

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 ヘフォームを送信します。
- 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。

Copyright 2018-2021 by Qualys, Inc. All Rights Reserved.

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。

Enternrice englications	All applications	
Default Directory - Azure Active Directory	All applications	
 Overview 	New application	on
Manage	Enterprise Applica	tions 🗸
	Application visibility	1
All applications	Any	~
Application proxy		
	First 20 shown, to	search all of your ap
User settings	33	
Convitu	NAME	HOMEPA
Security		
Conditional Access	Didn't find what ye	ou're looking for? C

「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。 Э Federated SSO タグを持つ 最初のアプリケーションを選択します。

gle Sign-on : All	User Account Management : A Qualys PCI Online Inc.	All Categories : All	Qualys US Platform 2
0	Qualys PCI	0	Qualys US Platform 2
	Ouslys Inc.		quaries of the the the
Qualys.	selvery 2: mo	Qualys.	Qualys, Inc.
0	Qualys US Platform 3	0	Qualys EU Platform
	Qualys.	Qualys US Platform 3 Qualys. Inc.	Qualys US Platform 3 Qualys. Inc. Qualys.

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。

Logo 🛈	Name * 🕕	
	QualysGuard	
	Publisher 🛈	Provisioning (i)
QUALY:	Qualys	Automatic provisioning is not supported
	Single Sign-On Mode ①	URL ①
	SAML-based Sign-on Linked Sign-on	https://www.qualysguard.com/
	Read our step-by-step Qualys	Guard integration tutorial
	Qualys	

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。

Uplo	ad metadata file 🤈 Change single sign-on	mode 🛛 🔚 Test this application	♡ Got feedback?
up	Single Sign-On with SAMI		
чр			
d the	configuration guide 🖄 for help integrating Qu	ialysGuard-Pod1.	
	Basic SAML Configuration		
	Basic SAML Configuration		C Edit
	Basic SAML Configuration	Required	Edit
	Basic SAML Configuration Identifier (Entity ID) Reply URL (Assertion Consumer Service URL)	Required Required	C Edit
	Basic SAML Configuration Identifier (Entity ID) Reply URL (Assertion Consumer Service URL) Sign on URL	Required Required Required	Edit
	Basic SAML Configuration Identifier (Entity ID) Reply URL (Assertion Consumer Service URL) Sign on URL Relay State	Required Required Required Optional	Edit

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		
	Default	
https://QualysGuard_SharedPlatform-SAML20-SP	0	1
Patterns: QualysGuard_SharedPlatform-SAML20-SP		
Reply URL (Assertion Consumer Service URL) * ①		
The default reply URL will be the destination in the SAML response for IDP-initiated SSO		
The default reply URL will be the destination in the SAML response for IDP-initiated SSO	Default	
The default reply URL will be the destination in the SAML response for IDP-initiated SSO https://qualysguard.qg3.apps.qualys.com/IdM/saml2/	Default	
The default reply URL will be the destination in the SAML response for IDP-initiated SSO https://qualysguard.qg3.apps.qualys.com/IdM/saml2/	Default ①	
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/	Default ©	
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/	Default ①	
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 * ①	Default ①	

入力サンプル :

Identifier: https://QualysGuard_SharedPlatform-SAML20-SP

Azure AD Integration with Qualys using SAML SSO

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。

sign-on				×
« 🤊	Change single sign-on mode	Switch to the old experience		
- 4	 Welcome to the new experience feedback. 	e for configuring SAML based SSO. Please click here to provi	^{de} →	
	Sign on URL	Optional		
	Relay State	Optional		
C			_	
•	User Attributes & Clair	ms 🥒		
	Givenname	user.givenname		
	Surname	user.surname		
	Emailaddress	user.mail		
	Name	user.userprincipalname		
	sign-on	sign-on Change single sign-on mode Welcome to the new experience Sign on URL Relay State User Attributes & Claim Givenname Surname Emailaddress	sign-on Change single sign-on mode Switch to the old experience Welcome to the new experience for configuring SAML based SSO. Please click here to provi feedback. Sign on URL Optional Relay State User Attributes & Claims Givenname Surname User.givenname Emailaddress User.mail	sign-on Change single sign-on mode Switch to the old experience Welcome to the new experience for configuring SAML based SSO. Please click here to provide Sign on URL Optional Relay State User Attributes & Claims Givenname Surname Emailaddress User.mail

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。

Home > Qualys -	gle sign-on > SAML-based sign-on > User Attributes & Claims	
×	× User Attributes & Claims	
	+ Add new claim	Click to change
ick. →	Name identifier value: user.userprincipalname	
^	CLAIM NAME	VALUE
	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
/	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	user.userprincipalname
	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

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。

Home > Qualys - S	ingle sign-on > SAML-based sign-on > User	Manage user o	laims	×
×	User Attributes & Claims	**		
	Add new claim	* Name	qualysguard_external_id	~
ck. →	Name identifier value: user.userprincipal	Namespace	Enter a namespace URI	
*	CLAIM NAME	Source	Attribute Transformation	
	http://schemas.xmlsoap.org/ws/2005/05/id	* Source attribute	user.mail	~
/	http://schemas.xmlsoap.org/ws/2005/05/id			
	http://schemas.xmlsoap.org/ws/2005/05/id			
	http://schemas.xmlsoap.org/ws/2005/05/id			
	http://schemas.xmlsoap.org/ws/2005/05/id			
-		Save		

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。

Qualys - SAML-based si Enterprise Application	gn-on
	 Change single sign-on mode Switch to the old experience
g ^q Users and groups	◆ Welcome to the new experience for configuring SAML based SSO. Please click here to provide feedback. →
Single sign-on	Certificate (Raw) Download
a Provisioning	Federation Metadata XML Download
Application proxy	
G Self-service	4 Set up Qualys
Security	You'll need to configure the application to link with Azure AD.
Conditional Access	Login URL https://login.microsoftonline.com/55
	Azure AD Identifier https://sts.windows.net/55026224-57
h Permissions	Logout URL https://login.microsoftonline.com/co
Activity	View step-by-step instructions
Sign-ins	

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 gropus]を選択します。

[Add user] ボタンをクリックします。

Qualys - Users and g	roups		>
Overview Getting started	C C C C C C C C C C C C C C C C C C C	emove PUpdate Credentials EE Co	lumns le to users?' to no in properties to prevent this. $ ightarrow$
Manage	DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
Properties	No application assignments found	3	
x ^R Users and groups			
Single sign-on			

[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。

Add Assignment Default Directory	×	Users and groups	
Users and groups None Selected	>	Select member or invite an external user 1 Search by name or email address	~
Select Role User	>	Ps Patrick Slimmer pslimmer@qualys.com	
		Selected members:	
		PS Patrick Slimmer pslimmer@qualys.com	Remove
Assign	-	Select	

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。

General Information	VeriSign Identity Protection (VIP)	
Locale	See off Not Registered	Verisign
Jser Role	VIP two-factor authentication	Protection
Asset Groups	Note: This option enables VIP two-factor authentication for user	rs to login into Qualys GUI. This
Permissions	setting impacts UI access only.	
Options	SAML SSO	
Security	Enable SAML SSO	

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 する必要 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。

Locale				
	First Name: *	Patrick	Address 1: *	919 E Hillsdale Blvd
User Role	> Last Name: *	Slimmer	Address 2:	4th
Asset Groups	> Company:	saml	City:	Foster City
Permissions	> Title: *	NA	Country: *	United States of America
Options	> Phone: *	(650) 801-6100	State:	California
Security	> Fax:		ZIP Code:	94404
	E-mail Address: *	pslimmer@qualys.com	External ID (Case Sensitive)	pslimmer@qualys.com

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 useres」オプション を選択します。

Dashboard Scans Reports Remedia	tion Assets KnowledgeBase Users	
Users Users Business Units	Distribution Groups Activity Log Setup	
User Permissions Set user permissions to restrict the view of certain user information and scheduled tasks.	Security Set security options to prevent unauthorized users from accessing the service.	Business Units Alow Managers to limit the number of new IP addresses that can be added by Unit Managers. Go >
	SAML SSO Setup - Mozilla Firefox	
SAML SSO Setup		
Go ≯ Activity Log Select the timeframe for your Activity Log: 7 days, 30 days, 90 days or 180 days Go ≯	SAML SSO Setup Enable SAML SSO Managers have the option to enable SAML SSO f authentication of hosted user accounts that can provides Qualys cloud security and compliance a that manages usernames, passwords and compliance when enabled, new users will be authenticated page. Enable SAML SSO for new users	for newly created users. This gives customers full control over the access Qualys. Using SAML, Qualys acts as a Service Provider and applications. Your organization's SSO solution acts as an Identity Provider figurations used to authenticate users for Qualys. via the configured corporate Identity Provider instead of the Qualys login Save Cancel

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。

Dashboard Scans Re	ports Reme	diation Assets	KnowledgeBase	Users			
Users Users Bu	usiness Units	Distribution Groups	Activity Log	Setup			
Actions (0) 🗸 New 🗸 Search	Filters 🗸						- 16 of 16 🗼 🏶 🗸
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
Suzy 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。

Search		
Name:		
Title:		
Business Unit:	All	
External ID:		
User Login:		
Role:	Manager Unit Manager Auditor Scanner Reader Remediation User Contact User Administrat	tor
Status:	Active Dinactive Pending Activation	
Not Logged In Since:	31	
Modified Since:	31	
SAML SSO:	Disabled Enabled	
		Search

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。

Dashboard	Scans Reports R	emediation	Assets Ki	nowledgeBase U	sers			
Users	Users Business Uni	ts Distri	bution Groups	Activity Log Se	tup			
Actions (5)	New 🗸 Search Filters 🗸						1 - 5 of 5	▶ **
Delete Enable SAML		Login	Role	 Business Unit 	Status	Last Login	Modified	SAML SSO
Disable SAML		quays_ps	Manager	Unassigned	Active	07/26/2018	05/23/2018	Disabled
Clear Selections		quays_tr2	Manager	Unassigned	Active	11/05/2018	07/26/2018	Disabled
Hana Fedasz		quays_hf	Scanner	Unassigned	Active	07/09/2018	07/09/2018	Disabled
UM Created Sca	anner	quays_us2	Scanner	BU1	Active	08/04/2017	01/03/2018	Disabled
🔽 Susan Schlemm	mer	quays_ts9	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。

Edit User		Launch Help	Ø	×
General Information	Extended Permissions			
Locale	Allow this user to perform the following actions:			
User Role	Manage exemailos tor users			
Permissions				
Options	>			
Account Activity	>			
Security	>			
Cancel		Se	ave	

最終更新日:2021年4月7日