SAML based SSO Implementation Guide

Service Provider

Document Details

Document #: 160_SG550_200423

Release Version: 05.50.00.00

Version Release Date: July 2017

Overview

Audience: The Operations staff supporting the on-premise CrunchTime Applications.

This document explains how to implement SAML based SSO from SP's perspective

System Requirements

- CES Release Version 05.50.00 or higher
- Be sure to grab the latest version of this document here: https://links.crunchtime.com/SG-SSOImplementationGuide-SP

Other Related Documentation

- SAML based SSO Implementation Guide-IdP: https://links.crunchtime.com/SG-SSOImplementationGuide-IdP
- SAML based SSO Implementation Guide-IdP-ADFS Addendum: https://links.crunchtime.com/SG-SSOImplementationGuide-IdP-ADFS

© 2021 CrunchTime! Information Systems, Inc. All Rights Reserved. | www.crunchtime.com

Service Provider Tasks

1. **Manage (self-signed) private key and certificate, if using encryption of assertion for SAML SSO.**
   - Private key store in in pkcs12 format
   - Password to the private key store
   - Alias for keystore entry
   - 509 certificate corresponding to the private key store (used below in metadata file)

2. **Create SP metadata files using the following template (replacing highlighted section), and provide it to IdP. One dedicated file should be created for each of the following:**
   - Prod NC
   - Prod EW
   - Test NC
   - Test EW

Crunchtime SAML SP metadata file template

```
<EntityDescriptor
    xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    entityID="https://[on-premise.net-chef.url]/sso/saml/post">

  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Data>
          <X509Certificate>
MIIFJDCCBAygAwIBAgIJAIji132BFnNVMA0GCSqGSIb3DQEBBQUAMIG8MQswCQYD
VQQGEwJVUzEWMBQGA1UECBMNTWFzc2FjaHVzZXR0czEPMA0GA1UEBxMGQm9zdG9u
MSgwJgYDVQQKDB9DcnVuY2h0aW1lISBJbmZvcm1hdGlvbiBTeXN0ZW1zMQswCQYD
VQQLEwJJVDEUMBIGA1UEAxMLaW50ZWdyYXRpb24xNzA1BgkqhkiG9w0BCQEWKGNy
dW5jaHRpbWUtaW5mcmFzdHJ1Y3R1cmVAY3J1bmNodGltZS5jb20wHhcNMTUwODI3
MTk1MjA5WhcNMzUwODIyMTk1MjA5WjCBvDELMAkGA1UEBhMCVVMxFjAUBgNVBAgT
DU1hc3NhY2h1c2V0dHMxDzANBgNVBAcTBkJvc3RvbjEoMCYGA1UECgwfQ3J1bmNo
dGltZSEgSW5mb3JtYXRpb24gU3lzdGVtczELMAkGA1UECxMCSVQxFDASBgNVBAMT
C2ludGVncmF0aW9uMTcwNQYJKoZIhvcNAQkBFihjcnVuY2h0aW1lLWluZnJhc3Ry
dWN0dXJlQGNydW5jaHRpbWUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA2DuHFpepdUt0FZupTHOeKda/9gcosZ9zAZOF1mvbyjUbrKJFinyRn+sK
r1Ed4w3++1Drb/u2x/B+faGURIEfJcaCDiZilXVtTRViP2Lt0Vv7y2zNv9GWNkY6
Fi5cEjbP94GwJMAdB0o0ddRIFSGUN/4+uxotEb9O0elS5Htp7/kfS8w6/bZYgKGO
J8lWDL0VfLSQh0wVSRqJdWPMjVKhL0TrBEhWLTpWXiIASUI90S+BZCIQfp49D4Oi
dCgWloU63BlPMQ6tdznL35sCH8TAi/ecYZITacB0lp5KKlO7j4gkcNmDBd0ZdU6/
ShbG1s44uHcMGAKoAJzMpDkEwHftcwIDAQABo4IBJTCCASEwHQYDVR0OBBYEFDSD
fbCB/zM3viq7ofPukNN609/4MIHxBgNVHSMEgekwgeaAFDSDfbCB/zM3viq7ofPu
kNN609/4oYHCpIG/MIG8MQswCQYDVQQGEwJVUzEWMBQGA1UECBMNTWFzc2FjaHVz
ZXR0czEPMA0GA1UEBxMGQm9zdG9uMSgwJgYDVQQKDB9DcnVuY2h0aW1lISBJbmZv
cm1hdGlvbiBTeXN0ZW1zMQswCQYDVQQLEwJJVDEUMBIGA1UEAxMLaW50ZWdyYXRp
b24xNzA1BgkqhkiG9w0BCQEWKGNydW5jaHRpbWUtaW5mcmFzdHJ1Y3R1cmVAY3J1
bmNodGltZS5jb22CCQCI4td9gRZzVTAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEB
BQUAA4IBAQCCspQPYVQjw2vPHCn37z117xJhqPjgI7Bjk1PH9Nb2UkdLwhw7va6P
a+jAa/TozReipi3vscp5JhTWTsP6KTQoSMTAATF/wUU4dm2Hos2/GBpisMTi32sK
fem7NHJixWlpHvtpLpNC5bwmodDkTGhGDzkF5P01odpRxh3HsR7Ldaa8/15bcNBs
hDSGAXrU6w0TUddVZ1XKQwStY5wMejV89cCl/xhE6EjRB2X5ZDpg7jOZetwO8n2o
pgaT1BBiJ7EbUme3LSIOKx5g0arAuEmRJBy0C0tsX5XoiQnXJRJyNYiNxn1BoMgB
10aPr3Om2uyqGgIbB07xx4ntI+cCcXMF
          </X509Certificate>
        </X509Data>
      </KeyInfo>
    </KeyDescriptor>
    <KeyDescriptor use="encryption">
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
```

© 2021 CrunchTime! Information Systems, Inc. All Rights Reserved. | www.crunchtime.com

Service Provider Tasks (Continued)

```
        <X509Data>
          <X509Certificate>
MIIFJDCCBAygAwIBAgIJAIji132BFnNVMA0GCSqGSIb3DQEBBQUAMIG8MQswCQYD
VQQGEwJVUzEWMBQGA1UECBMNTWFzc2FjaHVzZXR0czEPMA0GA1UEBxMGQm9zdG9u
MSgwJgYDVQQKDB9DcnVuY2h0aW1lISBJbmZvcm1hdGlvbiBTeXN0ZW1zMQswCQYD
VQQLEwJJVDEUMBIGA1UEAxMLaW50ZWdyYXRpb24xNzA1BgkqhkiG9w0BCQEWKGNy
dW5jaHRpbWUtaW5mcmFzdHJ1Y3R1cmVAY3J1bmNodGltZS5jb20wHhcNMTUwODI3
MTk1MjA5WhcNMzUwODIyMTk1MjA5WjCBvDELMAkGA1UEBhMCVVMxFjAUBgNVBAgT
DU1hc3NhY2h1c2V0dHMxDzANBgNVBAcTBkJvc3RvbjEoMCYGA1UECgwfQ3J1bmNo
dGltZSEgSW5mb3JtYXRpb24gU3lzdGVtczELMAkGA1UECxMCSVQxFDASBgNVBAMT
C2ludGVncmF0aW9uMTcwNQYJKoZIhvcNAQkBFihjcnVuY2h0aW1lLWluZnJhc3Ry
dWN0dXJlQGNydW5jaHRpbWUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA2DuHFpepdUt0FZupTHOeKda/9gcosZ9zAZOF1mvbyjUbrKJFinyRn+sK
r1Ed4w3++1Drb/u2x/B+faGURIEfJcaCDiZilXVtTRViP2Lt0Vv7y2zNv9GWNkY6
Fi5cEjbP94GwJMAdB0o0ddRIFSGUN/4+uxotEb9O0elS5Htp7/kfS8w6/bZYgKGO
J8lWDL0VfLSQh0wVSRqJdWPMjVKhL0TrBEhWLTpWXiIASUI90S+BZCIQfp49D4Oi
dCgWloU63BlPMQ6tdznL35sCH8TAi/ecYZITacB0lp5KKlO7j4gkcNmDBd0ZdU6/
ShbG1s44uHcMGAKoAJzMpDkEwHftcwIDAQABo4IBJTCCASEwHQYDVR0OBBYEFDSD
fbCB/zM3viq7ofPukNN609/4MIHxBgNVHSMEgekwgeaAFDSDfbCB/zM3viq7ofPu
kNN609/4oYHCpIG/MIG8MQswCQYDVQQGEwJVUzEWMBQGA1UECBMNTWFzc2FjaHVz
ZXR0czEPMA0GA1UEBxMGQm9zdG9uMSgwJgYDVQQKDB9DcnVuY2h0aW1lISBJbmZv
cm1hdGlvbiBTeXN0ZW1zMQswCQYDVQQLEwJJVDEUMBIGA1UEAxMLaW50ZWdyYXRp
b24xNzA1BgkqhkiG9w0BCQEWKGNydW5jaHRpbWUtaW5mcmFzdHJ1Y3R1cmVAY3J1
bmNodGltZS5jb22CCQCI4td9gRZzVTAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEB
BQUAA4IBAQCCspQPYVQjw2vPHCn37z117xJhqPjgI7Bjk1PH9Nb2UkdLwhw7va6P
a+jAa/TozReipi3vscp5JhTWTsP6KTQoSMTAATF/wUU4dm2Hos2/GBpisMTi32sK
fem7NHJixWlpHvtpLpNC5bwmodDkTGhGDzkF5P01odpRxh3HsR7Ldaa8/15bcNBs
hDSGAXrU6w0TUddVZ1XKQwStY5wMejV89cCl/xhE6EjRB2X5ZDpg7jOZetwO8n2o
pgaT1BBiJ7EbUme3LSIOKx5g0arAuEmRJBy0C0tsX5XoiQnXJRJyNYiNxn1BoMgB
10aPr3Om2uyqGgIbB07xx4ntI+cCcXMF
          </X509Certificate>
        </X509Data>
      </KeyInfo>
      <EncryptionMethod Algorithm=
                           "https://www.w3.org/2001/04/xmlenc#aes128-cbc">
        <KeySize xmlns="https://www.w3.org/2001/04/xmlenc#">256</KeySize>
      </EncryptionMethod>
    </KeyDescriptor>

    <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
    <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>

    <AssertionConsumerService index="1" isDefault="true"
                              Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                              Location="https://[on-premise.net-chef.url]/sso/saml/post"/>
    <md:AttributeConsumingService index="0"
                                  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
                                  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
      <md:ServiceName xml:lang="en">AttributeConsumingService</md:ServiceName>
      <md:ServiceDescription xml:lang="en">CrunchTime Service to extract username from SAML
Assertion</md:ServiceDescription>
      <md:RequestedAttribute isRequired="true"
                             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:string"
                             Name="username"
                             FriendlyName="username"/>
    </md:AttributeConsumingService>

  </SPSSODescriptor>

  <Organization>
    <OrganizationName xml:lang="en">CrunchTime</OrganizationName>
    <OrganizationDisplayName xml:lang="en">CrunchTime! Information Systems</OrganizationDisplayName>
    <OrganizationURL xml:lang="en">http://www.Crunchtime.com/</OrganizationURL>
  </Organization>
  <ContactPerson contactType="technical">
    <GivenName>Your</GivenName>
    <SurName>Admin</SurName>
    <EmailAddress>support@crunchtime.com</EmailAddress>
  </ContactPerson>
</EntityDescriptor>
```

© 2021 CrunchTime! Information Systems, Inc. All Rights Reserved. | www.crunchtime.com

Service Provider Tasks (Continued)

3. **Enable and configure SAML SSO in CrunchTime application**
   - Place the following files at /crunchtime/conf/saml/[sitename]/
     - Crunchtime keystore file in pkcs12 format (from above)
     - Crunchtime SAML SP metadata file (the NC file from above step)
     - IdP metadata file (the NC file from IdP)
   - Update T_application_setting table based on actual config filenames above for the following setting_name:
     - sso.saml.ct.keystore
     - sso.saml.ct.metadata
     - sso.saml.customer.metadata
   - Update T_application_setting table based on information from IdP:
     - sso.saml.assertion.signed
     - sso.saml.assertion.encrypted
   - T_application_setting.setting_value need to be set to 'true' for setting_name='sso.saml.enabled' to enable SAML SSO.
   - If customer will use CT mobile apps with SAML SSO, T_application_setting.setting_value need to be set to 'true' for setting_name='sso.saml.sp.init.enabled' to allow mobile apps to use SAML SSO.
   - If the above files or database settings are changed, site needs to be reloaded from server-admin (06.40.00.XX and higher), or Tomcat restarted (06.30.00.XX and lower) for the changes to take effect.
   - Edit /crunchtime/conf/sitekeys.json and enter the following to allow CrunchTime application to read the private key to decrypt encrypted assertion coming from IdP.

```
[
  {
    "site.name": "customer1",             -- this identifies the site this entry is for
    "ct_keystore_password": "YourPasswordHere",              -- this is the password used to open the
key store file
    "ct_key_entry_alias": "Crunchtime_Infrastructure"  -- this is the alias for the key entry stored
inside the key store file
  }
]
```

© 2021 CrunchTime! Information Systems, Inc. All Rights Reserved. | www.crunchtime.com