○	×	×	×	×
[トラブルシューティング（Troubleshoot）]	[救済（Resque）]	○	○	×	×	×	×
[トラブルシューティング（Troubleshoot）]	[Hawkeye]（チャート）	○	○	×	×	×	×

メニュー	オプション	サイト管理者	カスタマーサポート	アプリケーションのグローバル管理	グローバルに読み取り専用	アプリケーションのグローバル適用	エージェントインストーラ
[トラブルシューティング（Troubleshoot）]	[Abyss]（パイプライン）	○	○	×	×	×	×

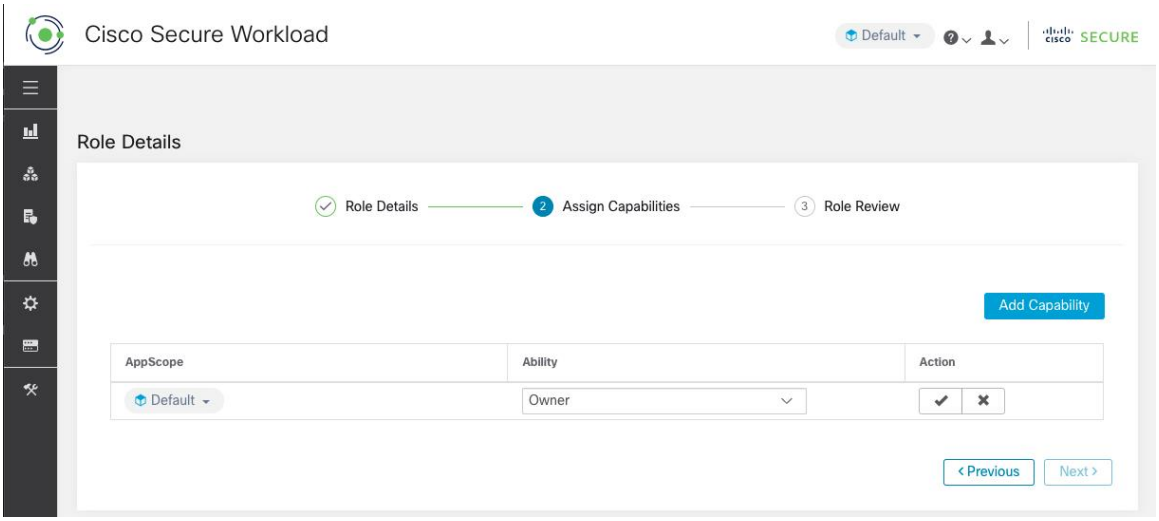
（注） [クラスタのステータス（Cluster Status）] オプションは、クラスタタイプが「物理」または「OCI」の場合に、サイト管理者およびカスタマーサポートのロールで使用できます。

新しいロールの作成

始める前に

[サイト管理者（Site Admin）] または [カスタマーサポート（Customer Support）] のユーザーロールが割り当てられている必要があります。

1. 左側のナビゲーションバーで、**[管理（Manage）]>[ロール（Roles）]** をクリックします。
2. [ロールの作成（Create Role）] ボタンをクリックします。[ロール（Roles）] パネルが表示されます。



[ロールの作成（Create Role）] ウィザードを使用したロールの作成は、3 つのステップから成るプロセスです。

ステップ 1 a) 以下のフィールドに適切な値を入力します。

フィールド	説明
[名前（Name）]	ロールを識別するための名前。
[説明（Description）]	ロールに関するコンテキストを追加するための簡単な説明。

b) [次へ（Next）] ボタンをクリックして次のステップに移動するか、[ロールページに戻る（Back to Roles Page）] をクリックして [ロール（Roles）] ページに戻ります。

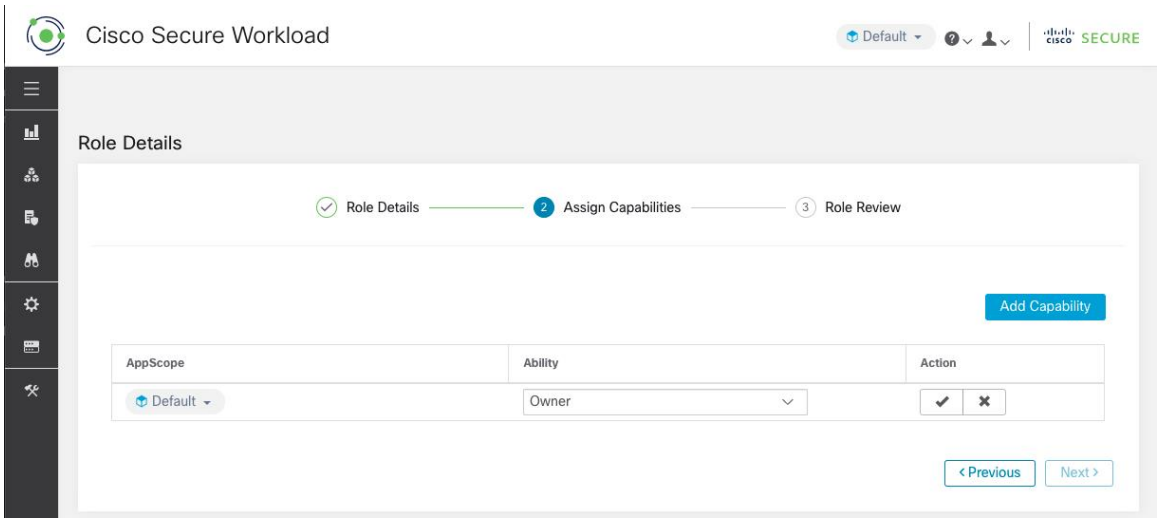
ステップ 2 a) [ケーパビリティの追加（Add Capability）] ボタンをクリックすると、一番上の行に作成フォームが表示されます。

b) 範囲と権限を選択します。

c) チェックマークボタンをクリックして新しいケーパビリティを作成するか、キャンセルボタンをクリックしてキャンセルします。

d) [次へ（Next）] ボタンをクリックしてロールの詳細を確認するか、[前へ（Previous）] をクリックして戻って編集します。

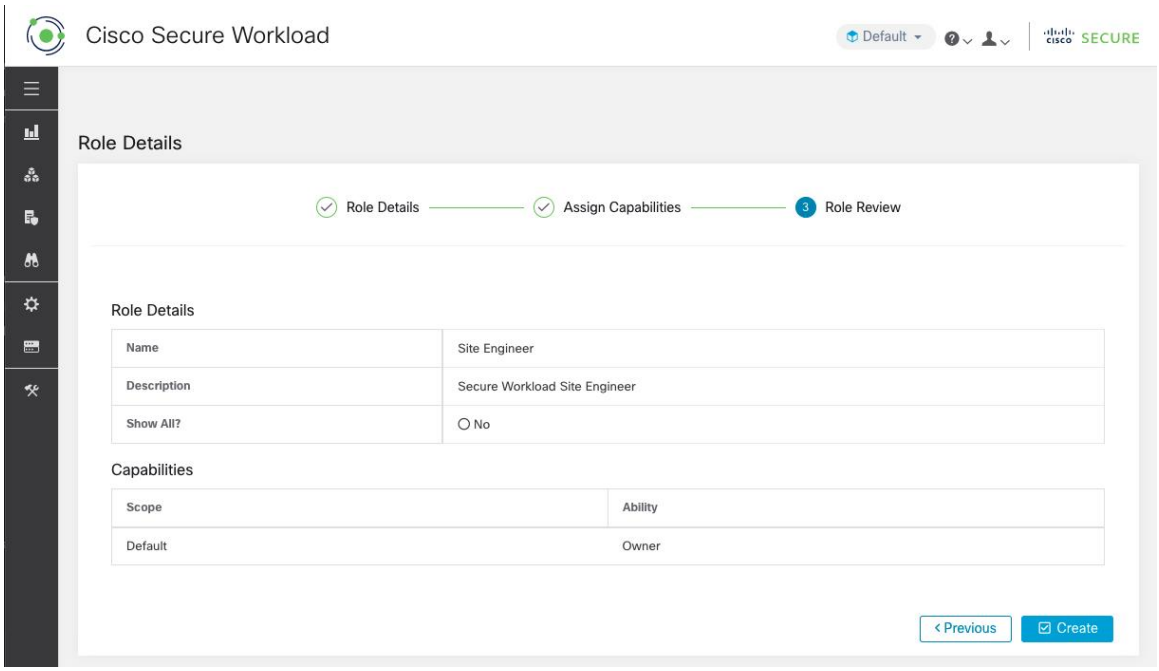
図 *25 :* ケーパビリティの割り当て



ステップ 3 a) ロールの詳細とケーパビリティを確認します。

b) [作成（Create）] をクリックして、ロールを作成します。

図 *26 :* ロールの確認



ロールの編集

このセクションでは、**サイト管理者**と**カスタマーサポートユーザー**がロールを編集する方法について説明します。

始める前に

サイト管理者またはカスタマーサポートユーザーである必要があります。

1. 左側のナビゲーションバーで、**[管理（Manage）]**>**[ロール（Roles）]**をクリックします。
2. 編集するロールの行で、右側の列にある [編集（Edit）] ボタンをクリックします。[ロール（Roles）] パネルが表示されます。

[ロールの編集（Edit Role）] ウィザードを使用したロールの編集は、3 つのステップから成るプロセスです。

ステップ 1 a) 必要に応じて、名前や説明を更新します。

b) [次へ（Next）] ボタンをクリックして次のステップに移動するか、[ロールページに戻る（Back to Roles Page）] をクリックして [ロール（Roles）] ページに戻ります。

ステップ 2 a) 必要に応じてケーパビリティを削除します。削除するケーパビリティの行で、右側の列にある [削除（Delete）] アイコンをクリックします。

b) 追加するには、[ケーパビリティの追加（Add Capability）] ボタンをクリックして、一番上の行に作成フォームを表示します。
c) 範囲と権限を選択します。
d) [次へ（Next）] ボタンをクリックしてロールの詳細を確認するか、[前へ（Previous）] をクリックして戻って編集します。

ステップ 3 a) ロールの詳細とケーパビリティを確認します。
b) [更新（Update）] をクリックしてロールを作成するか、[前へ（Previous）] をクリックして編集します。ロールの詳細とケーパビリティの割り当てへの変更は、[更新（Update）] をクリックした後に保存されます。

（注） ケーパビリティは編集できません。削除して作成し直す必要があります。

変更ログ：役割

ルート範囲で SCOPE_OWNER 機能を持つ [サイト管理者（Site Admins）] およびユーザーは、以下に示す [アクション（Action）] 列のアイコンをクリックして、各ロールのログの変更を表示できます。

図 *27*：ログの変更

該当するユーザーは、テーブルの下にある [削除されたロールを表示（View Deleted Roles）] リンクをクリックして、削除されたロールのリストを表示することもできます。

変更ログの詳細については、「ログの変更」を参照してください。ルート範囲の所有者は、その範囲に属するエンティティの変更ログエントリの表示に制限されます。

スコープ

（注） [範囲（Scopes）] ページは [インベントリ検索（Inventory Search）] と統合されました。以下のリンクのヘルプについては、[範囲とインベントリ（Scopes and Inventory）] ページを参照してください。

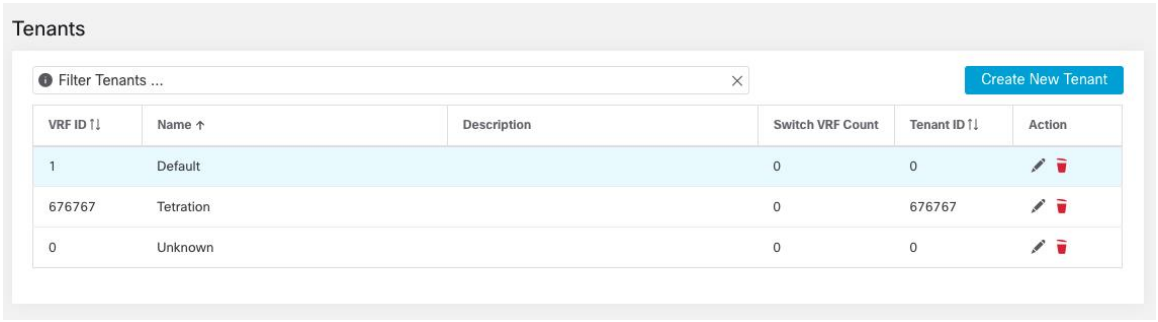
範囲とインベントリ（Scopes and Inventory）

テナント

サイト管理者および**カスタマーサポート**ユーザーは、左側にあるナビゲーションバーの**[プラットフォーム（Platform）]** > **[テナント（Tenants）]** メニューの下にある [テナント（Tenants）] ページにアクセスできます。このページには、現在構成されているすべてのテナントと VRF が表示されます。システムには、1つ以上のテナントとVRFが事前設定されています。テナントの追加、編集、削除が可能です。

（注） これらの値は、クラスタ出力の結果に影響します。システムへの影響を理解するために、これらの値を変更する前に Cisco TAC に相談することをお勧めします。

図 *28 :* テナント ページ



テナントの追加

始める前に

[サイト管理者（Site Admin）] または [カスタマーサポート（Customer Support）] ユーザーである必要があります。

ステップ 1 左側のナビゲーションバーで、**[プラットフォーム（Platform）]** > **[テナント（Tenants）]** をクリックします。

ステップ 2 [新しいテナントの作成（Create New Tenant）] をクリックします。

ステップ 3 以下のフィールドに適切な値を入力します。

フィールド	説明
Name	テナントの名前を入力します。
説明	（オプション）説明フィールドには、テナントに関する追加情報が含まれています。

フィールド	説明
スイッチ VRF	（オプション）この機能を構成して、複数のハードウェア（スイッチ）VRF を 1 つの Secure Workload ルート範囲/VRF にマッピングします。詳細については、以降に説明します。

ステップ 4 [作成（Create）] をクリックします。

テナントの編集

始める前に

サイト管理者または**カスタマーサポート**ユーザーである必要があります。

ステップ 1 左側のナビゲーションバーで、**[プラットフォーム（Platform）]** > **[テナント（Tenants）]** をクリックします。

ステップ 2 編集するテナントを見つけて、右側の列にある**鉛筆**アイコンをクリックします。

フィールド	説明
Name	テナントの名前を更新します。
説明	（オプション）テナントに関する追加情報が含まれている説明フィールドを更新します。
VRF ID	この特定のテナント/VRF の ID を表示します。
スイッチVRF（Switch VRFs）	（オプション）構成を更新して、複数のハードウェア（スイッチ）VRF を 1 つの Secure Workload ルート範囲/VRF にマッピングします。詳細については、以降に説明します。
変更ログ	変更ログアイコンをクリックすると、テナント/VRF のすべての変更ログを示す新しいページに移動します。

ステップ 3 **[更新（Update）]**をクリックします。

テナントへのスイッチ VRF の追加

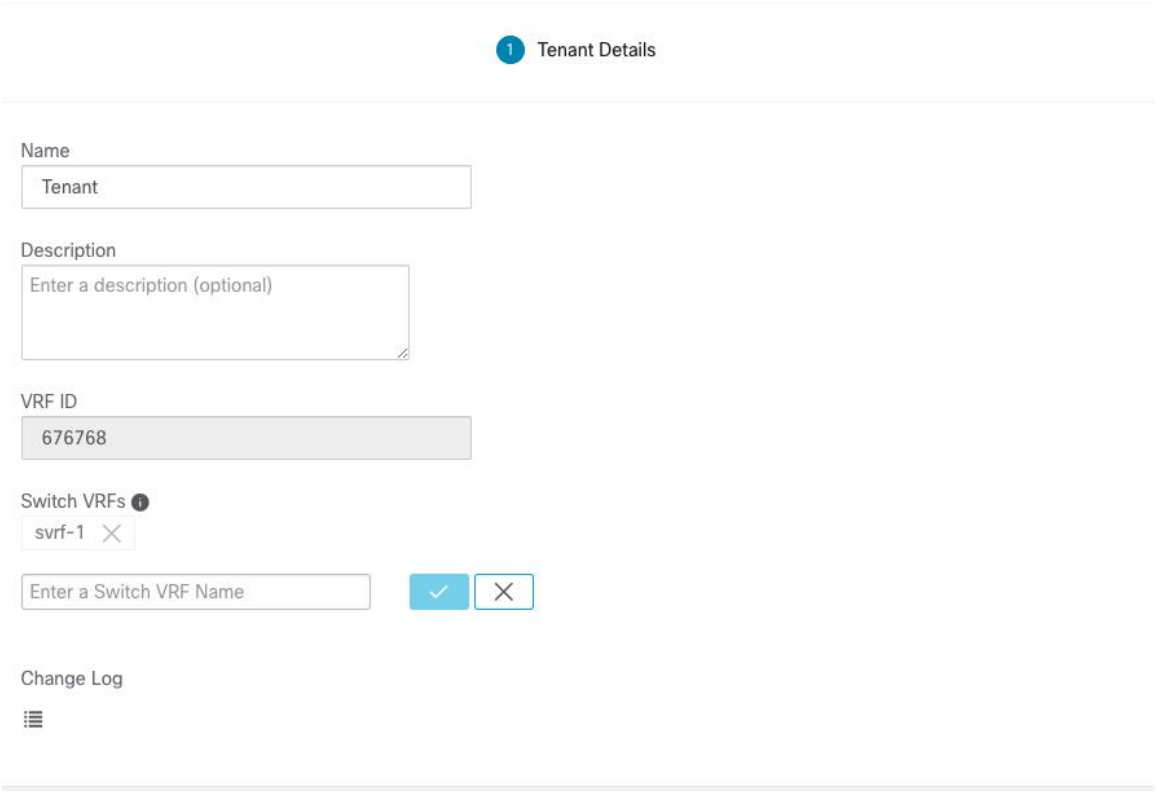
この機能を構成して、複数のハードウェア（スイッチ）VRF を 1 つの Secure Workload ルート範囲/VRF にマッピングします。Secure Workload の取り込みデータパス（コレクタ）は、ハードウェア VRF を 1 つの Secure Workload VRF にマッピングします。

警告 この機能は、マッピングされているすべてのハードウェア VRF に重複する IP がない場合に機能します。スイッチの VRF に重複する IP がある場合は、この機能を使用しないでください。

次に示すように、[テナントの追加/編集（Add/Edit Tenant）] モーダルで スイッチ VRF 名を入力し、**チェックマーク**アイコンをクリックすると、スイッチ VRF を VRF に追加できます。

ステップ 1 スイッチの VRF 名を入力し、以下に示すチェック ボタンをクリックします。

図 *29 : VRF* へのスイッチ *VRF* の追加

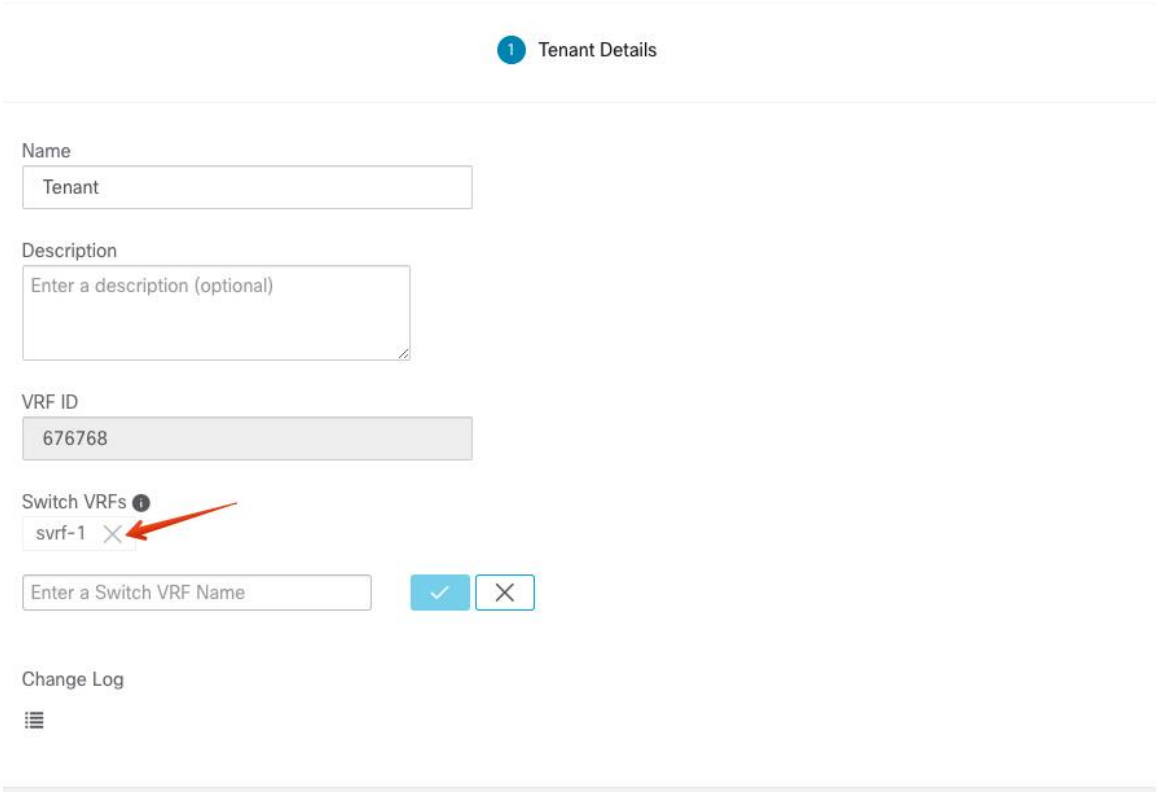


ステップ 2 [作成/更新（Create/Update）] ボタンをクリックして、スイッチ VRF を保存します。

スイッチ VRF の削除

[VRFの追加/編集（Add/Edit VRF）] ダイアログで、スイッチ VRF ラベルの横にある [x] ボタンをクリックすると、スイッチ VRF を VRF から削除できます。

図 *30* : スイッチ *VRF* の削除



[作成/更新（Create/Update）] ボタンをクリックして、変更内容を保存します。

ユーザ（Users）

サイト管理者とルート範囲の所有者は、ウィンドウの左側にあるナビゲーションバーの [管理（Manage）] メニューから [ユーザー（Users）] ページにアクセスできます。

このページには、すべてのサービス プロバイダー ユーザーと、ページヘッダーで選択した範囲に関連付けられているユーザーが表示されます。

マルチテナント機能

マルチテナント機能をサポートするために、ユーザーをルート範囲に割り当てることができます。これらのユーザーは、ルート範囲で「所有者」権限を持つユーザーによって管理され、同じ範囲に関連付けられたロールのみを割り当てることができます。

範囲のないユーザーは「サービスプロバイダー」と呼ばれ、これらのユーザーにはルート範囲全体でアクションを実行できる任意のロールを割り当てることができます。

新しいユーザーアカウントの追加

このセクションでは、**サイト管理者**およびルート範囲で**SCOPE_OWNER**機能を持つユーザーが新しいユーザーアカウントを追加する方法について説明します。

マルチテナント機能のためにユーザーにある範囲が割り当てられている場合、同じ範囲に割り当てられたロールのみを選択できます。

（注） このページは、ページヘッダーで選択された範囲設定によってフィルタリングされます。

始める前に

1. 左側のナビゲーションバーで、**[管理（Manage）]** > **[ユーザー（Users）]** をクリックします。
2. 該当する場合は、ページの右上から適切なルート範囲を選択します。
3. [新しいユーザーの追加（Add New User）] ボタンをクリックします。[ユーザー（Users）] ウィザードが表示されます。

ユーザーの作成は 3 段階のプロセスです。

ステップ 1 1. 以下のフィールドに適切な値を入力します。

フィールド	説明
E メール（Email）	新しいユーザーの電子メールアドレスを入力します。大文字と小文字は区別されません。メールに文字が含まれている場合は、小文字のバージョンを使用します。
[名（First Name）]	新しいユーザーの名を入力します。
[姓（Last Name）]	新しいユーザーの姓を入力します。
スコープ	マルチテナント機能のためにユーザーに割り当てられたルート範囲。

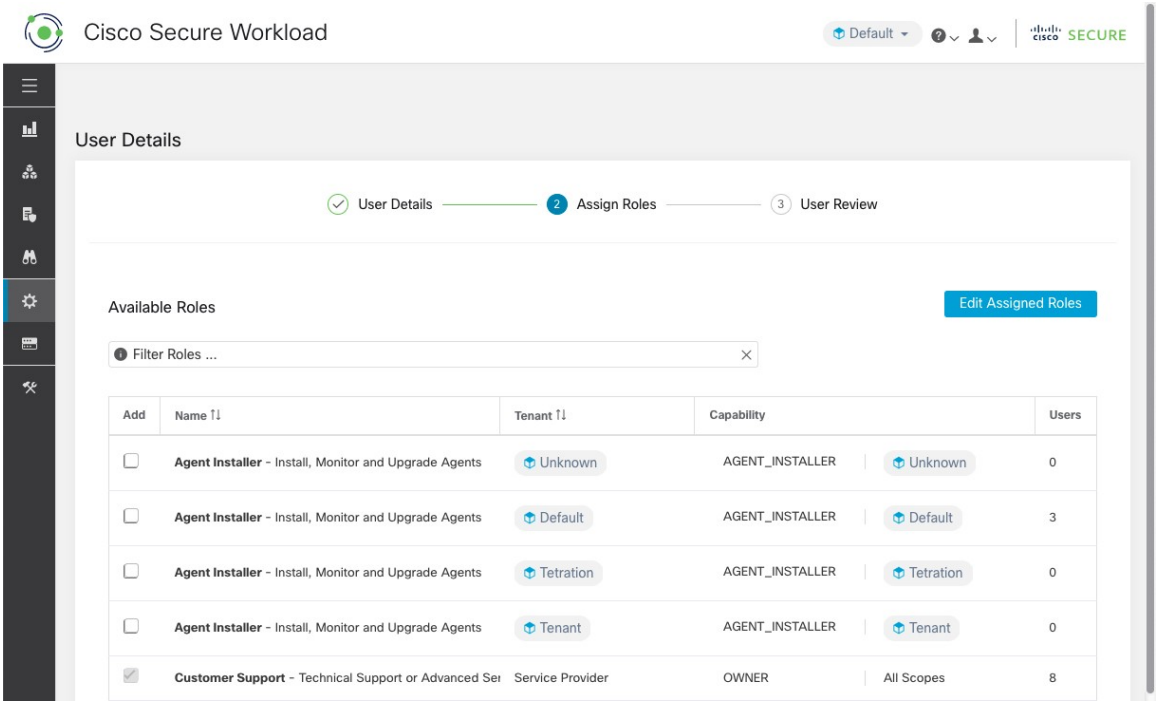
必要に応じて、SSH 公開キーを今すぐインポートすることも、後でインポートすることもできます。

2. [次へ（Next）] ボタンをクリックして次のステップに移動するか、[ユーザーリストに戻る（Back to Users List）] をクリックして [ユーザー（Users）] ページに戻ります。

ステップ 2 このビューでは、[ロールの追加（Add Roles）]、[ロールの削除（Delete Roles）]、または [ロールの選択（Select Roles）] を実行できます。

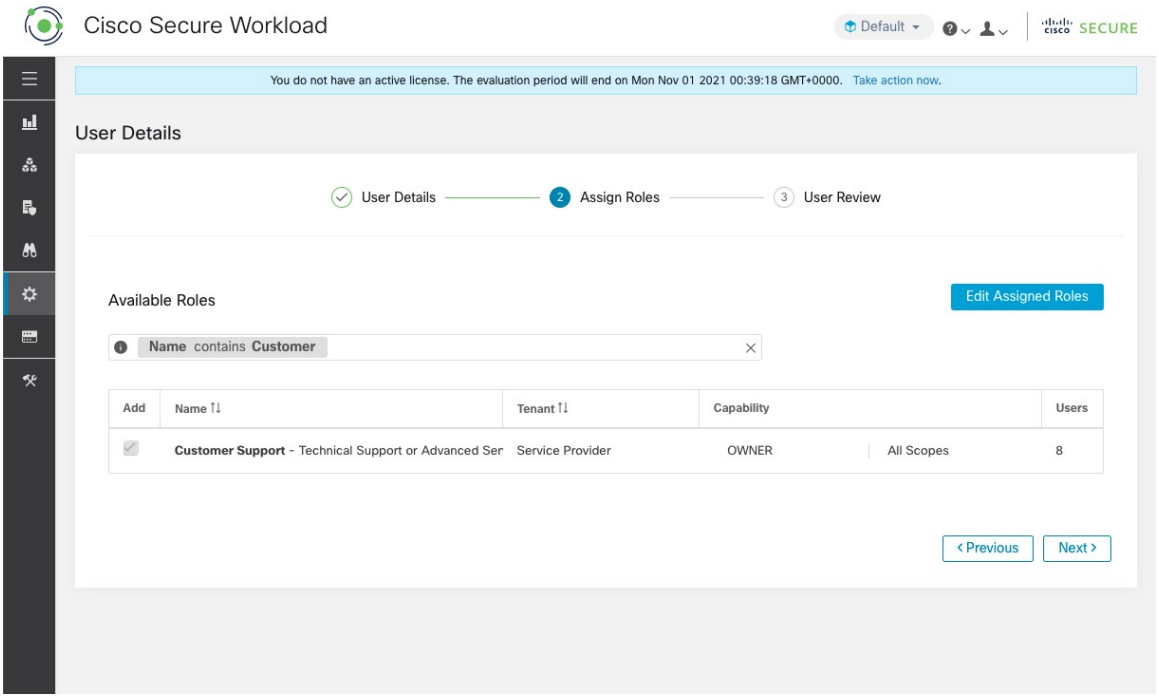
1. [ロールの追加（Add Roles）] をクリックして、ロールを割り当てます。

図 *31* : 使用可能な役割（***Available Roles***）



2. [割り当てられたロールの編集（Edit Assigned Roles）] をクリックしてロールを削除します。
3. [名前（Name）] と [テナント（Tenant）] でロールをフィルタ処理します。

図 *32* : ロールをフィルタ処理



4. [次へ（Next）] ボタンをクリックしてユーザーの詳細とロールの割り当てを確認するか、[前へ（Previous）] ボタンをクリックして戻って詳細を編集します。

ステップ 3 設定内容を確認して [作成（Create）] をクリックします。

外部認証が有効になっている場合、認証の詳細が表示されます。

（注） ユーザーを作成すると、そのユーザーはパスワードを設定するための電子メールを受け取ります。

ユーザー アカウントの編集

始める前に

ユーザーは、**サイト管理者**または**ルート範囲所有者**ユーザーである必要があります。

（注） このページは、ページヘッダーで選択された範囲設定によってフィルタリングされます。

1. 左側のナビゲーションバーで、**[管理（Manage）]** > **[ユーザー（Users）]** をクリックします。

2. 該当する場合は、ページの右上から適切なルート範囲を選択します。
3. 編集するアカウントの行で、右側の列にある [編集（Edit）] ボタンをクリックします。[ユーザー（Users）] ウィザードが表示されます。

ウィザードを使用したユーザーの編集は、3 つのステップから成るプロセスです。

ステップ 1 1. 必要に応じて、次のフィールドを更新します。

フィールド	説明
E メール（Email）	新規ユーザーの電子メールアドレスを更新します。
[名（First Name）]	新規ユーザーの名を更新します。
[姓（Last Name）]	新規ユーザーの姓を更新します。
スコープ	マルチテナンシーのためにユーザーに割り当てられたルート範囲。（サイト管理者が利用可能）

2. [次へ（Next）] ボタンをクリックして、[ロールの割り当て（Role Assignment）] に進みます。

ステップ 2 1. このビューでは、割り当てられたロールを削除できます。
2. [ロールの追加（Add Roles）] をクリックして、新しいロールを割り当てます。
3. [次へ（Next）] ボタンをクリックしてユーザーの詳細とロールの割り当てを確認するか、[前へ（Previous）] ボタンをクリックして戻って詳細を編集します。

ステップ 3 1. ユーザーの詳細とロールの割り当てを確認します。
2. [更新（Update）] をクリックしてユーザーを更新するか、[前へ（Previous）] をクリックして戻ってロールを編集します。ユーザーの詳細とロールの割り当てへの変更が保存されます。

外部認証が有効になっている場合、認証の詳細が表示されます。

ユーザーアカウントの非アクティブ化

（注） 変更ログ監査の一貫性を維持するために、ユーザーは非アクティブ化できますが、データベースからは削除されません。

始める前に

サイト管理者または**ルート範囲所有者**ユーザーの権限が必要です。

（注） このページは、ページヘッダーで選択された範囲設定に従ってフィルタリングされます。

ステップ 1 左側のナビゲーションバーで、**[管理（Manage）]** > **[ユーザー（Users）]** をクリックします。

ステップ 2 該当する場合は、ページの右上から適切なルート範囲を選択します。

ステップ 3 非アクティブ化するアカウントの行で、右側の列にある [非アクティブ化（Deactivate）] ボタンをクリックします。

非アクティブ化されたユーザーを表示するには、[削除されたユーザーを非表示（Hide Deleted Users）] ボタンを切り替えます。

ユーザーアカウントの再アクティブ化

ユーザーが非アクティブ化されている場合は、そのユーザーを再アクティブ化できます。

始める前に

サイト管理者または**ルート範囲所有者**ユーザーの権限が必要です。

（注） このページは、ページヘッダーで選択した範囲設定によってフィルタリングされます。

ステップ 1 左側のナビゲーションバーで、**[管理（Manage）]** > **[ユーザー（Users）]** をクリックします。

ステップ 2 該当する場合は、ページの右上から適切なルート範囲を選択します。

ステップ 3 [削除されたユーザーを非表示（Hide Deleted Users）] ボタンを切り替えると、非アクティブ化されたユーザーを含むすべてのユーザーが表示されます。

ステップ 4 再アクティブ化する非アクティブ化されたアカウントの行で、右側の列にある [復元（Restore）] ボタンをクリックします。

SSH 公開キーのインポート

コレクタ IP アドレスの 1 つを介した **ta_guest** ユーザーとしての SSH アクセスを有効にするために、SSH 公開キーをユーザーごとにインポートできます。このメニューは、**サイト管理者**およびルート範囲で SCOPE_OWNER 機能を持つユーザーのみが使用できます。SSH 公開キーは、7 日後に自動的に期限切れになります。

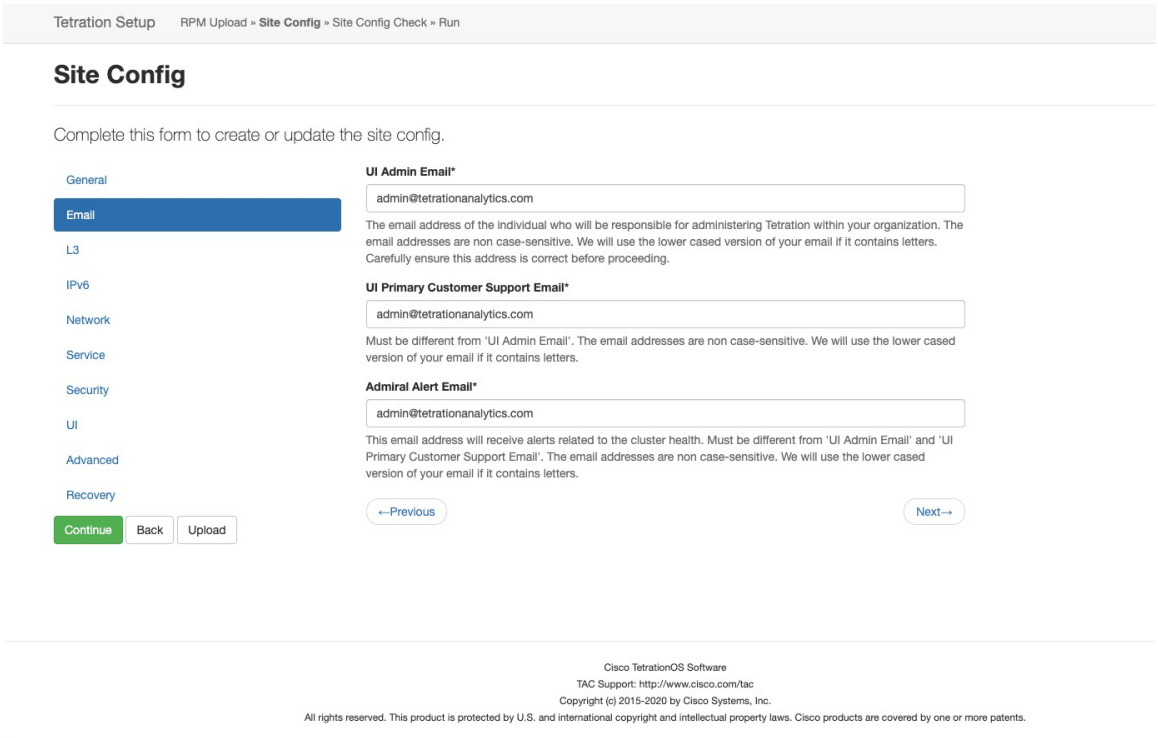
Secure Workload セットアップでのサイト設定

このセクションでは、[サイト管理者（Site Admins）] が Secure Workload のセットアッププロセス中にサイトをセットアップする方法について説明します。

フィールド	説明
[UI管理者の電子メール（UI Admin Email）]	組織内で Secure Workload の管理を担当する個人の電子メールアドレス。
[UIプライマリカスタマーサポートの電子メール（UI Primary Customer Support Email）]	プライマリサポートの電子メールアドレス。UI 管理者の電子メールとは別にする必要があります。
[アドミラルアラート電子メール（Admiral Alert Email）]	この電子メールアドレスは、クラスタ正常性に関連するアラートを受信します。UI管理者の電子メールおよびUIプライマリカスタマサポートの電子メールとは別にする必要があります。

電子メールアドレスでは大文字と小文字が区別されません。電子メールに文字が含まれている場合は、小文字のバージョンを使用します。

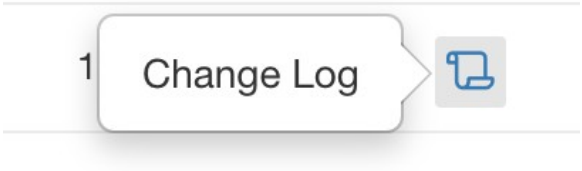
図 *33 : UI* 管理者、プライマリ カスタマー サポート、アドミラル管理者アラート メールの構成



ログの変更：ユーザー

ルート範囲で SCOPE_OWNER 機能を持つ [サイト管理者（Site Admins）] およびユーザーは、以下に示す [アクション（Actions）] アイコンをクリックして、各ユーザーのログの変更を表示できます。

図 *34* : ログの変更



ログの変更の詳細については、「ログの変更」を参照してください。ルート範囲の所有者は、その範囲に属するエンティティにおけるログの変更エントリの表示に制限されます。

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。