Integration Methodologies for Target Applications Using the NCEdCloud IAM Service

(Provisioning and Authentication)

Integration Methodologies

1. Provisioning

A user must have an account in a system in order to login and use that system. The NCEdCloud IAM Service will support two methods of implementing automated lifecycle management of accounts for both provisioning and de-provisioning.

1.1. Provisioning via SAML

1.1.1. The first method for target application account provisioning is via SAML. This method requires the target system to use a SAML Service Provider (SP) and it must support the on-demand creation (auto-provisioning) of user accounts via this method. Not all systems that provide SP capability support this method.

1.2. Provisioning via Data Synchronization

1.2.1. The second method for target application account provisioning is via data synchronization. One component of the NCEdCloud IAM service is Identity Automation's DSS product. Using DSS adapters, the IAM service will communicate directly with the target system in order to provision accounts. This process occurs in near real-time as user accounts are created and updated in the Central Directory. Depending on the authentication method used, this provisioning process may include synchronization of user credentials.

2. Authentication

The NCEdCloud IAM Service will support three methods of implementing a simplified authentication service for end users accessing target application systems. The term "simplified authentication" refers to the concept that users won't have to keep track of multiple credentials when accessing the different

target systems. From the end user perspective, this could be either a Single Sign-On (SSO) or Reduced Sign-On (RSO) experience, depending on the method used to provide the authentication integration.

The term single logout (SLO) is the counter solution to SSO. For example, if you log in to five applications via SSO, you could log out of all sessions with a single logout link. The NCEdCloud IAM service will provide a single logout capability for SAML-enabled applications, but cannot enforce its implementation by all target systems. So if an end-user clicks on the single logout option of an application, it would log them out of all sessions that were accessed using SAML. Unfortunately, only closing the browser application itself can guarantee that all sessions are absolutely ended.

2.1. SAML Authentication

2.1.1. The first (and preferred) method for target system authentication integration is via SAML. This method requires the target system to use a SAML Service Provider (SP). Once integrated, the login page for every target system using SAML will be the NCEdCloud IAM login page (branded to illustrate the use of the NCEdCloud Username and Password). The first application accessed will require the user to authenticate (via the IAM Service Login), however, each subsequent SAML-enabled application the user accesses will provide an SSO experience (no additional login required).

2.2. Native Authentication

2.2.1. The second method for target system authentication would be native authentication. With this method the user will access the target system and will login with credentials that have been synchronized to that system (See 1.2. Provisioning via Data Synchronization). In this case, the application is storing the user account credentials locally, thus it is using native authentication. This method will provide an RSO experience because the credentials used will be the same credentials as the NCEdCloud.

2.3. LDAP Authentication

2.3.1. The third method for target system authentication integration is via LDAP. This method requires the target system to support an option to use LDAP for authentication as an alternative to local/native authentication. The NCEdCloud IAM Service will provide a load balanced, fault tolerant LDAP endpoint for target systems for authentication. This method will provide an RSO experience because the credentials used will be the same credentials as the NCEdCloud.