

# SWAMID HowTo (Shibboleth 2.x)

Konfiguration för shibboleth 2.x IdP för SWAMID SAML WebSSO.

## relying-party.xml

Stoppa in följande block XML på relevant plats i relying-party.xml. Spara certifikatet från [SAML WebSSO](#) i filen /opt/shibboleth-idp/credentials/md-signer.crt.

Definiera att det nedladdade certifikatet ska användas för kontroll av signatur av Swamids metadata:

```
<!-- SWAMID-METADATA-Trustengine and SWAMID-TESTING-METADATA-Trustengine -->
<security:TrustEngine id="swamid-metadata-signer" xsi:type="security:StaticExplicitKeySignature">
  <security:Credential id="MyFederation1Credentials" xsi:type="security:X509Filesystem">
    <security:Certificate>/opt/shibboleth-idp/credentials/md-signer.crt</security:Certificate>
  </security:Credential>
</security:TrustEngine>
```

Hämta metadata för SWAMID med följande konfiguration:

```
<!-- SWAMID METADATA PROVIDER -->
<MetadataProvider id="SwamidMD" xsi:type="FileBackedHTTPMetadataProvider" xmlns="urn:mace:shibboleth:2.0:
metadata"
  metadataURL="http://md.swamid.se/md/swamid-1.0.xml"
  backingFile="/opt/shibboleth-idp/metadata/swamid-1.0.xml">
  <MetadataFilter xsi:type="ChainingFilter" xmlns="urn:mace:shibboleth:2.0:metadata">
    <MetadataFilter xsi:type="SignatureValidation" xmlns="urn:mace:shibboleth:2.0:metadata"
      trustEngineRef="swamid-metadata-signer"
      requireSignedMetadata="true" />
  </MetadataFilter>
</MetadataProvider>
```

Ni behöver även hämta metadata för Swamis testfederation för att tillåta realistiska tester för ej driftsatta tjänsteleverantörer (SP):

```
<!-- SWAMID TEST METADATA PROVIDER -->
<MetadataProvider id="SwamidTestMD" xsi:type="FileBackedHTTPMetadataProvider" xmlns="urn:mace:shibboleth:2.0:
metadata"
  metadataURL="http://md.swamid.se/md/swamid-testing-1.0.xml"
  backingFile="/opt/shibboleth-idp/metadata/swamid-testing-1.0.xml">
  <MetadataFilter xsi:type="ChainingFilter" xmlns="urn:mace:shibboleth:2.0:metadata">
    <MetadataFilter xsi:type="SignatureValidation" xmlns="urn:mace:shibboleth:2.0:metadata"
      trustEngineRef="swamid-metadata-signer"
      requireSignedMetadata="true" />
  </MetadataFilter>
</MetadataProvider>
```

## attribute-filter.xml

Följande AttributeFilterPolicy är den rekommenderade för SWAMID SAML WebSSO. Den ger tillgång till grundläggande personinformation för alla SPar i federationen, inkl. testfederationen. Glöm inte lägga in tillägg för [attributdefinitioner norEdu-familjen](#) och [rekommenderad release av statisk organisationsinformation](#) i attribute-release.xml.

Förutom denna konfiguration måste normalt ett antal attribut enablas som är utkommenterade per default i Shibboleth. Ett komplett exempel (för scope /domän example.com) finns här: [attribute-resolver.xml](#).

```

<!-- recommended initial attribute filter policy for swamid.se -->
<AttributeFilterPolicy id="swamid">
  <PolicyRequirementRule xsi:type="basic:OR">
    <basic:Rule xsi:type="saml:AttributeRequesterInEntityGroup" groupId="http://md.swamid.se/md/swamid-
1.0.xml" />
    <basic:Rule xsi:type="saml:AttributeRequesterInEntityGroup" groupId="http://md.swamid.se/md/swamid-
testing-1.0.xml" />
  </PolicyRequirementRule>
  <AttributeRule attributeID="givenName">
    <PermitValueRule xsi:type="basic:ANY" />
  </AttributeRule>
  <AttributeRule attributeID="surname">
    <PermitValueRule xsi:type="basic:ANY" />
  </AttributeRule>
  <AttributeRule attributeID="displayName">
    <PermitValueRule xsi:type="basic:ANY" />
  </AttributeRule>
  <AttributeRule attributeID="commonName">
    <PermitValueRule xsi:type="basic:ANY" />
  </AttributeRule>
  <AttributeRule attributeID="eduPersonPrincipalName">
    <PermitValueRule xsi:type="basic:ANY" />
  </AttributeRule>
  <AttributeRule attributeID="email">
    <PermitValueRule xsi:type="basic:ANY" />
  </AttributeRule>
  <AttributeRule attributeID="eduPersonScopedAffiliation">
    <PermitValueRule xsi:type="basic:OR">
      <basic:Rule xsi:type="basic:AttributeValueString" value="faculty" ignoreCase="true" />
      <basic:Rule xsi:type="basic:AttributeValueString" value="student" ignoreCase="true" />
      <basic:Rule xsi:type="basic:AttributeValueString" value="staff" ignoreCase="true" />
      <basic:Rule xsi:type="basic:AttributeValueString" value="alum" ignoreCase="true" />
      <basic:Rule xsi:type="basic:AttributeValueString" value="member" ignoreCase="true" />
      <basic:Rule xsi:type="basic:AttributeValueString" value="affiliate" ignoreCase="true" />
      <basic:Rule xsi:type="basic:AttributeValueString" value="employee" ignoreCase="true" />
      <basic:Rule xsi:type="basic:AttributeValueString" value="library-walk-in" ignoreCase="true" />
    </PermitValueRule>
  </AttributeRule>
</AttributeFilterPolicy>

```