insightsoftware

CERTENT CDM Site Administration Guide

CDM Site Administration Overview

Site Administration in Certent 365 is designed for users responsible for the administration of the CDM application.

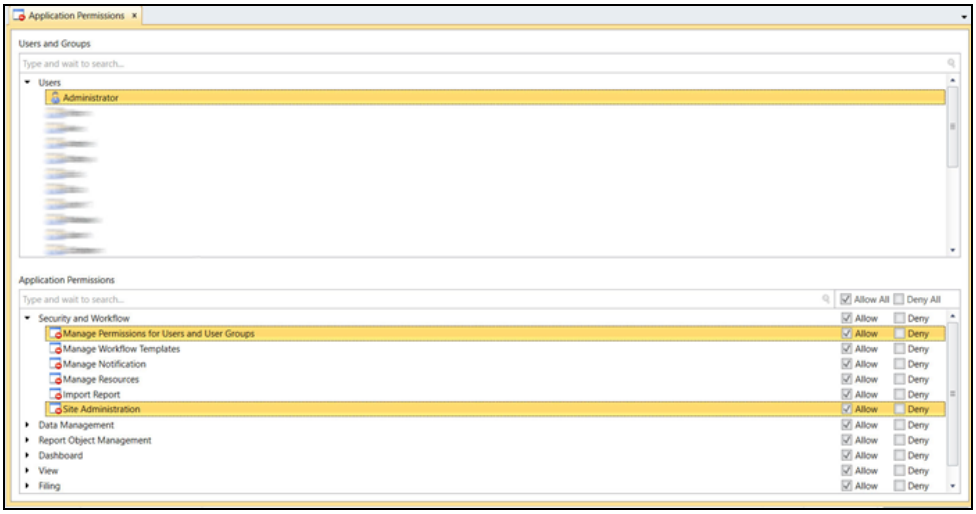
Required Permissions

In order to access Site Administration, you should have the following application permission allowed:

Application Permissions > **Security and Workflow** > **Site Administration**.

To set up single sign-on/modern authentication for users, you should also have the following application permission allowed:

Application Permissions > **Security and Workflow** > **Manage Permissions for Users and Groups**.

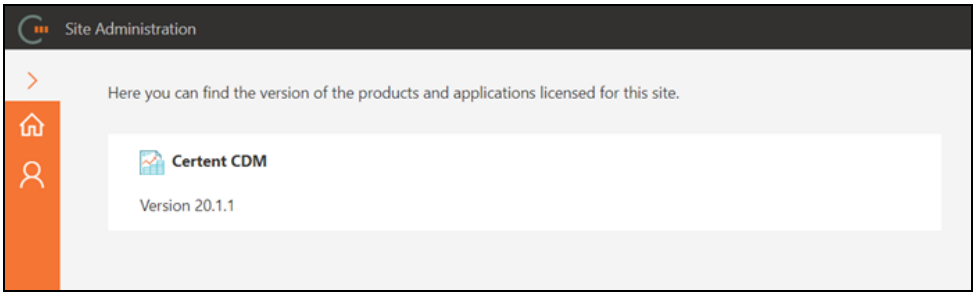


Access the Site Administration Page

You can use either of the following methods to open the Site Administration page:

- In Certent 365, click the waffle icon on the menu bar, then select **Site Administration**.
- Visit the page directly: `{PathToCDMServer}/Web/SiteAdministration`.

The main page displays the version of the CDM desktop client. Other information may be shown regarding other CDM applications in use by your organization.



Single Sign-On Configuration

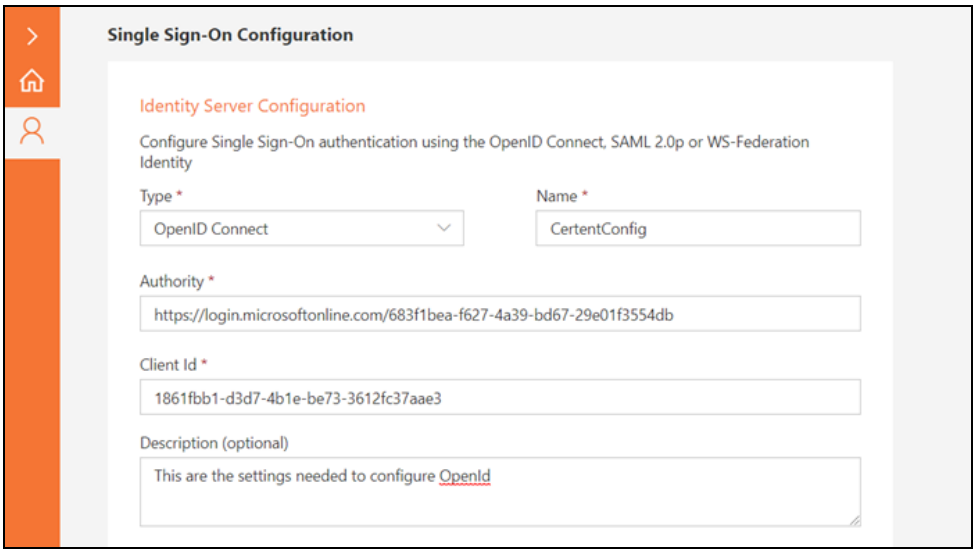
Through the Single Sign-On Configuration page, you can configure the authentication method for the organization. To do this, add the corresponding settings for your chosen protocol.

Common Settings

Type - The preferred protocol.

Name - The desired custom name for this configuration.

Description (optional) - The desired additional description for this configuration.



After adding all the required (*) information, when the administrator clicks **Save**, the system returns the Redirect URL that needs to be inserted in the Azure AD application settings.

Specific Settings for OpenID Connect

Authority - The URL address of your Identity Provider.

Client Id - The Client ID to identify your organization.

For example:

- Authority: `https://login.microsoftonline.com/683f1bea-f627-4a39-bd67-29e01f3554db`
- Client Id: `1861fbb1-d3d7-4b1e-be73-3612fc37aae3`

Specific Settings for WS FEDERATION

Metadata Address - The WS-Federation metadata URL of the AD server. Commonly ending with the path:/FederationMetadata/2007-06/FederationMetadata.xml.

Wtrealm - The AD FS relying party identifier.

For example:

- Metadata Address: `https://adfs.certent.com/FederationMetadata/2007-06/FederationMetadata.xml`
- Wtrealm: `https://portal.certent.com/`

Specific Settings for SAML2.0

SAML Application Id - The Client ID to identify your organization.

SAML IdpAddress - The OWIN authentication middleware type. Specify the value of the entityID attribute at the root of the federation metadata XML.

SAML Metadata Address - The WS-Federation metadata URL of the AD FS (STS) server. It typically ends with the path:/FederationMetadata/2007-06/FederationMetadata.xml.

For example:

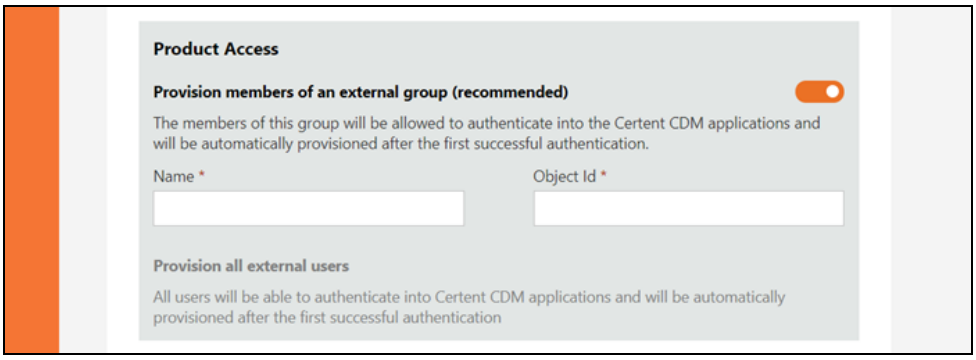
- SAML Application Id: `spn:71cba3e0-1fd6-464d-a032-7d3d982205fe`
- SAML IdpAddress: `https://sts.windows.net/683f1bea-f627-4a39-bd67-29e01f3554db/`
- SAML Metadata Address: `https://login.microsoftonline.com/683f1bea-f627-4a39-bd67-29e01f3554db/federationmetadata/2007-06/federationmetadata.xml`

You can optionally upload your own certificate. To do this, in the **SAML 2.0 Certificate** field, click **Upload**.

Redirect URL

The Single Sign-On Configuration page also indicates the Redirect URL that must be used by an organization's IT engineer to set up the Identity Provider authentication application for CDM.

Product Access



Just-in-time provisioning is a native feature of the CDM Access Management with Single Sign-On offering. Just-in-time provisioning allows for automatic provisioning of CDM App users from the Identity Provider(s) associated with an organization.

When configuring the authentication, you can choose from two options:

- Provision members of an external group
- Provision all external users