SAML based SSO Implementation Guide

Identity Provider

Document Details

Document #: 160_SG550_200423

Release Version: 05.50.00.00

Version Release Date: July 2017

Overview

Audience: The IT staff of CrunchTime's on-premise client managing IdP.

This document explains how to implement SAML based SSO from the IdP'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-IdP

Other Related Documentation

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

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

Identity Provider Tasks

1. **Provide the following SAML SSO information to CrunchTime Application Operator (SP).**
   - Whether Assertion will be encrypted
   - Whether Assertion will be signed
   - IdP metadata files, one for each of the following: prod-nc; prod-emw; test-nc; test-emw.

   Note: When signature is used, certs are provided inside IdP Metadata file for SP to verify the signature. Crunchtime application requires the same certs to be used for a NC-EMW pair. For example, test-NC and test-EMW should use the same certs; prod-NC and prod-EMW should use the same certs

2. **Import SAML SP metadata files provided by CrunchTime Application Operator into IdP**
   - There should be four metadata files, one for each of the following:
     - Production Net-Chef
     - Production EM Web
     - Test Net-Chef
     - Test EM Web
   - For IdP-Initiated SSO scenario, one link should be created for each of the following destination:
     - Production Net-Chef
     - Production EM Web
     - Test Net-Chef
     - Test EM Web
   - For SP-Initiated SSO scenario, provide the following landing URL to end users:
     - Production Net-Chef: https://[on-premise.net-chef.url]/sso/saml
     - Production EM Web: https://[on-premise.emweb.url]/sso/saml
     - Test Net-Chef: https://[on-premise-test.net-chef.url]/sso/saml
     - Test EM Web: https://[on-premise-test.emweb.url]/sso/saml

3. **Provision IdP to create SAML Response based on specification of CrunchTime Application**
   - The SAML assertion should contain statement for attribute named "username", whose value should be the username intended for the CrunchTime application.
   - The SAML assertion can be signed with a private key available to the IdP (recommended).
   - The SAML assertion can be encrypted with a public key (provided in SP metadata file), using algorithm aes128-cbc and key transport RSA-v1.5.

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

Sample SAML response expected by CrunchTime Application

Note: This is shown as unencrypted and unsigned only to demonstrate the content structure; the actual response would contain encrypted signed assertion and would be base64 encoded.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" ID="_1df9a098e9b0eccb98baef9d79dc3aa4"
InResponseTo="https://customer1.net-chef.com/sso/saml/post" IssueInstant="2015-09-07T19:15:15.000Z"
Version="2.0">
      <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://idp.customer1.com/SSO/SAML</saml2:Issuer>
      <saml2p:Status>
            <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
      </saml2p:Status>
      <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_352ef8965303ea724ff54d366856a3c3" IssueInstant="2015-09-07T19:15:15.000Z" Version="2.0">
            <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://idp.customer1.com/SSO/SAML</saml2:Issuer>
            <saml2:Subject>
                  <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">3f7b3dcf-1674-
4ecd-92c8-1544f346baf8</saml2:NameID>
                  <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                        <saml2:SubjectConfirmationData InResponseTo="https://customer1.net-
chef.com/sso/saml/post" NotOnOrAfter="2015-09-07T19:15:45.000Z" Recipient="https://customer1.net-
chef.com/sso/saml/post"/>
                  </saml2:SubjectConfirmation>
            </saml2:Subject>
            <saml2:Conditions NotBefore="2015-09-07T19:15:15.000Z" NotOnOrAfter="2015-09-07T19:15:45.000Z">
                  <saml2:AudienceRestriction>
                        <saml2:Audience>https://customer1.net-chef.com/sso/saml/post</saml2:Audience>
                  </saml2:AudienceRestriction>
            </saml2:Conditions>
            <saml2:AuthnStatement AuthnInstant="2015-09-07T19:15:15.000Z">
                  <saml2:AuthnContext>
      <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol</saml2:AuthnContextCl
assRef>
                  </saml2:AuthnContext>
            </saml2:AuthnStatement>
            <saml2:AttributeStatement>
                  <saml2:Attribute Name="username" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:string">
                        <saml2:AttributeValue>devgump</saml2:AttributeValue>
                  </saml2:Attribute>
            </saml2:AttributeStatement>
      </saml2:Assertion>
</saml2p:Response>
```

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