

Single Sign-On March 2024

Table of Contents

[Single Sign-On Overview 1](#_Toc162022957)

[Single Sign-On (SSO) Configurations 2](#_Toc162022958)

[Passwords and Users with Single Sign-On (SSO) 4](#_Toc162022959)

[SSO Integrations 5](#_Toc162022960)

[ADP Workforce Now (WFN) Single Sign-On (SSO) 6](#_Toc162022961)

[Cisco Webex Meetings SSO 7](#_Toc162022962)

[Google OAuth Inbound SSO 10](#_Toc162022963)

[InCommon SSO 12](#_Toc162022964)

[Microsoft Azure Active Directory (AD) One-Click Single Sign-On (SSO) 13](#_Toc162022965)

[UKG Pro™ Single Sign-on to Cornerstone 14](#_Toc162022966)

Single Sign-On Overview

Single Sign-On (SSO) Configurations

The SSO Configurations page enables administrators to upgrade and revert SSO certificates. Administrators can also download an existing SSO certificate.

Administrators are not able to add or edit SSO configurations.

To access the SSO Configurations page, go to Admin > Tools > Edge > Single Sign-On.

Permissions

|  |  |  |
| --- | --- | --- |
| PERMISSION NAME | PERMISSION DESCRIPTION | CATEGORY |

|  |  |  |
| --- | --- | --- |
| Single Sign On - CSOD Certificate | Grants ability to view, manage, and upgrade SSO certificates and configurations. This is an administrator permission. This permission cannot be constrained. | Core Administration |



Upgrade SSO Certificate

To comply with security requirements, Cornerstone is required to upgrade their SSO certificate for all inbound or outbound SSOs using the SHA256 CA-Verified Cert Signature. When a new version of a certificate is available, the certificate will be automatically upgraded on a specific date. Users who are in the system administrator role receive system-generated reminder emails prior to the SSO certificate auto-upgrade date. This reminder does not need to be configured by an administrator and is automatically sent at predefined intervals of 90, 60, 30, 15, 10, 7, 6, 5, 4, 3, 2, and 1 days before the auto-renewal date. The email is active for all portals, localized to the user's language, and will ignore dead box settings to ensure delivery to the intended recipient. If a portal has no SSO connectors that need upgrading, or if they have already been upgraded, then the email is not sent.

Administrators may upgrade the certificate using self-service, which they can upgrade at the same time they upgrade the certificate in their SSO configuration. This removes any need to coordinate with Cornerstone and allows organizations the flexibility to upgrade their certificate whenever they are ready.

To upgrade an existing SSO certificate, select the appropriate SSO connector. Then, select the Upgrade Now button. This button is only available if the selected connector has an upgrade available (i.e., the connector is not currently using the latest version of the certificate).

Revert SSO Certificate

To revert to a previous version of an existing SSO certificate, select the appropriate SSO connector. Then, select the Revert Now button. This button is only available if the connector is using the latest version of the certificate, and the older version of the certificate has not expired. If the older version of the certificate has expired, then this button is not available.

Download SSO Certificate

To download and view the SSO certificate for the existing connector, select the appropriate connector. Then, select the three-dot menu icon and select CSOD Public Certificate.

Note: This option is not available when viewing this page in a smaller mobile browser window.

Download Metadata for SSO Configuration

To download the metadata for a saved inbound or outbound SAML 2.0 Single Sign-On configuration, select the appropriate connector. Then, select the three-dot menu icon and select Metadata. This generates XML file tailored to the SSO configuration.

Passwords and Users with Single Sign-On (SSO)

SSO relies on a security key, rather than a password. For new users with SSO, the initial login process does not require a password.

Changes to a user's password do not impact their ability to SSO into the system. There is no security issue around users with SSO resetting their passwords.

SSO users do see the Change Password link within My Account. Although this may cause initial confusion, any password changes made by SSO users do not impact their ability to SSO into the system. Additionally, users must know their current password in order to successfully change it.

See Password Preferences for additional information.

SSO Integrations

ADP Workforce Now (WFN) Single Sign-On (SSO)

The ADP Workforce Now Single Sign-On integration is available from the Edge Marketplace. This enables organizations to quickly purchase, configure, and enable the integration.

Note: Organizations that have already implemented SSO from ADP to Cornerstone do not need to purchase and enable this integration.

Configuration

When configuring the integration, enter the following information:

* ADP Client ID

Implementation

The ADP Workforce Now Single Sign-On integration is available to try or to purchase via the Edge Marketplace. To access the Edge Marketplace, go to Admin > Tools > Edge > Marketplace.

This integration is available to all organizations. Organizations must have an existing ADP Workforce Now contract. Organizations that have an existing SSO integration from ADP to Cornerstone do not need to install this integration or migrate.

Security

The following existing permissions apply to this functionality:

|  |  |  |
| --- | --- | --- |
| PERMISSION NAME | PERMISSION DESCRIPTION | CATEGORY |

|  |  |  |
| --- | --- | --- |
| Edge Integrations - Manage | Grants access to the Integrations service for Edge Integrate, where the administrator can configure, enable, and disable their third-party integrations used within the Cornerstone system. This permission cannot be constrained. This is an administrator permission. | Edge |

|  |  |  |
| --- | --- | --- |
| Edge Marketplace - Manage | Grants access to the Marketplace service for Edge Integrate, where the administrator can browse integrations that can be used to extend the Cornerstone system. This permission cannot be constrained. This is an administrator permission. | Edge |

Cisco Webex Meetings SSO

The Cisco Webex integration enables organizations to utilize the Webex Single Sign On (SSO) functionality. When Webex SSO is enabled, Webex instructors are not required to enter their passwords when creating and launching meetings.

This integration includes Webex SSO Partner Delegated Authentication (PDA), which enables organizations to use their own SSO provider or have no SSO provider for their Webex portal.

Considerations

Organizations can use SSO for the Webex Administrator account. However, it is NOT supported to enable MFA (Multi-Factor-Authentication) in Webex for this account.

The Webex SSO (PDA) functionality only follows the "Launch Meeting as Instructor" workflow and does not support the creation of meetings or instructors.

Migration is not supported for this functionality. Webex SSO (PDA) only works for sessions that are created after the configuration. Sessions created prior to SSO (PDA) setup still require the integration to use instructor passwords.

Webex only allows one SAML certificate to authenticate users. This means that if SSO is set up between Cornerstone and Webex, the organization can only access Webex via the Cornerstone system. In this scenario, the organization cannot use SSO from multiple platforms into the same Webex account.

Implementation

* This functionality is disabled by default. Contact Global Customer Support to enable via a Billable Work Order across environments.
* Prior to enabling Webex SSO within the Cornerstone portal, organizations must request SSO from Webex and have the SAML metadata imported to their Webex support site.

Content

The following information is available within the this folder. Click a link to navigate directly to the appropriate topic:

Webex SSO: Webex Support Site

Prior to enabling Webex SSO within the Cornerstone portal, organizations must request SSO from Webex.

After SSO is enabled by Webex, organizations must have the SAML metadata imported to their Webex support site. This can be done via the SSO Configuration page within the Webex support site.





Webex SSO: Instructor Passwords

When Webex SSO is enabled, Webex instructor passwords are no longer necessary. Because of this, they are no longer stored within the Cornerstone portal.

When viewing the Instructor Details pop-up for a Webex instructor, the pop-up does not display password information if Webex SSO is enabled.



Google OAuth Inbound SSO

The Google OAuth Inbound SSO (Single Sign-on) connection is available to customers for a seamless user login experience to their Cornerstone CSX portal. This self-configurable connection is available in the user interface under the Single Sign-On menu in Edge.

This integration includes the following features:

* Hassle-free login experience
* Supports deep link feature
* User-friendly configuration
* Default or customizable Error, Timeout, and Logout URLs

How Does this Enhancement Benefit My Organization?

This feature provides a self-service plug-and-play SSO connection with less maintenance.

Implementation

There is a two-step process to purchase this functionality:

1. Purchase from Google Marketplace. This requires contacting Google directly to purchase, install, and configure with Google.
2. Contact your Account Manager to purchase the service.

After purchase, the service can be self-activated via Edge (Admin > Tools > Edge > Single Sign On). Select the new oAuth option and click “Add” to get to the setup screen. The setup requires Client ID and Client Secret parameters from Google. This connection does not support E-signature and mobile app connectivity.

Field Configuration Details - General Properties

| Field name | Field Description | Required? |
| --- | --- | --- |
| SSO ID  | Pre-filled with the next available OUID on the portal. This can be updated to another available value.  | Yes |
| Client ID  | Provided by Google  | Yes |
| Client Secret  | Provided by Google  | Yes |
| Error URL  | The Cornerstone error URL (common/ssoerror.aspx) is configured by default. A custom URL is also accepted. |  If left blank, this defaults to the Cornerstone URL. |
| Logout URL  | The Cornerstone logout URL (common/ssologout.htm) is configured by default. A custom URL is also accepted. |  If left blank, this defaults to the Cornerstone URL. |
| Timeout URL  | The Cornerstone timeout URL (common/ssotimeout.htm) is configured by default. A custom URL is also accepted. |  If left blank, this defaults to the Cornerstone URL. |
| Skew (seconds) | The default value is -10, and the maximum value is -20. | Yes |

Field Configuration Details - Contacts

| Field name | Field Description | Required? |
| --- | --- | --- |
| Name  | Update the customer’s Technical and System Administrator name. | Yes |
| Email  | Update the customer’s Technical and System Administrator email address. | Yes |

InCommon SSO

InCommon provides a secure and privacy-preserving trust fabric for research and higher education organizations and their partners in the United States. This new service allows for a seamless Single Sign On (SSO) integration with higher-ed clients. Organizations need to exchange the Entity ID in InCommon, and the metadata is imported directly for SSO setup. Certificate management for SSO automatically picks up changes when they are published by InCommon Federation.

Implementation

To enable this functionality via a paid technical project, contact Global Customer Support.

Microsoft Azure Active Directory (AD) One-Click Single Sign-On (SSO)

With this single sign-on integration, the one-click functionality provides customers with a quick and simplified process to configure and enable the integration in both Cornerstone and Azure AD with minimal manual effort.

The following features are supported:

* Deep Link
* Mobile SSO

How Does this Enhancement Benefit My Organization?

This integration provides uni-directional single sign-on from Microsoft Azure Active Directory to Cornerstone. Once implemented, Cornerstone customers that use Azure Active Directory for their identity and access management service will be able to single sign-on from Azure to their Cornerstone portal, eliminating the need to enter their Cornerstone credentials.

Implementation

This integration is available for self-activation in Edge Marketplace via the Microsoft Azure Active Directory One-Click Single-Sign-on integration tile. This integration is for Cornerstone customers that use Microsoft Azure Active Directory for their identity and access management service.

Permissions

The following existing permissions apply to this functionality:

|  |  |  |
| --- | --- | --- |
| PERMISSION NAME | PERMISSION DESCRIPTION | CATEGORY |

|  |  |  |
| --- | --- | --- |
| Edge Integrations - Manage | Grants access to the Integrations service for Edge Integrate, where the administrator can configure, enable, and disable their third-party integrations used within the Cornerstone system. This permission cannot be constrained. This is an administrator permission. | Edge |

|  |  |  |
| --- | --- | --- |
| Edge Marketplace - Manage | Grants access to the Marketplace service for Edge Integrate, where the administrator can browse integrations that can be used to extend the Cornerstone system. This permission cannot be constrained. This is an administrator permission. | Edge |

UKG Pro™ Single Sign-on to Cornerstone

The UKG Pro™ Single Sign-on to Cornerstone integration allows organizations to provide a seamless experience to their employees via Single Sign-on (SSO). Simply set up an outbound data feed from UKG to Cornerstone or the UKG Pro™ User & OU Data Inbound Integration and enable this integration to allow your employees to log in to Cornerstone from UKG.

Integration Settings

When configuring the UKG Pro™ Single Sign-on to Cornerstone integration, organizations must provide their UKG Pro™ Client ID. This value can be obtained by contacting the Ultimate Software Account Manager.

Implementation

The UKG Pro™ Single Sign-on to Cornerstone integration is available to try or to purchase via the Edge Marketplace. To access the Edge Marketplace, go to Admin > Tools > Edge > Marketplace.

This integration is available to all organizations. Organizations must have an existing UKG Pro™ contract. Organizations that have an existing SSO integration from UKG Pro™ to Cornerstone do not need to install this integration or migrate.

Security

The following existing permissions apply to this functionality:

|  |  |  |
| --- | --- | --- |
| PERMISSION NAME | PERMISSION DESCRIPTION | CATEGORY |

|  |  |  |
| --- | --- | --- |
| Edge Integrations - Manage | Grants access to the Integrations service for Edge Integrate, where the administrator can configure, enable, and disable their third-party integrations used within the Cornerstone system. This permission cannot be constrained. This is an administrator permission. | Edge |

|  |  |  |
| --- | --- | --- |
| Edge Marketplace - Manage | Grants access to the Marketplace service for Edge Integrate, where the administrator can browse integrations that can be used to extend the Cornerstone system. This permission cannot be constrained. This is an administrator permission. | Edge |