



Outbound athenaNet Single Sign-On

Integration Form

athenahealth, Inc.

Version 18.8 Published: August 2018

# Table of Contents

[Table of Contents 2](#_Toc520120089)

[Completing This Document 3](#_Toc520120090)

[Scope Review and Approval 3](#_Toc520120091)

[Project Information 4](#_Toc520120092)

[Product Description 5](#_Toc520120093)

[Outbound athenaNet Single Sign-On 5](#_Toc520120094)

[Workflow Overview 5](#_Toc520120095)

[IdP-Initiated SSO 5](#_Toc520120096)

[Project Tasks 5](#_Toc520120097)

[Tablespace Configuration 6](#_Toc520120098)

[Link Display Name 6](#_Toc520120099)

[Link Location 6](#_Toc520120100)

[Link Filtering 6](#_Toc520120101)

[Additional Comments 6](#_Toc520120102)

[Technical Configuration 7](#_Toc520120103)

[Metadata Exchange 7](#_Toc520120104)

[Service Provider Configurations 7](#_Toc520120105)

[Single Logout Functionality (SLO) 7](#_Toc520120106)

[IdP-Initiated SLO 7](#_Toc520120107)

[SP-Initiated SLO 8](#_Toc520120108)

[Attribute Mappings 8](#_Toc520120109)

[SAML Signature Policy 8](#_Toc520120110)

[Signing Certificate 8](#_Toc520120111)

[SAML Encryption Policy 8](#_Toc520120112)

# 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 interface design as described here in this document.

Date:

# Project Information

Please fill the following out to the best of your ability for this Outbound athenaNet Single Sign-On 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 Contact 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

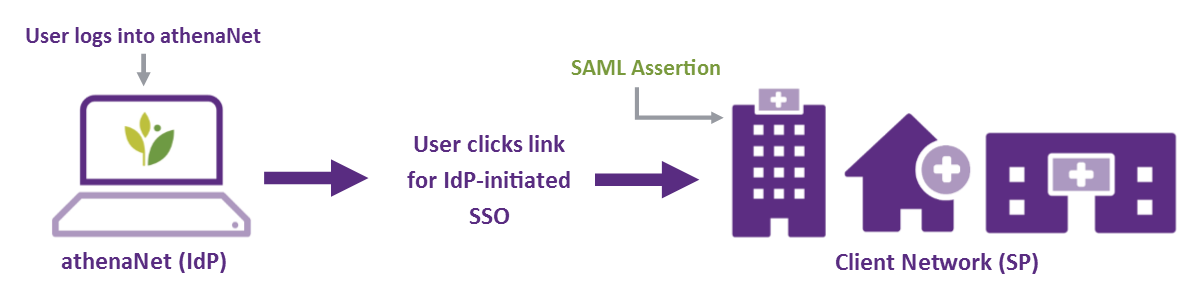
## Outbound athenaNet Single Sign-On

The **Outbound athenaNet Single Sign-On (SSO)** offering enables users to log into athenaNet and then access a third-party application without manually reentering user credentials. Athenahealth acts as the Identity Provider (IdP) and the third-party application is the Service Provider (SP). Athenahealth also uses the Security Assertion Markup Language 2.0 (SAML 2.0) standard for this Single Sign-On functionality, and therefore **compliance with SAML 2.0 is a requirement for this offering**.

**This offering only includes IdP-Initiated SSO**, meaning the user starts in athenaNet and from there can access the third-party system. Please note that athenahealth can only send your users’ athenaNet usernames and the Service Provider will need to maintain a mapping of user IDs in their system.

Workflow Overview

IdP-Initiated SSO



## Project Phases

|  |  |
| --- | --- |
| Phase | Actions |
| Scope | Review product features and options, exchange metadata and e-sign Integration Form |
| Build | Athenahealth (IdP) and the SP system build SAML 2.0 application integrations |
| Test | Functional testing, end-user validation & training (if applicable) in preview.athenahealth.com |
| Go-Live | Sign Go-Live Authorization and promote testing configurations to Production/LIVE systems |
| Monitoring | Long-term monitoring moved to Integration Network Monitoring (INM) and Customer Support Center (CSC) |

# Tablespace Configuration

## Link Location

In athenaNet, the link that users will click to access the third-party system can be either Patient Level, appearing on the Chart and/or Quickview, or Document Level, appearing on the header of clinical documents. From the Quickview, the link will be accessible from “Medical files” within the Registration Information section. From the Chart, the link will be accessible by expanding the menu found in the upper right-hand corner of the chart  and selecting “Third Party Applications”.

Please select from this list of options where you would like the link to be surfaced to users in athenaNet.

|  |  |
| --- | --- |
| Patient vs Document (choose one) | |
|  | Patient Level – Quickview and Chart |
|  | Patient Level – Quickview Only |
|  | Patient Level – Chart Only |
|  | Document Level |
|  | Document Level – linked to one Results Interface. Specify the interface or trading partner here: |

## Link Display Name

Use this section to enter the name of the link that users will see in athenaNet.

Click here to enter text.

## Link Filtering

You have the option to apply filtering to the link so that it only displays for users in certain departments or provider groups. The default and recommended option is to have no filtering which would mean the link would be accessible to all users in your tablespace.

|  |  |
| --- | --- |
| Filter Options (choose one) | |
|  | No Filtering (Default) |
|  | Provider Group Filtering  Filter only for the following Provider Groups: |
|  | Department Filtering  Filter only for the following Departments: |
|  | Provider Filtering  Filter only for the following Providers: |

## Additional Comments

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

# Technical Configuration

## Metadata Exchange

Are you able to provide your SAML metadata to your athenahealth Project Engineer in an .xml file (preferably via secure encrypted email)?  Yes is strongly recommended

**TIMELINE:** Providing metadata significantly expedites the build and trust establishment process by streamlining configuration. Your athenahealth Project Engineer will provide athenahealth’s IdP metadata once the connection has been created.

If you are able to provide metadata (answered ‘YES’ above), please skip the following section.

If you answered ‘NO’ above and are unable to provide metadata, please complete the remaining sections.

## Service Provider Configurations

|  |  |
| --- | --- |
| Item | Entry |
| Server Entity ID |  |
| Base URL |  |
| ACS Endpoint URL |  |
| IdP-Initiated SLO Endpoint URL |  |
| SP-Initiated SLO Endpoint URL | If applicable, provided by athenahealth |

**EXPLANATION OF TERMS**:

**Server Entity ID**: This is the unique identifier that will be put in the ‘audience restriction’ in the SAML response. If you’re not providing metadata and aren’t sure what this value should be, athenahealth strongly recommends that this value be a URL without spaces containing the domain name of the Service Provider.

**Base URL**: This is only required if you are providing a relative ACS URL that builds off the base.

**Assertion Consumer Service (ACS) Endpoint URL**: This is the URL that we will post the SAML assertion to for an SSO request. This can be an absolute URL, or a relative path referring to the base URL.

**IdP-Initiated Single Logout (SLO) Endpoint URL**: This is the URL where athena will post the SAML assertion to for an SLO request.

**SP-Initiated Single Logout (SLO) Endpoint URL:** This is the URL provided by athena that will post the SAML assertion to athena from the third-party portal for an SLO Request. Please work with your athenahealth Project Engineer to obtain the SLO endpoint needed to complete the SP-Initiated SLO.

## Single Logout Functionality (SLO)

By default, SLO functionality is not enabled, and therefore logging out of athenaNet would not impact the user’s browser session in the Service Provider’s system, and likewise logging out of the Service Provider’s system would have no impact on the user’s athenaNet session.

### IdP-Initiated SLO

With this option enabled: when a user logs out or is timed out of athenaNet, athena will post an SLO message to the Service Provider’s logout endpoint URL, with the expectation that the SP would then end the user’s session in their system as well.

Please indicate here if you would like to enable IdP-Initiated SLO:

### SP-Initiated SLO

With this option enabled: when a user logs out or is timed out of the third-party application, then athena would expect to receive an SLO message from the Service Provider, posted to our logout endpoint URL. Upon receipt, the user would be logged out of athenaNet as well.

Please indicate here if you would like to enable SP-Initiated SLO:

## Attribute Mappings

Below is a list of available data fields that athenaNet can send to the Service Provider system as attributes in the SAML assertion to support user authentication.

Please use this table to indicate which attributes you would like to receive:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| athenaNet Attribute Name | Description | Include | SAML\_SUBJECT (select one) | Alternative Attribute Name |
| subject | User’s athenaNet Username |  |  |  |
| email | User’s email address |  |  |  |
| fullName | User’s full name |  |  |  |
| firstName | User’s first name |  |  |  |
| lastName | User’s last name |  |  |  |
| practiceid | athena Context ID |  |  |  |
| departmentid | athena Department ID |  |  |  |
| patientid | athena Enterprise ID |  |  |  |
| extraidentifier | Custom field in client tablespace.  Custom Field Name:  OR  User Identity Mapped from Inbound-to-athena SSO |  |  |  |
| Static Text | Static text value(s) |  |  |  |

## SAML Signature Policy

Select here whether you need athena to always post signed SAML assertions. By default, this will not be enabled and the SAML assertions will not be signed.

Please select the desired SAML signature policy:

## Signing Certificate

By default, athenahealth uses RSA SHA256 as our signing algorithm. If desired, we could use SHA384 or SHA512 instead. Please indicate here which signing algorithm you would like used for this connection:

## SAML Encryption Policy

Select here whether you need athena to post and receive encrypted SAML assertions. By default, this additional encryption is not enabled.

Please select the desired SAML encryption policy:

If you select the option to encrypt only certain attributes, please list the attributes here: