Michigan Health Information Network

Single Sign-On Implementation Guide

Version 10

August 18, 2015

Document History

Date	Version	Section(s) Revised	Description	Modifier
8/28/14	1	All	Initial Draft	Talley
8/29/14	2	Multiple	Rewording, Edited Data Flow Diagrams, General Review	Talley Seggie Ward
9/4/14	3	Multiple	Added URLs for and updated links	Talley
9/11/14	4	Multiple	Provided language.	Talley
9/16/14	5	Multiple	General cleanup	Livesay
9/17/14	6	All	Moved to new template	Seggie
9/23/14	7	Multiple	Update URL language and Links with some definitions	Talley
8/11/15	8	All	Move to new template, added language.	Baker
8/17/15	9	All	Review, edits, notes for completion	D.Livesay
8/18/15	10	3	Additional Onboarding documentation	Baker
8/24/15	11	All	Review, edits	D. Livesay
8/25/15	12	All	Final draft for review	D. Livesay

Abbreviations and Acronyms

AD	Active Directory
CAS	Ping Identity's Cloud Access Service
CMS	Centers for Medicare & Medicaid Services
CSP	Credential Service Provider
HIPAA	Health Insurance Portability and Accountability Act
HISP	Health Information Service Provider
IdP	Identity Provider
IEH	Identity Exchange Hub
ISO	International Organization for Standardization
JIT	Just-In-Time
LoA	Level of Assurance
MiHIN	Michigan Health Information Network Shared Services
NIST	National Institute of Standards and Technology
PIV	Personal Identity Verification
PO	Participating Organization
QO	Qualified Organization
RA	Registration Authority
RMF	Risk Management Framework
RP	Relying Party
SAML	Security Assertion Markup Language
SP	Service Provider
SSN	Social Security Number
SSO	Single Sign-On
TDSO	Trusted Data Sharing Organization
TDSOA	Trusted Data Sharing Organization Agreement

Table of Contents

1 Introduction

1.1 Purpose of Use Case

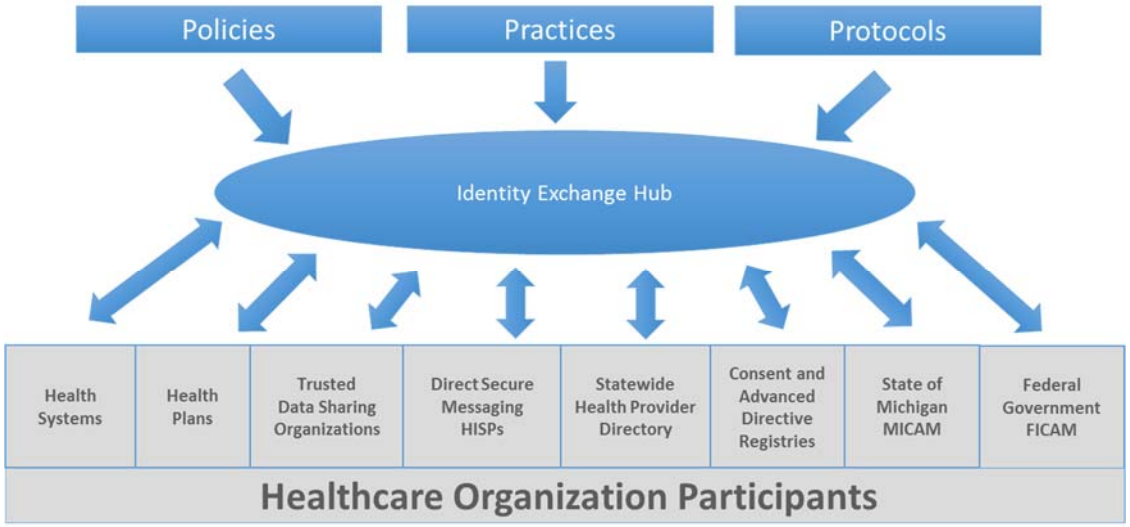
Currently the task of electronically accessing health information often means logging into multiple, disconnected networks, portals or databases, meaning users must maintain and remember unique login IDs and passwords for each data source. This creates obvious productivity-draining issues resulting from forgotten login information, recovering and resetting passwords, and auto-lockout after multiple failed login attempts, as well as security risks inherent in users writing down passwords or keeping them simple or identical to ease memorization. The issues multiply with each additional login and password combination that a user must maintain, creating additional security risks and potentially taking health professionals' valuable time away from patient care.

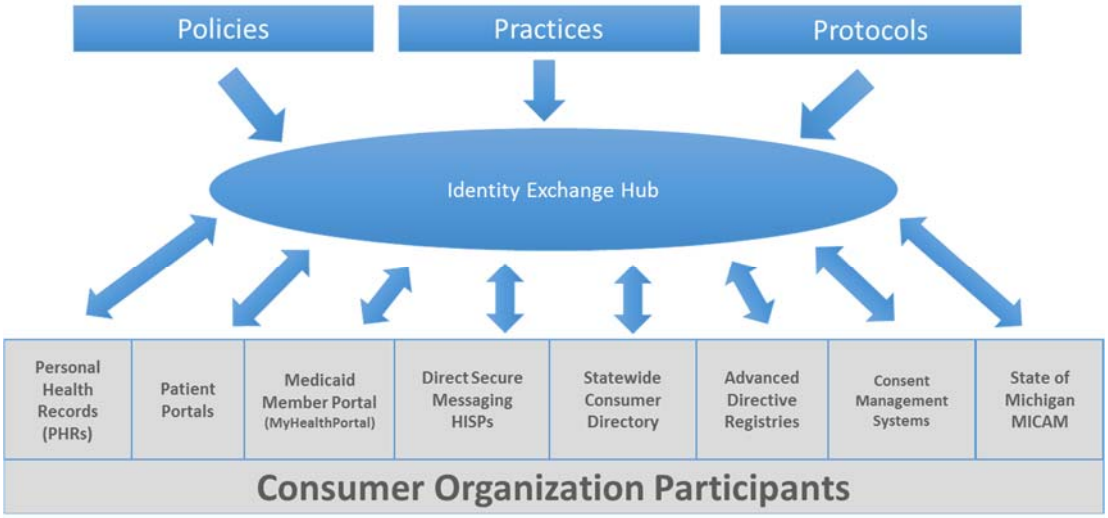
Popular Internet companies have enabled users to employ one login ID and password to access multiple web sites. For example, a Google login ID and password now also accesses Facebook, YouTube, LinkedIn and a growing list of web sites that enable shared 'identities.' This ability to 'share' one identity across multiple networks, web sites or software applications is popularly called Single Sign-On or SSO and gained immediate acceptance as users enjoyed the freedom from remembering so many unique login/password combinations.

Single Sign-On applied to health information can similarly solve issues inherent in having to access multiple data sources, but when using data sources that provide access to Protected Health Information (PHI) we must additionally consider federal laws and regulations regarding who may access a person's PHI. Specifically, on the public Internet there is no standard way to verify someone's identity, so in the world of health information SSO, a shared login ID and password should only be provided to someone whose identity has been thoroughly verified.

This Single Sign-On Use Case leverages a body of technology and legal trust called Federated Identity Management (FIdM) which consists of **Policies, Practices and Protocols** which are defined below and more fully described in the SSO Use Case Implementation Guide. These Policies, Practices and Protocols are the three major components of FIdM to allow Federated Organizations to utilize trusted identities together.

1.2 Data Flow and Actors





For more information about this Use Case, refer to the documents linked below:

Use Case Summary:
http://mihin.org/wp-content/uploads/2013/07/MiHIN-UCS-Single-Sign-On-v28-published-09-16-15.docx
Use Case Agreement:
http://mihin.org/wp-content/uploads/2013/07/MiHIN-UCA-Single-Sign-On-PUBLISHED-v9-08-17-15.docx

2 Overview

2.1 Connecting to the Identity Exchange Hub

Trusted Data Sharing Organizations (TDSOs) that have executed the Single Sign-On Use Case Agreement will connect to the Identity Exchange Hub (IEH) using the Ping Identity PingOne Cloud Access Service (CAS). Once connected to the IEH, a TDSO will be able to share authentication information and/or application access for the purpose of allowing participants to employ single sign-on for multiple, disparate networks of other TDSOs that are signed up for the Single Sign-On Use Case.

Identity Providers are participating organizations that have one or more individuals logging in to access applications through Single Sign-On. These Identity Providers can manage and assign rights to their users' identities for accessing various applications. These rights are managed and assigned by inclusion in groups with specific access permissions.

This functionality allows an Identity Provider to selectively show only the application(s) that would be appropriate for each particular group of individuals within an organization. For example, a consumer would not need to access an application intended only to be used by healthcare professionals and vice versa.

Currently PingOne allows connections using the following methods:

1. Any SAML 2.0 enabled identity management platform
2. PingFederate
3. Active Directory (AD) Connect
4. Other connection options available on request, may require additional charges

Please see the PingOne Data Sheet for more information about the technical requirements to connect with the PingOne Cloud Access Service:

https://www.pingidentity.com/content/dam/pic/downloads/resources/data-sheets/pingone-data-sheet.pdf

3 Onboarding Process

3.1 Initial Onboarding

Organizations wishing to participate in this or any other Use Case with MiHIN must complete legal and technical connectivity onboarding processes. These onboarding processes may happen concurrently: the organization can review and complete legal agreements with MiHIN while simultaneously establishing and testing technical connectivity. The two processes are described in more detail below.

To initiate onboarding, please notify MiHIN via email at help@mihin.org.

3.1.1 Initial Legal Onboarding Process

The legal onboarding process at MiHIN begins with review and execution of a Trusted Data Sharing Organization Agreement (TDSOA.) Execution of this agreement allows an organization to become a Qualified Organization (QO) and enter into one or more Use Cases via Use Case Agreements. There are various TDSOAs for different kinds of organizations, available for review at:

http://mihin.org/about-mihin/resources/mihin-legal-document-templates

An organization can then enter into an unlimited number of Use Cases with MiHIN. Use Cases currently available for participation are located at the following links:

http://mihin.org/about-mihin/resources/use-cases-in-production/
http://mihin.org/about-mihin/resources/use-cases-in-pilot/

3.1.2 Initial Technical Connectivity Onboarding Process

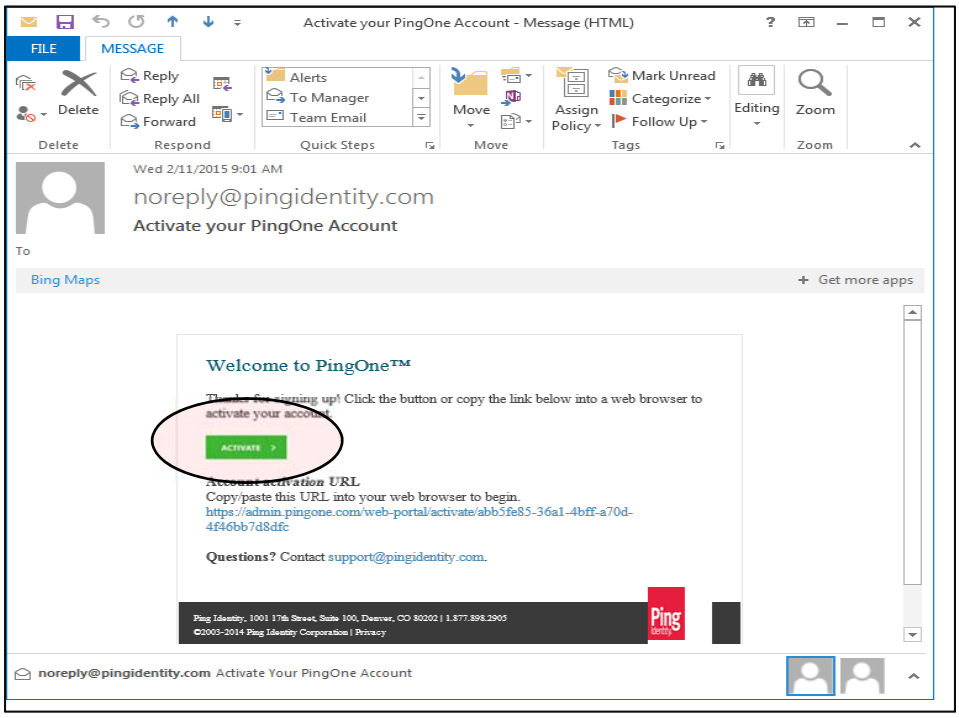
The technical connectivity onboarding process with MiHIN begins with an "onboarding kickoff" meeting. During this meeting the MiHIN operations team guides an organization through step-by-step details to establish and test connectivity, and answers any questions regarding the technical connectivity onboarding process.

3.1.2.1 Connecting an Identity Provider to the Identity Exchange Hub

Following the onboarding kickoff meeting, organizations will begin connectivity setup when the MiHIN Identity Exchange Hub Administrator invites a TDSO to participate in the Identity Exchange Hub (IEH). The TDSO will receive an automated email from Ping Identity containing a link to create an account in PingOne connected to the Identity Exchange Hub.

Follow the steps outlined on the screen shots below to complete connectivity setup.

3.1.2.1.1 INITIAL CONNECTIVITY STEPS FOR ALL TYPES OF IDENTITY PROVIDERS



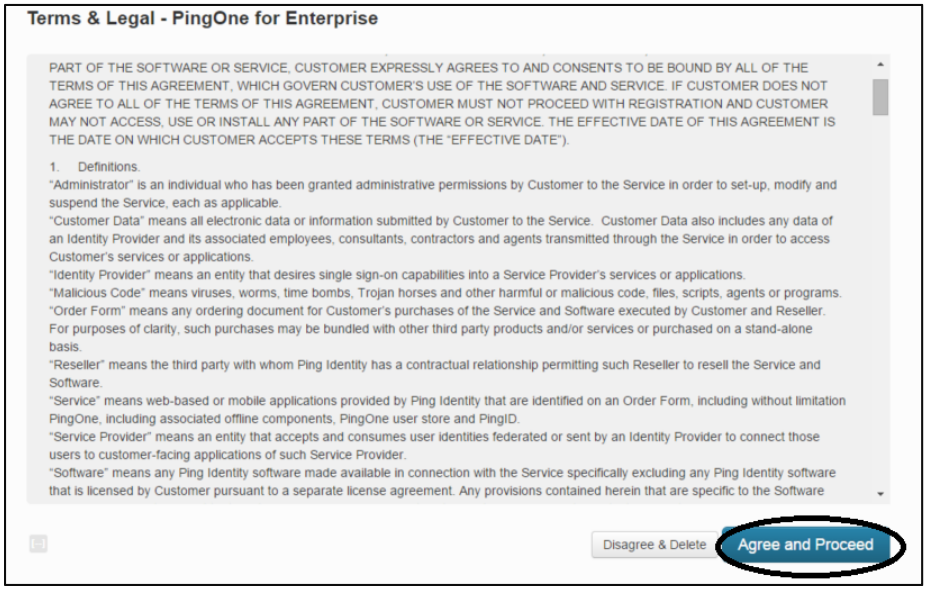
Screen One: Email from Ping Identity

Click the 'Activate' button in the automated email to log in and create an account.

NOTE: depending on your email settings this button may appear as a link.

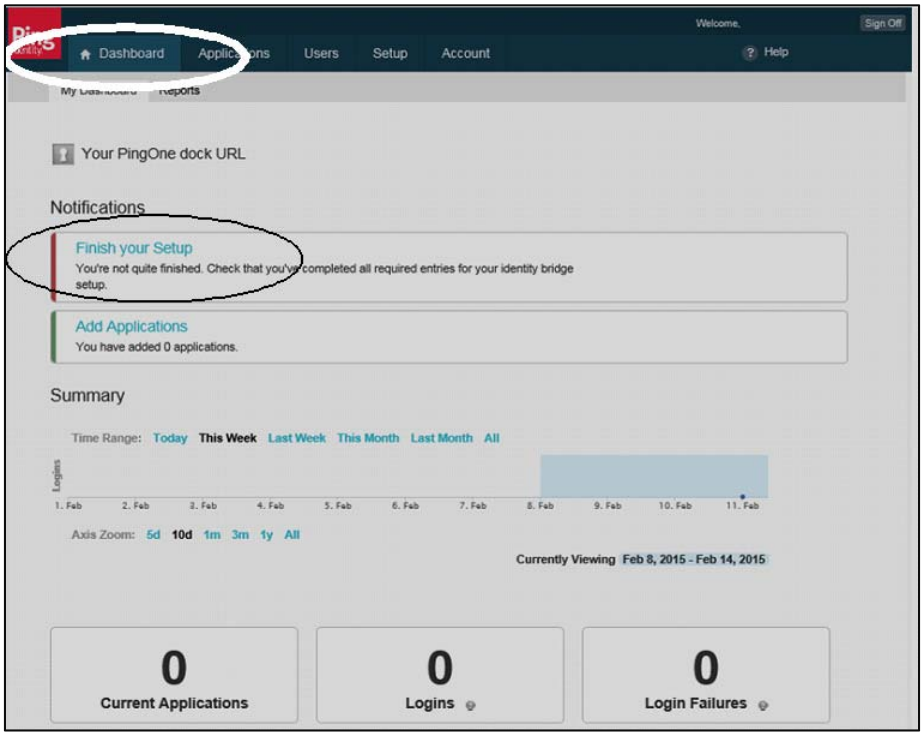
Screen Two: Set Password

You will need to create a password for your PingOne account and click 'Submit.' The email address that received the original invitation will be used as the username for the account.



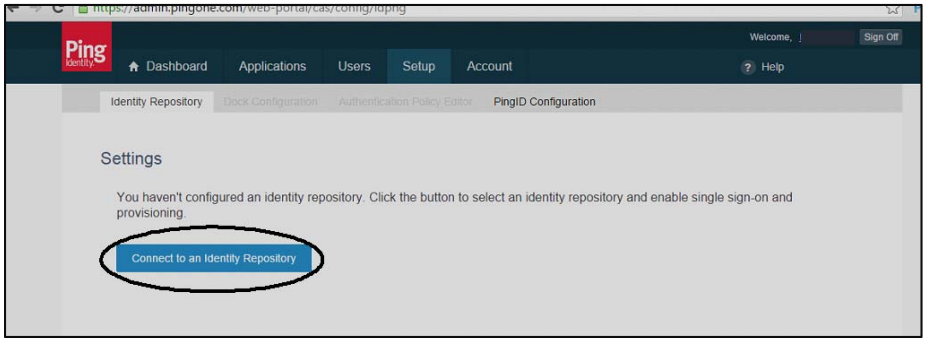
Screen Three: Terms and Conditions

Read the PingOne Terms and select 'Agree and Proceed' to finish setup.



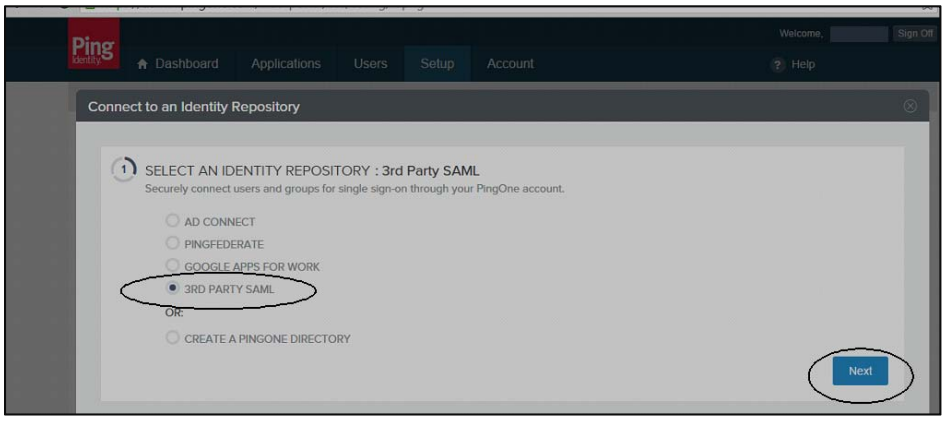
Screen Four: Dashboard

On the Dashboard screen select 'Finish your Setup,' then select 'Connect to an Identity Repository' on the following screen.



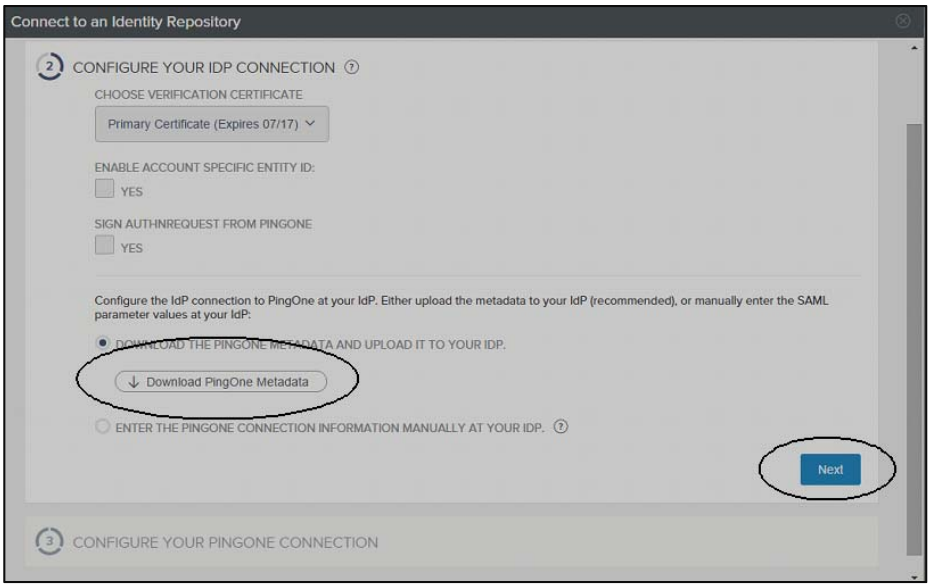
Screen Five: Settings

3.1.2.1.2 REMAINING STEPS FOR CONNECTING A SAML 2.0 IDENTITY PROVIDER



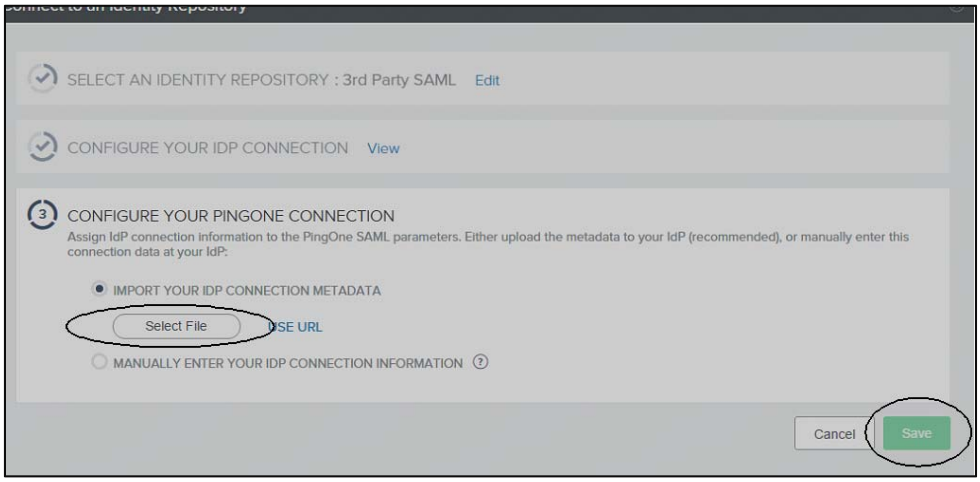
Screen Six: Select Identity Repository

Select '3rd Party SAML' as the Identity Repository to which you want to connect, and click 'Next'.



Screen Seven: Configure IDP Connection

Next, select the 'Download the PingOne Metadata and Upload it to your IDP' radio button. Click the 'Download PingOne Metadata' button to save the connection metadata file to your computer. You will need to upload this file to your Identity Provider. The method for uploading this file will depend on your chosen Identity Provider. Once the file has been uploaded to the Identity Provider click 'Next.'

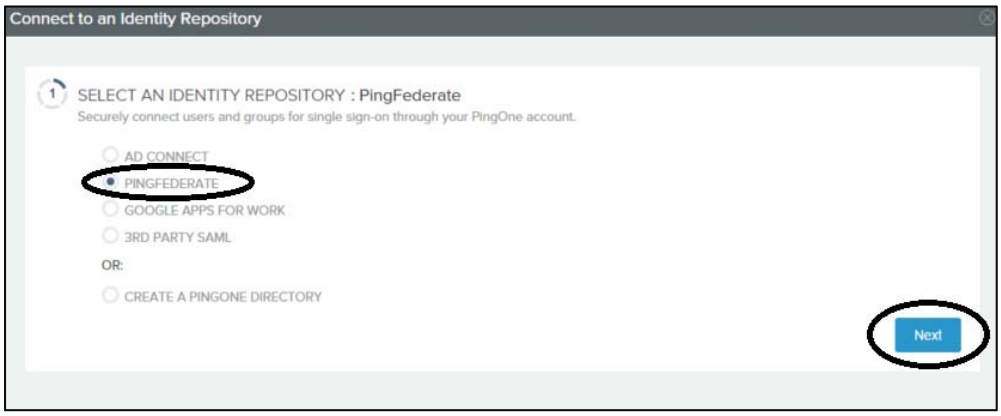


Screen Eight: Configure PingOne Connection

Next you will need to upload your Identity Provider's connection metadata to PingOne. To do this, first download the connection metadata file from your Identity Provider and save it to your computer. Then, under the Configure your PingOne Connection section, choose the 'Import Your IDP Connection Metadata' radio button, select the connection metadata file you just downloaded from your Identity Provider to import, and click Save to upload the file to PingOne.

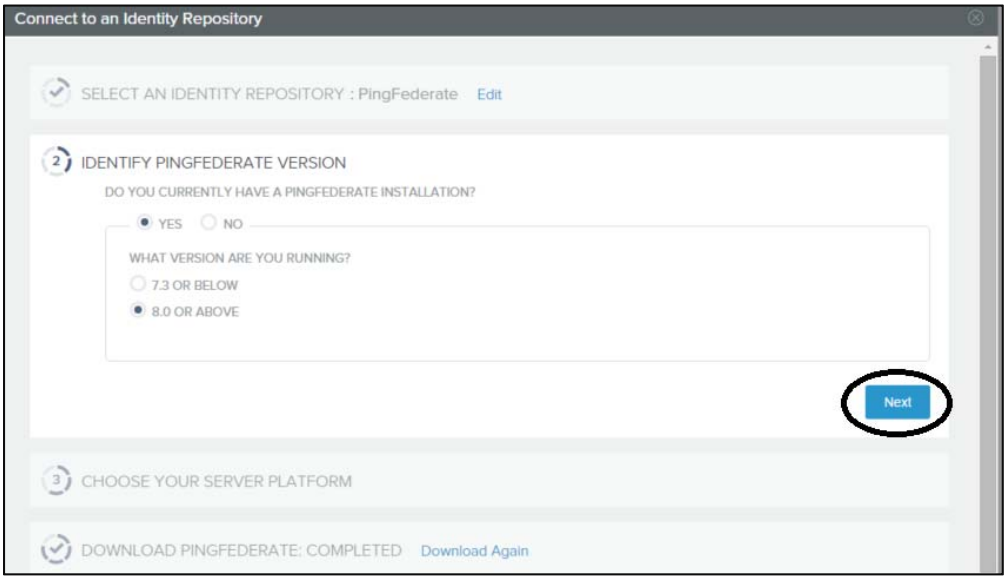
You have now successfully connected to the Identity Exchange Hub!

3.1.2.1.3 REMAINING STEPS FOR CONNECTING WITH PINGFEDERATE



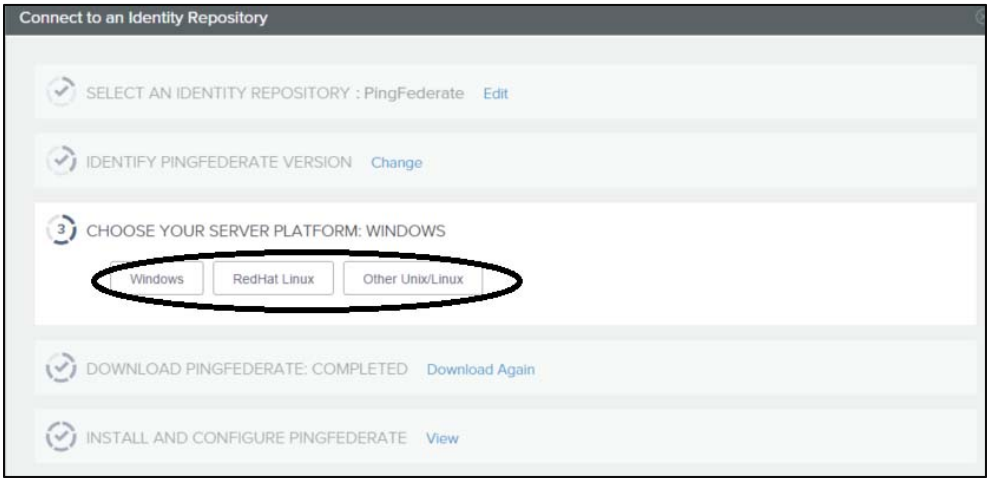
Screen Nine: Select and Identity Repository

Select 'PINGFEDERATE' as the Identity Repository to which you want to connect, and click 'Next'.



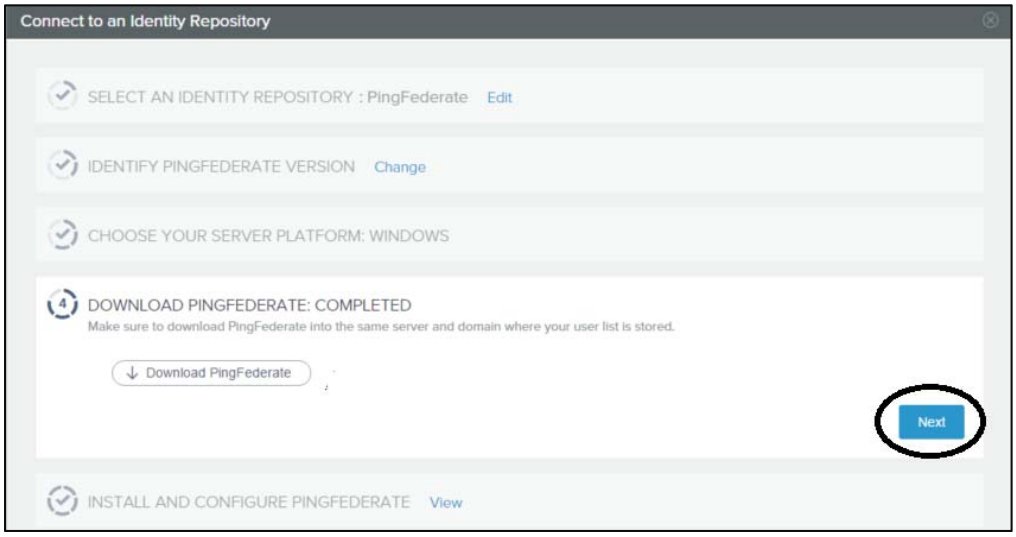
Screen Ten: Identify PingFederate Version

Select the PingFederate Version that you have installed on your server, and click 'Next'.



Screen 11: Choose Your Server Platform

Select the server platform.

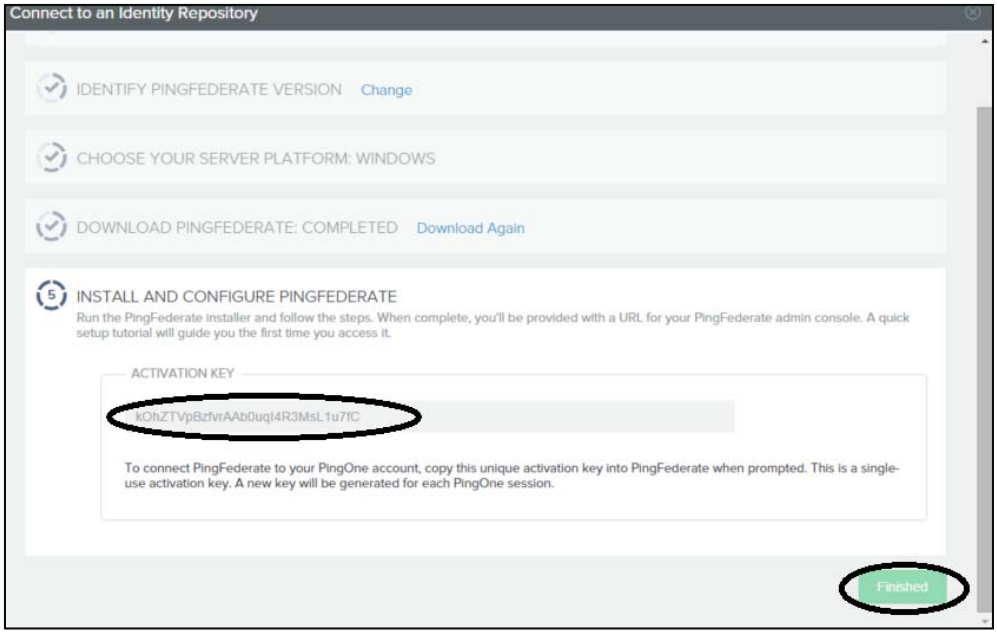


Screen 12: Download PingFederate

If you do not already have PingFederate installed you can download it here using the 'Download PingFederate' button.

For more information on installing PingFederate you can review the documentation on the Ping Identity website: https://www.pingidentity.com/en.html.

If you already have PingFederate installed click 'Next'.



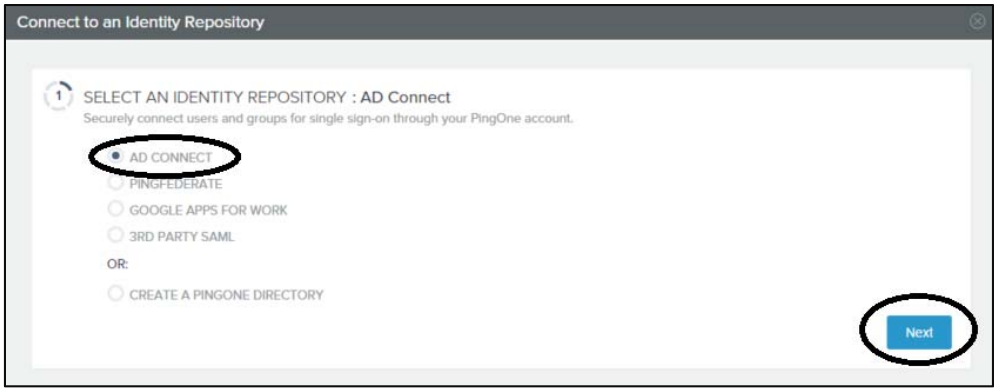
Screen 13: Configure PingFederate

You will need to enter an Activation Key as part of the connection setup in PingFederate. The steps to connect PingFederate with PingOne differ by the PingFederate version and are outlined in the respective PingFederate setup documentation on: https://www.pingidentity.com/en.html.

Once PingFederate has been properly configured click 'Finished'.

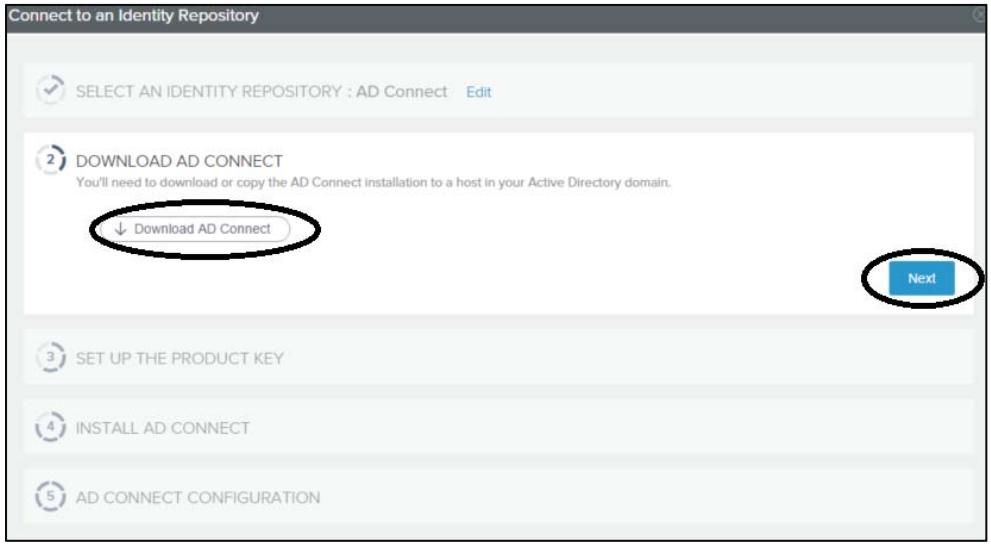
You have now successfully connected to the Identity Exchange Hub!

3.1.2.1.4 REMAINING STEPS FOR CONNECTING WITH ADCONNECT



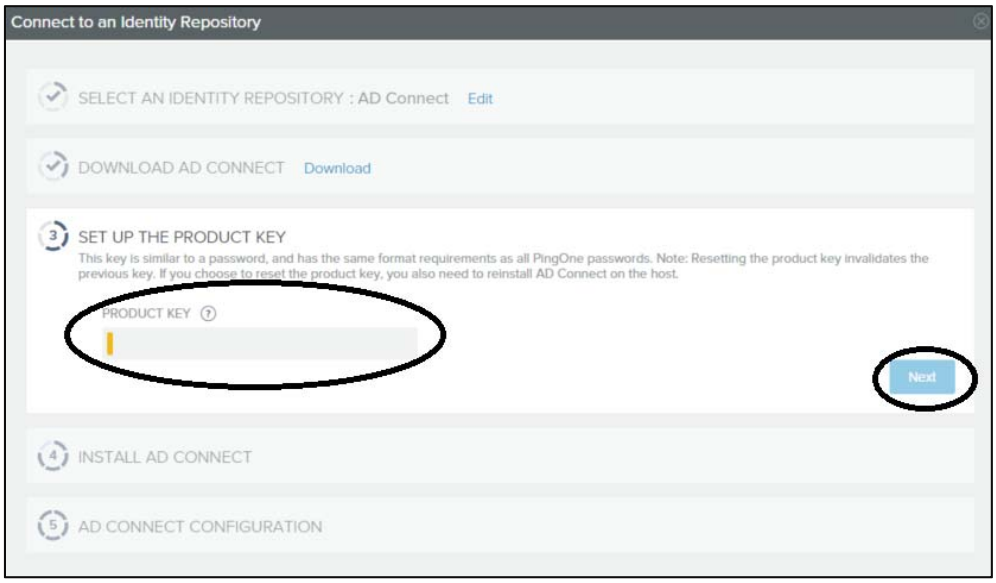
Screen 14: Select and Identity Repository

Select 'AD CONNECT' as the Identity Repository to which you want to connect, and click 'Next'.



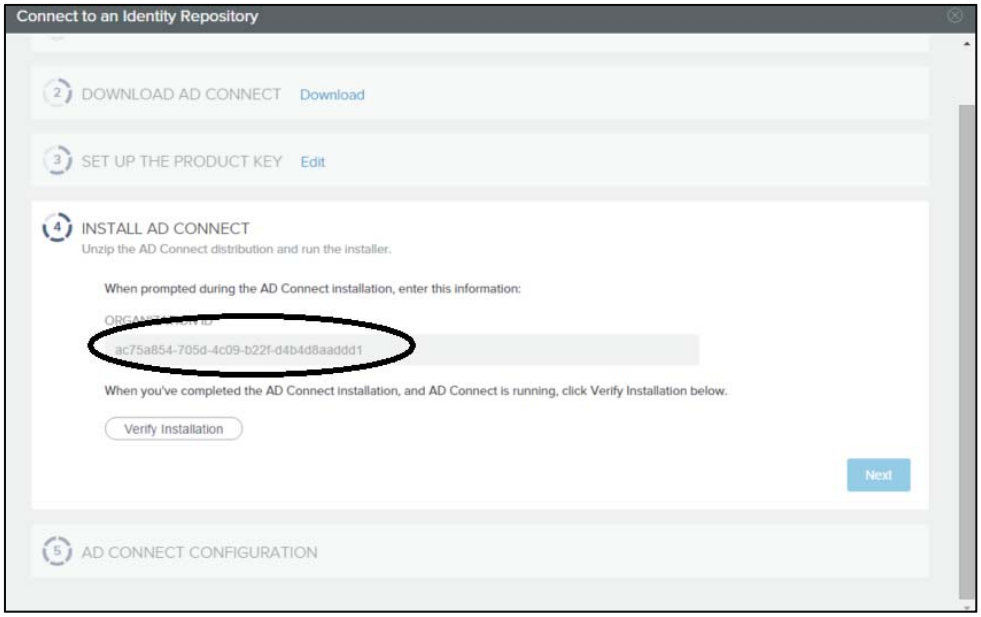
Screen 15: Download AD Connect

Download AD Connect using the 'Download AD Connect' button, and click 'Next'.



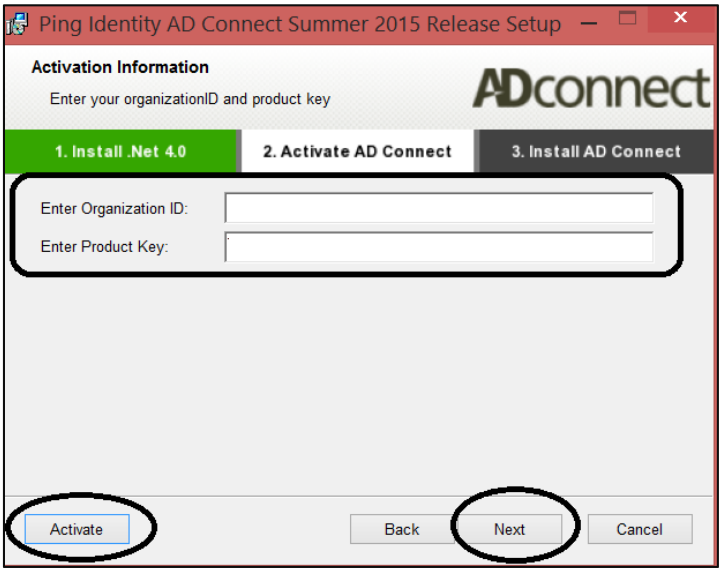
Screen 16: Set Up the Product Key

Create a Product key that you will use during the AD Connect installation process, and click 'Next'.



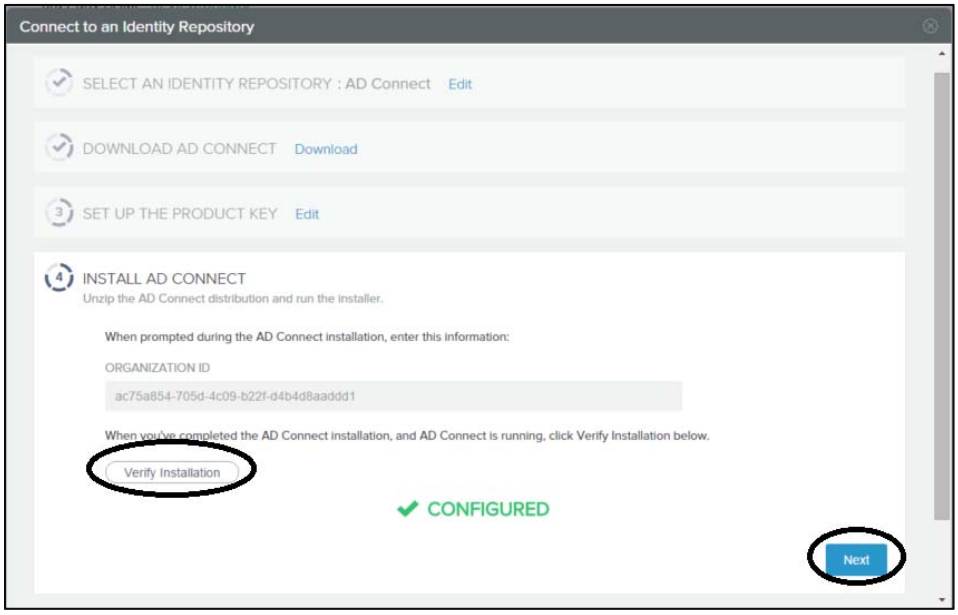
Screen 17: Install AD Connect

Next you will need to run the installer for AD Connect that you have downloaded. You will use the Organization ID shown above along with the Product Key you created previously during the installation process.



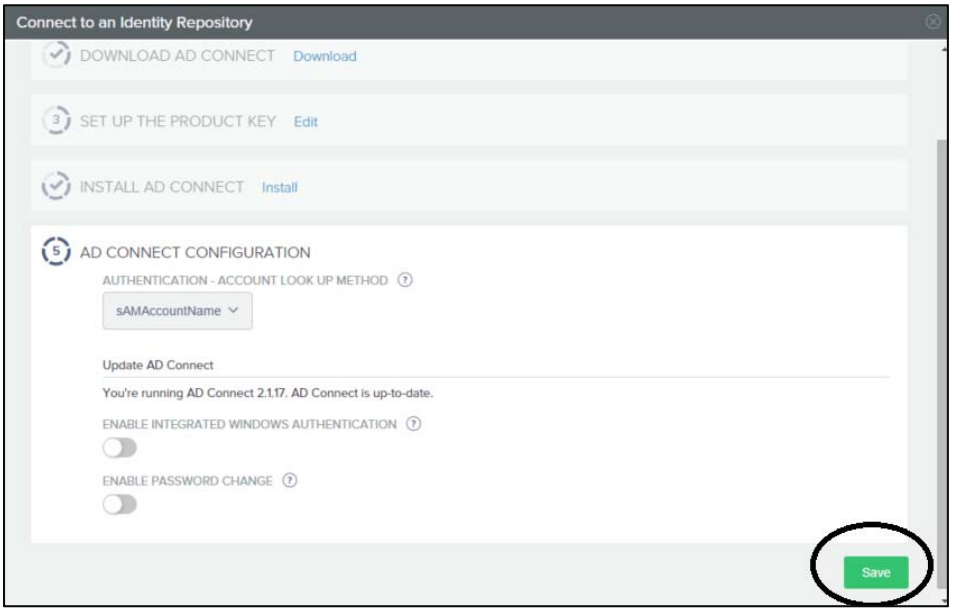
Screen 18: Enter Organization ID and Product Key

The above screen shot is from the AD Connect Installer, you will need to copy the Organization ID from the PingOne portal and enter the Product Key you created here. Once both are entered click 'Activate' on the installer. You then can select 'Next' on the installer and finish the installation of AD Connect.



Screen 19: Verify AD Connect Installation

After the installation is complete, return to the PingOne Portal and click the 'Verify Installation' button. Once the system verifies the installation it will display a green "Configured" message and you can click 'Next'. If you have any issues with verifying the installation please follow the instructions provided by PingOne or contact help@mihin.org.



Screen 20: AD Connect Configuration

Configure the remaining options based on your system and click 'Save'.

You have now successfully connected to the Identity Exchange Hub!

3.1.2.2 Connecting a Service Provider to the Identity Exchange Hub

Service Providers (organizations providing applications for access through the Identity Exchange Hub) follow a more unique, individualized process to connect. The MiHIN Identity Exchange Hub Administrator will work directly with each Service Provider to configure the Identity Exchange Hub and the Service Provider's application to enable connectivity. The two parties will exchange metadata files and the Service Provider will provide a list of all attributes the application accepts including the attributes that are required for a user to access the application.

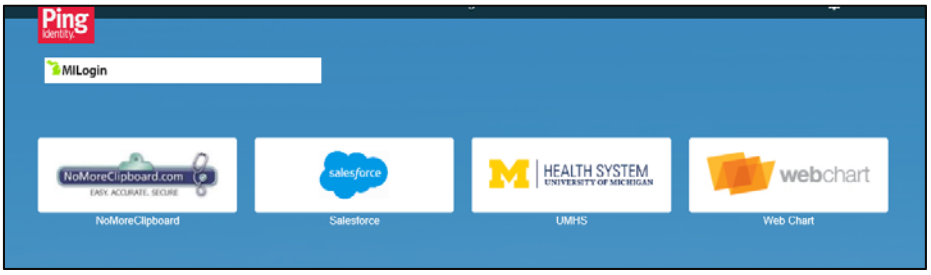
To initiate connectivity as a service provider, please contact help@mihin.org.

3.1.3 Initial Technical Connectivity Testing

3.1.3.1 Testing connectivity between Identity Exchange Hub and Identity Provider

Before testing connectivity with the Identity Exchange Hub please make sure you have added the Ping Identity Single Sign-On portal to your web portal. This process will be covered in the initial onboarding kickoff meeting.

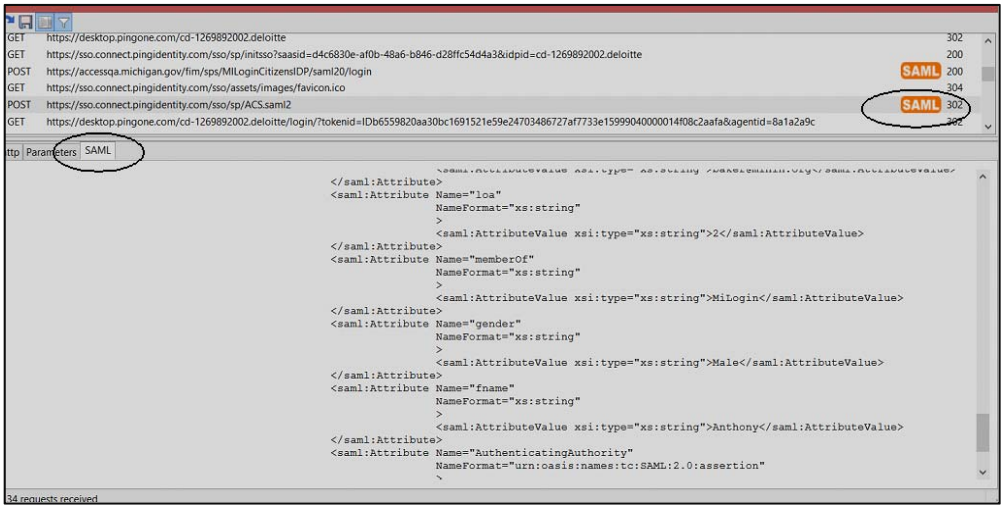
Once the Ping Identity Single Sign-On portal is added to your web portal, simply log on to the Ping portal from your web portal. The Ping Identity portal should look similar to the below screen shot. *NOTE: The applications shown on this page will depend on which applications have been configured for the user's group as designated by the Identity Provider. To learn about configuring groups please review the End to End Testing section of this document.*



Screen 21: Example Login Page for Ping Identity Single Sign-On Portal

3.1.3.2 Connectivity Troubleshooting

If you are having connection issues with PingOne you can use tools such as the SSO tracer add-on for Firefox, https://addons.mozilla.org/En-us/firefox/addon/sso-tracer/. After launching the SSO Tracer from the tools menu, reattempt the connection that failed in Firefox. In the SSO Tracer window that opened when launching the application, you should see all of the HTTP(S) traffic from the Firefox browser including the SAML. This can be a useful tool to verify the correct information is being transmitted. If you need help interpreting this information contact help@mihin.org.



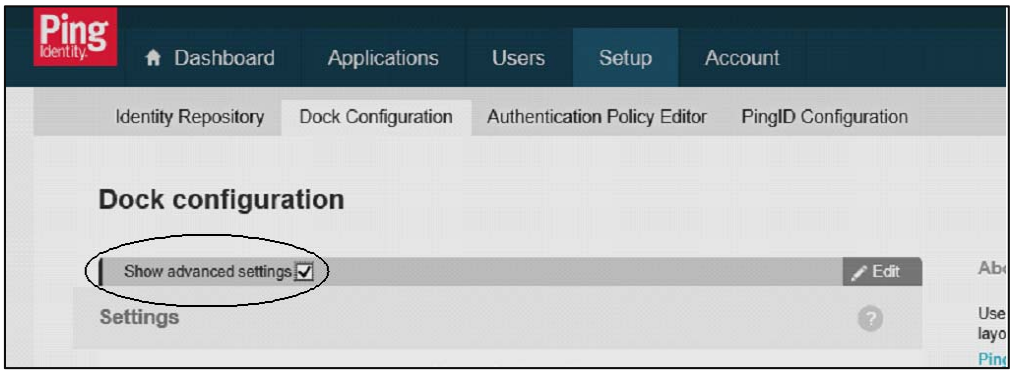
Screen 22: Metadata display from SSO Tracer add-on for Firefox

3.1.3.3 End-to-End connectivity testing from Identity Provider to Service Provider

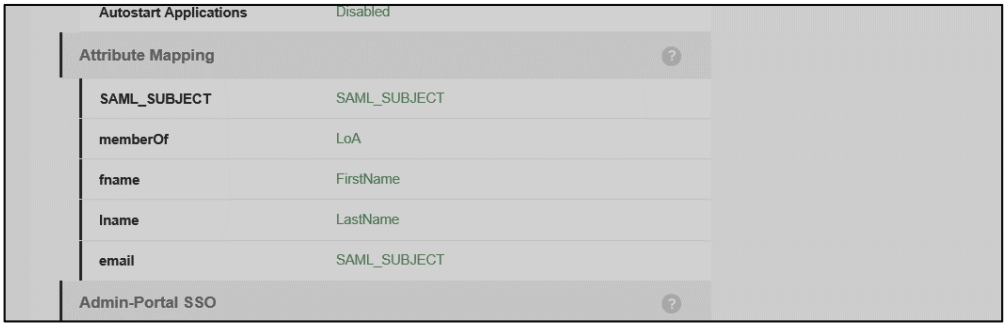
Go to the "Setup" tab in the PingOne admin portal and then click on the Dock Configuration subtab as shown in Screen 23 below. Select the check box to 'Show Advanced Settings.'

This will display the attributes that need to be mapped as shown in Screen 24 below so you can correct any discrepancies with the default attribute mappings to match the names of the attributes being sent by the Identity Provider.

NOTE: Values might not be the same – names/attributes from each identity provider may be different, and must be mapped to PingOne.

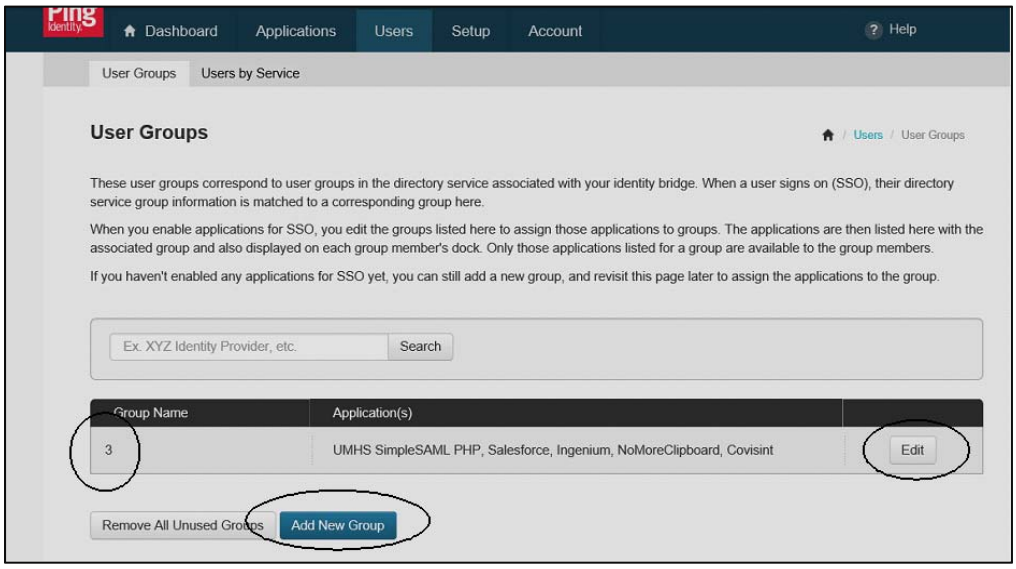


Screen 23: Dock Configuration



Screen 24: Advanced Settings

Next you will need to define and configure your user groups, starting with the group name. A valid group name is the value passed in the "memberOf" attribute shown in the previous screen. Select the Users tab, and the User Groups sub-tab in that section to edit or add new User Groups.

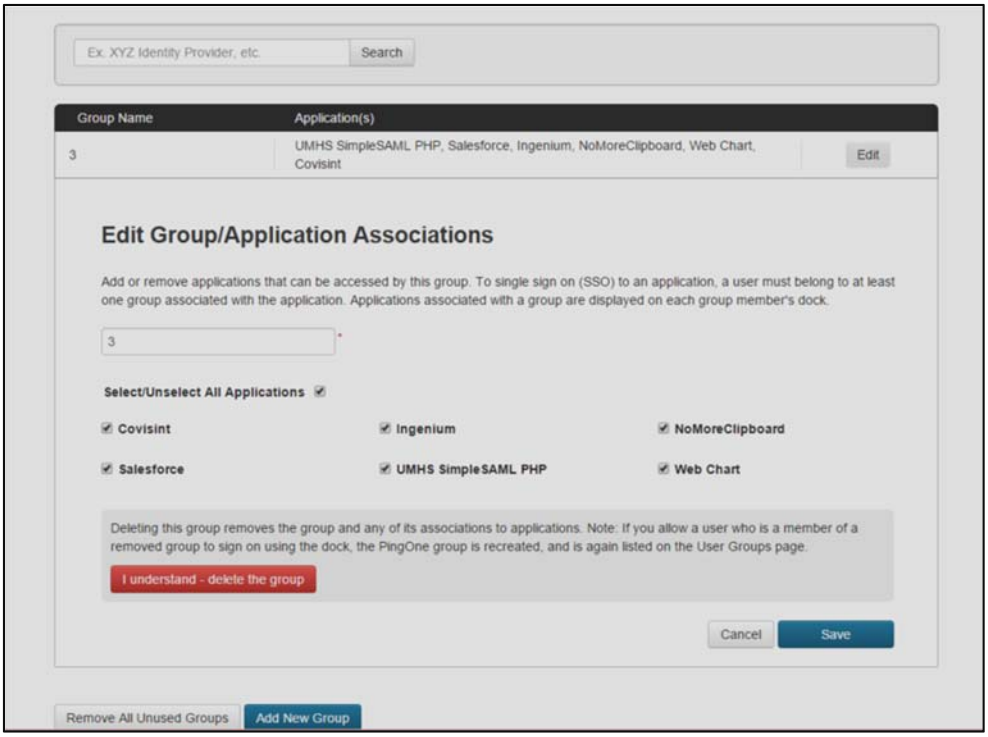


Screen 25: User Groups

If not all possible values of the "memberOf" attribute are covered by the current list of group names, a new group can be added using the "Add New Group" button. You can add or remove access to applications within a group by using the "Edit" button.

NOTE: All of these values and attributes are case sensitive.

Verify that all test groups to be used for end-to-end testing have the corresponding test Service Provider Application listed in the correct group under the "User Groups" tab. Identity Providers are invited to connect with Service Provider Applications by the MiHIN Identity Exchange Hub Administrator and the process to configure each of the applications is the same as the process outlined in **Section 3.2** below.



Screen 26: Editing Group Application Permissions

The Identity Provider can restrict access to certain applications on a group level by selecting 'Edit' for the group on the 'User' page, and deselecting any application the group should not be able to access.

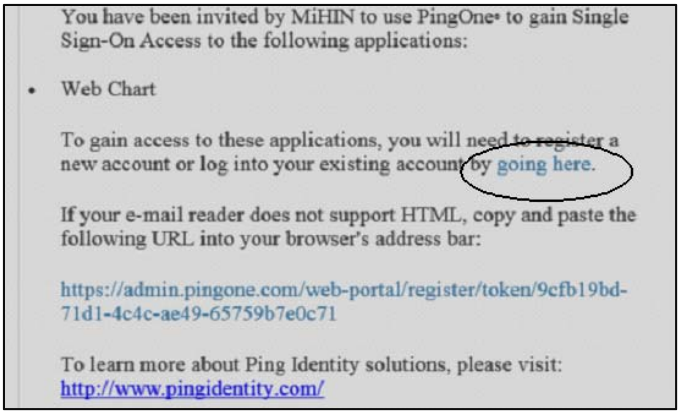
NOTE: To continue testing, please make sure the test identity you are using is in the correct group with the correct application assigned to that group.

A successful connection will allow the user to open the target application being used for end-to-end testing from the Ping Single Sign-On Portal and the user will be automatically signed in to that application. In case of issues, please follow the same troubleshooting procedures with Firefox's SSO Tracer described in Section 3.1.3.2 to verify all mappings were correct and the proper attributes are being sent.

NOTE: If the test application does not support Just In Time account creation, users would need to already possess an account with the Service Provider Application that they are trying to access for instant login to that application.

3.2 Onboarding Additional Applications

Once a new application is added to the SSO Use Case, the MiHIN Identity Exchange Hub Administrator will send invitations to Identity Providers to add the new application to their User Groups. The Identity Provider's administrator for the Ping portal will receive an email containing a link that will initiate configuration of the new application.


You have been invited by MiHIN to use PingOne• to gain Single Sign-On Access to the following applications:

- Web Chart

To gain access to these applications, you will need to register a new account or log into your existing account by going here.

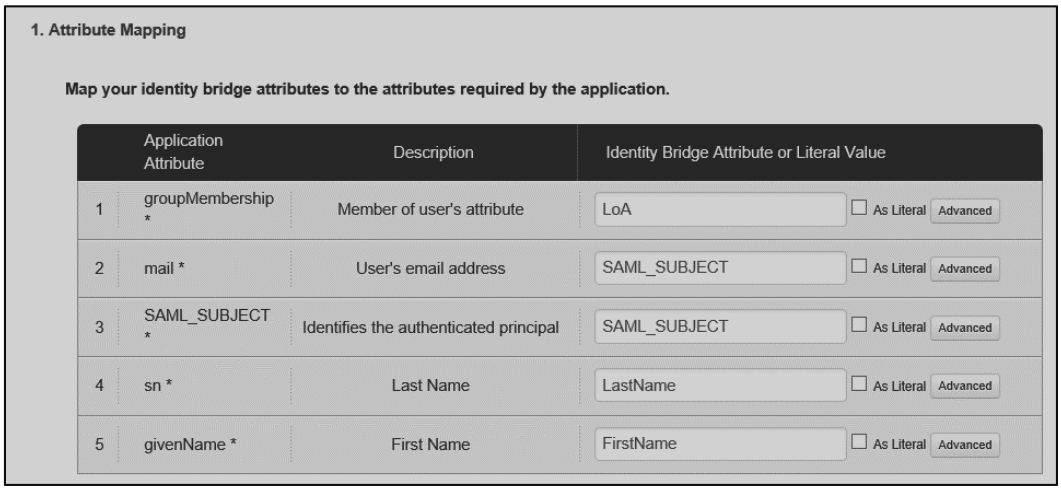
If your e-mail reader does not support HTML, copy and paste the following URL into your browser's address bar:

https://admin.pingone.com/web-portal/register/token/9cfb19bd-71d1-4c4c-ae49-65759b7e0c71

To learn more about Ping Identity solutions, please visit:
http://www.pingidentity.com/

Screen 27: New Application Invitation Email

The Identity Provider's administrator will be asked to confirm names of the Identity Provider's Attributes that are mapped to the Service Provider's Application Attributes.


1. Attribute Mapping

Map your identity bridge attributes to the attributes required by the application.

	Application Attribute	Description	Identity Bridge Attribute or Literal Value
1	groupMembership *	Member of user's attribute	LoA ☐ As Literal Advanced
2	mail *	User's email address	SAML_SUBJECT ☐ As Literal Advanced
3	SAML_SUBJECT *	Identifies the authenticated principal	SAML_SUBJECT ☐ As Literal Advanced
4	sn *	Last Name	LastName ☐ As Literal Advanced
5	givenName *	First Name	FirstName ☐ As Literal Advanced

Screen 28: Attribute Mapping for New Application

Once the mapping configuration to the new Service Provider Application is complete, the Identity Provider's Administrator should follow steps under **Section 3.1.3.3 End-To-End testing from Identity Provider to Service Provider** above to ensure all fields are properly configured.

4 Resources and Specifications

4.1 Identity Issuance and Authentication

This section is intended to provide requirements for identity proofing and authenticating an individual based on the National Institute of Standards and Technology (NIST) Levels of Assurance (LoA) as outlined in NIST 800-63-2.

The notion of Level of Assurance is an important concept for Participating Organizations (POs) that have signed the Single Sign-On Use Case Agreement. POs are

required to understand the Levels of Assurance outlined in NIST 800-63-2 and to ensure all requirements and procedures outlined in the specification are followed. Other POs are making decisions based on the Level of Assurance indicated in the attributes of a transaction, so it is imperative that all POs use the NIST 800-63-2 specification when determining if their policies, procedures and implementation warrant a certain level of assurance. Sections 5, 6 and 7 of NIST 800-63-2, which discuss the requirements for Identity Issuance and Identity Proofing, Tokens, and Authentication and Credential Management respectively, should be fully understood by users of this Implementation Guide.

4.1.1 Assurance Level 0

No assurances are being made about the identity of the user in any way.

4.1.2 Assurance Level 1

No identity proofing claims are made about the user but some assurance is provided that the person who created the account is the same as the person accessing the account now. At level 1, online guessing and replay attacks should be prevented. For more information about the security requirements for level 1 refer to NIST 800-63-2.

4.1.2.1 Authentication

The authentication mechanism used by the provider offers some assurance that the same Claimant who participated in previous transactions is accessing the protected transaction or data. Assurance level 1 allows a wide range of available authentication technologies to be employed and permits the use of any of the token methods of Levels 2, 3, or 4 specified in NIST 800-63-2. If a token is used, successful authentication requires that the Claimant prove through a secure authentication protocol that the he or she possesses and controls the token.

4.1.3 Assurance Level 2

Identity proofing is required for assurance level 2 and above before issuing the identity. Identity proofing can be performed in person or remotely. In addition to preventing against attacks mentioned in level 1, level 2 should also address eavesdropper attacks. For more information about the security requirements for level 2 refer to NIST 800-63-2.

4.1.3.1 Identity Proofing

In-Person Identity Proofing: Applicant must possess a valid current primary government picture ID that contains the Applicant's picture and either address of record or nationality of record. Registration Authority inspects photo ID and compares picture to Applicant. Credentials are issued in a way to confirm claimed address or phone number.

Remote Identity Proofing: Applicant must possess a valid current government ID number and a financial or utility account number. Registration Authority (RA) inspects

both ID and account (e.g. for correct number of digits). The RA must verify either the government ID or account number via record checks, and confirm the personal information in the records are consistent with the application and sufficient to identify a unique individual. Utility account number verification can be done by verifying knowledge of recent account activity. RA also verifies through online video that ID picture matches applicant.

4.1.3.2 Authentication

Level 2 provides single factor remote network authentication. A wide range of available authentication technologies can be employed at Level 2. For single factor authentication, Memorized Secret Tokens, Pre-Registered Knowledge Tokens, Look-up Secret Tokens, Out of Band Tokens, and Single Factor One-Time Password Devices are allowed at Level 2. This level of assurance also permits any of the token methods of Levels 3 or 4. If using a token, successful authentication requires that the Claimant prove through a secure authentication protocol that he or she controls the token. Online guessing, replay, session hijacking, and eavesdropping attacks are resisted. Protocols are also required to be at least weakly resistant to man-in-the-middle attacks as defined in Section 8.2.2 of NIST 800-63-2.

Long-term shared authentication secrets, if used, are never revealed to any other party except Verifiers operated by the Credential Service Provider (CSP); however, session shared secrets may be provided to independent Verifiers by the CSP. In addition to Level 1 requirements, assertions are resistant to disclosure, redirection, capture and substitution attacks. Approved cryptographic techniques are required for all assertion protocols used at Level 2 and above.

4.1.4 Assurance Level 3

Identity proofing is required for assurance level 3 before issuing the identity. Identity proofing can be done in person or remotely. In addition to preventing against attacks mentioned in level 1 and 2, level 3 should also should address verifier impersonation and man-in-the-middle attacks. For more information about the security requirements for level 3 refer to NIST 800-63-2.

4.1.4.1 Identity Proofing

In-Person Identity Proofing: Applicant must possess a valid current primary government picture ID that contains the Applicant's picture and either address of record or nationality of record. Registration Authority inspects photo ID, compares picture to Applicant, verifies via the issuing agency, and confirms that the personal information matches that of the application. Credentials are issued in a way that confirms claimed address or phone number.

Remote Identity Proofing: Applicant must possess a valid current government ID number and a financial or utility account number. The RA must verify both the government ID and account number via record checks, and confirm the personal

information in the records are consistent with the application and sufficient to identify a unique individual. Utility account number verification can be done by verifying knowledge of recent account activity. RA also verifies through online video that ID picture matches applicant. At a minimum the records check of both the government ID number and account number should confirm the name and address of the applicant. Credentials are issued in a way to confirm the ability of the applicant to receive messages at the verified physical or electronic address.

4.1.4.2 Authentication

Level 3 provides multi-factor remote network authentication. At least two authentication factors are required. Level 3 authentication is based on proof of possession of the allowed types of tokens through a cryptographic protocol. Multi-factor Software Cryptographic Tokens are allowed at Level 3. This level of assurance also permits any of the token methods of Level 4. Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token against compromise by the protocol threats for all threats at Level 2 as well as verifier impersonation attacks. Various types of tokens may be used as described in Section 6 of NIST 800-63-2.

Authentication requires that the Claimant prove, through a secure authentication protocol, that he or she controls the token. The Claimant unlocks the token with a password or biometric, or uses a secure multi-token authentication protocol to establish two-factor authentication (through proof of possession of a physical or software token in combination with some memorized secret knowledge). Long-term shared authentication secrets, if used, are never revealed to any party except the Claimant and Verifiers operated directly by the CSP; however, session shared secrets may be provided to independent Verifiers by the CSP. In addition to Level 2 requirements, assertions are protected against repudiation by the Verifier.

4.1.5 Assurance Level 4

Identity proofing is required for assurance level 4 before issuing the identity and must be done in person. In addition to preventing against attacks mentioned in levels 1, 2 and 3, level 4 should also should address session hijacking attacks. For more information about the security requirements for level 4 refer to NIST 800-63-2.

4.1.5.1 Identity Proofing

In-Person Identity Proofing: Applicant must possess a valid current primary government picture ID that contains the Applicant's picture and either address of record or nationality of record, and a second independent Government ID, document or financial account number. Registration Authority inspects photo ID, compares picture to Applicant, verifies via the issuing agency, and confirms that the personal information matches that of the application. The RA will verify the financial account number or inspect the secondary government ID and confirm that the personal information is

consistent with the primary photo ID. RA records a current biometric of the applicant. Credentials are issued in a way that confirms address of record.

4.1.5.2 Authentication

Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that only "hard" cryptographic tokens are allowed. The token is required to be a hardware cryptographic module validated at Federal Information Processing Standard (FIPS) 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. Level 4 token requirements can be met by using the PIV authentication key of a FIPS 201 compliant Personal Identity Verification (PIV) Card.

Level 4 requires strong cryptographic authentication of all communicating parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that the Claimant prove through a secure authentication protocol that he or she controls the token. All protocol threats at Level 3 are required to be prevented at Level 4. Protocols shall also be strongly resistant to man-in-the-middle attacks. Long-term shared authentication secrets, if used, are never revealed to any party except the Claimant and Verifiers operated directly by the CSP; however, session (temporary) shared secrets may be provided to independent Verifiers by the CSP. Approved cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process.

At Level 4, "bearer" assertions (as defined in Section 9 of NIST 800-63-2) are not used to establish the identity of the Claimant to the Relying Party (RP). "Holder-of-key" assertions (as defined in Section 9) may be used, provided that the assertion contains a reference to a key that is possessed by the Subscriber and is cryptographically linked to the Level 4 token used to authenticate to the Verifier. The RP should maintain records of the assertions it receives, to support detection of a compromised verifier impersonating the subscriber.

4.2 General Requirements

Every provider taking part in the Single Sign-On Use Case must be able to communicate with the Ping Identity PingOne Cloud Access Service. More information on the technical requirements for a Provider to connect with PingOne can be found at: https://www.pingidentity.com/content/dam/pic/downloads/resources/data-sheets/pingone-data-sheet.pdf .

Currently PingOne allows connections from providers using the following methods:

1. Any SAML 2.0 enabled identity management platform
2. PingFederate
3. AD Connect

4. Other connection options available on request, may require additional charges

The provider must be aware of the levels of assurance outlined in NIST 800-63-2. The provider is responsible that the method of connecting to the Identity Exchange Hub meets all the requirements outlined in the NIST specification to prevent against the different types of attacks for the highest Level of Assurance transaction the Provider will make.

4.2.1 Logging Requirements

4.2.1.1 Participating Organization

Participating Organization shall, at a minimum, log the following information:

(i) Date and time Message Content was exchanged and identity (e.g., unique identifier) of individual or system, as applicable, accessing the Message Content;

(ii) Date and time Message Content was transmitted through the Identity Exchange Platform and identity of individual or system, as applicable, transmitting the Message Content;

(iii) Unique message identifier for the Message Content accessed, sent, or received;

(iv) Message Content accessed;

(v) Verification of the user attributes exchanged with any Federated Organization; and

(vi) Any failures, or network events.

4.2.1.2 HIN

HIN shall, at a minimum, log the following information:

(i) Name of Participating Organization accessing the Identity Exchange Platform;

(ii) Identity of the Principal (e.g., unique identifier) making an access request to a Federated Organization;

(iii) Date and time the access occurred;

(iv) Source IP address of the request;

(v) Any applicable error messages received from a Federated Organization or the Identity Exchange Platform.

Except as provided in the foregoing, HIN shall not be obligated to maintain and shall not be responsible for either maintaining records of the content of any Message exchange between the Parties or inspecting the content of such Messages.

4.2.1 Additional Standards Organizations

4.2.1.1 National Institute of Standards and Technology (NIST)

NIST 800-63-2 covers the "Registration, Credential Issuance and Maintenance" profiles for "E-Authentication" as standard guidelines. Section 5.3.1 defines the general requirements per assurance level and Table 3 defines the "Identity Proofing Requirements."

It is recommended that reviewers of this implementation guide refer to the Executive Summary of NIST 800-63-2 for definitions of the four (4) levels of assurance as most patient data exchanges will most likely, after risk assessment, require an LOA Three.

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf;

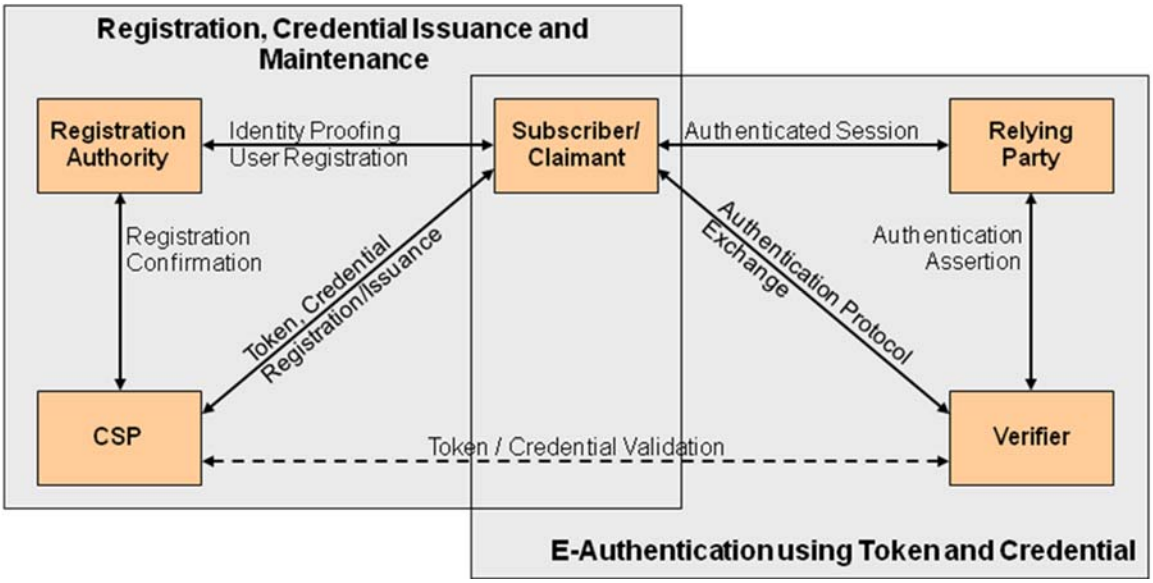


Diagram One: Overview of Credential Issuance and e-Authentication

It is further recommended that readers of this implementation guide also review "Identity Proofing" in Section 5, "Cryptographic keys"(certificates) in Section 6, "Token and Credential Management" in Section 7 and finally, SAML Assertions (2.0) in Section 9.

All useful NIST 800 series, Computer Security Profiles, such as NIST 800-30, "Guides for Conducting Risk Assessments" can be found at:

http://csrc.nist.gov/publications;

It is recommended that reviewers focus on Chapter Two of the "Guides for Conducting Risk Assessments", which defines the Fundamentals of the Risk Assessment Process and Chapter Three which illustrates the process of preparing the risk assessment, conducting the assessment, communicating the assessment, and maintaining the assessment.

Each "risk" should systemically generate a "value," which quantifies the level of risk to the organization, from which can be assigned a level of assurance relative to NIST 800-63-2.

Steps for determining the values of the risk assessment are defined in Section 2.4.3 "Risk Assessments at the Information Tier" and for those wishing further guidance, NIST 800-30 provides a recommendation to review NIST 800-37, "Risk Management Framework." However, NIST 800-30 provides the necessary information for conducting a risk assessment and NIST 800-37 is optional.

NIST 800-145 and NIST 800-76-2 are recommended for those interested in NIST "SOA Cloud Standards." For those implementing HIPAA Security Rules, a basic working resource and knowledge of "HIPAA Security Rules", NIST 800-66 - Revision 1 is highly recommended.

4.2.1.2 International Organization for Standardization (ISO)

Review of ISO standards is optional for implementers but you may find ISO 27002 useful as it is a collection of best practices for information security management which have been agreed upon by organizations nationally. The focus is on confidentiality, (Authorized access), integrity, (Accuracy of data) and availability (Authorized users have access).

Reviewers are recommended to focus on Section 2, which pertains to the scope of the standard. Section 3 provides best practice guidance on malware, backup, logging, monitoring, control of operational software, vulnerabilities, and audit. Section 6 is for information security in supplier relationships and supplier service delivery systems.

4.3 SAML Attributes

4.3.1 List of Attributes

To participate in the Single Sign-On Use Case, you will need to transmit the following attributes:

	User Attributes List:	Required for IdP to Send
1	First Name	Yes
2	Middle Initial	No
3	Last Name	Yes
4	Display Name	No
5	Street Address	No
6	City	No
7	State	No
8	Zip Code	No
9	Email Address	Yes
10	Direct Address	No

11	Phone Number	No
12	Date Of Birth	Yes
13	SSN	No
14	Assurance Level	Yes
15	Role	Yes
16	Group Name	Yes
17	Unique Identifier	No
18	NPI Number	No
19	Common Key Service	No
20	Gender	No

4.3.2 Attribute Definitions

4.3.2.1 First Name

The user's legal first name.

4.3.2.2 Middle Initial

The initial of the user's middle name. If the user has multiple middle names this will be the initial of the first middle name.

4.3.2.3 Last Name

The user's legal last name.

4.3.2.4 Display Name

The display name for the user, may also be called username.

4.3.2.5 Street Address

A street address where the user receives mail.

4.3.2.6 City

The city where the user receives mail.

4.3.2.7 State

The two-letter State abbreviation where the user receives mail.

4.3.2.8 ZIP Code

The five digit ZIP code where the user receives mail.

4.3.2.9 Email Address

An email address where the user can be contacted.

4.3.2.10 Direct Address

A Direct Secure Messaging Address issued to the user by an accredited HISP that allows for secure transfer of email.

4.3.2.11 Phone Number

A primary 10-digit phone number where the user can be contacted.

4.3.2.12 Date of Birth

The date when the user was born in MM/DD/YYYY format.

4.3.2.13 SSN

The last four digits of the user's Social Security Number.

4.3.2.14 Assurance Level

A number between 0 and 4 that represents the Level of Assurance that the Identity Provider authenticates that the person is who they claim to be. Please view section 4.1 for detailed information about the requirements for each level.

4.3.2.15 Role

The type of position the user has at the organization. Can be used with Assurance Level to determine the type of access a user gets to a service provider's application. The current valid roles are "Provider" and "General."

4.3.2.15.1 PROVIDER

The "Provider" role is used for a healthcare professional (e.g. a doctor of medicine or osteopathy, podiatrist, dentist, chiropractor, clinical psychologist, optometrist, nurse practitioner, nurse-midwife, clinical social worker, etc.) who is authorized to practice by the State and performing within the scope of their practice as defined by State law.

4.3.2.15.2 GENERAL

The "General" role is used for any person who does not meet the requirements for any of the other roles contained in this section.

NOTE: Additional roles may be added

4.3.2.16 Group Name

This value is used to allow access to different applications in the Ping portal. An Identity Provider can limit access to certain applications to only users of certain groups. The values of these attributes must match the configuration in the Ping portal under the groups tab.

4.3.2.17 Unique Identifier

An identifier that is used by the Identity Provider to uniquely identify the user.

4.3.2.18 NPI Number

A ten-digit National Provider Identifier assigned by the Centers for Medicare and Medicaid services.

4.3.2.19 Common Key Service

The Common Key is a system identifier used for patient matching to help identify individuals.

4.3.2.19 Gender

A value indicating the gender of the user, valid values are: “Male,” “Female,” “Other,” and “Unknown.”

4.3.3 Just In Time Account Creation

Applications can be configured to support Just In Time (JIT) account creation (automatic account provisioning). When a user from a participating Identity Provider logs in to an application that supports JIT account creation for the first time from the Identity Exchange Hub, an account for that application is automatically created for the user. The creation of the account would only occur if all data points in the SAML attributes are properly conveyed to the service provider, which may include attributes marked as not required, but which are required for initial account creation.

For example one application could potentially have marked only half of the attributes as required to log in to an existing account, but if the application also supports JIT account creation it may require all of the optional attributes to be populated to create a new account.

The Service Provider has the right to limit JIT account creation to transactions with a minimum level of assurance or other limiting factors, including but not limited to user role. Assuming the requirements are met there is no need to have any prior account set up with the participating services when logging in via the Identity Exchange Hub for the first time.

NOTE: If additional attributes or information need to be captured beyond what is available in attributes list, the Service Provider is responsible for providing a mechanism to capture the additional attributes.

5 Troubleshooting

A list of common questions and issues regarding the Ping Identity PingOne Cloud Access Service can be found at:

https://ping.force.com/Support/PingIdentityCommunityHome

If experiencing difficulties or have questions, please contact the MiHIN Help Desk:

Email: help@mihin.org
Phone: (517) 336-1430
Monday – Friday 8:00 AM – 5:00 PM (Eastern)

6 Legal Advisory Language

This reminder applies to all Use Cases covering the exchange of electronic health information:
The Trusted Data Sharing Organization Agreement (TDSOA) establishes the legal framework under which Participating Organizations can exchange messages through the HIN Platform, and sets forth the following approved reasons for which messages may be exchanged:

(a) By health care providers for Treatment, Payment and/or Health Care Operations consistent with the requirements set forth in HIPAA;
(b) Public health activities and reporting as permitted by HIPAA and other Applicable Laws and Standards;
(c) To facilitate the implementation of "Meaningful Use" criteria as specified in the American Recovery and Reinvestment Act of 2009 and as permitted by HIPAA;
(d) Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the Message or such individual's personal representative in accordance with HIPAA;
(e) By Data Sharing Organizations for any and all purposes, including but not limited to pilot programs and testing, provided that such purposes are consistent with Applicable Laws and Standards; and
(f) **For any additional purposes as specified in any Use Case, provided that such purposes are consistent with Applicable Laws and Standards**.

Under the DSA, "***Applicable Laws and Standards***" means all applicable federal, state, and local laws, statutes, acts, ordinances, rules, codes, standards, regulations and judicial or administrative decisions promulgated by any governmental or self-regulatory agency, including the State of Michigan, the Michigan Health Information Technology Commission, or the Michigan Health and Hospital Association, as any of the foregoing may be amended, modified, codified, reenacted, promulgated or published, in whole or in part, and in effect from time to time. "Applicable Laws and Standards" includes but is not limited to HIPAA; the federal Confidentiality of Alcohol and Drug Abuse Patient Records statute, section 543 of the Public Health Service Act, 42 U.S.C. 290dd-2, and its implementing regulation, 42 CFR Part 2; the Michigan Mental Health Code, at MCLA §§ 333.1748 and 333.1748a; and the Michigan Public Health Code, at MCL § 333.5131, 5114a.

It is each QO's obligation and responsibility to ensure that it is aware of Applicable Laws and Standards as they pertain to the content of each message sent, and that its delivery of each message complies with the Applicable Laws and Standards. This means, for example, that if a Use Case is directed to the exchange of physical health information that may be exchanged without patient authorization under HIPAA, the QO must not deliver any message containing

health information for which an express patient authorization or consent is required (e.g., mental or behavioral health information).

Disclaimer: The information contained in this implementation guide was current as of the date of the latest revision in the Document History in this guide. However, NIST policies are subject to change. Therefore, links to any source documents have been provided within this guide for reference. MiHIN applies its best efforts to keep all information in this guide up-to-date. It is ultimately the responsibility of the Participating Organization and Sending Facilities to be knowledgeable of changes outside of MiHIN's control.