



Connectivity Methods Overview

athenahealth, Inc.

Version 18.10 Published: February 2019

athenaClinicals® Service

Q3 2013 Edition

athenahealth, Inc.

Published: July 2013

1. Table of Contents

[1 Table of Contents 2](#_Toc524955299)

[2 Connectivity Methods 3](#_Toc524955300)

[2.1 athena-Hosted SFTP 3](#_Toc524955301)

[2.2 Locally-Hosted SFTP 4](#_Toc524955303)

[2.3 Establishing a VPN 5](#_Toc524955304)

[2.3.1 VPN Socket 6](#_Toc524955305)

[2.3.2 FTP Through VPN 6](#_Toc524955306)

[2.4 Webservices 7](#_Toc524955304)

[2.4.1 Continuity of Care Document Exchange 7](#_Toc524955305)

[2.4 athenaLightning 7](#_Toc524955302)

3 Specialized Connectivity Methods 8

3.1 Report-Based Interfaces 8

3.2 Webservices 8

3.2.1 Continuity of Care Document Exchange 8

1. Connectivity Methods

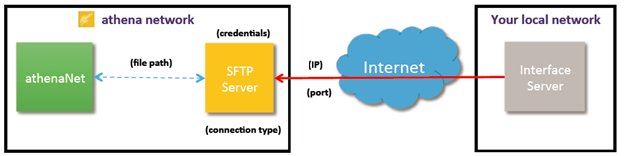
As part of interface implementation, athenahealth will need to establish a secure method of transfer for electronic data to and from a third party system. Please note that not all options will be available for all interface types. For questions, please contact your Interface Project Engineer.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | athena Hosted SFTP | Locally Hosted SFTP | VPN Socket | VPN FTP | Webservices | athena Lightning |
| Secure | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Easy to Troubleshoot | ✓ | ✓ | ✓ | ✓ |  |  |
| Easy Setup  *(Separate connectivity specialist not required)* | ✓ | ✓ |  |  |  | ✓ |
| Real-Time Transmission |  |  | ✓ |  | ✓ | ✓ |
| Maintained Solely by athena | ✓ |  |  |  |  |  |
| athena Infrastructure Only | ✓ |  |  |  |  |  |

* 1. athena-Hosted SFTP

These connections are initiated externally by the client or third-party system to a SSH-FTP server in athenahealth’s data center. The client or third-party system is provided with an athena-issued DNS name, username, and password. Once the client-initiated SSH tunnel is established, the client is able to securely transfer files to or from athenahealth.

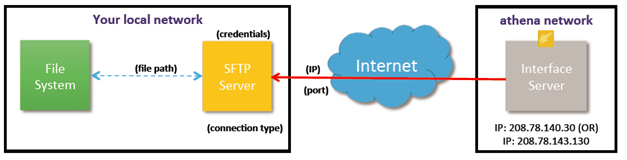
**Integration examples:** Bi-directional HL7v2 exchanges



* 1. Locally-Hosted SFTP

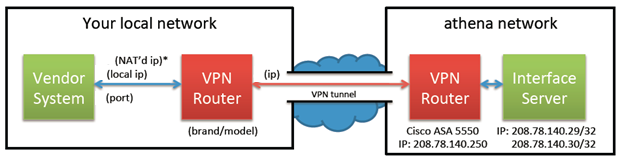
athenahealth can initiate outbound connections to a third-party or client-hosted SSH2 server. The client provides an IP (or DNS name), username, and password for athenahealth to initiate an outbound SSH connection. Once the SSH tunnel is established we can exchange files locally using SFTP.

**Integration examples:** Bi-directional HL7v2 exchanges, DWF, Reports, Flatfiles



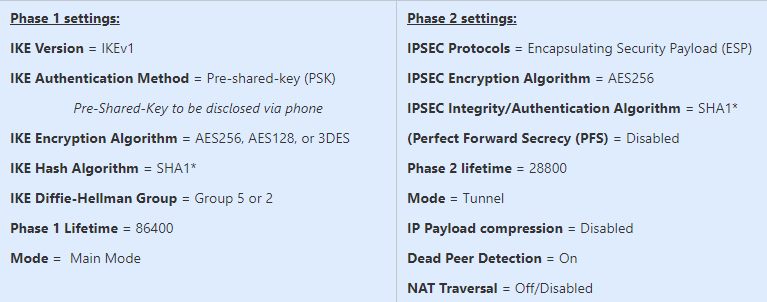
* 1. Establishing a VPN

athenahealth network operations staff can work to establish a point-to-point VPN tunnel (sometimes referred to as site-to-site) between two networks as needed. Once the VPN is in place we can perform file based transfers through plain FTP or run an HL7-receiver / HL7-sender (MLLP TCP/IP socket based transfers). Coordination of VPN staff on both the athenahealth and remote side will add additional time to the project.



\* **NAT routing** – athenahealth requires your network to either provide a public host IP or be configured to NAT your private host IP address to another private IP address athena will provide in order to avoid IP overlaps within our network. If you do not have access to network engineering resources to configure a NAT or do not wish to NAT your traffic, we recommend a standardized connectivity method rather than VPN

**VPN Setup Call** – Your network’s VPN and NAT configurations should be complete and tested prior to the VPN setup call. Failure to complete configuration prior to this call will lead to substantial delays in establishing connectivity.



Additional VPN Requirements

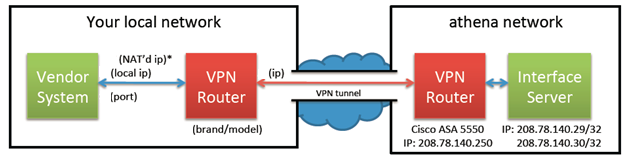
1. Must provide public addresses for all hosts OR have the ability to perform static 1:1 NAT between private addresses
2. Must be able to define all hosts in encryption domain (endpoint interface servers) with /32 IP addresses.
3. If multiple hosts are required to be in the VPN tunnel, the firewall must be able to define interesting traffic with non-consecutive /32 IP addresses.

Unsupported Configurations

1. IKEv2
2. IKEv1 Aggressive mode
3. ANY Phase 1 / Phase 2 settings outside of those set forth by athena
4. Perfect forward secrecy (PFS)
5. NAT traversal (NAT-T)
6. Multiple hosts defined as a subnet (All hosts must be defined separately with a /32 mask)
   * 1. VPN Socket

Another way of sending or receiving data through a VPN is via MLLP TCP/IP socket based connections. This is accomplished by running an HL7-sender on one end of the tunnel and an HL7-listener on the other end. The source system always runs the “sender” while the receiving (consuming) system always runs the “listener.”

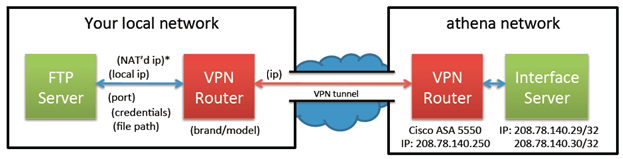
**Integration examples:** Bi-directional HL7v2 exchanges, Flatfile



* + 1. FTP Transfer Through VPN

This option requires an established VPN and client-hosted FTP server. The client provides an IP (or DNS name), username, and password for athenahealth to initiate an outbound FTP connection. Once the connection is in place we can securely and automatically transfer files to and from the client-hosted FTP server.

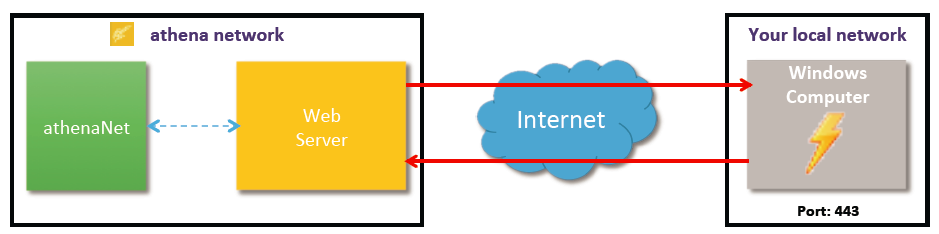
**Integration examples:** Bi-directional HL7v2 exchanges, Flatfile



2.5 athenaLightning

athenaLightning is a program that can be downloaded and installed inside of a third-party network. It opens an SSL tunnel out to athenahealth and supports file-based data transfers to and from other applications running inside the client-network.

**Integration examples:** Bi-directional HL7v2 exchanges, Flatfile, File Transfer



1. Specialized Connectivity Methods

The connectivity methods outlined in this section are specific to the following interface types.

* 1. Report-Based Interfaces

For many report-based interfaces, such as Data Warehouse Feed and Outbound Automated Reports, locally-hosted SFTP is the only supported connectivity method.

3.2 Webservices

Web Services is a connectivity type that depends on the World Wide Web and most commonly HTTP. Interfaces such as Single Sign-On, XDS.b (ex. C-CDA), or athenaLightning, leverage web services protocols and standards. In order to complete a Web Services connection, endpoints (URLs similar to those for API calls) from the client are needed. While these endpoints provide the destination of the data, certificates (certs) provide authentication and encryption. In order to facilitate message interoperability, headers or wrappers specified by protocol such as SOAP are found at the beginning of the payload.

3.2.1 Continuity of Care Document Exchange

Continuity of Care Document Exchange connectivity methods will be dependent on the transfer method selected in the Interface Scoping Questionnaire. For XDS.b, XDR and PIX Query transactions web service endpoints must be used. In these instances, the following connectivity worksheets should be used:

* *For XDS.b*: Connectivity Worksheet: XDS.b for Continuity of Care Document Exchange
* *For XDR or PIX or other web services connections*: Connectivity Worksheet: Web Services