AVI
Networks®

SAML Authentication for Single Sign-On

Avi Technical Reference (v20.1)

SAML Authentication for Single Sign-On

view online

Starting with release 17.2.4, Avi Vantage supports single sign-on (SSO) to the Avi Controller's UI using Security Assertion Markup Language (SAML). SAML is an XML-based markup language for exchanging authentication and authorization between an identity provider (IdP) and a service provider(SP).

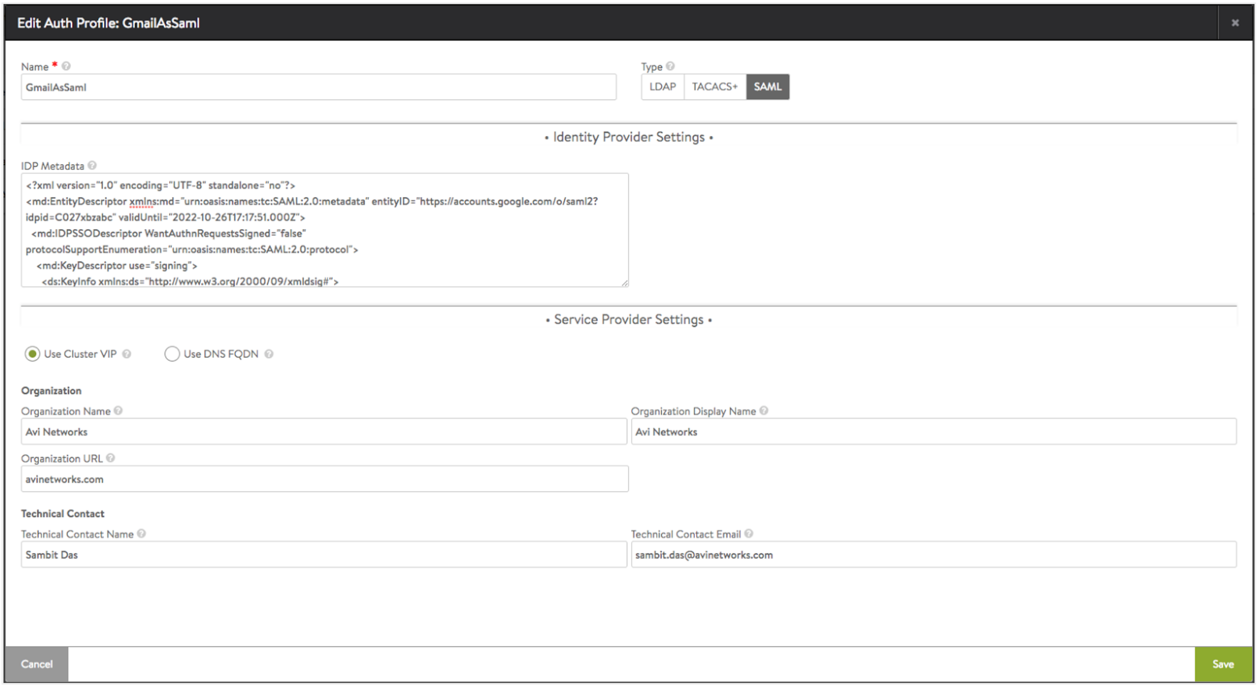
Avi has verified interoperability with the Google, Okta and OneLogin IdPs. Contact your Avi sales team if you require integration with other IdPs.

Configuring SSO with SAML via the Avi UI

SAML settings can be configured in the authentication profile. Navigate to Templates > Security > Auth Profile. Enter a name for the profile and select SAML as Type.

Settings

Any node acting as a service provider must generate a metadata file for registration with the IdP. The file contains configuration and integration details for SAML single sign-on. Obtain the metadate file from your identity provider.



Edit Auth Profile: GmailAsSaml

Name *: GmailAsSaml

Type: LDAP TACACS+ [✓ SAML]

• Identity Provider Settings •

IDP Metadata

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://accounts.google.com/o/saml2?
idpid=C027xbzabc" validUntil="2022-10-26T17:17:51.000Z">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
```

• Service Provider Settings •

● Use Cluster VIP ○ Use DNS FQDN

Organization

Organization Name: Avi Networks

Organization Display Name: Avi Networks

Organization URL: avinetworks.com

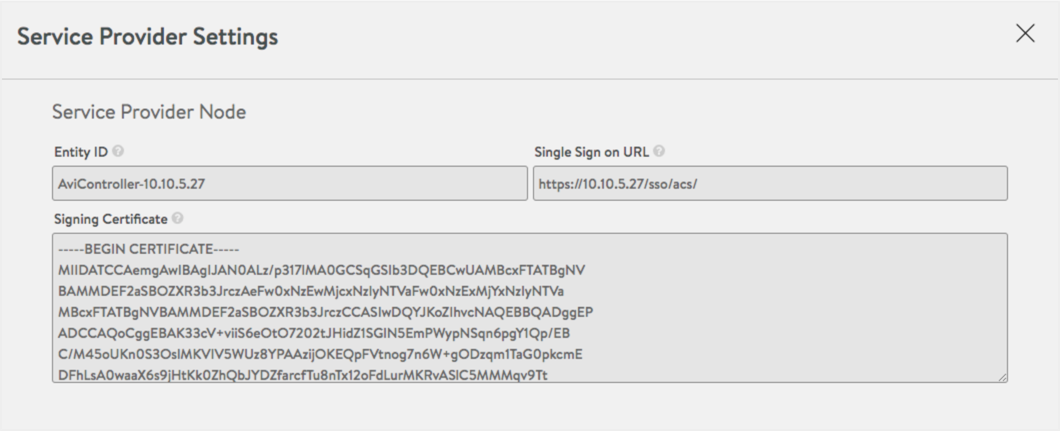
Technical Contact

Technical Contact Name: Sambit Das

Technical Contact Email: sambit.das@avinetworks.com

Figure 1. Authentication profile editor

Service provider metadata contains keys, services and URLs defining SAML endpoints of the Avi Controller. The Avi Controller can be registered using its cluster IP or a DNS-resolvable FQDN. If ?Use Cluster IP? is selected, then the cluster IP is picked up automatically. If ?Use DNS FQDN? is chosen, the user will be prompted to provide an FQDN.



Service Provider Settings

Service Provider Node

Entity ID: AviController-10.10.5.27

Single Sign on URL: https://10.10.5.27/sso/acs/

Signing Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDATCCAemgAwIBAgIJAN0ALz/p317IMA0GCSqGSIb3DQEBCwUAMBcxFTATBgNV
BAMMDEF2aSBOZXR3b3JrczAeFw0xNzEwMjcxNzIyNTVaFw0xNzExMjYxNzIyNTVa
MBcxFTATBgNVBAMMDEF2aSBOZXR3b3JrczCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAK33cV+viiS6eOtO7202tJHidZ1SGIN5EmPWypNSqn6pgY1Qp/EB
C/M45oUKn0S3OsIMKVIV5WUz8YPAAzijOKEQpFVtnog7n6W+gODzqm1TaG0pkcmE
DFhLsA0waaX6s9jHtKk0ZhQbJYDZfarcfTu8nTx12oFdLurMKRvASIC5MMMqv9Tt
```

Figure 2. Service provider settings

Service provider settings can be retrieved by clicking on the ? button on the list page. This page contains the service provider entity-ID and the single sign-on URL generated by the Avi Controller. The signing certificate is a self-signed certificate with common name set to the entity-id. This certificate is used by the IdP for encrypting the assertion response.

Create Application on the IdP

A SAML application needs to be created on the IdP using this Controller-generated information. The entity-ID and the single sign-on URL required while creating the application on IdP needs to precisely match the Avi-generated configuration.

In the case of certain identity providers, IdP metadata can be retrieved after the SAML application has been created. In those cases, the recommended workflow is to create a SAML authentication profile on Avi Vantage without IdP metadata and then use the Avi-generated attributes to create the SAML application. Once the application has been created, the IdP metadata can be plugged into the authentication profile. The authentication profile cannot be attached to the system configuration without valid IdP metadata.

Note: Starting with Avi Vantage version 20.1.1, both SAML assertion and response signing are mandatory for successful SAML authentication.

Local Admin or User Logon

After SAML-based access is enabled, you may occasionally want to have the Avi Vantage web console display the logon UI *without* redirecting to the SAML authentication profile configured on the IdP logon page. To do so, send the Controller or cluster IP address a URL which takes on one of the following two forms:

- `https://ControllerIP/#!/login?local=1`
- `https://FQDN/#!/login?local=1`