Crunchtime SSO Remote Administration and Remote Authentication

Reference Guide

Document Details

Document #: 160_SSOG_260605

Overview

This document provides an overview of how the Crunchtime Enterprise Solution (CES) defines the steps necessary to implement Crunchtime's Remote User Administration for entering and updating user information, and Remote User Authentication for allowing CES access for SAML based SSO.

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

… or scan the QR code to the left.

Related Documentation

- CT-SAML based SSO Customer Implementation Guide: https://links.crunchtime.com/SG-SSOCustomerImplGuide

© 2026 Crunchtime - All Rights Reserved

REFERENCE GUIDE

Crunchtime SSO Remote Administration and Remote Authentication

Introduction

Crunchtime has developed, and continues to enhance capabilities to streamline management of users and passwords. These capabilities fall into 3 distinct feature sets:

- Remote Administration
- Remote Authentication
- Single Sign On (SSO) using SAML Token

Definitions

For purposes of this document, Crunchtime defines these terms as follows:

Remote Administration – Application user information is maintained in a separate system (such as Active Directory) and kept in sync with CES. This can be done through an application user import or direct connection with Active Directory.

Remote Authentication – Validation of username and password through Active Directory rather than the application user record in CES. This eliminates password management in CES and simplifies password management for end users. This can be used with Remote Administration (but is not required).

Single Sign On – Management of username and password is through a portal maintained by the client. A token is passed to CES for verification. This allows a user to access Crunchtime without entering a user or password but requires infrastructure to be maintained by the client.

(Continued)

© 2026 Crunchtime - All Rights Reserved

REFERENCE GUIDE

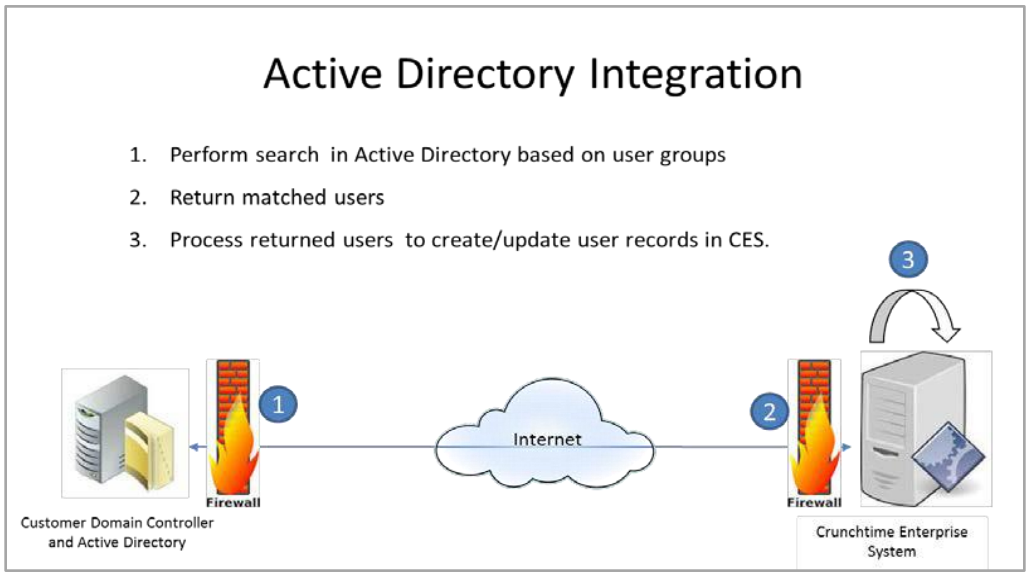
Crunchtime SSO Remote Administration and Remote Authentication

Remote Administration

When implemented, Crunchtime's Remote Administration allows user information to be created and maintained in one system and pushed into the CES. This can be done one of two ways:

1. Use the Application User file format to create and update user information via the Crunchtime Data Pump (CDP). This requires the client to generate a file in the correct format, but could potentially work with any external user management system.
2. Sync CT application users with Active Directory. The following diagram illustrates this process.

Responsibilities when Implementing Active Directory Integration



Crunchtime IT Department

- Provide a block of IP address of CT servers to customer IT for AD interaction.
- Configuration of CES application based on client's AD setup.

Client IT

- Expose AD to CT Server IP block via LDAPS protocol.
- Create an account in AD for the integration function, with sufficient permissions.
- Perform AD configurations per documentation, and communicate to CT IT.

Client Admin

- Create mapping between CES locations and client AD locations in CES UI.
- Create mapping between CES user groups and client AD groups in CES UI.

These mapping processes are described more fully in the following sections.

(Continued)

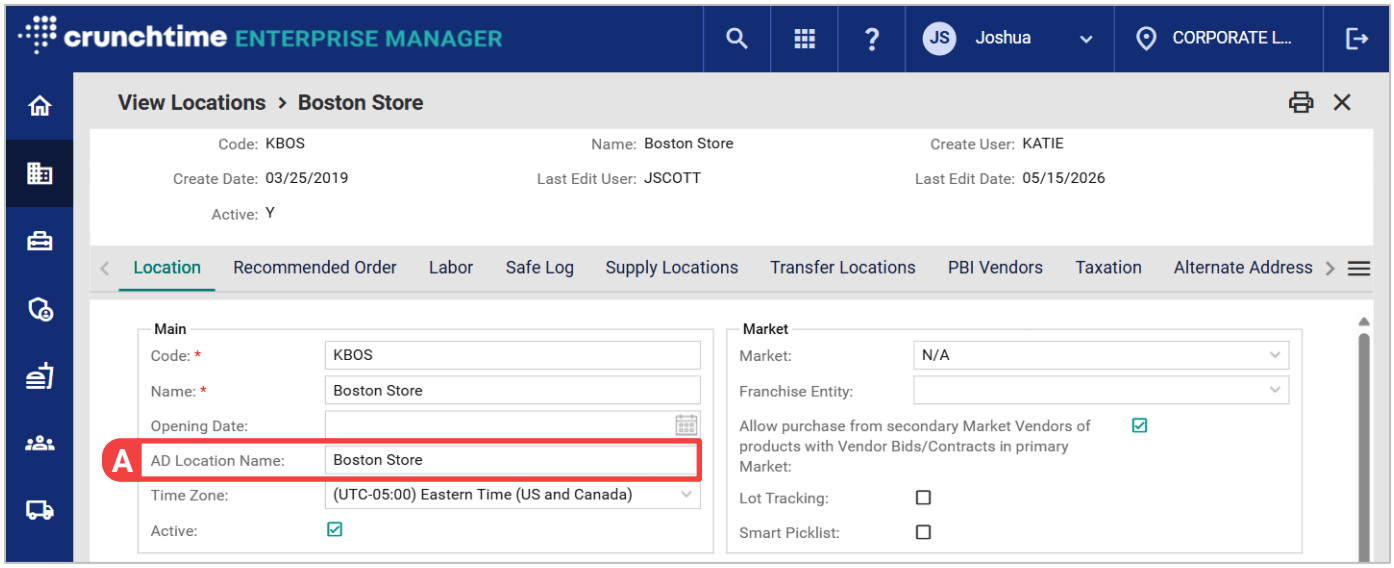
Crunchtime SSO Remote Administration and Remote Authentication

Remote Administration (Continued)

Mapping Between CES Locations and AD Locations in CES

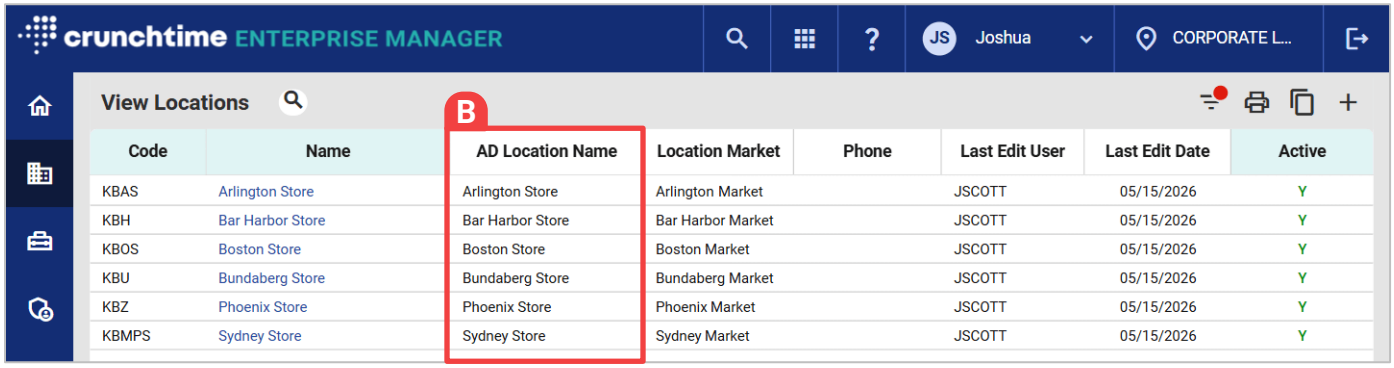
As part of integrating AD and CES, each CES location that has a counterpart in the customer's AD will have that counterpart's name entered in the CES Locations screen.

Edit the Location Details



A Enter the *AD Location Name* here.

View the Locations



B The *AD Location Name* for the location is displayed here.

(Continued)

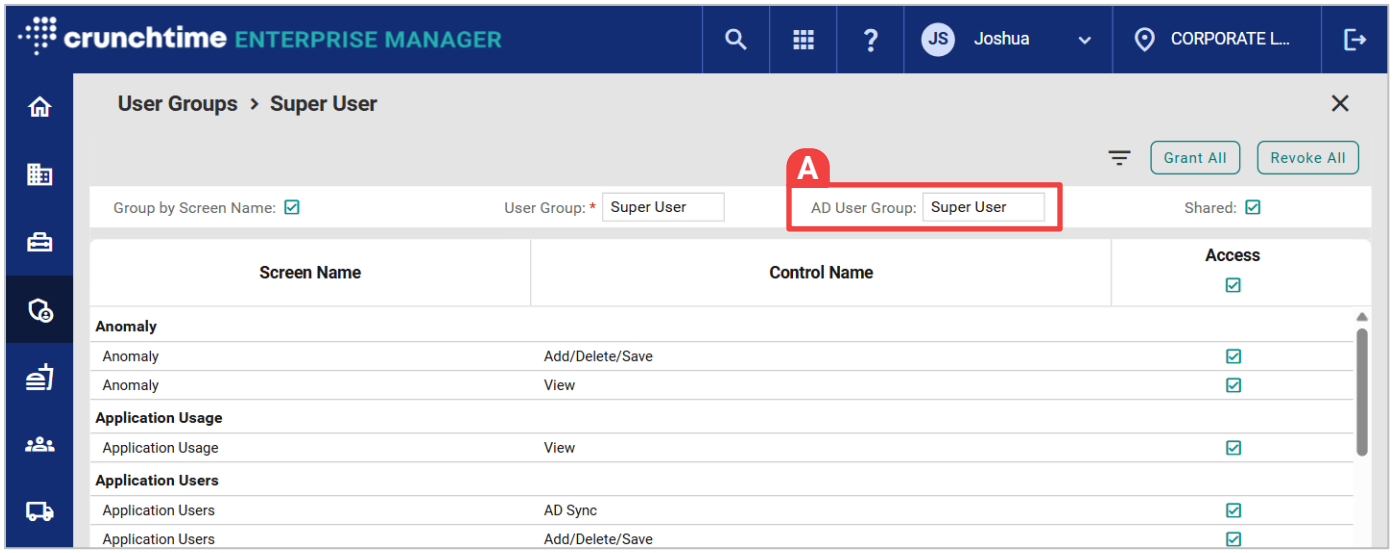
Crunchtime SSO Remote Administration and Remote Authentication

Remote Administration (Continued)

Mapping Between CES User Groups and AD User Groups in CES

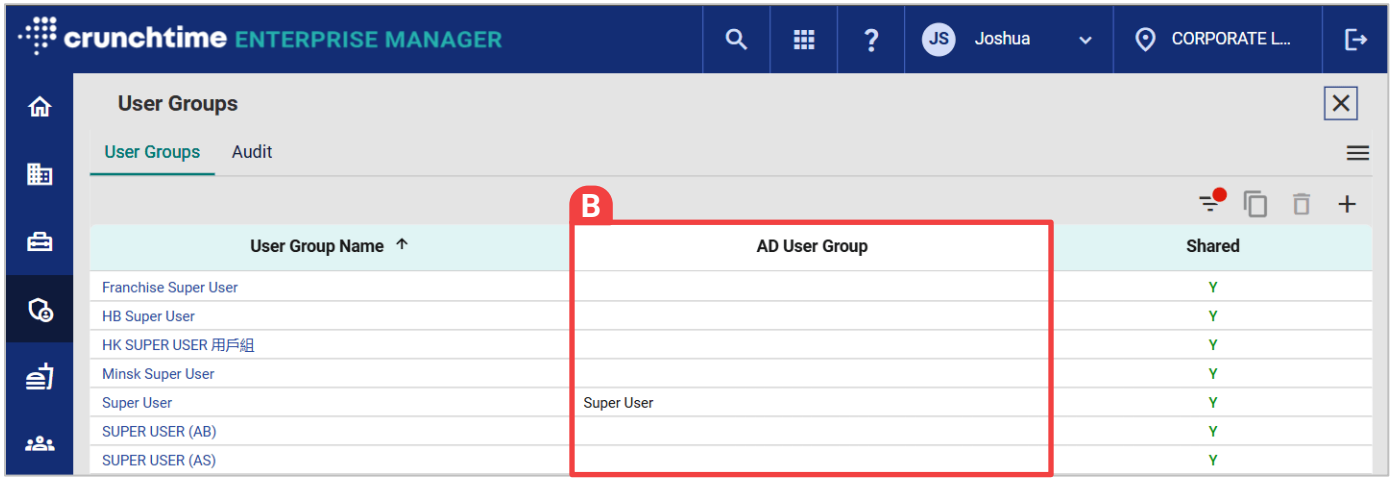
As part of integrating AD and CES, each CES User Group that has a counterpart in the customer's AD will have that counterpart's name entered in the CES User Groups screen.

Edit the User Group Details



A Enter the *AD User Group* name here.

View the User Groups



B The *AD User Group* name is displayed here.

(Continued)

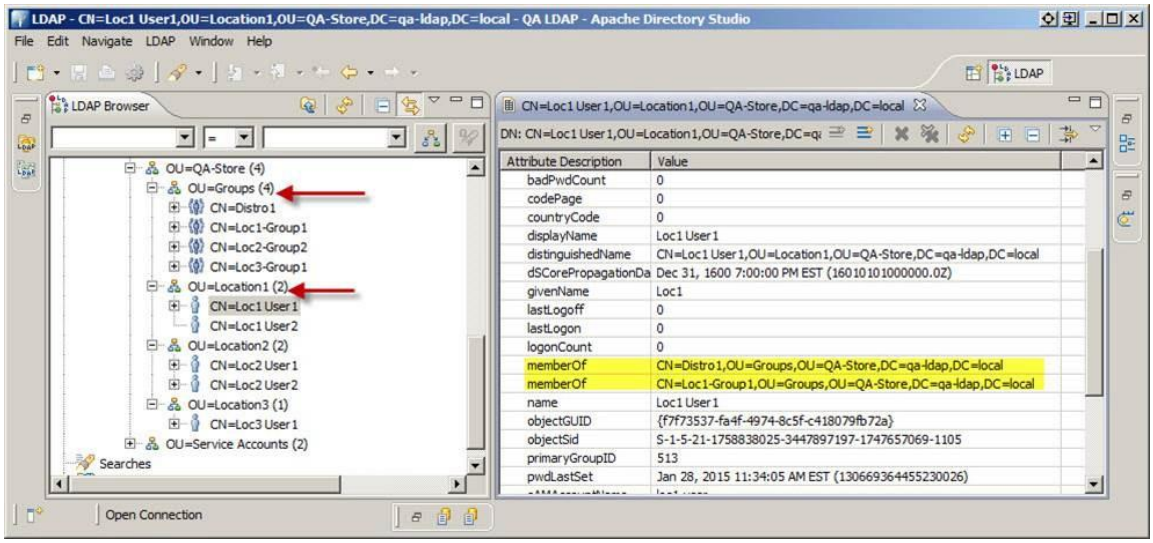
Crunchtime SSO Remote Administration and Remote Authentication

Remote Administration (Continued)

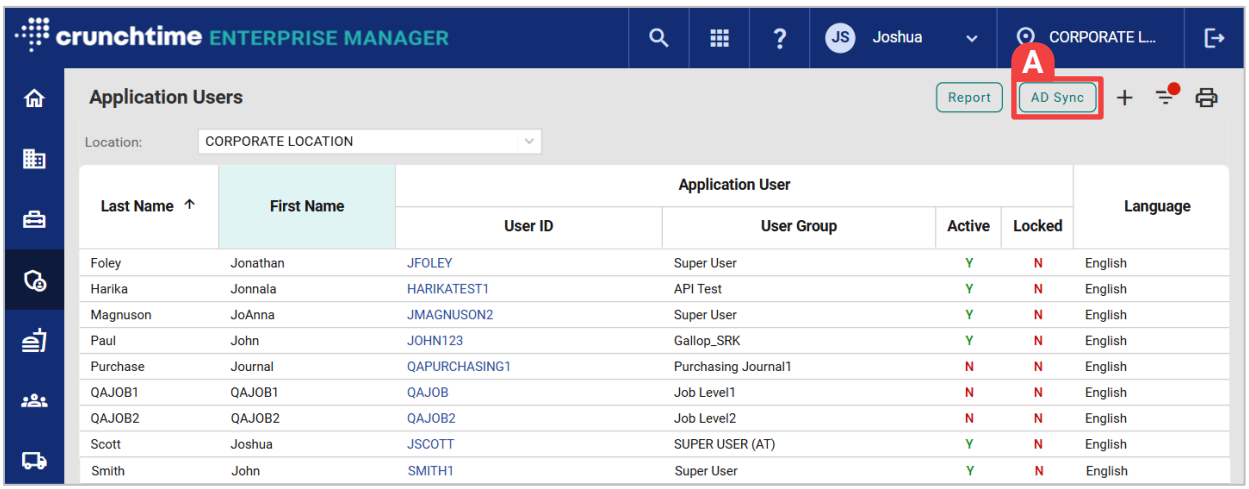
Synchronizing the CES and AD

After integration of AD and CES, a synchronization function in the CES pulls user information from AD into the CES. Synchronization between AD and CES is **based on**:

- Username is the same between AD and CES.
- A user in the remote AD will only be considered a CES user if the username is a member of an AD group that is mapped to a CT group as shown below.



- The synchronize function works with limited properties during user creation and update.



A The synch is triggered by the *AD Sync* button on the "Application Users" screen, as shown above.

(Continued)

Crunchtime SSO Remote Administration and Remote Authentication

Remote Administration (Continued)

Use Cases – Active Directory Integration

User Creation Driven by AD

When a new user is added in AD, and is a member of a mapped CT User Group, the synchronization will create this user in CT based on the following info:

- Username
- First Name
- Last Name
- Email
- User Group
- Location (optional)

Similar to the current process, a random password will be created for this user and emailed to its email address. (If the customer also uses Remote Authentication or SSO, the password step will be omitted).

User Update Driven by AD

When a user that exists in both CES and AD is updated in AD, the synchronization will apply the changes to CES. Currently the only field that will be updated is the **User Group** field.

Activation/Deactivation Driven by AD

When an active user that exists in both CES and AD is updated in AD by removing it from a mapped user group, or is deleted altogether from AD, it is marked as inactive in the CES system.

If this user is added again in AD with correctly mapped user group membership, or re-added to a mapped user group, the synchronization will mark it as active in CES.

CT-Only Users

By default, all users in CES are considered CT users. The synchronization process will not modify a CT-only user unless a link is established (finding a match based on Username and User Group) between AD and CT for that user.

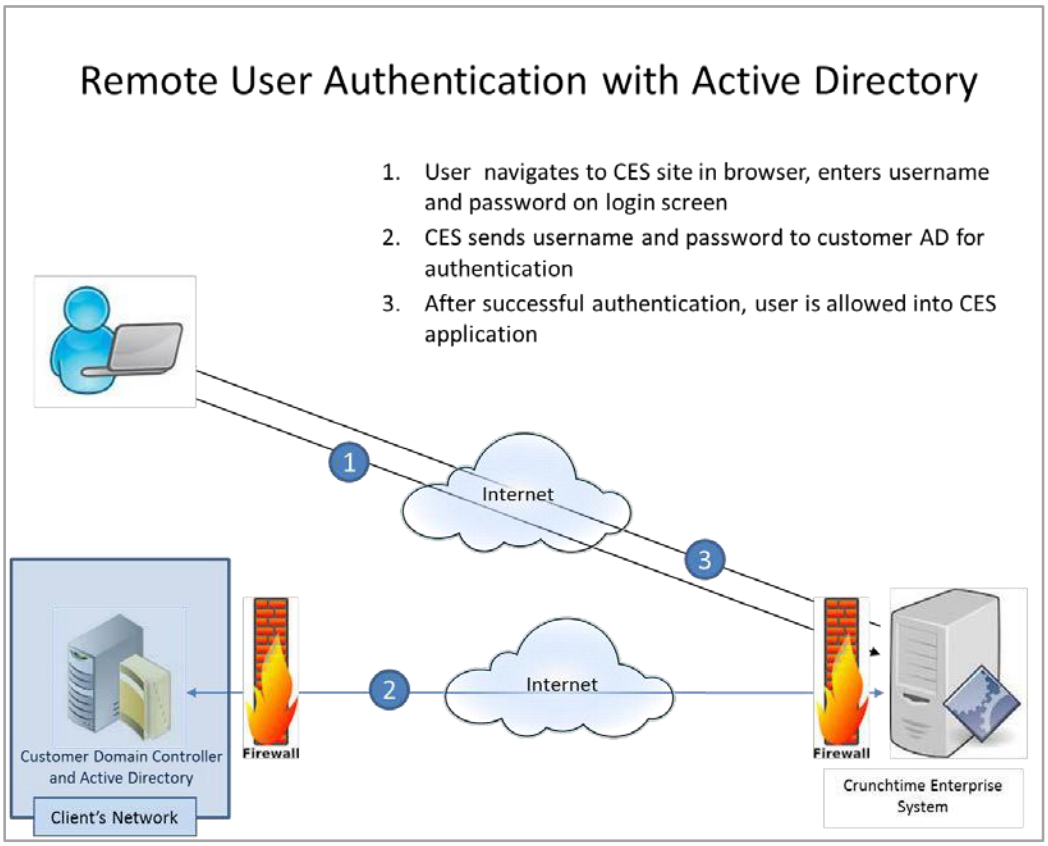
© 2026 Crunchtime - All Rights Reserved

REFERENCE GUIDE

Crunchtime SSO Remote Administration and Remote Authentication

Remote Authentication

When implemented, Crunchtime's Remote Authentication allows user access to the system after confirming their credentials via the client's Active Directory. The steps are illustrated below:



The benefits of this system are to:

- **Eliminate** password management for the CES altogether.
- **Simplify** password management for customer end-users.

User Setup and Maintenance Options

Remote User Authentication requires that each CES user is set up and maintained in both the CES, **and** in the client's Active Directory. There are two ways to do so:

1. **Manually** enter and maintain users in both systems

OR

2. Use Crunchtime's **Remote Administration** to setup and maintain user data.

(Continued)

Crunchtime SSO Remote Administration and Remote Authentication

Remote Authentication (Continued)

Responsibilities when Implementing Active Directory Integration

Crunchtime IT Department

- Provide a block of IP address of CT servers to customer IT for AD interaction.
- Configuration of CES application based on client's AD setup.

Client IT

- Expose AD to CT Server IP block via LDAPS protocol.
- Create an account in AD for the integration function, with sufficient permissions.
- Perform AD configurations per documentation, and communicate to CT IT.

Client Admin

- Create mapping between CES locations and client AD locations in CES UI.
- Create mapping between CES user groups and client AD groups in CES UI.

These mapping processes are described more fully in the *Remote Administration* section above.

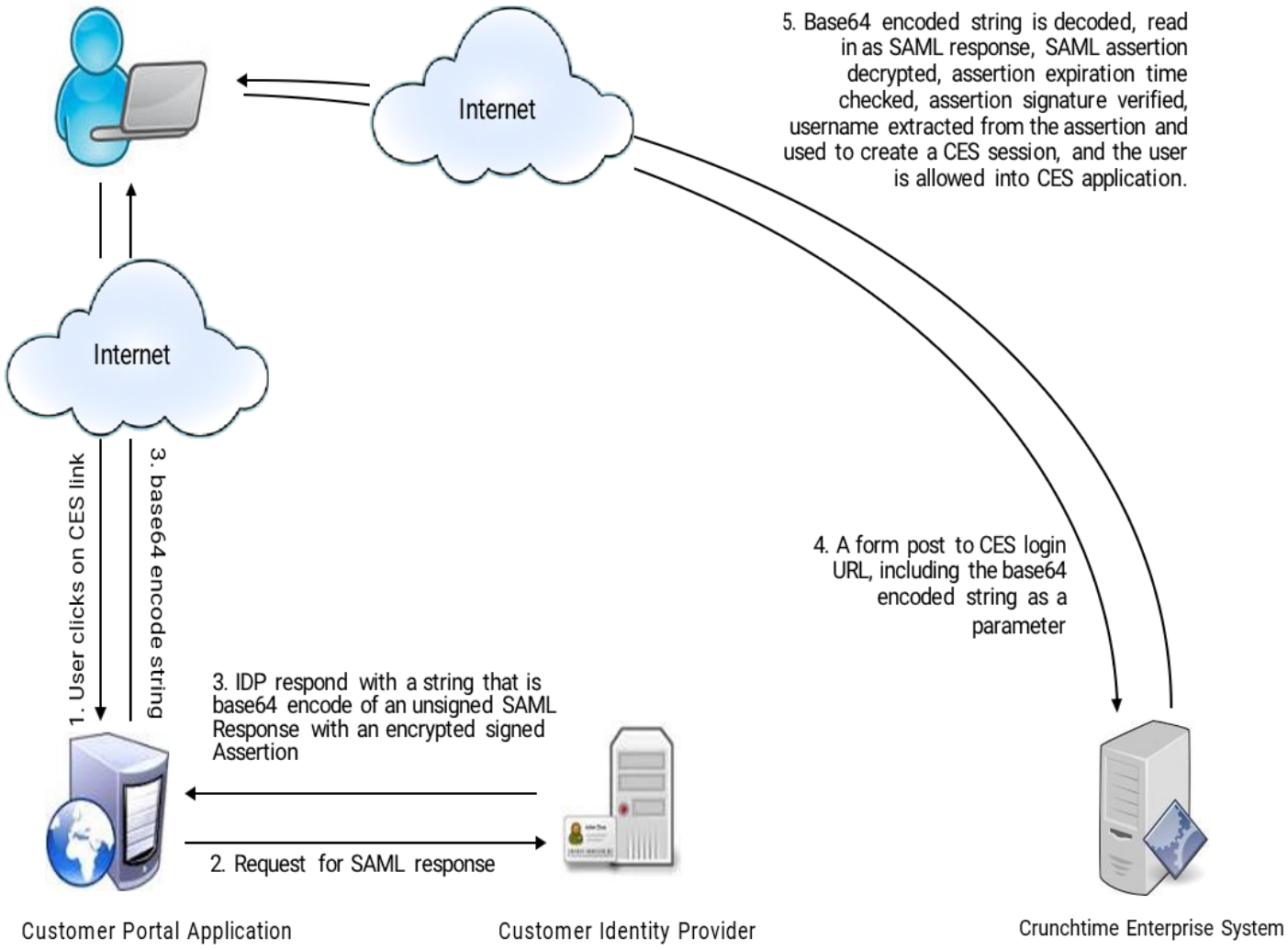
(Continued)

© 2026 Crunchtime - All Rights Reserved

Crunchtime SSO Remote Administration and Remote Authentication

Remote Authentication (Continued)

SAML-based Single Sign On Workflow



(Continued)

Crunchtime SSO Remote Administration and Remote Authentication

Customer Tasks

Create SAML Auth response based on Crunchtime specification on IDP

- The SAML assertion should contain statement for attribute named ‘username’, whose value should be the username intended for the CES system.
- The SAML assertion should be signed with Customer private key.
- The SAML assertion should be encrypted with Crunchtime public key (in the SP metadata file).
- The SAML assertion should be valid for a period of 30 seconds.
- The whole SAML response should be serialized and then Based64 encoded.

Perform a form post to CES (Crunchtime Enterprise System) from portal link

- The form action should point to CES login endpoint. Net-Chef and EM Web have two different endpoints.
- The form should include a parameter sso-login with the value `'true'`.
- The form should include a parameter sso-login-mode with the value `'saml'`.
- The form should include a parameter sso-saml-response with IDP's SAML response above as its value.

Provide IDP metadata file to Crunchtime

- CES will read in the customer IDP metadata file to obtain customer public key, which will be used to validate signature on assertion.

Further details are available in the CT-SAML based SSO Customer Implementation Guide, found here: https://links.crunchtime.com/SG-SSOCustomerImplGuide

© 2026 Crunchtime - All Rights Reserved