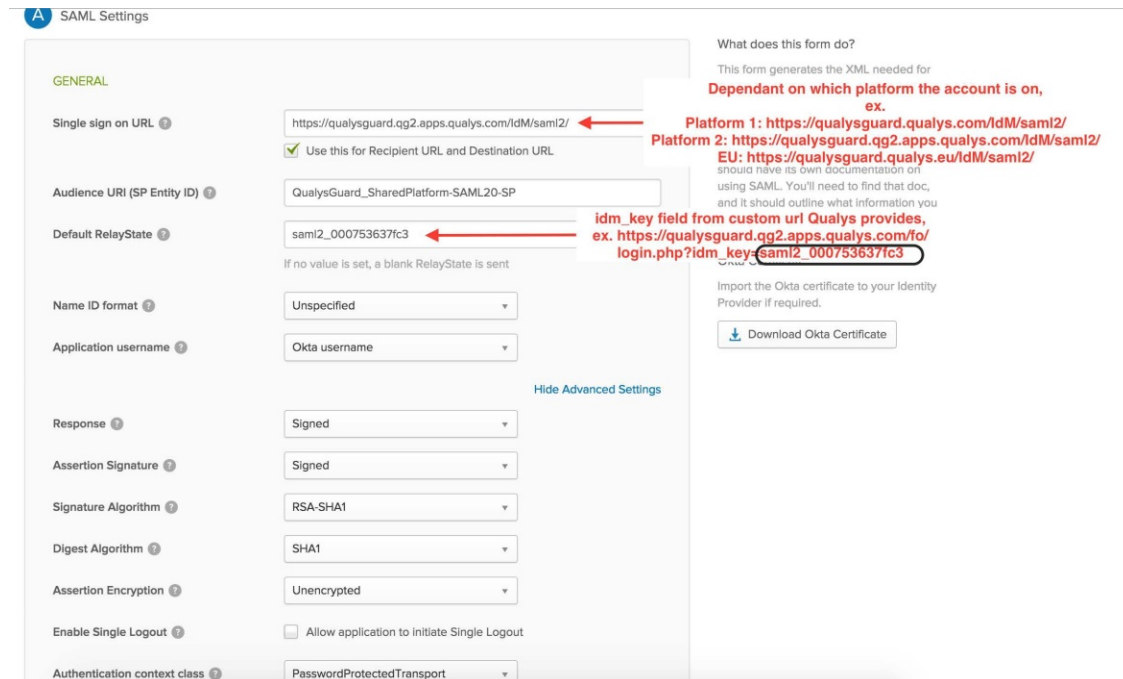


Qualys SAML & Okta Integration

Below is a screenshot of a typical Okta IdP SSO initiated SAML 2.0 integration with Qualys. Please be sure that you are creating a “New App” for Qualys and not using a “Community Created” App.

When sending the SAML assertion response to Qualys you can use SHA1 or SHA256 as the signing algorithm. Please note, if you are doing a SP-initiated SSO SAML 2.0 integration the “Default RelayState” should be left blank.

[Click here](#) for complete information on Qualys SAML Support.



SAML Settings

GENERAL

Single sign on URL
 Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID)

Default RelayState
 If no value is set, a blank RelayState is sent

Name ID format

Application username

Response

Assertion Signature

Signature Algorithm

Digest Algorithm

Assertion Encryption

Enable Single Logout Allow application to initiate Single Logout

Authentication context class

What does this form do?
This form generates the XML needed for
Dependant on which platform the account is on,
ex.
Platform 1: https://qualysguard.qualys.com/IdM/saml2/
Platform 2: https://qualysguard.qg2.apps.qualys.com/IdM/saml2/
EU: https://qualysguard.qualys.eu/IdM/saml2/
SPROU please see its own documentation on using SAML. You'll need to find that doc, and it should outline what information you should provide.

idm_key field from custom url Qualys provides, ex. https://qualysguard.qg2.apps.qualys.com/fo/login.php?idm_key=saml2_000753637fc3

Import the Okta certificate to your Identity Provider if required.

[Hide Advanced Settings](#)

Last updated: December 12, 2018