



---

## Connectivity Implementation Guide

---

Version 2.0, March 2015

---

*Document History*

<b>Version</b>	<b>Date</b>	<b>Update Origin</b>	<b>Written by</b>	<b>Verified by</b>
1.00	3/25/2011	Initial Draft	Mike DeAlto	Sue Merk
1.08	11/03/11	Final for customer use	Sue Merk	Sue Merk
2.0	3/4/15	Updated information for connectivity methods, provisioning and onboarding.	Kelly Llewellyn	Sue Merk



## Table of Contents

1	Overview .....	4
1.1	Purpose .....	4
1.2	Intended Audience.....	4
2	AS2 Protocol, Communication and Certificate Handling with the HIE .....	4
2.1	AS2 Standard Protocol .....	5
2.2	Communication.....	5
2.3	Certificate Handling .....	7
3	Connectivity to the HIE .....	7
3.1	Activator Connectivity Gateway Software (Synchrony Endpoint Activator) .....	8
4	Sending and Receiving Messages using the Activator .....	15
4.1	Activator Directories .....	15
4.2	Directory Message Transfer.....	17
4.3	Directory Message Management.....	17
5	Viewing Message Activity in the HIE using the Activator .....	17
5.1	Viewing Message Activity .....	17
6	HIE Operations Change Management .....	24
7	Appendix .....	26
7.1	Detailed Overview of Activator Installation Process.....	26
7.2	Connection Using AS2 Commercial Software .....	33

# 1 Overview

---

Welcome to the OneHealthPort Health Information Exchange (HIE) Connectivity Implementation Guide. Establishing connectivity to the OneHealthPort HIE is the next step in securely exchanging clinical, public health reporting and administrative information with other trading partners.

Unlike traditional, point-to-point connectivity which typically involves deep integration of a data feed between two systems (such as HL7 interfaces), the OneHealthPort HIE supports a connectivity approach that uses a secure communication channel and data encryption to deliver messages to the HIE where messages are then routed to trading partners for intake into their systems. This approach allows trading partners to “connect once” and securely send any number and variety of standard transactions (supported by the HIE) to any number of trading partners in the HIE community.

## 1.1 Purpose

The purpose of this document is to describe the end point connectivity solutions used to securely connect to the OneHealthPort HIE. The connectivity solutions supported by the HIE are:

1. **Connection** to the HIE using an organization’s commercial software that supports the AS2 protocol.
2. **Activator software gateway solution** (Axway’s Synchrony Endpoint Activator) - A self-contained, small-footprint AS2 software application installed in the trading partner’s environment that manages secure message movement between the organization and the HIE B2Bi Hub engine.

## 1.2 Intended Audience

This document is intended for:

- New trading partners requiring information about connectivity to the OneHealthPort HIE.
- Parties responsible for implementing and managing connectivity to the OneHealthPort HIE.

# 2 AS2 Protocol, Communication and Certificate Handling with the HIE

---

The following sections describe the AS2 communication protocol, message flow and certificate handling approach used for trading partners connecting to the OneHealthPort HIE.

## 2.1 AS2 Standard Protocol

The AS2 standard protocol was selected and is used by the OneHealthPort HIE to manage security and exchange of messages between trading partners and the HIE B2Bi Hub engine. Specifically, the AS2 protocol was chosen because it provides the following:

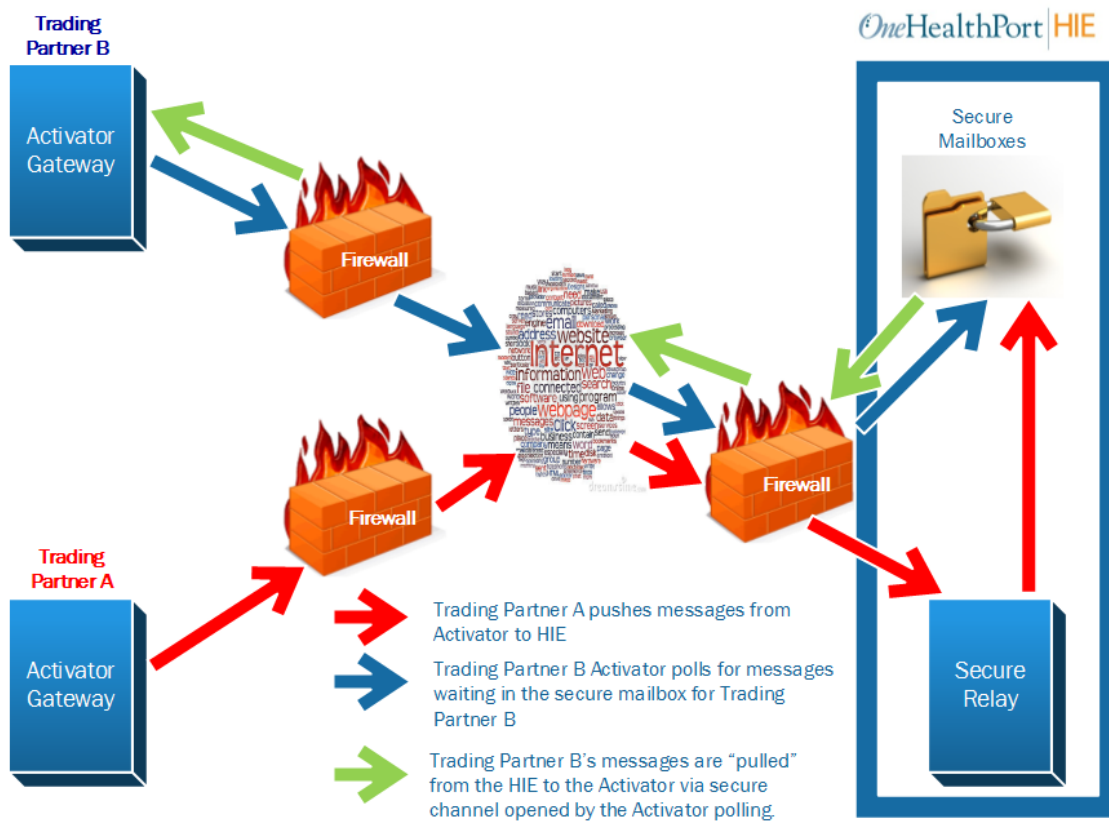
1. **Encryption** - AS2 focuses on encrypting the data, providing end-to-end security. The channel is also encrypted with SSL on top of the payload encryption.
2. **Non-repudiation** - AS2 provides a hashing process to ensure that a file was not tampered with during delivery. It also ensures that a party to a communication cannot deny the authenticity of a message that they originated.
3. **Certificate Management** - AS2 uses digital certificates to ensure that documents are “guaranteed delivery” only to the intended recipient. The certificates also ensure that the messages are secured in transit and that the sender can be verified. Trading partners that use the Activator benefit from certificate management handled by OneHealthPort and a fully automated PKI process between the Activator and the B2Bi Hub engine.
4. **Message Management** - The AS2 standard provides a status message called the Message Disposition Notification (MDN). Because AS2 places a message in an envelope to enable it to be transmitted over the internet, trading partners need to know that the message was successfully extracted from that envelope. After transmission of a message AS2 sends an MDN (receipt) indicating whether the document was successfully or unsuccessfully extracted from the envelope.
5. **Ease of Use and Interoperability** - The AS2 standard was designed specifically for B2B e-commerce transactions over the internet. The Axway B2Bi engine, used by the OneHealthPort HIE, is backed by the Drummond Group, an organization which performs certification testing on all vendor software to verify its interoperability with products from other vendors.

## 2.2 Communication

Trading partners connect and communicate with the OneHealthPort HIE using AS2 over HTTPS. Trading partners will use port 443 for HTTPS, for outbound and inbound communications. The most common setup will have the trading partner initiate by sending (outbound), or retrieving (inbound) for all communications.

1. **Outbound messages**, from the trading partner to the HIE (for delivery to another trading partner), are **PUSHED to the HIE** and received by the HIE.
2. **Inbound messages** from the HIE to the trading partner, are **POLLED** for by the trading partner’s Activator then **PULLED** from an assigned secure web mailbox at the HIE hub. Note: The secure web mailbox is used only for those trading partners using the Activator gateway software.

- If used by the trading partner, the Activator can be set to poll for messages from the secure mailbox at desired intervals.
  - The secure mailbox can be set to notify the Activator when messages are waiting to elicit a “pull”.
  - The Activator is configured with the trading partner’s secure mailbox address during installation of the Activator.
3. All inbound and outbound messages are encrypted until validated and decrypted by the Activator or the trading partner’s AS2 commercial software used for the connection.
  4. All messages **outbound from the trading partner** to the HIE are validated with the signing certificate and decrypted with the sending trading partner’s public key by the HIE programmatically. The messages are programmatically re-encrypted with the receiving trading partner’s public key and digitally signed by the HIE before passing the message to the receiving trading partner’s secure web mailbox (if using an Activator) or to their AS2 commercial software for pickup providing full PKI security.
  5. A small agent on the Activator is used to communicate software upgrades and certificate changes from the HIE. These changes are communicated to and scheduled with trading partners prior to implementation.



## 2.3 Certificate Handling

The certificate generated for trading partner connectivity to the HIE is unique for each partner. The trust relationship is created between each partner and the OneHealthPort HIE through execution of the HIE Participation Agreement.

Each trading partner will only require the certificate of the OneHealthPort HIE to trade with the entire OneHealthPort HIE trading community. The OneHealthPort HIE is designed as a spoke and hub model with a single connection from each participant (trading partner) to the HIE (Hub). Data will flow from the sending party to the HIE Hub and then the data is polled from a designated secure web mailbox by the receiving party.

The following describes the certificate handling when a trading partner (A) sends a document to a trading partner (B) through the OneHealthPort HIE.

1. Trading partner (A) will encrypt the document to be sent with the public key of the OneHealthPort HIE community, and sign the document with their (A) private key.
2. The OneHealthPort HIE will pick up the message and validate the signature using the public certificate of the trading partner (A).
3. Next, the OneHealthPort HIE will programmatically decrypt the message using the OneHealthPort HIE private key.
4. The document will then be programmatically checked for application of business rules such as the application of SOAP/SAML or special message routing rules.
5. After any business rules are applied, the document will be encrypted using the public key of the receiving trading partner (B) and signed with the private key of the OneHealthPort HIE.
6. The receiving trading partner (B) will validate the signature of the OneHealthPort HIE using the public certificate of the OneHealthPort HIE.
7. The receiving trading partner (B) will decrypt the document using their (B) private key.

## 3 Connectivity to the HIE

---

The OneHealthPort HIE supports trading partner connectivity using the AS2 protocol through use of a commercial software connection to the Hub B2Bi engine or through the use of the Activator Synchrony Endpoint gateway software. The information below describes connectivity to the HIE using the Activator software, the most common way trading partners connect to the HIE. Description of the process to connect to the HIE using an organization's commercial software is provided in the Appendix.

## 3.1 Activator Connectivity Gateway Software (Synchrony Endpoint Activator)

Axway's Synchrony Endpoint Activator is a self-contained AS2 software application installed in the trading partner's environment that manages secure message movement between the organization and the HIE B2Bi Hub engine.

The information below provides an overview about Activator implementation, features, system requirements and the installation process.

### 3.1.1 Activator Implementation Overview

The Activator is implemented in the trading partner's environment and is used to manage the following:

1. Inbound and outbound communications with the HIE (using directories on the Activator set up for the Production and UAT environments).
2. Validation of messages – using Public Key Infrastructure (PKI) certificates.
3. Decryption of inbound messages/encryption of outbound messages.
4. Storage of certificates (public signing cert from the HIE, private signing cert for the trading partner) – the trading partner ONLY deals with certificates from the HIE and not all trading partners. The HIE manages all certificates as a service to all trading partners.
5. Retrieving (pulling) of messages from trading partner's dedicated HIE secure web mailbox.
6. Routing of inbound messages to internal systems by message type/routing id.

### 3.1.2 Activator Features

The Activator is a java-based application (connector solution) that securely moves transactions from trading partners to the OneHealthPort HIE B2Bi Hub engine over HTTPS. The Activator also polls the HIE Hub for messages from trading partners and generates acknowledgements back to the sending trading partner if configured to do so.

The Activator uses the self-signed certificates created by the HIE Hub for that specific Activator. The Activator signs an individual message or batch file with a signing certificate and encrypts it with the HIE Hub's key. It then sends the message or file via a SSL encrypted channel to the HIE Hub where it is decrypted with the public key for that Activator and the signed message is verified for that sender. The routing rules are read in the header or meta-data layer of the message and the message is re-signed with the HIE Hub certificate and re-encrypted with the public key of the receiver's Activator before routing to the second party.



Certificates used in the Activator are created when the software package is provisioned for a trading partner and set up for use during installation. This certificate is unique for the trading partner's Activator and can only be used with the OneHealthPort HIE.

### 3.1.3 System Requirements

#### 3.1.3.1 *Minimum Hardware Requirements (for target server Activator hosting)*

- 800MHz or faster Pentium III-class processor
- 512 megabytes RAM, 1 gigabyte is recommended
- 500MB disk space for Activator installation
- 200-400MB disk space for data storage (more if the organization will be moving high volumes of data)
- SVGA monitor
- TCP/IP network interface card
- Local area network (LAN) card (Windows only)

#### 3.1.3.2 *Temporary Directories*

- The temporary directory of the computer or server running the Activator must have enough space to handle the largest messages traded.
- As a rule of thumb, the temporary directory should be 5 times larger than the largest message times the number of messages concurrently being processed.

#### 3.1.3.3 *Operating System Compatibility*

- Windows Server 2008
- Windows Server 2008 - 64-bit
- Windows Server 2008 R2
- Windows Server 2012
- Windows 7 - 32 bit
  
- AIX 5.2, 5.3-OSSP3 and 6.1-OSSP3
  
- HP-UX 11i v2 (PA-RISC)
- HP-UX 11i v3 (IA-64) Itanium
- Red Hat Enterprise Linux 3, 4 and 5
- Red Hat Enterprise 5 - 64-bit
- Solaris 9 (SPARC)
- Solaris 10 (SPARC and x86)
- SUSE Linux Enterprise Server 9 and 10
- SUSE Linux Enterprise Server 11 - 64-bit

### 3.1.3.4 Internet Browser Requirements

- The Activator browser-based user interface and online help supports Microsoft Internet Explorer 9 or later, Chrome and Mozilla Firefox 1.0 or later.
- Pop-up blocking software in browsers may interfere with the use of the Activator. Therefore, it is recommended this blocking software be disabled or uninstalled.

### 3.1.3.5 Port and IP Addresses

The OneHealthPort HIE uses the following IP addresses and ports with the Activator.

- To Install the Activator Software from OHP HIE: onehealthport-provisioning.axwaycloud.com => 54.85.28.83
- To Send/Receive messages to OHP HIE UAT environment: uat-onehealthport.axwaycloud.com => 107.23.97.226
- To Send/Receive messages to OHP HIE PROD environment: onehealthport.axwaycloud.com => 107.21.52.70
- All the traffic between the trading partner and the HIE will be on Port 443. The OneHealthPort HIE won't initiate any connection to the trading partner's network. The connectivity is always initiated from the trading partner via the Activator to the OneHealthPort HIE Hub.

## 3.1.4 Installation Process

The steps outlined below support the Activator installation process:

1. Trading partner submits a OneHealthPort HIE Support Request form to request connectivity set-up using an Activator.

<http://www.formstack.com/forms/?1688456-sjNVJY8V7I>

2. OneHealthPort meets with the trading partner to review system requirements and readiness for installation of the Activator.
3. Activator installation takes approximately 90 minutes. OneHealthPort collects the following information to organize the installation session:
  - a. Name and contact information of the trading partner's team member performing the Activator installation with the OneHealthPort team.
  - b. Several dates/times trading partner is available for the Activator installation session.
  - c. Operating system used on the server (or virtual server) the Activator will be installed on.
  - d. Email address for the trading partner's IT Support Desk (or some other monitored email) that the OneHealthPort Hub engine can send transaction

failure notifications to and that the OneHealthPort HIE Operations Team can use for distribution of system and maintenance notifications.

4. Using information collected from the trading partner interviews, the Activator package is created.
5. During the installation session, the trading partner receives a secure email with a link to download the Activator package.
6. ***Only when directed by the OneHealthPort HIE technical consultant***, the trading partner accesses the software link and begins the Activator software download and installation process. For an overview and step-by-step screenshots of the Activator installation process, please see the Appendix.
7. When the Activator installation process is completed and connectivity is tested, the trading partner will be instructed to change the password to the Activator User Interface. Instructions for changing the Activator password are provided in the following section.
8. Trading partners using the Activator for connectivity to the OneHealthPort HIE will be provided with the *Axway Activator Administrator's Guide* for reference.

### 3.1.5 Changing the Activator Password

Using strong passwords lowers overall risk of a security breach. Therefore, trading partners are strongly recommended to change the password after Activator installation and on regular basis.

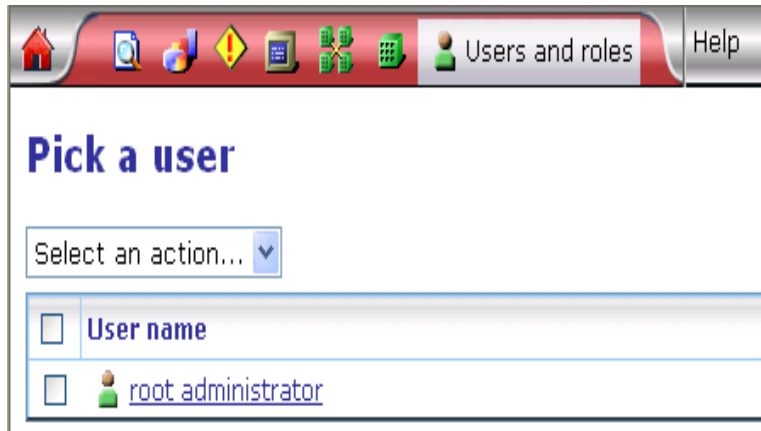
Failing to successfully login to the Activator after three consecutive attempts will lock the user out of the Activator for a period of 15 minutes. If you are unable to recall your password, please submit a OneHealthPort HIE Support Request form for assistance.

To change the password in the Activator, perform the following:

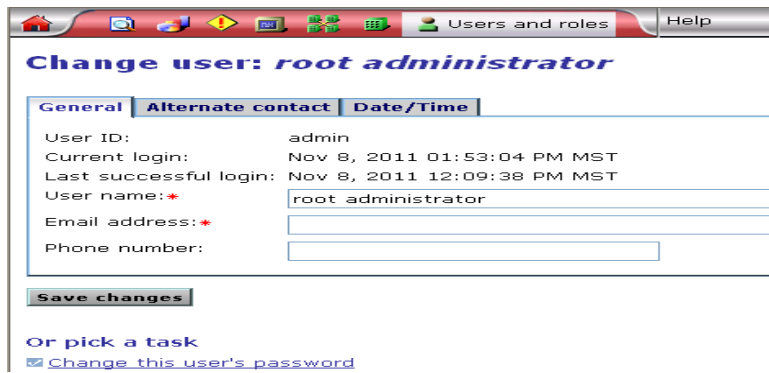
- Sign in to the Activator user interface.
- Click on “User and roles” icon and select “Manage users”. The “Pick a user” screen will appear.



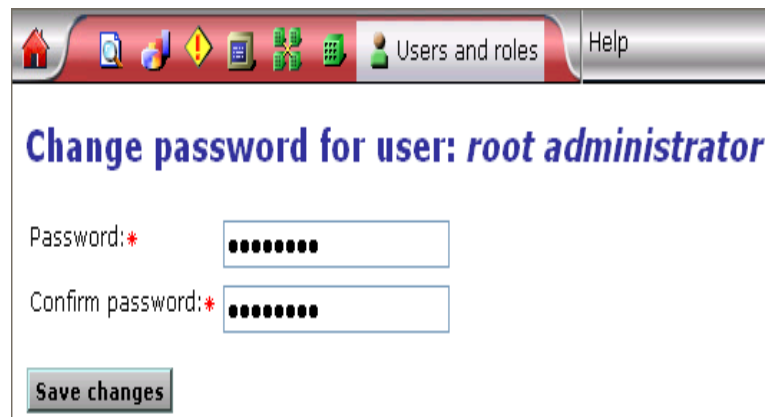
- The user id is “Admin” and user name is “root administrator”. Click on the “root administrator” link. The “Change user: root administrator” screen will appear.



- Click on “Change this user’s password” link. The “Change password for user: root administrator” screen will appear.



- Type the new password twice in the fields and click Save changes. The new password is effective the next time the user logs on.
- Note: Passwords are case sensitive.



Change password for user: *root administrator*

Password:\*

Confirm password:\*

### 3.1.6 Periodic Software Changes and Certificate Updates for the Activator

The Activator software is managed from the OneHealthPort HIE Hub. Software changes typically performed by the Hub include software upgrades to the Activator, a certificate change from the OneHealthPort HIE Hub, and a certificate change needed on the trading partner's Activator.

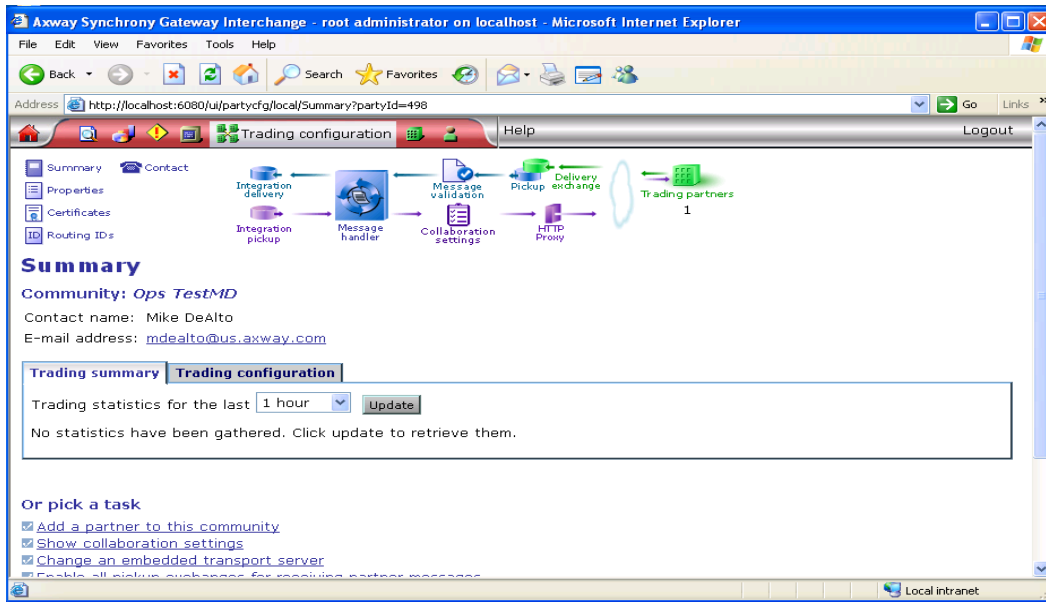
When a change needs to occur to the Activator software, a notification from the OneHealthPort HIE Operations Team will be sent to trading partners providing the following information:

- Purpose of the software change.
- Description of the change and impact to the trading partner.
- Actions or instructions (if any) trading partner need to perform as part of the software change process.
- Date and time for implementation of the change.

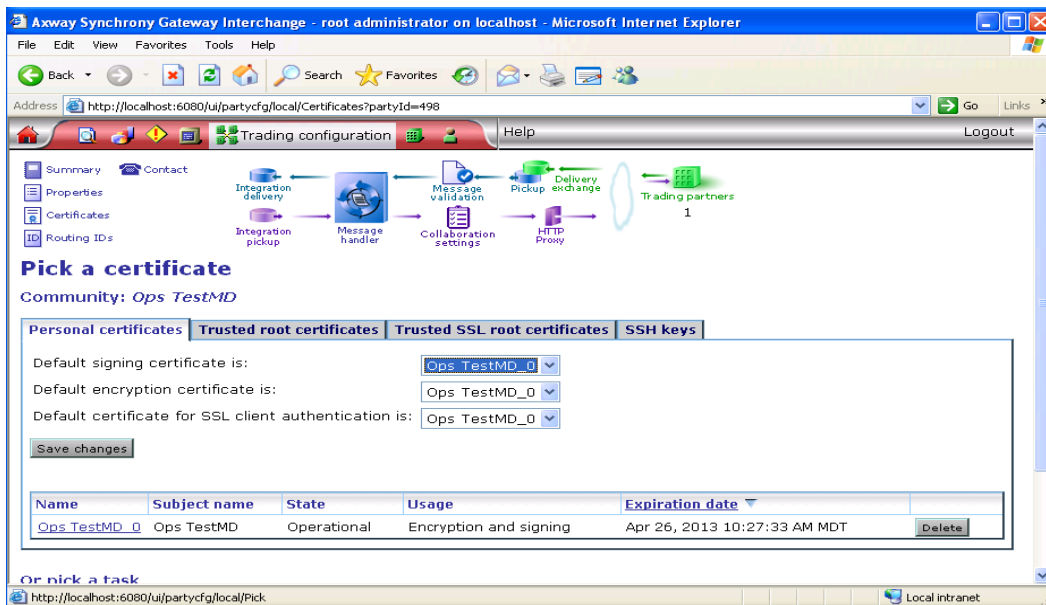
#### 3.1.6.1 Viewing Certificates in the Activator

To view the certificate you will be using to communicate with the OneHealthPort HIE Hub, navigate to the following screen in the Activator user interface.

- 1) Choose the Trading Configuration tab (the 6<sup>th</sup> icon on the top of the screen) and click on the community listed. The following screen will be displayed:

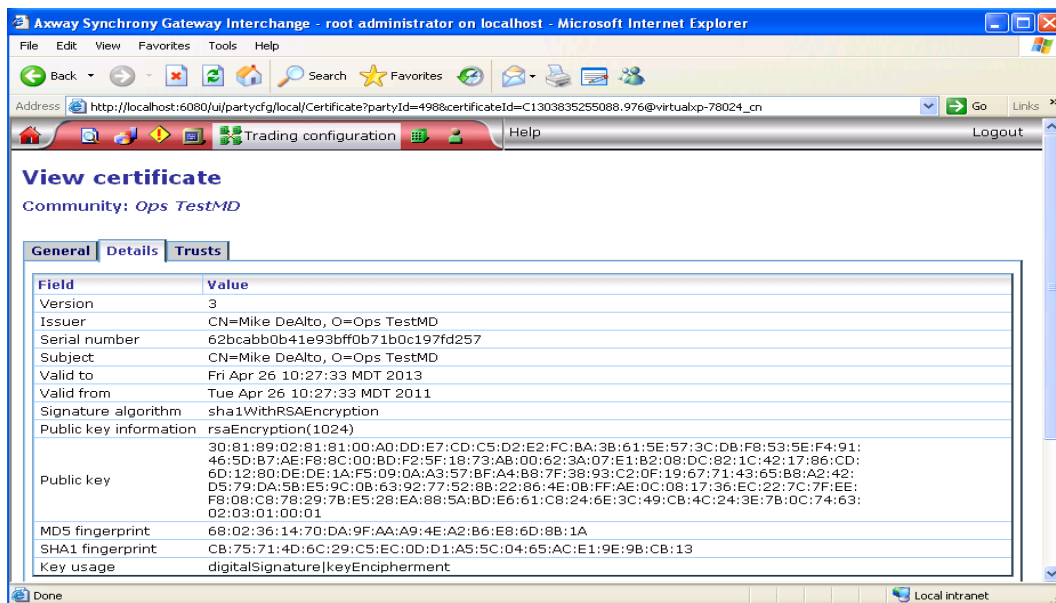


2) Click on the certificate icon on the left side of the screen and the following is displayed:



This is the certificate that is used for Encryption and Signing as stated above. This certificate is named accordingly; the name of the community with underscores ( \_ ) and a zero ( 0 ) at the end. In the above example it is Ops\_TestMD\_0.

3) To display the details, which will show the serial number and other information about the certificate, click on the name which is Ops TestMD\_0 in the above example and select the Details tab. The following will be displayed.



## 4 Sending and Receiving Messages using the Activator

The Activator gateway software uses a directory system for file submission and retrieval. Two directory profiles are set up on the Activator at the time of installation – UAT and Production. Each profile includes an outbound and inbound directory. These directories are linked to the HIE environments the data submissions will pass through to the trading partner.

The user acceptance testing (UAT) environment is used for testing. This environment is HIPAA-compliant and fully secured so production Test data can be used in this environment. Once trading partners have successfully tested transactions, then the data submission for that transaction can be promoted to the Production environment.

### 4.1 Activator Directories

**Outbound** directories are where messages are sent for encryption and submission to the HIE Hub engine then ultimately routed and delivered to the destination trading partner.

**Inbound** directories are where messages from other trading partners arrive for decryption and then are ready to be moved to the appropriate location, i.e. for use in another system, saved to another server or transferred to database.

During installation, the Activator is configured to create a unique sub-directory within the inbound directory structure that organizes incoming messages by document type for streamlined message management.

**Example of Activator directory structure.**

**Production Inbound Directory and Sub-Directories** - Messages from trading partners are delivered to the sub-directories based on document type.

**Production Outbound Directory** - Messages are sent to this directory for delivery through the Production environment of the HIE to the destination trading partner. Sub-folders are not created by document type in this directory because no messages are stored. They are delivered immediately to the HIE Hub engine.



## 4.2 Directory Message Transfer

Any message type supported by the OneHealthPort HIE and used by the trading partner for information exchange can be sent and retrieved through the use of the outbound and inbound directories. Trading partners use various means (programming scripts, parsing scripts etc.) to deliver and retrieve messages from the Activator connectivity solution. A demonstration of how messages can be set up for transfer to and from the directories is provided during the installation process. Trading partners with specific requests for information about message transfer processes can submit a OneHealthPort Support Request form for a technical consultation.

## 4.3 Directory Message Management

The Activator software contains a database designed to assist with short term management of messages flowing outbound to and inbound from the OneHealthPort HIE Hub engine. The Activator database is not equipped to store messages long term. Therefore, operations teams need to establish policies and processes to move messages delivered to inbound directories and sub-directories to appropriate destinations (EMR systems, administrative systems, servers, databases, etc.) within the organization to ensure optimal functionality of the Activator.

# 5 Viewing Message Activity in the HIE using the Activator

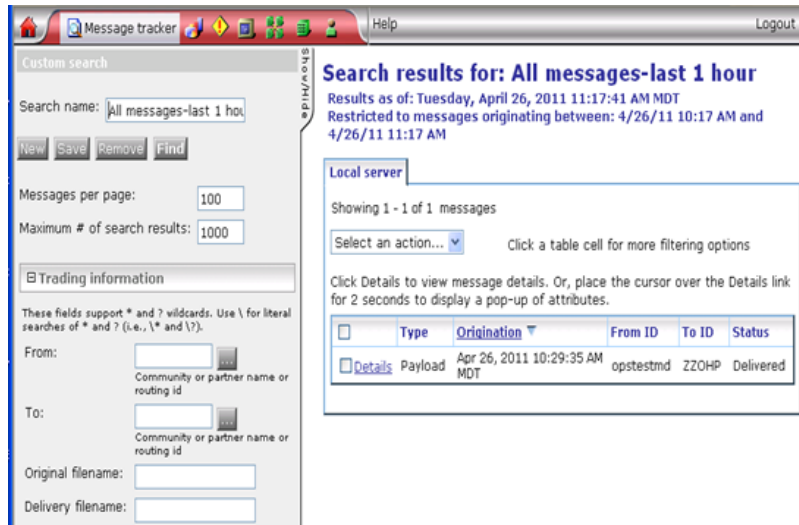
---

Trading partners that use the Activator for connectivity to the HIE can view message activity using the Activator UI and a tool called Message Tracker. This tool can be used to monitor messages sent to the OneHealthPort HIE, the payloads, message receipts and acknowledgements from trading partners.

## 5.1 Viewing Message Activity

To check the status of files sent to the OneHealthPort HIE Hub, click on 'Message tracker' icon located on the top toolbar to open the search page.

**Example of Message Tracker - Custom search is on the left and Search results on the right**

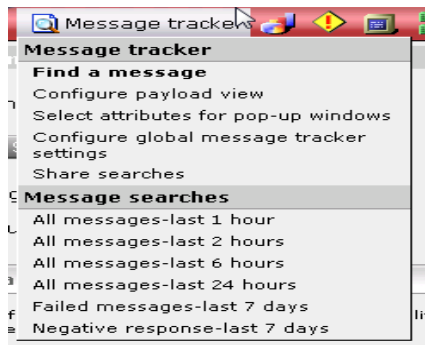


Message activity is retrieved by using 'Default' or 'Custom search' searches.

'Default searches' are located in the 'Message searches' section of the 'Message tracker' menu. These searches are set up to find all messages traded within past hours or days and also to find failed messages or negative responses to messages within a certain number of days.

Messages matching your default search conditions are displayed on the 'Search results' area of the page. When a 'Default search' is selected it changes the values in the 'Custom search' area.

**Message searches found in Message tracker**



Controls on the 'Custom search' panel on the left side of the main 'Message Tracker' page let you search for messages by conditions you specify. Messages matching your search conditions are displayed on the search results area of the page.

**Example of 'Custom search' options**

**Custom search fields:**

**Search name**

- With the Search name field blank, click Find. Messages matching conditions set in the trading information and date areas on the custom search panel are searched for. Once search results are displayed, a name can be typed in the field to identify the search for later use. Click Save. The same search can be run later by selecting Message tracker > [name of saved search] under ‘My searches’ on the menu.

**New**

- New is a clearing function. Use this button to clear the page of search results and begin a new search.

**Save**

- Save lets you save the conditions for a search that was performed and then use the search again at a later date without having to set up the conditions again.
- To save a search, set conditions for a search and click Find to run the search. When the search results are displayed, type a name for the query in the search name field at the top left of the main transaction search page and click Save. To perform a saved search, select Message tracker > [name of saved search] under My searches on the menu.

**Remove**

- Remove deletes the search identified in the search name field from the My searches menu list.

**Find**

- Find searches for all records matching the conditions specified on the search page, if any have been specified. If no conditions are specified, the default action is to search for all messages traded within the number of days specified in the Number of days for default searches field, on the Message Tracker global settings page (see Changing search default settings).

#### Messages per page

- The value of this field is the maximum number of search results to display per search results page. If the number of found messages exceeds the page limit, the results are displayed across multiple pages.
- This maximum can be set on a search-by-search basis.

#### Maximum # of search results

- The value of this field is the maximum number of messages that will return after a search is executed. If a search finds more than this number, the results are trimmed to return only the number up to the maximum of *20,000* messages.
- This value can be set on a search-by-search basis, but only to the maximum allowed by a field on the Message Tracker global settings page. Administrators also can change the default value of this field on the global settings page. For more information see Changing search default settings.

### Trading information fields:

Listed below are the fields under the trading information heading. Use of these fields is optional.

#### From

- The message sender. You can type a community or partner name or routing ID. Or, click the ellipsis button to select a party. Also, wildcard characters (asterisks) can be used in this field.

#### To

- The message receiver. You can type a community or partner name or routing ID. Or, click the ellipsis button to select a party. Also, wildcard characters (asterisks) can be used in this.

#### Original filename

- The original name of the message file received from a partner or picked up from integration. Using this in conjunction with date or time conditions may result in more useful search results. Wildcard characters (asterisks) can be used in this field.

#### Delivery filename

- The name of the message file sent to a partner or delivered to integration. Using this in conjunction with date or time conditions may result in more useful search results. Wildcard characters (asterisks) can be used in this field.

#### Document ID

- The control ID of an EDI document. Wildcard characters (asterisks) can be used in this field.

#### Status

- The status of the messages to search for: any, delivered, failed, ignored, in process, negative response, resubmitted, resubmitted original, scheduled production, split and waiting for receipt.
- Messages fail for various reasons. Commonly, messages fail because the sender or receiver could not be identified. The trading engine may have been unable to find a sender or receiver's routing ID in a parsed message. If a message fails because the sender or receiver could not be determined, check the document for valid routing IDs. If searching for any status, all states but ignored are included. The ignored status is applied to messages the trading engine has determined lack worthwhile content (for example, an extraneous message received in addition to a message receipt).
- For negative response searches, Message Tracker returns payloads with negative responses from partners. If "Hide receipts" is turned off, a search also returns negative response receipts.
- With searches for messages with delivered status, negative responses also are returned. This is because a negative response is a delivered state.
- The trading engine marks as delivered any outbound message for which an acknowledgment was received, whether positive or negative. An outbound message also is marked as delivered when no acknowledgment is requested. An outbound message in a delivered state has an indicator, viewable in the message details, showing the acknowledgment as positive or negative.

#### Direction

- The direction of the messages to search for: any, inbound, outbound, internal, external.
- If you search for **any** direction, all messages are included in the search regardless of origination. A search for **inbound** finds messages received from trading partners and routed to integration. A search for **outbound** finds messages the HIE Hub engine picked up from integration, packaged and sent to trading partners.

#### Consumption URL

- Not applicable.

#### Document type

- This is EDI document types such as 850, 862. For ebXML, you can use values such as MessageError, Ping, Pong, StatusRequest, StatusResponse, SOAP Fault. For RosettaNet, values include Signal and Action.
- When you start typing in this field, autocomplete values display, unless an administrator has disabled attribute collecting.

#### Document class

- Values include Tradacoms, X12, XML, Edifact, Binary. For other classes, you can use the content MIME type without the application/ prefix (for example, use octet-stream instead of application/octet-stream).

#### MIME type

- Not applicable

**Attribute**

- Not applicable

**Message ID**

- Not applicable

**Core ID**

- Not applicable

**Conversation ID**

- Not applicable

**Integration ID**

- Not applicable

**Hide receipts**

- Show or hide message receipts in search results.

**Hide subordinate messages**

- Not applicable

**Hide pings**

- Not applicable

**Date**

- To search by date, expand the Date area on the left side below the Trading information area. The selection Don't search by date means date conditions are not used in searches. To search by date, select Origination or Delivered and select the date or time conditions.
- The default settings for searching by date is the Origination or Delivered date Within the last [n] days. If a search is performed without changing the date defaults, expected results may not be received if the database records are older than the number of days specified in the Within the last [n] days option.
- The After and Before option lets you search for messages traded after or before the date and time specified. The maximum days after or before the specified date and time can be set on a search-by-search basis.
- The Specify the dates option allows a search for records whose dates are within a range of dates and times indicated.

**Columns in Message Tracker:**

- To adjust the column display of the search results, expand the Columns area on the left side below the Date area and select the columns you want to show or hide on search results pages. Any custom column display set up by a user applies only to the user and not to other users.
- Under Columns, check boxes to select the order for sorting search results. Left-click and hold to drag a column name and reorder search results. If search results already are displayed, this action dynamically reorders the columns in the search results table.

**Column name selections in Message Tracker.**

▼ Columns

Left-click and hold to drag a column name and reorder search results

- Type
- Document class
- Document type
- MIME type
- Origination
- Delivered
- From
- From ID
- To
- To ID
- Pickup protocol
- Delivery protocol
- Status
- Failure reason
- Direction
- Consumption URL
- Core ID
- Document ID
- Message ID
- DMZ Zone
- Conversation ID
- Integration ID
- Original filename
- Delivery filename
- Receipt content
- Produced Message Size
- Consumed Message Size

Sort by:  ▼  ▼

## 6 HIE Operations Change Management

Trading partners will need to incorporate management of HIE connectivity and data submission activity monitoring into existing system management and operational change management processes. In addition to daily activities, processes and resources will also need to be organized to support monthly HIE maintenance activities and unplanned outages. The information listed below can be used for HIE operations planning.

**OneHealthPort HIE System Availability Notifications** – The OneHealthPort HIE website posts system availability in the notification box shown below. Current system status is posted and updates are provided via Twitter feeds. Operations teams can sign up to follow Twitter feeds announcing system events at Tweets@ohphie.

Unplanned outages are posted on the website, as well as upcoming scheduled maintenance downtimes. Monthly maintenance schedules are also posted annually for use in operational planning.

<http://www.onehealthport.com/hie>

In addition to website postings, detailed system announcements and notifications are sent via email distribution. Contact information for organizations is collected and set-up in the distribution list by OneHealthPort at the time connectivity is established with the HIE.

***HIE SYSTEM AVAILABILITY NOTICES***

- Current system status below:

Tweets by @ohphie

\*\*\*\*\*

***SCHEDULED HIE EXTENDED MAINTENANCE***

- Maintenance is scheduled monthly for up to a 4-hour outage starting at 5 PM PT
- Next scheduled outage is Friday, February 20, 2015
- See [2015 Maintenance Schedule](#)
- [HIE Support Request Form](#)



**OneHealthPort HIE Support Request Form** – Use this form to obtain technical support or assistance with issues related to information exchange activities with the OneHealthPort HIE. The support request form is located on the OneHealthPort HIE website and the link is also provided below. The form is monitored by HIE technical consultants and business team members to ensure proper resources are quickly deployed to respond to customer issues.

<http://www.formstack.com/forms/?1688456-sjNVJY8V7I>

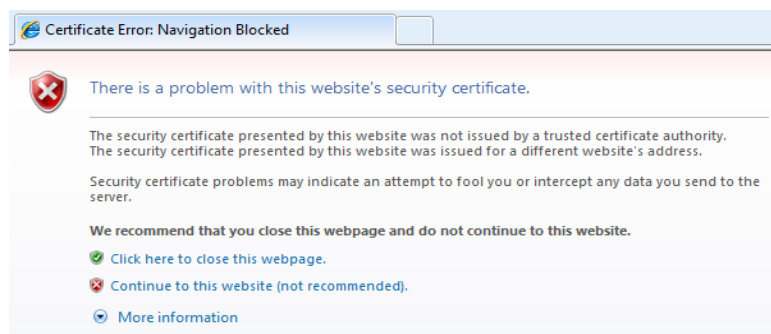
## 7 Appendix

### 7.1 Detailed Overview of Activator Installation Process

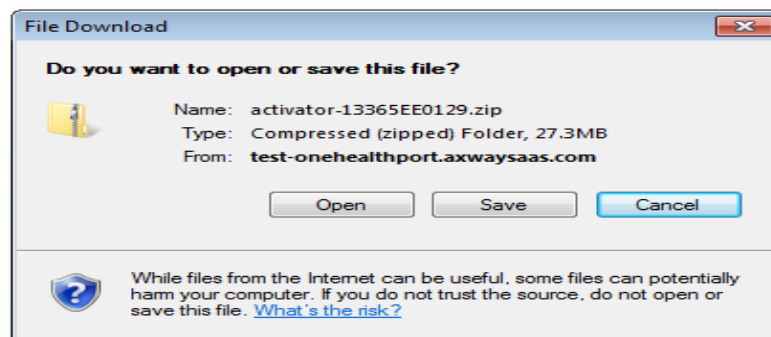
The following steps provide a detailed overview of the Activator installation process. The process is facilitated by a OneHealthPort HIE technical consultant with the trading partner’s designated technical contact through a web session.

#### Step 1) Download and save image from URL link provided in the secure email.

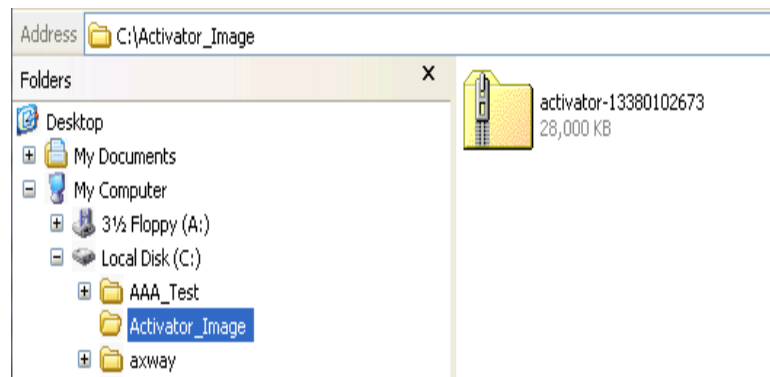
- Click the URL link provided in the “Synchrony (Activator) Download Available for” secure email to start the Activator image download process.
- A “Security Alert” dialog box may appear during download requesting the acceptance of a certificate which is not trusted. Click “yes” button to proceed.



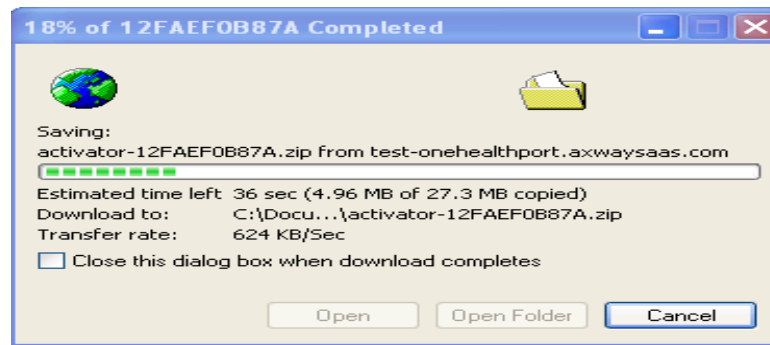
- A “File Download” dialog box will appear prompting to open or save the image.



- Save download image to a folder which is easy to locate such as “C:\Activator\_Image”

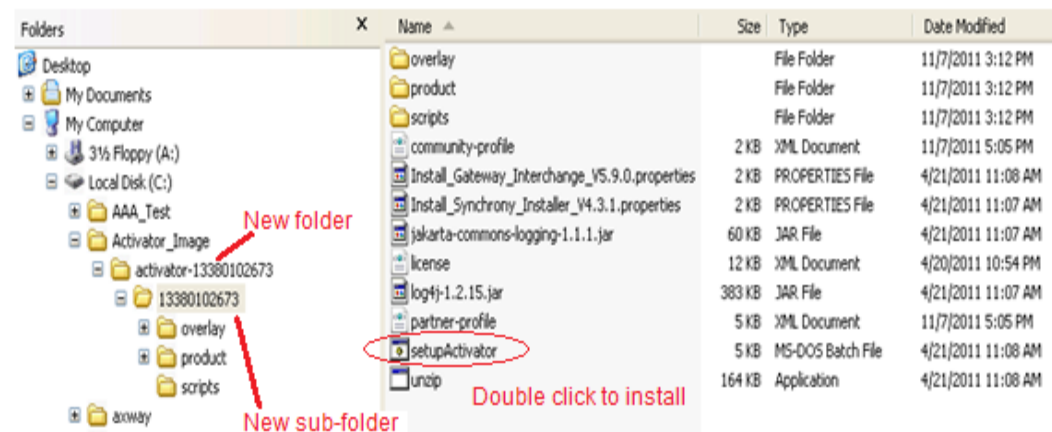


- When the download dialog box closes the image has been saved to the selected folder location and is ready to be unzipped and installed.



**Step 2) Unzip the installation image.**

- Unzip Activator image into the same folder as the downloaded image.
- Unzipped image will create a folder, with name of “activator-” + unique Activator alphanumeric code, and sub-folder with the name of the unique Activator alphanumeric code.
- Open sub-folder and locate “setupActivator” batch file.



**Step 3) Start the installation.**

- Start installation by doing one of the following
  - Windows = double click “setupActivator” batch file.
  - Unix = ./setupActivator.sh
- “Welcome to Activator Installer” dialog box appears. This dialog box allows you to set the install location of the Activator application.
  - Accept default location = Press “Enter” button.
    - Drive: + “\axway\” + unique Activator alphanumeric code.
  - Set location = type complete path and press “Enter” button

```

C:\WINDOWS\system32\cmd.exe
Welcome to Activator Installer.
-----
Please enter the directory where you would like to install Activator or press enter
to accept the default [default: \axway\12FAEF0B87A1:

```

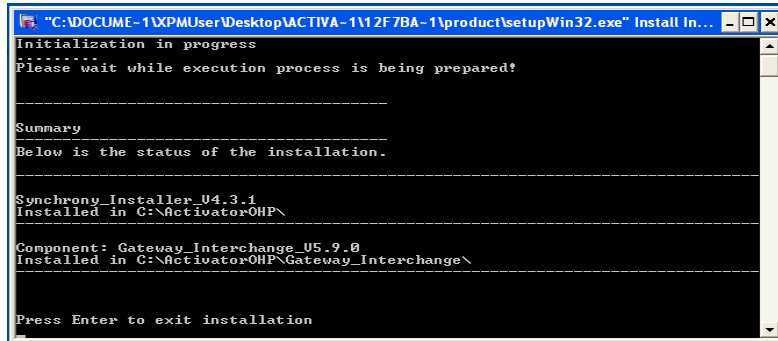
- Installation script is copied and the software download will commence.
- Installation will automatically start once the download is complete.
- Application download and install may take from 5 to 10 minutes.
- Dialog box will display the status of install.

```

C:\WINDOWS\system32\cmd.exe
Extracting the java run time...
Extraction Complete
Copying the JRE files...
581 File(s) copied
23:50:10 - [main] INFO <PortTester.testOutboundConnection:55> - testing outboun
d connection to test-onehealthport.axwaysaas.com, port 4880
23:50:10 - [main] INFO <PortTester.testOutboundConnection:59> - outbound connec
tion to test-onehealthport.axwaysaas.com, port 4880 was successful
Downloading software...this can take several minutes
DO NOT CLOSE THIS WINDOW!!
.....
..
Download complete
Installing Activator. This may take several minutes.
The status is logged to C:\ActivatorOHP\synInstall\install.log.

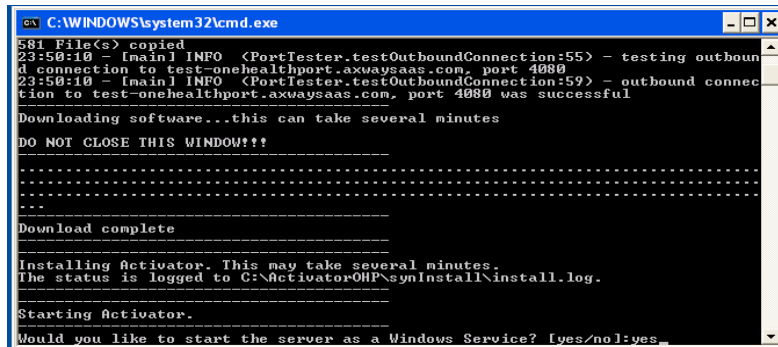
```

Below screen indicates a successful installation

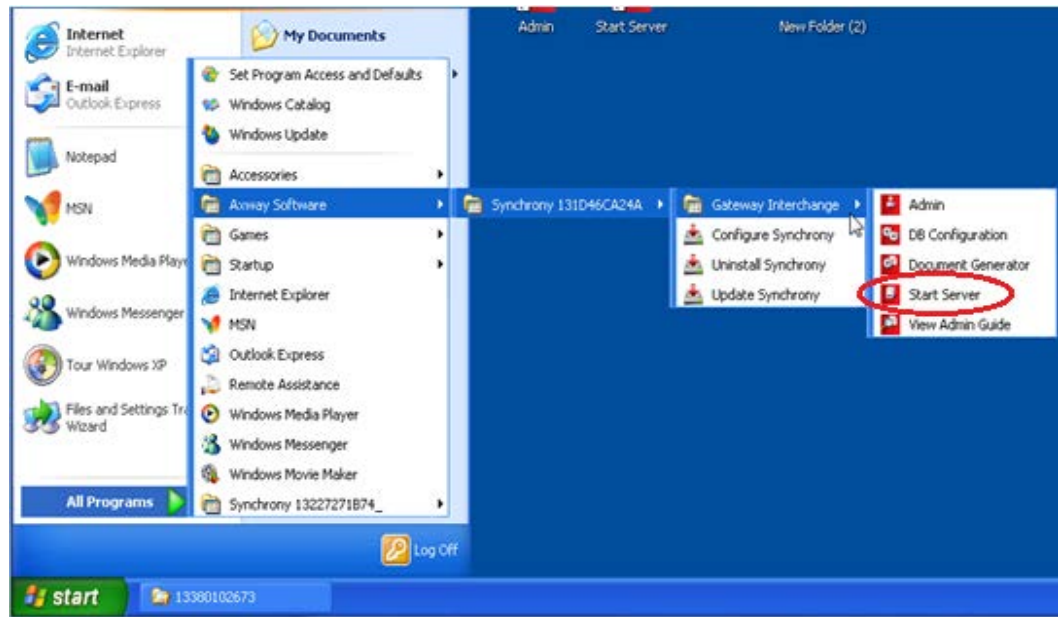


**Step 4) Start the server.**

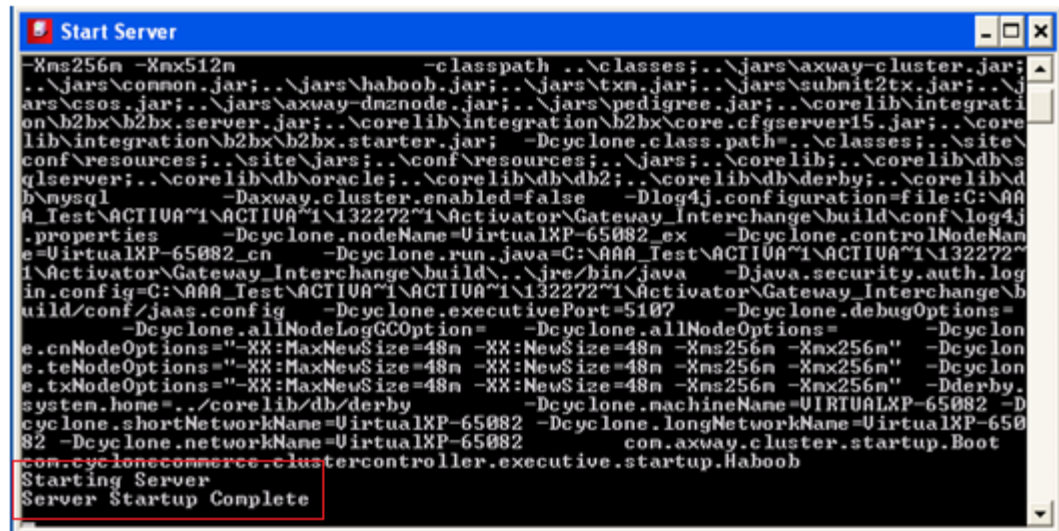
- After the installation is successful, you will be prompted to install the server as a Windows service. Respond “yes” to this prompt (if you respond no, when the system is rebooted the Activator process will not start automatically).



- After responding “yes” to create a Windows service, the above window will close. The service created is named **GatewayInterchangeService** and the server will be started.
- If you responded “no” to create a Windows service you will need to manually start the Activator server.
  - Starting Activator server will take 5 - 10 minutes to start.
  - Press “Start server” from “Start \ All Programs \ Axway Software \ Synchrony”



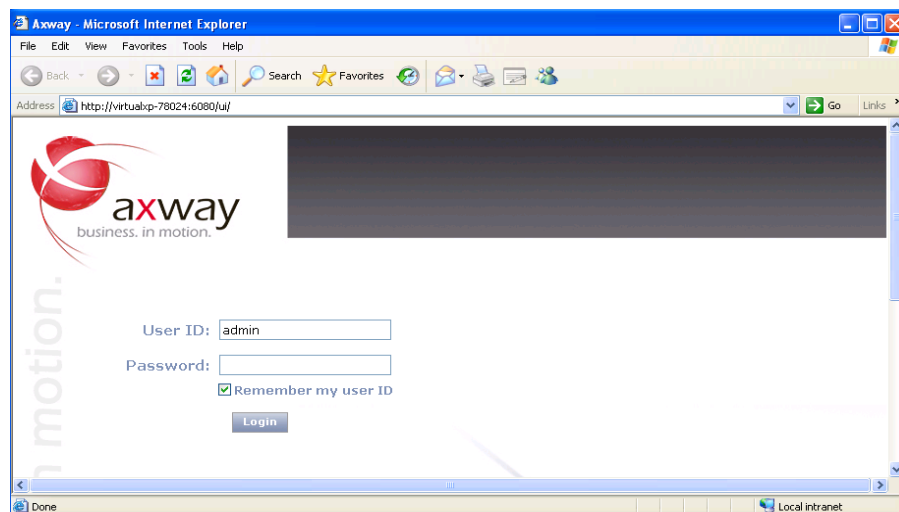
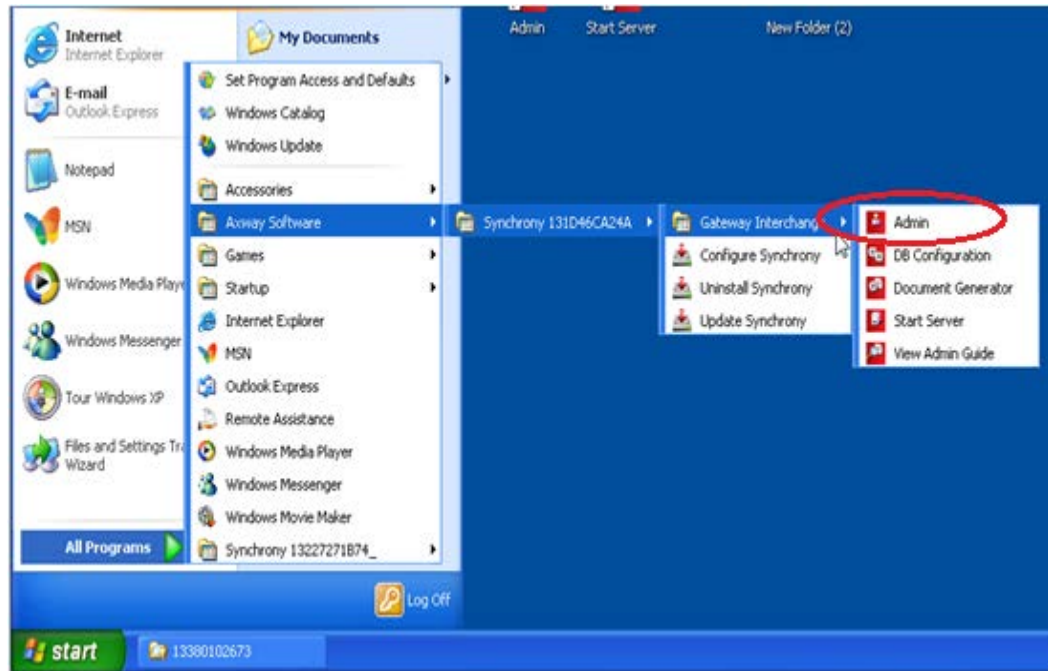
- “Start Server” dialog box will appear during the Activator server startup. **DO NOT** close dialog box until you are done using the Activator. Closing the “Start Server” dialog box stops the Activator server.
- “Start Server” dialog box will appear and display “Server Startup Complete” message when Activator is started.



- The install script also creates YOUR COMMUNITY, partner profiles and links your instance of Activator with the OneHealthPort HIE Hub.
- Once started a test document will be sent to the OneHealthPort HIE Hub to confirm connectivity.

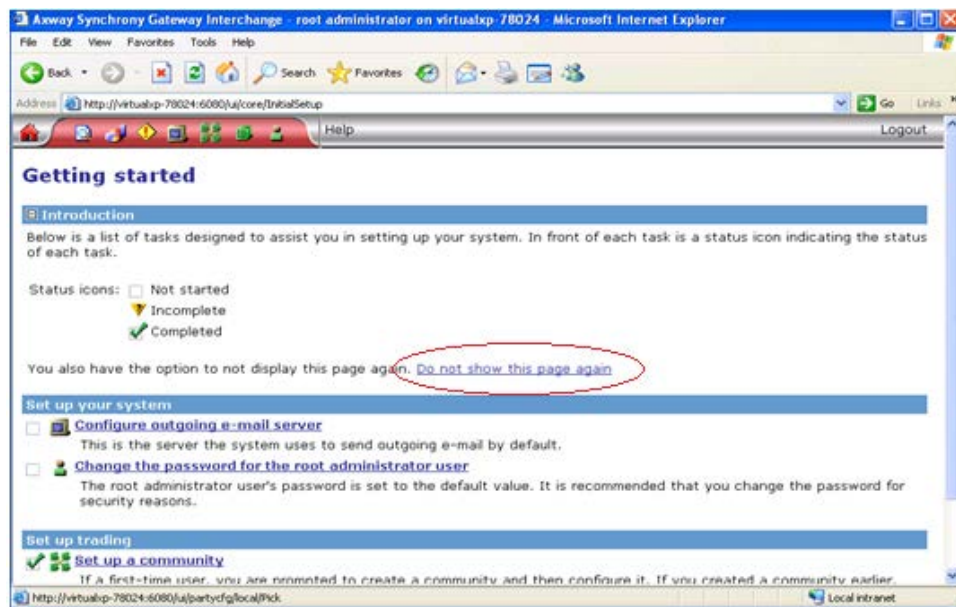
**Step 5) Accessing the Activator User Interface.**

- To launch the Activator user interface (UI) navigate to the Admin menu located in “Start \ All Programs \ Axway Software \ Synchrony”

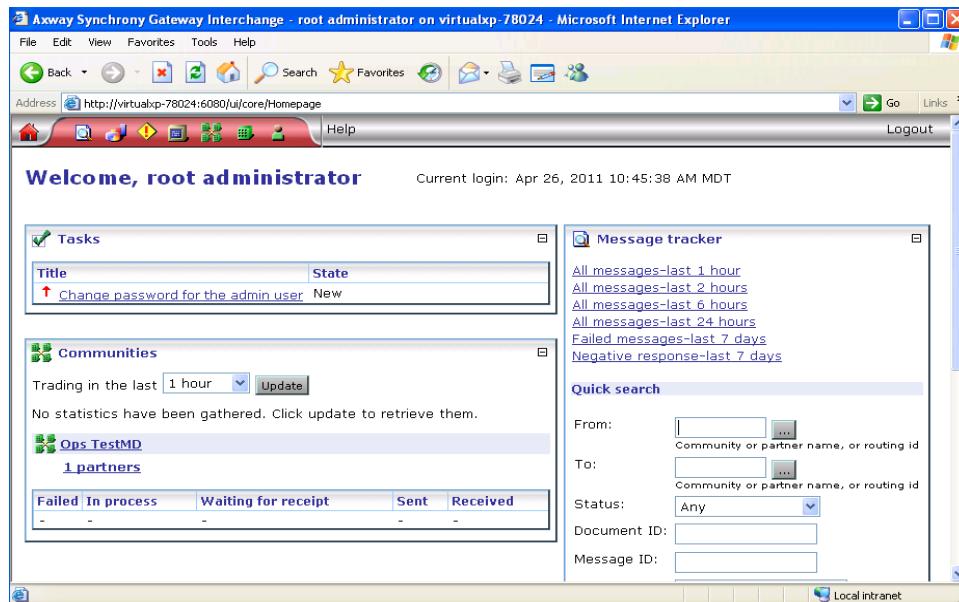


- Activator logon screen will appear.
- To log in, use the user id / password credentials sent in the secure email.
- The “Getting Started” screen will appear next.
- Click on “Do not show this page again” link near the middle of the page. This is a one-time task and will stop the “Getting started” screen from appearing each time you log into Activator.





- The “Welcome” screen will appear, this is the home page for the Activator





## 7.2 Connection Using AS2 Commercial Software

A new OneHealthPort HIE trading partner may choose to establish communication to the OneHealthPort HIE by using commercial software that supports the AS2 protocol. To setup the connection with the OneHealthPort HIE the trading partner will need complete the following tasks:

### 7.2.1 Submit a Request for Connectivity with the OneHealthPort HIE

Information required for connectivity setup and configuration will be obtained during the connectivity interview process. To begin the process, submit a OneHealthPort HIE Support Request form.

<http://www.formstack.com/forms/?1688456-sjNVJY8V7I>

### 7.2.2 AS2 Commercial Software Connectivity Questionnaire

A connectivity questionnaire is sent to trading partners to provide and obtain information for establishing a connection to the OneHealthPort HIE Hub using commercial software. The questionnaire includes the following information for both the Production and UAT environments. Note: The UAT environment is a HIPAA-compliant, locked down test environment:

- URLs
- Ports
- IP addresses
- Certificate (encryption and signing)

The information collected on the questionnaire is used by both the trading partner and OneHealthPort to prepare for the connectivity process.

### 7.2.3 Digital certificate

A digital certificate will be required for secure exchange of data. This may be in the form of either a DER encoded binary X.509 (.cer) or Cryptographic Message Syntax Standard PKCS #7 (.p7b, .p7c). If a .p7b/.p7c file is going to be used please export the entire certificate chain for use during the connectivity process.

OneHealthPort uses secure email during the connectivity process to exchange certificates with the trading partner.

#### 7.2.4 AS2 Commercial Software Connectivity Process

Once the information from the connectivity questionnaire is shared between the trading partner and OneHealthPort and any open issues, concerns, or additional information requirements are addressed the following process is implemented to establish connectivity:

1. OneHealthPort arranges a connectivity web session and conference call with the trading partner and HIE technical consultants. The session typically takes about two hours.
2. Connectivity is established and OneHealthPort and the trading partner exchange test messages (provided by OneHealthPort).
3. OneHealthPort validates test message movement through the HIE B2Bi Hub engine and that appropriate receipting occurs, i.e. MDN is properly generated and sent.
4. Trading partner validates receipt of test message and content.