Customer Implementation

SAML based SSO to Crunchtime Enterprise Systems

Setup Guide

Document Details

Document #: 160_SSOSG_260713
Release Version: 11.00.00.00 or higher
Version Release Date: October 2023

Overview

This document explains how to implement SAML based SSO to Crunchtime Enterprise Systems.

Download the latest version of this document here:
https://links.crunchtime.com/SG-SSOCustomerImplGuide

… or scan the QR code to the left.

© 2026 Crunchtime - All Rights Reserved

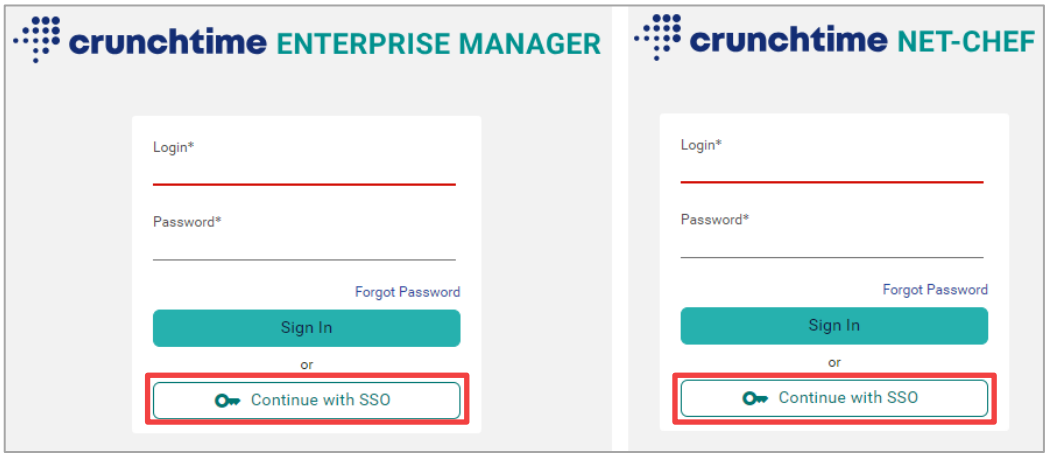
Customer Tasks

1. Provide the following SAML SSO information to Crunchtime (SP).
   - Indicate whether Assertion will be encrypted (recommendation: No)
   - Indicate whether Assertion will be signed (recommendation: Yes)
   - IdP metadata URLs (preferred) or files

Note: We typically enable SAML SSO in customer test site first and verify proper SSO function before enabling SSO for customer production site.

Note: NC and EM use different URLs and can be considered different applications. For purpose of SSO, NC and EM can use either the same or different values for IdP metadata URL/file and signing certificate (if using signature).

Note: Crunchtime will configure SAML SSO for requested customer site and enable SSO link on NC/EM login screen. Crunchtime will also provide NC and EM SP metadata files to customer.



2. Create EM/NC/TWX SSO app profiles in IdP either manually based on the content of SP metadata files provided by Crunchtime or by importing them.
3. Configure EM/NC/TWX SSO app profiles in IdP to create SAML Response based on specification of Crunchtime Application.
   - For EM/NC, the SAML assertion should contain a statement for the “username” attribute, whose value should be the username for the EM/NC user. (*See screens on following pages*.)
   - For TWX, the SAML assertion should contain a statement for the “employeeNumber” attribute, whose value should be the Employee Number for the Teamworx user, which must match the entry in the employee record in Net-Chef.
   - 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 (not recommended).

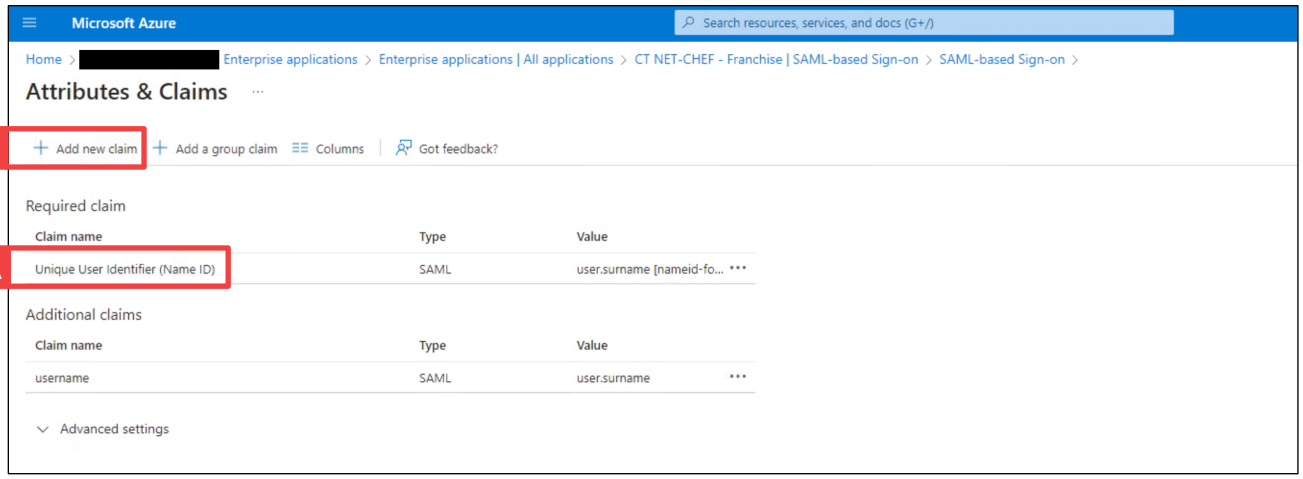
(Continued)

© 2026 Crunchtime - All Rights Reserved

Customer Tasks

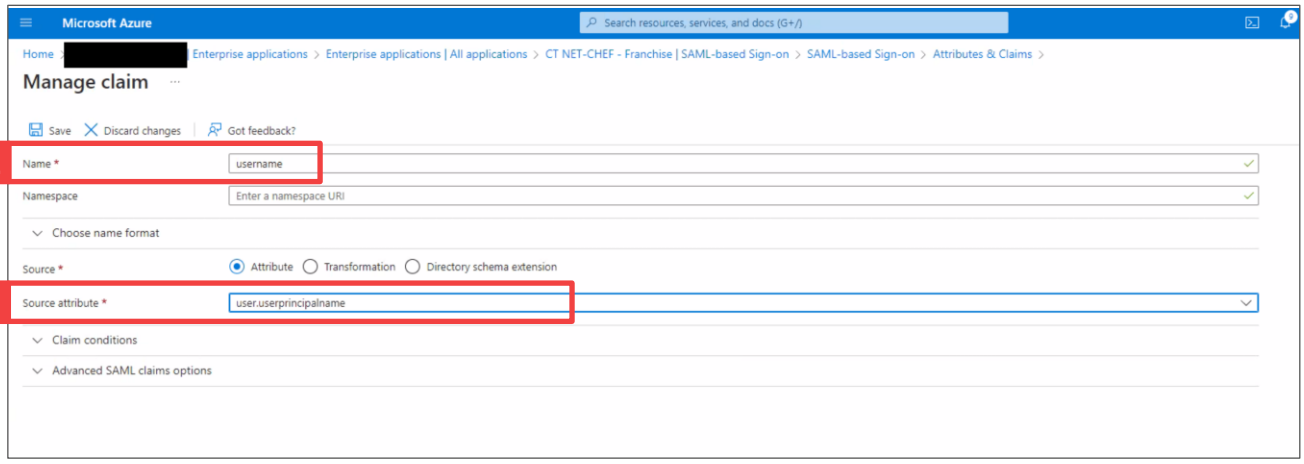
(Continued)

Microsoft Entra Configuration



A CES ignores this field. You need to custom map the “username” attribute.

1 Under “Attributes and Claims”, select **+** *Add new claim*.



2 In the *Name* field, enter ‘username’ in all lower case.

3 In the *Source attribute* field, select the attribute that matches the User ID in CES.

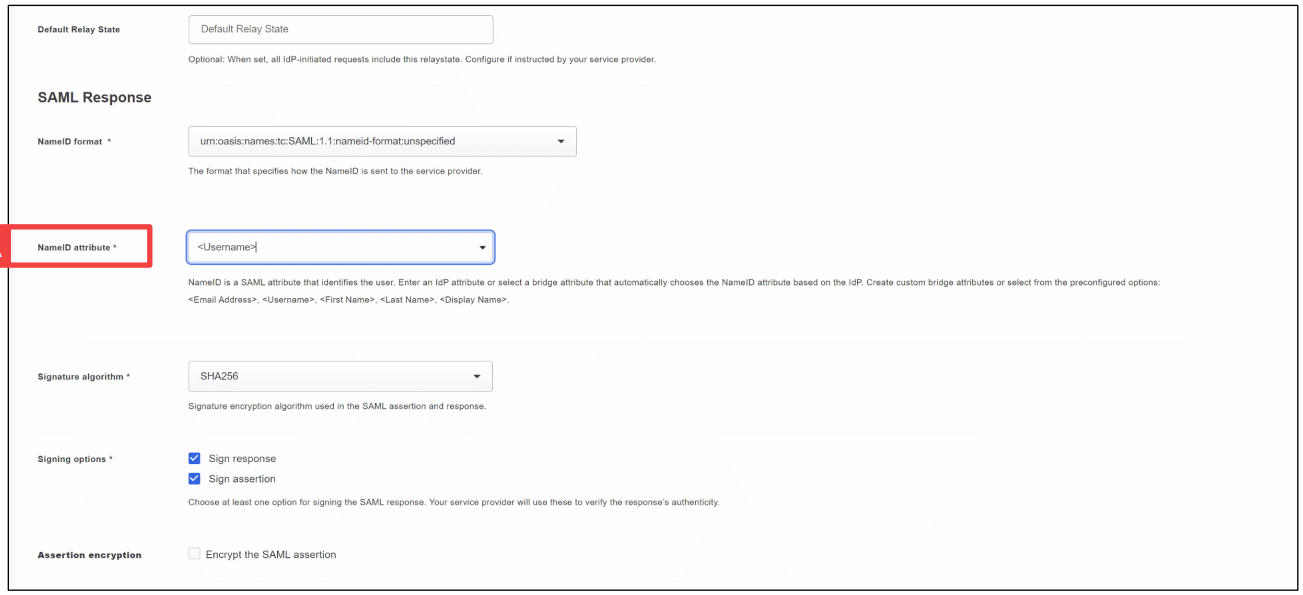
(Continued)

© 2026 Crunchtime - All Rights Reserved | www.crunchtime.com | 3

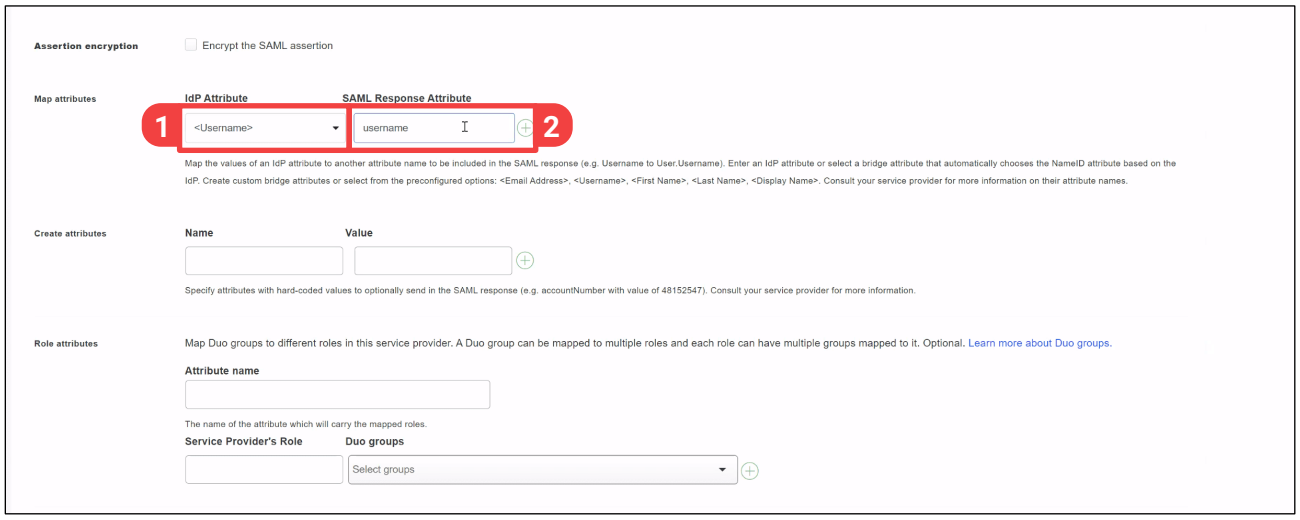
Customer Tasks

(Continued)

Cisco Duo Configuration



A CES ignores this field. You need to custom map the “username” attribute.



1 Under “Map attributes”, in the *IdP Attribute* field, select the attribute that matches the User ID in CES.

2 In the *SAML Response Attribute* field, enter ‘username’ in all lower case.

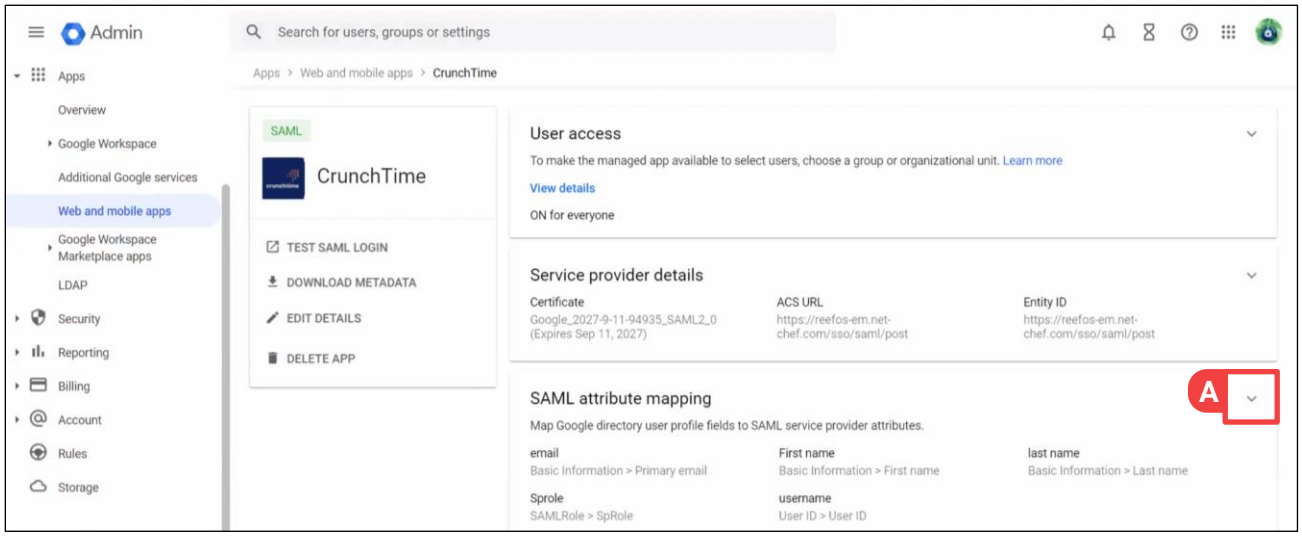
(Continued)

© 2026 Crunchtime - All Rights Reserved

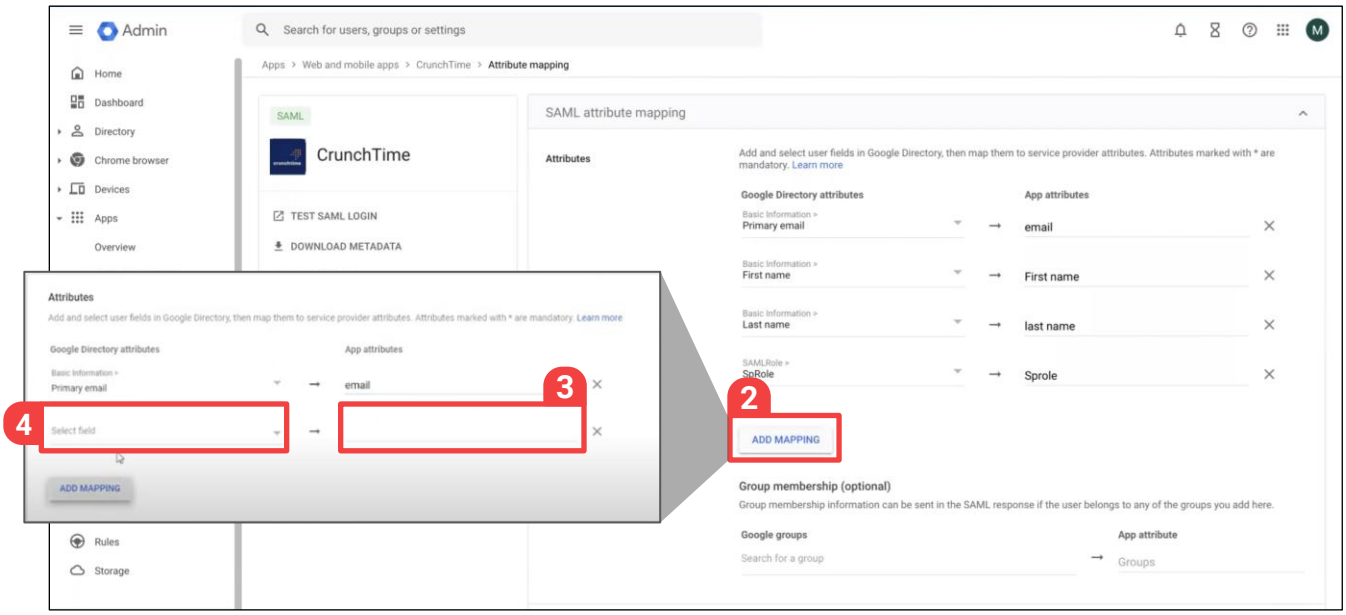
Customer Tasks

(Continued)

Google Directory Configuration



1. Under the *SAML attribute mapping* section, select the **V** (Expand) icon.



2. In the expanded section, select *Add Mapping*.
3. In the *App attributes* field, enter ‘username’ in all lower case.
4. In the *Google Directory attributes* field, select the attribute that matches the User ID in CES.

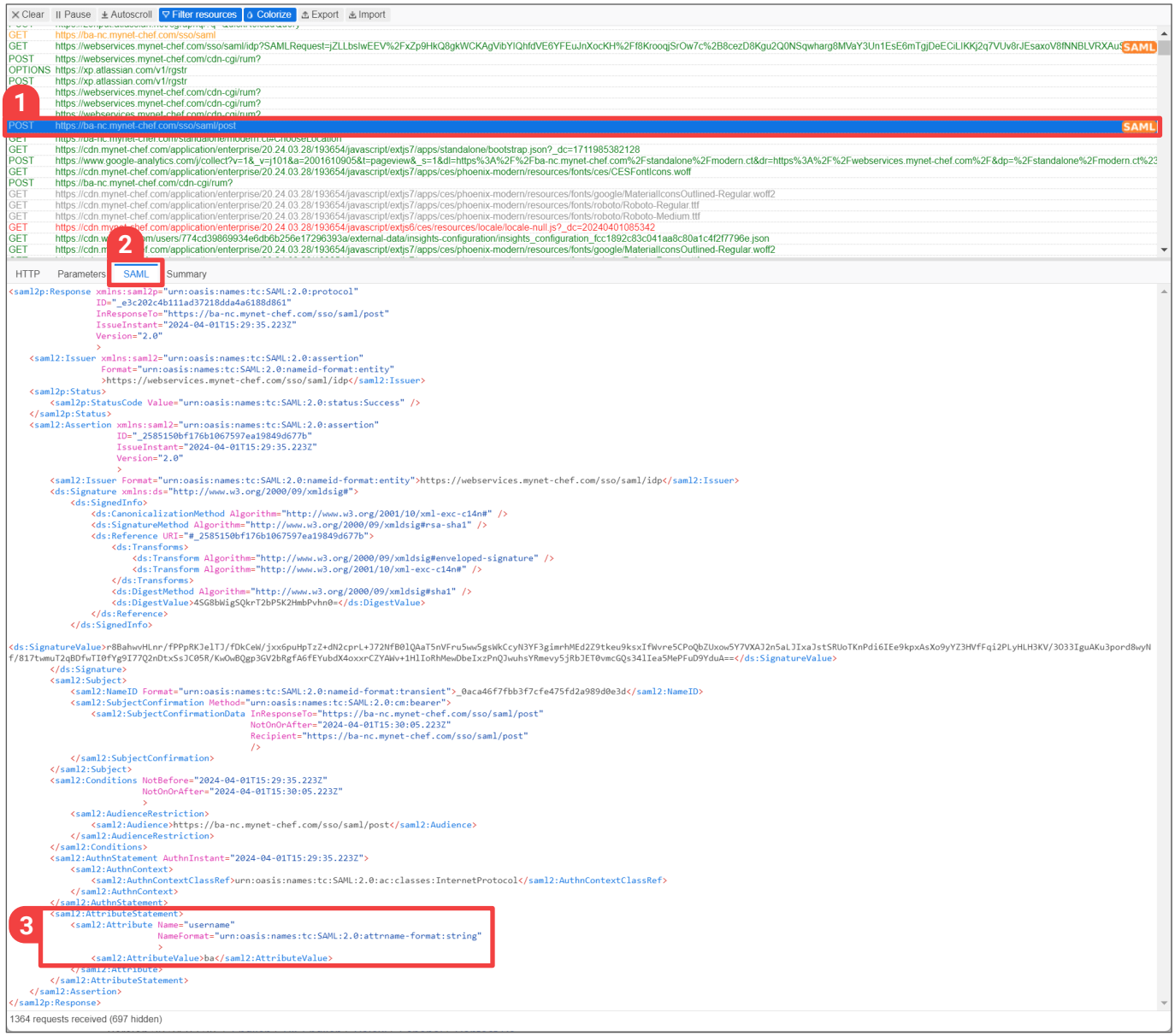
(Continued)

© 2026 Crunchtime - All Rights Reserved

Customer Tasks

(Continued)

If you need troubleshoot your “username” attribute, use the SamlTracer browser extension to view and verify that the attribute is sent with the desired values.



1. In the tracer screen, locate the *Post* query for your Net-Chef instance.
2. Select the *SAML* tab.
3. Find the “username” attribute in the SAML response and verify the attribute value.

© 2026 Crunchtime - All Rights Reserved