insightsoftware

CERTENT CDM Modern Authentication Guide

CDM Identity Providers

CDM provides a modern authentication experience, as well as adding support for the OpenID Connect, SAML 2.0, and WS-Federation protocols (CDM Identity Providers). CDM authentication is integrated with Identity Providers that support authentication flows using the previously named protocols, in effect: Microsoft Azure AD, Microsoft AD FS, IBM ID, and so on.

Certified Identity Providers and Protocols

Provider	Protocols
Azure AD	OpenID Connect, SAML2.0, AD FS
OKTA	OpenID Connect
IBM ID	OpenID Connect

Certent's default and preferred protocol is OpenID Connect for all providers.

While these protocols are standard, each provider has options for implementations. As such, Certent cannot guarantee all provider/protocol combinations will work. For providers or protocols not identified here, you can still attempt to connect and have success. However, if you are unsuccessful, contact Certent to assess the viability of certifying that provider/protocol with you.

Classic CDM AD/LDAP Authentication Import Sources

The classic CDM AD/LDAP Authentication Import Sources (CDM Authentication Import Sources) are seamlessly supported after upgrading to CDM 19.12.1.

At any time, a CDM application owner can choose to convert a CDM AD/LDAP Authentication Import Source to a modern CDM Identity Provider. Once that happens, the CDM users will authenticate through the familiar corporate authentication form. For a detailed procedure on how to achieve this, contact Certent CDM Support.

Classic CDM IBM Cognos Access Manager and IBM ID Authentication Import Sources

The classic CDM IBM Cognos Access Manager (CAM) and IBM ID Authentication Import Sources are no longer supported.

- Before upgrading to CDM 19.12.1, CDM users must be temporarily converted to native CDM users.
- After upgrading to CDM 19.12.1, CDM authentication can be integrated with IBM ID using OpenID Connect or the underlying Identity Provider using the appropriate protocol. Direct integration with IBM CAM is no longer supported.

Once configured, users will authenticate using the familiar IBM CAM or IBM ID authentication form.

Authentication Flow

Users are guided through the same authentication forms, regardless of whether they are authenticating to the CDM desktop client or a CDM web application.

User Identification

The account is identified by introducing the username or the email address associated to the CDM account.

The browser will typically offer auto-complete options when returning to the CDM desktop client or the CDM web applications.

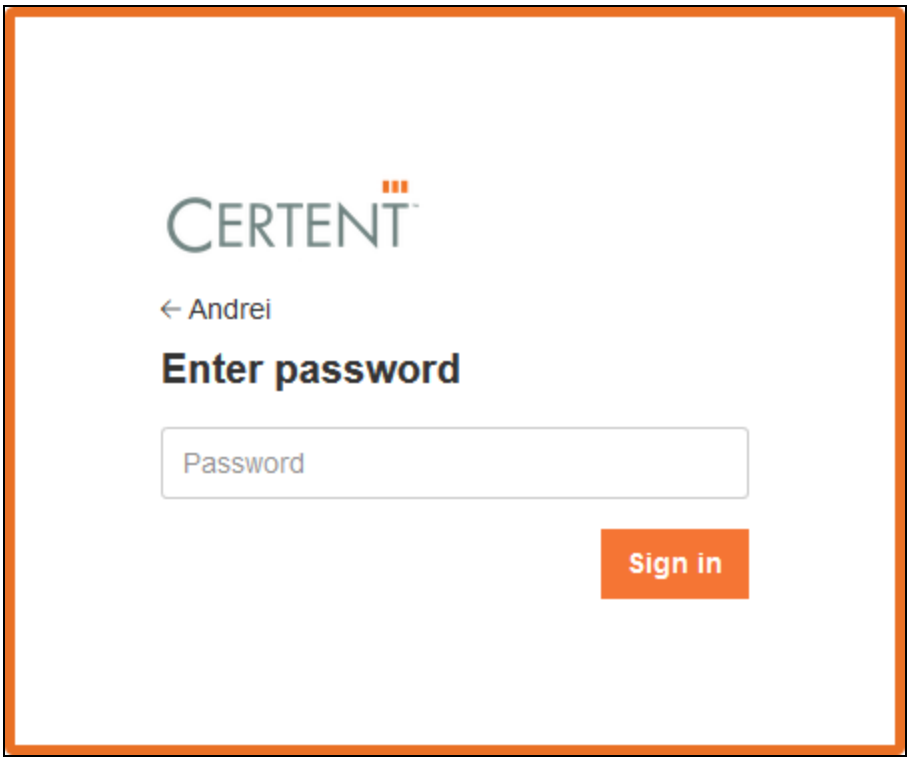
For AD/LDAP accounts, users are no longer required to select the import source (domain). The domain is automatically identified.

User Password

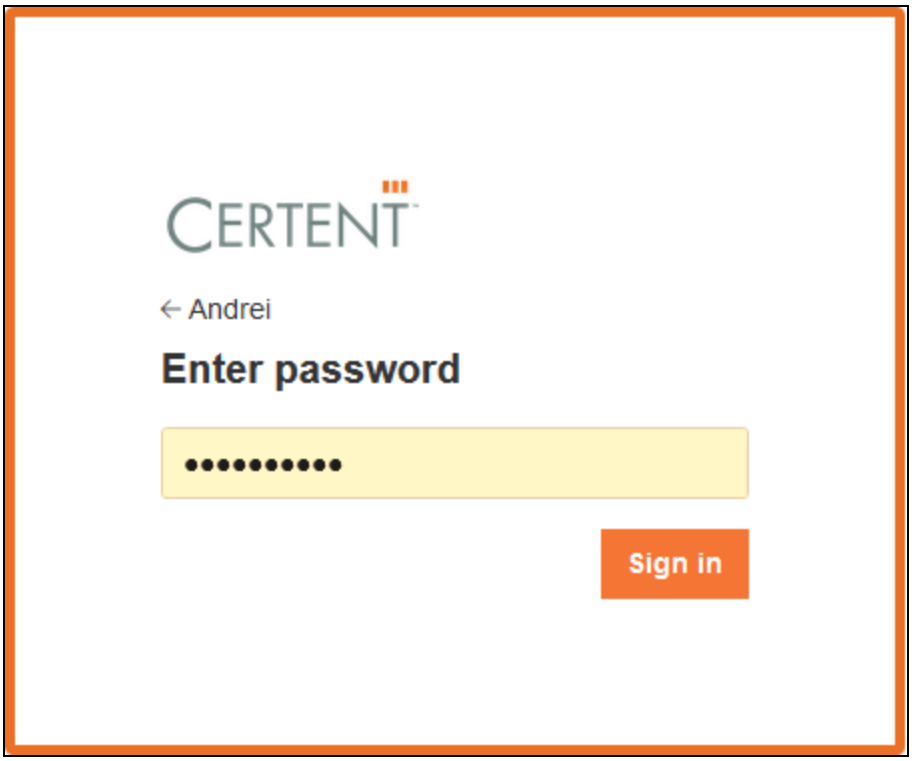
After introducing the username or email address, users are redirected to the appropriate password step depending on the account type.

CDM Native Users and CDM AD/LDAP Import Source Users

For CDM native or AD/LDAP accounts, users are shown the CDM password form.

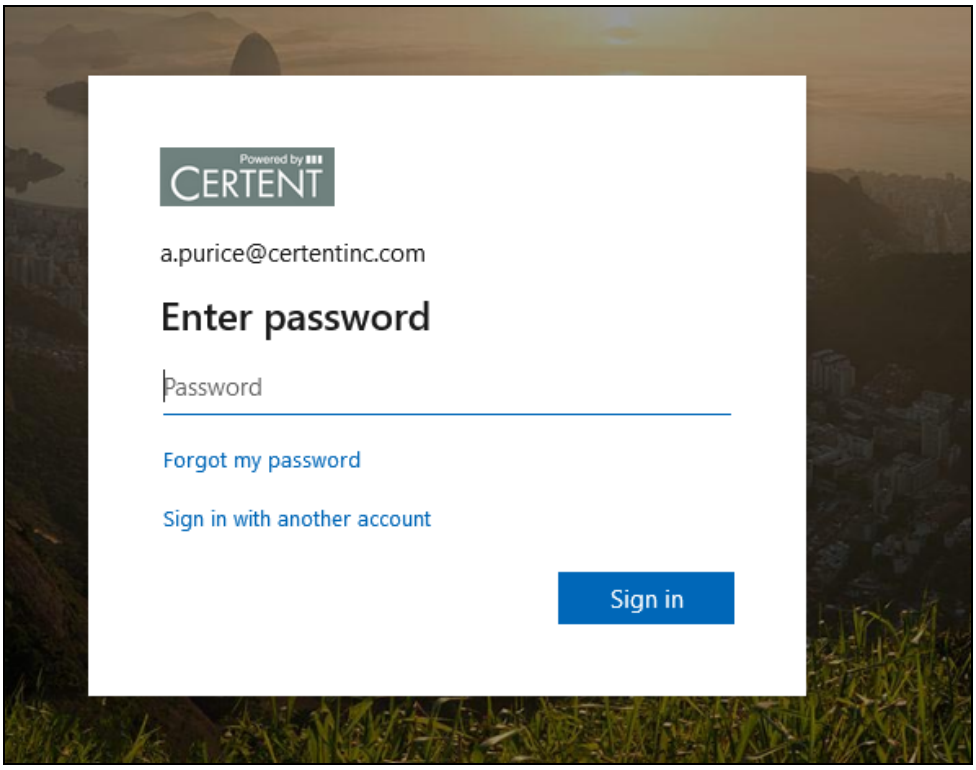


If the username or email address is not entered correctly, the user can go back and correct it. Credentials can now be saved to the browser passwords and, when doing so, the password step will auto-complete the password.



External Identity Provider Accounts

For accounts imported from an OpenID Connect, SAML 2.0p, or WS-Federation Identity Provider, CDM will redirect the user to the familiar corporate authentication form.



After a successful authentication, the user is redirected to the CDM desktop client or the CDM web application that initiated the authentication operation.

Multi Factor Authentication (MFA) is supported, and CDM does not limit the MFA configuration options.

No Password Authentication

When the security token obtained after a successful authentication has not yet expired and the security cookie is still available in the browser, the authentication flow directs the user directly to the application without needing to enter the user name or password.

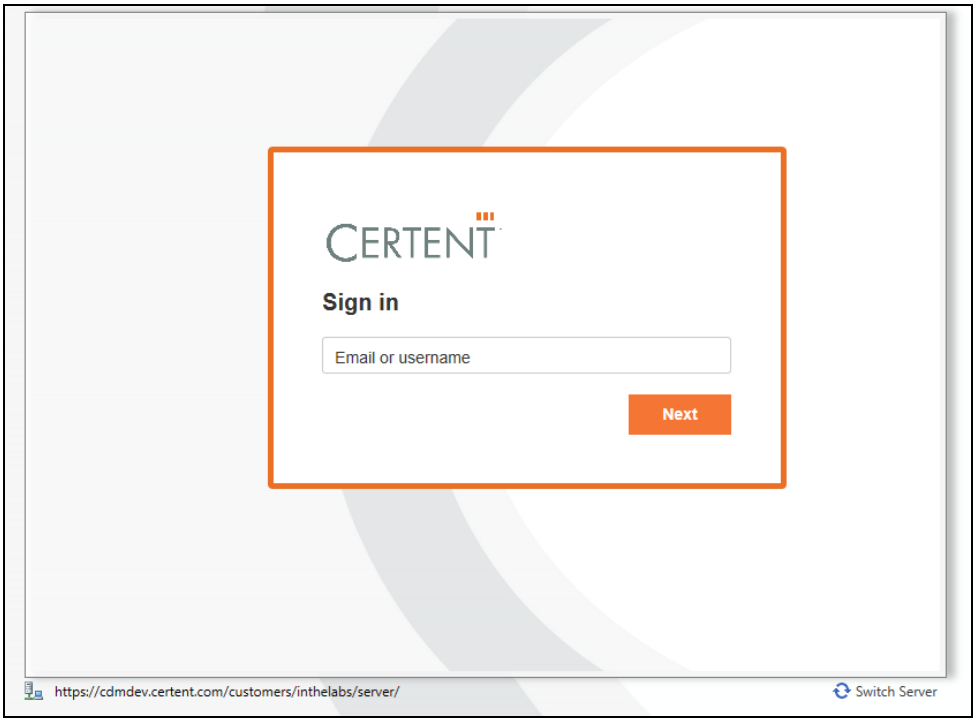
Integrated Windows Authentication

If the CDM Identity Server component is configured for Integrated Windows Authentication, a user is identified and validated automatically. Assuming the user has CDM product access, they are greeted and offered the option to advance to the application or sign in with a different account.

Server Selection for the CDM Desktop Client

The CDM desktop client can be used to connect to multiple CDM application servers, such as a development, test, or UAT server.

When opening the CDM desktop client, the authentication flow is initiated against the user's default CDM application server. The user identification form of the authentication flow and the greeting form of the Integrated Windows Authentication flow show the CDMServer URL that the user is opening. The user is also able to switch to a different server.



Automatic Provisioning of Users

The CDM application can be configured to provision users automatically the first time the user's credentials are validated by the CDM Identity Provider or the CDM Import Sources, hereby called just-in-time provisioning.

Whenever the username or email for a user attempting to authenticate cannot be matched with an existing CDM account, the application attempts to provision one:

- CDM defers the validation of the account to the CDM Identity Provider, if it exists.
- Otherwise, the user credentials are validated against the CDM Authentication Import Sources.

If credentials are validated, CDM provisions an account for the user using the First Name, Last Name, Display Name, and Email Address, obtained from the Identity Provider or Import Source. If multiple AD/LDAP-configured Import Sources exist, the CDM account is associated to the one that first validates the credentials.

The CDM Identity Providers support just-in-time provisioning at the Identity Provider application level or just-in-time provisioning within a single group from the Identity Provider. CDM Import Sources only support just-in-time provisioning with groups.

Just-in-Time Provisioning

When CDM is configured for Just-in-time provisioning, an account is created for any user that have their credentials validated by the external Identity Provider. An account being provisioned using just-in-time provisioning will have no application and report permission assigned. Appropriate application and report permissions must be assigned after that.

Just-in-Time Provisioning with Groups

Identity Provider

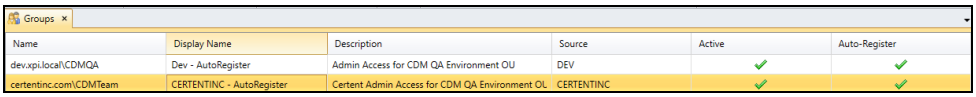
When a CDM Identity Provider is configured with just-in-time provisioning with a group, a CDM account is created only for users that have their credentials validated by the external Identity Provider's group.

An imported user that was removed from the group that is configured to control access to the CDM application, or was deactivated, will no longer be able to authenticate into CDM. When the account details for a user are changed in the external Identity Provider, the details are updated into CDM after the first authentication attempt. An account being provisioned using just-in-time provisioning will have no application and report permission assigned. Appropriate application and report permissions must be assigned after that within the CDM application.

Import Source

When a CDM Import Source is configured with just-in-time provisioning with a group or groups, a CDM account is created only for users that have their credentials validated by the Import Source, only if they are also members in one of the groups that are configured to control access to the application.

In the following example, the CDMTeam is a group imported from the CERTENTINC domain and is marked to control access to the CDM application (auto registerable).



Whenever a user authenticates into the CDM application using an account that was created through just-in-time provisioning, their group membership into external groups is recalculated and the application and report permissions set accordingly based on the CDM group(s).

An imported user that was removed from the group that is configured to control access to the CDM application, or was deactivated, will no longer be able to authenticate into CDM. When the account details for a user are changed in the Import Source, the details are updated into CDM after the first authentication attempt.

Migrate Existing CDM Users

CDM 20.7.1 and later

This topic describes the steps to migrate existing CDM users, so they can leverage a modern authentication provider such as Azure AD.

1. You must be using CDM version 20.7.1 or later.
2. In Certent 365, go to the **Site Administration** page and define the authentication provider you wish to use through the **Single Sign-On Configuration** page as described in the *CDM Site Administration Guide*.
3. Open the CDM desktop client and navigate to **Administration** > **Security** > **Users**.
4. For each user that you wish to convert to the new identity provider, confirm the user EMAIL is the correct one for use with your new identity provider. If it is not, update their email accordingly. This email will be the username they will use to log into CDM once converted.
5. Right-click the user and select **Set Source** and confirm your change.

Note:

- Classic AD/LDAP users that were provisioned automatically will no longer be automatically assigned to classic auto-registering AD/LDAP groups after being converted to modern authentication users. Please confirm any CDM permissions you may have in place via classic AD groups.
- Local authentication and AD/LDAP users can be converted using the preceding method.