

# USER GUIDE

---

## Edge Testing Tool

## Table of Contents

1.0	OVERVIEW.....	5
1.1	Edge Testing Tool.....	5
1.2	Purpose.....	5
1.3	Access.....	5
1.4	Testing Overview.....	6
2.0	TESTING CONFIGURATION FOR EDGE SYSTEM.....	7
2.1	Registration.....	7
2.2	Configuration Steps.....	8
2.2.1	Profile Creation.....	8
2.2.2	Reporting.....	9
2.3	Documentation.....	10
3.0	LOCAL INSTALLATION AND CONFIGURATION.....	12
3.1	Configuration Steps.....	12
3.2	Apache James Server v3.0.....	12
3.3	Installing Local XDSTOOLS2 Instance.....	14
3.4	Installing Local MDHT C-CDA Validation Software.....	14
4.0	DIRECT - SUT SENDING.....	15
4.1	Register a Direct Contact Address.....	15
5.0	SENDING C-CDA MESSAGES TO THE DIRECT LISTENER.....	17
5.1	Send a Direct Message to the ETT.....	17
5.2	Send a Direct + XDM Message to the ETT.....	18
5.3	Send a SOAP Message to the ETT.....	18
6.0	SENDING MESSAGES FROM THE EDGE TESTING TOOL TO A SYSTEM UNDER TEST.....	19
6.1	Send a Direct Message to a System Under Test.....	19
6.2	Send a Direct + XDM Message to a System Under Test.....	21
7.0	SMTP TESTING.....	22
7.1	SMTP Test Cases.....	22
7.1.1	SMTP Test Cases 1-8, 14, 18 (Sender).....	22
7.1.1.1	Testing Steps.....	22
7.1.2	SMTP Test Cases 9, 16, 20 (Receiver).....	24
7.1.2.1	Testing Steps.....	25
7.1.3	SMTP Test Case 10 (Receiver – Reject Invalid Data).....	27
7.1.3.1	Testing Steps.....	28
7.1.4	SMTP Test Case 11 (Receiver – Reject Bad Commands).....	30
7.1.4.1	Testing Steps.....	31
7.1.5	SMTP Test Case 13 (Receiver – Command Timeout).....	33
7.1.5.1	Testing Steps.....	34
7.1.6	SMTP Test Case 17 (Receiver - Reject Invalid STARTTLS).....	36
7.1.6.1	Testing Steps.....	37
7.1.7	SMTP Test Case 22 (Receiver - Reject Invalid Username/Password).....	38
7.1.7.1	Testing Steps.....	39

7.1.8 SMTP Test Cases 25(a)-(f) (Receiver - Text and CCDA, Pdf and CCDA, Text and XDM, CCDA and Text, CCDA and Pdf, and XDM and Text) .....	41
7.1.8.1 Testing Steps .....	42
7.1.9 SMTP Test Cases 26(a-b) (Receiver – Receive Bad CCDA).....	45
7.1.9.1 Testing Steps .....	46
7.1.10 SMTP Test Cases 27 (Receiver – Receive XDM with Bad XHTML).....	47
7.1.10.1 Testing Steps .....	48
7.1.11 SMTP Test Case 28 (Receiver - Receive XDM with MIME type 'application/octet-stream') .....	50
7.1.11.1 Testing Steps .....	51
7.1.12 SMTP Test Case 29 (Receiver – Receive XDM with MIME type 'application/xml').....	52
7.1.12.1 Testing Steps .....	53
8.0 SMTP MESSAGE TRACKING .....	56
8.1 SMTP Message Tracking (MT) Test Cases .....	56
8.1.1 SMTP MT Test Case 17 - Generate Unique Message-ID (Processed MDN suite) .....	56
8.1.1.1 Testing Steps .....	57
8.1.2 SMTP MT Test Cases 18 & 18(a) - Accept failure message for invalid recipient (Processed MDN suite - IMAP/POP Receiver & SMTP Receiver).....	59
8.1.2.1 Testing Steps .....	59
8.1.3 SMTP MT Test Case 45 - Generate Unique Message-ID (IG for Delivery Notification Suite) .....	62
8.1.3.1 Testing Steps .....	63
8.1.4 SMTP MT Test Case 46 (Generate Disposition Notification Options Header).....	65
8.1.4.1 Testing Steps .....	65
8.1.5 SMTP MT Test Cases 47 & 47(a) - Accept failure message for invalid recipient (IG for Delivery Notification Suite - IMAP/POP Receiver & SMTP Receiver) .....	67
8.1.5.1 Testing Steps .....	68
9.0 IMAP TESTING.....	72
10.0 POP3 TESTING.....	73
11.0 XDR TESTING .....	74
11.1 XDR Test Cases.....	74
11.1.1 XDR Test Case 1 (Sender).....	74
11.1.1.1 Testing Steps .....	74
11.1.2 XDR Test Case 2 (Sender).....	77
11.1.2.1 Testing Steps .....	78
11.1.3 XDR Test Case 6 (Sender).....	80
11.1.3.1 Testing Steps .....	81
11.1.4 XDR Test Case 7 (Sender).....	83
11.1.4.1 Testing Steps .....	84
11.1.5 XDR Test Case 3 (Receiver) .....	86
11.1.5.1 Testing Steps .....	87
11.1.6 XDR Test Cases 4a & 4b (Receiver) .....	88
11.1.6.1 Testing Steps .....	89
11.1.6.1.1 4a.....	89
11.1.6.1.2 4b .....	91
11.1.7 XDR Test Case 5 (Receiver) .....	93
11.1.7.1 Testing Steps .....	94
11.1.8 XDR Test Case 8 (Receiver) .....	95
11.1.8.1 Testing Steps .....	96
11.1.9 XDR Test Case 9 (Receiver) .....	98
11.1.9.1 Testing Steps .....	99

12.0	XDR MESSAGE TRACKING .....	102
12.1	Message Tracking (MT) Test Cases .....	102
12.1.1	XDR MT Test Case 19 (Sender).....	102
12.1.1.1	Testing Steps .....	103
12.1.2	XDR MT Test Cases 20a & 20b (Sender) .....	105
12.1.2.1	Testing Steps .....	106
12.1.2.1.1	20a.....	106
12.1.2.1.2	20b.....	108
12.1.3	XDR MT Test Case 48 (Sender).....	111
12.1.3.1	Testing Steps .....	112
12.1.4	XDR MT Test Case 49 (Sender).....	114
12.1.4.1	Testing Steps .....	115
12.1.5	XDR MT Test Cases 50a & 50b (Sender) .....	117
12.1.5.1	Testing Steps .....	118
12.1.5.1.1	50a.....	118
12.1.5.1.2	50b.....	120
13.0	HISP TESTING & DELIVERY NOTIFICATION .....	124
13.1	HISP Testing and Delivery Notification .....	124
14.0	MESSAGE VALIDATORS.....	125

## 1.0 OVERVIEW

### 1.1 Edge Testing Tool

The Edge Testing Tool (ETT) was developed by NIST to test requirements and standards related to message transport specifications expressed within the 2014/2015 Edition of the Office of the National Coordinator for Health Information Technology (ONC) Standards & Certification Criteria<sup>1</sup>. The ETT tests for: (1) adherence to the Edge Protocol standards during valid communication sessions between the ETT and a System Under Test (SUT), and (2) Direct.

At a broad level of applicability and usage, ONC-Authorized Testing Laboratories (ATLs) and Associated Certification Bodies (ONC ACBs) of electronic health record (EHR) providers can utilize the ETT to certify EHR module achievement against 2014/2015 Edition Objectives of selected ONC Standards & Certification Criteria. The methods by which messages should be sent and received are outlined further within this User Guide.

### 1.2 Purpose

Edge Systems (e.g., EHRs) and Health Information Service Providers (HISPs) can specifically use the ETT to perform certification testing against Edge Protocols. The purpose of this ETT User Guide is to outline the process by which Edge Systems and HISPs may send and receive messages and C-CDA attachments to the ETT for the purposes of transport testing as required by ONC.

An Edge System or HISP vendor can leverage the Transport Testing Tool (TTT) to certify against Direct, Direct + XDM, or SOAP / XDR and the ETT to certify against the four Edge Protocols. To maintain security while exchanging XDR message information and authentication/authorization data, the ETT implements TLS, and the TTT implements SAML.

Within the scope of testing and test procedure context for ETT Test Cases, the term ‘SUT’ is commonly used in an abstract form. The SUT can act as either an Edge System or HISP, depending on the specific testing need. Both can send and receive as a SUT. Typically, the Edge System can act as the SUT for Edge testing and the HISP for both Edge and Direct testing.

### 1.3 Access

The ETT can be accessed through two (2) interfaces: web or local.

- **Web Interface** – The production version of the ETT is accessible online through the following link: <https://tppedge.sitenv.org//>. This web interface link is referred to within the ETT User Guide and accompanying resources as the Home Page. Any product version updates will be announced on the Home Page.
- **Local Interface** – A downloadable and executable instance of the ETT is available for use. Please refer to [Section 3.0 Local Installation and Configuration](#) for further details.

## **1.4      Testing Overview**

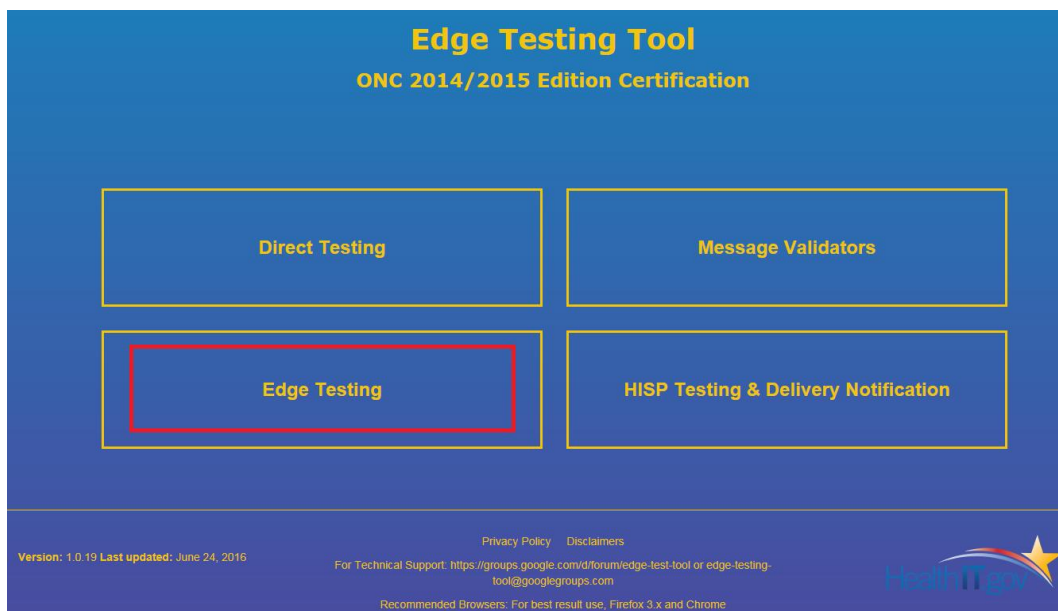
- The ETT will allow vendors to send and receive messages using various transport methods to and from the SUT, dependent upon specific testing objectives, or to test Direct.

## 2.0 TESTING CONFIGURATION FOR EDGE SYSTEM

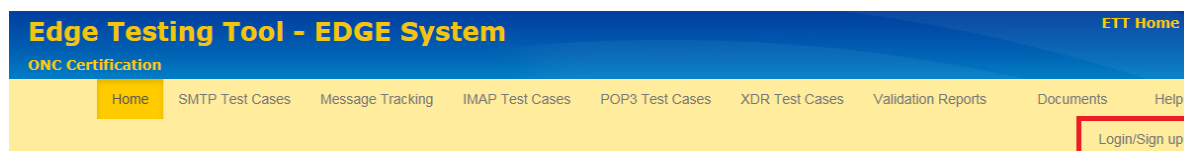
This section guides the vendor through the necessary configuration and preparation steps for a web application Profile creation and Test Case execution.

### 2.1 Registration

1. Navigate to the [ETT Home Page](#), and select the **Edge Testing** option.



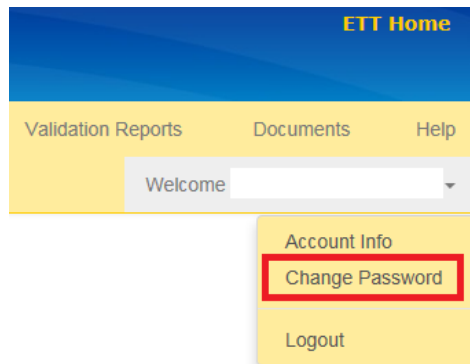
2. From the ETT Home Page, the vendor can select the intended email address to test their SUT. A response message disposition notification (MDN) will be sent from an ETT email address upon receipt of a simple mail transfer protocol (SMTP) message.
3. Click **Login/Sign up** and then **Sign up** to create a unique user account within the ETT. Enter a **Username** email address, **Password**, **Repeat Password**, and then click **Sign Up**.



Before executing any tests within the ETT, **Login** using the credentials created during **Sign Up**. A success message will appear upon successful Sign Up and Logout.

***Note:** The **Username** email address is used for account creation, historic testing session saves, and delivery notification of ETT-specific information by ONC staff. It is not specifically used as a component of SMTP and/or XDR testing. Testing email addresses are configured within specific Profile instances and applicable for target Test Cases.*

If either the login **Username** or **Password** is entered incorrectly, an error message will appear prompting the vendor to re-enter credentials. To reset an ETT account **Password**, click the **Forgot password?** link within the **Login** prompt box. This action sends a temporary password to the username's email address. An account **Password** can also be reset through the navigation Bar after successful login.



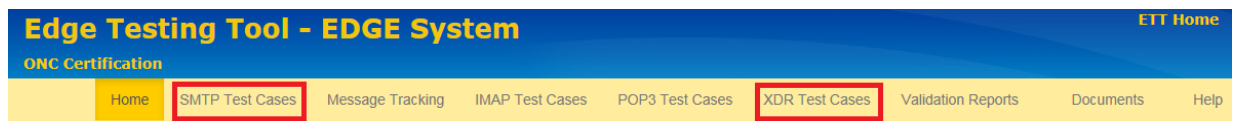
***Note:** The user account **Password** reset is a self-service feature within the ETT. No ETT administrator assistance is required. The vendor follows on-screen prompts and email instructions.*

## 2.2 Configuration Steps

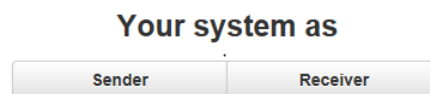
In order to operate the ETT as intended and generate expected/successful testing results per Test Case executed, the vendor must perform the following series of steps.

### 2.2.1 Profile Creation

1. Select the SMTP or XDR target Test Case through the **SMTP Test Cases** or **XDR Test Cases** links on the navigation bar. This enables the testing Profile feature of the ETT.



2. Select either the **Sender** or **Receiver** testing role for the SUT.



3. From the testing **Profile**, enter the:

Profile Data Field	Description
Profile Name	The Profile name can be edited and customized based on testing needs by the vendor. This feature can be accessed by clicking on the Profile header. Saved Profiles can be accessed from within the ETT account



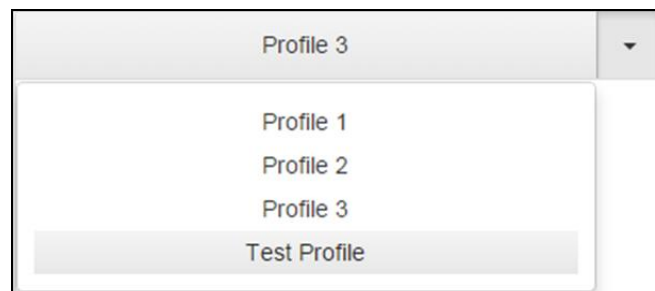
created during sign up/registration.

<b>Vendor SMTP Hostname / IP</b>	SMTP or IP address of the vendor's email server. This should directly connect with the vendor SMTP Email Address
<b>Vendor SMTP Email Address</b>	Vendor SMTP Email Address should correspond to the vendor SMTP Hostname / IP. This email address will be used to send/receive ETT SMTP Test Case validation messages.
<b>Vendor SMTP Username and Password</b>	These should correspond to the vendor SMTP Email Address. The username and password are mainly used for authentication-based Test Cases so the ETT can login to the SUT.

***Note:** For information on how to find the SMTP/IP of your email client/server, please refer to vendor specific documentation or click **Help** on the ETT navigation bar.*

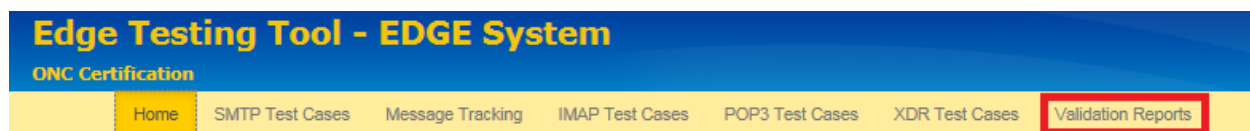
- Before saving a Profile, assign a unique name (the default Profile name is **Default Profile**). Click the Profile name, delete the existing text, and type a new name. Upon population of the testing Profile, click **Save**. To delete a saved Profile, click **Remove**.
- A successful message will appear upon successful **Save** or **Remove**.

Saved Profiles can be retrieved and applied to subsequent/future tests by selecting the target Profile from the drop-down menu.



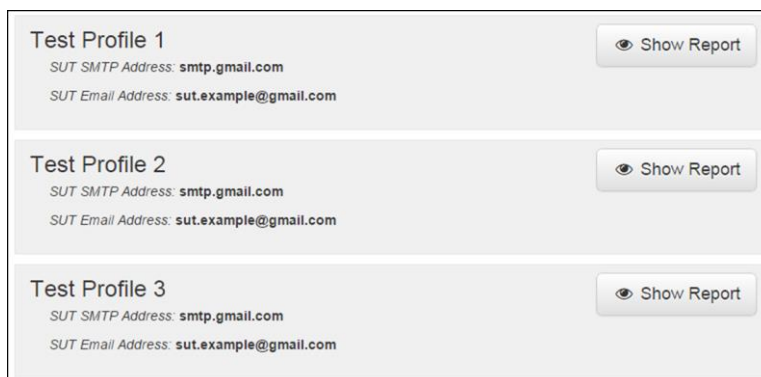
### 2.2.2 Reporting

- During a testing session, the vendor can review a high-level synopsis of all Test Cases executed through the **Validation Reports** tab on the navigation bar.



- Within the **Validation Reports** tab, tests are organized by ETT testing Profiles. For reference, the **SUT SMTP Address** and **SUT Email Address** configured for each

Profile are displayed. For a given testing session, the total number of ETT testing Profiles used will be displayed within the Validation Reports tab.



- By clicking on the **Show Report** button, the vendor is given the Test Case executed, a timestamp of when the test was run, and success or failure of each test. The log for each executed Test Case provides detailed information, including evidence to support success or failure.

Validation report for profile: Test Profile 1		
Test Case	Timestamp	Result
SMTP test 17	Dec 16, 2014 12:17:15 PM	✓
SMTP test 13	Dec 16, 2014 12:13:58 PM	✗
SMTP test 9, 16, 20	Dec 16, 2014 12:11:37 PM	✓
SMTP test 11	Dec 16, 2014 12:12:15 PM	✓
SMTP test 22	Dec 16, 2014 12:17:24 PM	✓
SMTP test 10	Dec 16, 2014 12:12:10 PM	✓

## 2.3 Documentation

Documentation relevant to the ETT, including this ETT User Guide, CCDA/C32/CCR samples and test data package, the ONC 2015 test procedures and companion guides, and other development-related artifacts will be made available in the **Documents** section, accessible from the navigation bar.

### Guides

- Edge Testing Tool User Guide (v3.0)
- Slides from 2015 Edition ETT Detailed Training [Download](#)

### Samples

- CCDA/C32/CCR Samples [Download](#)
- C-CDA Test Data Package [Download](#)

### Documents

- 2015 Test Procedures and Companion Guides [Download](#)

## ETT Instruction/Demonstration Videos

- Demonstration Videos

## 3.0 LOCAL INSTALLATION AND CONFIGURATION

This section guides the vendor through the necessary configurations and preparation steps for tool local download, configuration, and execution.

In order to operate the ETT as intended and generate expected/successful testing results per Test Case executed, the vendor must perform the following series of steps.

### 3.1 Configuration Steps

1. Navigate to the ETT's downloadable and executable .jar file (ett.jar) located in the directory located [here](#). The needed configuration information (contained within the application properties file) is also in this directory.
2. The ETT leverages a custom MySQL database schema. The MySQL application can be downloaded [here](#) and the custom ETT schema can be accessed from the directory located [here](#).
  - a. As a prerequisite, the vendor should have a local instance of MySQL database installed, configured, and running before applying the ETT's custom schema. The recommended usage version for local ETT install is release 5.6.25 MySQL Community Server (GPL). The ETT development team does not guarantee compatibility with other MySQL versions.
3. Navigate to the Apache James Server URL and download the application's build. The Apache James Server is leveraged by the ETT as a mail server. The recommended usage version for local ETT install is release v3.0.

### 3.2 Apache James Server v3.0

1. Apache James Server v3.0 (Early James Server) can be downloaded [here](#). Select the Binary (Unix TAR) format.
2. Confirm that the SUT system/user account being used has full administrative privileges.
  - a. Save the Apache James Server v3.0 downloaded file to the directory location */usr/local/apache*.
3. Decompress (un-tar) the *apache-james-3.0...app.tar.gz* file and extract the package contents.
4. In the *conf* directory:
  - a. Rename the configuration file *smtpserver-template.conf* to *smtpserver.conf*.
5. Within the *log4j.properties* file:
  - a. Set *log4j.logger.james.smtpserver=DEBUG*, *SMTPSERVER* (set to *DEBUG*, not *INFO*)

- b. Configure *./james* start as root.
6. To add users:
  - a. Change the directory to */path/james/bin*.
    - i. For POSIX, run *james-cli.sh*.
    - ii. For Windows, run *james-cli.bat* with the following parameters:
      1. *james-cli.sh -h localhost -p 9999 adddomain domainname*
      2. *james-cli.sh -h localhost -p 9999 adduser user@domainname password*
  - b. The ETT requires that a defined list of users and mailboxes be installed within the Apache James Server v3.0. This list can be accessed from the directory located [here](#).
7. To configure the ETT's custom MySQL database schema:
  - a. With the download and install on the SUT:
    - i. Create local user credentials (i.e., username and password)
    - ii. Assign the database a name (for use and communication with the ETT)
      1. The values selected must align with those contained within the *application.properties* file.
        - a. *ttt.db.username=username*
        - b. *ttt.db.userpassword=password*
        - c. *ttt.db.hostname=localhost*
        - d. *ttt.db.dbname=direct*
      2. The default database name is *direct*. If a different name is desired, the file *ttt.db.dbname* within the *application.properties* file must be updated.
8. For STARTTLS:
  - a. Generate the keystore:
    - i. *keytool -genkey -alias james -keyalg RSA -keystore /path/to/james/conf/keystore*
  - b. In the certificate, configure the first and last name consistent with the SUT machine name.
  - c. Copy the *sunjce\_provider.jar* to */path/james/lib* directory.
  - d. For requiring STARTTLS:
    - i. The Apache James Server v3.0 downloaded file must be added to the directory location */path/james/conf/lib*.

- ii. The *smtpserver.xml* must contain the following additional line in the `<smtpserver>` section:
  1. `<handler`  
`class="gov.nist.healthcare.ttt.jamesext.RequireTLSAuthCmdHan`  
`der"/>`
    - a. This can be stored under the group of handlers at the end and will intercept the AUTH command if the STARTTLS is not issued:
      - i. *AUTH LOGIN*
      - ii. *503 5.7.0* must issue a STARTTLS command first

9. For IMAP:

- a. Enable STARTTLS for IMAP on Port 993 (on the Apache James Server v3.0). IMAP currently must be run on Port 110 for internal data pulls.
- b. Each testing account created for the Apache James Server v3.0 will have four folders (e.g., INBOX, Folder, FOLDER, folder) to satisfy ETT case-sensitive testing requirements.
- c. Pre-load each Apache James Server v3.0 testing account and associated 4 folders with test messages (with and without CCDA).

### 3.3 Installing Local XDSTOOLS2 Instance

The ETT depends on a version of XDSTOOLS2 for its XD\* related components. The user can either point the configuration file to the public copy available online (see the default instructions) or can point to a copy running on their local system.

Download the most recent version of *xdstools2.war* from the following link: <https://github.com/siteadmin>. This is a web archive that will need to be deployed from a local Tomcat instance. Detailed installation and configuration instructions are included in the accompanying README file. *xdstool2.war*.

### 3.4 Installing Local MDHT C-CDA Validation Software

The ETT depends on an instance of the MDHT C-CDA Validation Suite for its document validation component. An item in the configuration file will allow the system to point to a locally installed copy of the MDHT software.

Download the most recent copy of *referenceccdaservice-bundle-\*.zip* from the following link: <https://github.com/siteadmin>. This zip file contains a web archive that will need to be added to a local Tomcat instance. This zip file contains instructions on how to deploy and configure the necessary software components.

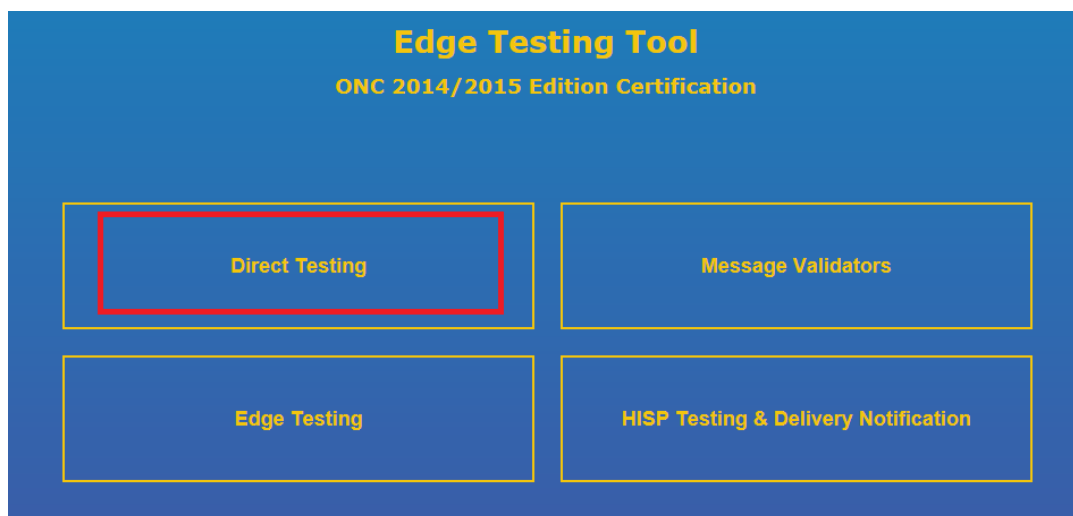
## 4.0 DIRECT - SUT SENDING

Within the following Test Cases, tests are executed from the following actor perspective:

Test Actor	Testing Role
SUT	Sends test message in alignment with Testing Procedures and Conformance Test Details
ETT	Receives test message and validates alignment with Testing Procedures and Conformance Test Details

### 4.1 Register a Direct Contact Address

To register a Direct web address within the ETT environment, users must navigate to the Home Page and click on **Direct Testing**.



On the **Register Direct** tab, users will be asked to provide a Direct Email Address. Users who do not register their Direct web address will not be recognized by the ETT and therefore will be unable to send or receive Direct or Direct/XDM messages.

Once users have registered, they will be placed on a “white list” of approved email addresses from which the ETT will accept messages. After user registration is complete and email addresses are successfully created/ added, navigate back to the Home Page.

***Note:** Users utilizing the SOAP send and receive features of the ETT do not need to pre-register on the Register Direct tab. However, users will need to register their endpoints used to access the ETT. This will be completed at the time of message sending and/or receiving. Because the process is interactive, the validation results are displayed on the user’s screen, so there is no need to register a contact email address.*



## 5.0 SENDING C-CDA MESSAGES TO THE DIRECT LISTENER

### 5.1 Send a Direct Message to the ETT

Sending messages via Direct is the required mechanism for Message Tracking (MT) outlined by the Objectives contained within the 2014/2015 Edition of the ONC Standards & Certification Criteria. The prerequisite to sending messages to the ETT via Direct is registering a Direct email address. To register a Direct email address, refer to [Section 4.1](#) of this User Guide.

1. Once registered with the ETT, select the ONC Objective that is representative and appropriate for the content you are sending. The sender will include the public key signing certificate in messages sent to the ETT. The sending content will automatically be validated and a validation report will be sent to the contact email address entered during sign up/registration. Each email address can also accept text/plain MIME formats to assist in validating human-readable text. <host-address> is set to the address of the user endpoint (i.e., local machine) the ETT is in operation on.
2. Select the Direct email addresses to send the content.

The Objectives against which a user can test his/her system, currently supported by the ETT, are listed in Table 1 below:

**Table 1: Direct Address**

Direct (To) Address	Purpose
<b>direct-clinical-summary@ttpedge.stenv.org</b>	ONC 2014 Edition Certification 170.314(e)(2) - Clinical Summary
<b>direct-ambulatory2@ttpedge.stenv.org</b>	ONC 2014 Edition Certification 170.314(b)(2) Transition of Care/Referral Summary - For Ambulatory Care
<b>direct-ambulatory7@ttpedge.stenv.org</b>	ONC 2014 Edition Certification 170.314(b)(7) Data Portability - For Ambulatory Care
<b>direct-ambulatory1@ttpedge.stenv.org</b>	ONC 2014 Edition Certification 170.314(b)(1) Transition of Care Receive - For Ambulatory Care
<b>direct-inpatient2@ttpedge.stenv.org</b>	ONC 2014 Edition Certification 170.314(b)(2) Transition of Care/Referral Summary - For Inpatient Care
<b>direct-inpatient7@ttpedge.stenv.org</b>	ONC 2014 Edition Certification 170.314(b)(7) Data Portability - For Inpatient Care
<b>direct-inpatient1@ttpedge.stenv.org</b>	MU 2 170.314(b)(1) Transition of Care Receive - For Inpatient Care
<b>direct-vdt-ambulatory@ttpedge.stenv.org</b>	ONC 2014 Edition Certification 170.314 (e)(1) Ambulatory Summary
<b>direct-vdt-inpatient@ttpedge.stenv.org</b>	ONC 2014 Edition Certification 170.314 (e)(1) Inpatient Summary
<b>ccda@ttpedge.stenv.org</b>	Non-specific CCDA

## 5.2 Send a Direct + XDM Message to the ETT

Sending messages via Direct + XDM is an optional mechanism for delivery notification outlined by the Objectives contained within ONC's Standards & Certification Criteria 2014/2015 Edition.

The prerequisite to sending messages to the ETT via Direct + XDM is registering a Direct email address. To register a Direct email address, refer to [Section 4.1](#) of this User Guide.

1. Once registered with the ETT, select the ONC Objective that is representative and appropriate for content you are sending. The sending content will automatically be validated and a validation report will be sent to the contact email address entered during sign up/registration.
2. Select the Direct email addresses to send the content.

## 5.3 Send a SOAP Message to the ETT

Sending messages via SOAP is a mechanism for Message Tracking (MT) outlined in the objectives contained within ONC's Standards & Certification Criteria 2015 Edition. Unlike the previous mechanisms, Direct and Direct + XDM, SOAP allows a user to make a remote function call over the internet using the same process one would for a normal web address.

There are two Objectives for which a user can send messages via SOAP:

- Transitions of Care (*Ambulatory*)
- Transitions of Care (*Inpatient*)

**Note:** The endpoints above are sample only. The actual endpoints are generated by the ETT.

## 6.0 SENDING MESSAGES FROM THE EDGE TESTING TOOL TO A SYSTEM UNDER TEST

As outlined in the [Section 1.4](#) of this User Guide and per ONC's Standards & Certification Criteria 2015 Edition, there are three (3) different mechanisms via which users can receive messages with CCR, C-CDA, or C32 attachments from the ETT:

**Table 2: ETT Message Receiving**

	Direct								
	S/MIME			XDM Attachment Messages			SOAP		
	CCR	C-CDA	C32	CCR <i>S/MIMI</i> <i>XDM</i>	C-CDA <i>S/MIMI</i> <i>XDM</i>	C32 <i>S/MIMI</i> <i>XDM</i>	CCR	C-CDA	C32
<b>Required</b>									
<b>Optional</b>									

Required  Optional

### 6.1 Send a Direct Message to a System Under Test

A user may receive CCR, CDA, and/or C32 files from the ETT via Direct messages. The process to receive Direct messages is outlined below.

1. From the Home Page, click **Direct Testing**, and then click on the **Send Direct Message** tab on the toolbar.

2. Data input into the **Direct From Address** field must align with the address the SUT is expecting to receive email from. The MDN will be sent back to the ETT using this address and the associated name will appear in the From field of the message sent.
3. In the **Direct To Address** field, input the Direct address where the message will be sent. This field will only accept one email address; not multiple. Send a Direct message with the attached C-CDA document to an authorized email addresses corresponding to the Objective under test (refer to **Table 1: Direct Address** in [Section 5.1](#) of this User Guide).
4. Complete the **Subject** line and enter a **Text Message**, if desired.
5. Select from one of the six samples within the **Choose document to be sent as the message content** pull-down menu. There are two (2) C-CCDA, two (2) CCR and two (2) C32 samples to select from. Or, you may **Upload your own CCDA** by clicking the **Upload File** button or **Drag and Drop** your file into the upload box. There is an XDM version for each of the samples. Do not select samples ending with \_in\_XDM.
6. Select a message format of **Wrapped** or **Unwrapped**. These actions will either wrap (or not) a message according to RFC 5751. All applications must support Unwrapped. Wrapped is optional.

7. Select the **Signing Certificate** or select **message with invalid digest** (message which has been altered).
8. Select the **Encryption Certificate**.
9. Click the **Send** button to send the Direct message.
10. Verify the MDN was received using the instructions within [Section 6.0](#) in this User Guide.

## 6.2 Send a Direct + XDM Message to a System Under Test

A user may receive CCR, C-CDA, and/or C32 attachments from the ETT via Direct + XDM. The process to receive Direct + XDM messages is outlined below.

1. From the [Home Page](#), click **Direct Testing**, and then click on the **Send Direct Message** tab. When the ETT is sending a Direct message to a SUT, no validation report will be sent to the SUT's contact email address.
2. In the **Direct From Address** field, this must be the address the SUT is expecting to receive mail from. The MDN will be sent back to ETT using this address and this name will appear in the message sent in the From field.
3. In the **Direct To Address** field, input the Direct address where the message will be sent. This field will only accept one email address; not multiple. Send a Direct message with the attached C-CDA document to an authorized email addresses corresponding to the Objective under test (refer to **Table 1: Direct Address** in [Section 5.1](#) of this User Guide).
4. Complete the **Subject** line and enter a **Text Message**, if desired.
5. Select from one of the six samples within the **Choose document to be sent as the message content** pull-down menu. There are two (2) C-CCDA, two (2) CCR and two (2) C32 samples to select from. Or, you may **Upload your own CCDA** by clicking the **Upload File** button or **Drag and Drop** your file into the upload box. There is an XDM version for each of the samples. Select samples ending with **\_in\_XDM**.
6. Select a message format of **Wrapped** or **Unwrapped**. These actions will either wrap (or not) a message according to RFC 5751. All applications must support Unwrapped. Wrapped is optional.
7. Select the **Signing Certificate** or select **message with invalid digest** (message which had been altered).
8. Select the **Encryption Certificate**.
9. Click the **Send** button to send the Direct message.
10. Verify the MDN was received using the instructions within [Section 6.0](#) in this User Guide.

## 7.0 SMTP TESTING

### 7.1 SMTP Test Cases

*Note: Within the ETT User Interface (UI), SMTP Test Cases 1 – 8, 14, and 18 are condensed into a single executable test. Therefore, the testing steps performed for these Test Cases are consistent across the set.*

#### 7.1.1 SMTP Test Cases 1-8, 14, 18 (Sender)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the sender, can initiate and execute the correct sequence of SMTP protocols and commands needed to successfully establish a connection with a HISP (i.e., ETT), acting as the receiver.

The testing details for conformance testing flow are as follows:

1. The vendor performing this Test Case and in operation of the SUT will navigate to their SMTP email client and create a single new message. This message must be accurately formed and in the correct syntax. The SUT will send the message to the target ETT endpoint recipient: [wellformed1@tppedge.sitenv.org](mailto:wellformed1@tppedge.sitenv.org). The SUT will attempt to initiate a secure connection with the ETT based on the STARTTLS protocols.
2. The vendor validates that the SUT successfully transmitted the message, executed the correct sequence of STARTTLS protocols and commands to establish a secure connection with the ETT, received the correct STARTTLS response command, and conformed to the specified requirements within [RFC 2487, Section 5](#).

This is a **conditional test** and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.2.3 of the [Implementation Guide for Direct Edge Protocols](#) document.

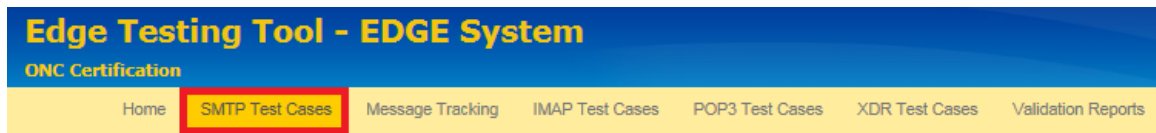
This test correlates to Test ID 14 of the SMTP Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and §170.314(b)(8) – 3.01 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

##### 7.1.1.1 Testing Steps

To execute SMTP Test 1-8, 14, 18 and assess the SUT's ability to accurately create a conformant message and establish a secure connection with the ETT through using the correct sequence of STARTTLS protocols and commands, the vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).

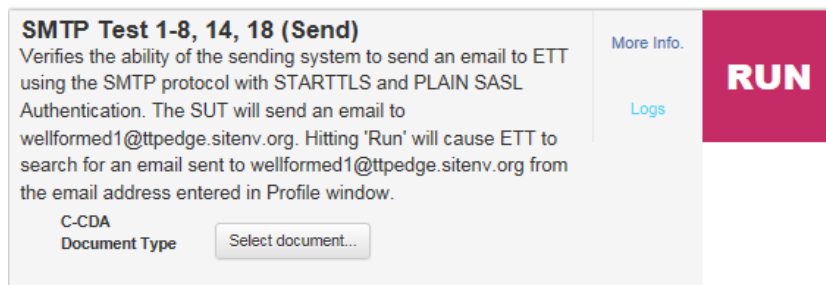
- For this target SMTP test, select **SMTP Test Cases** from the navigation bar (after clicking on Edge Testing from the Home Page). This enables the testing Profile feature of the tool.



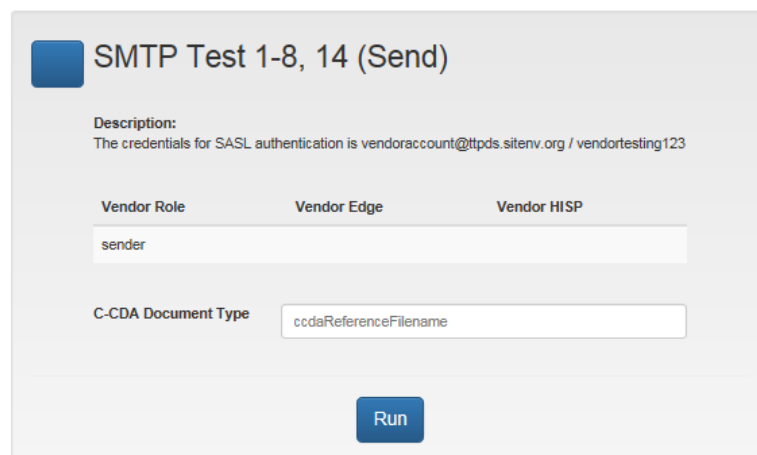
- From the testing Profile, select **Sender**.

Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.2.1 Profile Creation](#).

- To initiate SMTP Test Case 14 (in ETT UI as SMTP Test 1-8, 14, 18), the vendor navigates to the Test Case's execution interface.



To gain additional information concerning SMTP Test 1-8, 14, 18's intended purpose (including description and vendor/SUT roles), click the **More Info** link for the Test Case.



- With the Profile saved, More Info reviewed, and **SMTP Test 1-8, 14, 18** selected, the vendor performs the following test steps:

- A. Navigate to the SUT's messaging client/interface for **vendor SMTP Email Address** (specified in the Profile).
  - B. Create a single new message and send it to the ETT endpoint recipient [wellformed1@tppedge.sitenv.org](mailto:wellformed1@tppedge.sitenv.org).
  - C. Navigate to the ETT and SMTP Test 1-8, 14, 18 execution interface:
    - a. Wait at least 60 seconds from sending the message to allow for successful transmission to the ETT endpoint recipient.
    - b. Click **Run** to execute the test.
6. The test will process and render one of two results in the Test Case execution interface:
- Pass or Fail.**
- A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
  - A test Fail prompts the vendor to **Retry** the test.
  - The **Clear** button resets the test and any data input field values.
  - For test with Fail results, reference Section 3.0 Testing Configuration for Edge System and Section 2.2.1 Profile Creation of this ETT User Manual to assure that the accurate configurations have been implemented.
7. To validate that the test results conformed to the testing Objective(s) and gain additional information concerning the results or outcome of SMTP Test 1-8, 14, 18, click the **Logs** link.

Testing outcomes can be reviewed by analyzing the applicable results for **Criteria Met**, **Request Timeout**, **Proctored**, **Time elapsed**, **Request responses**, and **Attachments**.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Pass** or **Fail**). The **Log** is generated to view individual test result details (e.g., constraints, conformance details, contributing factors for **Pass** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view validation results by Profile configured and Test Case(s) executed.*

### 7.1.2 SMTP Test Cases 9, 16, 20 (Receiver)

***Note:** Within the ETT IU, SMTP Test Cases 9, 16, and 20 are condensed into a single executable test. Thus, the Testing Steps performed for these Test Cases are consistent across the set.*

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the receiver, can accept a request from the HISP (i.e., ETT), acting as the sender, to establish a secure connection and execute the needed sequence of SMTP protocols and commands.

The testing details for conformance testing flow are as follows:



1. The vendor navigates to the SMTP Test Case Profile and populates the vendor SMTP Hostname/IP, vendor SMTP Email Address, vendor SMTP Username, and vendor Password with accurate information (all fields should correlate so the ETT and SUT can communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
2. The vendor executes the test by clicking **Run** in the ETT for the target Test Case. Once the ETT processes the test, the vendor is presented with a **Waiting Validation** prompt.
3. The vendor performing this Test Case and in operation of the SUT will navigate to their SMTP email client and check for a new message from the ETT sending endpoint [wellformed1@ttpedge.sitenv.org](mailto:wellformed1@ttpedge.sitenv.org). If successful, the ETT will leverage the SMTP Profile data and send a message to the SMTP email client. This message will have the header of *Testing STARTTLS & PLAIN SASL AUTHENTICATION (Test Cases 9, 16, 20)!* and a *CCDA\_Ambulatory.XML* attachment (attachment contains sample metadata).
4. The vendor validates that the SUT successfully transmitted the message, the message header and attachment conformed to testing details/parameters, the SUT accepted the ETT's request to initiate a secure session using SMTP protocols/commands, and testing conformed to the specified requirements within [RFC 2821](#).

This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.2.1 and 1.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 9 of the SMTP Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 5.07, TE170.314(b)(8) – 5.08, and TE170.314(b)(8) – 5.09 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

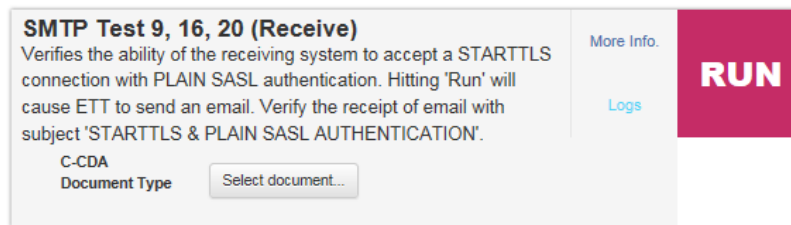
### 7.1.2.1 Testing Steps

To execute SMTP Test Case 9 and assess the SUT's ability to accept a request from the ETT to initiate a secure session using SMTP protocols/commands, the vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the navigation bar. This enables the testing Profile feature of the tool.
3. From the testing Profile, select **Receiver**.

Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.2.1 Profile Creation](#).

4. To initiate SMTP Test Case 9, the vendor navigates to the Test Case's execution interface.



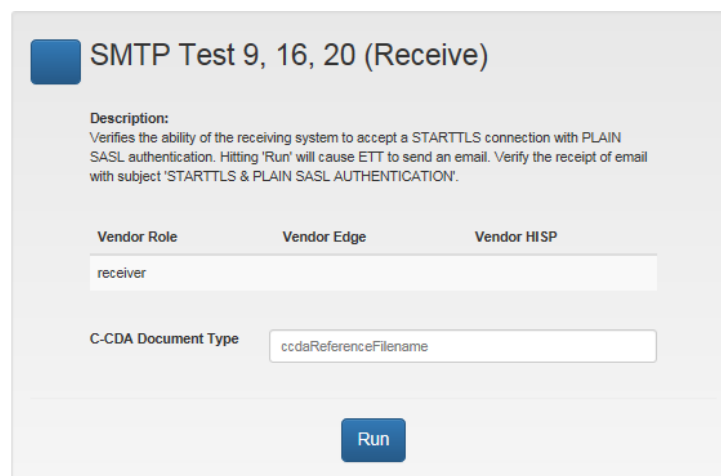
**SMTP Test 9, 16, 20 (Receive)**  
 Verifies the ability of the receiving system to accept a STARTTLS connection with PLAIN SASL authentication. Hitting 'Run' will cause ETT to send an email. Verify the receipt of email with subject 'STARTTLS & PLAIN SASL AUTHENTICATION'.

[More Info.](#)  
[Logs](#)

**RUN**

C-CDA Document Type

To gain additional information concerning SMTP Test 9's intended purpose (including Description, Vendor/SUT roles), click the **More Info** link for the Test Case.



**SMTP Test 9, 16, 20 (Receive)**

**Description:**  
 Verifies the ability of the receiving system to accept a STARTTLS connection with PLAIN SASL authentication. Hitting 'Run' will cause ETT to send an email. Verify the receipt of email with subject 'STARTTLS & PLAIN SASL AUTHENTICATION'.

Vendor Role	Vendor Edge	Vendor HISP
receiver		

C-CDA Document Type

**Run**

5. With the Profile saved, More Info reviewed, and **SMTP Test 9** selected, the vendor performs the following Test Steps:
  - A. Click **Run** to execute the test.
  - B. Navigate to the SUT's messaging client/interface for **Vendor SMTP Email Address** (specified in the Profile).
    - a. Wait at least 60 seconds from executing the test to allow successful transmission to the SUT.
    - b. Check the **Vendor SMTP Email Address** to validate that a new message is present.
6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
  - A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
  - A test Fail prompts the vendor to **Retry** the test.
  - The **Clear** button resets the test and any data input field values.

- For test with Fail results, refer to Section 2.0 (Testing Configuration for Edge System) and Section 2.2.1 (Profile Creation) of this ETT User Guide to ensure that the accurate configurations have been implemented.
7. To validate that the test results conformed to the testing objective(s) and gain additional information concerning the results or outcome of SMTP Test 9, click the **Log** link.

Testing outcomes can be reviewed by analyzing the applicable results for **Criteria Met, Request Timeout, Proctored, Time Elapsed, Request Response, and Attachments**.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Pass** or **Fail**). The **Log** is generated to view individual test result details (e.g., constraints, conformance details, contributing factors for **Pass** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view validation results by Profile configured and Test Case(s) executed.*

### 7.1.3 SMTP Test Case 10 (Receiver – Reject Invalid Data)

The objective of this **negative test** sequence is to determine if an Edge System (i.e., SUT), acting as the receiver, can reject invalid data (e.g., bad line feeds) sent from a HISP (i.e., ETT), acting as the sender, as a DATA command component during a secure connection attempt.

The testing details for conformance testing flow are as follows:

1. The vendor navigates to the SMTP Test Case Profile and populates the vendor SMTP Hostname/IP, vendor SMTP Email Address, vendor SMTP Username, and vendor Password with accurate information (all fields should correlate so the ETT and SUT can communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
2. Upon test execution, the vendor performing this Test Case and in operation of the SUT will navigate to their SMTP email client and check to ensure that a new message from the ETT sending endpoint [wellformed3@tppedge.sitenv.org](mailto:wellformed3@tppedge.sitenv.org) is not present. The presence of a new message indicates a test fail.
3. The vendor validates that the SUT successfully acknowledged the ETT's invalid DATA command and rejected the connection attempt, successfully rejected the ETT sending endpoint's message transmission attempt, and that testing conformed to the specified requirements within [RFC 2821](#).

This test and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.2.1 and 1.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 10 of the SMTP Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 5.10 within the [ONC 2014 Edition approved Test Procedure](#)

[requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

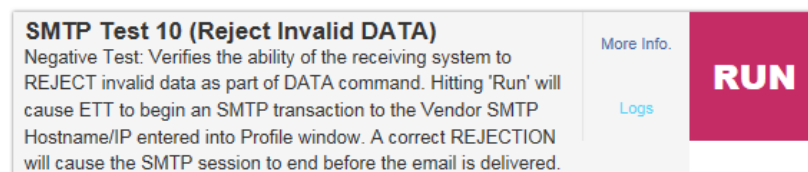
### 7.1.3.1 Testing Steps

To execute SMTP Test Case 10 and assess the SUT's ability to successfully acknowledge and reject a connection attempt from a HISP using an invalid DATA command, the vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the navigation bar. This enables the testing Profile feature of the tool.
3. From the testing Profile, select **Receiver**.

Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.2.1 Profile Creation](#).

4. To initiate SMTP Test Case 10, the vendor navigates to the Test Case's execution interface.



To gain additional information concerning SMTP Test 10's intended purpose (including description and vendor/SUT roles), click the **More Info** link for the Test Case.

### SMTP Test 10 (Reject Invalid DATA)

**Description:**  
 The objective of this test sequence is to determine if an Edge System (e.g., SUT), acting as the receiver, rejects data sent from a HISP (e.g., ETT), acting as the sender, as a component of a successfully established and active session. Successful establishment of an end-point to end-point connection between the SUT and ETT is a necessary function for SMTP Test Case 10 execution. The details for conformance testing flow are as follows: The ETT will initiate a connected session with the SUT and attempt to send an invalid data via the DATA command (e.g., bad line feeds). This is required test and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.2.1 and 1.2.2 of the 'Implementation Guide for Direct Edge Protocols' document. The test correlates to Test ID 10 of the SMTP Test Cases (tab) within the 'DirectEdgeProtocols' spreadsheet.

Vendor Role	Vendor Edge	Vendor HISP
receiver		

Run

5. With the Profile saved, More Info reviewed, and **SMTP Test 10** selected, perform the following Test Steps:

- A. Click **Run** to execute the test.
- B. Navigate the to SUT's messaging client/interface for **Vendor SMTP Email Address** (specified in the Profile).
  - a. Wait at least 60 seconds from executing the test to allow successful transmission to the SUT.
  - b. Check the **Vendor SMTP Email Address** to validate that a new message is not present from the ETT sending endpoint [wellformed3@ttpedge.sitenv.org](mailto:wellformed3@ttpedge.sitenv.org) (this is a negative test).

***Note:** The vendor, in execution of SMTP Test Case 10, should not receive a message in the **Vendor SMTP Email Address** from the ETT. This is a negative test attempting to assess the capability of the SUT to reject a connection attempt that uses an invalid DATA command. Thus, the SUT should reject the data and terminate the connection before receiving the transmission of a message from the ETT sending endpoint [wellformed3@ttpedge.sitenv.gov](mailto:wellformed3@ttpedge.sitenv.gov). The presence of an email from this endpoint indicates a test **Fail**.*

6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
  - a. A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
  - b. A test Fail prompts the vendor to **Retry** the test.
  - c. The **Clear** button resets the test and any data input field values.
  - d. For test with Fail results, refer to Section 2.0 (Testing Configuration for Edge System) and Section 2.2.1 (Profile Creation) of this ETT User Guide to ensure that the accurate configurations have been implemented.

7. To validate that the test results conformed to the testing Objective(s) and gain additional information concerning the results or outcome of SMTP Test 10, click the **Log** link.

Testing outcomes can be reviewed by analyzing the applicable results for **Criteria Met**, **Request Timeout**, **Proctored**, **Time Elapsed**, **Request Response**, and **Attachments**.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Pass** or **Fail**). The **Log** is generated to view individual test result details (e.g., constraints, conformance details, contributing factors for **Pass** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view validation results by Profile configured and Test Case(s) executed.*

#### 7.1.4 SMTP Test Case 11 (Receiver – Reject Bad Commands)

The objective of this **negative test** sequence is to determine if an Edge System (i.e., SUT), acting as the receiver, can reject an invalid command sent from a HISP (i.e., ETT), acting as the sender, during an SMTP session connection attempt.

The testing details for conformance testing flow are as follows:

1. The vendor navigates to the SMTP Test Case Profile and populates the Vendor SMTP Hostname/IP, Vendor SMTP Email Address, Vendor SMTP Username, and Vendor Password with accurate information (all fields should correlate so the ETT and SUT can communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
2. Upon test execution, the vendor performing this Test Case and in operation of the SUT will navigate to their SMTP email client and check to assure a new message from the ETT has not been sent. The session should terminate before a message transaction has been sent.
3. The vendor validates that the SUT successfully acknowledged the ETT's attempt to connect using invalid SMTP commands, successfully rejected the SMTP connection attempt from the ETT, and that testing conformed to the specified requirements within [RFC 2821, Sections 4.1.1 and 4.1.4](#).

This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.2.1 and 1.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 11 of the SMTP Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and TE 170.314(b)(1) the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

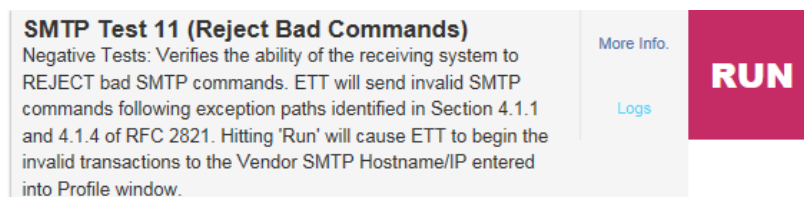
### 7.1.4.1 Testing Steps

To execute SMTP Test Case 11 and assess the SUT's ability to successfully acknowledge and reject a connection attempt from a HISP using an invalid SMTP commands, the vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the navigation bar. This enables the testing Profile feature of the tool.
3. From the testing Profile, select **Receiver**.

Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.2.1 Profile Creation](#).

4. To initiate SMTP Test Case 11, the Vendor navigates to the Test Case's execution interface.



To gain additional information concerning SMTP Test 11's intended purpose (including description and vendor/SUT roles), click the **More Info** link for the Test Case.

### SMTP Test 11 (Reject Bad Commands)

**Description:**  
 The objective of this test sequence is to determine if an Edge System (e.g., SUT), acting as the receiver, rejects as invalid the commands sent from a HISP (e.g., ETT), acting as the sender. The details for conformance testing flow are as follows: The ETT attempts to initiate a session with the SUT by sending an invalid SMTP command following identified exception paths. The test attempts to determine if the SUT rejects the command sent by the Edge Testing Tool as invalid and responds using the appropriate mechanisms. This is conducted in accordance with RFC 2811, Section 4.1.1 and 4.1.4 (e.g., closing the session abruptly). This is required test and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.2.1 and 1.2.2 of the 'Implementation Guide for Direct Edge Protocols' document. The test correlates to Test ID 11 of the SMTP Test Cases (tab) within the 'DirectEdgeProtocols' spreadsheet.

Vendor Role	Vendor Edge	Vendor HISP
receiver		

Run

5. With the Profile saved, More Info reviewed, and **SMTP Test 11** selected, the vendor performs the following test steps:
  - A. Click **Run** to execute the test.
  - B. Navigate the to SUT's messaging client/interface for **Vendor SMTP Email Address** (specified in the Profile).
    - a. Wait at least 60 seconds from executing the test to allow successful transmission to the SUT.
    - b. Check the **Vendor SMTP Email Address** to validate that a new message is not present (this is a negative test).

**Note:** The vendor, in execution of SMTP Test Case 10, should not receive a message in the **Vendor SMTP Email Address** from the ETT. This is a negative test attempting to assess the capability of the SUT to reject a connection attempt that uses invalid SMTP commands. Thus, the SUT should terminate the connection before receiving the transmission of a message.

6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
  - a. A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
  - b. A test Fail prompts the vendor to **Retry** the test.
  - c. The **Clear** button resets the test and any data input field values.
  - d. For test with Fail results, refer to Section 2.0 (Testing Configuration for Edge System) and Section 2.2.1 (Profile Creation) of this ETT User Guide to ensure that the accurate configurations have been implemented.



7. To validate that the test results conformed to the testing Objective(s) and gain additional information concerning the results or outcome of SMTP Test 11, click the **Log** link.

Testing outcomes can be reviewed by analyzing the applicable results for **Criteria Met, Request Timeout, Proctored, Time Elapsed, Request Response**, and **Attachments**.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Pass** or **Fail**). The **Log** is generated to view individual test result details (e.g., constraints, conformance details, contributing factors for **Pass** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view validation results by Profile configured and Test Case(s) executed.*

### 7.1.5 SMTP Test Case 13 (Receiver – Command Timeout)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the receiver, can successfully initiate, establish, and close an active session with a HISP (i.e., ETT), acting as the sender, in conformance with SMTP timeout specifications.

The testing details for conformance testing flow are as follows:

1. The vendor navigates to the SMTP Test Case Profile and populates the Vendor SMTP Hostname/IP, Vendor SMTP Email Address, Vendor SMTP Username, and Vendor Password with accurate information (all fields should correlate so the ETT and SUT and communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
2. The vendor will identify the constrainable target timeout duration (represented in seconds) the SUT will be tested against.
3. Upon test execution, the vendor performing this Test Case will wait for the timeout value entered to expire.
4. The vendor validates that the SUT successfully initiated and established a SMTP connection with the ETT, the SUT closed the active session per the entered timeout value, and that testing conformed to the specified requirements within [RFC 2821, Section 4.5.3.2](#).

This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.2.1 and 1.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 13 of the SMTP Test Cases tab within the [Direct Edge Protocols](#) spreadsheet TE170.314(b)(8) – 5.13 within the [ONC 2014 Edition approved Test Procedure](#)

[requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

### 7.1.5.1 Testing Steps

To execute SMTP Test Case 13 and assess the SUT's ability to successfully initiate, establish, and close an active SMTP session per specified timeout constraints, the vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the navigation bar. This enables the testing Profile feature of the tool.
3. From the testing Profile, select **Receiver**.

Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.2.1 Profile Creation](#).

4. To initiate SMTP Test Case 13, the Vendor navigates to the Test Case's execution interface.

**SMTP Test 13 (Command Timeout)**  
 Verifies the ability of the receiving system to correctly timeout for various SMTP commands. The tool will keep the transaction open until a timeout is noted. As there are no required time limits in RFC 2821 section 4.5.3.2, this test is configurable. Hitting 'Run' will begin the ETT's timer based on the value in seconds entered below. The default entry, 0, allows a maximum time-out (no limit). Enter a value greater than your systems time-out period to perform this test.

More Info.

Logs

**RUN**

Command timeout in seconds:

To gain additional information concerning SMTP Test 13's intended purpose (including Description, Vendor/SUT roles), click **More Info** link for the Test Case.

SMTP Test 13 (Command Timeout)

**Description:**  
The objective of this test sequence is to determine if an Edge System (e.g., SUT), acting as the receiver, can successfully establish an active session with a HISP (e.g., ETT), acting as the sender, and conform to the specific timeout requirements within the RFC and SMTP command. The details for conformance testing flow are as follows: The ETT will initiate a connected session with the SUT. The SUT will attempt to keep a transaction open with the ETT for beyond the specified time constraints found within RFC 2821, Section 4.5.3.2. This is required test and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.2.1 and 1.2.2 of the 'Implementation Guide for Direct Edge Protocols' document.

Vendor Role

Vendor Edge

Vendor HISP

receiver

Command timeout in seconds

sutCommandTimeoutInSeconds

Run

5. With the Profile saved, More Info reviewed, and **SMTP Test 13** selected, the vendor performs the following test steps:
  - A. On the SMTP Test 13's execution interface, enter the specific timeout threshold to test the SUT against in the **Command Timeout in Seconds** field.
  - B. Click **Run** to execute the test.

**Note:** The vendor, in execution of SMTP Test Case 13, must enter the timeout threshold value specific to the SUT testing need. RFC 2821, Section 4.5.3.2 does not require specific time dependent testing restrictions. However, examples of testable timeout constraints include:

- Initial 220 Message: 300 seconds
- MAIL Command: 300 seconds
- RCPT Command: 300 seconds
- DATA Initiation: 120 seconds

6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
  - a. A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
  - b. A test Fail prompts the vendor to **Retry** the test.
  - c. The **Clear** button resets the test and any data input field values.
  - d. For test with Fail results, refer to Section 2.0 (Testing Configuration for Edge System) and Section 2.2.1 (Profile Creation) of this ETT User Guide to ensure that the accurate configurations have been implemented.
7. To validate that the test results conformed to the testing objective(s) and gain additional information concerning the results or outcome of SMTP Test 13, click the **Log** link.

Testing outcomes can be reviewed by analyzing the applicable results for **Criteria Met, Request Timeout, Proctored, Time Elapsed, Request Response**, and **Attachments**.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Pass** or **Fail**). The **Log** is generated to view individual test result details (e.g., constraints, conformance details, contributing factors for **Pass** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view validation results by Profile configured and Test Case(s) executed.*

### 7.1.6 SMTP Test Case 17 (Receiver - Reject Invalid STARTTLS)

The objective of this **negative test** sequence is to determine if an Edge System (i.e., SUT), acting as the receiver, can reject an invalid STARTTLS command send from a HISP (i.e., ETT), acting as the sender, during a secure TLS session connection attempt.

The testing details for conformance testing flow are as follows:

1. The vendor navigates to the SMTP Test Case Profile and populates the Vendor SMTP Hostname/IP, Vendor SMTP Email Address, Vendor SMTP Username, and Vendor Password with accurate information (all fields should correlate so the ETT and SUT and communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
2. Upon test execution, the vendor performing this Test Case and in operation of the SUT will navigate to their SMTP email client and check to assure a new message from the ETT has not been sent. The session should terminate before a message transaction has been sent.
3. The vendor validates that the SUT successfully acknowledged the ETT's TLS connection attempt, identified the ETT's invalid STARTTLS commands and reject the session initiation attempt, and that testing conformed to the specified requirements within [RFC 2487](#).

This is a **conditional test** and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.2.3 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 17 of the SMTP Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 5.02 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

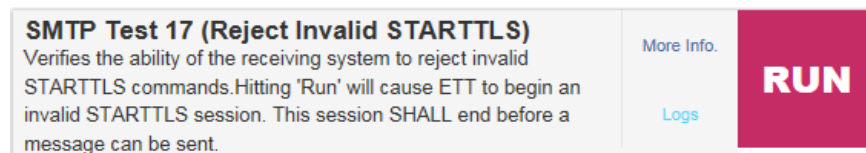
### 7.1.6.1 Testing Steps

To execute SMTP Test Case 17 and assess the SUT's ability to reject a TLS connection attempt using invalid STARTTLS commands, the vendor must perform the following steps:

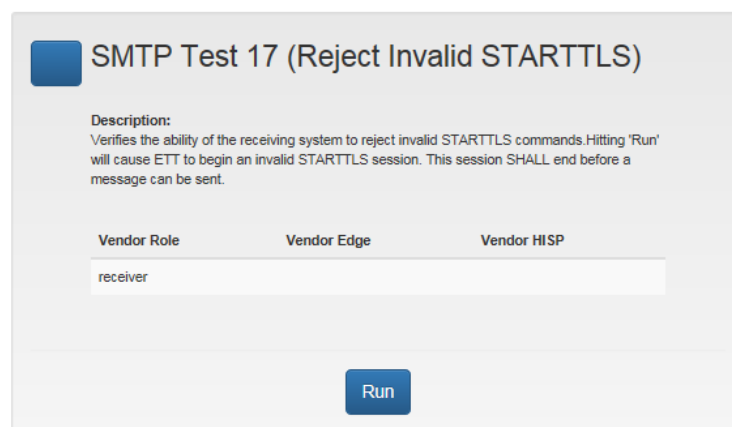
1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target SMTP test, select '**SMTP Test Cases**' from the navigation bar. This enables the testing Profile feature of the tool.
3. From the testing Profile, select **Receiver**.

Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.2.1 Profile Creation](#).

4. To initiate SMTP Test Case 17, the vendor navigates to the Test Case's execution interface.



To gain additional information concerning SMTP Test Case 17's intended purpose (including Description, Vendor/SUT roles), click the **More Info** link for the Test Case.



5. With the Profile saved, More Info reviewed, and **SMTP Test 17** selected, the Vendor performs the following Test Steps:

A. Click **Run** to execute the test.

- Note:** The vendor, in execution of SMTP Test Case 17, should not receive a message in the **Vendor SMTP Email Address** from the ETT. This is a negative test attempting to assess the capability of the SUT to reject a connection attempt that uses an invalid STARTTLS command. Thus, the SUT should reject the data and terminate the connection before receiving the transmission of a message.

- Testing outcomes can be reviewed by analyzing the applicable results for **Criteria Met, Request Timeout, Proctored, Time Elapsed, Request Response**, and **Attachments**.

**Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Pass** or **Fail**). The **Log** is generated to view individual test result details (e.g., constraints, conformance details, contributing factors for **Pass** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view validation results by Profile configured and Test Case(s) executed.

### 7.1.7

The testing details for conformance testing flow are as follows:

1. The Tester (i.e., Vendor) navigates to the SMTP Test Case Profile and populates the Vendor SMTP Hostname/IP, Vendor SMTP Email Address, Vendor SMTP Username, and Vendor Password with accurate information (all fields should correlate so the ETT and SUT and communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
2. Upon test execution, the Vendor performing this Test Case and in operation of the SUT will navigate to their SMTP email client and check to assure a new message from the ETT has not been sent. The session should terminate before a message transaction has been sent.
3. The Vendor validates that the SUT successfully acknowledged the ETT's authentication attempt, identified the ETT's invalid PLAIN SASL credentials and rejected the authentication attempt, and that testing conformed to the specified requirements within [RFC 2831](#) and [RFC 4616](#).

This is a **conditional test** and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.2.4 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 22 of the SMTP Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 5.05 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

#### **7.1.7.1 Testing Steps**

To execute SMTP Test Case 22 and assess the SUT's ability to reject an authentication connection attempt using invalid PLAIN SASL credentials, the vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the navigation bar. This enables the testing Profile feature of the tool.
3. From the testing Profile, select **Receiver**.

Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.2.1 Profile Creation](#).

4. To initiate SMTP Test Case 22, the vendor navigates to the Test Case's execution interface.



### SMTP Test 22 (Reject invalid username/password)

Verifies the ability of the receiving to reject a PLAIN SASL connection. Hitting 'Run' will cause ETT to use an invalid username/password to authenticate to the system entered into Vendor SMTP Hostname/IP in the profile window.

[More Info.](#)  
  
[Logs](#)

RUN

To gain additional information concerning SMTP Test 22's intended purpose (including Description, Vendor/SUT roles), click **More Info** link for the Test Case.

SMTP Test 22 (Reject invalid username/password)

**Description:**  
The objective of this test sequence is to determine if an Edge System (e.g., SUT), acting as the receiver, will reject and fail to authenticate an invalid PLAIN SASL request sent from a HISP (e.g., ETT), acting as the sender. The details for conformance testing flow are as follows: The ETT will send an invalid PLAIN SASL username/password authentication scheme to the SUT. The SUT will receive the invalid PLAIN SASL username/password, reject the credentials, and fail to established authentication to the ETT. The PLAIN SASL connection mechanisms will conform to the specified requirements within RFC 4616, Section 2. This is conditional test and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.2.4 of the 'Implementation Guide for Direct Edge Protocols' document. The test correlates to Test ID 22 of the SMTP Test Cases (tab) within the 'DirectEdgeProtocols' spreadsheet.

Vendor Role	Vendor Edge	Vendor HISP
receiver		

Run

5. With the Profile saved, More Info reviewed, and **SMTP Test 22** selected, the Vendor performs the following Test Steps:
  - A. Click **Run** to execute the test.
  - B. Navigate the to SUT's messaging client/interface for **Vendor SMTP Email Address** (specified in the Profile).
    - a. Wait at least 60 seconds from executing the test to allow successful transmission to the SUT.
    - b. Check the **Vendor SMTP Email Address** to validate that a new message is not present (this is a negative test).

**Note:** The vendor, in execution of SMTP Test Case 22, should not receive a message in the **Vendor SMTP Email Address** from the ETT. This is a negative test attempting to assess the capability of the SUT to reject a connection attempt that uses invalid PLAIN SASL credentials. Thus, the SUT should reject the data and terminate the connection before receiving the transmission of a message.



6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
  - A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
  - A test Fail prompts the vendor to **Retry** the test.
  - The **Clear** button resets the test and any data input field values.
  - For test with Fail results, refer to Section 2.0 (Testing Configuration for Edge System) and Section 2.2.1 (Profile Creation) of this ETT User Guide to ensure that the accurate configurations have been implemented.
7. To validate that the test results conformed to the testing objective(s) and gain additional information concerning the results or outcome of SMTP Test 22, click the **Log** link.

Testing outcomes can be reviewed by analyzing the applicable results for **Criteria Met, Request Timeout, Proctored, Time Elapsed, Request Response, and Attachments**.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Pass** or **Fail**). The **Log** is generated to view individual test result details (e.g., constraints, conformance details, contributing factors for **Pass** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view validation results by Profile configured and Test Case(s) executed.*

### 7.1.8 SMTP Test Cases 25(a)-(f) (Receiver - Text and CCDA, Pdf and CCDA, Text and XDM, CCDA and Text, CCDA and Pdf, and XDM and Text)

The objective of this test series of tests is to determine if an Edge System (i.e., SUT), acting as the receiver, can receive the following from the HISP (i.e., ETT), acting as the sender:

1. 25(a) Text and CCDA attachments;
2. 25(b) Pdf and CCDA attachments;
3. 25(c) Text and XDM attachments;
4. 25(d) CCDA and Text attachments;
5. 25(e) CCDA and Pdf attachments, and
6. 25(f) XDM and Text attachments.

The testing details for conformance testing flow are as follows:

1. The vendor navigates to the SMTP Test Case Profile and populates the vendor SMTP Hostname/IP, vendor SMTP Email Address, vendor SMTP Username, and vendor Password with accurate information (all fields should correlate so the ETT and SUT can communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).

2. The vendor executes the test by clicking **Run** in the ETT for the target Test Case. Once the ETT processes the test, the vendor is presented with a **Waiting Validation** prompt.
3. The vendor performing this Test Case and in operation of the SUT will navigate to their SMTP email client and check for a new message from the ETT sending endpoint [wellformed1@ttpedge.sitenv.org](mailto:wellformed1@ttpedge.sitenv.org). If successful, the ETT will leverage the SMTP Profile data and send a message to the SMTP email client. This message will have the attachment outline above that is appropriate to each test containing sample metadata.
4. The vendor validates that the SUT successfully transmitted the message, the message attachment conformed to testing details/parameters, the SUT accepted the ETT's request to initiate a secure session using SMTP protocols/commands, and testing conformed to the specified requirements within [RFC 2821](#).

This test and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.2.1 and 1.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 9 of the SMTP Test Cases tab within the [Direct Edge Protocols](#) spreadsheet within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

### **7.1.8.1 Testing Steps**

To execute SMTP Test Cases 25(a-f) and assess the SUT's ability to accept attachments, the vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the navigation bar. This enables the testing Profile feature of the tool.
3. From the testing Profile, select **Receiver**.

Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.2.1 Profile Creation](#).

4. To initiate SMTP Test Cases 25(a-f), the vendor navigates to the Test Case's execution interface.

<b>SMTP Test 25(a) (Receive Text and CCDA)</b> Verifies the ability of SUT to receive text and CCDA attachments	<a href="#">More Info.</a>  <a href="#">Logs</a>	<b>RUN</b>
<b>SMTP Test 25(b) (Receive PDF and CCDA)</b> Verifies the ability of SUT to receive PDF and CCDA attachments	<a href="#">More Info.</a>  <a href="#">Logs</a>	<b>RUN</b>
<b>SMTP Test 25(c) (Receive Text and XDM)</b> Verifies the ability of SUT to receive text and XDM attachments	<a href="#">More Info.</a>  <a href="#">Logs</a>	<b>RUN</b>
<b>SMTP Test 25(d) (Receive CCDA and Text)</b> Verifies the ability of SUT to receive CCDA and text attachments	<a href="#">More Info.</a>  <a href="#">Logs</a>	<b>RUN</b>
<b>SMTP Test 25(e) (Receive CCDA and Pdf)</b> Verifies the ability of SUT to receive CCDA and PDF attachments	<a href="#">More Info.</a>  <a href="#">Logs</a>	<b>RUN</b>
<b>SMTP Test 25(f) (Receive XDM and Text)</b> Verifies the ability of SUT to receive XDM and text attachments	<a href="#">More Info.</a>  <a href="#">Logs</a>	<b>RUN</b>

To gain additional information concerning SMTP Test Cases 25(a-f) intended purpose (including Description, Vendor/SUT roles), click **More Info** link for the Test Case. An example is below:

The screenshot shows a web interface for configuring a test. At the top, there is a blue square icon followed by the title "SMTP Test 25(a) (Receive Text and CCDA)". Below the title, a "Description:" label is followed by the text "Verifies the ability of SUT to receive text and CCDA attachments". Underneath, there are three labels: "Vendor Role", "Vendor Edge", and "Vendor HISP". Below these labels is a text input field containing the word "receiver". At the bottom center of the form is a blue button with the text "Run".

5. With the Profile saved, More Info reviewed, and **SMTP Test 25(a-f)** selected, the vendor performs the following Test Steps:
  - C. Click **Run** to execute the test.
  - D. Navigate the to SUT's messaging client/interface for **Vendor SMTP Email Address** (specified in the Profile).
    - a. Wait at least 60 seconds from executing the test to allow successful transmission to the SUT.
    - b. Check the **Vendor SMTP Email Address** to validate that a new message is present.
6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
  - A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
  - A test Fail prompts the vendor to **Retry** the test.
  - The **Clear** button resets the test and any data input field values.
  - For test with Fail results, refer to Section 2.0 (Testing Configuration for Edge System) and Section 2.2.1 (Profile Creation) of this ETT User Guide to ensure that the accurate configurations have been implemented.
7. To validate that the test results conformed to the testing objective(s) and gain additional information concerning the results or outcome of SMTP Test 25(a-f), click the **Log** link.

Testing outcomes can be reviewed by analyzing the applicable results for **Criteria Met, Request Timeout, Proctored, Time Elapsed, Request Response**, and **Attachments**.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Pass** or **Fail**). The **Log** is generated to view individual test result details (e.g., constraints, conformance details, contributing factors for **Pass** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view validation results by Profile configured and Test Case(s) executed.*

### 7.1.9 SMTP Test Cases 26(a-b) (Receiver – Receive Bad CCDA)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the receiver, can accept a request from the HISP (i.e., ETT), acting as the sender, to establish a secure connection, execute the needed sequence of SMTP protocols and commands and receive a bad CCDA.

The testing details for conformance testing flow are as follows:

1. The vendor navigates to the SMTP Test Case Profile and populates the vendor SMTP Hostname/IP, vendor SMTP Email Address, vendor SMTP Username, and vendor Password with accurate information (all fields should correlate so the ETT and SUT can communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
2. The vendor executes the test by clicking **Run** in the ETT for the target Test Case. Once the ETT processes the test, the vendor is presented with a **Waiting Validation** prompt.
3. The vendor performing this Test Case and in operation of the SUT will navigate to their SMTP email client and check for a new message from the ETT sending endpoint [wellformed1@tppedge.sitenv.org](mailto:wellformed1@tppedge.sitenv.org). If successful, the ETT will leverage the SMTP Profile data and send a message to the SMTP email client. This message will contain a CCDA document that either (1) includes a broken reference to a style-sheet or (2) with a good reference to an invalid style-sheet.
4. The vendor validates that the SUT successfully transmitted the message, the message header and attachment conformed to testing details/parameters, the SUT accepted the ETT's request to initiate a secure session using SMTP protocols/commands, and testing conformed to the specified requirements within [RFC 2821](#).

This test and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.2.1 and 1.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 9 of the SMTP Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

### 7.1.9.1 Testing Steps

To execute SMTP Test Cases 26(a-b) and assess the SUT's ability to accept a request from the ETT to initiate a secure session using SMTP protocols/commands, the vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the navigation bar. This enables the testing Profile feature of the tool.
3. From the testing Profile, select **Receiver**.

Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.2.1 Profile Creation](#).

4. To initiate SMTP Test Cases 26(a-b), the vendor navigates to the Test Case's execution interface.

<b>SMTP Test 26(a) (Receive bad CCDA)</b> Verifies the ability of SUT to receive a CCDA document that includes a broken reference to a style-sheet	<a href="#">More Info.</a>  <a href="#">Logs</a>	<b>RUN</b>
<b>SMTP Test 26(b) (Receive bad CCDA)</b> Verifies the ability of SUT to receive a CCDA document with good reference to an invalid style-sheet	<a href="#">More Info.</a>  <a href="#">Logs</a>	<b>RUN</b>

To gain additional information concerning SMTP Test 26(a-b)'s intended purpose (including Description, Vendor/SUT roles), click the **More Info** link for the Test Case.


**SMTP Test 26(a) (Receive bad CCDA)**

**Description:**  
Verifies the ability of SUT to receive a CCDA document that includes a broken reference to a style-sheet

Vendor Role	Vendor Edge	Vendor HISP
receiver		

Run

5. With the Profile saved, More Info reviewed, and **SMTP Test 26(a-b)** selected, the vendor performs the following Test Steps:
  - A. Click **Run** to execute the test.
  - B. Navigate the to SUT's messaging client/interface for **Vendor SMTP Email Address** (specified in the Profile).
    - a. Wait at least 60 seconds from executing the test to allow successful transmission to the SUT.
    - b. Check the **Vendor SMTP Email Address** to validate that a new message is present.
6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
  - A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
  - A test Fail prompts the vendor to **Retry** the test.
  - The **Clear** button resets the test and any data input field values.
  - For test with Fail results, refer to Section 2.0 (Testing Configuration for Edge System) and Section 2.2.1 (Profile Creation) of this ETT User Guide to ensure that the accurate configurations have been implemented.
7. To validate that the test results conformed to the testing objective(s) and gain additional information concerning the results or outcome of SMTP Test 26(a-b), click the **Log** link.

Testing outcomes can be reviewed by analyzing the applicable results for **Criteria Met, Request Timeout, Proctored, Time Elapsed, Request Response, and Attachments**.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Pass** or **Fail**). The **Log** is generated to view individual test result details (e.g., constraints, conformance details, contributing factors for **Pass** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view validation results by Profile configured and Test Case(s) executed.*

#### **7.1.10 SMTP Test Cases 27 (Receiver – Receive XDM with Bad XHTML)**

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the receiver, can accept a request from the HISP (i.e., ETT), acting as the sender, to establish a secure connection, execute the needed sequence of SMTP protocols and commands and receive an XDM package containing a bad XHTML file.

The testing details for conformance testing flow are as follows:

1. The vendor navigates to the SMTP Test Case Profile and populates the vendor SMTP Hostname/IP, vendor SMTP Email Address, vendor SMTP Username, and vendor

Password with accurate information (all fields should correlate so the ETT and SUT can communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).

2. The vendor executes the test by clicking **Run** in the ETT for the target Test Case. Once the ETT processes the test, the vendor is presented with a **Waiting Validation** prompt.
3. The vendor performing this Test Case and in operation of the SUT will navigate to their SMTP email client and check for a new message from the ETT sending endpoint [wellformed1@ttpedge.sitenv.org](mailto:wellformed1@ttpedge.sitenv.org). If successful, the ETT will leverage the SMTP Profile data and send a message to the SMTP email client. This message will contain an XDM package containing a bad XHTML file
4. The vendor validates that the SUT successfully transmitted the message, the message header and attachment conformed to testing details/parameters, the SUT accepted the ETT's request to initiate a secure session using SMTP protocols/commands, and testing conformed to the specified requirements within [RFC 2821](#).

This test and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.2.1 and 1.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 9 of the SMTP Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

#### 7.1.10.1 Testing Steps

To execute SMTP Test Cases 27 and assess the SUT's ability to accept a request from the ETT to initiate a secure session using SMTP protocols/commands, the vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the navigation bar. This enables the testing Profile feature of the tool.
3. From the testing Profile, select **Receiver**.

Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.2.1 Profile Creation](#).

4. To initiate SMTP Test Cases 27, the vendor navigates to the Test Case's execution interface.



<b>SMTP Test 27 (Receive XDM with bad XHTML)</b> Verifies the ability of SUT to receive an XDM package containing a bad XHTML file	<a href="#">More Info.</a>  <a href="#">Logs</a>	<div><b>RUN</b></div>
---	--	-----------------------

To gain additional information concerning SMTP Test 27's intended purpose (including Description, Vendor/SUT roles), click the **More Info** link for the Test Case.

SMTP Test 27 (Receive XDM with bad XHTML)

**Description:**  
Verifies the ability of SUT to receive an XDM package containing a bad XHTML file

Vendor Role	Vendor Edge	Vendor HISP
receiver		

Run

5. With the Profile saved, More Info reviewed, and **SMTP Test 27** selected, the vendor performs the following Test Steps:
  - A. Click **Run** to execute the test.
  - B. Navigate the to SUT's messaging client/interface for **Vendor SMTP Email Address** (specified in the Profile).
    - a. Wait at least 60 seconds from executing the test to allow successful transmission to the SUT.
    - b. Check the **Vendor SMTP Email Address** to validate that a new message is present.
6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
  - A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
  - A test Fail prompts the vendor to **Retry** the test.
  - The **Clear** button resets the test and any data input field values.
  - For test with Fail results, refer to Section 2.0 (Testing Configuration for Edge System) and Section 2.2.1 (Profile Creation) of this ETT User Guide to ensure that the accurate configurations have been implemented.
7. To validate that the test results conformed to the testing objective(s) and gain additional information concerning the results or outcome of SMTP Test 27, click the **Log** link.

Testing outcomes can be reviewed by analyzing the applicable results for **Criteria Met, Request Timeout, Proctored, Time Elapsed, Request Response**, and **Attachments**.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Pass** or **Fail**). The **Log** is generated to view individual test result details (e.g., constraints, conformance details, contributing factors for **Pass** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view validation results by Profile configured and Test Case(s) executed.*

### **7.1.11 SMTP Test Case 28 (Receiver - Receive XDM with MIME type 'application/octet-stream')**

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the receiver, can accept a request from the HISP (i.e., ETT), acting as the sender, to establish a secure connection, execute the needed sequence of SMTP protocols and commands and receive an XDM package with MIME-type 'application/octet-stream' at the SMTP layer.

The testing details for conformance testing flow are as follows:

1. The vendor navigates to the SMTP Test Case Profile and populates the vendor SMTP Hostname/IP, vendor SMTP Email Address, vendor SMTP Username, and vendor Password with accurate information (all fields should correlate so the ETT and SUT can communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
2. The vendor executes the test by clicking **Run** in the ETT for the target Test Case. Once the ETT processes the test, the vendor is presented with a **Waiting Validation** prompt.
3. The vendor performing this Test Case and in operation of the SUT will navigate to their SMTP email client and check for a new message from the ETT sending endpoint [wellformed1@ttpedge.sitenv.org](mailto:wellformed1@ttpedge.sitenv.org). If successful, the ETT will leverage the SMTP Profile data and send a message to the SMTP email client. This message will contain an XDM package with MIME-type 'application/octet-stream' at the SMTP layer.
4. The vendor validates that the SUT successfully transmitted the message, the message header and attachment conformed to testing details/parameters, the SUT accepted the ETT's request to initiate a secure session using SMTP protocols/commands, and testing conformed to the specified requirements within [RFC 2821](#).

This test and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.2.1 and 1.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 9 of the SMTP Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

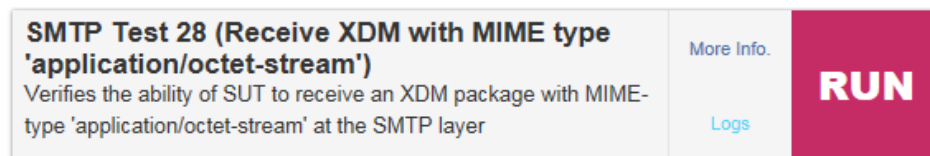
### 7.1.11.1 Testing Steps

To execute SMTP Test Cases 28 and assess the SUT's ability to accept a request from the ETT to initiate a secure session using SMTP protocols/commands, the vendor must perform the following steps:

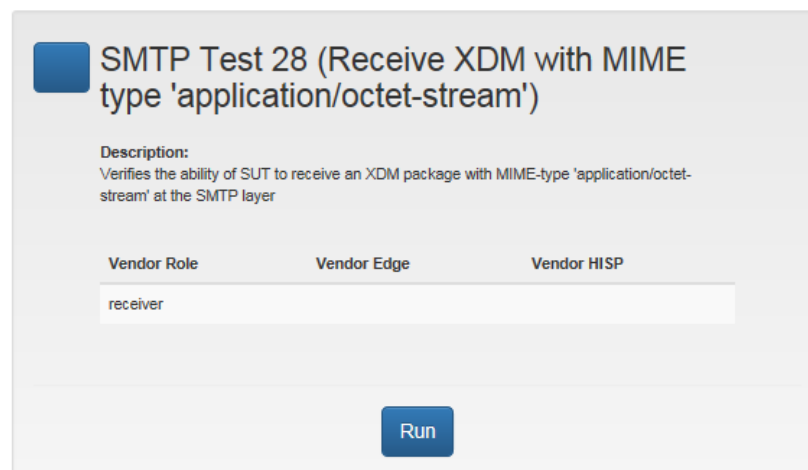
1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the navigation bar. This enables the testing Profile feature of the tool.
3. From the testing Profile, select **Receiver**.

Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.2.1 Profile Creation](#).

4. To initiate SMTP Test Cases 28, the vendor navigates to the Test Case's execution interface.



To gain additional information concerning SMTP Test 28's intended purpose (including Description, Vendor/SUT roles), click the **More Info** link for the Test Case.



5. With the Profile saved, More Info reviewed, and **SMTP Test 28** selected, the vendor performs the following Test Steps:
  - A. Click **Run** to execute the test.
  - B. Navigate the to SUT's messaging client/interface for **Vendor SMTP Email Address** (specified in the Profile).
    - a. Wait at least 60 seconds from executing the test to allow successful transmission to the SUT.
    - b. Check the **Vendor SMTP Email Address** to validate that a new message is present.
6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
  - A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
  - A test Fail prompts the vendor to **Retry** the test.
  - The **Clear** button resets the test and any data input field values.
  - For test with Fail results, refer to Section 2.0 (Testing Configuration for Edge System) and Section 2.2.1 (Profile Creation) of this ETT User Guide to ensure that the accurate configurations have been implemented.
7. To validate that the test results conformed to the testing objective(s) and gain additional information concerning the results or outcome of SMTP Test 28, click the **Log** link.

Testing outcomes can be reviewed by analyzing the applicable results for **Criteria Met, Request Timeout, Proctored, Time Elapsed, Request Response, and Attachments**.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Pass** or **Fail**). The **Log** is generated to view individual test result details (e.g., constraints, conformance details, contributing factors for **Pass** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view validation results by Profile configured and Test Case(s) executed.*

#### **7.1.12 SMTP Test Case 29 (Receiver – Receive XDM with MIME type 'application/xml')**

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the receiver, can accept a request from the HISP (i.e., ETT), acting as the sender, to establish a secure connection, execute the needed sequence of SMTP protocols and commands and receive an XDM package with MIME-type 'application/xml' at the XDM layer (in METADATA.XML)

The testing details for conformance testing flow are as follows:

1. The vendor navigates to the SMTP Test Case Profile and populates the vendor SMTP Hostname/IP, vendor SMTP Email Address, vendor SMTP Username, and vendor Password with accurate information (all fields should correlate so the ETT and SUT can communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
2. The vendor executes the test by clicking **Run** in the ETT for the target Test Case. Once the ETT processes the test, the vendor is presented with a **Waiting Validation** prompt.
3. The vendor performing this Test Case and in operation of the SUT will navigate to their SMTP email client and check for a new message from the ETT sending endpoint [wellformed1@tppedge.sitenv.org](mailto:wellformed1@tppedge.sitenv.org). If successful, the ETT will leverage the SMTP Profile data and send a message to the SMTP email client. This message will contain an XDM package with MIME-type 'application/xml' at the XDM layer (in METADATA.XML).
4. The vendor validates that the SUT successfully transmitted the message, the message header and attachment conformed to testing details/parameters, the SUT accepted the ETT's request to initiate a secure session using SMTP protocols/commands, and testing conformed to the specified requirements within [RFC 2821](#).

This test and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.2.1 and 1.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 9 of the SMTP Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

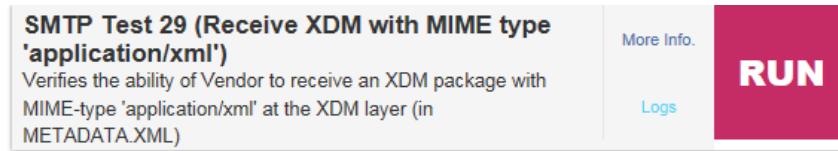
#### 7.1.12.1 Testing Steps

To execute SMTP Test Cases 29 and assess the SUT's ability to accept a request from the ETT to initiate a secure session using SMTP protocols/commands, the vendor must perform the following steps:

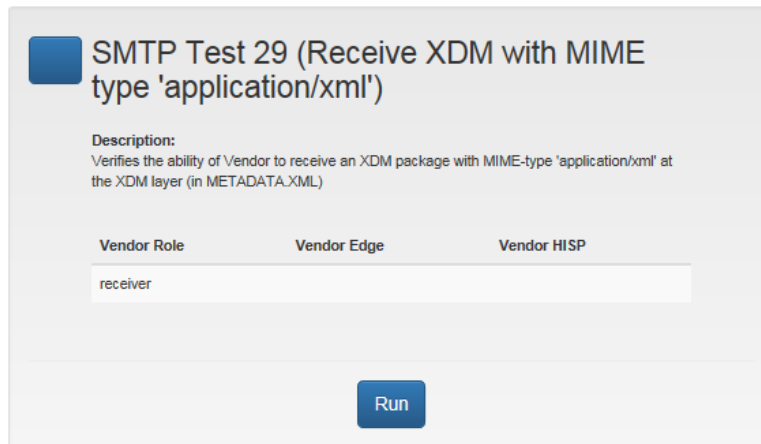
1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the navigation bar. This enables the testing Profile feature of the tool.
3. From the testing Profile, select **Receiver**.

Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.2.1 Profile Creation](#).

4. To initiate SMTP Test Cases 29, the vendor navigates to the Test Case's execution interface.



To gain additional information concerning SMTP Test 29's intended purpose (including Description, Vendor/SUT roles), click the **More Info** link for the Test Case.



5. With the Profile saved, More Info reviewed, and **SMTP Test 29** selected, the vendor performs the following Test Steps:
  - A. Click **Run** to execute the test.
  - B. Navigate the to SUT's messaging client/interface for **Vendor SMTP Email Address** (specified in the Profile).
    - a. Wait at least 60 seconds from executing the test to allow successful transmission to the SUT.
    - b. Check the **Vendor SMTP Email Address** to validate that a new message is present.
6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
  - A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
  - A test Fail prompts the vendor to **Retry** the test.
  - The **Clear** button resets the test and any data input field values.
  - For test with Fail results, refer to Section 2.0 (Testing Configuration for Edge System) and Section 2.2.1 (Profile Creation) of this ETT User Guide to ensure that the accurate configurations have been implemented.

7. To validate that the test results conformed to the testing objective(s) and gain additional information concerning the results or outcome of SMTP Test 29, click the **Log** link.

Testing outcomes can be reviewed by analyzing the applicable results for **Criteria Met**, **Request Timeout**, **Proctored**, **Time Elapsed**, **Request Response**, and **Attachments**.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Pass** or **Fail**). The **Log** is generated to view individual test result details (e.g., constraints, conformance details, contributing factors for **Pass** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view validation results by Profile configured and Test Case(s) executed.*

## 8.0 SMTP MESSAGE TRACKING

### 8.1 SMTP Message Tracking (MT) Test Cases

#### 8.1.1 SMTP MT Test Case 17 - Generate Unique Message-ID (Processed MDN suite)

The objective of this test sequence is to verify the ability of the receiving system to reject invalid STARTTLS commands. This test determines if an Edge System (i.e., SUT), acting as a sender, can successfully generate and transmit a series of email messages containing unique message IDs to a HISP (i.e., ETT), acting as the receiver.

The testing details for conformance testing flow are as follows:

1. As a precondition for this Test Case, the SUT must implement processed MDN tracking as defined within [Applicability Statement for Secure Health Transport v1.1](#) for the mechanism used to assure, verify, and trust message delivery.
2. The vendor performing this Test Case and in operation of the SUT will navigate to their SMTP email client and create three (3) new messages. These messages must be accurately formed and in the correct syntax. Each of the 3 messages must contain a unique message ID and no duplicates (the vendor must be able to manipulate the message ID to accurately execute this Test Case). The SUT will send the 3 messages (in a series) to the target ETT endpoint recipient: [wellformed14@ttpedge.sitenv.org](mailto:wellformed14@ttpedge.sitenv.org). Upon sending each message, the SUT will generate and send to the ETT a standard conformant processed MDN notification. The ETT will receive the 3 messages and processed MDN notifications and validate that each message ID is indeed unique.
3. The vendor validates that the SUT successfully transmitted the 3 messages, the ETT successfully received the 3 messages, the ETT detected that each of the 3 messages had unique IDs, the SUT successfully transmitted a process MDN notification for each of the 3 messages, and the specified requirements within [RFC 5322](#) were conformed to.

This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.5.1.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

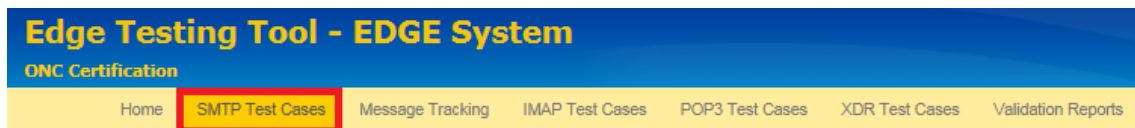
This test correlates to Test ID 17 of the MU Tracking tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 3.08 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.



### 8.1.1.1 Testing Steps

To execute SMTP Message Tracking (MT) 17 and assess the SUT's ability to successfully generate and transmit a series of email messages containing unique message IDs and send standard conformant processed MDNs, the vendor must perform the following steps:

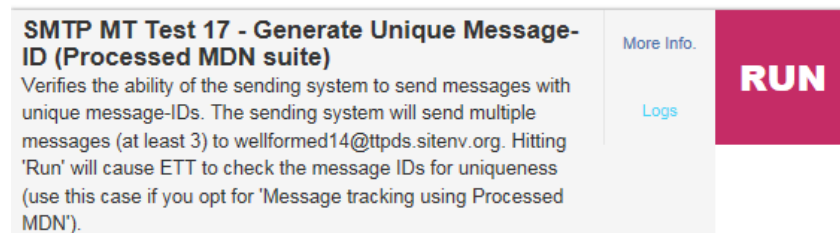
1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the navigation bar. This enables the testing Profile feature of the tool.



3. From the testing Profile, select **Sender**.

Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.2.1 Profile Creation](#).

4. To initiate SMTP Message Tracking (MT) 17, the vendor navigates to the Test Case's execution interface.



To gain additional information concerning SMTP Message Tracking (MT) 17's intended purpose (including description and Vendor/SUT roles), click the **More Info** link for the Test Case.

**SMTP MT Test 17 - Generate Unique Message-ID (Processed MDN suite)**

**Description:**  
The credentials for authentication is vendoraccount@ttpds.sitenv.org / vendortesting123

Vendor Role      Vendor Edge      Vendor HISP

sender

Run

5. With the Profile saved, More Info reviewed, and **SMTP Test 17** selected, the vendor performs the following Test Steps:
  - A. Navigate the to SUT's messaging client/interface for **vendor SMTP Email Address** (specified in the Profile).
  - B. Create three (3) new messages:
    - a. Each message must contain a unique message ID (no duplicates).
    - b. The 3 messages must be transmitted in a series.
    - c. The messages must be sent to the ETT endpoint recipient [wellformed14@ttpedge.sitenv.org](mailto:wellformed14@ttpedge.sitenv.org).
  - C. Navigate to the ETT and SMTP Test 17 execution interface:
    - a. Wait at least 60 seconds from sending the final message (in the series) to allow successful transmission to the ETT endpoint recipient.
    - b. Click **Run** to execute the test.
6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
  - A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
  - A test Fail prompts the vendor to **Retry** the test.
  - The **Clear** button resets the test and any data input field values.
  - For test with Fail results, refer to Section 2.0 (Testing Configuration for Edge System) and Section 2.2.1 (Profile Creation) of this ETT User Guide to ensure that the accurate configurations have been implemented.
7. To validate that the test results conformed to the testing objective(s) and gain additional information concerning the results or outcome of SMTP Test 17, click the vendor selects the **Log** link.

Testing outcomes can be reviewed by analyzing the applicable results for **Criteria Met**, **Request Timeout**, **Proctored**, **Time Elapsed**, **Request Response**, and **Attachments**.

**Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Pass** or **Fail**). The **Log** is generated to view individual test result details (e.g., constraints, conformance details, contributing factors for **Pass** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view validation results by Profile configured and Test Case(s) executed.

### 8.1.2 SMTP MT Test Cases 18 & 18(a) - Accept failure message for invalid recipient (Processed MDN suite - IMAP/POP Receiver & SMTP Receiver)

The objective of this test sequence is to verify the ability of the system to accept failure messages for some of the recipients. This test determines if an Edge System (i.e., SUT), acting as the receiver, can successfully receive failure messages from the HISP (i.e., ETT), acting as the sender.

The testing details for conformance testing flow are as follows:

1. As a precondition for this Test Case, the SUT must implement processed MDN tracking as defined within [Applicability Statement for Secure Health Transport v1.1](#) for the mechanism used to assure, verify, and trust message delivery.
2. The vendor performing this Test Case and in operation of the SUT will navigate to their SMTP email client and validate that the system received a single email to multiple recipients: valid one (goodaddress-plain@tppedge.sitenv.org) and an invalid address (noaddressfailure9-plain@dnsops.tppedge.sitenv.org ). The MDNs are delivered to the 'Mail From' address. The failure MDN for invalid recipient noaddressfailure9-plain@dnsops.tppedge.sitenv.org needs to be verified.
3. The vendor must also verify that the specified requirements within [RFC 5322](#) were conformed to.

This test and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.5.1.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 18 & 18(a) of the MU Tracking tab within the [Direct Edge Protocols](#) spreadsheet and within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

#### 8.1.2.1 Testing Steps

To execute SMTP Message Tracking (MT) 18 & 18(a) and assess the SUT's ability to successfully receive the email messages outlined above and receive standard conformant processed MDNs, the vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the navigation bar. This enables the testing Profile feature of the tool.
3. From the testing Profile, select **Sender**.

Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.2.1 Profile Creation](#).

4. To initiate SMTP Message Tracking (MT) 18 & 18(a), the vendor navigates to the Test Case's execution interface.

<p><b>SMTP MT Test 18 - Accept failure message for invalid recipient (Processed MDN suite - IMAP/POP Receiver)</b></p> <p>Verifies the ability of the system to accept failure messages for some of the recipients. The system shall send a single email to multiple recipients: valid one (goodaddress-plain@tppedge.sitenv.org) and an invalid address (noaddressfailure9-plain@dnsops.tppedge.sitenv.org ). The MDNs are delivered to the 'Mail From' address. The failure MDN for invalid recipient noaddressfailure9-plain@dnsops.tppedge.sitenv.org needs to be verified.</p>	<a href="#">More Info.</a>	<b>RUN</b>
<p><b>SMTP MT Test 18(a) - Accept failure message for invalid recipient (Processed MDN suite - SMTP Receiver)</b></p> <p>Verifies the ability of the system to accept failure messages for some of the recipients. The system shall send a single email to multiple recipients: valid one (goodaddress-plain@tppedge.sitenv.org) and an invalid address (noaddressfailure9-plain@dnsops.tppedge.sitenv.org ). Hitting 'Run' will cause the MDNs to be delivered using the account information specified in the profile using SMTP protocol with STARTTLS and SASL. The failure MDN for invalid recipient noaddressfailure9-plain@dnsops.tppedge.sitenv.org needs to be verified.</p>	<a href="#">More Info.</a>	<b>RUN</b>

To gain additional information concerning SMTP Message Tracking (MT) 18 & 18(a)'s intended purpose (including description and Vendor/SUT roles), click the **More Info** link for the Test Case.

### SMTP MT Test 18 - Accept failure message for invalid recipient (Processed MDN suite - IMAP/POP Receiver)

**Description:**  
The credentials for authentication is vendoraccount@ttpds.sitenv.org / vendortesting123

Vendor Role	Vendor Edge	Vendor HISP
sender		

Run

### SMTP MT Test 18(a) - Accept failure message for invalid recipient (Processed MDN suite - SMTP Receiver)

**Description:**  
The credentials for authentication is vendor1smtpsmtp@ttpds.sitenv.org / vendortesting123.  
This is a test case for systems that receive using SMTP.

Vendor Role	Vendor Edge	Vendor HISP
sender		

Run

5. With the Profile saved, More Info reviewed, and **SMTP Test 18 or 18(a)** selected, the vendor performs the following Test Steps:
  - A. Navigate the to SUT's messaging client/interface for **vendor SMTP Email Address** (specified in the Profile).
  - B. For Test 18, the MDNs are delivered to the 'Mail From' address. The failure MDN for invalid recipient noaddressfailure9-plain@dnsops.ttpedge.sitenv.org needs to be verified.
  - C. For Test 18(a), hitting 'Run' will cause the MDNs to be delivered using the account information specified in the profile using SMTP protocol with STARTTLS and SASL. The failure MDN for invalid recipient noaddressfailure9-plain@dnsops.ttpedge.sitenv.org needs to be verified.
  - D. Navigate to the ETT and SMTP Test 18 & 18(a) execution interface:

- a. Click **Run** to execute the test.
6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
    - A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
    - A test Fail prompts the vendor to **Retry** the test.
    - The **Clear** button resets the test and any data input field values.
    - For test with Fail results, refer to Section 2.0 (Testing Configuration for Edge System) and Section 2.2.1 (Profile Creation) of this ETT User Guide to ensure that the accurate configurations have been implemented.
  7. To validate that the test results conformed to the testing objective(s) and gain additional information concerning the results or outcome of SMTP Test 18 & 18(a), click the vendor selects the **Log** link.

Testing outcomes can be reviewed by analyzing the applicable results for **Criteria Met, Request Timeout, Proctored, Time Elapsed, Request Response, and Attachments**.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Pass** or **Fail**). The **Log** is generated to view individual test result details (e.g., constraints, conformance details, contributing factors for **Pass** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view validation results by Profile configured and Test Case(s) executed.*

### 8.1.3 SMTP MT Test Case 45 - Generate Unique Message-ID (IG for Delivery Notification Suite)

The objective of this test sequence is to verify the ability of the sending system to send messages with unique message-IDs. This test determines if an Edge System (i.e., SUT), acting as a sender, can successfully generate and transmit a series of email messages containing unique message IDs to a HISP (i.e., ETT), acting as the receiver.

The testing details for conformance testing flow are as follows:

1. As a precondition for this Test Case, the SUT must implement processed MDN tracking as defined within [Applicability Statement for Secure Health Transport v1.1](#) for the mechanism used to assure, verify, and trust message delivery.
2. The vendor performing this Test Case and in operation of the SUT will navigate to their SMTP email client and create three (3) new messages. These messages must be accurately formed and in the correct syntax. Each of the 3 messages must contain a unique message ID and no duplicates (the vendor must be able to manipulate the message ID to accurately execute this Test Case). The SUT will send the 3 messages (in a series) to the target ETT endpoint recipient: [wellformed14@tppedge.sitenv.org](mailto:wellformed14@tppedge.sitenv.org). Upon sending each message, the SUT will generate and send to the ETT a standard conformant

processed MDN notification. The ETT will receive the 3 messages and processed MDN notifications and validate that each message ID is indeed unique.

3. The vendor validates that the SUT successfully transmitted the 3 messages, the ETT successfully received the 3 messages, the ETT detected that each of the 3 messages had unique IDs, the SUT successfully transmitted a process MDN notification for each of the 3 messages, and the specified requirements within [RFC 5322](#) were conformed to.

This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.5.1.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 45 of the MU Tracking tab within the [Direct Edge Protocols](#) spreadsheet and the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

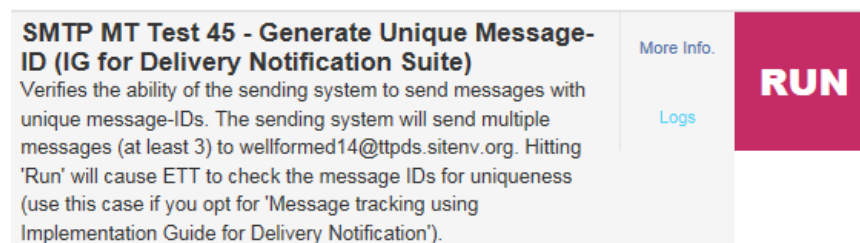
### 8.1.3.1 Testing Steps

To execute SMTP Message Tracking (MT) 45 and assess the SUT's ability to successfully generate and transmit a series of email messages containing unique message IDs and send standard conformant processed MDNs, the vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the navigation bar. This enables the testing Profile feature of the tool.
3. From the testing Profile, select **Sender**.

Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.2.1 Profile Creation](#).

4. To initiate SMTP Message Tracking (MT) 45, the vendor navigates to the Test Case's execution interface.



To gain additional information concerning SMTP Message Tracking (MT) 45's intended purpose (including description and Vendor/SUT roles), click the **More Info** link for the Test Case.



**SMTP MT Test 45 - Generate Unique Message-ID (IG for Delivery Notification Suite)**

**Description:**  
The credentials for authentication is vendoraccount@ttpds.sitenv.org / vendortesting123

Vendor Role      Vendor Edge      Vendor HISP

sender

Run

5. With the Profile saved, More Info reviewed, and **SMTP Test 45** selected, the vendor performs the following Test Steps:
  - E. Navigate the to SUT's messaging client/interface for **vendor SMTP Email Address** (specified in the Profile).
  - F. Create three (3) new messages:
    - a. Each message must contain a unique message ID (no duplicates).
    - b. The 3 messages must be transmitted in a series.
    - c. The messages must be sent to the ETT endpoint recipient [wellformed14@ttpedge.sitenv.org](mailto:wellformed14@ttpedge.sitenv.org).
  - G. Navigate to the ETT and SMTP Test 45 execution interface:
    - a. Wait at least 60 seconds from sending the final message (in the series) to allow successful transmission to the ETT endpoint recipient.
    - b. Click **Run** to execute the test.
6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
  - A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
  - A test Fail prompts the vendor to **Retry** the test.
  - The **Clear** button resets the test and any data input field values.
  - For test with Fail results, refer to Section 2.0 (Testing Configuration for Edge System) and Section 2.2.1 (Profile Creation) of this ETT User Guide to ensure that the accurate configurations have been implemented.
7. To validate that the test results conformed to the testing objective(s) and gain additional information concerning the results or outcome of SMTP Test 17, click the vendor selects the **Log** link.

Testing outcomes can be reviewed by analyzing the applicable results for **Criteria Met, Request Timeout, Proctored, Time Elapsed, Request Response, and Attachments**.



***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Pass** or **Fail**). The **Log** is generated to view individual test result details (e.g., constraints, conformance details, contributing factors for **Pass** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view validation results by Profile configured and Test Case(s) executed.*

#### **8.1.4 SMTP MT Test Case 46 (Generate Disposition Notification Options Header)**

The objective of this test sequence is to verify the ability of the sending system to send messages with a correct Disposition Notification Options Header. This test determines if an Edge System (i.e., SUT), acting as a sender, can successfully send an email messages to a HISP (i.e., ETT), acting as the receiver.

The testing details for conformance testing flow are as follows:

1. As a precondition for this Test Case, the SUT must implement processed MDN tracking as defined within [Applicability Statement for Secure Health Transport v1.1](#) for the mechanism used to assure, verify, and trust message delivery.
2. The vendor performing this Test Case and in operation of the SUT will navigate to their SMTP email client and create a new message. This message must be accurately formed and in the correct syntax. The messages must contain the correct disposition notification options header. The SUT will send the messages to the target ETT endpoint recipient: [wellformed14@tppedge.sitenv.org](mailto:wellformed14@tppedge.sitenv.org). Upon sending the message, the SUT will generate and send to the ETT a standard conformant processed MDN notification. The ETT will receive the message and validate that the header is correct.
3. The vendor validates that the SUT successfully transmitted the message, the ETT successfully received the message, the ETT detected that the message contained the correct header, and the specified requirements within [RFC 5322](#) were conformed to.

This test and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.5.1.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 17 of the MU Tracking tab within the [Direct Edge Protocols](#) spreadsheet and the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

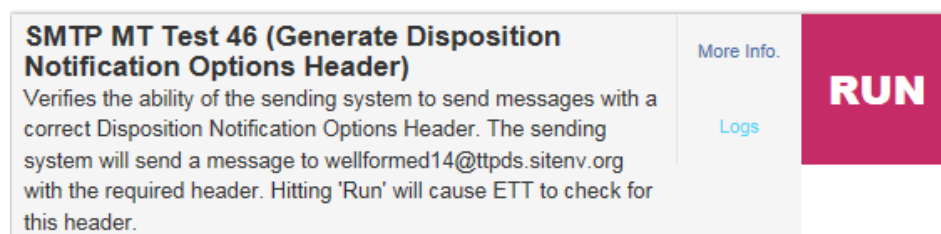
##### **8.1.4.1 Testing Steps**

To execute SMTP Message Tracking (MT) 46 and assess the SUT's ability to successfully generate and transmit a message with a correct Disposition Notification Options Header, the vendor must perform the following steps:

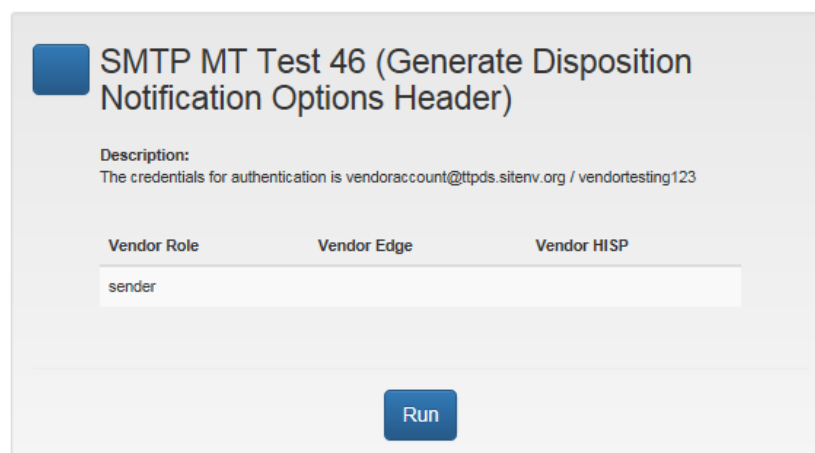
1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the navigation bar. This enables the testing Profile feature of the tool.
3. From the testing Profile, select **Sender**.

Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.2.1 Profile Creation](#).

4. To initiate SMTP Message Tracking (MT) 46, the vendor navigates to the Test Case's execution interface.



To gain additional information concerning SMTP Message Tracking (MT) 46's intended purpose (including description and Vendor/SUT roles), click the **More Info** link for the Test Case.



5. With the Profile saved, More Info reviewed, and **SMTP Test 46** selected, the vendor performs the following Test Steps:

- A. Navigate the to SUT's messaging client/interface for **vendor SMTP Email Address** (specified in the Profile).
  - B. Create a new message to be sent to the ETT endpoint recipient [wellformed14@tppedge.sitenv.org](mailto:wellformed14@tppedge.sitenv.org).
  - C. Navigate to the ETT and SMTP Test 46 execution interface:
    - a. Wait at least 60 seconds from sending the final message (in the series) to allow successful transmission to the ETT endpoint recipient.
    - b. Click **Run** to execute the test.
6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
- A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
  - A test Fail prompts the vendor to **Retry** the test.
  - The **Clear** button resets the test and any data input field values.
  - For test with Fail results, refer to Section 2.0 (Testing Configuration for Edge System) and Section 2.2.1 (Profile Creation) of this ETT User Guide to ensure that the accurate configurations have been implemented.
7. To validate that the test results conformed to the testing objective(s) and gain additional information concerning the results or outcome of SMTP Test 46, click the vendor selects the **Log** link.

Testing outcomes can be reviewed by analyzing the applicable results for **Criteria Met, Request Timeout, Proctored, Time Elapsed, Request Response, and Attachments**.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Pass** or **Fail**). The **Log** is generated to view individual test result details (e.g., constraints, conformance details, contributing factors for **Pass** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view validation results by Profile configured and Test Case(s) executed.*

### **8.1.5 SMTP MT Test Cases 47 & 47(a) - Accept failure message for invalid recipient (IG for Delivery Notification Suite - IMAP/POP Receiver & SMTP Receiver)**

The objective of this test sequence is to verify the ability of the receiving system to accept failure messages for some of the recipients. This test determines if an Edge System (i.e., SUT), acting as a sender, can successfully generate and transmit an email messages containing to a HISP (i.e., ETT), acting as the receiver.

The testing details for conformance testing flow are as follows:

1. As a precondition for this Test Case, the SUT must implement processed MDN tracking as defined within [Applicability Statement for Secure Health Transport v1.1](#) for the mechanism used to assure, verify, and trust message delivery.
2. For Test 47, the system shall send a single email to multiple recipients: valid one (dispatchedonly-plain@ttpedge.sitenv.org) and an invalid address (noaddressfailure9-plain@dnsops.ttpedge.sitenv.org ). The MDNs are delivered to the 'Mail From' address. The failure MDN for invalid recipient noaddressfailure9-plain@dnsops.ttpedge.sitenv.org needs to be verified.
3. For Test 47(a), The system shall send a single email to multiple recipients: valid one (dispatchedonly-plain@ttpedge.sitenv.org) and an invalid address (noaddressfailure9-plain@dnsops.ttpedge.sitenv.org ). Hitting 'Run' will cause the MDNs to be delivered using the account information specified in the profile using SMTP protocol with STARTTLS and SASL. The failure MDN for invalid recipient noaddressfailure9-plain@dnsops.ttpedge.sitenv.org needs to be verified.
4. The vendor validates that the SUT successfully transmitted the message, the ETT successfully received the message, and the specified requirements within [RFC 5322](#) were conformed to.

This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.5.1.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 17 of the MU Tracking tab within the [Direct Edge Protocols](#) spreadsheet and within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

### 8.1.5.1 Testing Steps

To execute SMTP Message Tracking (MT) 47 & 47(a) and assess the SUT's ability to successfully accept failure message for some of the recipients, the vendor must perform the following steps:


1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the navigation bar. This enables the testing Profile feature of the tool.
3. From the testing Profile, select **Sender**.

Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.2.1 Profile Creation](#).

4. To initiate SMTP Message Tracking (MT) 47 & 47(a), the vendor navigates to the Test Case's execution interface.


<b>SMTP MT Test 47 - Accept failure message for invalid recipient (IG for Delivery Notification Suite - IMAP/POP Receiver)</b> Verifies the ability of the system to accept failure messages for some of the recipients. The system shall send a single email to multiple recipients: valid one (dispatchedonly-plain@ttpedge.sitenv.org) and an invalid address (noaddressfailure9-plain@dnsops.ttpedge.sitenv.org ). The MDNs are delivered to the 'Mail From' address. The failure MDN for invalid recipient noaddressfailure9-plain@dnsops.ttpedge.sitenv.org needs to be verified.	<a href="#">More Info.</a> <a href="#">Logs</a>	<b>RUN</b>
<b>SMTP MT Test 47(a) - Accept failure message for invalid recipient (IG for Delivery Notification Suite - SMTP Receiver)</b> Verifies the ability of the system to accept failure messages for some of the recipients. The system shall send a single email to multiple recipients: valid one (dispatchedonly-plain@ttpedge.sitenv.org) and an invalid address (noaddressfailure9-plain@dnsops.ttpedge.sitenv.org ). Hitting 'Run' will cause the MDNs to be delivered using the account information specified in the profile using SMTP protocol with STARTTLS and SASL. The failure MDN for invalid recipient noaddressfailure9-plain@dnsops.ttpedge.sitenv.org needs to be verified.	<a href="#">More Info.</a> <a href="#">Logs</a>	<b>RUN</b>

To gain additional information concerning SMTP Message Tracking (MT) 47 & 47(a)'s intended purpose (including description and Vendor/SUT roles), click the **More Info** link for the Test Case.


**SMTP MT Test 47 - Accept failure message for invalid recipient (IG for Delivery Notification Suite - IMAP/POP Receiver)**

**Description:**  
 The credentials for authentication is vendoraccount@tpds.sitenv.org / vendortesting123. This is a test case for systems that receive using SMTP.

Vendor Role	Vendor Edge	Vendor HISP
sender		



SMTP MT Test 47(a) - Accept failure message for invalid recipient (IG for Delivery Notification Suite - SMTP Receiver)

Description:

The credentials for authentication is vendor1smtpsmtp@ttpds.sitenv.org / vendortesting123

Vendor Role	Vendor Edge	Vendor HISP
sender		

Run

5. With the Profile saved, More Info reviewed, and **SMTP Test 47 or 47(a)** selected, the vendor performs the following Test Steps:
  - A. Navigate the to SUT's messaging client/interface for **vendor SMTP Email Address** (specified in the Profile).
  - B. For Test 47, Create the new message to multiple recipients: valid one (dispatchedonly-plain@ttpedge.sitenv.org) and an invalid address (noaddressfailure9-plain@dnsops.ttpedge.sitenv.org ). The MDNs are delivered to the 'Mail From' address. The failure MDN for invalid recipient noaddressfailure9-plain@dnsops.ttpedge.sitenv.org needs to be verified.
  - C. For Test 47(a), Create the new message to multiple recipients: valid one (dispatchedonly-plain@ttpedge.sitenv.org) and an invalid address (noaddressfailure9-plain@dnsops.ttpedge.sitenv.org ). Hitting 'Run' will cause the MDNs to be delivered using the account information specified in the profile using SMTP protocol with STARTTLS and SASL. The failure MDN for invalid recipient noaddressfailure9-plain@dnsops.ttpedge.sitenv.org needs to be verified.
  - D. Navigate to the ETT and SMTP Test 47 & 47(a) execution interface:
    - a. Wait at least 60 seconds from sending the final message to allow successful transmission to the ETT endpoint recipient.
    - b. Click **Run** to execute the test.
6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
  - A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
  - A test Fail prompts the vendor to **Retry** the test.
  - The **Clear** button resets the test and any data input field values.

- For test with Fail results, refer to Section 2.0 (Testing Configuration for Edge System) and Section 2.2.1 (Profile Creation) of this ETT User Guide to ensure that the accurate configurations have been implemented.
7. To validate that the test results conformed to the testing objective(s) and gain additional information concerning the results or outcome of SMTP Test 47 & 47(a), click the vendor selects the **Log** link.

Testing outcomes can be reviewed by analyzing the applicable results for **Criteria Met, Request Timeout, Proctored, Time Elapsed, Request Response**, and **Attachments**.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Pass** or **Fail**). The **Log** is generated to view individual test result details (e.g., constraints, conformance details, contributing factors for **Pass** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view validation results by Profile configured and Test Case(s) executed.*

## 9.0 IMAP TESTING



## 10.0 POP3 TESTING

## 11.0 XDR TESTING

### 11.1 XDR Test Cases

#### 11.1.1 XDR Test Case 1 (Sender)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the sender, can create and transmit an XDR message to a HISP (i.e., ETT), acting as the receiver, per give conformance specifications.

The testing details for conformance testing flow are as follows:

1. The vendor assures that the appropriate XDR Certificates have been downloaded from the ETT (direct download link [here](#)) and imported into the SUT's trust store before executing the test.
2. With the trust relationship established, the vendor navigates to the target Test Case and populates the **Direct From Address** field with the SUT's accurate information (all fields should correlate so the ETT and SUT and communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
3. The vendor performing this Test Case and in operation of the SUT executes first Test Step by clicking **Run** for the target Test Case. The ETT generates two endpoints (TLS and Non-TLS).
4. The vendor executes the second Test Step by sending the ETT generated TLS / Non-TLS endpoint an XDR message from the SUT. The correct syntax of the message must meet accuracy requirements for XDR Message Checklist, XDS Metadata Checklist for **Limited Metadata** Document Source, and Direct Address Block.
5. The vendor validates through **Log** review that the SUT successfully transmitted a message to the ETT generated endpoint, the message met testing constraints, and testing adhered to the specified requirements within [XDR and XDM for Direct Messaging v1.0](#) and [IHE XDR Profile for Limited Metadata Document Sources](#).

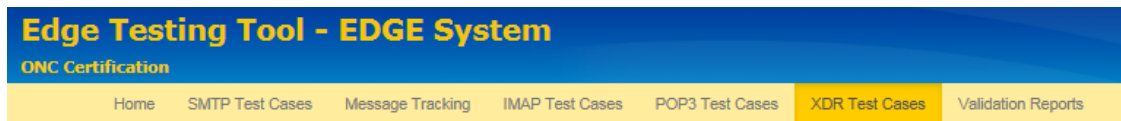
This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 1 of the XDR Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 2.03 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

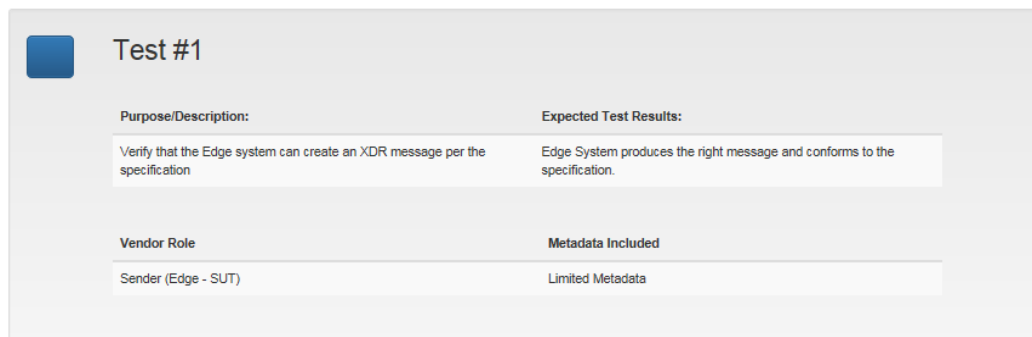
##### 11.1.1.1 Testing Steps

To execute XDR Test Case 1 and assess the SUT's ability to create and transmit an XDR message per give conformance specifications for XDR Message Checklist, XDS Metadata Checklist for **Limited Metadata** Document Source, and Direct Address Block, the Vendor must perform the following steps:

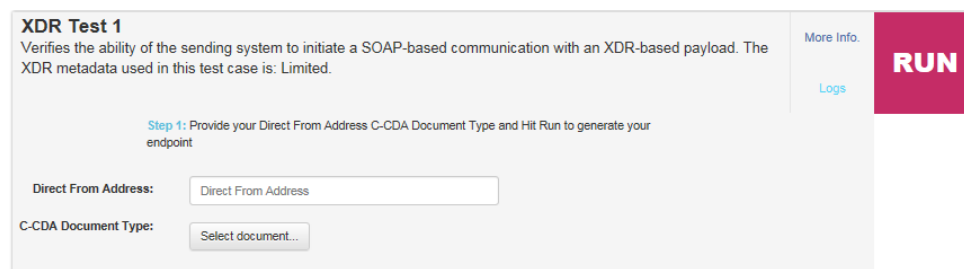
1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the navigation bar.



3. From the testing options available, select **Your System as: Sender**. This will enable test case selection. Please note that the XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.
4. To gain additional information concerning XDR Test 1's intended focus, purpose/description, expected test results, vendor role, and metadata inclusion, click the **More Info** link for the Test Case.



5. To initiate XDR Test 1, the Vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly.



6. Once the SUT's Direct From Address has been populated in the Test Case, clicking **Run** initiates the first testing step.

7. The vendor is prompted to navigate to the SUT's messaging client and create a new XDR message. The new message must be accurately formed in the correct syntax. The vendor will send the XDR message to one of the two ETT generated endpoints (TLS or non-TLS) for the Test Case.
8. Once the XDR message has been transmitted from the SUT to the ETT endpoint, the vendor clicks the **Pending Refresh** button for the Test Case.
9. The ETT checks the generated endpoints for the presence of newly received XDR messages. The vendor is prompted to manually validate if the test results conformed to the testing objectives. To complete this, the vendor clicks the **Waiting Validation** button
10. The vendor is presented with the Test Case **Log** screen. The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test 1, the vendor will select the **Response** tab to review the ETT logged response received from the SUT after transmission of the XDR message.
11. Within the Log, the vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
  - a. Accurately attempted to established a connection with the ETT;
  - b. Formed/transmitted the XDR message correctly; and
  - c. Successfully initiated SOAP-based communication with the ETT;
  - d. Successfully included an XDR-based payload with Limited metadata along with the message transmission.
12. If the vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected. Accept XDR selections correlate with Test Case Success results. Likewise, Reject XDR selections correlate with Test Case Failures. Only if the testing objective for a Test Case is in the negative, where the vendor has verified message rejection, will a Reject XDR selection correlate with a Test Success.
13. The ETT presents vendor conformation (XDR validation passed or failed) based upon the selection made.
14. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case. XDR message rejection results in a red X and prompts the Vendor to **Retry** the test. The vendor can select the **Clear** button to reset the test. XDR message acceptance results in a green check. The vendor can select the **Clear** button to reset the test.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Success** or **Fail**). The **Log** is generated to view individual test result details (e.g., contributing factors for **Success** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view result outcomes. This enables the vendor to validate the acceptance of the message received by the SUT.*

15. All completed test session data is then available through the ETT's **Validation Report** tab on the navigation bar.

### 11.1.2 XDR Test Case 2 (Sender)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the sender, can create and transmit an XDR message to a HISP (i.e., ETT), acting as the receiver, per given conformance specifications.

The testing details for conformance testing flow are as follows:

1. The vendor assures that the appropriate XDR Certificates have been downloaded from the ETT (direct download link [here](#)) and imported into the SUT's trust store before executing the test.
2. With the trust relationship established, the Vendor navigates to the target Test Case and populates the **Direct From Address** field with the SUT's accurate information (all fields should correlate so the ETT and SUT can communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
3. The vendor performing this Test Case and in operation of the SUT executes first Test Step by clicking **Run** for the target Test Case. The ETT generates two endpoints (TLS and Non-TLS).
4. The vendor executes the second Test Step by sending the ETT generated TLS / Non-TLS endpoint an XDR message from the SUT. The correct syntax of the message must meet accuracy requirements for XDR Message Checklist, XDS Metadata Checklist for **Full Metadata** Document Source, and Direct XDS Checklist.
5. The vendor validates through **Log** review that the SUT successfully transmitted a message to the ETT generated endpoint, the message met testing constraints, and testing adhered to the specified requirements within [XDR and XDM for Direct Messaging v1.0](#) and [IHE XDR Profile for Limited Metadata Document Sources](#).

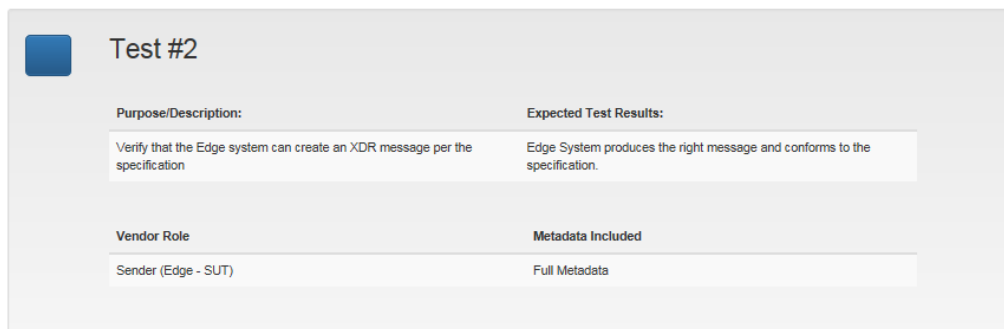
This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 2 of the XDR Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 2.04 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

### 11.1.2.1 Testing Steps

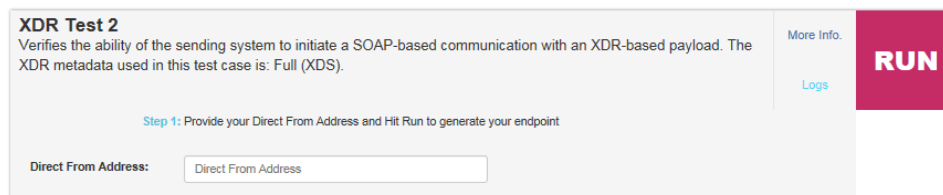
To execute XDR Test Case 2 and assess the SUT's ability to create and transmit an XDR message per give conformance specifications for XDR Message Checklist, XDS Metadata Checklist for **Full Metadata** Document Source, and Direct XDS Checklist, the Vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the navigation bar.
3. From the testing options available, select **Your System as: Sender**. This will enable Test Case selection. Please note that the XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.
4. To gain additional information concerning XDR Test 2's intended focus, purpose/description, expected test results, vendor role, and metadata inclusion, click the **More Info** link for the Test Case.



Test #2	
<b>Purpose/Description:</b>	<b>Expected Test Results:</b>
Verify that the Edge system can create an XDR message per the specification	Edge System produces the right message and conforms to the specification.
<b>Vendor Role</b>	<b>Metadata Included</b>
Sender (Edge - SUT)	Full Metadata

5. To initiate XDR Test 2, the vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly.



**XDR Test 2**  
 Verifies the ability of the sending system to initiate a SOAP-based communication with an XDR-based payload. The XDR metadata used in this test case is: Full (XDS).

[More Info.](#)  
[Logs](#)

**RUN**

Step 1: Provide your Direct From Address and Hit Run to generate your endpoint

Direct From Address:

6. Once the SUT's Direct From Address has been populated in the Test Case, clicking **Run** initiates the first testing step.

7. The vendor is prompted to navigate to the SUT's messaging client and create a new XDR message. The new message must be accurately formed in the correct syntax. The vendor will send the XDR message to one of the two ETT generated endpoints (TLS or non-TLS) for the Test Case.
8. Once the XDR message has been transmitted from the SUT to the ETT endpoint, the vendor clicks the **Pending Refresh** button for the Test Case.
9. The ETT checks the generated endpoints for the presence of a newly received XDR message. The vendor is prompted to manually validate if the test results conformed to the testing objectives. To complete this, the vendor clicks the **Waiting Validation** button
10. The vendor is presented with the Test Case **Log** screen. The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test 2, the vendor will select the **Response** tab to review the ETT logged response received from the SUT after transmission of the XDR message.
11. Within the Log, the vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
  - a. Accurately attempted to established a connection with the ETT;
  - b. Formed/transmitted the XDR message correctly; and
  - c. Successfully initiated SOAP-based communication with the ETT;
  - d. Successfully included an XDR-based payload with Full XDS metadata along with the message transmission.
12. If the vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected. Accept XDR selections correlate with Test Case Success results. Likewise, Reject XDR selections correlate with Test Case Failures. Only if the testing objective for a Test Case is in the negative, where the vendor has verified message rejection, will a Reject XDR selection correlate with a Test Success.
13. The ETT presents vendor conformation (XDR validation passed or failed) based upon the selection made.
14. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case. XDR message rejection results in a red X and prompts the vendor to **Retry** the test. The vendor can select the **Clear** button to reset the test. XDR message acceptance results in a green check. The Vvendor can select the **Clear** button to reset the test.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Success** or **Fail**). The **Log** is generated to view individual test result details (e.g., contributing factors for **Success** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view result outcomes. This enables the vendor to validate the acceptance of the message received by the SUT.*

15. All completed test session data is then available through the ETT's **Validation Report** tab on the navigation bar.

### 11.1.3 XDR Test Case 6 (Sender)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the sender, can establish a mutual TLS connection with a HISP (i.e., ETT), acting as the receiver, and successfully authenticate before transmitting data.

The testing details for conformance testing flow are as follows:

1. The vendor ensures that the appropriate XDR Certificates have been downloaded from the ETT (direct download link [here](#)) and imported into the SUT's trust store before executing the test.
2. With the trust relationship established, the vendor navigates to the target Test Case and populates the **Direct From Address** field with the SUT's accurate information (all fields should correlate so the ETT and SUT and communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
3. The vendor performing this Test Case and in operation of the SUT executes the first Test Step by clicking **Run** for the target Test Case. The ETT generates two endpoints (TLS and Non-TLS).
4. The vendor executes the second Test Step by sending the ETT generated TLS / Non-TLS endpoint a message from the SUT.
5. The vendor validates through **Log** review that the SUT successfully established a Mutual TLS connection with the ETT generated endpoint, the SUT authenticated with the ETT generated endpoint before transmitting data, the message met testing constraints, and testing adhered to the specified requirements within [XDR and XDM for Direct Messaging v1.0](#) and [IHE XDR Profile for Limited Metadata Document Sources](#).

This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.



This test correlates to Test ID 7 of the XDR Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 2.01 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

### 11.1.3.1 Testing Steps

To execute XDR Test Case 6 and assess the SUT's ability to successfully authenticate during a Mutual TLS connection attempt before transmitting data, the vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the navigation bar.
3. From the testing options available, select **Your System as: Sender**. This will enable Test Case selection. XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.
4. To gain additional information concerning XDR Test 6's intended focus, purpose/descriptions, expected test results, vendor role, and metadata inclusion, click the **More Info** link for the Test Case.

Test #6	
<b>Purpose/Description:</b> Verify that Mutual TLS session is established between the Sender and the Receiver before transmitting data. The Tester (i.e., Vendor) assures that the appropriate XDR Certificates have been downloaded from the ETT and imported into the SUT trust store before executing the test.	<b>Expected Test Results:</b> Edge System is capable of establishing the Mutual TLS connection prior to transmitting the data.
<b>Vendor Role</b> Sender (Edge - SUT)	<b>Metadata Included</b> N/A

5. To initiate XDR Test 6, the vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly.

**XDR Test 6**  
 Verifies the ability of the sending system to complete a mutual TLS handshake before data is sent across. Note that an unsuccessful TLS attempt may result in the Pending Refresh button being displayed instead of a Fail. A disconnection happening at the server level would cause the communication not to be forwarded to the application level.

[More Info.](#)  
[Logs](#)

**RUN**

**Step 1:** Provide your Direct From Address and Hit Run to generate your endpoint

**Direct From Address:**

6. Once the SUT's Direct From Address has been populated in the Test Case, clicking **Run** initiates the first testing step.
7. The vendor is prompted to navigate to the SUT's messaging client and create a new XDR message. The new message must be accurately formed in the correct syntax. The vendor will send the XDR message to one of the two ETT generated endpoints (TLS or non-TLS) for the Test Case.
8. Once the XDR message has been transmitted from the SUT to the ETT endpoint, the vendor clicks the **Pending Refresh** button for the Test Case.
9. The ETT checks the generated endpoints for the presence of newly received XDR messages. The vendor is prompted to manually validate if the test results conformed to the testing objectives. To complete this, the vendor clicks the **Waiting Validation** button
10. The vendor is presented with the Test Case **Log** screen. The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test 6, the vendor will select the **Response** tab to review the ETT logged response received from the SUT after transmission of the XDR message.
11. Within the **Log**, the vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
  - a. Accurately established a connection with the ETT;
  - b. Formed/transmitted the XDR message correctly; and
  - c. Completed a mutual TLS handshake with the ETT before transmitting data.
12. If the vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected. Accept XDR selections correlate with Test Case Success results. Likewise, Reject XDR selections correlate with Test Case Failures. Only if the testing objective for a Test Case is in the negative, where the vendor has verified message rejection, will a Reject XDR selection correlate with a Test Success.
13. The ETT presents vendor conformation (XDR validation passed or failed) based upon the selection made.
14. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case. XDR message rejection results in a red X and prompts the vendor to **Retry** the test. The vendor can select the **Clear** button to reset the test. XDR message acceptance results in a green check. The vendor can select the **Clear** button to reset the test.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case’s generated test results (either a **Success** or **Fail**). The **Log** is generated to view individual test result details (e.g., factors for **Success** or **Fail**) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to validate the acceptance of the message received by the SUT*

15. All completed test session data is then available through the ETT’s **Validation Report** tab on the navigation bar.

#### **11.1.4 XDR Test Case 7 (Sender)**

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the sender, can detect an invalid certificate provided by a HISP (i.e., ETT), acting as the receiver, during a Mutual TLS connection attempt and successfully disconnect.

The testing details for conformance testing flow are as follows:

1. The vendor assures that the appropriate XDR Certificates have been downloaded from the ETT (direct download link [here](#)) and imported into the SUT’s trust store before executing the test.
2. With the trust relationship established, the vendor navigates to the target Test Case and populates the **IP Address** field with the SUT’s accurate information (all fields should correlate so the ETT and SUT and communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
3. The vendor performing this Test Case and in operation of the SUT executes first Test Step by clicking **Run** for the target Test Case. The ETT generates an endpoint (IP address and port).
4. The vendor executes the second Test Step by sending the ETT generated endpoint a message from the SUT.
5. The vendor validates through **Log** review that the SUT attempted to established a Mutual TLS connection with the ETT generated endpoint, the SUT identified during authentication invalid certificates provided by the ETT, the SUT successfully disconnected from the ETT without authenticating and/or transmitting any data, and testing adhered to the specified requirements within [XDR and XDM for Direct Messaging v1.0](#) and [IHE XDR Profile for Limited Metadata Document Sources](#).

This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 7 of the XDR Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 2.02 within the [ONC 2014 Edition approved Test Procedure](#)

[requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

### 11.1.4.1 Testing Steps

To execute XDR Test Case 7 and assess the SUT's ability to successfully identify invalid certificates provided during a Mutual TLS connection attempt and terminate a session, the vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the navigation bar.
3. From the testing options available, select **Your System as: Sender**. This will enable test case selection. XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.
4. To gain additional information concerning XDR Test 7's intended focus, purpose/descriptions, expected test results, vendor role, and metadata inclusion, click the **More Info** link for the Test Case.

Test #7	
Purpose/Description:	Expected Test Results:
Verify that Edge disconnects when the Server provided certificate is invalid.	Edge System rejects the connection from the Server due to bad certificate.
Vendor Role	Metadata Included
Sender (Edge - SUT)	N/A

5. To initiate XDR Test 7, the vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly.

**XDR Test 7**  
Verifies the ability of the sending system to reject a mutual TLS connection where the certificate provided by the ETT is invalid. If you experience Pending Refresh or a Fail that you think is incorrect, please run this test again but wait 15 seconds after the connection has been dropped for the ETT to fully test the socket connection.

[More Info.](#)  
[Logs](#)

**RUN**

Step 1: Provide your IP Address and Hit Run to generate your endpoint

IP Address:

6. Once the SUT's IP Address has been populated in the Test Case, clicking **Run** initiates the first testing step.

7. The vendor is prompted to navigate to the SUT's messaging client and create a new XDR message. The new message must be accurately formed in the correct syntax. The Vendor will send the XDR message to one of the two ETT generated endpoints (TLS or non-TLS) for the Test Case.
8. Once the XDR message has been transmitted from the SUT to the ETT endpoint, the vendor clicks the **Pending Refresh** button for the Test Case.
9. The ETT checks the generated endpoints for the presence of newly received XDR messages. The vendor is prompted to manually validate if the test results conformed to the testing objectives. To complete this, the vendor clicks the **Waiting Validation** button.
10. The vendor is presented with the Test Case **Log** screen. The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test 7, the vendor will select the **Response** tab to review the ETT logged response received from the SUT after transmission of the XDR message.
11. Within the Log, the vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
  - a. Formed/transmitted the XDR message correctly;
  - b. Attempted to established a connection with the ETT;
  - c. Acknowledged the certificate provided by the ETT as invalid; and
  - d. Successfully rejected a mutual TLS connection with the ETT.
12. If the vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected. Accept XDR selections correlate with Test Case Success results. Likewise, Reject XDR selections correlate with Test Case Failures. Only if the testing objective for a Test Case is in the negative, where the vendor has verified message rejection, will a Reject XDR selection correlate with a Test Success.
13. The ETT presents vendor conformation (XDR validation passed or failed) based upon the selection made.
14. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case. XDR message rejection results in a red X and prompts the vendor to **Retry** the test. The vendor can select the **Clear** button to reset the test. XDR message acceptance results in a green check. The vendor can select the **Clear** button to reset the test.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case’s generated test results (either a **Success** or **Fail**). The **Log** is generated to view individual test result details (e.g., factors for **Success** or **Fail**) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to validate the acceptance of the message received by the SUT*

15. All completed test session data is then available through the ETT’s **Validation Report** tab on the navigation bar.

### 11.1.5 XDR Test Case 3 (Receiver)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the receiver, can process a transmitted XDR message from a HISP (i.e., ETT), acting as the sender, that conforms to given specifications.

The testing details for conformance testing flow are as follows:

1. The vendor assures that the appropriate XDR Certificates have been downloaded from the ETT (direct download link [here](#)) and imported into the SUT’s trust store before executing the test.
2. With the trust relationship established, the vendor navigates to the target Test Case and populates the **Non TLS Endpoint** field with the SUT’s accurate information (all fields should correlate so the ETT and SUT can communicate to execute this test; reference [Section 2.2.1 Profile Creation](#) of this ETT User Guide).
3. The vendor performing this Test Case and in operation of the SUT executes first Test Step by clicking **Run** for the target Test Case.
4. The vendor validates through **Log** review that the SUT successfully received/processed the transmitted XDR message from the ETT and generated the correct response, the XDR message was correctly formatted with **Limited Metadata** and met testing constraints, and testing adhered to the specified requirements within [XDR and XDM for Direct Messaging v1.0](#) and [IHE XDR Profile for Limited Metadata Document Sources](#).

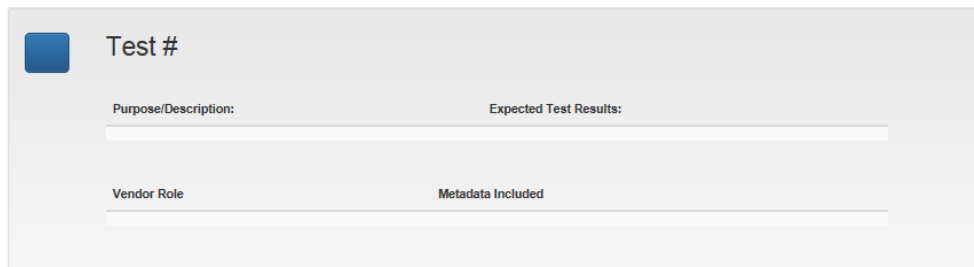
This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 3 of the XDR Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 4.03 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

### 11.1.5.1 Testing Steps

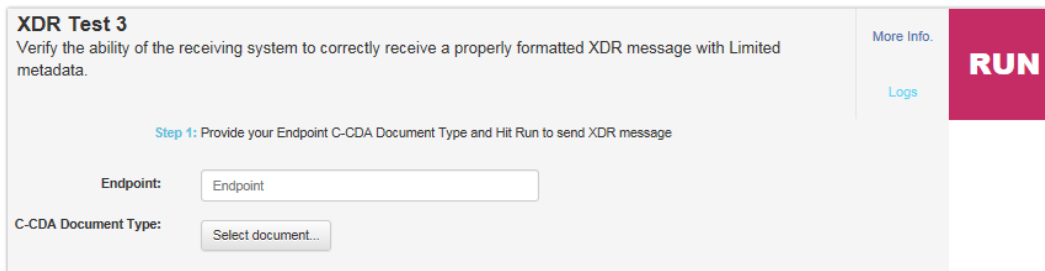
To execute XDR Test Case 3 and assess the SUT's ability to receive/process/respond to an XDR message with Limited Metadata and created in conformance of given specifications, the Vendor must perform the following steps. Within the ETT, XDR Test Case 3 is broken down into four executable tests: 3, 3 – HITSP/C32, 4c, and 3 – CCR. The steps of each are described within the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the navigation bar.
3. From the testing options available, select **Your System as: Receiver**. This will enable test case selection. XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.
4. To gain additional information concerning a target XDR Test Case 3's intended focus, purpose/descriptions, expected test results, vendor role, and metadata inclusion, click the **More Info** link for the Test Case.



The screenshot shows a form titled "Test #". It contains four input fields arranged in a 2x2 grid. The top-left field is labeled "Purpose/Description:", the top-right is "Expected Test Results:", the bottom-left is "Vendor Role", and the bottom-right is "Metadata Included". Each field has a corresponding label above it.

5. To initiate XDR Test Case 3, the vendor must provide the **Endpoint** for the SUT (e.g., operated and managed Edge system). This enables the ETT to communicate with and send an XDR message to the SUT. The provided **Endpoint** of the SUT is the message recipient for this Test Case.



The screenshot shows the "XDR Test 3" configuration page. It includes a description: "Verify the ability of the receiving system to correctly receive a properly formatted XDR message with Limited metadata." Below this, there is a step instruction: "Step 1: Provide your Endpoint C-CDA Document Type and Hit Run to send XDR message". The form contains two main input fields: "Endpoint:" with a text box labeled "Endpoint", and "C-CDA Document Type:" with a button labeled "Select document...". On the right side, there are links for "More Info." and "Logs", and a large red "RUN" button.

6. Once the SUT's Non TLS Endpoint has been inserted, clicking **Run** initiates the test and XDR message transmission from the ETT to SUT.



7. Once the XDR message has been sent, the vendor is prompted to manually validate if the test results conformed to the testing objective. To complete this, the vendor clicks the **Waiting Validation** button.
8. The vendor is presented with the Test Case **Log** screen. The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test Case 3, the vendor will select the **Response** tab to review the ETT logged response received from the SUT after the XDR message has been transmitted.
9. Within the Log, the vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT provided the appropriate testing objective responses for receiving a properly formatted XDR message with Limited Metadata and a Consolidated CDA document attachment.
10. If the vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected. Accept XDR selections correlate with Test Case Success results. Likewise, Reject XDR selections correlate with Test Case Failures. Only if the testing objective for a Test Case is in the negative, where the vendor has verified message rejection, will a Reject XDR selection correlate with a Test Success.
11. The ETT presents vendor conformation (XDR validation passed or failed) based upon the selection made.
12. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case. XDR message rejection results in a red X and prompts the vendor to **Retry** the test. The vendor can select the **Clear** button to reset the test. XDR message acceptance results in a green check. The Vendor can select the **Clear** button to reset the test.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Success** or **Fail**). The **Log** is generated to view individual test result details (e.g., factors for **Success** or **Fail**) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to validate the acceptance of the message received by the SUT*

13. All completed testing session data is then available through the ETT's **Validation Report** tab on the navigation bar.

### 11.1.6 XDR Test Cases 4a & 4b (Receiver)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the receiver, can reject multiple invalid XDR messages from a HISP (i.e., ETT), acting as the sender.



The testing details for conformance testing flow are as follows:

1. The vendor assures that the appropriate XDR Certificates have been downloaded from the ETT (direct download link [here](#)) and imported into the SUT's trust store before executing the test.
2. With the trust relationship established, the vendor navigates to the target Test Case and populates the **Non TLS Endpoint** field with the SUT's accurate information (all fields should correlate so the ETT and SUT can communicate to execute this test; reference [Section 2.2.1 Profile Creation](#) of this ETT User Guide).
3. The vendor performing this Test Case and in operation of the SUT executes the first Test Step by clicking **Run** for the target Test Case.
4. The vendor validates through **Log** review that the SUT successfully received/processed the transmitted XDR messages from the ETT and generated the correct response, the SUT detected the XDR messages contained the invalid conditions of: invalid/inaccurate SOAP Body Details; missing Metadata elements; missing associations between ebRIM constructs; and missing Direct Address Block, and testing adhered to the specified requirements within [XDR and XDM for Direct Messaging v1.0](#) and [IHE XDR Profile for Limited Metadata Document Sources](#).

This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 4 of the XDR Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 4.05, TE170.314(b)(8) – 4.06, TE170.314(b)(8) – 4.07, TE170.314(b)(8) – 4.08, and TE170.314(b)(8) – 4.09 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

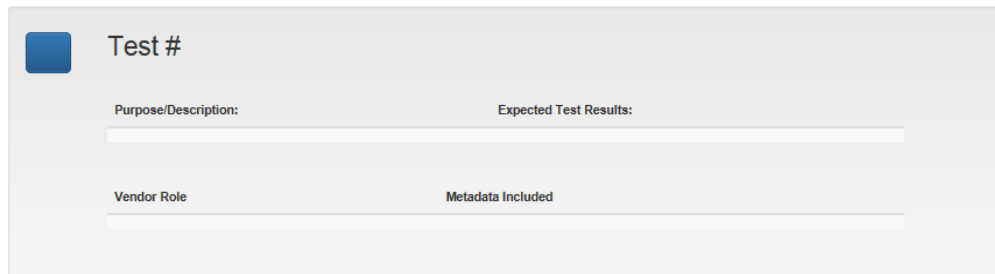
#### 11.1.6.1 Testing Steps

To execute XDR Test Case 4 and assess the SUT's ability to receive/process and reject XDR messages with the invalid construct elements of invalid/inaccurate SOAP Body Details, missing Metadata elements, missing associations between ebRIM constructs, and missing Direct Address Block, the vendor must perform the following steps. Within the ETT, XDR Test Case 4 is broken down into four executable tests: 4a, 4b, 4c, and 4d. The steps of each are described within the following steps.

##### 11.1.6.1.1 4a

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the navigation bar.

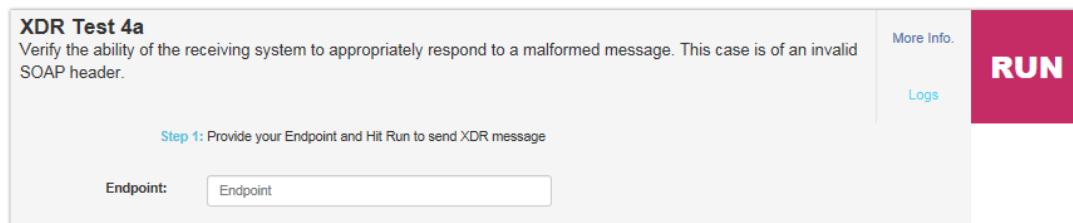
3. From the testing options available, select **Your System as: Receiver**. This will enable test case selection. XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.
4. To gain additional information concerning a target XDR Test Case 4a's intended focus, purpose/description, expected test results, vendor role, and metadata inclusion, click the **More Info** link for the Test Case.



The screenshot shows a form titled "Test #" with a blue square icon to the left. The form is divided into four sections by horizontal lines:

- Purpose/Description:** A text input field.
- Expected Test Results:** A text input field.
- Vendor Role:** A text input field.
- Metadata Included:** A text input field.

5. To initiate XDR Test Case 4a, the vendor must provide the **Non TLS Endpoint** for the SUT (e.g., operated and managed Edge system). This enables the ETT to communicate with and send an XDR message to the SUT. The provided **Non TLS Endpoint** of the SUT is the message recipient for this Test Case.



The screenshot shows the "XDR Test 4a" configuration screen. On the left, there is a description: "Verify the ability of the receiving system to appropriately respond to a malformed message. This case is of an invalid SOAP header." Below this, a step indicator says "Step 1: Provide your Endpoint and Hit Run to send XDR message". There is an "Endpoint:" label followed by a text input field containing the word "Endpoint". On the right side, there are two links: "More Info." and "Logs". A large red button labeled "RUN" is positioned to the right of the "More Info." link.

6. Once the SUT's Non TLS Endpoint has been inserted, clicking **Run** initiates the test and XDR message transmission from the ETT to SUT.
7. Once the XDR message has been sent, the vendor is prompted to manually validate if the test results conformed to the testing objective. To complete this, the vendor clicks the **Waiting Validation** button.
8. The vendor is presented with the Test Case **Log** screen. The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test Case 4a, the vendor will select the **Response** tab to review the ETT logged response received from the SUT after the XDR message has been transmitted.
9. Within the Log, the vendor reviews the testing data content/metadata and performs manual validation to determining if the SUT provided the appropriate testing objective responses for receiving a malformed XDR message with an invalid SOAP header.

10. If the vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected. Accept XDR selections correlate with Test Case Success results. Likewise, Reject XDR selections correlate with Test Case Failures. Only if the testing objective for a Test Case is in the negative, where the vendor has verified message rejection, will a Reject XDR selection correlate with a Test Success.
11. The ETT presents vendor conformation (XDR validation passed or failed) based upon the selection made.
12. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case. XDR message rejection results in a red X and prompts the vendor to **Retry** the test. The vendor can select the **Clear** button to reset the test. XDR message acceptance results in a green check. The vendor can select the **Clear** button to reset the test.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Success** or **Fail**). The **Log** is generated to view individual test result details (e.g., factors for **Success** or **Fail**) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to validate the acceptance of the message received by the SUT*

13. All completed testing session data is then available through the ETT's **Validation Report** tab on the navigation bar.

#### **11.1.6.1.2 4b**

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the navigation bar.
3. From the testing options available, select **Your System as: Receiver**. This will enable test case selection. XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.
4. To gain additional information concerning a target XDR Test Case 4b's intended focus, purpose/descriptions, expected test results, vendor role, and metadata inclusion, click the **More Info** link for the Test Case.

5. To initiate XDR Test Case 4b, the vendor must provide the **Non TLS Endpoint** for the SUT (e.g., operated and managed Edge system). This enables the ETT to communicate with and send an XDR message to the SUT. The provided **Non TLS Endpoint** of the SUT is the message recipient for this Test Case.

6. Once the SUT's Non TLS Endpoint has been inserted, clicking **Run** initiates the test and XDR message transmission from the ETT to SUT.
7. Once the XDR message has been sent, the vendor is prompted to manually validate if the test results conformed to the testing objective. To complete this, the Vendor clicks the **Waiting Validation** button.
8. The vendor is presented with the Test Case **Log** screen. The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test Case 4b, the vendor will select the **Response** tab to review the ETT logged response received from the SUT after the XDR message has been transmitted.
9. Within the Log, the vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT provided the appropriate testing objective responses for receiving a malformed XDR message with an invalid SOAP body.
10. If the vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected. Accept XDR selections correlate with Test Case Success results. Likewise, Reject XDR selections correlate with Test Case Failures. Only if the testing objective for a Test Case is in the negative, where the vendor has verified message rejection, will a Reject XDR selection correlate with a Test Success.

11. The ETT presents vendor conformation (XDR validation passed or failed) based upon the selection made.
12. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case. XDR message rejection results in a red X and prompts the vendor to **Retry** the test. The vendor can select the **Clear** button to reset the test. XDR message acceptance results in a green check. The vendor can select the **Clear** button to reset the test.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Success** or **Fail**). The **Log** is generated to view individual test result details (e.g., factors for **Success** or **Fail**) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to validate the acceptance of the message received by the SUT*

13. All completed testing session data is then available through the ETT's **Validation Report** tab on the navigation bar.

### **11.1.7 XDR Test Case 5 (Receiver)**

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the receiver, can receive/process a properly formatted XDR message from a HISP (i.e., ETT), acting as the sender.

The testing details for conformance testing flow are as follows:

1. The vendor assures that the appropriate XDR Certificates have been downloaded from the ETT (direct download link [here](#)) and imported into the SUT's trust store before executing the test.
2. With the trust relationship established, the vendor navigates to the target Test Case and populates the **Non TLS Endpoint** field with the SUT's accurate information (all fields should correlate so the ETT and SUT can communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
3. The vendor performing this Test Case and in operation of the SUT executes first Test Step by clicking **Run** for the target Test Case.
4. The vendor validates through **Log** review that the SUT successfully received and processed the transmitted XDR message from the ETT and generated the correct response, the SUT acknowledged the message contained **Full Metadata**, and testing adhered to the specified requirements within [XDR and XDM for Direct Messaging v1.0](#) and [IHE XDR Profile for Limited Metadata Document Sources](#).

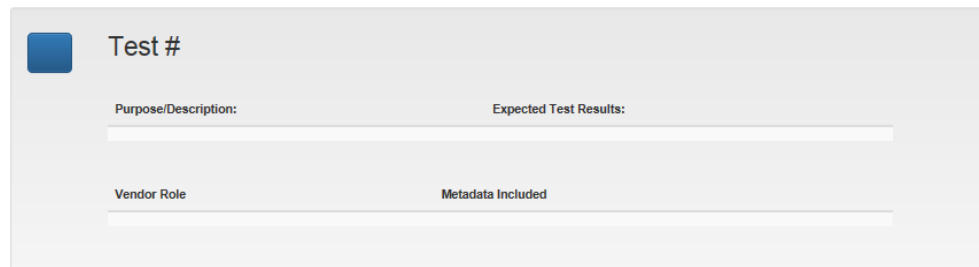
This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 5 of the XDR Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 4.04 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

### 11.1.7.1 Testing Steps

To execute XDR Test Case 5 and assess the SUT's ability to receive/process a properly formatted XDR message with Full Metadata, the vendor must perform the following steps:

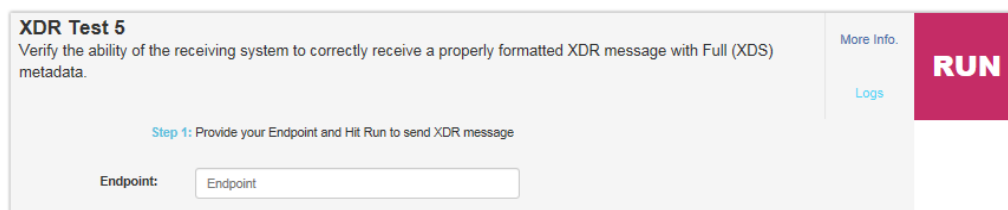
1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the navigation bar.
3. From the testing options available, select **Your System as: Receiver**. This will enable test case selection. XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.
4. To gain additional information concerning XDR Test 5's intended focus, purpose/descriptions, expected test results, vendor role, and metadata inclusion, click the **More Info** link for the Test Case.



The screenshot shows a form titled "Test #" with a blue square icon. It contains four input fields arranged in a 2x2 grid:

- Top-left: Purpose/Description:
- Top-right: Expected Test Results:
- Bottom-left: Vendor Role
- Bottom-right: Metadata Included

5. To initiate XDR Test 5, the vendor must provide the **Endpoint** for the SUT (e.g., operated and managed Edge system). This enables the ETT to communicate with and send an XDR message to the SUT. The provided **Endpoint** of the SUT is the message recipient for this Test Case



The screenshot shows the "XDR Test 5" configuration form. It includes a description: "Verify the ability of the receiving system to correctly receive a properly formatted XDR message with Full (XDS) metadata." and a "More Info." link. Below the description, it says "Step 1: Provide your Endpoint and Hit Run to send XDR message". There is an "Endpoint:" label and an input field. To the right, there is a "Logs" link and a large red "RUN" button.

6. Once the SUT's Endpoint has been inserted, clicking **Run** initiates the test and XDR message transmission from the ETT to SUT.
7. Once the XDR message has been sent, the vendor is prompted to manually validate if the test results conformed to the testing objective(s). To complete this, the vendor clicks the **Waiting Validation** button. The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test Case 5, the vendor will select the **Response** tab to review the ETT logged response received from the SUT after the XDR message has been transmitted.
8. Within the Log, the vendor reviews the testing data content/metadata and performs manual validation to determining if the SUT provided the appropriate testing objective responses for receiving a properly formatted XDR message with Full XDS metadata.
9. If the vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected. Accept XDR selections correlate with Test Case Success results. Likewise, Reject XDR selections correlate with Test Case Failures. Only if the testing objective for a Test Case is in the negative, where the vendor has verified message rejection, will a Reject XDR selection correlate with a Test Success.
10. The ETT presents vendor conformation (XDR validation passed or failed) based upon the selection made.
11. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case. XDR message rejection results in a red X and prompts the Vendor to **Retry** the test. The vendor can select the **Clear** button to reset the test. XDR message acceptance results in a green check. The vendor can select the **Clear** button to reset the test.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Success** or **Fail**). The **Log** is generated to view individual test result details (e.g., factors for **Success** or **Fail**) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to validate the acceptance of the message received by the SUT*

### 11.1.8 XDR Test Case 8 (Receiver)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the receiver, can establish a mutual TLS connection with a HISP (i.e., ETT), acting as the sender, and successfully authenticate before transmitting data.

The testing details for conformance testing flow are as follows:



1. The vendor assures that the appropriate XDR Certificates have been downloaded from the ETT (direct download link [here](#)) and imported into the SUT's trust store before executing the test.
2. With the trust relationship established, the vendor navigates to the target Test Case and populates the **IP Address** and **Port** fields with the SUT's accurate information (all fields should correlate so the ETT and SUT and communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
3. The vendor performing this Test Case and in operation of the SUT executes the first Test Step by clicking **Run** for the target Test Case.
4. The vendor validates through **Log** review that the SUT successfully received the ETT's request to established a Mutual TLS connection, the SUT authenticated with the ETT before transmitting data, and testing adhered to the specified requirements within [XDR and XDM for Direct Messaging v1.0](#) and [IHE XDR Profile for Limited Metadata Document Sources](#).

This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 8 of the XDR Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 4.01 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

#### **11.1.8.1 Testing Steps**

To execute XDR Test Case 8 and assess the SUT's ability to accept an authentication attempt from the ETT and successfully establish a mutual TLS connection, the vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the navigation bar.
3. From the testing options available, select **Your System as: Receiver**. This will enable test case selection. XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.
4. To gain additional information concerning XDR Test Case 8's intended focus, purpose/descriptions, expected test results, vendor role, and metadata inclusion, click the **More Info** link for the Test Case.



Test #8	
<b>Purpose/Description:</b>	<b>Expected Test Results:</b>
Test Tool authenticates with the Edge using Mutual TLS correctly	Edge System is capable of accepting and validating a Mutual TLS connection.
<b>Vendor Role</b>	<b>Metadata Included</b>
Receiver (Edge - SUT)	N/A

- To initiate XDR Test Case 8, the vendor must provide the **IP Address** and **Port** for the SUT (e.g., operated and managed Edge system). This enables the ETT to communicate with and send an XDR message to the SUT. The provided **IP Address** and **Port** of the SUT is the message endpoint recipient for this Test Case.

**XDR Test 8**

Verifies the ability of the receiving system to complete a mutual TLS handshake before data is sent across. Certificates for this test can be downloaded from the link at the top of this page. As this is a socket-level test, the full endpoint is not necessary and only hostname and port are to be entered below.

Step 1: Provide your IP Address Port and Hit Run to send XDR message

IP Address:

Port:

More Info.

Logs

**RUN**

- Once the SUT's IP Address and Port has been inserted, clicking **Run** initiates the test and XDR message transmission from the ETT to SUT.
- Once the XDR message has been sent, the vendor is prompted to manually validate if the test results conformed to the testing objective. To complete this, the vendor clicks the **Waiting Validation** button.
- The vendor is presented with the Test Case **Log** screen. The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test Case 8, the vendor will select the **Response** tab to review the ETT logged response received from the SUT after the XDR message has been transmitted. The vendor validates that the SUT completed a mutual TLS handshake with the ETT before sending data.
- Within the Log, the vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT completed a mutual TLS handshake with the ETT before transmitting any data.
- If the vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected.

Accept XDR selections correlate with Test Case Success results. Likewise, Reject XDR selections correlate with Test Case Failures. Only if the testing objective for a Test Case is in the negative, where the vendor has verified message rejection, will a Reject XDR selection correlate with a Test Success.

11. The ETT presents vendor conformation based upon the selection made.
12. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case. XDR message rejection results in a red X and prompts the vendor to **Retry** the test. The vendor can select the **Clear** button to reset the test. XDR message acceptance results in a green check. The vendor can select the **Clear** button to reset the test.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Success** or **Fail**). The **Log** is generated to view individual test result details (e.g., factors for **Success** or **Fail**) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to validate the acceptance of the message received by the SUT*

13. All completed testing session data is then available through the ETT's **Validation Report** tab on the navigation bar.

### 11.1.9 XDR Test Case 9 (Receiver)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the receiver, can detect an invalid certificate provided by a HISP (i.e., ETT), acting as the sender, during a Mutual TLS connection attempt and successfully disconnect.

The testing details for conformance testing flow are as follows:

1. The Tester vendor assures that the appropriate XDR Certificates have been downloaded from the ETT (direct download link [here](#)) and imported into the SUT's trust store before executing the test.
2. With the trust relationship established, the vendor navigates to the target Test Case and populates the **IP Address** and **Port** fields with the SUT's accurate information (all fields should correlate so the ETT and SUT can communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
3. The vendor performing this Test Case and in operation of the SUT executes the first Test Step by clicking **Run** for the target Test Case.
4. The vendor validates through **Log** review that the SUT attempted to establish a Mutual TLS connection with the ETT, the SUT identified during authentication invalid certificates provided by the ETT, the SUT successfully disconnected from the ETT without authenticating and/or transmitting any data, and testing adhered to the specified

requirements within [XDR and XDM for Direct Messaging v1.0](#) and [IHE XDR Profile for Limited Metadata Document Sources](#).

This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 9 of the XDR Test Cases tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 4.02 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion

### 11.1.9.1 Testing Steps

To execute XDR Test Case 9 and assess the SUT's ability to successfully identify invalid certificates provided during a Mutual TLS connection attempt and terminate a session, the vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the navigation bar.
3. From the testing options available, select **Your System as: Receiver**. This will enable test case selection. XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.
4. To gain additional information concerning XDR Test Case 9's intended focus, purpose/descriptions, expected test results, vendor role, and metadata inclusion, click the **More Info** link for the Test Case.

Test #9	
Purpose/Description:	Expected Test Results:
Test Tool authenticates with the Edge using bad certificates	Edge System rejects the connection due to the bad certificate published by the Test Tool.
Vendor Role	Metadata Included
Receiver (Edge - SUT)	N/A

5. To initiate XDR Test Case 9, the vendor must provide the **IP Address** and **Port** for the SUT (e.g., operated and managed Edge system). This enables the ETT to communicate with and send an XDR message to the SUT. The provided **IP Address** and **Port** of the SUT is the message endpoint recipient for this Test Case.

**XDR Test 9**  
 Verifies the ability of the receiving system to reject a mutual TLS connection where the certificate provided by the ETT is invalid. Certificates for this test can be downloaded from the link at the top of this page. As this is a socket-level test, the full endpoint is not necessary and only hostname and port are to be entered below. The SUT MUST attempt an HTTPS connection.

[More Info.](#)

[Log](#)

**RUN**

Step 1: Provide your IP Address Port and Hit Run to send XDR message

IP Address:

Port:

6. Once the SUT's IP Address and Port has been inserted, clicking **Run** initiates the test and XDR message transmission from the ETT to SUT.
7. Once the XDR message has been sent, the vendor is prompted to manually validate if the test results conformed to the testing objective. To compete this, the vendor clicks the **Waiting Validation** button.
8. The vendor is presented with the Test Case **Log** screen. The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test Case 9, the vendor will select the **Response** tab to review the ETT logged response received from the SUT after the XDR message has been transmitted. The vendor validates that the SUT attempted to establish a connection to the ETT, received/detected an invalid certificate during the mutual TLS handshake process, and terminated the connection to the ETT before any data was transmitted.
9. Within the Log, the vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT terminated a mutual TLS connection attempt from the ETT due to an invalid certificate (this is a negative test).
10. If the vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected. Accept XDR selections correlate with Test Case Success results. Likewise, Reject XDR selections correlate with Test Case Failures. Only if the testing objective for a Test Case is in the negative, where the vendor has verified message rejection, will a Reject XDR selection correlate with a Test Success.
11. The ETT presents vendor conformation (XDR validation passed or failed) based upon the selection made.
12. Acceptance or rejection of the XDR message Log content results in the overall success of failure of a Test Case. XDR message rejection results in a red X and prompts the vendor to **Retry** the test. The vendor can select the **Clear** button to reset the test. XDR message acceptance results in a green check. The vendor can select the **Clear** button to reset the test.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Success** or **Fail**). The **Log** is generated to view individual test result details (e.g., factors for **Success** or **Fail**) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to validate the acceptance of the message received by the SUT*

13. All completed testing session data is then available through the ETT's **Validation Report** tab on the navigation bar.

## 12.0 XDR MESSAGE TRACKING

### 12.1 Message Tracking (MT) Test Cases

#### 12.1.1 XDR MT Test Case 19 (Sender)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the sender, can establish a connection to a HISP (i.e., ETT), acting as the receiver, and successfully generate and transmit a series of XDR messages containing unique IDs.

The testing details for conformance testing flow are as follows:

1. The vendor assures that the appropriate XDR Certificates have been downloaded from the ETT (direct download link [here](#)) and imported into the SUT's trust store before executing the test.
2. With the trust relationship established, the vendor navigates to the target Test Case and populates the **Direct From Address** field with the SUT's accurate information (all fields should correlate so the ETT and SUT and communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
3. The vendor performing this Test Case and in operation of the SUT executes the first Test Step by clicking **Run** for the target Test Case. The ETT generates two endpoints (TLS and Non-TLS).
4. The vendor executes the second Test Step by navigating to the SUT's messaging client and creating three (3) new XDR messages. These new message must be accurately formed in the correct syntax and contain unique message IDs (no duplicates). The SUT will send the 3 XDR messages in a series to one (and only one) of the two ETT generated endpoints (TLS or non-TLS) for the Test Case.
5. The vendor validates through **Log** review that the SUT successfully transmitted the 3 XDR messages, each transmitted message has a unique ID (no duplicates) in the WS-Addressing header element, the SUT successfully transmitted message tracking information to the ETT through a processed MDN notification for each of the 3 messages, established a connection (Mutual TLS) with the ETT generated endpoint, the SUT authenticated with the ETT generated endpoint before transmitting data, the messages met testing constraints, and testing adhered to the specified requirements within [XDR and XDM for Direct Messaging v1.0](#) and [IHE XDR Profile for Limited Metadata Document Sources](#).

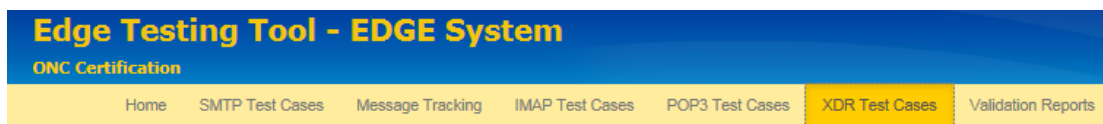
This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.5.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 19 of the Message Tracking (MT) tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 2.07 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

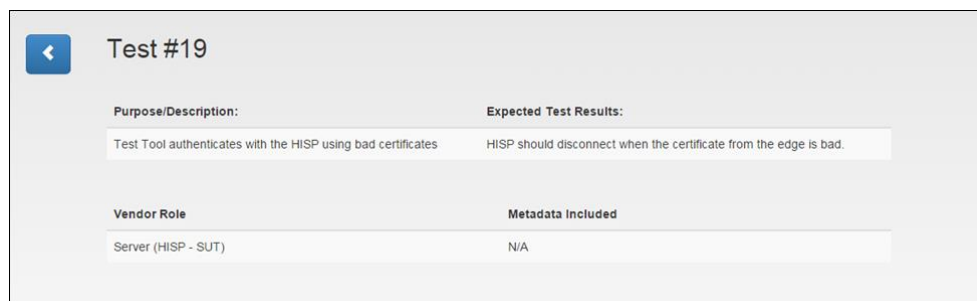
### 12.1.1.1 Testing Steps

To execute XDR Message Tracking (MT) 19 and assess the SUT's ability to successfully generate and transmit a series of XDR messages containing unique IDs, the vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the navigation bar.



3. From the testing options available, select **Your System as: Sender**. This will enable Test Case selection. XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.
4. To gain additional information concerning XDR Message Tracking (MT) 19's intended focus, purpose/descriptions, expected test results, vendor role, and Metadata inclusion, click the **More Info** link for the Test Case.



5. To initiate XDR Message Tracking (MT) 19, the vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT process/present log data accordingly.

**XDR MT Test 19**  
Verifies the ability of the sending system to send messages with unique message-IDs. Hit 'RUN' and then the sending system will send three messages with unique identifiers to the endpoint provided. When all three messages have been completely sent, press the 'Pending Refresh' button.

[More Info.](#) [Logs](#) **RUN**

Step 1: Provide your Direct From Address and Hit Run to generate your endpoint

Direct From Address:

6. Once the SUT's Direct From Address has been populated in the Test Case, clicking **Run** initiates the first testing step.
7. The vendor is prompted to navigate to the SUT's messaging client and create three (3) new XDR messages. These new messages must be accurately formed in the correct syntax and contain unique message IDs (no duplicates). The vendor will send the 3 XDR messages in a series to one (and only one) of the two ETT generated endpoints (TLS or non-TLS) for the Test Case.
8. Once the 3 XDR messages have been transmitted from the SUT to the ETT endpoints, the vendor clicks the **Pending Refresh** button for the Test Case.
9. The ETT checks the generated endpoints for the presence of newly received XDR messages. The vendor is prompted to manually validate if the test results conformed to the testing objectives. To complete this, the vendor clicks the **Waiting Validation** button.
10. The vendor is presented with the Test Case **Log** screen. The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Message Tracking (MT) 19, the vendor will select the **Response** tab to review the ETT logged response received from the SUT after transmission of the XDR messages.
11. Within the Log, the vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
  - a. Accurately established a connection with the ETT;
  - b. Formed/transmitted 3 XDR messages with unique IDs; and
  - c. Generated conformant Processed MDNs for messaging tracking purposes.
12. If the vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected. Accept XDR selections correlate with Test Case Success results. Likewise, Reject XDR selections correlate with Test Case Failures. Only if the testing objective for a Test Case is in the negative, where the vendor has verified message rejection, will a Reject XDR selection correlate with a Test Success.
13. The ETT presents vendor conformation (XDR validation passed or failed) based upon the selection made.



14. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case. XDR message rejection results in a red X and prompts the vendor to **Retry** the test. The vendor can select the **Clear** button to reset the test. XDR message acceptance results in a green check. The vendor can select the **Clear** button to reset the test.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Success** or **Fail**). The **Log** is generated to view individual test result details (e.g., factors for **Success** or **Fail**) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to validate the acceptance of the message received by the SUT*

15. All completed test session data is then available through the ETT's **Validation Report** tab on the navigation bar.

### 12.1.2 XDR MT Test Cases 20a & 20b (Sender)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the sender, can initiate an XDR message transaction with both a valid and invalid HISP recipient (i.e., ETT), acting as the receiver, and generate process MDNs successfully.

The testing details for conformance testing flow are as follows:

1. The vendor assures that the appropriate XDR Certificates have been downloaded from the ETT (direct download link [here](#)) and imported into the SUT's trust store before executing the test.
2. With the trust relationship established, the vendor navigates to the target Test Case and populates the **Direct From Address** field with the SUT's accurate information (all fields should correlate so the ETT and SUT and communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
3. The vendor performing this Test Case and in operation of the SUT executes the first Test Step by clicking **Run** for the target Test Case. The ETT generates two endpoints (TLS and Non-TLS).
4. The vendor executes the second Test Step by navigating to the SUT's messaging client and creating two (2) new XDR messages. These new message must be accurately formed in the correct syntax. The SUT will send the 2 XDR messages in a series to one (and only one) of the two ETT generated endpoints (TLS or non-TLS) for the Test Case. The vendor will also specify a valid and invalid recipient for each of the 2 XDR messages (these are in addition to the ETT generated endpoints).

5. The vendor validates through **Log** review that the SUT successfully transmitted the 2 XDR messages, each transmitted message included a valid/invalid recipient, the SUT successfully transmitted message tracking information to the ETT through a processed MDN notifications for each of the 2 messages, the SUT generated and handled appropriately the process MDNs for both the valid and invalid recipients, the messages met testing constraints, and testing adhered to the specified requirements within [XDR and XDM for Direct Messaging v1.0](#) and [IHE XDR Profile for Limited Metadata Document Sources](#).

This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.5.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 20 of the Message Tracking (MT) tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 2.08 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion

### 12.1.2.1 Testing Steps

To execute XDR Message Tracking (MT) 20a & 20b and assess the SUT's ability to send an XDR message to both valid/invalid recipients and generate/handle process MDNs successfully, the vendor must perform the following steps. Within the ETT, XDR Message Tracking (MT) 20 is broken down into two executable tests: 20a and 20b. The steps of each are described within the following steps.

#### 12.1.2.1.1 20a

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the navigation bar.
3. From the testing options available, select **Your System as: Sender**. This will enable test case selection. Please note that the XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.
4. To gain additional information concerning XDR Message Tracking (MT) 20a's intended focus, purpose/description, expected test results, vendor role, and metadata inclusion, click the **More Info** link for the Test Case.

5. To initiate XDR Message Tracking (MT) 20a, the vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly. For this Test Case, the TLS Endpoint is provided by the vendor.

6. Once the SUT's Direct From Address has been populated in the Test Case, clicking **Run** initiates the first testing step.
7. The vendor is prompted to navigate to the SUT's messaging client and create two a new XDR message. These new message must be accurately formed in the correct syntax. The vendor will send the XDR message to one of the two ETT generated endpoints (TLS or non-TLS) for the Test Case. The vendor will also specify a valid recipient for the XDR messages (in addition to the ETT generated endpoint).
8. Once the XDR message has been transmitted from the SUT to the ETT endpoint, the vendor clicks the **Pending Refresh** button for the Test Case.
9. The ETT checks the generated endpoint(s) for the presence of a newly received XDR message. The vendor is prompted to manually validate if the test results conformed to the testing objectives. To compete this, the vendor clicks the **Waiting Validation** button.
10. The Vendor is presented with the Test Case **Log** screen. The vendor is prompted to check the SUT's local logs and validate that the process MDNs generated as a result of sending the XDR message to both the ETT and valid recipients were handled correctly.
11. After the vendor has reviewed and validated the SUT's log, the vendor navigates back to the ETT's Log screen for XDR Message Tracking (MT) 20a. The vendor finalizes the

review of the testing data by viewing the Log's option tabs message **Request** and **Response** data.

12. The vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
  - a. Accurately established a connection with the ETT;
  - b. Correctly created and transmitted the XDR message to the provided ETT endpoint recipient and additional valid message recipient;
  - c. Produced conformant process MDNs for messaging tracking purposes (valid recipient); and
  - d. Correctly receive and handle a process MDN notification sent from the ETT.
13. If the vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected. Accept XDR selections correlate with Test Case Success results. Likewise, Reject XDR selections correlate with Test Case Failures. Only if the testing objective for a Test Case is in the negative, where the vendor has verified message rejection, will a Reject XDR selection correlate with a Test Success.
14. The ETT presents vendor conformation (XDR validation passed or failed) based upon the selection made.
15. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case. XDR message rejection results in a red X and prompts the vendor to **Retry** the test. The vendor can select the **Clear** button to reset the test. XDR message acceptance results in a green check. The vendor can select the **Clear** button to reset the test.

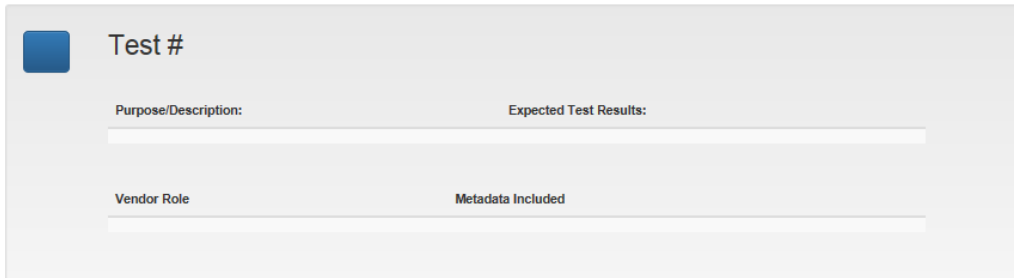
***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Success** or **Fail**). The **Log** is generated to view individual test result details (e.g., contributing factors for **Success** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view result outcomes. This enables the vendor to validate the acceptance of the message received by the SUT.*

16. All completed test session data is then available through the ETT's **Validation Report** tab on the navigation bar.

#### 12.1.2.1.2 20b

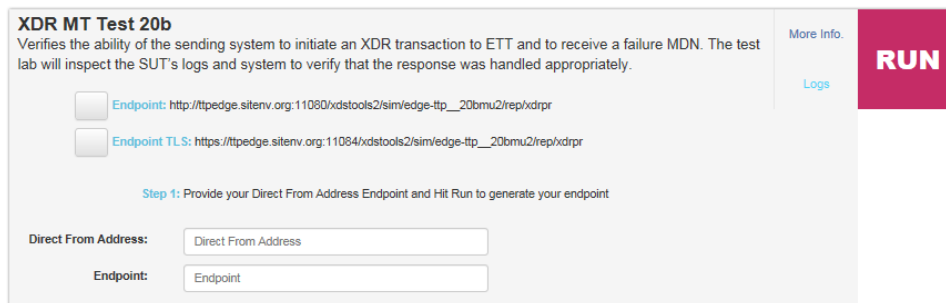
1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the navigation bar.

3. From the testing options available, select **Your System as: Sender**. This will enable test case selection. Please note that the XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.
4. To gain additional information concerning XDR Message Tracking (MT) 20b's intended focus, purpose/description, expected test results, vendor role, and metadata inclusion, click the **More Info** link for the Test Case.



The screenshot shows a form titled "Test #". It contains four input fields arranged in a 2x2 grid. The top-left field is labeled "Purpose/Description:", the top-right is "Expected Test Results:", the bottom-left is "Vendor Role", and the bottom-right is "Metadata Included". Each field has a corresponding label above it.

5. To initiate XDR Message Tracking (MT) 20b, the vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly.



The screenshot shows the "XDR MT Test 20b" configuration page. It includes a description: "Verifies the ability of the sending system to initiate an XDR transaction to ETT and to receive a failure MDN. The test lab will inspect the SUT's logs and system to verify that the response was handled appropriately." Below this are two input fields for "Endpoint" and "Endpoint TLS". A "More Info" link is visible. A "RUN" button is prominently displayed on the right. Below the input fields, there is a "Step 1: Provide your Direct From Address Endpoint and Hit Run to generate your endpoint" instruction. At the bottom, there are input fields for "Direct From Address:" and "Endpoint:".

6. Once the SUT's Direct From Address has been populated in the Test Case, clicking **Run** initiates the first testing step. For this Test Case, the TLS Endpoint is provided by the vendor.
7. The vendor is prompted to navigate to the SUT's messaging client and create two a new XDR message. These new message must be accurately formed in the correct syntax. The vendor will send the XDR message to one of the two ETT generated endpoints (TLS or non-TLS) for the Test Case. The vendor will also specify an invalid recipient for the XDR messages (in addition to the ETT generated endpoint).
8. Once the XDR message has been transmitted from the SUT to the ETT endpoint, the vendor clicks the **Pending Refresh** button for the Test Case.

9. The ETT checks the generated endpoint(s) for the presence of a newly received XDR message. The vendor is prompted to manually validate if the test results conformed to the testing objectives. To complete this, the vendor clicks the **Waiting Validation** button.
10. The vendor is presented with the Test Case **Log** screen. The Vendor is prompted to check the SUT's local logs and validate that the process MDNs generated as a result of sending the XDR message to both the ETT and invalid recipients were handled correctly.
11. After the vendor has reviewed and validated the SUT's log, the vendor navigates back to the ETT's Log screen for XDR Message Tracking (MT) 20b. The vendor finalizes the review of the testing data by viewing the Log's option tabs message **Request** and **Response** data.
12. The Vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
  - a. Accurately established a connection with the ETT;
  - b. Correctly created and transmitted the XDR message to the provided ETT endpoint recipient and additional valid message recipient;
  - c. Produced conformant process MDNs for messaging tracking purposes (valid recipient); and
  - d. Correctly received and handled a process MDN failure notification sent from the ETT.
13. If the vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected. Accept XDR selections correlate with Test Case Success results. Likewise, Reject XDR selections correlate with Test Case Failures. Only if the testing objective for a Test Case is in the negative, where the vendor has verified message rejection, will a Reject XDR selection correlate with a Test Success.
14. The ETT presents vendor conformation (XDR validation passed or failed) based upon the selection made.
15. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case. XDR message rejection results in a red X and prompts the vendor to **Retry** the test. The vendor can select the **Clear** button to reset the test. XDR message acceptance results in a green check. The vendor can select the **Clear** button to reset the test.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case’s generated test results (either a **Success** or **Fail**). The **Log** is generated to view individual test result details (e.g., contributing factors for **Success** or **Fail** outcomes) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to view result outcomes. This enables the vendor to validate the acceptance of the message received by the SUT.*

16. All completed test session data is then available through the ETT’s **Validation Report** tab on the navigation bar.

### 12.1.3 XDR MT Test Case 48 (Sender)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the sender, can establish successfully generate and transmit a series of XDR messages containing unique IDs to a HISP (i.e., ETT), acting as the receiver.

The testing details for conformance testing flow are as follows:

1. As a precondition for this Test Case, the SUT must implement the additional constraints defined within [Implementation Guide for Message Tracking \(MT\) for Direct v1.0](#) for Message Tracking (MT) messaging and increased levels of message transmission assurance.
2. The vendor assures that the appropriate XDR Certificates have been downloaded from the ETT (direct download link [here](#)) and imported into the SUT’s trust store before executing the test.
3. With the trust relationship established, the vendor navigates to the target Test Case and populates the **Direct From Address** field with the SUT’s accurate information (all fields should correlate so the ETT and SUT and communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
4. The vendor performing this Test Case and in operation of the SUT executes first Test Step by clicking **Run** for the target Test Case. The ETT generates two endpoints (TLS and Non-TLS).
5. The vendor executes the second Test Step by navigating to the SUT’s messaging client and creating three (3) new XDR messages. These messages must be accurately formed in the correct syntax and contain unique message IDs (no duplicates). The SUT will send the 3 XDR messages in a series to one of the two ETT generated endpoints (TLS or non-TLS) for the Test Case.
6. The vendor validates through **Log** review that the SUT successfully transmitted the 3 XDR messages, each transmitted message had a unique ID (no duplicates) in the WS-Addressing header element, the SUT successfully transmitted message tracking information to the ETT through a processed MDN notification for each of the 3



messages, established a Mutual TLS connection with the ETT generated endpoint, the SUT authenticated with the ETT generated endpoint before transmitting data, the messages met testing constraints, and testing adhered to the specified requirements within [XDR and XDM for Direct Messaging v1.0](#) and [IHE XDR Profile for Limited Metadata Document Sources](#).

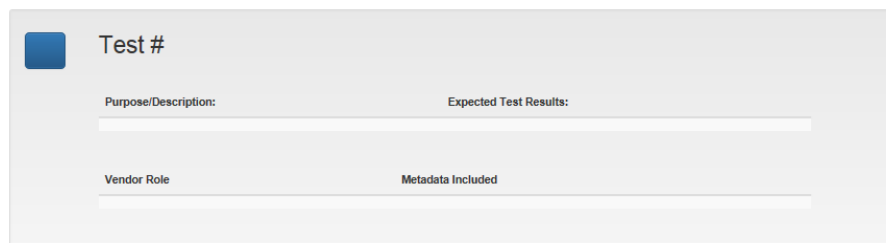
This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.5.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 19 of the Message Tracking (MT) tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 2.09 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

### 12.1.3.1 Testing Steps

To execute XDR Message Tracking (MT) 48 and assess the SUT’s ability to successfully generate and transmit a series of XDR messages containing unique IDs in conformance with message tracking using Implementation Guide for Message Tracking (MT) requirements, the vendor must perform the following steps:

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the navigation Bar.
3. From the testing options available, select **Your System as: Sender**. This will enable test case selection. XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.
4. To gain additional information concerning XDR Message Tracking (MT) 48’s intended focus, purpose/descriptions, expected test results, vendor role, and metadata inclusion, click the **More Info** link for the Test Case.



Test #	
Purpose/Description:	Expected Test Results:
Vendor Role	Metadata Included

5. To initiate XDR Message Tracking (MT) 48, the vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly.



### XDR MT Test 48

Verifies the ability of the sending system to send messages with unique message-IDs. Hit 'RUN' and then the sending system will send three messages with unique identifiers to the endpoint provided. When all three messages have been completely sent, press the 'Pending Refresh' button. (Message Tracking Using "Implementation Guide for Delivery Notification")

Step 1: Provide your Direct From Address and Hit Run to generate your endpoint

Direct From Address:

[More Info.](#)

[Logs](#)

**RUN**

6. Once the SUT's Direct From Address has been populated in the Test Case, clicking **Run** initiates the first testing step.
7. The vendor is prompted to navigate to the SUT's messaging client and create three (3) new XDR messages. These new messages must be accurately formed in the correct syntax and contain unique message IDs (no duplicates). The vendor will send the 3 XDR messages in a series to one (and only one) of the two ETT generated endpoints (TLS or non-TLS) for the Test Case.
8. Once the 3 XDR messages have been transmitted from the SUT to the ETT endpoints, the vendor clicks the **Pending Refresh** button for the Test Case.
9. The ETT checks the generated endpoints for the presence of newly received XDR messages. The Vendor is prompted to manually validate if the test results conformed to the testing objectives. To complete this, the Vendor clicks the **Waiting Validation** button.
10. The Vendor is presented with the Test Case **Log** screen. The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Message Tracking (MT) 48, the vendor will select the **Response** tab to review the ETT logged response received from the SUT after transmission of the XDR messages.
11. Within the Log, the vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
  - a. Accurately established a connection with the ETT;
  - b. Formed/transmitted 3 XDR messages with unique message IDs;
  - c. Upheld conformance with message tracking using Implementation Guide for Message Tracking (MT) requirements; and
  - d. Generated conformant process MDNs for messaging tracking purposes.
12. If the vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected. Accept XDR selections correlate with Test Case Success results. Likewise, Reject XDR selections correlate with Test Case Failures. Only if the testing objective for a Test Case

is in the negative, where the vendor has verified message rejection, will a Reject XDR selection correlate with a Test Success.

13. The ETT presents Vendor conformation (XDR validation passed or failed) based upon the selection made.
14. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case. XDR message rejection results in a red X and prompts the vendor to **Retry** the test. The vendor can select the **Clear** button to reset the test. XDR message acceptance results in a green check. The vendor can select the **Clear** button to reset the test.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Success** or **Fail**). The **Log** is generated to view individual test result details (e.g., factors for **Success** or **Fail**) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to validate the acceptance of the message received by the SUT*

15. All completed test session data is then available through the ETT's **Validation Report** tab on the navigation bar.

#### 12.1.4 XDR MT Test Case 49 (Sender)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the sender, can form and send an XDR message to a HISP (i.e., ETT), acting as the receiver, that conforms to standards for Direct address blocks and Message Tracking (MT) elements.

The testing details for conformance testing flow are as follows:

1. The vendor assures that the appropriate XDR Certificates have been downloaded from the ETT (direct download link [here](#)) and imported into the SUT's trust store before executing the test.
2. With the trust relationship established, the vendor navigates to the target Test Case and populates the **Direct From Address** field with the SUT's accurate information (all fields should correlate so the ETT and SUT and communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
3. The vendor performing this Test Case and in operation of the SUT executes first Test Step by clicking **Run** for the target Test Case. The ETT generates two endpoints (TLS and Non-TLS).
4. The vendor executes the second Test Step by navigating to the SUT's messaging client and creating a new XDR message. This message must be accurately formed in the correct syntax and contain a Direct address block in conformant with Section 4.0 of the [XDR and XDM for Direct Messaging v1.0](#) publication and Section 1.3 of the [Implementation](#)

[Guide for Direct Edge Protocols](#) publication. The SUT will send the XDR message in to one of the two ETT generated endpoints (TLS or non-TLS) for the Test Case.

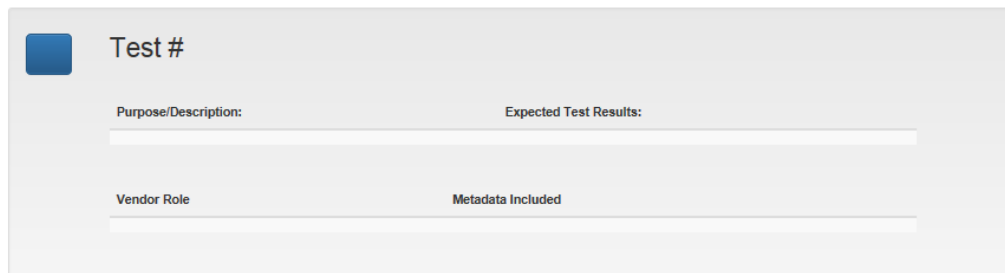
5. The Vendor validates through Log review that the SUT successfully transmitted the XDR message, each transmitted message had a conformant Direct address block (reference Section 4.0 of the [XDR and XDM for Direct Messaging v1.0](#) publication and Section 1.3 of the [Implementation Guide for Direct Edge Protocols](#) publication), assured the messages met testing constraints, and testing adhered to the specified requirements within [IHE XDR Profile for Limited Metadata Document Sources](#).

This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.5.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 20 of the Message Tracking (MT) tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 2.10 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

#### 12.1.4.1 Testing Steps

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the navigation bar.
3. From the testing options available, select **Your System as: Sender**. This will enable test case selection. XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.
4. To gain additional information concerning XDR Message Tracking (MT) 49's intended focus, purpose/descriptions, expected test results, vendor role, and metadata inclusion, click the **More Info** link for the Test Case.



The screenshot shows a light gray rectangular box containing a form. At the top left is a blue square icon followed by the text "Test #". Below this, there are four labeled input fields arranged in a 2x2 grid. The top row contains "Purpose/Description:" and "Expected Test Results:". The bottom row contains "Vendor Role" and "Metadata Included". Each label is positioned to the left of a horizontal white input line.

5. To initiate XDR Message Tracking (MT) 49, the vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly.

**XDR MT Test 49**  
 Verify the ability of the sending system to correctly use a direct address block per the section 4.0 XDR and XDM Messaging for Direct v1.0 and per section 1.3 of the "Implementation Guide for Delivery Notification for Direct v1.0". The SOAP header will be inspected for the appropriate content.

[More Info.](#) [Logs](#) **RUN**

Step 1: Provide your Direct From Address and Hit Run to generate your endpoint

Direct From Address:

6. Once the SUT's Direct From Address has been populated in the Test Case, clicking **Run** initiates the first testing step. Instructions are labeled in sequential order (e.g., **Step 1**, **Step 2**, **Step 3**, etc.) in the content description of the Test Case.
7. The vendor is prompted to navigate to the SUT's messaging client and create a new XDR message. These new message must be accurately formed in the correct syntax and contain a Direct address block in conformant with Section 4.0 of the [XDR and XDM for Direct Messaging v1.0](#) publication and Section 1.3 of the [Implementation Guide for Direct Edge Protocols](#) publication. The vendor will send the message to one (and only one) of the two ETT generated endpoints (TLS or non-TLS) for the Test Case.
8. Once the message has been transmitted from the SUT to the ETT endpoints, the vendor clicks the **Pending Refresh** button for the Test Case.
9. The ETT checks the generated endpoints for the presence of newly received XDR messages. The vendor is prompted to manually validate if the test results conformed to the testing objectives. To compete this, the vendor clicks the **Waiting Validation** button.
10. The vendor is presented with the Test Case **Log** screen. The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Message Tracking (MT) 49, the vendor will select the **Response** tab to review the ETT logged response received from the SUT after transmission of the XDR messages.
11. Within the Log, the vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
  - a. Accurately established a connection with the ETT;
  - b. Formed/transmitted the XDR messages; and
  - c. Upheld compliance with the Direct address block conformance requirements within Section 4.0 of the [XDR and XDM for Direct Messaging v1.0](#) publication and Section 1.3 of the [Implementation Guide for Direct Edge Protocols](#) publication.
12. If the vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected. Accept XDR selections correlate with Test Case Success results. Likewise, Reject XDR

selections correlate with Test Case Failures. Only if the testing objective for a Test Case is in the negative, where the vendor has verified message rejection, will a Reject XDR selection correlate with a Test Success.

13. The ETT presents vendor conformation (XDR validation passed or failed) based upon the selection made.
14. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case. XDR message rejection results in a red X and prompts the vendor to **Retry** the test. The Vendor can select the **Clear** button to reset the test. XDR message acceptance results in a green check. The vendor can select the **Clear** button to reset the test.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Success** or **Fail**). The **Log** is generated to view individual test result details (e.g., factors for **Success** or **Fail**) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to validate the acceptance of the message received by the SUT*

15. All completed test session data is then available through the ETT's **Validation Report** tab on the navigation bar.

### 12.1.5 XDR MT Test Cases 50a & 50b (Sender)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the sender, can create and transmit both valid and invalid XDR messages to a HISP (i.e., ETT), acting as the receiver, and process the cases accurately.

The testing details for conformance testing flow are as follows:

1. The vendor assures that the appropriate XDR Certificates have been downloaded from the ETT (direct download link [here](#)) and imported into the SUT's trust store before executing the test.
2. With the trust relationship established, the vendor navigates to the target Test Case and populates the **Direct From Address** field with the SUT's accurate information (all fields should correlate so the ETT and SUT and communicate to execute this Test Case; reference [2.2.1 Profile Creation](#)).
3. The vendor performing this Test Case and in operation of the SUT executes first Test Step by clicking **Run** for the target Test Case. The ETT generates two endpoints (valid and invalid).
4. The vendor executes the second Test Step by navigating to the SUT's messaging client and creating two (2) new XDR messages. These new messages must be accurately formed in the correct syntax. The SUT will send the 2 XDR messages in a series to one

(and only one) of the two ETT generated endpoints (TLS or non-TLS) for the Test Case. The vendor will also specify a valid and invalid recipient for each of the 2 XDR messages (these are in addition to the ETT generated endpoints).

5. The vendor validates through Log review that the SUT successfully transmitted both the valid and invalid XDR messages, each transmitted message was sent to both a ETT generated endpoint and valid/invalid endpoint recipient, the SUT generated the correct response for both the valid/invalid endpoint recipients, the SUT handled the valid/invalid cases correctly, assured the messages met testing constraints, and testing adhered to the specified requirements within [XDR and XDM for Direct Messaging v1.0](#) and [IHE XDR Profile for Limited Metadata Document Sources](#).

This test maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.5.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 50 of the Message Tracking (MT) tab within the [Direct Edge Protocols](#) spreadsheet and TE170.314(b)(8) – 2.01 within the [ONC 2014 Edition approved Test Procedure requirements document](#). The exact same requirements included in the 2014 Edition are intended to duplicate in the 2015 Edition for this specific criterion.

### 12.1.5.1 Testing Steps

To execute XDR Test Case 50 and assess the SUT's ability to create and transmit both valid and invalid XDR messages to a HISP and process the cases accurately, the vendor must perform the following steps. Within the ETT, XDR Test Case 50 is broken down into two executable tests: 50a and 50b. The steps of each are described within the following steps.

#### 12.1.5.1.1 50a

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the navigation bar.
3. From the testing options available, select **Your System as: Sender**. This will enable test case selection. XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.
4. To gain additional information concerning XDR Message Tracking (MT) 50a's intended focus, purpose/descriptions, expected test results, vendor role, and metadata inclusion, click the **More Info** link for the Test Case.

The screenshot shows a form titled "Test #". It contains four input fields arranged in a 2x2 grid. The top-left field is labeled "Purpose/Description:", the top-right is "Expected Test Results:", the bottom-left is "Vendor Role", and the bottom-right is "Metadata Included". Each field has a horizontal line indicating where to enter text.

5. To initiate XDR Message Tracking (MT) 50a, the vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly. For this Test Case, the Endpoint is provided by the vendor.

The screenshot shows a configuration screen for "XDR MT Test 50a". It includes a description: "Verify the ability of the sending system to correctly handle the case of sending XDR messages to valid recipients. The SUT is expected to appropriately track success messages." Below this are two input fields for "Endpoint" and "Endpoint TLS", both with pre-filled URLs. A "Step 1" instruction says: "Provide your Direct From Address Endpoint and Hit Run to generate your endpoint". At the bottom, there are two input fields labeled "Direct From Address:" and "Endpoint:". On the right side, there is a "More Info." link, a "Logs" link, and a large red "RUN" button.

6. Once the SUT's Direct From Address has been populated in the Test Case, clicking **Run** initiates the first testing step.
7. The vendor is prompted to navigate to the SUT's messaging client and create a new XDR message. These new message must be accurately formed in the correct syntax. The vendor will send the XDR message to one of the two ETT generated endpoints (TLS or non-TLS) for the Test Case. The vendor will also specify a valid recipient for the XDR message (in addition to the ETT generated endpoint).
8. Once the XDR message has been transmitted from the SUT to the ETT endpoint, the vendor clicks the **Pending Refresh** button for the Test Case.
9. The ETT checks the generated endpoint(s) for the presence of a newly received XDR message. The vendor is prompted to manually validate if the test results conformed to the testing objectives. To complete this, the Vendor clicks the **Waiting Validation** button.
10. The vendor is presented with the Test Case **Log** screen. The vendor is prompted to check the SUT's local logs and validate that the process MDNs generated as a result of sending the XDR message to both the ETT and valid recipients were handled correctly.
11. After the vendor has reviewed and validated the SUT's log, the vendor navigates back to the ETT's Log screen for XDR Message Tracking (MT) 50a. The vendor finalizes the



review of the testing data by viewing the Log's option tabs message **Request** and **Response** data.

12. The vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
  - d. Accurately established a connection with the ETT;
  - e. Correctly created and transmitted the XDR message to the provided ETT endpoint recipient and additional valid message recipient;
  - f. Produced conformant process MDNs for messaging tracking purposes (valid recipient); and
  - g. Correctly receive and handle a process MDN notification sent from the ETT.
13. If the vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected. Accept XDR selections correlate with Test Case Success results. Likewise, Reject XDR selections correlate with Test Case Failures. Only if the testing objective for a Test Case is in the negative, where the vendor has verified message rejection, will a Reject XDR selection correlate with a Test Success.
14. The ETT presents vendor conformation (XDR validation passed or failed) based upon the selection made.
15. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case. XDR message rejection results in a red X and prompts the vendor to **Retry** the test. The vendor can select the **Clear** button to reset the test. XDR message acceptance results in a green check. The vendor can select the **Clear** button to reset the test.

***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Success** or **Fail**). The **Log** is generated to view individual test result details (e.g., factors for **Success** or **Fail**) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to validate the acceptance of the message received by the SUT*

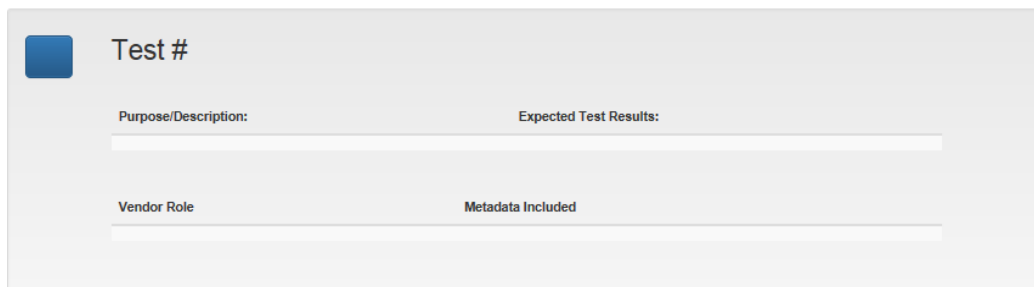
16. All completed test session data is then available through the ETT's **Validation Report** tab on the navigation bar.

### 12.1.5.1.2 50b

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 3 within [2.1 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the navigation bar.



- From the testing options available, select **Your System as: Sender**. This will enable test case selection. XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.
- To gain additional information concerning XDR Message Tracking (MT) Case 50b's intended focus, purpose/descriptions, expected test results, vendor role, and metadata inclusion, click the **More Info** link for the Test Case.

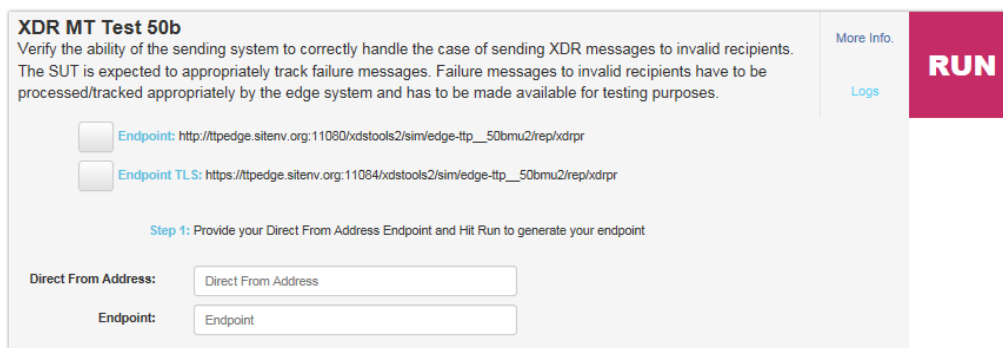


Test #

Purpose/Description: \_\_\_\_\_ Expected Test Results: \_\_\_\_\_

Vendor Role \_\_\_\_\_ Metadata Included \_\_\_\_\_

- To initiate XDR Message Tracking (MT) Case 50b, the vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly. For this Test Case, the Endpoint is provided by the vendor.



**XDR MT Test 50b**  
 Verify the ability of the sending system to correctly handle the case of sending XDR messages to invalid recipients. The SUT is expected to appropriately track failure messages. Failure messages to invalid recipients have to be processed/tracked appropriately by the edge system and has to be made available for testing purposes.

[More Info.](#) [Logs](#) **RUN**

☐ Endpoint: [http://tpege.sitenv.org:11080/xdstools2/sim/edge-ftp\\_\\_50bmu2/rep/xdpr](http://tpege.sitenv.org:11080/xdstools2/sim/edge-ftp__50bmu2/rep/xdpr)

☐ Endpoint TLS: [https://tpege.sitenv.org:11084/xdstools2/sim/edge-ftp\\_\\_50bmu2/rep/xdpr](https://tpege.sitenv.org:11084/xdstools2/sim/edge-ftp__50bmu2/rep/xdpr)

Step 1: Provide your Direct From Address Endpoint and Hit Run to generate your endpoint

Direct From Address:

Endpoint:

- Once the SUT's Direct From Address has been populated in the Test Case, clicking **Run** initiates the first testing step.
- The vendor is prompted to navigate to the SUT's messaging client and create two a new XDR message. These new message must be accurately formed in the correct syntax. The vendor will send the XDR message to one of the two ETT generated endpoints (TLS or non-TLS) for the Test Case. The vendor will also specify an invalid recipient for the XDR messages (in addition to the ETT generated endpoint).
- Once the XDR message has been transmitted from the SUT to the ETT endpoint, the vendor clicks the **Pending Refresh** button for the Test Case.

9. The ETT checks the generated endpoint(s) for the presence of a newly received XDR message. The vendor is prompted to manually validate if the test results conformed to the testing objectives. To complete this, the vendor clicks the **Waiting Validation** button.
10. The vendor is presented with the Test Case **Log** screen. The vendor is prompted to check the SUT's local logs and validate that the process MDNs generated as a result of sending the XDR message to both the ETT and invalid recipients were handled correctly.
11. After the vendor has reviewed and validated the SUT's log, the vendor navigates back to the ETT's Log screen for XDR Message Tracking (MT) Case 50b. The vendor finalizes the review of the testing data by viewing the Log's option tabs message **Request** and **Response** data.
12. The vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
  - h. Accurately established a connection with the ETT;
  - i. Correctly created and transmitted the XDR message to the provided ETT endpoint recipient and additional valid message recipient;
  - j. Produced conformant process MDNs for messaging tracking purposes (valid recipient); and
  - k. Correctly received and handled a process MDN failure notification sent from the ETT.
13. If the vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected. Accept XDR selections correlate with Test Case Success results. Likewise, Reject XDR selections correlate with Test Case Failures. Only if the testing objective for a Test Case is in the negative, where the vendor has verified message rejection, will a Reject XDR selection correlate with a Test Success.
14. The ETT presents vendor conformation (XDR validation passed or failed) based upon the selection made.
15. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case. XDR message rejection results in a red X and prompts the vendor to **Retry** the test. The vendor can select the **Clear** button to reset the test. XDR message acceptance results in a green check. The vendor can select the **Clear** button to reset the test.

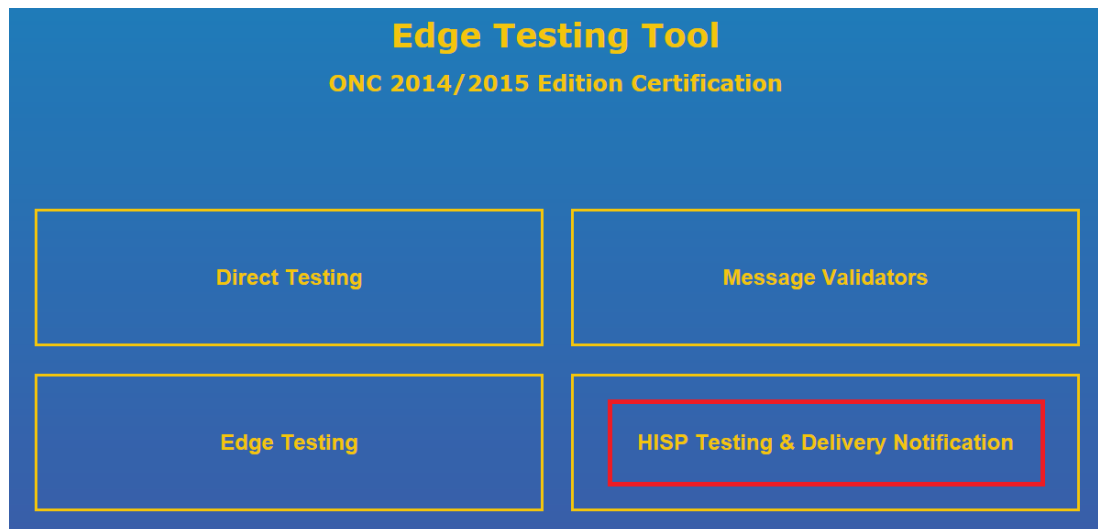
***Note:** Within the Test Procedures, the **Log** directly references a single Test Case's generated test results (either a **Success** or **Fail**). The **Log** is generated to view individual test result details (e.g., factors for **Success** or **Fail**) and stands as a testing artifact. The **Validation Report** represents the aggregation of all Test Cases executed within a given testing session and enables a vendor to validate the acceptance of the message received by the SUT*

16. All completed test session data is then available through the ETT's **Validation Report** tab on the navigation bar.

## 13.0 HISP TESTING & DELIVERY NOTIFICATION

### 13.1 HISP Testing and Delivery Notification

The HISP Testing and Delivery Notification is located on the Home Page.



On the ‘*Direct Registration*’ tab, users will be asked to provide the following information:

- Contact Email Address (e.g., personal email address); and
- Direct Email Address.

## 14.0 MESSAGE VALIDATORS

<This section TBD>