Project Overview

The N.C. Department of Information Technology is updating the N.C. Identity Management (NCID) service through the Citizen Identity Project. This involves enhancing security, improving self-service and moving external user identities from the department's on-prem infrastructure to a modern cloud-based service. Additional details and timeline information can be found at: https://it.nc.gov/support/ncid/ncid-citizen-identity-project

SAML Integration Overview

Currently, when a user tries to access a SAML integrated application, NetIQ Access Manager handles authentication of internal and external users against NCID eDirectory. At cutover, the configuration changes on NetIQ will perform authentication for internal users against NCID eDirectory and external users against Simeio-Ping directory. After cutover, the Applications will need to be re-configured to establish trust relationship to go to Simeio IdP such that, when a user accesses an application, Simeio Ping Federate will perform authentication for internal users against NCID eDirectory and external users against Simeio-Ping directory.

Definitions

- **Cutover:** At this point in time, all External identities would be migrated from NCID eDirectory to Simeio-Ping Directory in Production.
- **Co-existence phase:** This will be the phase when the new Simeio-hosted systems are available for external users' registration and self-service, but application integration with Simeio systems is not yet complete.
- **External user identities:** Individual user accounts and Business user accounts
- **Internal user identities:** State employee user accounts and Local Govt employee user accounts
- **NCID eDirectory:** It is a repository that currently stores internal and external user identities. After successful migration to Simeio, NCID eDirectory will act as the source of truth for all identity attributes associated with the internal user's profile.
- **NetIQ AM:** NetIQ Access Manager.
- **Ping Directory:** It is an LDAP repository that stores the external user identities. It will act as the source of truth for all identity attributes associated with the external user's profile.
- **Ping Federate:** It is a federation server that enables external user authentication and Single Sign-On for applications (**HTTP Proxy & SAML Apps**). It delegates authentication of internal users to **NetIQ AM** (1FA) and **Azure AD** (MFA).
- **Ping One:** It provides Multi-Factor Authentication (MFA) for external users.

Application User Impact after Cutover

1) For New User Registration for NCID Account and for Self-Service options (Forgot Username, Forgot Password, Unlock Account)
   - External Users (Individual Users and Business Users): They would go to https://myncid.nc.gov.
   - Internal Users (State Employee Users and Local Govt Employee Users): No change. They would continue to go to https://ncid.nc.gov.
2) Application access flow: No change.

Application Admin Impact after Cutover

1) Role Assignment:
   - To manually assign a role to External users (Individual Users and Business Users): They would go to https://myncid.nc.gov.
   - To manually assign a role to Internal Users (State Employee Users and Local Govt Employee Users): No change. They would continue to go to https://ncid.nc.gov.
   - To programmatically assign a role to External or Internal users through Web Service Integration: No change.

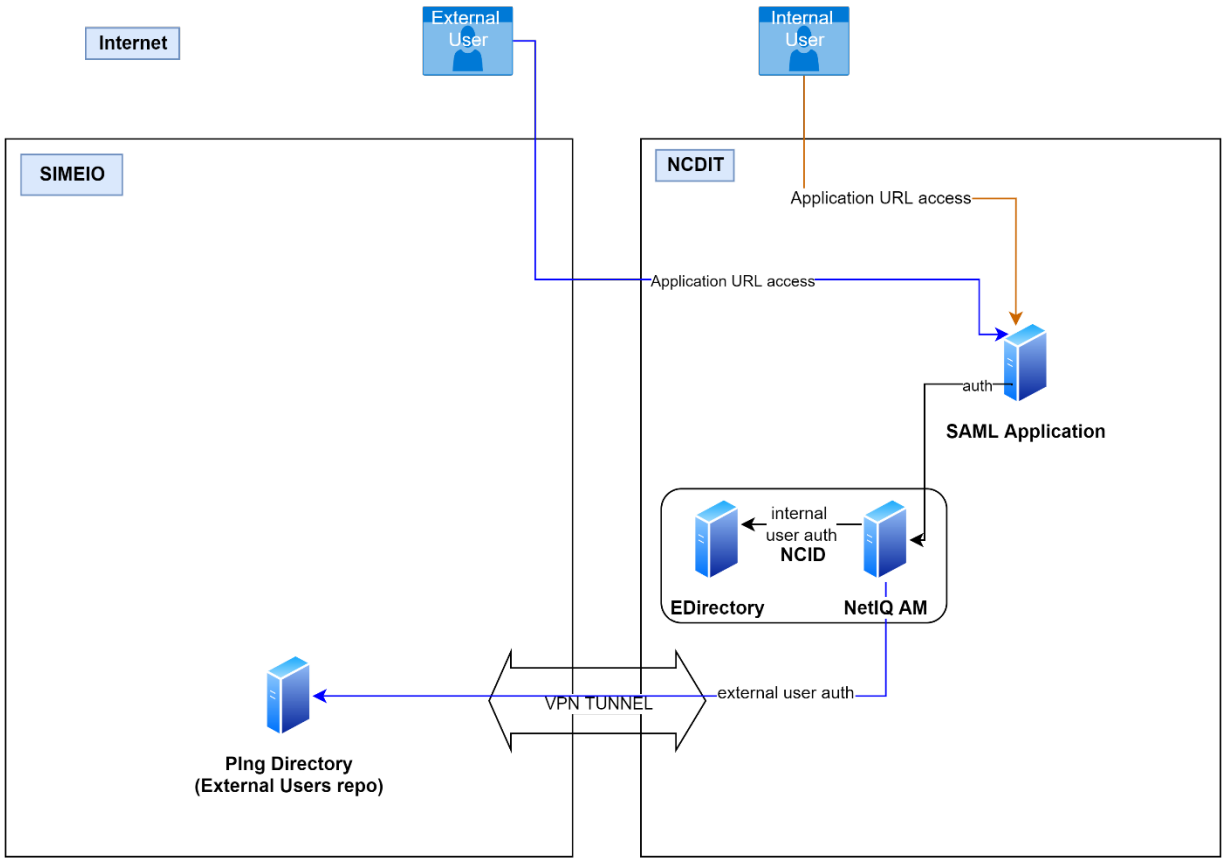
2) App Membership Report:
   - To view the report for External users (Individual Users and Business Users): They would go to https://myncid.nc.gov
   - To view the report for Internal Users (State Employee Users and Local Govt Employee Users): No change. They would continue to go to https://ncid.nc.gov.

Preparing for Cutover

- **NCID Team** will ensure that at the time of cutover, config change is in place in NETIQ to handle multiple data stores. This will ensure that it can perform authentication for internal users against NCID directory and external users against Simeio-Ping directory.
- **Application team** will ensure that right after cutover:
  - An existing external user (whose account was migrated from NCID to Simeio) can successfully access their application.
  - A new external user (who registered their NCID account in Simeio after cutover and was provided appropriate access to the application by the application admin) can successfully access their application.
  - If applicable, an internal user can successfully access their application.

At Cutover

At cutover, the application is still with NCID. Applications are still using the existing SAML Solution.
NetIQ Access Manager in the backend will authenticate external users against Simeio Ping Directory.



SAML based applications Co-existence

Preparing to Migrate applications to Simeio

- **Application Team** will need to work with Simeio Team to exchange meta data in each environment (Dev/Pre-Prod/Production), re-configure the application to establish trust relationship to go to Simeio IdP and perform functional testing.

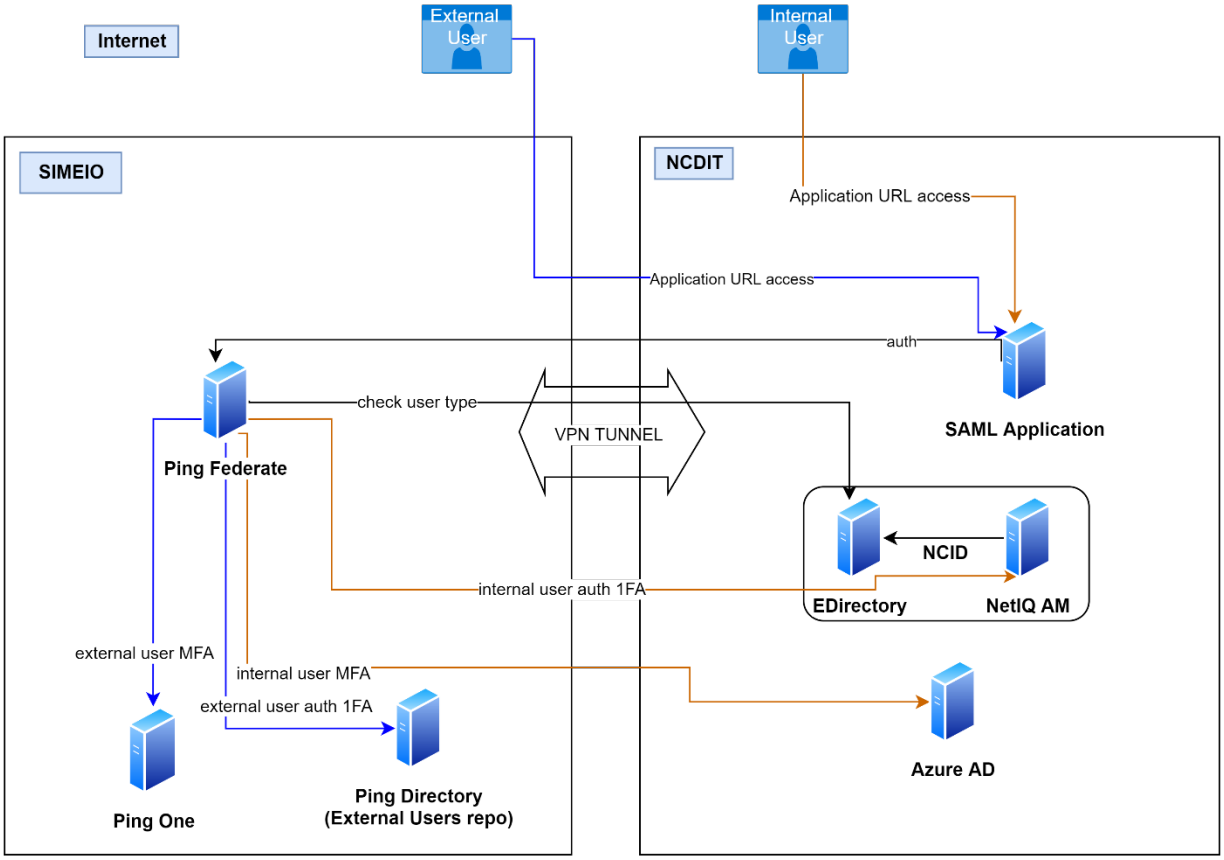
After Application Migration

- **NCID Team** will disable trust relationship between the application and NCID IdP.

User Login Flow after Migration

- A user attempts to access the application protected by the PingFederate using the SAML protocol.
  - The user is redirected to the PingFederate server for authentication if the session does not exist.
  - If the session already exists, the user is granted immediate access.
- Ping Federate checks the user type
  - For internal users, the PingFederate server redirects the user's browser to NetIQ (1FA) or Azure AD (MFA) for authentication using the SAML protocol. The IdP partner authenticates the user and returns a SAML assertion. PingFederate validates the assertion and creates an assertion for the user including any configured attributes. PingFederate then redirects the browser, including the assertion back to the Application.
  - For external users, The PingFederate authenticates the user against Ping Directory (1FA) and/or Ping One (MFA). PingFederate creates the assertion for the user including any configured attributes. PingFederate then redirects the browser, including the assertion back to the Application.
- The Application verifies the assertion and grants access to the protected resource, as appropriate.

NCID CITIZEN IDENTITY PROJECT – SAML INTEGRATION



SAML based applications - Final state