

Cora Sequence Authentication Methods

Last Modified on 08/03/2022 9:31 am EDT

V9.x and later

Overview

Authentication is the process used to verify the identity of a person, service, or device that wants to access data, resources, or applications. Authentication validates the identity and establishes a trust relationship for further interactions. There are several authentication methods, depending on network settings, operating system, and connection types.



Authentication scenarios

There are mainly three authentication scenarios.

- **Human to machine communication:** users need to provide credentials to access Cora SeSequence resources.
- **External services to Cora SeSequence:** external services or applications need to authenticate themselves to consume Cora SeSequence resources.
- **Cora SeSequence to external services:** Cora SeSequence needs to authenticate itself to consume external services.

Human to machine authentication

In this scenario, the authentication process can be configured to use username and password, or with single-sign on (SSO). Single sign-on (SSO) is an authentication process that allows a user to sign in once and access several applications.

| Version | Protocols/methods | Description | SSO support |
|------------------|------------------------|--|--|
| Earlier than 8.0 | Windows Authentication | Process to prove the authenticity of a user or service attempting to access Windows. |  Kerberos and NTLM |
| Earlier than 8.0 | WS-Federation | With this method, a Security Token Service (STS) in one trust domain provides authentication information to an STS in another trust domain when there is a trust relationship between the two domains. |  |





















| Version | Protocols/methods | Description | SSO support |
|------------------|--------------------------------|---|--|
| 8.5 | SAML 2.0 | XML-based protocol that uses security tokens containing assertions to pass information about a principal (usually an end user) between a SAML authority, named an Identity Provider, and a SAML consumer, named a Service Provider. |  SSO configuration supports SP and IDP-initiated Single Sign-On POST Binding flow. |
| 8.6.2 | OpenID Connect | Authentication layer on top of the OAuth 2.0 protocol. With OpenID Connect, clients verify the identity of end-users based on the authentication performed by an authorization server, and obtain basic profile information about the connecting end-user in an interoperable and REST-like manner. |  Authorization Code Flow only |
| Earlier than 8.0 | Username/Password | Cora SeSequence built-in authentication method. -- only for unsecured development environment -- only for post installation procedures to configure Sequence users for example. | Non-SSO |
| Earlier than 8.0 | Basic | Authentication scheme built onto the HTTP protocol. The client sends the user name and password as unencrypted base64 encoded text. | Non-SSO |
| Earlier than 8.0 | Anonymous | Process that allows a user to log in to a website without credentials. | Non-SSO |
| Earlier than 8.0 | Custom | Authentication methods configured to match specific customer or service requirements. | Non-SSO |

External services to Cora SeSequence

| Version | Protocol |
|------------------|--|
| Earlier than 8.0 | Windows Authentication |
| 8.7 | OAuth 2.0 (bearer token in the authorization header) |
| Earlier than 8.0 | Basic |

| Version | Protocol |
|------------------|-----------|
| Earlier than 8.0 | Anonymous |
| Earlier than 8.0 | Custom |

Cora Sequence to external services

| Activity | Windows | OAuth 2.0 | User/pass. | Basic | Custom | On-behalf-of Flow |
|----------------------|---|---|---|---|---|---|
| Azure Service Bus | | | | |  Shared Access Signature and Access Control Service | |
| Database Listener | | | | |  Authentication is part of the specific database connection string. | |
| Email Listener | |  |  | | | |
| HTTP Consumer |  |  | |  |  |  V9.8.3 and later |
| REST Consumer |  | | | |  | |
| WCF Consumer |  | | | |  | |
| Web Service Consumer |  | | |  | | |
| File Writer |  | |  | |  | |
| SAP RFC Consumer | | |  | | | |
| CRM activities | | |  | | | |

NOTE

Unless indicated, the authentication protocol is supported since the release of the specific activity.

V8.6.2 and earlier

Overview

Authentication is the process used to verify the identity of a person, service, or device that wants to access data, resources, or applications. Authentication validates the identity and establishes a trust relationship for further interactions. There are several authentication methods, depending on network settings, operating system, and connection types.



Authentication scenarios


There are mainly three authentication scenarios.

- **Human to machine communication:** users need to provide credentials to access Cora SeQUENCE resources.
- **External services to Cora SeQUENCE:** external services or applications need to authenticate themselves to consume Cora SeQUENCE resources.
- **Cora SeQUENCE to external services:** Cora SeQUENCE needs to authenticate itself to consume external services.

Human to machine authentication

In this scenario, the authentication process can be configured to use username and password, or with single-sign on (SSO). Single sign-on (SSO) is an authentication process that allows a user to sign in once and access several applications.

| Version | Protocols/methods | Description | SSO support |
|------------------|------------------------|--|--|
| Earlier than 8.0 | Windows Authentication | Process to prove the authenticity of a user or service attempting to access Windows. |  Kerberos and NTLM |
| Earlier than 8.0 | WS-Federation | With this method, a Security Token Service (STS) in one trust domain provides authentication information to an STS in another trust domain when there is a trust relationship between the two domains. |  |




















| Version | Protocols/methods | Description | SSO support |
|------------------|--------------------------------|---|--|
| 8.5 | SAML 2.0 | XML-based protocol that uses security tokens containing assertions to pass information about a principal (usually an end user) between a SAML authority, named an Identity Provider, and a SAML consumer, named a Service Provider. |  SSO configuration supports SP and IDP-initiated Single Sign-On POST Binding flow. |
| 8.6.2 | OpenID Connect | Authentication layer on top of the OAuth 2.0 protocol. With OpenID Connect, clients verify the identity of end-users based on the authentication performed by an authorization server, and obtain basic profile information about the connecting end-user in an interoperable and REST-like manner. |  Authorization Code Flow only |
| Earlier than 8.0 | Username/Password | Cora SeSequence built-in authentication method. -- only for unsecured development environment -- only for post installation procedures to configure Sequence users for example. | Non-SSO |
| Earlier than 8.0 | Basic | Authentication scheme built onto the HTTP protocol. The client sends the user name and password as unencrypted base64 encoded text. | Non-SSO |
| Earlier than 8.0 | Anonymous | Process that allows a user to log in to a website without credentials. | Non-SSO |
| Earlier than 8.0 | Custom | Authentication methods configured to match specific customer or service requirements. | Non-SSO |

External services to Cora SeSequence

| Version | Protocol |
|------------------|--|
| Earlier than 8.0 | Windows Authentication |
| 8.7 | OAuth 2.0 (bearer token in the authorization header) |
| Earlier than 8.0 | Basic |

| Version | Protocol |
|------------------|-----------|
| Earlier than 8.0 | Anonymous |
| Earlier than 8.0 | Custom |

Cora SeSequence to external services

| Activity | Windows | OAuth 2.0 | User/pass. | Basic | Custom |
|----------------------|---|---|---|--|---|
| Azure Service Bus | | | | |  Shared Access Signature and Access Control Service |
| Database Listener | | | | |  Authentication is part of the specific database connection string. |
| Email Listener | |  |  | | |
| HTTP Consumer |  |  | |  |  |
| REST Consumer |  | | | |  |
| WCF Consumer |  | | | |  |
| Web Service Consumer |  | | |  | |
| File Writer |  | |  | |  |
| SAP RFC Consumer | | |  | | |
| CRM activities | | |  | | |

Note: Unless indicated, the authentication protocol is supported since the release of the specific activity.

