# Single Sign-On (SSO)

CISL provides single login/single sign on with Active Directory Federated Services (ADFS) for the organization.  This service allows users to authenticate with their standard UCAR CIT Active Directory (AD) account, and if enrolled, DUO multi-factor authentication (MFA), with applications where a trust has been established.  This allows for a more simplified authentication experience for our customers in reducing the number of usernames and passwords needed as well as establishes a more secure authentication method with MFA enabled.

## Scope

The purpose of this document is to provide information on the terminology used for the single login infrastructure, outline roles and responsibilities for both CISL and the application owner, and give general information on the technical setup that is needed to create a trust as well as support the trust.

## Terminology

| Term | Definition |
|---|---|
| Authentication | Confirming your identity |
| Authorization | Granting access to a system |
| Active Directory | Microsoft's management technology for managing users and computers access and authorization to our network resources from a single directory. Our domain for UCAR is CIT. |
| Active Directory Federated Services (ADFS) | Microsoft's single sign on system used with CIT authentication. A trust is created within ADFS between ADFS and the application. |
| Multi-Factor Authentication (MFA) | DUO is our current MFA solution that is used in combination with your CIT username and password in conjunction with a third method of authenticating including a push to the DUO app on your smartphone. |
| Identity Provider (IdP) | An identity provider implements and manages the framework for authentication and authorization federation. CISL as the administrators of AD, ADFS, and DUO are the identity providers for the organization. |
| Service Provider (SP) | The administrator or owner of the application and federation partner with the IdP providing service to the end user. |

## Roles and Responsibilities

### Roles and Responsibilities for IdP

- Maintain staff and infrastructure to support the AD, ADFS, and DUO environments
- Maintain a secure environment using security best practices
- Maintaining accurate and working metadata
- Coordinate with service providers to set up trusts on the ADFS side
- Communicate certificate updates, metadata updates, infrastructure upgrades, etc

Service-Level Agreements (SLAs)

### Roles and Responsibilities for SP

- Have technical information needed to setup trust on service application side
- Provide technical details needed to IAM team for ADFS trust to be setup
- Be prepared to update and test service side whenever changes are communicated by IdP including certificate updates during off-business hours.  Provide a point of contact and backup for communications, communicate any changes to these contacts over time.
- Manage end user service questions and authentication issues with SP submitting a ticket to CISL with any issues

## Technical Details

In general please start with a ticket request and then CISL will work with you to establish the trust between your application and ADFS. Each trust needs the following information in order to be setup. At the same time, we have also found that each trust can have an extra component to setup that can only be determined through testing. Please submit a request for a trust to be setup.

The first step is to determine if your environment should be setup in a test domain, CIT domain, or both depending on your environment. During the trust setup process, we will test with you to confirm authentication is working with your application. In preparation for a request, the following technical details are needed to get started.

### Service Provider (SP) will supply:

- URL for the metadata of the application
- Determine which attributes will be passed for claims; typically this is SAM-Account-Name and Name ID, but others can be used as well.

- Determine the TokenLifetime setting of the application; each app is different depending on needs, but we typically recommend 480 or 8 hours for a token to be active for a full work day

## Identity Provider (IdP) will supply:

- URL for the ADFS metadata, depending on domain
- Logout URL, depending on domain
- Set TokenLifetime to match the setting of the application