



Inbound athenaNet Single Sign-On

Integration Form

athenahealth, Inc.

Version 18.12 Published December 2018

# Completing This Document

## Scope Review and Approval

Please read the entire Integration Form and complete all form fields and check-boxes to the best of your ability. Should you have questions about the configuration options presented in this document please do not hesitate to discuss with your project engineer.

When this document is completed to your satisfaction, please approve the scope by typing your name below.

I,      , agree to the integration design as described here in this document.

Date:

# Project Information

Please fill the following out to the best of your ability for this Inbound athenaNet Single Sign-On (SSO) project.

|  |  |
| --- | --- |
| General Information |  |
| athenahealth Practice Name: | Click here to enter text. |
| athenahealth Practice Context ID: | Click here to enter text. |
| athenahealth Project Engineer: | Click here to enter text. |
| athenahealth Project Engineer Contact Information: | Click here to enter text. |
| Event Number (for internal athenahealth tracking): | Click here to enter text. |

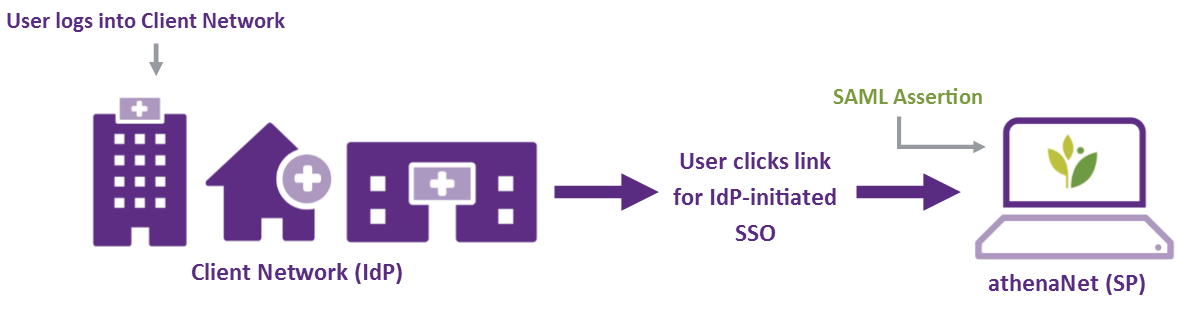
|  |  |  |  |
| --- | --- | --- | --- |
| Client Information | | | |
| Contact | Role | Details | |
| Project Business Contact | Responsible for overall success of the project | Name: |  |
| Phone: |  |
| Email: |  |
| Project Technical Contact | Responsible for SSO configuration on client side | Name: |  |
| Phone: |  |
| Email: |  |

# Product Description

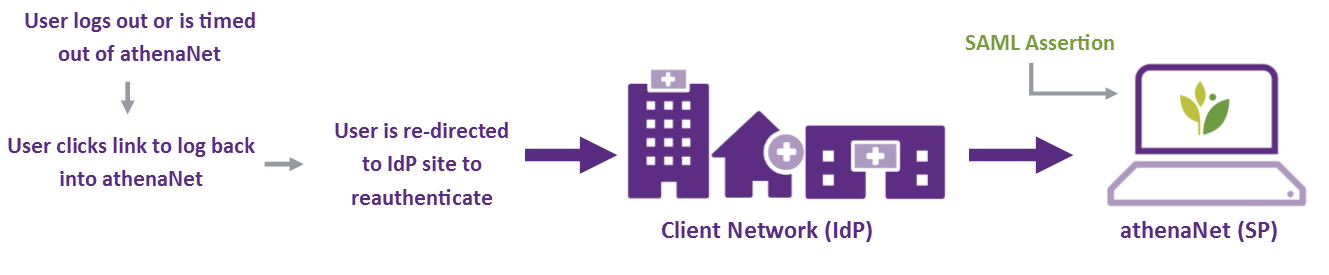
## Inbound athenaNet Single Sign-On

**Inbound athenaNet Single Sign-On (SSO)** enables users to log into a third-party system (Identity Provider, IdP) and gain access to athenaNet (Service Provider, SP) without being prompted to enter athenaNet credentials. Athenahealth uses Security Assertion Markup Language 2.0 (SAML 2.0) for this offering and therefore **compliance with SAML 2.0 is required**.

### IdP-Initiated SSO



### SP-Initiated SSO



### Additional Functionality

|  |  |
| --- | --- |
| Consideration | Description |
| User Auto-Provisioning | This offering does not support federated user auto-provisioning. |
| The practice will still need to create new users in athenaNet, adding their ID mapping, and correctly managing user changes or removals. |
| Access & Timeout | SSO users will no longer be able to log into athenaNet using their athenaNet credentials. |
| Users will only be able to log into athenaNet if they are coming from the IdP system. |
| If users log out, are timed out or attempt to access athenanet.athenahealth.com from the general Internet, they will be presented a screen informing them that their account requires SSO authentication and a link for SP-initiated SSO. |
| Support Environments | This SSO workflow is enabled for all athenaNet environments that your practice uses. |
| This includes environments such as Production, Preview, ClientTrain, and Backup (backup.athenahealth.com), the read-only edition of athenaNet. |
| We cannot make SSO-related environment-specific changes to the configuration. |
| These all use one connection in our federation server, meaning we cannot make environment specific changes to the configuration |
| Environment-specific URLs | There will be one URL per athenaNet environment. It is the practice’s responsibility to appropriately manage and distribute these URLs to your user base. The standard URLs provided will land users on the athenaNet department selection screen and then homepage. |
| 2FA/MFA | With inbound SSO, two-factor authentication policies can be managed in the IdP system. Athenahealth does not currently offer 2FA for standard athenaNet login to clients regardless of access via SSO or standard login. |

# Application Configurations

## User Population

The **Single Sign-On** practice setting can be changed in order to control the user population to which the SSO applies:

|  |  |  |
| --- | --- | --- |
| Preference | Setting | Description |
|  | ON | Single Sign-On enabled for all users without exception  ON is recommended |
| ADMINONLY | Single Sign-On enabled only for users with the SSO Authentication Permission. |
| Please provide a business reason for this decision: |
| Practice staff are responsible for controlling the SSO workflow on a per-user basis. |
| This setting is leveraged during testing. To ensure this setting only affects designated test users, please confirm that no users have the SSO Authentication permission: |

## EPCS Single Sign-On Workflow

Do your providers use athenaClinicals E-Prescribing of Controlled Substances (EPCS) functionality? If ‘No’, skip to the next section.

Per regulations, EPCS always requires two-factor authentication where the user must fully re-authenticate. While the second factor is always a Symantec time-based token, with this integration the **first factor authentication method can be modified**.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. athenaNet Visit | ►  ►  ► | 2. First-Factor Authentication | | ►  ►  ► | 3. Second-Factor Authentication | 4. athenaNet Visit |
| Provider begins EPCS Workflow | ON | Provider redirected to IdP system for credentials | Symantec time-based token | Provider continues EPCS Visit Workflow |
| OFF | Provider enters credentials in athenaNet iFrame |

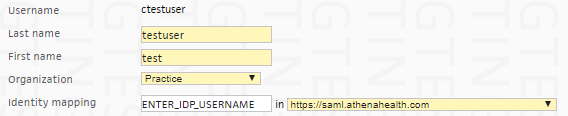
Given the workflow options above, please confirm the desired setting below.

|  |  |  |
| --- | --- | --- |
| Preference | Setting | Considerations |
|  | ON – IdP credentials for EPCS | Providers do not need to keep track of their athenaNet credentials. |
| The EPCS SSO Amendment to MSA must be signed and returned. Please provide the following: |
| The Directory Service used by your system:  If ‘Other’, please specify: |
| OFF – SP credentials for EPCS | Provider can still change athenaNet password, however EPCS first-factor authentication accepts expired athenaNet passwords |

**EPCS PRACTICE SETTING:** This setting is applied at the tablespace-level and affects all EPCS providers.

## User Identity Mapping

In order to set up users for single sign-on, athenaNet usernames will need to be mapped to usernames from the Identity Provider system. To facilitate this new step, a new field, “Identity mapping” will be added to the User Admin console (Gear >> User >> Users) allowing practice staff to update the upstream username to the user (ENTER\_IDP\_USERNAME value in screenshot below).



**MAPPINGS:** athenaNet does not support one-to-many user identity management and, therefore, all IdP usernames must have one active athenaNet username in order to access the correct athenaNet user account.

**If there are fewer than 100 active SSO users in the tablespace**, practice staff will need to manually add the mappings in athenaNet Production.

**If there are more than 100 active users in the tablespace**, your project engineer can perform a username mapping import. A partially completed spreadsheet workbook containing the username, first name, last name and email of your tablespace users along with a column where user mappings may be entered will be provided. Once completed by practice staff, your project engineer will import these prior to bringing the single sign-on live for your tablespace.

## Provisioning and Testing Process

Athenahealth uses Okta as its identity management platform for federation. To equip your practice with SSO, your practice's IdP will need to be linked to the Okta platform by an exchange of metadata and configurational testing. The technical setup will be done by your SSO resource alongside the athenahealth project engineer.

Unlike other interfaces, Inbound-to-athena SSO testing, begins in athenaNet Production. This process avoids User Admin changes that refresh nightly from athenaNet Production to support environments. If critically important, we can make accommodations to test in Preview prior to Production.

To mitigate the risk, the SSO Practice Setting is set to ADMINONLY during testing and only designated dummy test users (or users without critical athenaNet workflows available for testing) are given the SSO Authentication Role and are mapped to the IdP connection.

## Additional Comments

Please use this section for any additional questions or comments related to this integration.