Qualys SAML 2.0 Single Sign-On (SSO) Technical Brief

Qualys provides its customers the option to use SAML 2.0 Single SignOn (SSO) authentication with their Qualys subscription. When implemented, Qualys users can seamlessly open a session using their corporate credentials and their web browser.

Qualys acts as a SAML 2.0 Service Provider (SP) and can establish a trust relationship with any customer's SAML 2.0 Identity Provider (IdP). Customers can use any SAML 2.0 IdP vendor of their choice including but not limited to Ping Identity, Shibboleth, Oracle Identity Federation and more.

Benefits

Enabling SAML 2.0 SSO with Qualys gives customers many benefits:

- Provides customers with full control over authentication of hosted user accounts that can access Qualys.

- Allows users to use their corporate credentials to open a Qualys session.

- Automatically enforce password policies applied centrally and reduces the risk of having weak passwords or lost passwords by enforcing a single password policy that is unique to the customer's SAML deployment.

- Simplifies the process of granting and removing the access to Qualys from a central management console.

- Reduces the time that users spend to remember and manage multiple passwords.

On Boarding Process

To start using SAML 2.0 SSO to open Qualys sessions, the following onboarding process has to be completed:

1) Customer sends an email to "support@qualys.com" to request SAML 2.0 SSO activation for their Qualys subscription. A CRM ticket is automatically created and will be used as a reference and tracking for all discussions concerning the activation of SAML 2.0 SSO.

2) Qualys Support replies to the ticket by email to share and request technical information used to establish the trusted relationship between the customer's IdP and the Qualys SP and as follows (please see the Appendix for full details Warning: this information might not be up-to-date. Support will share the latest version when the request is filled):

- Questions about customer's SAML 2.0 Identity Provider (IdP)

- Technical information about Qualys SAML 2.0 Service Provider (SP) that will be used to configure the customer's IdP.

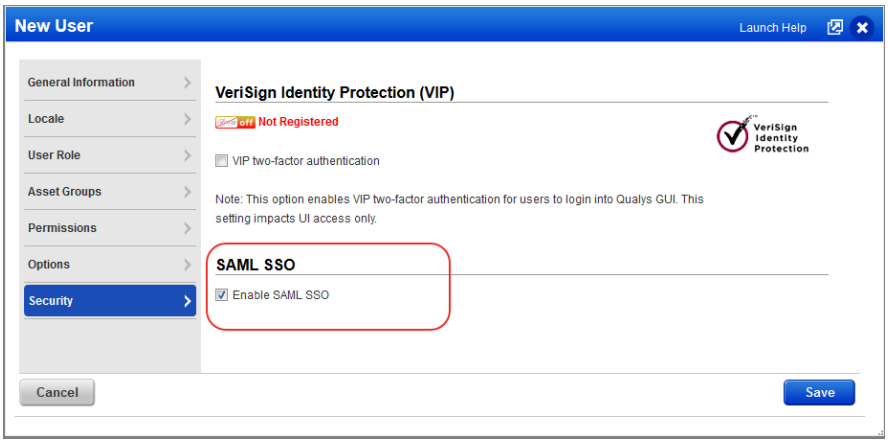
3) Upon receipt of the customer's response, Qualys will configure the trust relationship between the customer Idp and the Qualys SP. This process takes approximately one week to complete.

4) Qualys will set up the trust relationship and notifies the customer once SAML has been enabled for their subscription. Then Qualys will provide a new unique URL specific to their subscription that users must use to open a session with SAML SSO (for example https://qualysguard.qualys.com/fo/login.php?idm_key=XYZ, where XYZ is a unique numerical identifier generated by Qualys to identify the customer's subscription).

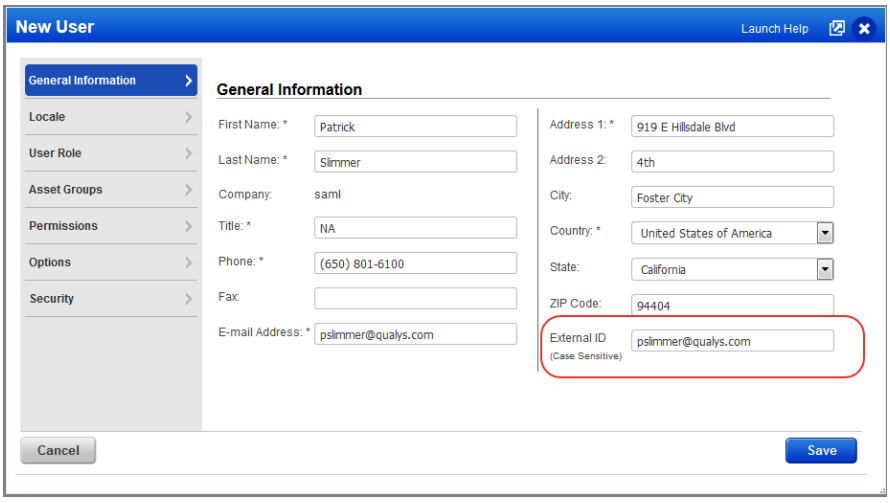
How to test

At this point customer can start testing that SAML SSO has been properly configured for their subscription using the following procedure:

1) A Qualys Manager enables SAML for a test user as shown in the screenshot here:



Optional: if the customer chose to identify the user using the "External ID" field in the Qualys user settings, this information needs to be added as shown in the screenshot below (more details provided in the User Provisioning section):



In the example above, the email address has been used for the "External ID".

2) The user testing SAML SSO should follow these steps

- Use a web browser and open the unique URL provided by Qualys.

- As a result the web browser should be redirected to the customer's SAML SSO page where the user can enter their corporate login/password (for instance the Active Directory username and password).

- Upon successful authentication, the web browser should be redirected to Qualys and a valid session should be opened with the expected user identity.

- When logging out from Qualys, the web browser should be redirected to the optional exit URL provided by the customer.

User Provisioning

Qualys SAML 2.0 supports Single SignOn authentication for user accounts that already exist in customer subscriptions. The customer needs to create a process to provision Qualys user accounts whether it's a manual process using the Qualys User Interface or an automatic process using the Qualys API (see further details below).

To properly identify each user authenticated using SAML SSO, a mapping between the customer's user identity (in the user store) and the Qualys accounts must be provided using one of the methods as described below. The customer has the option to choose the method that is most convenient for their environment:

1) Add Qualys user login names to the SAML user identity (in the user store).

2) Update Qualys accounts to add a unique user identifier in the "External ID" user property.

Customers who would like use the Qualys API for user creation and provisioning will need to develop a software program. This program will combine user account data extracted from the customer user store (such as first name, last name, email address, etc) and additional Qualys specific user information including the required Qualys user role (Manager, Unit Manager, Scanner, Reader, etc) and user scope (list of asset groups). For example the Qualys user role and scope can be derived from a group membership user information in the customer's user store. In this case the framework that describes the mapping logic between these groups and Qualys user roles and scopes must be created by the customer.

Thank You

Thank you for your interest in Qualys SAML 2.0 Single SignOn. If you have questions or if you want to provide us with feedback, please contact Qualys Support (www.qualys.com/support).

Appendix 1: Customer On Boarding Questionnaire

In order to establish the trust relationship between the customer's SAML 2.0 Identity Provider and the Qualys SAML 2.0 Service Provider, technical information needs to be provided by the customer as listed below (Refer to the information sent by Qualys support for the latest details):

Thank you for your interest in SAML. In order to get started with this feature, please provide the following information. Your responses will be entered directly into a request for our Operations team to begin the SAML integration, so filling in the questions individually and completely will assist in efficient turnaround of your request.

1) EntityID string from your IdP (SAML Identity Provider) (typically has a format like urn:mace:incommon:example.com)

2) Public key certificate for the IdP (your organization's IdP certificate)

3) Your organization's SAML IdP SSO URL (SP initiated authentication requests)

4) Subscription (Qualys Manager Primary Contact username for the subscription, such as abcd_ef)

5) Custom exit URL for a subscription (Optional). This is the URL where the user will be redirected when logging out from Qualys. For instance it can be the URL of the your corporate web site.

For your information, Operations has provided the following:

1) QWEB SP entityID: QualysGuard_SharedPlatformSAML20SP

2) ACS URL for QWEB: https://qualysguard.qualys.com/IdM/saml2/

3) Managers will be able to enable SAML support for sub-accounts after the feature is functioning on your subscription.

We will provide an update when SAML integration is complete, or if we need any additional information. Please do let me know if you have any other questions in the meantime.

Appendix 2: FAQ

Tell me about the unique Qualys SSO URL provided by Qualys

The unique URL https://qualysguard.qualys.com/fo/login.php?idm_key=XYZ provided by Qualys as part of the on boarding process must be used to open a Qualys session using SAML SSO. The customer needs to share this URL with all user who will access Qualys with SAML SSO. Users can bookmarked the URL in their web browsers. If users will log in from the customer's security intranet, the customer can insert the URL into a web page within their environment.

Tell me about two factor authentication

The customer can choose to implement two factor authentication at their discretion and if their SAML IdP implementation supports this. It is the responsibility of the customer to enable/enforce a two factor authentication mechanism for their SAML SSO IdP.

How does a user change their password?

When SAML SSO is enabled for a user, passwords are not managed by Qualys. Instead, the user should be able to change their SAML SSO password according to its company's policy.

Tell me about Qualys API access

Qualys API requires valid user credentials for authentication, and SAML SSO can't be used for this. A normal Qualys login/password must be used for all Qualys API requests.

Tell me about users who have two accounts in the same Qualys subscription

Upon successful authentication, Qualys will prompt the user to pick the user account that the user would like to use.

What if a customer has two Qualys subscriptions?

The on boarding process needs to be done twice. Once per Qualys subscription. You will receive two unique URLs, one URL for each subscription.

Are there any special Qualys account requirements?

Yes, the subscription must have the New Data Security Model enabled.

Does Qualys support SAML 1.1 or 2.0?

As of August 2012, Qualys only supports SAML 2.0.

Is it IDP initiated SSO or SP initiated?

Both Identity Provider (IDP) initiated and Service Provider (SP) initiated.

Which SAML 2.0 binding?

For SP initiated, Qualys will be using the HTTP Redirect binding to send the user to IDP and expects the SAML response via HTTP POST. For IDP initiated, Qualys expects the SAML response via HTTP POST.

When SAML is turned on for our account, can we use our own internal Active Directory user IDs or do we need to have a field in our AD user accounts that match the Qualys usernames (for example "aem_dp")?

Users have the option to either store in their Active Directory the Qualys username in each user record, or use a unique ID coming from their AD and stored in Qualys user profile under the "External ID" field. For more details, refer to the "User Provisioning" section in this document

Last updated: November 27, 2018