

Tutorial: Azure Active Directory Integration with Qualys Cloud Platform using SAML SSO

このチュートリアルでは、SAML 2.0 SP によって開始された SSO を使用して、Microsoft Azure Active Directory (Azure AD) と Qualys Cloud Platform を統合する方法について説明します。

Qualys Cloud Platform を Azure AD と統合すると、次のようなメリットがあります。

1. Azure AD から Qualys Cloud Platform にアクセスできるユーザーを制限することができる。
2. ユーザーが自分の Azure AD 資格情報を使用して Qualys に自動的にログインできる。
3. Azure ポータルからアカウントを管理できる。

前提条件

- Qualys クラウド プラットフォームのサブスクリプションが必要です。
- サブスクリプションに対して SAML SSO を有効にする必要があります。この機能を利用するには、以下の手順に従ってください。
- サブスクリプションに対して新しいデータセキュリティモデルを受け入れる必要があります。マネージャは、Qualys UI の Users > Setup > Security に移動してオプトインできます。

SAML SSO をリクエストする方法

SAML オンボーディングを開始するには、次の手順を実行します。

- 1) [SAML 2.0 Integration Request Form](#) のセクション 1 と 2 をダウンロードして完了します。 次の詳細を指定します。
 - IdP (SAML ID Provider) からの Entity ID 文字列
 - IdP の公開鍵証明書 (.txt 形式の組織の IdP base64 証明書)
 - 組織の SAML IdP SSO URL (SP が処理した認証要求)
 - Qualys サブスクリプション ログイン(マネージャ POC 用)
 - サブスクリプションのカスタム exit URL (オプション)

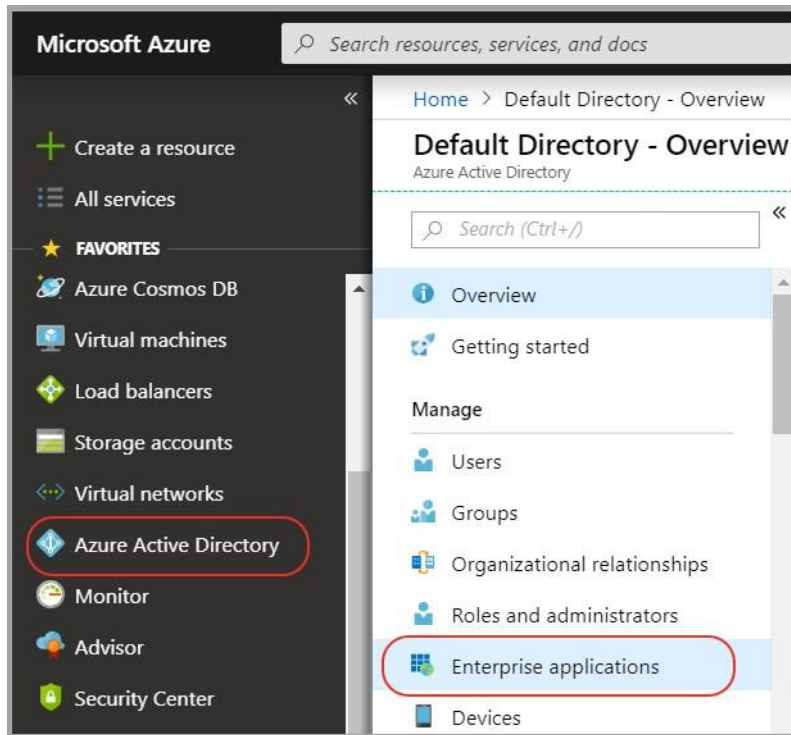
- 2) [Qualys Support](#) へフォームを送信します。
- 3) Qualys サポートは、お客様と協力して、お客様の ID プロバイダ (IdP) と Qualys SAML 2.0 サービス プロバイダ (SP) の間の信頼関係を設定します。Qualys は、識別子と応答 URL の 2 つの URL を提供します。これらの URL は、Azure ポータルで Azure AD を構成するために必要になります。

Azure Active Directory の構成

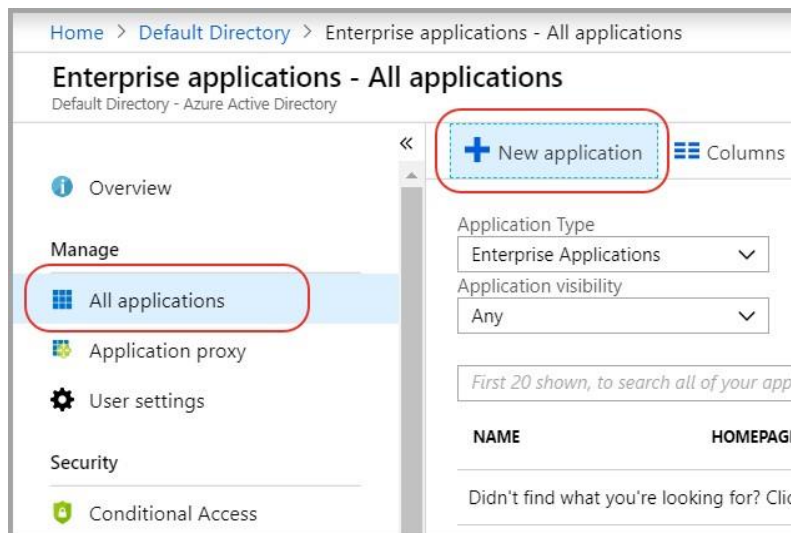
Azure portal で次の手順を実行します。

新しいアプリケーションを追加する (ギャラリー以外のアプリケーション)

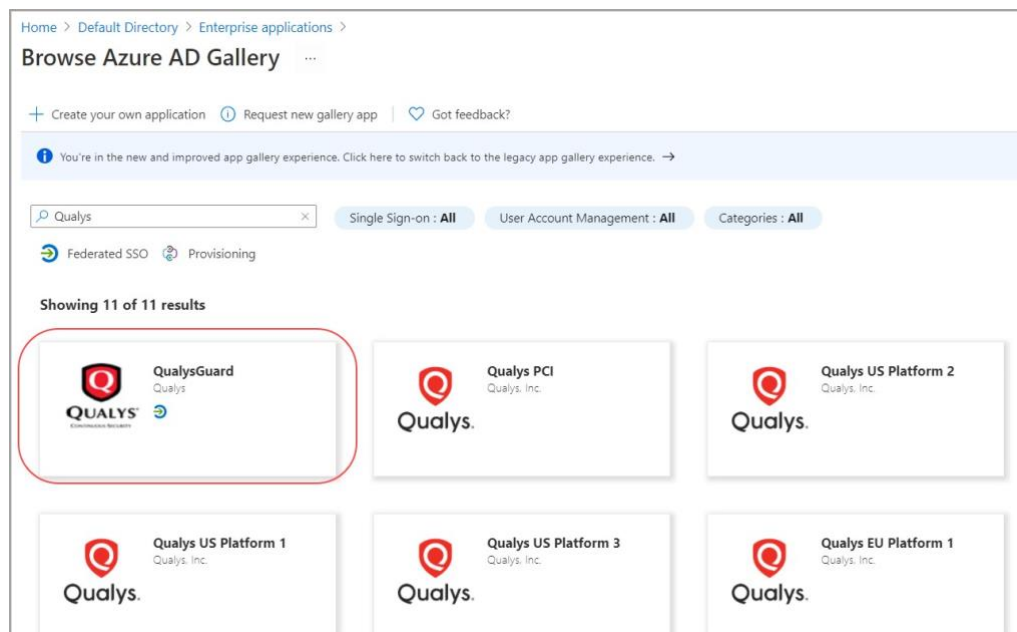
左側のナビゲーション ウィンドウで [Azure Active Directory] を選択します。次に、[Enterprise applications] を選択します。



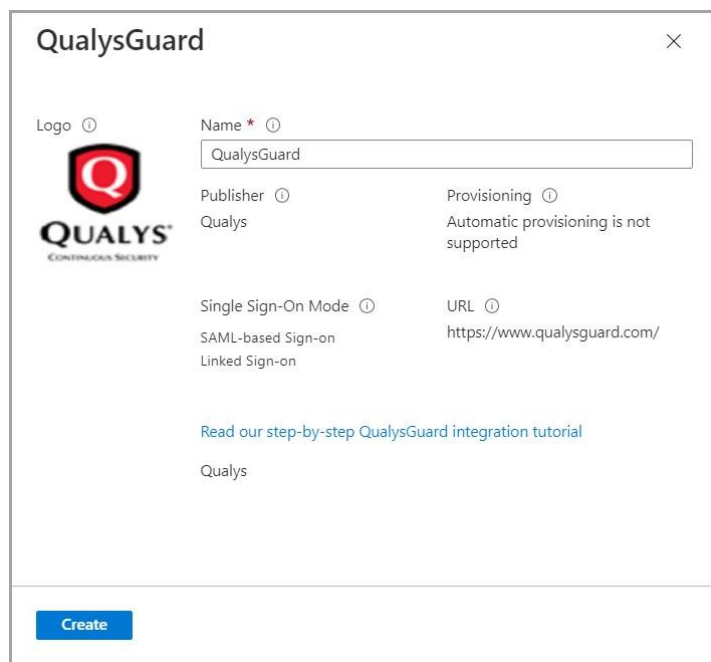
「All applications」を選択し、「New application」をクリックします。



「Qualys」で検索を実行します。さまざまな Qualys アプリケーションが利用可能です。🔗 Federated SSO タグを持つ最初のアプリケーションを選択します。



Federated SSO タグが付いたアプリケーションをクリックすると、右側のペインにアプリケーションが表示されます。「Create」をクリックします。



新しいアプリケーションが追加され、SAML シングルサインオンを使用するように構成できるようになります。

SAML シングル サインオンを使用するようにアプリケーションを構成する

Qualys アプリケーション ページで [シングル サインオン] を選択し、サインオン方法として [SAML] を選択します。

以下のセクションで SAML 構成の詳細を指定します。

- 1) 基本的な SAML 設定。 [編集(Edit)] アイコンをクリックして、必要な SAML 設定を指定します。

Field	Requirement
Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Required
Relay State	Optional
Logout Url	Optional

Qualys から提供された [Identifier(Entity ID)], [Reply URL]、および [Sign On URL] を入力します。他の値は必要ありません。各フィールドの画面に表示されるパターンに従います。

Identifier (Entity ID) * ⓘ
The default identifier will be the audience of the SAML response for IDP-initiated SSO

https://QualysGuard_SharedPlatform-SAML20-SP

Patterns: QualysGuard_SharedPlatform-SAML20-SP

Reply URL (Assertion Consumer Service URL) * ⓘ
The default reply URL will be the destination in the SAML response for IDP-initiated SSO

https://qualysguard.qg3.apps.qualys.com/IdM/saml2/

Patterns: https://qualysguard.qg1.apps.qualys.in/IdM/saml2/

Sign on URL * ⓘ

https://qualysguard.qg3.apps.qualys.com/

Patterns: https://qualysguard.qg1.apps.qualys.in/

入力サンプル :

Identifier: https://QualysGuard_SharedPlatform-SAML20-SP

Reply URL (based on the Qualys Cloud Platform for your subscription):

https://qualysguard.qualys.com/IdM/saml2/

https://qualysguard.qg2.apps.qualys.com/IdM/saml2/

https://qualysguard.qg3.apps.qualys.com/IdM/saml2/

https://qualysguard.qualys.eu/IdM/saml2/

https://qualysguard.qg2.apps.qualys.eu/IdM/saml2/

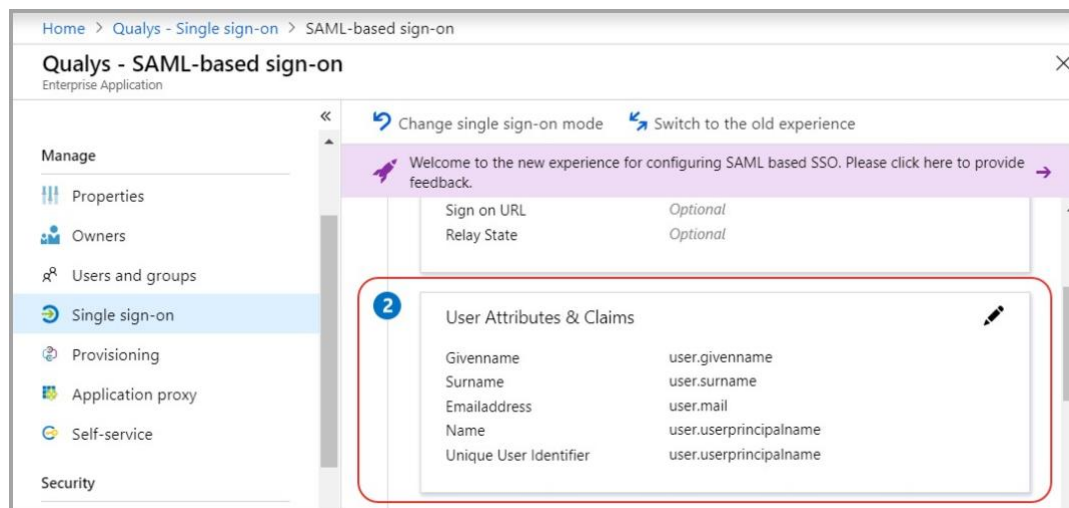
https://qualysguard.qg1.apps.qualys.in/IdM/saml2/

https://qualysguard.BASE_URL/IdM/saml2/ (for Private Cloud Platform)

2) User Attributes & Claims. ユーザーが SAML 2.0 プロトコルを使用して Azure AD を介してアプリケーションに対して認証を行うと、Azure AD は SAML 認証応答の一部として (HTTP POST を介して) トークンをアプリケーションに送信します。

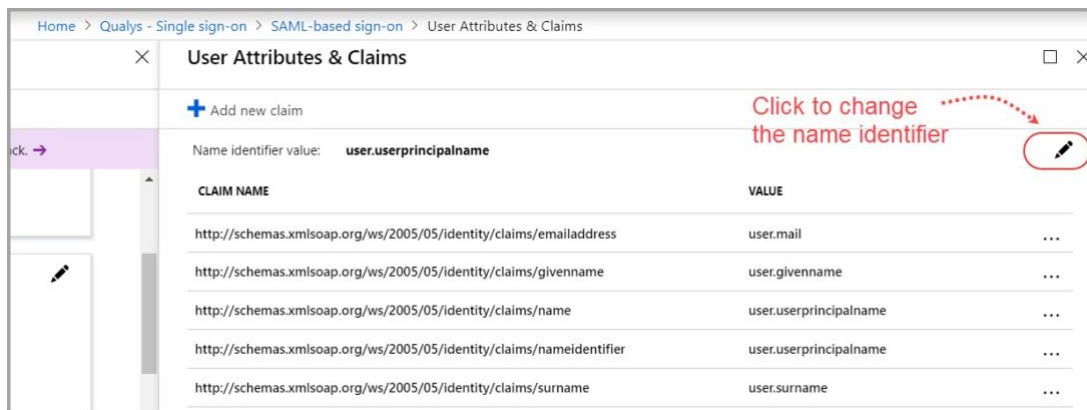
次に、アプリケーションは、ユーザー名とパスワードの入力を求める代わりに、トークンを検証して使用してユーザーをログインさせます。これらの SAML トークンには、"クレーム" と呼ばれるユーザーに

関する情報が含まれています。



name identifier の変更(optional)

一意のユーザー識別子が Azure ユーザーのユーザー名 (user.userprincipalname) の値にマップされていることがわかります。「編集」アイコンをクリックして、名前識別子を user.employeeid などの別のソース属性に変更します。



Qualys external ID の要求の追加 (必須)

既定では、Qualys クラウド プラットフォームは、SAML トークンで発行された `qualysguard_external_id` の値を解析するように構成されています。この要求をリストに追加する必要があります。

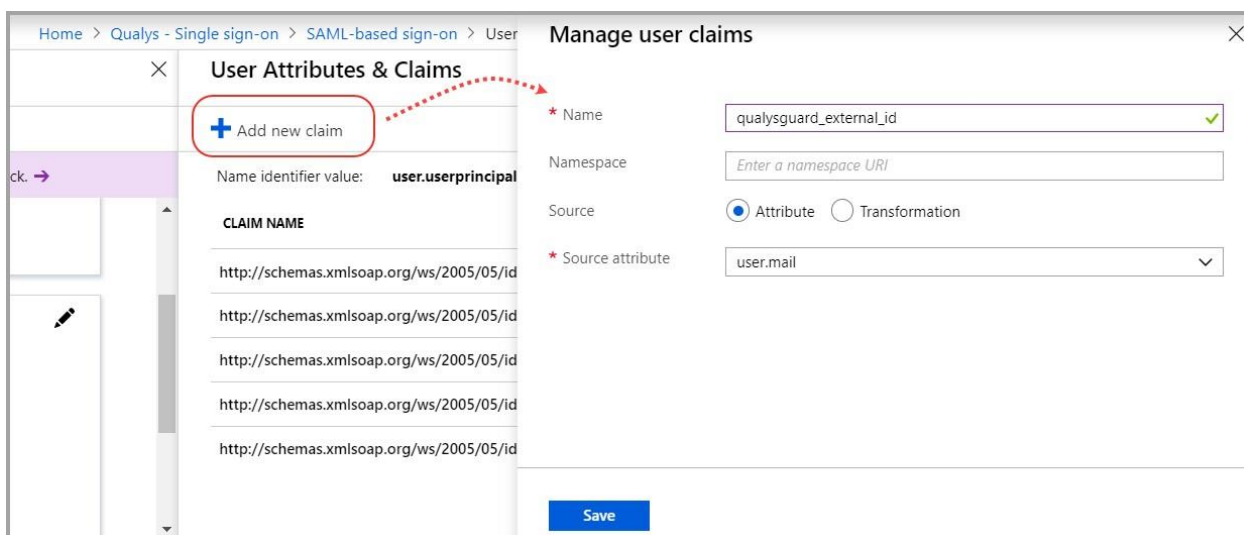
[Add new claim] をクリックし、次の設定を指定します。

Name: `qualysguard_external_id`

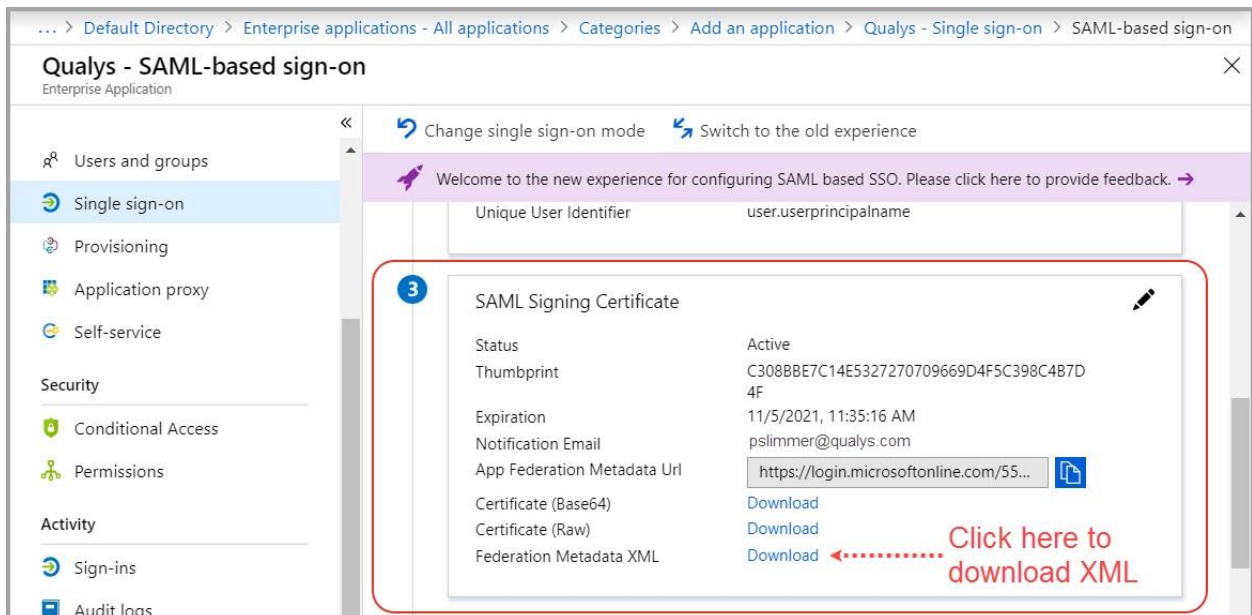
Namespace: leave blank

Source attribute: `user.mail` (recommended)

source 属性が `user.mail` に設定されている場合は、ユーザーの Qualys アカウントの [外部 ID] フィールドにユーザーのメール アドレスを入力して、要求を検証します。ソース属性を別の値に設定することもできます。その場合は、必ず [外部 ID] の値を一致するように設定してください。



3) SAML 署名証明書。[Federation Metadata XML] の横にある [Download] をクリックして、メタデータ ファイルをコンピューターに保存します。このファイルを Qualys に送信します。

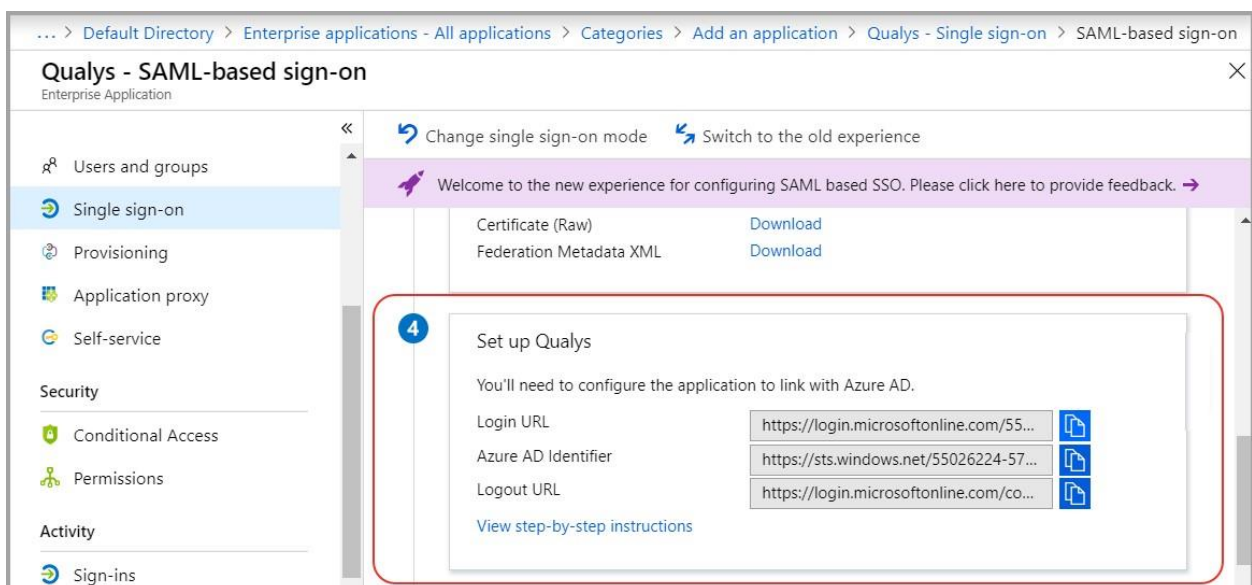


フェデレーション メタデータ XML ファイルは、サブスクリプションの IDP および IDM プロファイルを作成するために Qualys によって使用されます。

これには、IDP エンティティ ID、SSO リダイレクト URL、Base64 でエンコードされたトークン署名証明書などの有用な情報が含まれています。

4) Qualys の設定をします。前の手順でダウンロードしたフェデレーション メタデータ XML ファイルには、Qualys が必要とする情報が含まれています。ログアウト URL をカスタマイズする場合を除き、この手順はスキップできます。

デフォルトでは、ログアウト URL は <https://www.qualys.com> に設定されています。カスタムログアウト URL を [SAML 2.0 Integration Request Form](#) のセクション 2 にて追加できます。

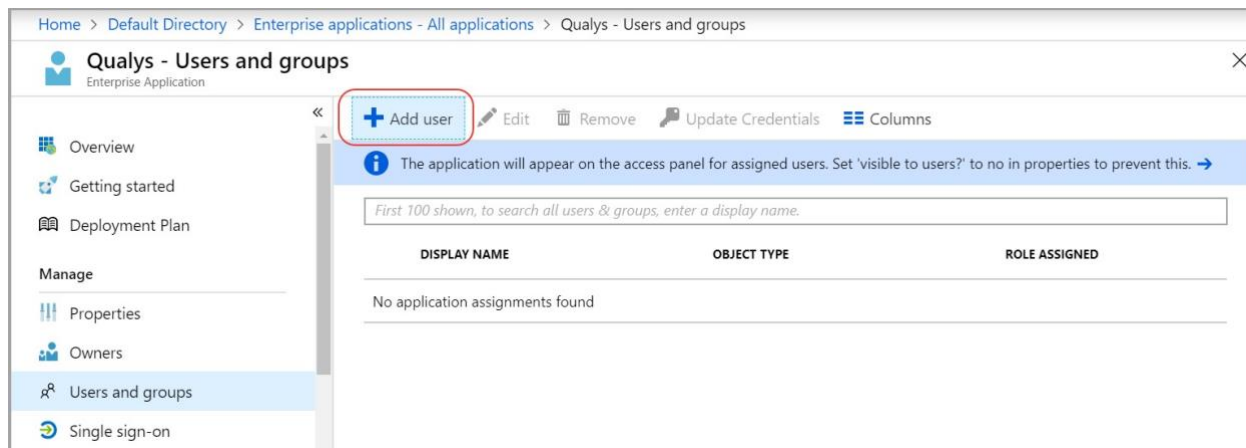


Azure AD ユーザーを Qualys アプリケーションに割り当てる

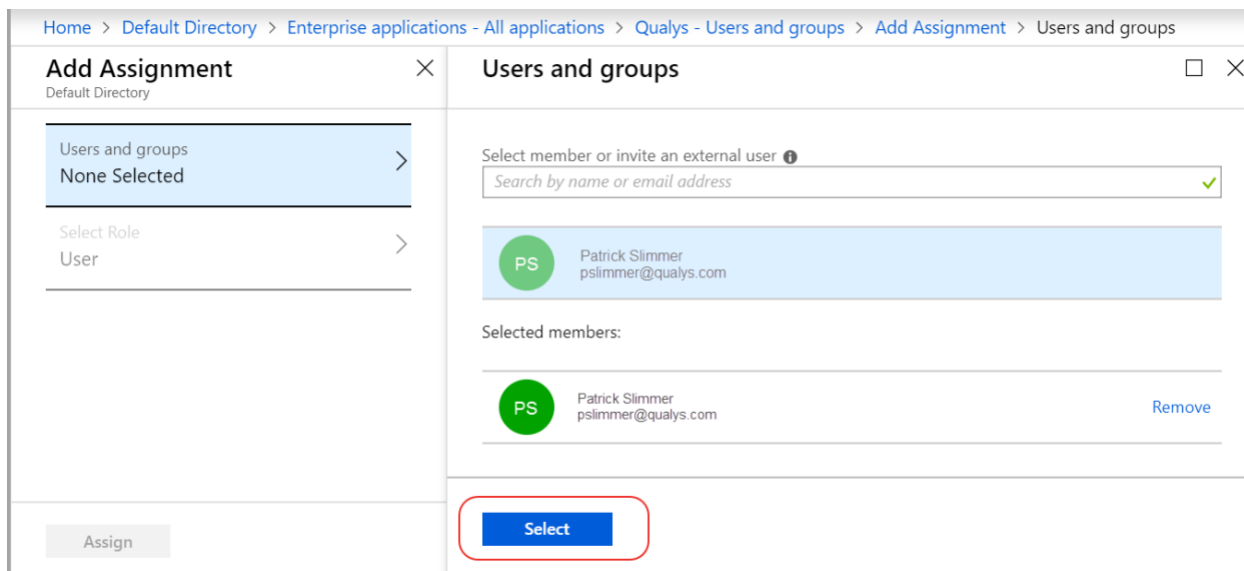
アプリケーションにユーザーまたはグループを割り当てる必要があります。Azure AD では、Azure AD がユーザーにアクセスを許可していない限り、ユーザーは Qualys アプリケーションにサインインできません。

アプリケーションの一覧から Qualys アプリケーションを選択します。次に、[Users and groups] を選択します。

[Add user] ボタンをクリックします。



[Add Assignment] で [Users and groups] を選択します。リスト内の 1 人以上のユーザーをクリックして選択し、[Select] ボタンをクリックします。



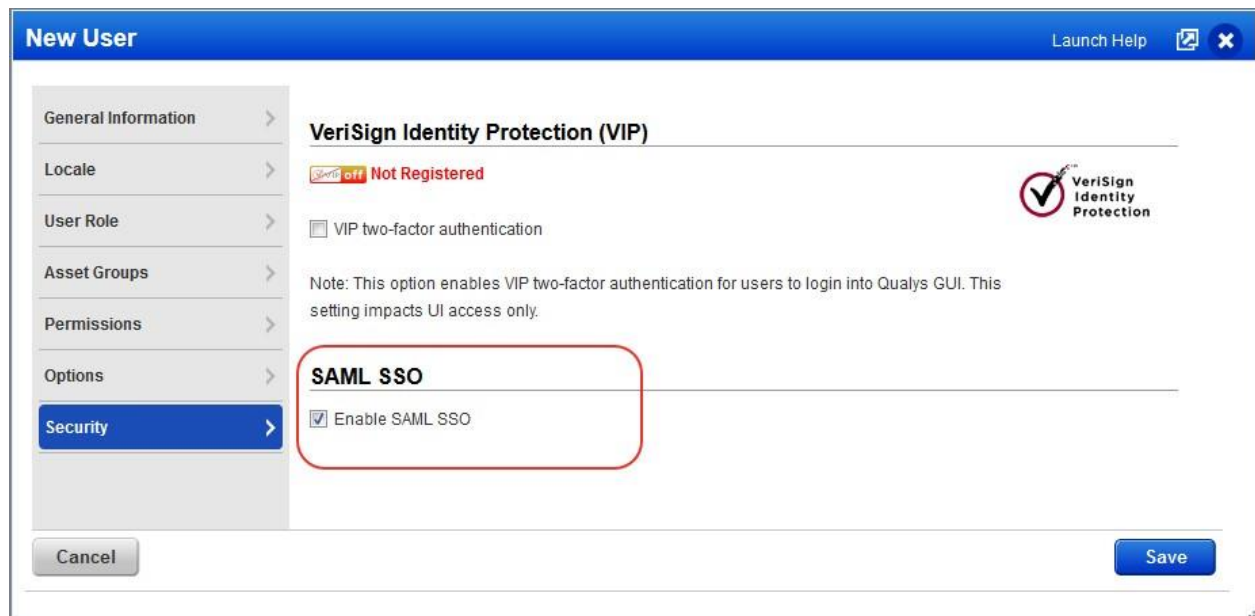
最後に、[Assign] ボタンをクリックします。これで、選択したユーザーに Qualys アプリケーションが割り当てられます。

Qualys ユーザの SAML SSO の有効化

Qualys Cloud Platform を使用して次の手順を実行します。

ユーザーアカウントで SAML SSO を有効にする

Qualys UI の [Users]セクションに移動します。新しいユーザーを作成するか、既存のユーザーを編集します。ユーザー アカウント設定の [Security] セクションで、[Enable SAML SSO] を選択します。



The screenshot shows the 'New User' dialog box with the 'Security' section selected. The 'SAML SSO' section is highlighted with a red box, and the 'Enable SAML SSO' checkbox is checked. Other sections include 'VeriSign Identity Protection (VIP)' with a 'Not Registered' status and a 'VIP two-factor authentication' checkbox.

external ID を設定する

ユーザーの外部 ID を設定する必要があります。外部 ID の値は、Azure SAML 構成で定義した `qualysguard_external_id` 要求に対応します。外部 ID はユーザーのメール アドレスに設定することをお勧めします。これを SAML 認証応答に存在する別の属性に変更した可能性があります。

外部 ID は、UI (以下を参照) または ユーザーの追加/編集 API (`/msp/user.php`) を使用して設定できます。詳細については、『[Qualys API\(VM,PC\)ユーザガイド](#)』を参照してください。

知っておくと良いこと

- 外部 ID は任意の文字列に設定できますが、文字列はサブスクリプション内の ユーザーごとに 一意である必要があり、同じ値を要求で渡す必要があります。
- 既定では、外部 ID の検証では大文字と小文字が区別されます。大文字と小文字を区別しないように 必要がある場合は、そのように構成できます。Qualys サポートに連絡して、IDM 設定をカスタマイズしてください。

- 初期状態では、マネージャの主取引先責任者のみがユーザの外部 ID を編集する権限を持っています。
- 他のマネージャには、この権限が付与されている場合があります。詳細については、[ここをクリックしてください](#)。

SAML SSO を使用した Qualys ログインのテスト

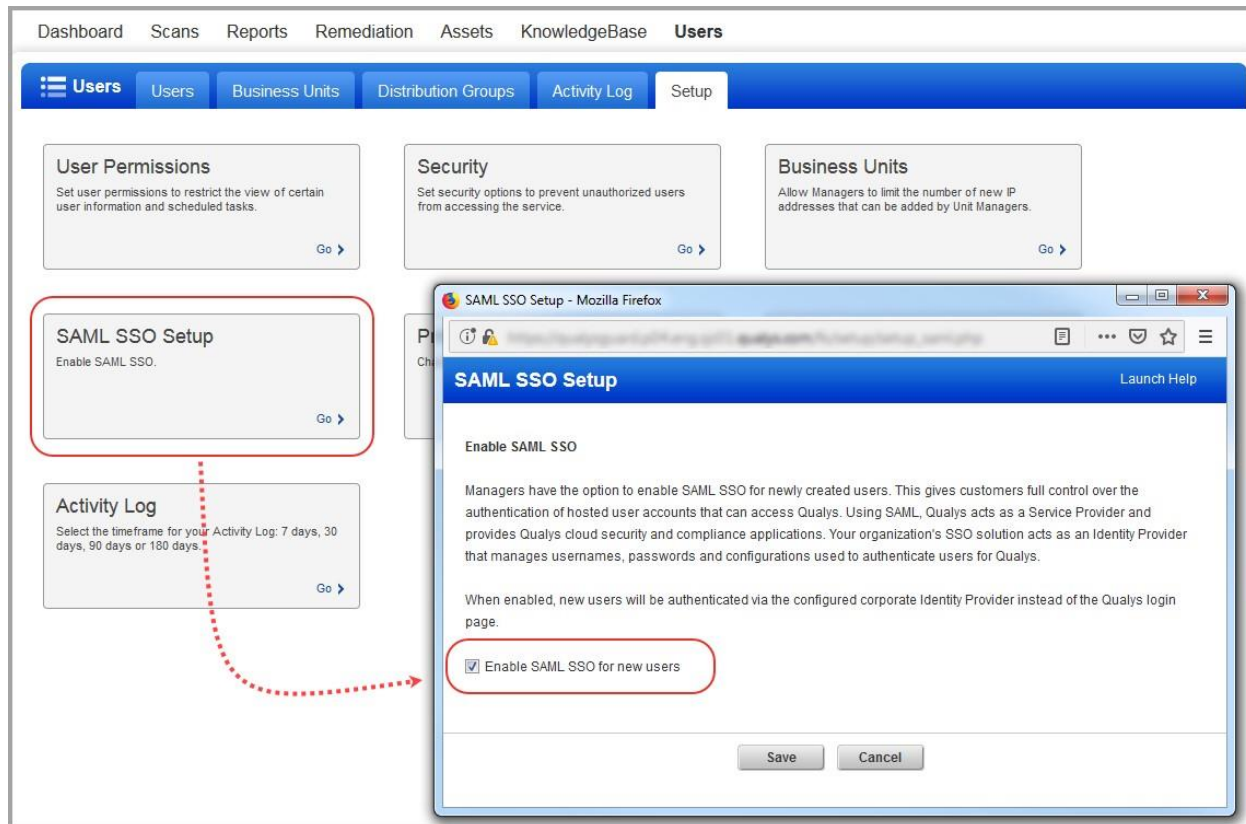
- 1) Web ブラウザを使用して、一意のログイン URL を開きます
- 2) Web ブラウザによって SAML SSO ページにリダイレクトされ、そこで Azure Active Directory のログインとパスワードを入力します。
- 3) 認証が成功すると、Web ブラウザが Qualys にリダイレクトされ、予期されるユーザ ID で有効なセッションが開かれます。
- 4) Qualys からログアウトする場合、Web ブラウザは、顧客から提供された <https://www.qualys.com> またはカスタム ログアウト URL にリダイレクトする必要があります。

より多くの Qualys ユーザーへの SAML SSO のロールアウト

すべての新規ユーザーまたは一部のユーザーに対して SAML SSO を有効にすることができます。

すべての新規ユーザーに対して SAML SSO を有効にする

[Users > Setup] > [SAML SSO Setup] に移動します。「Enable SAML SSO for new users」オプションを選択します。



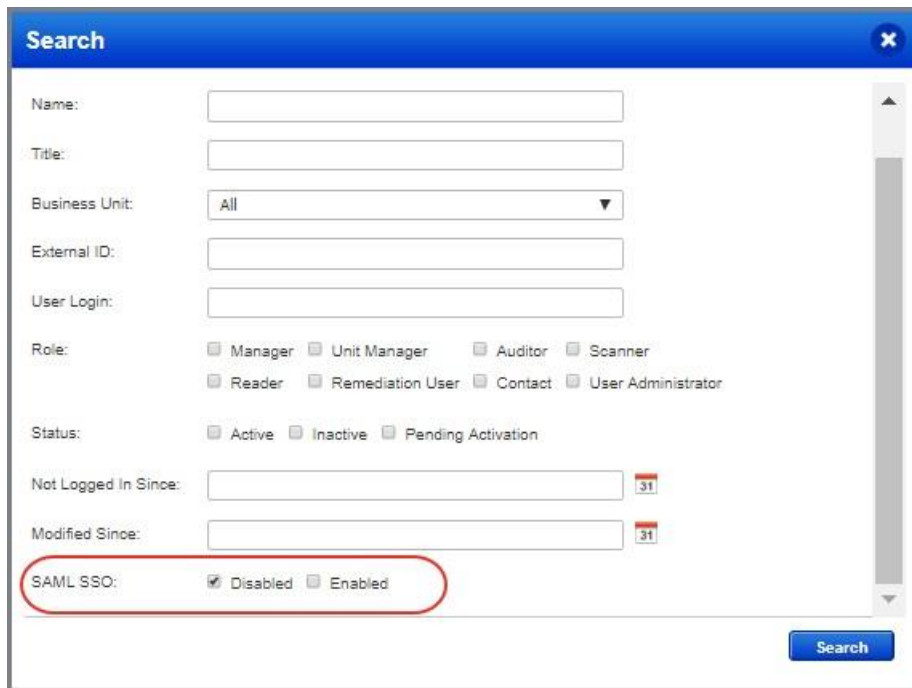
複数のユーザーに対して SAML SSO を一括有効化する

[ユーザー] リストには、ユーザーが SAML SSO を有効にしているかどうかが表示されます。

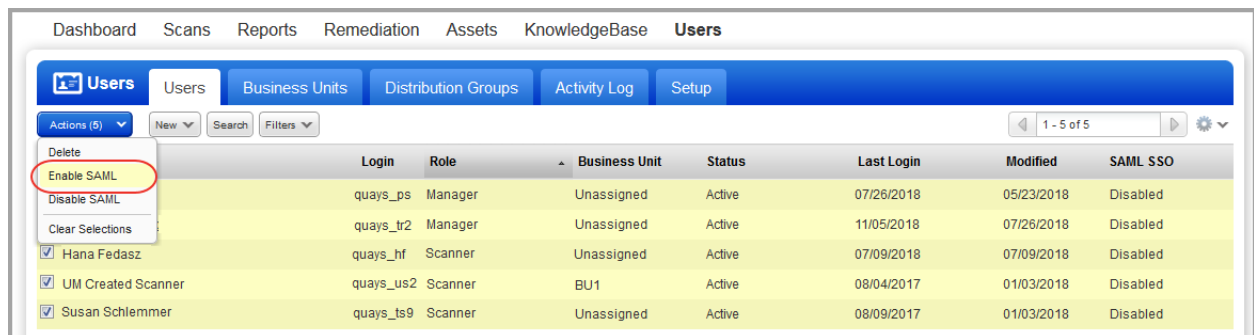
The screenshot shows the 'Users' list in the Qualys interface. The 'SAML SSO' column is highlighted with a red box, showing the status for each user.

Name	Login	Role	Business Unit	Status	Last Login	Modified	SAML SSO
Brendan Skulan	quays_bs1	Auditor	Unassigned	Active	08/04/2017	07/31/2018	Enabled
Jason Kim	quays_ak4	Manager	Unassigned	Active	05/01/2017	05/01/2017	Enabled
Patrick Slimmer *	quays_ps	Manager	Unassigned	Active	07/26/2018	05/23/2018	Disabled
Suzu Van Pelt	quays_sx22	Reader	Unassigned	Active	07/31/2018	06/11/2018	Enabled
Hana Fedasz	quays_hf	Scanner	Unassigned	Active	11/05/2018	07/26/2018	Disabled
Jake Anthony	quays_aa9	Scanner	Unassigned	Active	07/12/2018	07/12/2018	Enabled
Susan Schlemmer	quays_ts9	Scanner	Unassigned	Active	07/09/2018	07/09/2018	Disabled
UM Created Scanner	quays_us2	Scanner	BU1	Active	08/04/2017	01/03/2018	Disabled
James Adrian	quays_aa32	Unit Manager	BU1	Active	07/31/2018	07/31/2018	Enabled

リストの上にある「Search」ボタンをクリックすると、SAML SSO が無効になっているアカウントをすばやく見つけることができます。



検索結果のすべての行を選択し、「Actions」メニューから「Enable SAML」を選択します。[Disable SAML] を選択することで、これと同じ方法で SAML を無効にできます。



	Login	Role	Business Unit	Status	Last Login	Modified	SAML SSO
<input type="checkbox"/>	quays_ps	Manager	Unassigned	Active	07/26/2018	05/23/2018	Disabled
<input type="checkbox"/>	quays_tr2	Manager	Unassigned	Active	11/05/2018	07/26/2018	Disabled
<input checked="" type="checkbox"/>	Hana Fedasz	Scanner	Unassigned	Active	07/09/2018	07/09/2018	Disabled
<input checked="" type="checkbox"/>	UM Created Scanner	Scanner	BU1	Active	08/04/2017	01/03/2018	Disabled
<input checked="" type="checkbox"/>	Susan Schlemmer	Scanner	Unassigned	Active	08/09/2017	01/03/2018	Disabled

External ID を追加する権限をマネージャーに付与する

External ID は、マネージャーのプライマリ連絡先 (サブスクリプション用) によって追加できます。

マネージャの主連絡先には、次の手順に従って、他のマネージャ、ユニットマネージャ、およびユーザ管理者がユーザの外部 ID を編集できるようにするオプションがあります。

1) Users > Settings > Permissions に移動し、「Manage external IDs for users」を選択します。

External IDs

As the Manager Primary Contact you can assign/edit the external ID for users. Select this option if you want to grant this permission to other Managers, Unit Managers and User Administrator. You do this by editing their account settings.

Allow other users to manage external IDs

マネージャのアカウントを編集して、この拡張アクセス権を付与します。付与されると、マネージャーは External ID を他のユーザーに割り当てることができます。

The screenshot shows the 'Edit User' dialog box with the 'Permissions' tab selected. The 'Extended Permissions' section is active, showing a list of permissions. The permission 'Manage external IDs for users' is checked and circled in red. The dialog box has a 'Cancel' button on the left and a 'Save' button on the right. The top right corner has a 'Launch Help' button and a close button (X).

Edit User Launch Help ✕

General Information > **Extended Permissions**

Locale > Allow this user to perform the following actions:

Manage external IDs for users

User Role >

Permissions >

Options >

Account Activity >

Security >

Cancel **Save**

最終更新日:2021 年 4 月 7 日