

January 4, 2016  
Revision 2.0

## USER GUIDE

# Edge Testing Tool



## Table of Contents

1.0	OVERVIEW .....	4
1.1	Role of NIST .....	4
1.2	Edge Testing Tool .....	4
1.3	Purpose .....	4
1.4	Access .....	5
1.5	Testing Overview .....	5
2.0	TESTING CONFIGURATION FOR EDGE SYSTEM .....	6
2.1	Configuration Steps .....	6
2.2	Registration .....	6
2.3	Profile Creation .....	9
2.4	Reporting .....	12
2.5	Documentation .....	13
3.0	LOCAL INSTALLATION AND CONFIGURATION .....	14
3.1	Configuration Steps .....	14
3.2	Apache James Server v3.0 .....	14
4.0	DIRECT - SUT SENDING .....	17
4.1	Register a DIRECT Contact Address .....	17
5.0	SENDING C-CDA MESSAGES TO THE DIRECT LISTNER .....	19
5.1	Send a DIRECT Message to the ETT .....	19
5.2	Sending Steps .....	19
5.3	Send a DIRECT + XDM Message to the ETT .....	20
5.4	Send a SOAP Message to the ETT .....	21
6.0	SENDING MESSAGES FROM THE EDGE TESTING TOOL TO A SYSTEM UNDER TEST .....	22
6.1	Send a DIRECT Message to a System Under Test .....	23
6.2	Send a DIRECT + XDM Message to a System Under Test .....	24
7.0	SMTP TESTING .....	26
7.1	SMTP Test Case 14 .....	26
7.1.1	Testing Steps .....	26
7.1.2	SMTP Test Case 18 .....	30
7.1.3	SMTP Test Cases 1 through 8 .....	31
7.1.4	SMTP Message Tracking (MT) 17 .....	34
7.1.5	SMTP Message Tracking (MT) 45 .....	70
7.1.6	SMTP Message Tracking (MT) 46 .....	75
7.1.7	SMTP Message Tracking (MT) 47 .....	80
7.2	SUT Receiving .....	85
7.2.1	SMTP Test Case 16 .....	34
7.2.2	SMTP Test Case 17 .....	57
7.2.3	SMTP Test Case 20 .....	40
7.2.4	SMTP Test Case 22 .....	61
7.2.5	SMTP Test Case 9 .....	34
7.2.6	SMTP Test Case 10 .....	40
7.2.7	SMTP Test Case 11 .....	46

7.2.8	SMTP Test Case 13 .....	52
7.3	XDR Sending .....	57
7.3.1	XDR Test Case 6 .....	85
7.3.2	XDR Test Case 7 .....	92
7.3.3	XDR Test Case 1 .....	98
7.3.4	XDR Test Case 2 .....	104
7.3.5	XDR Message Tracking (MT) 19 .....	110
7.3.6	XDR Message Tracking (MT) 20 .....	116
7.3.7	XDR Message Tracking (MT) 48 .....	128
7.3.8	XDR Message Tracking (MT) 49 .....	135
7.3.9	XDR Message Tracking (MT) 50 .....	141
7.4	XDR Receiving .....	153
7.4.1	XDR Test Case 8 .....	153
7.4.2	XDR Test Case 9 .....	159
7.4.3	XDR Test Case 3 .....	164
7.4.4	XDR Test Case 4 .....	178
7.4.5	XDR Test Case 5 .....	196

## 1.0 OVERVIEW

### 1.1 Role of NIST

Since its foundation in 1901, the National Institute of Standards and Technology (NIST) has been devoted to promoting innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve human qualities of life. In support of this mission, NIST has strategically acknowledged the need for opportunity discovery within the private sector's range of vital industries and technology areas. Under the American Recovery and Reinvestment Act of 2009 (Recovery Act), NIST was called upon to consult the Office of the National Coordinator (ONC) in its mission to encourage greater adoption of interoperable health IT technologies and capabilities. To accomplish this mission, NIST is collaborating with ONC to develop a structured program that eligible professionals, hospitals, and critical access hospitals (CAHs) can achieve that demonstrates compliance with applicable Meaningful Use Stage 2 (MU2)<sup>1</sup> (and forthcoming Stage 3 (MU3)<sup>2</sup>) criteria and requirements. NIST's primary role is to assist ONC in establishing the necessary functional and conformance testing requirements, Test Cases, and testing tool sets need to successfully implement a voluntary health IT certification program.

### 1.2 Edge Testing Tool

NIST has developed a tool to test requirements and standards related to message transport specifications expressed within the 2014/2015 Edition of the ONC Standards & Certification Criteria<sup>3</sup>. The tool, commonly referred to within this document and accompanying resources as the Edge Testing Tool (ETT), tests for adherence to the Edge Protocol standards during valid communication sessions between the ETT and a System Under Test (SUT). The Edge testing tool has also been designed to test 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.

### 1.3 Purpose

To perform certification testing to the Direct and Edge Protocols of ONC 2014/2015 Edition Certification Edition Objectives for message transport, NIST has developed the Transport Testing Tool (TTT) and ETT. Edge Systems (e.g., EHRs) and Health Information Service Providers (HISPs) can specifically use the TTT to perform certification testing against Direct standards and ETT to perform certification testing against Edge Protocols.



**Note:** The TTT has a separate stand-alone User Guide. Thus, it is not discussed in detail within this ETT User Guide and only utilized within the context of EHR certification testing and HISPs Vendor reference.

The purpose of this ETT User Guide is to outline the process by which Edge Systems (e.g., EHRs) 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 (e.g., EHR) or HISPs Vendor can leverage the 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 (e.g., EHR) or HISPs, depending on the specific testing need. Both can send and receive as a SUT. Typically, the Edge System (e.g., EHR) can act as the SUT for Edge testing and the HISPs for both Edge and Direct testing.

#### 1.4 Access

The ETT can be accessed through two (2) interfaces: Web and Local.

- **Web Interface** – The production version of the ETT is accessible online through the following link: <http://edge.nist.gov/>. This web interface link is referred to within the ETT User Guide and accompanying resources as 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.



**Note:** The URL to the **production** version of the ETT is: <http://edge.nist.gov>. The URL to the **development** version of the ETT is: <http://hit-dev.nist.gov:12080/ttt/#home>. NIST will notify ETT users prior to any production version updates. The development version will have ETT's latest code; however, documentation, content, and testing engine availability cannot be guaranteed. Thus, the development version will be updated as needed.

#### 1.5 Testing Overview

- The ETT will allow Testers (i.e., Vendors) to send and receive messages using various transport methods to and from the SUT (acting as either a HISPs or Edge System) dependent upon specific testing objectives. The ETT tool can also test DIRECT.

## 2.0 TESTING CONFIGURATION FOR EDGE SYSTEM

This section guides the Tester (i.e., Vendor) through the necessary configuration and preparation steps for and web application Profile creation and Test Case execution.

### 2.1 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 Registration

1. Navigate to the ETT [Home Page](#) by either clicking the following link or entering it directly into a web browser: <http://edge.nist.gov>.
2. On the ETT [Home Page](#), select the **Edge Testing** option.



*Note: The ETT Date Created, most recent and Last Update, and current Version can be found at the bottom of the ETT's Welcome Screen.*

3. Selecting the **Edge Testing** option will bring up the tool's Home Screen. From here, the Vendor can select the intended Email Address to test their SUT. A response MDN will be sent from ETT email address upon reception of a SMTP message.



**Note:** In its current version and build, the ETT supports the functionality and feature sets to test against the loaded Simple Mail Transfer Protocol (SMTP), Cross-Enterprise Document Reliable Interchange (XDR), and tracking of Message Disposition Notifications (MDNs) using SMTP and XDR.

4. Click **Login/Sign up** and **Sign up** to create a unique user account within the ETT. Enter a **Username** email address and **Password** and click **Sign Up**.

Edge Testing Tool - EDGE System

ONC Certification

Home SMTP Test Cases Message Tracking IMAP Test Cases POP3 Test Cases XDR Test Cases Validation Reports Documents Help

Click Here → Login/Sign up

★ Login

Don't have an account? [Sign up](#)

Username

sut.example@gmail.com

Password

Forgot password?

.....

Remember me

Cancel Login

Before executing any tests within the ETT, **Login** using the credentials created during **Sign Up**.

Edge Testing Tool - EDGE System

ONC Certification

Home SMTP Test Cases Message Tracking IMAP Test Cases POP3 Test Cases XDR Test Cases Validation Reports Documents Help

★ Sign Up

Username

Enter Email Address

Password

Enter password

Repeat Password

Confirm password

Cancel Sign Up

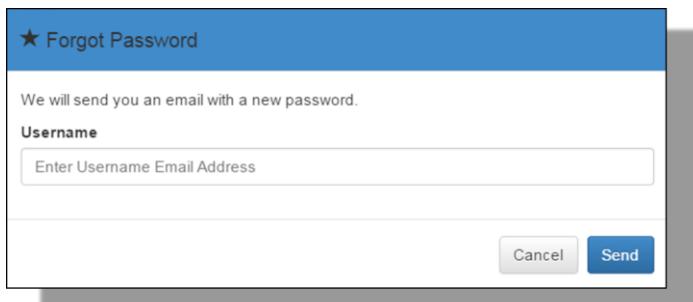


**Note:** The **Username** email address is used for account creation, historic testing session saves, and delivery notification of ETT specific information by NIST personnel. It is not specifically used as a component of SMTP and/or XDR testing. Testing email addresses are configured within specific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

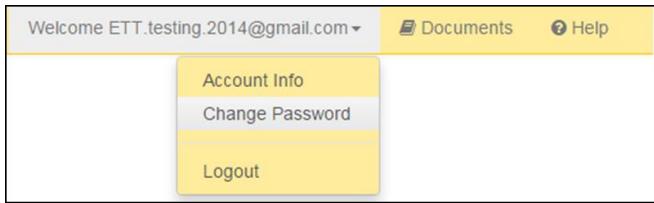
If either the **Login Username** or **Password** is entered incorrectly, an error message will appear prompting the Vendor to reenter credentials.



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 linked email address.



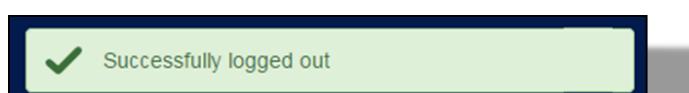
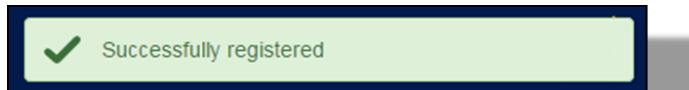
An account **Password** can also be reset through the Navigation Bar after successful **Login**.





**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.

5. A success message will appear upon successful **Sign Up**, **Login**, and **Logout**.

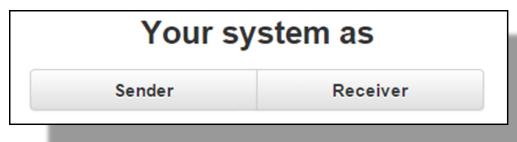


### 2.3 Profile Creation

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.

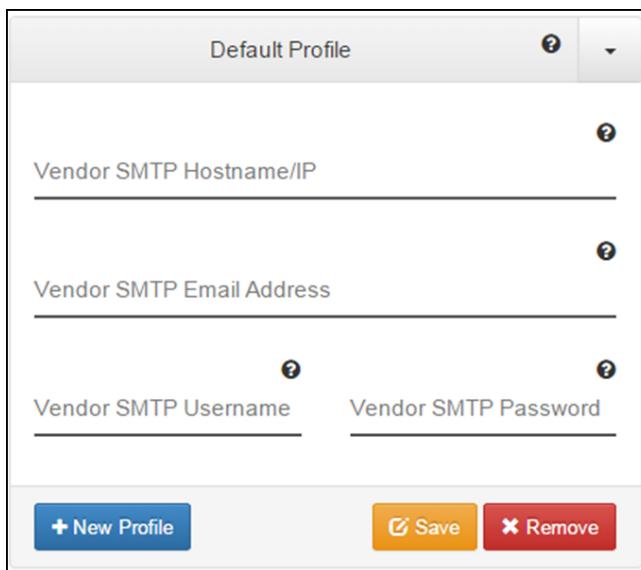


2. Select either the **Sender** or **Receiver** testing role for the SUT.



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

Profile Data Field	Description
<b>Profile Name</b>	The Profile name can be edited and customized based on testing needs by the Vendor. This feature can be accessed by clicking on the <b>Profile</b> header. Saved Profiles can be accessed from within the ETT account created during <a href="#">2.2 Registration</a> .
<b>Vendor SMTP Hostname / IP</b>	SMTP or IP address of the Vendor's email server. This should directly connect with the <b>Vendor SMTP Email Address</b>
<b>Vendor SMTP Email Address</b>	Vendor SMTP Email Address should correspond to the <b>Vendor SMTP Hostname / IP</b> . 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 <b>Vendor SMTP Email Address</b> . The Username and Password are mainly used for authentication based Test Cases so the ETT can login to the SUT.



Hovering over the ? for each **Profile** data field reveals a pop-up containing further explanation/instruction.

Hostname/IP address of the vendor SMTP system  
Default Profile  
Click on the text to edit profile name  
Vendor SMTP Hostname/IP  
Email address of the vendor SMTP system  
Vendor SMTP Email Address  
Username of the vendor SMTP system  
Password of the vendor SMTP system  
Vendor SMTP Username  
Vendor SMTP Password  
+ New Profile      Save      Remove



*Note: For information on how to find the SMTP / IP of your email client/server, please reference vendor specific documentation or the **Help** button located on the ETT's Navigation Bar.*

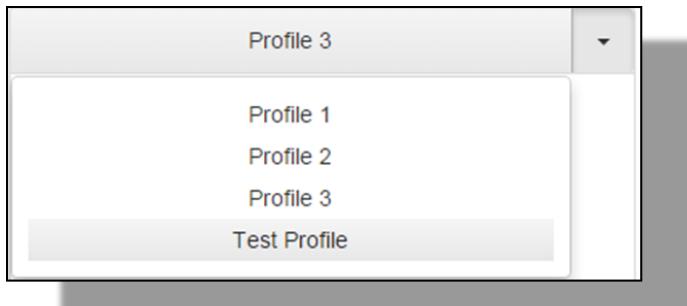
4. Before saving a Profile, assign a unique name (the default Profile name is **Default Profile**). Click the Profile name, delete the existing text, and type a new name. Upon population of the testing Profile, select **Save**. To delete a saved Profile, select **Remove**

+ New Profile      Save      Remove

5. A successful message will appear upon successful **Save** or **Remove**.

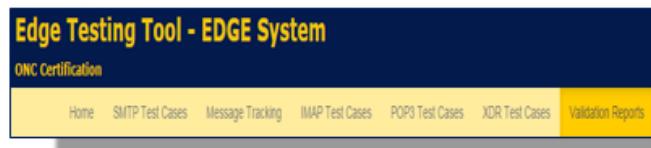


6. Saved Profiles can be retrieved and applied to subsequent/future tests by selecting the target Profile from the drop-down menu.



## 2.4 Reporting

1. 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.



2. 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.



*Note: For a given testing session, the total number of ETT testing **Profiles** used will be displayed within the **Validation Report** tab.*

3. By clicking on the **Show Report** button, the Vendor is given the Test Case executed, a time ran, and Success or Failure of the test. The ‘**Log**’ for each executed Test Case provides further detailed information concerning evidence to support Success or Failure.

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	✓

## 2.5 Documentation

Documentation relevant to the ETT, Test Case execution (including this ETT User Guide), Test Procedures, ONC 2014/2015 Edition Certification Edge Protocol testing objectives, NIST Health IT testing guideline, or other development related artifacts will be made available through the ‘**Documents**’ tab on the Navigation Bar.



## 3.0 LOCAL INSTALLATION AND CONFIGURATION

This section guides the Tester (i.e., 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 at the following directory location [here](#). The needed configuration information (contained within the *application.properties* file) is also in this directory location.



*Note: Data within the application.properties file contains comments and should be mostly self-explanatory for use.*

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 following directory location [here](#).



*Note: 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 assert nor guarantee compatibility with other MySQL versions.*

3. Navigate to the Apache James Server URL and download the application's build.



*Note: 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 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 a defined list of users and mailboxes be installed within the Apache James Server v3.0. This list can be accessed from the following directory location [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 is desired, *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.RequireTLSAuthCmdHandler"/>*
          - 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 ran on Port 110 for internal data pulls.
  - b. Each testing account created for the Apache James Server v3.0 will have four (4) 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 from xdstools2.war from the following link:  
<https://bitbucket.org/jperugini/ett/downloads>. 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 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://bitbucket.org/jperugini/ett/downloads>. 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".



*Note: Users who do not register their DIRECT web address will not be recognized by the ETT and therefore be unable to send or receive DIRECT OR DIRECT/XDM messages.*

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.

Home Register Direct Send Direct Message Message Validator CCDA Validators Login/Sign up Documents Help

## Registration for Transport Testing Tool

These instructions cover the special requirements for sending Direct messages to the NIST Transport Testing Tool Direct message validation system. By its nature, it is difficult to get feedback from the recipient of a Direct/SMTP message. So, to enable message validation feedback, we require pre-registration. This pre-registration links a Direct (From) address that is used to send to the validator to a normal email account. Validation reports are sent back to the email account for review by the user. This panel allows the user to register their email account and link one or more Direct (From) account to it. Direct messages sent from a non-registered Direct (From) address will not be validated nor reported on.

### Register a Direct Email Address

Direct email address

Enter here →

Up



The National Institute of Standards and Technology (NIST) is an agency of the U.S. Department of Commerce.



Privacy policy / security notice / accessibility statement / Disclaimer /

Date created: July 9, 2014 | Last updated: Nov 12, 2015 | Version: 0.0.8

Browsers supported: For best result, Firefox 3.x and Chrome are recommended

#### Registration Steps:

1. Provide a contact email address. This address will be used to email all validation reports.
2. Provide a ‘from’ email address. This address will be registered in the ETT. Any valid content from this address will be validated and the corresponding validation report emailed to the contact address.

Once users have registered, they will be placed on a “white list” of approved email addresses from which the ETT will accept messages.



**Note:** Users not who do not register their contact and DIRECT email addresses will not be recognized by the ETT and therefore not be able to send and/or receive messages.

After user registration is complete and email addresses are successfully created/added, navigate back to the [‘Home Page’](#) tab.

Once complete, refer to [Section 4.0](#) of this User Guide.



**Note:** Users utilizing the SOAP send and receive features of the ETT do not need to pre-register in the ‘Registration’ tab/section. 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.

Since the interaction 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 LISTNER

### 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 ONC's Standards & Certification Criteria 2014/2015 Edition.

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



*Note: MU objectives with the same DIRECT email address (in the table below) use the same validation service in the MDHT validator (i.e., the C-CDA is the same). They are represented in the here to provide clarity to for address and objective mappability.*

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

**Table 3: DIRECT Address**

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.

### 5.2 Sending Steps

1. The Sender will include the Public Key signing certificate. In messages sent to the ETT. Once registered with the ETT, the user selects the ONC objective that is representative and appropriate for the content they are sending (e.g., C-CDA or human readable text).

The sending content will automatically be validated and a report sent to the contact email address entered when during registration.

2. Select the DIRECT email addresses to send the content.
3. The validation report will be sent to the email address created/added during registration.



*Note:* <host-address> is set to the address of the user endpoint (i.e., local machine) the ETT is in operation on.



*Note:* Each email address can also accept text/plain MIME formats to assist in validating human-readable text.

### 5.3 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. This step must be performed using the [Transport Testing Tool](#) (TTT).



*Note:* <host-address> is set to the address of the user endpoint (i.e., local machine) the ETT is in operation on.

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 3.1](#) of this User Guide.

Once registered with the ETT, the user selects the objective/purpose that is representative and appropriate for the content they are sending (e.g., C-CDA or human readable text). The sending content will automatically be validated and a report sent to the contact email address entered when during registration.

1. Based on the objective/purpose the user is testing against, select the DIRECT email addresses to send the content
2. The validation report will be sent to the email address created/added during registration.



*Note:* <host-address> is set to the address of the user endpoint (i.e., local machine) the ETT is in operation on.



*Note: Each email address can also accept text/plain MIME formats to assist in validating human-readable text.*

#### 5.4 Send a SOAP Message to the ETT

Sending messages via SOAP is a mechanism for Message Tracking (MT). 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 1.6](#) of this User Guide Testing Overview 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:

	DIRECT						SOAP		
	S/MIME			XDM Attachment Messages					
	CCR	C-CDA	C32	CCR S/MIMI XDM	C-CDA S/MIMI XDM	C32 S/MIMI XDM	CCR	C-CDA	C32
Requirement									
Optional									

Required ■ Optional ■

Table 6: ETT Message Receiving

- **Direct with S/MIME (Required)**
  - CCR via S/MIME
  - C-CDA via S/MIME
  - C32 via S/MIME
- **Direct with XDM Attachment Messages (Optional)**
  - a. CCR via S/MIME XDM (Optional)
  - b. C-CDA via S/MIME XDM (Optional)
  - c. C32 via S/MIME XDM (Optional)
- **Simple Object Access Protocol (SOAP) (Optional)**
  - CCR via SOAP (Optional)
  - C-CDA via SOAP (Optional)
  - C32 via SOAP(Optional)

For each of the three (3) mechanisms, there are two Objectives for which users can receive C-CDA, CCR, and/or C32 files:

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

## 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](#)' tab, click 'Send Direct Message' link from the 'Direct' column.

Send a Direct Message

Send a Direct message from this tool to a HISp of your choosing

Direct From Address

Format: account\_name@domain

The message content will be signed using the private key for this sending domain (hit-testing.nist.gov) which was inserted into the receiving HISp to validate the content.

Direct To Address

Choose document to be sent as the message content

Message format

Unwrapped Wrapped

2. Send a DIRECT message with the attached C-CDA document to an authorized email addresses corresponding to the MU2 objective under test (reference *Table 3: DIRECT Address to MU2 Objective* in [Section 4.1](#) of this User Guide).
3. Data input into the 'Direct From Address' field must align with address the SUT is expecting to receive email from. The MDN will be sent back to ETT using this address and the associated name will appear in the from field of the message sent.
4. In the 'Direct To Address' field, input the DIRECT address where the message will be sent. This field will only accept one (1) email address, not multiple.
5. Select from one (1) of the six (6) samples within the pull-down menu. There are two (2) C-CCDA, two (2) CCR and two (2) C32 samples to select from.



*Note: 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.



**Note:** All applications must support ‘Unwrapped’. ‘Wrapped is optional.

7. Click the ‘Browse’ button and upload the certificate to be used for encrypting the sent message (Public Key).
8. Click ‘Submit’ to send the DIRECT message.
9. Verify the MDN was received using the instruction 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](#)’ tab, click ‘Send Direct Message’ link from the ‘Direct’ column.



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. Send a DIRECT message with the attached C-CDA document to an authorized email addresses corresponding to the MU2 objective under test (reference *Table 3: DIRECT Address to MU2 Objective* in [Section 4.1](#) of this User Guide).

3. 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.
4. Data input into the ‘*Direct From Address*’ field must align with address the SUT is expecting to receive email from. The MDN will be sent back to ETT using this address and the associated name will appear in the from field of the message sent.
5. In the ‘*Direct To Address*’ field, input the DIRECT address where the message will be sent. This field will only accept one (1) email address, not multiple.
6. Select from one (1) of the six (6) samples within the pull-down menu. There are two (2) C-CCDA, two (2) CCR and two (2) C32 samples to select from.



*Note: Select samples ending with \_in\_XDM.*

7. Select a message format of ‘*Wrapped*’ or “*Unwrapped*”. These actions will either wrap (or not) a message according to RFC 5751.



*Note: All applications must support ‘Unwrapped’. ‘Wrapped’ is optional.*

8. Click the ‘*Browse*’ button and upload the certificate to be used for encrypting the sent message (Public Key).
9. Click ‘*Submit*’ to send the DIRECT message.
10. Verify the MDN was received using the instruction within [Section 6.0](#) in this User Guide.

## 7.0 SMTP TESTING

### 7.1 SMTP TEST CASES

#### 7.1.1 SMTP TEST CASE 14 (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:

- The Tester (i.e., 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@edge.nist.gov](mailto:wellformed1@edge.nist.gov). The SUT will attempt to initiate a secure connection with the ETT based on the STARTTLS protocols.
- 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 [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 3.01 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

##### 7.1.1.1 Testing Steps

To execute SMTP Test 14 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:



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

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 7 within [2.2 Registration](#).

2. For this target SMTP test, select **SMTP Test Cases** from the Navigation Bar. This enables the testing Profile feature of the tool.

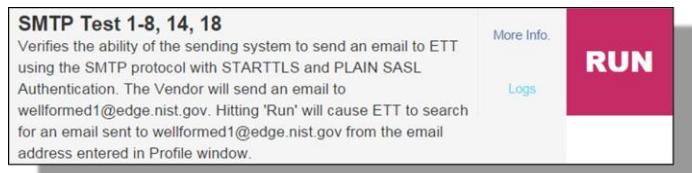


3. From the testing Profile, select **Sender**.

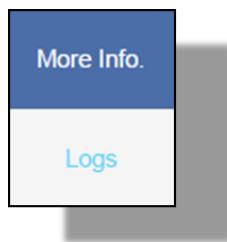


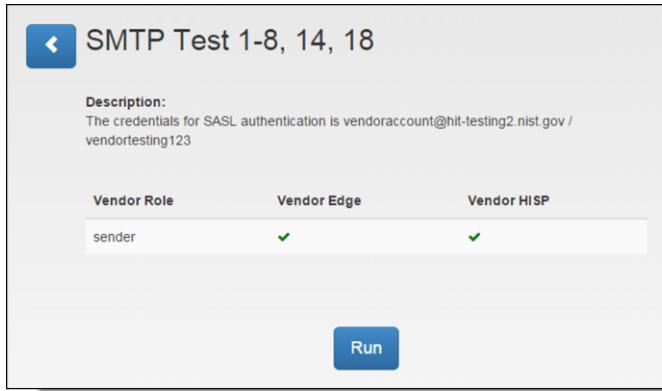
Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 Profile Creation](#).

4. 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, Vendor/SUT roles), click the **More Info** link for the Test Case.





5. With the Profile saved, More Info reviewed, and **SMTP Test 1-8, 14, 18** 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 single new message and send it to the ETT endpoint recipient [wellformed1@edge.nist.gov](mailto:wellformed1@edge.nist.gov).
  - 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.

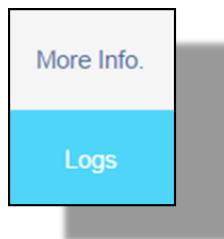


6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
  - A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
  - A test Fail prompts the Vendor to **Retry** the test.
  - The **Clear** button resets the test and any data input field values.



*Note: For tests with 'Fail' results, reference **Section 2.0** (Testing Configuration for Edge System) and **Section 2.3** (Profile Creation) of this ETT User Guide 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 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**.

The screenshot shows a web-based log interface for an SMTP test. At the top, a blue header bar contains a back arrow and the text "Log SMTP Test 1-8, 14, 18". Below the header, a green banner displays "Test result #1: ✓ Pass". A table follows, with columns: Criteria Met, Request Time out, Proctored, and Time elapsed (seconds). All three rows under "Criteria Met" and "Request Time out" have red "X" marks, while "Proctored" has a red "X" and "Time elapsed (seconds)" shows "0". Below the table is a section titled "Request responses" containing a large block of raw text representing an email message header and body.

Criteria Met	Request Time out	Proctored	Time elapsed (seconds)
X	X	X	0

**Request responses**

```
Content-Type: multipart/alternative; boundary=089e01634b906425100514cb5ceb0K1
M-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=gmail.com; s=20120113;
h=mime-version:date:message-id:subject:from:to:content-type;
bh=w2eRWQF6ugsEB2yeh2H4vJ28T+pY3Z01Cak6PT1L1E=;
b=xmhpXXAebArLM84D0jjrjx4BNXl2elmTyLBCpxGOC06VR/m+KoumZvbhUlkEewp4
qCKFuITVQ5si+caJvxRP0n4TDPghnqht3f43E11K2zbhCjoA1/C2RwWMTlt9qtk0Bb
mfIKhNQlttyhny1esEzdyImfjzwB3h2cDMgvNhsH1270418LkvIycsg+dALF8CPbHO
OJWqEVSDQ304h5AKSh+xpZ58H1R1PjbowkIGYE3GMknB9jaJH08DC4P/g62vluoyA1
81qXvTSpM5oSFKU1KGNk3Xs13uraJ+TVWrsly6OfzzAGGU3JNlOpJyBBByssttgAKUT
aNNw=Date: Tue, 28 Apr 2015 12:29:08 -0400Delivered-To: ======From
m: test test <sut.example@gmail.com>IMIE-Version: 1.0Message-ID: <CAJ3juw-JWM_4
D-8g23wiVTEsVsya-jVAodgf_Q1vgPapivjSk=g@mail.gmail.com>Received: by 10.76.14
6.4 with HTTP; Tue, 28 Apr 2015 09:29:04 -0700 (PDT)Return-Path: <sut.example@gmail.com>Subject: testTo: wellformed1@edge.nist.govX-Received: by 10.182.13
1.130 with SMTP id om2mr15291721obb.70.1430238544535;
Tue, 28 Apr 2015 09:29:04 -0700 (PDT)
```

**Attachments:**

```
{"bodyPart [1]": "test\r\n", "bodyPart
[2]": "<div dir=\"ltr\">test</div>\r\n"}
```



**Note:** Within the Test Procedures, the '**Log**' directly references a single Test Case's generated test results (either '**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 Tester (i.e., Vendor) to view validation results by Profile configured and Test Case(s) executed.

### 7.1.2 SMTP TEST CASE 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 and PLAIN SASL protocols and commands needed to successfully authenticate and establish a secure connection with a HISp (i.e., ETT), acting as the receiver.

The testing details for conformance testing flow are as follows:

- The Tester (i.e., Vendor) navigates to the SMTP Test Case Profile and populates the Vendor SMTP Username and Vendor SMTP Password fields with the accurate information for the Vendor SMTP Email Address (all fields should correlate so the ETT and SUT and communicate to execute this Test Case; reference [2.3 Profile Creation](#)).
- 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@edge.nist.gov](mailto:wellformed1@edge.nist.gov). The SUT will attempt to initiate a secure connection with the ETT and perform PLAIN SASL authentication.
- The Vendor validates that the SUT successfully transmitted the message, executed the correct sequence of PLAIN SASL authentication mechanism protocols and commands to establish a secure connection with the ETT, , and conformed to the specified requirements within [RFC 4616](#).

This is a **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 1.2.4 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 18 of the SMTP Test Cases tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 3.03 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

#### 7.1.2.1 Testing Steps

To execute SMPT Test Case 18 and assess the SUT's ability to accurately create a conformant message and establish a secure connection with the ETT through PLAIN SASL authentication, the Tester (i.e., Vendor) must perform the following steps:



*Note: Within the ETT UI, SMTP Test Cases 1 through 8, 14, and 18 are condensed into a single executable test. Thus, the Testing Steps performed for these Test Cases are consistent across the set. Reference Section 3.1.1 for the Testing Steps needed to execute SMTP Test Case 18.*

#### 7.1.3 SMTP TEST CASES 1 THROUGH 8 (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:

- The Tester (i.e., 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@edge.nist.gov](mailto:wellformed1@edge.nist.gov). The SUT will attempt to initiate a secure connection with the ETT and execute the correct SMTP sequence of protocols defined by requirements (e.g., RFC).
- The Vendor validates that the SUT successfully transmitted the message, executed the correct sequence of SMTP protocols and commands to establish a secure connection with the ETT, and conformed to the specified requirements within [RFC 2821, Sections: 3.1, 3.3, 4.1.1.1 - 4.1.1.4, 2.3.5, 2.3.7, 2.3.9 - 2.3.10, and 4.5.3.1.](#)

This is a **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 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test IDs 1 through 8 of the SMTP Test Cases tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 3.05 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

The testing objective and conformance test detail for Test Cases 1 through 8 are represented within the following table.

<b>SMTP Test Case</b>	<b>Testing Objective / Conformance Test Detail</b>
1	<ul style="list-style-type: none"><li>- The SUT will attempt to initiate a secure connection with the ETT and execute the correct SMTP sequence.</li><li>- The ETT will receive the SMTP protocol command sequence, perform validation, and initiate a successful connection with the SUT.</li><li>- The sequence of mail transaction connection commands will conform to the specified requirements within <a href="#"><u>RFC 2821, Section 3.1 (Session Initiation) and 4.1.1.1 (Extended HELO or EHLO)</u></a>.</li></ul>
2	<ul style="list-style-type: none"><li>- The SUT will attempt to send a HELO / EHLO command sequence to the ETT.</li><li>- The ETT will receive the HELO / EHLO command sequence, perform validation, and initiate a successful connection with the SUT.</li><li>- The sequence of mail transaction connection commands will conform to the specified requirements within <a href="#"><u>RFC 2821, Section 4.1.1.1 (Extended HELO or EHLO)</u></a>.</li></ul>
3	<ul style="list-style-type: none"><li>- The SUT will attempt to send the MAIL FROM, RCPT TO, and DATA command sequences to the ETT.</li><li>- The ETT will receive the MAIL FROM, RCPT TO, and DATA command sequences, perform validation, and initiate a successful connection with the SUT.</li></ul>

	<ul style="list-style-type: none"><li>- The sequence of mail transaction connection commands will conform to the specified requirements within <a href="#"><u>RFC 2821, Section 3.1 (Session Initiation)</u></a>.</li></ul>
4	<ul style="list-style-type: none"><li>- The SUT will attempt to send the MAIL command sequence to the ETT.</li><li>- The ETT will receive the MAIL command sequence, perform validation, and initiate a successful connection with the SUT.</li><li>- The sequence of mail transaction connection commands will conform to the specified requirements within <a href="#"><u>RFC 2821, Section 4.1.1.2</u></a>.</li></ul>
5	<ul style="list-style-type: none"><li>- The SUT will attempt to send the RCPT TO command sequence to the ETT.</li><li>- The ETT will receive the RCPT TO command sequence, perform validation, and initiate a successful connection with the SUT.</li><li>- The sequence of mail transaction connection commands will conform to the specified requirements within <a href="#"><u>RFC 2821, Section 4.1.1.3</u></a>.</li></ul>
6	<ul style="list-style-type: none"><li>- The SUT will attempt to send the DATA command sequence to the ETT.</li><li>- The ETT will receive the DATA command sequence, perform validation, and initiate a successful connection with the SUT.</li><li>- The sequence of mail transaction connection commands will conform to the specified requirements within <a href="#"><u>RFC 2821, Section 2.3.7, 2.3.9, and 4.1.1.4</u></a>.</li></ul>
7	<ul style="list-style-type: none"><li>- The SUT will attempt to send the correctly formatted Domain Name command sequence to the ETT.</li><li>- The ETT will receive the correctly formatted Domain Name command sequence, perform validation, and initiate a successful connection with the SUT.</li><li>- The sequence of mail transaction connection commands will conform to the specified requirements within <a href="#"><u>RFC 2821, Section 2.3.5</u></a>.</li></ul>
8	<ul style="list-style-type: none"><li>- The SUT will attempt to send the correctly configured and formatted Mailbox and Address to the ETT.</li><li>- The ETT will receive the correctly configured and formatted Mailbox and Address, perform validation, and initiate a successful connection with the SUT.</li><li>- The sequence of mail transaction connection commands will conform to the specified requirements within <a href="#"><u>RFC 2821, Section 2.3.10 and 4.5.3.1</u></a>.</li></ul>

### 7.1.3.1 Testing Steps

To execute SMTP Test Cases 1 through 8 and assess the ability of the SUT to initiate and execute the correct sequence of SMTP protocols and commands needed to successfully establish a connection with the ETT, the Vendor must perform the following steps:



*Note: Within the ETT UI, SMTP Test Cases 1 through 8, 14, and 18 are condensed into a single executable test. Thus, the Testing Steps performed for these Test Cases are consistent across the set. Reference [Section 3.1.1](#) for the Testing Steps needed to execute SMTP Test Cases 1 through 8.*

#### 7.1.4 SMTP 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 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:

- 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 [2.3 Profile Creation](#)).
- The Vendor executes the test by clicking ‘Run’ in the ETT for the target Test Case. Once the ETT process the test, the Vendor is presented with a ‘Waiting Validation’ prompt.
- 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@hit-testing2.nist.gov](mailto:wellformed1@hit-testing2.nist.gov). 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).
- 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 and conformed to the specified requirements within [RFC 2821](#).

This is a **required 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 [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 5.07, TE170.314(b)(8) – 5.08, and TE170.314(b)(8) – 5.09 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

#### 7.1.4.1 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:



**Note:** Within the ETT UI, 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. Reference [Section 4.1.1](#) for the Testing Steps needed to execute SMTP Test Case 9.

#### 7.1.5 SMTP TEST CASE 16 (RECEIVER)

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 initiate a secure connection using the STARTTLS protocols and send the correct series of responses back.

The testing details for conformance testing flow are as follows:

- 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 [2.3 Profile Creation](#)).
- The Vendor executes the test by clicking '**Run**' in the ETT for the target Test Case. Once the ETT process the test, the Vendor is presented with a '**Waiting Validation**' prompt.
- 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@hit-testing2.nist.gov](mailto:wellformed1@hit-testing2.nist.gov). 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).
- 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 the STARTTLS protocols/commands, and testing and 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 16 of the SMTP Test Cases tab within the *DirectEdgeProtocols* spreadsheet and TE170.314(b)(8) – 5.01 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

### 7.1.5.1 Testing Steps

To execute SMTP Test Case 16 and assess the SUT's ability to accept a request from the ETT to initiate a secure session using the STARTTLS protocol/command, the Vendor must perform the following steps:

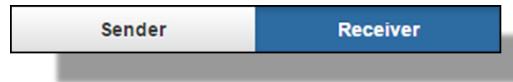


*Note: Within the ETT UI, SMTP Test Cases 9, 16, and 20 are condensed into a single executable test. Thus, the Testing Steps performed for these Test Cases are consistent across the set.*

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 7 within [2.2 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the Navigation Bar. This enables the testing Profile feature of the tool.

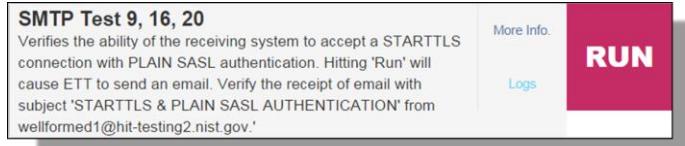


3. From the testing Profile, select **Receiver**.

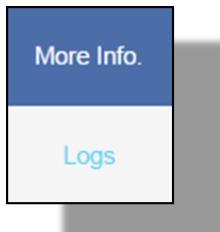


Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 Profile Creation](#).

4. To initiate SMTP Test Case 16 (in ETT UI as SMTP Test 9, 16, 20), the Vendor navigates to the Test Case's execution interface.



To gain additional information concerning SMTP Test 9, 16, 20's intended purpose (including Description, Vendor/SUT roles), click **More Info** link for the Test Case.



The screenshot shows the "SMTP Test 9, 16, 20" test case details. It includes a "Description" section with a detailed explanation of the test, a table showing vendor roles (Vendor Role, Vendor Edge, Vendor HISP) for the receiver, and a "Run" button at the bottom.

Vendor Role	Vendor Edge	Vendor HISP
receiver	✓	✓

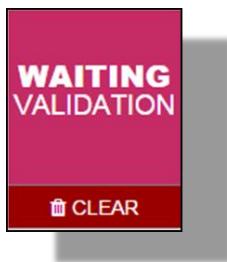
5. With the Profile saved, More Info reviewed, and **SMTP Test 9, 16, 20** selected, the Vendor performs the following Test Steps:
  - A. Select the sample attachment type (**CCDA**, **CCR**, or **C32**) to be sent with the message.



- B. Click **Run** to execute the test.



- C. 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** for the presence of a new received message.
    - i. The test message header/subject should read: **Testing STARTTLS & PLAIN SASL AUTHENTICATION (Test Case 9, 16, 20)**!
    - ii. The test message should have a sample file attachment named consistent to the sample chosen before test execution (e.g., **CCDA\_Ambulatory**). The attachment will be in XML format.
6. 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.



7. The Vendor performs manual validation by reviewing the **Log** data for SMTP Test 9, 16, 20. The Vendor must review the test results and confirm that the SUT successfully received a message transmission from the ETT that conforms to testing objectives and specifications.

Log SMTP Test 9, 16, 20

Test result #1:

Criteria Met	Request Time out	Proctored	Time elapsed (seconds)
✗	✗	✓	0

Request responses

```
1: SENDING STARTTLS & PLAIN SASL AUTHENTICATION EMAIL TO sut.example@gmail.com  
WITH ATTACHMENT CCDA_Ambulatory.xml  
2: Email sent Successfully
```

Attachments:

```
{}
```

8. If the Vendor accepts the SUT/ETT provided communication response(s) and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept** button is selected. However, if the Vendor does not accept the SUT/ETT provided communication response(s) after review of Log data/metadata, then the **Reject** button is selected. A selection must be made to complete the test.



9. The Vendor's selection per manual validation testing 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.





**Note:** Within the Test Procedures, the '**Log**' directly references a single Test Case's generated test results (either '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 Tester (i.e., Vendor) to view validation results by Profile configured and Test Case(s) executed.

### 7.1.6 SMTP TEST CASE 20 (RECEIVER)

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 initiate a secure connection and perform PLAIN SASL authentication.

The testing details for conformance testing flow are as follows:

- 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 [2.3 Profile Creation](#)).
- The Vendor executes the test by clicking '**Run**' in the ETT for the target Test Case. Once the ETT process the test, the Vendor is presented with a '**Waiting Validation**' prompt.
- 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@hit-testing2.nist.gov](mailto:wellformed1@hit-testing2.nist.gov). 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).
- 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 and accepted a PLAIN SASL authentication attempt, and testing and conformed to the specified requirements within [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 16 of the SMTP Test Cases tab within the [\*DirectEdgeProtocols\*](#) spreadsheet and TE170.314(b)(8) – 5.03 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

#### 7.1.6.1 Testing Steps

To execute SMTP Test Case 20 and assess the SUT's ability to accept a request from the ETT to initiate a secure session and authenticate using PLAIN SASL, the Vendor must perform the following steps:



*Note: Within the ETT UI, 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. Reference [Section 4.1.1](#) for the Testing Steps needed to execute SMTP Test Case 20.*

#### 7.1.7 SMTP TEST CASE 10 (RECEIVER)

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:

- 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 [2.3 Profile Creation](#)).
- 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 sending endpoint [wellformed3@hit-testing2.nist.gov](mailto:wellformed3@hit-testing2.nist.gov) is not present. The presence pf a new message indicates a test fail.
- 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 is a **required 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 *DirectEdgeProtocols* spreadsheet and TE170.314(b)(8) – 5.10 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

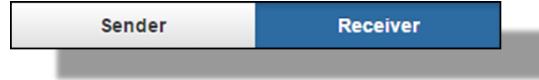
#### 7.1.7.1 Testing Steps

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 7 within [2.2 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the Navigation Bar. This enables the testing Profile feature of the tool.

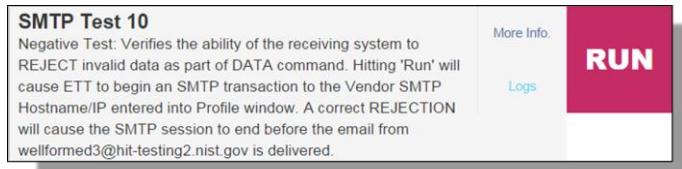


3. From the testing Profile, select **Receiver**.



Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 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, Vendor/SUT roles), click **More Info** link for the Test Case.

The screenshot shows the 'SMTP Test 10' configuration screen. At the top, there is a blue header bar with the text 'More Info.' and a 'Logs' button below it. Below the header, the title 'SMTP Test 10' is displayed with a back arrow icon. The main content area has a section titled 'Description:' which contains detailed text about the test objective and flow. Below the description is a table with three columns: 'Vendor Role', 'Vendor Edge', and 'Vendor HISp'. The table shows one row where 'receiver' is listed under 'Vendor Role', with a green checkmark under 'Vendor Edge' and another under 'Vendor HISp'. At the bottom right of the configuration area is a blue 'Run' button.

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@hit-testing.nist.gov](mailto:wellformed3@hit-testing.nist.gov) (this is a negative test).



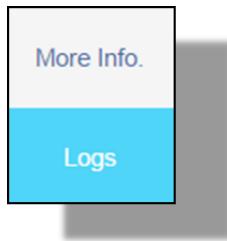
*Note: The Vendor, in execution of SMTP Test Case 10, should **not** receive a message in the 'Vendor SMTP Email Address' from the ETT. This is a negative test attempting to assess the capability of the SUT to reject a connection attempt that uses an invalid DATA command. Thus, the SUT should reject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



*Note: For tests with 'Fail' results, reference **Section 2.0** (Testing Configuration for Edge System) and **Section 2.3** (Profile Creation) of this ETT User Guide 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 10, 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**.

The screenshot shows a test result for "Log SMTP Test 10". At the top, there is a navigation bar with a back arrow and the title "Log SMTP Test 10". Below the title, it says "Test result #1: ✓ Pass".

Criteria Met	Request Time out	Proctored	Time elapsed (seconds)
✗	✗	✗	30

Under "Request responses", there is a text box containing the following SMTP session log:

```
DATA This is sample DATA.: -02 Custom Message: Socket Timeout occurredEHLO tt
t.nist.gov
: 250-mx.google.com at your service, [129.6.24.35]
250-SIZE 35882577
250-8BITMIME
250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN XOAUTH
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250-SMTPUTF8
MAIL FROM:<daemon@ttt.nist.gov>
: 250 2.1.0 OK n62sm6128087qge.27 - gsmtp
RCPT TO:<daemon@ttt.nist.gov>
: 250 2.1.5 OK n62sm6128087qge.27 - gsmtp
```

At the bottom, there is a section for "Attachments:" with a placeholder box containing "{}".



**Note:** Within the Test Procedures, the '**Log**' directly references a single Test Case's generated test results (either '**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 Tester (i.e., Vendor) to view validation results by Profile configured and Test Case(s) executed.

### 7.1.8 SMTP TEST CASE 11 (RECEIVER)

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:

- 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 [2.3 Profile Creation](#)).
- 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.
- 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](#).

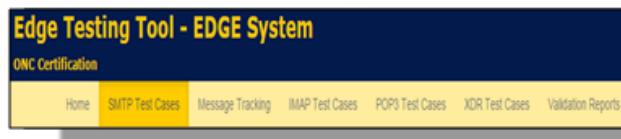
This is a **required test** and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.2.1 and 1.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 11 of the SMTP Test Cases tab within the [DirectEdgeProtocols](#) spreadsheet TE170.314(b)(8) – 5.11 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

### 7.1.8.1 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 7 within [2.2 Registration](#).
2. For this target SMTP MU2 test, select **SMTP Test Cases** from the Navigation Bar. This enables the testing Profile feature of the tool.

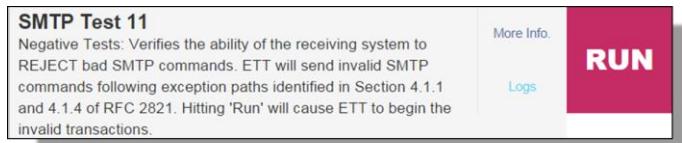


3. From the testing Profile, select **Receiver**.

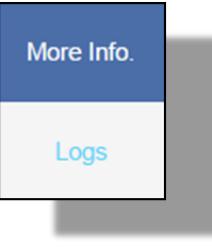


Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 Profile Creation](#).

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, Vendor/SUT roles), click **More Info** link for the Test Case.



The screenshot shows a modal window titled "SMTP Test 11". At the top left is a back arrow icon. The main area contains a "Description" section with detailed text about the test sequence. Below it is a table with three columns: "Vendor Role", "Vendor Edge", and "Vendor HISP". A single row shows "receiver" in the first column, with checkmarks in both the second and third columns. At the bottom right of the modal is a blue "Run" button.

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).



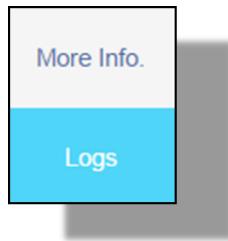
*Note: The Vendor, in execution of SMTP Test Case 11, should **not** receive a message in the 'Vendor SMTP Email Address' from the ETT. This is a negative test attempting to assess the capability of the SUT to reject a connection attempt that uses invalid SMTP commands. Thus, the SUT should terminate 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.



*Note: For tests with 'Fail' results, reference **Section 2.0** (Testing Configuration for Edge System) and **Section 2.3** (Profile Creation) of this ETT User Guide 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 11, 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**.

Log SMTP Test 11

Test result #1: ✓ Pass

Criteria Met	Request Time out	Proctored	Time elapsed (seconds)
x	x	x	0

Request responses

```
EHLO ttt.nist.gov
: 250-mx.google.com at your service, [129.6.24.35]
250-SIZE 35882577
250-8BITMIME
250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN XOAUTH
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250-SMTPUTF8
RCPT TO:<daemon@ttt.nist.gov>
: 503 5.5.1 MAIL first. 139sm13505969qhb.26 - gsmtp
```

Attachments:

{}

Test result #2: ✓ Pass

Criteria Met	Request Time out	Proctored	Time elapsed (seconds)
x	x	x	0

Request responses

```
DATA
Message: DATA before MAIL
-
: 451 4.5.0 SMTP protocol violation, see RFC 2821 104sm13623930qgj.43 - gsmtp
EHLO ttt.nist.gov
: 250-mx.google.com at your service, [129.6.24.35]
250-SIZE 35882577
250-8BITMIME
250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN XOAUTH
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250-SMTPUTF8
```

Attachments:

{}



**Note:** Within the Test Procedures, the 'Log' directly references a single Test Case's generated test results (either '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 Tester (i.e., Vendor) to view validation results by Profile configured and Test Case(s) executed.

### 7.1.9 SMTP TEST CASE 13 (RECEIVER)

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:

- 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 [2.3 Profile Creation](#)).
- The Vendor will identify the constrainable target timeout duration (represented in seconds) the SUT will be tested against.
- Upon test execution, the Vendor performing this Test Case will wait for the timeout value entered to expire.
- 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 is a **required 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 13 of the SMTP Test Cases tab within the [DirectEdgeProtocols](#) spreadsheet TE170.314(b)(8) – 5.13 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

### 7.1.9.1 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 7 within [2.2 Registration](#).
2. For this target SMTP MU2 test, select **SMTP Test Cases** from the Navigation Bar. This enables the testing Profile feature of the tool.

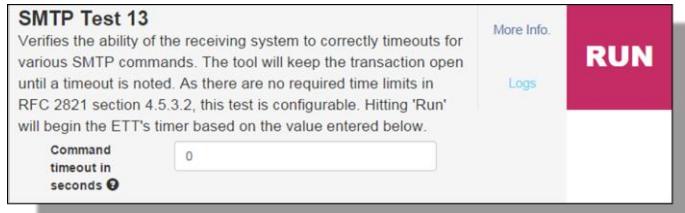


3. From the testing Profile, select **Receiver**.

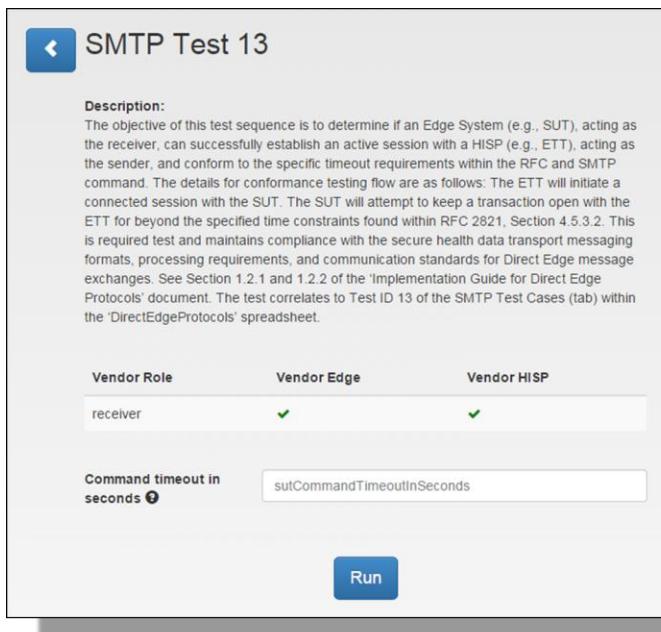


Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 Profile Creation](#).

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



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



5. With the Profile saved, More Info reviewed, and **SMTP Test 13** selected, the Vendor performs the following Test Steps:

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





**Note:** The Vendor, in execution of SMTP Test Case 13, must enter the timeout threshold value specific to 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:

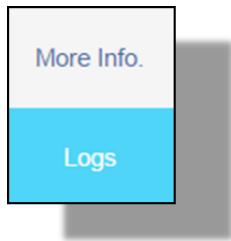
- Initial 220 Message: 5 minutes (300 seconds);
- MAIL Command: 5 minutes (300 seconds);
- RCPT Command: 5 minutes (300 seconds);
- DATA Initiation: 2 minutes (120 seconds);
- DATA Block: 3 minutes (180 seconds);
- DATA Termination: 10 minutes (600 seconds); and
- Waiting for next command from sender: 5 minutes (300 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.



**Note:** For tests with '**Fail**' results, reference **Section 2.0** (Testing Configuration for Edge System) and **Section 2.3** (Profile Creation) of this ETT User Guide 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 13, 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**.

Log SMTP Test 13

Test result #1: ✓ Pass

Criteria Met	Request Time out	Proctored	Time elapsed (seconds)
✗	✗	✗	15

Request responses

```
: -02 Custom Message: Socket Timeout occurredEHLO ttt.nist.gov
: 354 Go ahead f4sm1648122qhe.9 - gsmtp
EHLO ttt.nist.gov
: 250 2.5.0 google.com at your service, [129.6.24.35]
250-SIZE 35882577
250-8BITTIME
250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN XOAUTH
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250-SMTPUTF8
MAIL FROM:<daemon@ttt.nist.gov>
: 250 2.1.0 OK f4sm1648122qhe.9 - gsmtp
RCPT TO:<daemon@ttt.nist.gov>
: 250 2.1.5 OK f4sm1648122qhe.9 - gsmtp
```

Attachments:

{}  
Test result #2: ✓ Pass

Criteria Met	Request Time out	Proctored	Time elapsed (seconds)
✗	✗	✗	15

Request responses

```
: -02 Custom Message: Socket Timeout occurredEHLO ttt.nist.gov
: 354 Go ahead f4sm13458875qr.41 - gsmtp
EHLO ttt.nist.gov
: 250 2.5.0 google.com at your service, [129.6.24.35]
250-SIZE 35882577
250-8BITTIME
250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN XOAUTH
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250-SMTPUTF8
MAIL FROM:<daemon@ttt.nist.gov>
: 250 2.1.0 OK f4sm13458875qr.41 - gsmtp
RCPT TO:<daemon@ttt.nist.gov>
: 250 2.1.5 OK f4sm13458875qr.41 - gsmtp
```

Attachments:

{}  
{}  
{}}



*Note: Within the Test Procedures, the 'Log' directly references a single Test Case's generated test results (either '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 Tester (i.e., Vendor) to view validation results by Profile configured and Test Case(s) executed.*

## 7.2 XDR 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

### 7.2.1 SMTP TEST CASE 17 (RECEIVER)

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:

- 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 [2.3 Profile Creation](#)).
- 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.
- 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 [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 5.02 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

### 7.2.1.1 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 7 within [2.2 Registration](#).
2. For this target SMTP test, select '**SMTP Test Cases**' from the Navigation Bar. This enables the testing Profile feature of the tool.

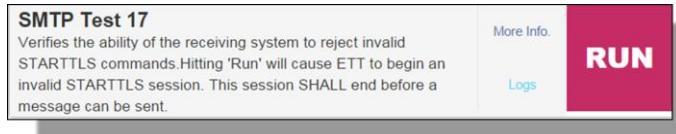


3. From the testing Profile, select **Receiver**.

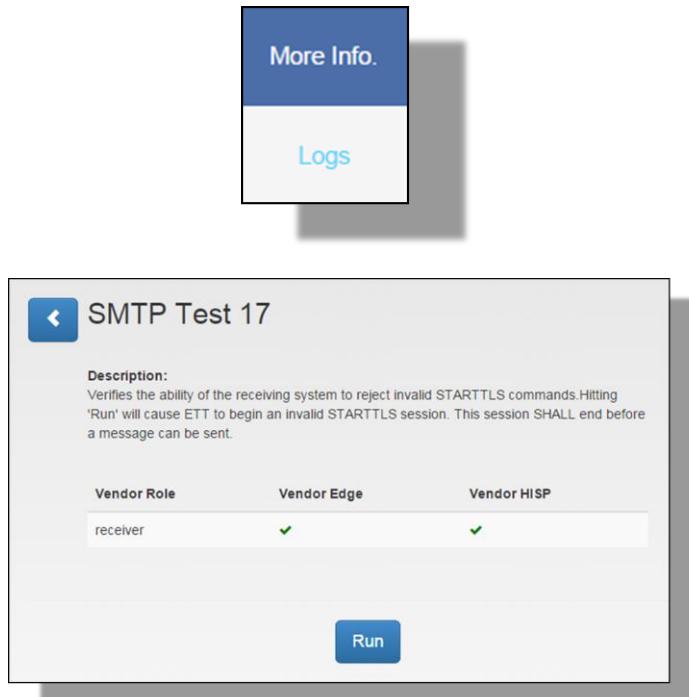


Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 Profile Creation](#).

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 **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.



- 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).



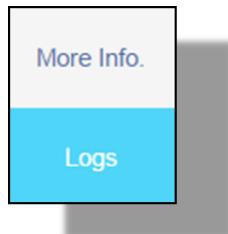
**Note:** The Vendor, in execution of SMTP Test Case 17, should **not** receive a message in the ‘Vendor SMTP Email Address’ from the ETT. This is a negative test attempting to assess the capability of the SUT to reject a connection attempt that uses an invalid STARTTLS command. Thus, the SUT should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

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.



**Note:** For tests with ‘Fail’ results, reference **Section 2.0 (Testing Configuration for Edge System)** and **Section 2.3 (Profile Creation)** of this ETT User Guide 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 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**.

The screenshot shows a test log titled "Log SMTP Test 17". The main header says "Test result #1: Pass". Below it is a table with four columns: "Criteria Met", "Request Time out", "Proctored", and "Time elapsed (seconds)". All three columns have an "X" in them, and the time elapsed is 0 seconds. Under "Request responses", there is a text box containing the following log entries:  
HELO testing.com  
: 250 mx.google.com at your service  
STARTTLS abcd  
: 555 5.5.2 Syntax error. g184sm13526427qhc.6 - gsmtp



*Note: Within the Test Procedures, the 'Log' directly references a single Test Case's generated test results (either '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 Tester (i.e., Vendor) to view validation results by Profile configured and Test Case(s) executed.*

### 7.2.2 SMTP TEST CASE 22 (RECEIVER)

The objective of this **negative test** sequence is to determine if an Edge System (i.e., SUT), acting as the receiver, can reject an authentication attempt from a HISIP (i.e., ETT), acting as the sender, using invalid PLAIN SASL credentials (username/password).

The testing details for conformance testing flow are as follows:

- 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 [2.3 Profile Creation](#)).

- 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.
- 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 [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 5.05 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

#### 7.2.2.1 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 7 within [2.2 Registration](#).
2. For this target SMTP test, select **SMTP Test Cases** from the Navigation Bar. This enables the testing Profile feature of the tool.

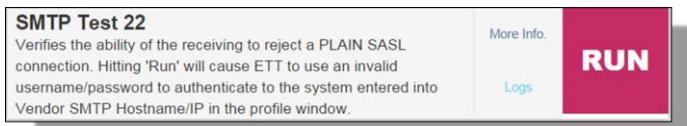


3. From the testing Profile, select **Receiver**.

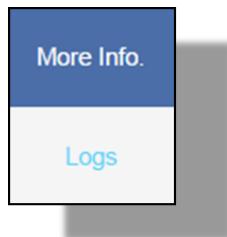


Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 Profile Creation](#).

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



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



This screenshot shows the detailed description page for "SMTP Test 22". At the top left is a back arrow icon. The title "SMTP Test 22" is centered above a table. The table has three columns: "Vendor Role", "Vendor Edge", and "Vendor HISp". Under the "Vendor Role" column, there is one row labeled "receiver" with a green checkmark under both "Vendor Edge" and "Vendor HISp". At the bottom of the page is a blue "Run" button.

Vendor Role	Vendor Edge	Vendor HISp
receiver	✓	✓

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**.

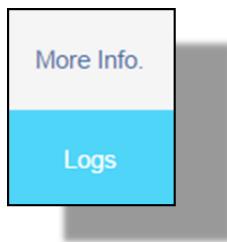
- A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
- A test Fail prompts the Vendor to **Retry** the test.
- The **Clear** button resets the test and any data input field values.





**Note:** For tests with 'Fail' results, reference **Section 2.0 (Testing Configuration for Edge System)** and **Section 2.3 (Profile Creation)** of this ETT User Guide 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 22, 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**.

The screenshot shows a web-based log viewer for SMTP Test 22. At the top, it displays "Test result #1: ✓ Pass". Below this, there is a table with four columns: "Criteria Met", "Request Time out", "Proctored", and "Time elapsed (seconds)". The first two columns have red "X" marks, while the third has a green checkmark and the fourth shows "0". Under the "Request responses" section, a message box contains the text: "SUCCESS: Vendor rejects bad Username/Password combination :535-5.7.8 Username and Password not accepted. Learn more at 535 5.7.8 http://support.google.com/mail/bin/answer.py?answer=14257 j40sm13455 689qkh.46 - gsmtp". The "Attachments:" section shows an empty box with a "(0)" label.



**Note:** Within the Test Procedures, the '**Log**' directly references a single Test Case's generated test results (either '**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 Tester (i.e., Vendor) to view validation results by Profile configured and Test Case(s) executed.

## 7.3 MESSAGE TRACKING

### 7.3.1 SMTP MESSAGE TRACKING (MT) 17 (SENDER)

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:

- 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.
- 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@hit-testing2.nist.gov](mailto:wellformed14@hit-testing2.nist.gov). 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.
- 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.

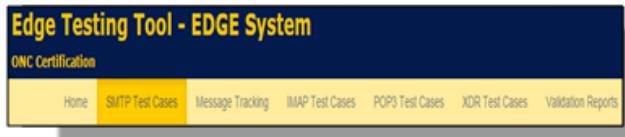
This is a **required test** and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.5.1.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 17 of the MU Tracking tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 3.08 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

### 7.3.1.1 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 7 within [2.2 Registration](#).
2. For this target SMTP MU2 test, select **SMTP Test Cases** from the Navigation Bar. This enables the testing Profile feature of the tool.

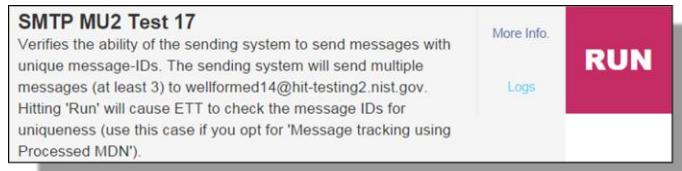


3. From the testing Profile, select **Sender**.

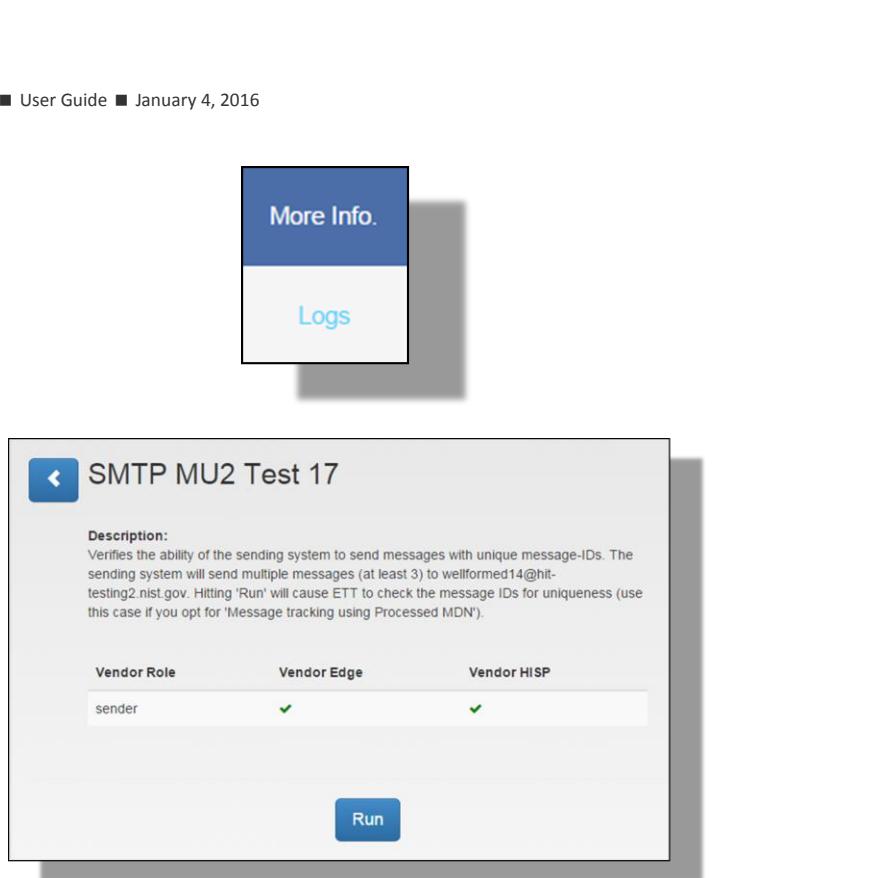


Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 Profile Creation](#).

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, Vendor/SUT roles), click **More Info** link for the Test Case.

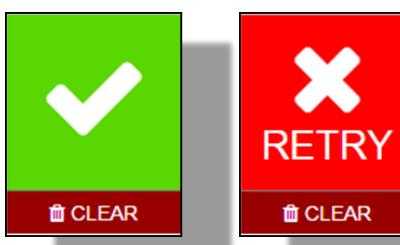


5. With the Profile saved, More Info reviewed, and **SMTP MU2 Test 17** selected, the Vendor performs the following Test Steps:
  - A. Navigate the to SUT's messaging client/interface for **Vendor SMTP Email Address** (specified in the Profile).
  - B. Create three (3) new messages:
    - a. Each message 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@hit-testing2.nist.gov](mailto:wellformed14@hit-testing2.nist.gov).
  - C. Navigate to the ETT and SMTP MU2 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.



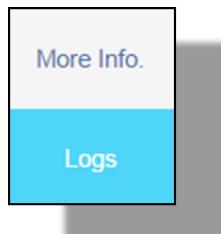
Comment [a1]: Delete?

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.



*Note: For tests with 'Fail' results, reference **Section 2.0** (Testing Configuration for Edge System) and **Section 2.3** (Profile Creation) of this ETT User Guide 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 MU2 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**.

The screenshot shows a web-based log interface for a test case. At the top, it says "Log SMTP MU2 Test 17". Below that, it displays "Test result #1: ✓ Pass". A table row below shows the status for four criteria: "Criteria Met" (X), "Request Time out" (X), "Proctored" (X), and "Time elapsed (seconds)" (0). Under "Request responses", there is a box containing three message IDs: Message-ID 1, 2, and 3. Under "Attachments:", there is a box with a single brace icon {}.



*Note: Within the Test Procedures, the 'Log' directly references a single Test Case's generated test results (either '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 Tester (i.e., Vendor) to view validation results by Profile configured and Test Case(s) executed.*

### 7.3.2 SMTP MESSAGE TRACKING (MT) 45 (SENDER)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the 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:

- 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.

- 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@hit-testing2.nist.gov](mailto:wellformed14@hit-testing2.nist.gov). 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.
- 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 is a **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 1.5.1.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

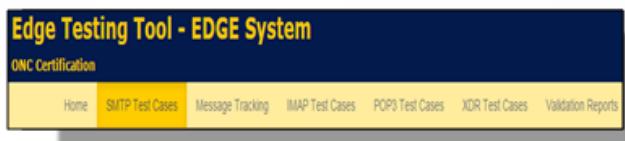
This test correlates to Test ID 45 of the MU Tracking tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 3.09 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

**Comment [a2]:** Need link

### 7.3.2.1 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 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 7 within [2.2 Registration](#).
2. For this target SMTP MU2 test, select **SMTP Test Cases** from the Navigation Bar. This enables the testing Profile feature of the tool.

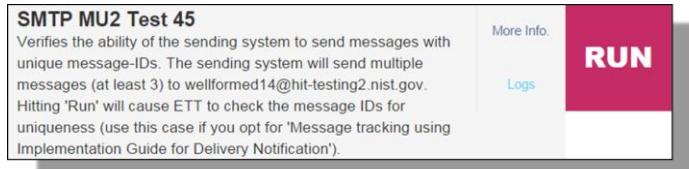


3. From the testing Profile, select **Sender**.

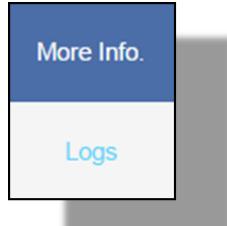


Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 Profile Creation](#).

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



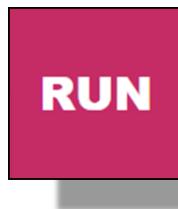
To gain additional information concerning SMTP Message Tracking (MT) 45's intended purpose (including Description, Vendor/SUT roles), click **More Info** link for the Test Case.





5. With the Profile saved, More Info reviewed, and 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@hit-testing2.nist.gov](mailto:wellformed14@hit-testing2.nist.gov).
- C. Navigate to the ETT and SMTP MU2 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.



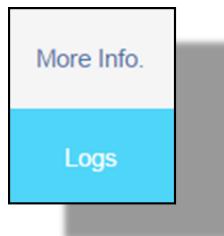
*Note: SMTP MU2 Test 45 should be executed under the constraint that a Vendor/SUT opts for message tracking using Implementation Guide for Delivery Notifications specific requirements.*

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.



*Note: For tests with 'Fail' results, reference **Section 2.0 (Testing Configuration for Edge System)** and **Section 2.3 (Profile Creation)** of this ETT User Guide 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 MU2 Test 45, 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**.

The screenshot shows a test log for 'Log SMTP MU2 Test 45'. The top bar has a back arrow and the title. Below it, a section titled 'Test result #1: ✓ Pass' is shown. A table below lists four criteria: 'Criteria Met' (all crossed out), 'Request Time out' (all crossed out), 'Proctored' (all crossed out), and 'Time elapsed (seconds)' (value 0). Under 'Request responses', there is a box containing three message IDs: Message-ID 1, 2, and 3, each with a unique identifier. There is also a section for 'Attachments' which is currently empty.



*Note:* Within the Test Procedures, the 'Log' directly references a single Test Case's generated test results (either '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 Tester (i.e., Vendor) to view validation results by Profile configured and Test Case(s) executed.

### 7.3.3 SMTP MESSAGE TRACKING (MT) 46 (SENDER)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the sender, can successfully generate and transmit a series of email messages with unique header information to a HISp (i.e., ETT), acting as the receiver.

The testing details for conformance testing flow are as follows:

- The Tester (i.e., 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 Disposition-Notification-Option header with no duplicates. This allows the ETT to correlate the processed MDN with the Message Tracking (MT) message (the Vendor must be able to manipulate the message ID and to accurately

execute this Test Case). The SUT will send the 3 messages (in a series) to the target ETT endpoint recipient: [wellformed14@hit-testing2.nist.gov](mailto:wellformed14@hit-testing2.nist.gov). Upon the sending of each message, the SUT will generate and send a Message Tracking (MT) message (containing the Disposition-Notification-Option header and processed MDN notification) to the ETT. The ETT will receive the 3 messages and Message Tracking (MT) message (Message Tracking (MT) message (containing the Disposition-Notification-Option header and processed MDN notification), and respond to the SUT and validate that each message ID and Disposition-Notification-Option header is indeed unique.

- 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 and Disposition-Notification-Option headers, the SUT successfully transmitted a process MDN notification for each of the 3 messages, and the specified requirements within [RFC 5322, Sections 2.1 and 2.2](#), [RFC 3501](#), [RFC 4616](#), and [RFC 2831](#) were conformed to.

This is a **required test** and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.3 and 1.5.1.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 46 of the MU Tracking tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 3.10 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

#### 7.3.3.1 Testing Steps

To execute SMTP Message Tracking (MT) 46 and assess the SUT's ability to successfully generate and transmit a series of email messages containing unique message IDs and Disposition-Notification-Option headers and send standard conformant 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 7 within [2.2 Registration](#).
2. For this target SMTP MU2 test, select **SMTP Test Cases** from the Navigation Bar. This enables the testing Profile feature of the tool.

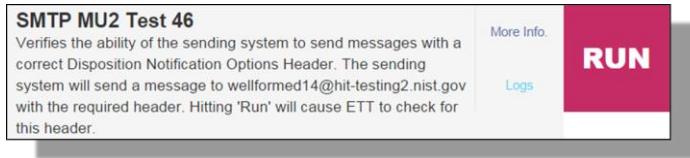


3. From the testing Profile, select **Sender**.

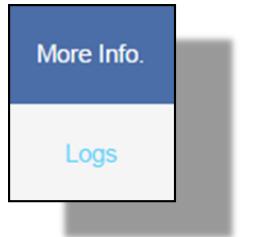


Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 Profile Creation](#).

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, Vendor/SUT roles), click **More Info** link for the Test Case.



5. With the Profile saved, More Info reviewed, and **SMTP MU2 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 three (3) new messages.
    - a. Each message must contain a unique message ID and Disposition-Notification-Option header (no duplicates for either).
    - b. The 3 messages must be transmitted in a series.
    - c. The messages must be sent to the ETT endpoint recipient [wellformed14@hit-testing2.nist.gov](mailto:wellformed14@hit-testing2.nist.gov).
  - C. Navigate to the ETT and SMTP MU2 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.

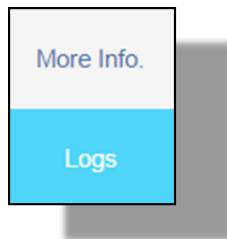


6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
  - A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
  - A test Fail prompts the Vendor to **Retry** the test.
  - The **Clear** button resets the test and any data input field values.

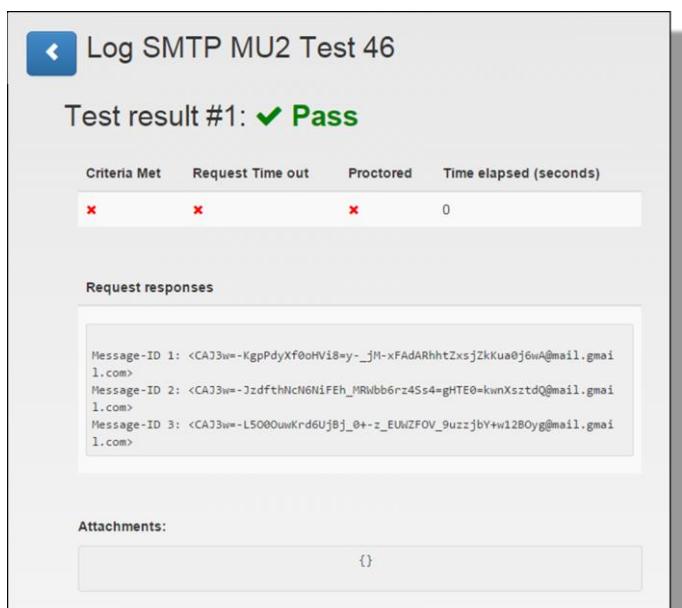


*Note: For tests with 'Fail' results, reference **Section 2.0 (Testing Configuration for Edge System)** and **Section 2.3 (Profile Creation)** of this ETT User Guide to assure that the accurate configurations have been implemented.*

7. To validate that the test results conformed to the testing objective(s) and gain additional information concerning the results or outcome of SMTP MU2 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**.



Criteria Met	Request Time out	Proctored	Time elapsed (seconds)
X	X	X	0
X	X	X	0
X	X	X	0

Request responses

```
Message-ID 1: <CAJ3w=-KgpPdyXf0oHVi8=y-_jM-xFAdARhhtZxsjZkKua0j6wA@mail.gmail.com>
Message-ID 2: <CAJ3w=-JzdfthNcN6NiFEh_MRvb6r4Ss4=gHTE0=kwnXsztDQ@mail.gmail.com>
Message-ID 3: <CAJ3w=L5000UuvKrd6UjBj_0+-z_EUwZFOV_9uzzjbY+w12B0yg@mail.gmail.com>
```

Attachments:



**Note:** Within the Test Procedures, the '**Log**' directly references a single Test Case's generated test results (either '**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 Tester (i.e., Vendor) to view validation results by Profile configured and Test Case(s) executed.

#### 7.3.4 SMTP MESSAGE TRACKING (MT) 47 (SENDER)

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the sender, can accept an invalid recipient notification from an email message sent to a HISp (i.e., ETT), acting as the receiver.

The testing details for conformance testing flow are as follows:

- The Tester (i.e., Vendor) performing this Test Case and in operation of the SUT will navigate to their SMTP email client and create a single new message. The Vendor will add multiple valid and at least one invalid recipient to the message. The available **valid** target ETT endpoint recipients are: [wellformed1@edge.nist.gov](mailto:wellformed1@edge.nist.gov) and [wellformed14@hit-testing2.nist.gov](mailto:wellformed14@hit-testing2.nist.gov). The available **invalid** target ETT endpoint recipient is: [noaddress@hit-testing2.nist.gov](mailto:noaddress@hit-testing2.nist.gov). The message must be accurately formed and in the correct syntax. The SUT will send the message to the target ETT endpoint recipients. The SUT will receive an invalid message recipient response message to the SMTP email client and the Vendor must manually validate the test results.
- The Vendor validates that the SUT successfully transmitted the message, multiple valid and at least one invalid recipient was added to the message, the invalid message response message was received in the SMTP email client for the SUT, and the specified requirements within [RFC 5322](#) were conformed to.

This is a **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 1.5.1.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 47 of the MU Tracking tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 3.11 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

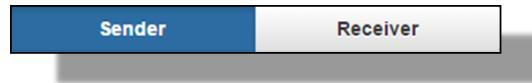
### 7.3.4.1 Testing Steps

To execute SMTP Message Tracking (MT) 47 and assess the SUT's ability to successfully accept a notification from an email message sent to an invalid recipient, 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 7 within [2.2 Registration](#).
2. For this target SMTP MU2 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**.

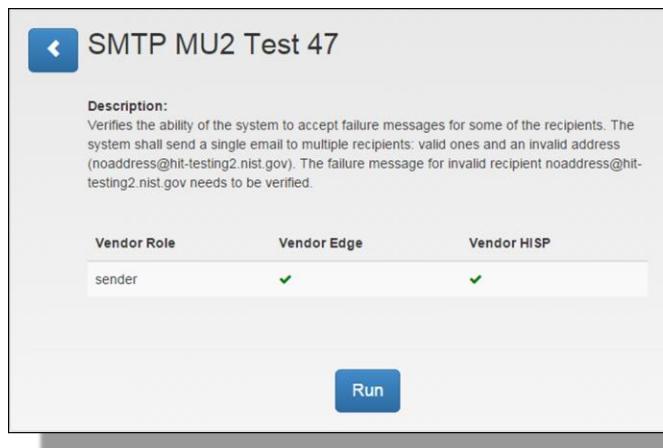


Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 Profile Creation](#).

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



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



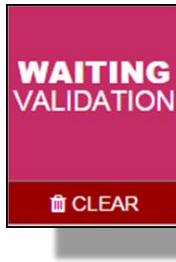
5. With the Profile saved, More Info reviewed, and **SMTP MU2 Test 47** selected, the Vendor performs the following Test Steps:

- A. Navigate the to SUT's messaging client/interface for **Vendor SMTP Email Address** (specified in the Profile).
- B. Create a single new message.
  - a. Send the message to both valid and invalid recipients (Vendor specified; other than those provided by the ETT).
    - i. At least one message recipient must be the invalid ETT endpoint [noaddress@hit-testing2.nist.gov](mailto:noaddress@hit-testing2.nist.gov).
- C. Navigate to the ETT and SMTP MU2 Test 47 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.



*Note: The Vendor, in execution of SMTP MU2 Test 47, should receive a message delivery error notification to the 'Vendor SMTP Email Address' when attempting to transmit the invalid ETT endpoint recipient [noaddress@hit-testing2.nist.gov](mailto:noaddress@hit-testing2.nist.gov).*

6. The ETT checks the specified endpoints for the presence of newly received 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



7. The Vendor performs manual validation by reviewing the **Log** data for SMTP MU2 Test 47.

The screenshot shows a web-based interface for a log review. At the top, a blue header bar contains a back arrow and the text "Log SMTP MU2 Test 47". Below the header, the title "Test result #1:" is displayed. A table with four columns is shown, with all entries marked with a red "X": "Criteria Met", "Request Time out", "Proctored", and "Time elapsed (seconds)". Under the "Request responses" section, a message states: "Awaiting confirmation from proctor: Proctor needs to verify the failure message from invalid recipient." The "Attachments:" section is empty, showing a placeholder icon.

During Log review and manual validation, the Vendor must attest that the SUT successfully received a message transmission failure notification from the invalid ETT endpoint recipient [noaddress@hit-testing2.nist.gov](mailto:noaddress@hit-testing2.nist.gov).

8. If the Vendor accepts the SUT/ETT provided communication response(s) and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept** button is selected. However, if the Vendor does not accept the SUT/ETT provided communication response(s) after review of Log data/metadata, then the **Reject** button is selected. A selection must be made to complete the test.



9. The Vendor's selection per manual validation testing 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.



*Note: Within the Test Procedures, the 'Log' directly references a single Test Case's generated test results (either '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 Tester (i.e., Vendor) to view validation results by Profile configured and Test Case(s) executed.*

## 7.4 SUT Receiving

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

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

## 7.5 XDR Test Cases

### 7.5.1 XDR TEST CASE 6

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:

- The Tester (i.e., 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.

- 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 [2.3 Profile Creation](#)).
- 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).
- The Vendor executes the second Test Step by sending the ETT generated TLS / Non-TLS endpoint a message from the SUT.
- 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](#).

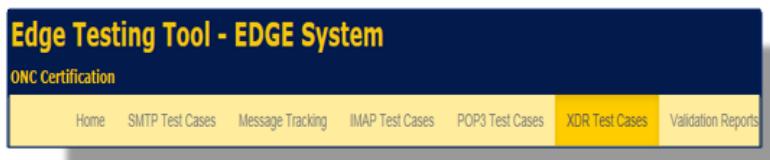
This is a **required test** and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 7 of the XDR Test Cases tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 2.01 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

#### 7.5.1.1 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 7 within [2.2 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.

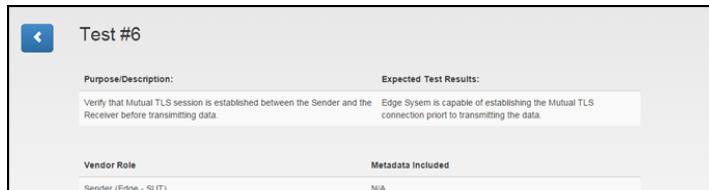
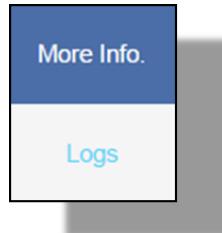


3. From the testing options available, select **Your System as: Sender**. This will enable Test Case selection.

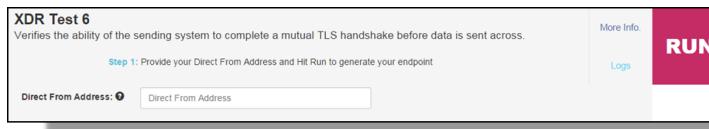


*Note: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

4. To gain additional information concerning XDR MU2 Test 6's intended focus, purpose/descriptions, conditional requirements, and expected test results, Vendor role, and Metadata inclusion, click the **More Information** link for the Test Case.



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.

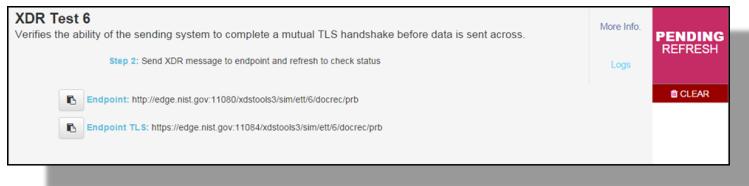


- Once the SUT's Direct From Address has been populated in the Test Case, clicking **Run** initiates the first testing step.



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the **TLS Endpoint** is provided by the Tester (e.g., Vendor).*

- 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.



- 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.



- 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 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:

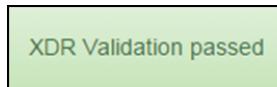
- a. Accurately established a connection with the ETT;
- b. Formed/transmitted the XDR message correctly; and
- c. Competed a mutual TLS handshake with the ETT before transmitting data.

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.



**Note:** ‘Accept XDR’ selections correlate with Test Case Success results (e.g., green check mark). Likewise, ‘Reject XDR’ selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a ‘Reject XDR’ selection correlate with a Test Success).

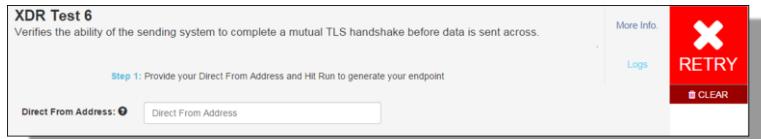
13. The ETT presents Vendor conformation based upon the selection made.





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 (reference Step 1 within [Section 5.1.1](#) to perform further retesting). 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: In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The '**Validation Report**' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., 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 (reference [Section 2.4 Reporting](#)).



### 7.5.2 XDR TEST CASE 7

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:

- The Tester (i.e., 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.
- 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 communicate to execute this Test Case; reference [2.3 Profile Creation](#)).
- 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).
- The Vendor executes the second Test Step by sending the ETT generated endpoint a message from the SUT.
- The Vendor validates through '**Log**' review that the SUT attempted to establish 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 is a **required test** and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.

**Comment [a3]:** Need link

This test correlates to Test ID 7 of the XDR Test Cases tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 2.02 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

#### 7.5.2.1 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 7 within [2.2 Registration](#).

2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.



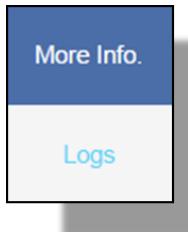
3. From the testing options available, select **Your System as: Sender**. This will enable test case selection.

Your System as: Sender



*Note: 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, conditional requirements, and expected test results, Vendor role, and Metadata inclusion, click the **More Information** link for the Test Case.



A screenshot of a "Test #7" details page. It includes sections for Purpose/Description, Expected Test Results, Vendor Role, and Metadata Included.

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.

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

IP Address:  IP Address

More Info. | Logos | RUN

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



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the 'TLS Endpoint' is provided by the Tester (e.g., Vendor).*

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.

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.

Step 2: Send XDR message to endpoint and refresh to check status

Endpoint: edge.nist.gov:12084

More Info. | Logos | PENDING REFRESH | CLEAR

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.



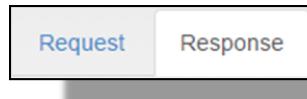
9. The ETT checks the generated endpoints for the presence of newly received XDR messages. The Vendor is prompted to manually validate if the test results conformed to the testing objectives. To complete this, the Vendor clicks the **Waiting Validation** button.



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 establish 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.

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=IDEBoundary112233445566778899; type="application/xop+xml"; start=<doc@ihexds.nist.gov>; start-info="application/soap+xml"
Content-Transfer-Encoding: chunked
Date: Tue, 13 Jan 2015 16:41:20 GMT

--IDEBoundary112233445566778899
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <doc@ihexds.nist.gov>

<?xml version="1.0" encoding="UTF-8"?>
<Envelope xmlns="http://www.w3.org/2003/05/soap-envelope">
  <Header>
    <Action s:mustUnderstand="1" xmlns:s="http://www.w3.org/2003/05/soap-envelope">
      http://www.w3.org/2005/08/addressing/urn:he:iti:2007:Pro104AndRegisterDocumentSet-&Response</Action>
    <RelatesTo xmlns:wsa="http://www.w3.org/2005/08/addressing">15ddcb7-4287-45f7-99c7-67fb78f4372</RelatesTo>
  </Header>
  <Body>
    <registryResponse status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
      <xmldrs:urn:oasis:names:tc:ebxml-regrep:xsd:3.0/>
    </Body>
  </Envelope>
--IDEBBoundary112233445566778899--
```

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.



*Note: 'Accept XDR' selections correlate with Test Case Success results (e.g., green check mark). Likewise, 'Reject XDR' selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a 'Reject XDR' selection correlate with a Test Success).*

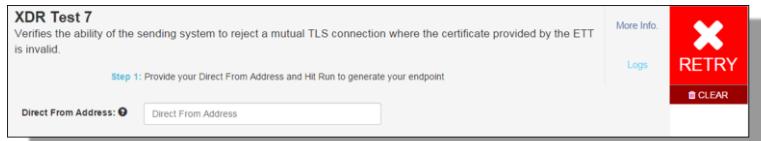
13. The ETT presents Vendor conformation based upon the selection made.

XDR Validation passed



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 (reference Step 1 within [Section 5.2.1](#) to perform further retesting). The Vendor can select the **Clear** button to reset the test.

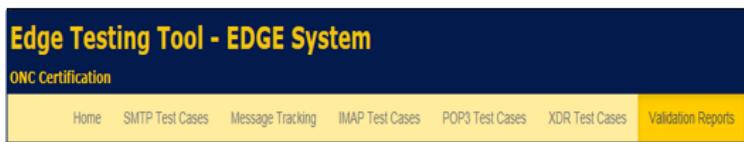


XDR message acceptance results in a green check. The Vendor can select the **Clear** button to reset the test.



*Note: In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The '**Validation Report**' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., 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 (reference [Section 2.4 Reporting](#)).



### 7.5.3 XDR TEST CASE 1

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:

- The Tester (i.e., 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.
- 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 [2.3 Profile Creation](#)).
- 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).
- 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.
- 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 is a **required test** and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.

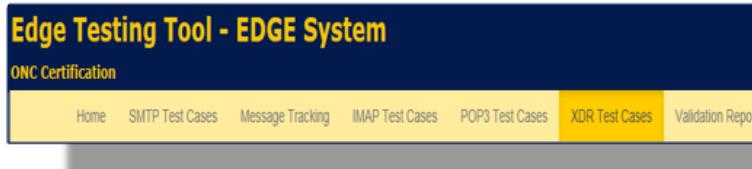
This test correlates to Test ID 1 of the XDR Test Cases tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 2.03 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

**Comment [a4]:** Need link

#### 7.5.3.1 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 7 within [2.2 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.



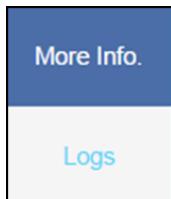
3. From the testing options available, select **Your System as: Sender**. This will enable test case selection.

Your System as: Sender



*Note: 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/descriptions, conditional requirements, and expected test results, Vendor role, and Metadata inclusion, click the **More Information** link for the Test Case.

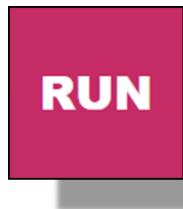


The screenshot shows a test case configuration window. At the top is a header bar with a back arrow and the title "Test #1". Below the header are two main sections: "Purpose/Description" and "Expected Test Results". The "Purpose/Description" section contains the text: "Verify that the Edge system can create an XDR message per the specification". The "Expected Test Results" section contains the text: "Edge System produces the right message and conforms to the specification". Below these are two more sections: "Vendor Role" and "Metadata Included". The "Vendor Role" section lists "Sender (Edge - SUT)". The "Metadata Included" section lists "Limited Metadata".

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.

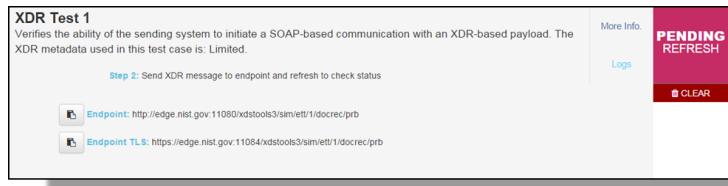
The screenshot shows the first step of an XDR test case. The step is titled "XDR Test 1" and has a description: "Verifies the ability of the sending system to initiate a SOAP-based communication with an XDR-based payload. The XDR metadata used in this test case is: Limited." Below the description is a "Step 1" instruction: "Provide your Direct From Address and Hit Run to generate your endpoint". On the right side of the step, there is a "RUN" button in a red box. At the bottom left, there is a "Direct From Address" input field with a placeholder "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.



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the 'TLS Endpoint' is provided by the Tester (e.g., Vendor).*

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.



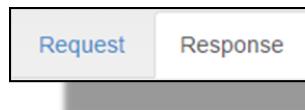
9. The ETT checks the generated endpoints for the presence of newly received XDR messages. The Vendor is prompted to manually validate if the test results conformed to the testing objectives. To complete this, the Vendor clicks the **Waiting Validation** button



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:

  - Accurately attempted to established a connection with the ETT;
  - Formed/transmitted the XDR message correctly; and
  - Successfully initiated SOAP-based communication with the ETT;
  - 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.



**Note:** ‘Accept XDR’ selections correlate with Test Case Success results (e.g., green check mark). Likewise, ‘Reject XDR’ selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a ‘Reject XDR’ selection correlate with a Test Success).

13. The ETT presents Vendor conformation 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 (reference Step 1 within [Section 5.1.1](#) to perform further retesting). 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: In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The '**Validation Report**' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., 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 (reference [Section 2.4 Reporting](#)).



#### 7.5.4 XDR TEST CASE 2

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:

- The Tester (i.e., 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.
- 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 [2.3 Profile Creation](#)).
- 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).
- 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.
- 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 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 Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.

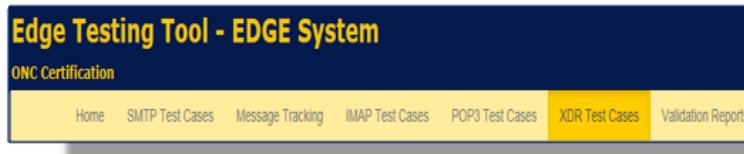
This test correlates to Test ID 2 of the XDR Test Cases tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 2.04 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

Comment [a5]: Need link

#### 7.5.4.1 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 7 within [2.2 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.

Your System as: Sender



*Note: 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/descriptions, conditional requirements, and expected test results, Vendor role, and Metadata inclusion, click the **More Information** link for the Test Case.

The screenshot shows a test configuration window titled "Test #2". It includes fields for "Purpose/Description" (specifying the goal of the test) and "Expected Test Results" (describing what the system should produce). It also lists "Vendor Role" (Sender) and "Metadata Included" (Full Metadata). A "RUN" button is visible at the bottom right.

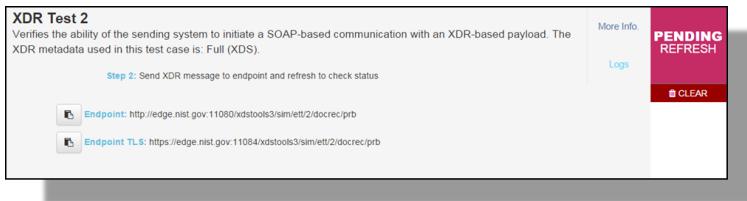
16. To initiate XDR Test 2, the Vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly.

The screenshot shows the "XDR Test 2" configuration screen. It includes a "More Info." link, a "Logs" link, and a prominent red "RUN" button. A note at the top states: "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)." Below this, a step 1 instruction says: "Step 1: Provide your Direct From Address and Hit Run to generate your endpoint." A "Direct From Address" input field is shown.



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the 'TLS Endpoint' is provided by the Tester (e.g., Vendor).*

5. 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.



- 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.



- 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



- 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.



9. Within the Log, the Vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
    - a. Accurately attempted to establish 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.

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.



**Note:** ‘Accept XDR’ selections correlate with Test Case Success results (e.g., green check mark). Likewise, ‘Reject XDR’ selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify 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 (reference Step 1 within [Section 5.4.1](#) to perform further retesting). 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: In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The '**Validation Report**' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., Vendor) to validate the acceptance of the message received by the SUT.*

13. All completed test session data is then available through the ETT's **Validation Report** tab (reference [Section 2.4 Reporting](#)).



### 7.5.5 XDR MESSAGE TRACKING (MT) 19

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:

- The Tester (i.e., 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.
- 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 [2.3 Profile Creation](#)).
- 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).
- 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.
- 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 is a **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 1.5.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 19 of the Message Tracking (MT) tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 2.07 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

Comment [a6]: Need link

### 7.5.5.1 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:

14. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 7 within [2.2 Registration](#).
15. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.



16. From the testing options available, select **Your System as: Sender**. This will enable test case selection.

Your System as: Sender



*Note: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

17. To gain additional information concerning XDR Message Tracking (MT) 19's intended focus, purpose/descriptions, conditional requirements, and expected test results, Vendor role, and Metadata inclusion, click the **More Information** link for the Test Case.

The screenshot shows a test case interface with the following details:

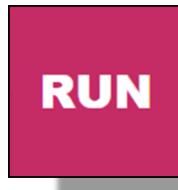
- Test #19**
- Purpose/Description:** Test Tool authenticates with the HISP using bad certificates.
- Expected Test Results:** HISP should disconnect when the certificate from the edge is bad.
- Vendor Role:** Server (HISP - SUT)
- Metadata Included:** N/A

18. 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 and process/present log data accordingly.

The screenshot shows the configuration for 'XDR MU2 Test 19'. It includes:

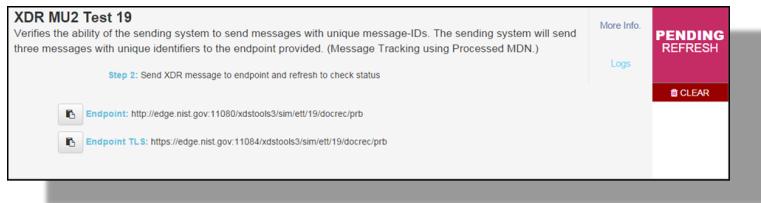
- XDR MU2 Test 19**: Verifies the ability of the sending system to send messages with unique message-IDs. The sending system will send three messages with unique identifiers to the endpoint provided. (Message Tracking using Processed MDN.)
- Step 1:** Provide your Direct From Address and Hit Run to generate your endpoint.
- Direct From Address:** [Input field]
- More Info.**
- Log.**
- RUN** (A large red button)

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



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the 'TLS Endpoint' is provided by the Tester (e.g., Vendor).*

20. 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.



21. 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.



22. 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.



23. 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

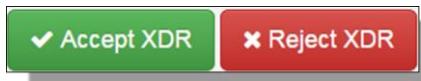
select the **Response** tab to review the ETT logged response received from the SUT after transmission of the XDR messages.



24. Within the Log, the Vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
- Accurately established a connection with the ETT;
  - Formed/transmitted 3 XDR messages with unique IDs; and
  - Generated conformant Processed MDNs for messaging tracking purposes.

A screenshot of a log window titled "Log for XDR MU2 Test 19". The window has a "Request" tab and a "Response" tab. The "Response" tab is selected, showing a large amount of XML log data. At the bottom of the window are two buttons: a green "Accept XDR" button with a checkmark icon and a red "Reject XDR" button with a cross icon.

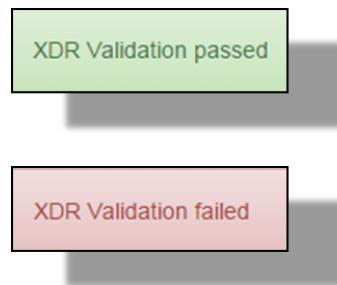
25. If the Vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected.





**Note:** ‘Accept XDR’ selections correlate with Test Case Success results (e.g., green check mark). Likewise, ‘Reject XDR’ selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a ‘Reject XDR’ selection correlate with a Test Success).

26. The ETT presents Vendor conformation based upon the selection made.



27. 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 (reference Step 1 within [Section 5.5.1](#) to perform further retesting). The Vendor can select the **Clear** button to reset the test.

**XDR MU2 Test 19**  
Verifies the ability of the sending system to send messages with unique message-IDs. The sending system will send three messages with unique identifiers to the endpoint provided. (Message Tracking using Processed MDN.)  
Step 1: Provide your Direct From Address and Hit Run to generate your endpoint  
More Info  
Logs  
RETRY  
CLEAR

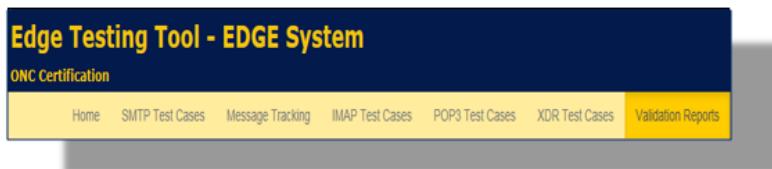
XDR message acceptance results in a green check. The Vendor can select the **Clear** button to reset the test.

**XDR MU2 Test 19**  
Verifies the ability of the sending system to send messages with unique message-IDs. The sending system will send three messages with unique identifiers to the endpoint provided. (Message Tracking using Processed MDN.)  
More Info  
Logs  
CLEAR



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

28. All completed test session data is then available through the ETT's **Validation Report** tab (reference [Section 2.4 Reporting](#)).



#### 7.5.6 XDR MESSAGE TRACKING (MT) 20

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 HISIP recipient (i.e., ETT), acting as the receiver, and generate process MDNs successfully.

The testing details for conformance testing flow are as follows:

- The Tester (i.e., 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.
- 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 communicate to execute this Test Case; reference [2.3 Profile Creation](#)).
- 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).
- 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).

- 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 is a **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 1.5.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 20 of the Message Tracking (MT) tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 2.08 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

#### **7.5.6.1 Testing Steps**

To execute XDR Message Tracking (MT) 20 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.

##### **7.5.6.1.1 20a**

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 7 within [2.2 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.

**Your System as: Sender**



*Note: 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/descriptions, conditional requirements, and expected test results, Vendor role, and Metadata inclusion, click the **More Information** link for the Test Case.

**More Info.**  
**Logs**

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

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.

**XDR Test MU2 20a**  
Verifies the ability of the sending system to initiate an XDR transaction to ETT and to receive a process MDN. The test lab will inspect the SUT's logs and system to verify that the process MDN was handled appropriately.

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

More Info.  
Logs  
**RUN**

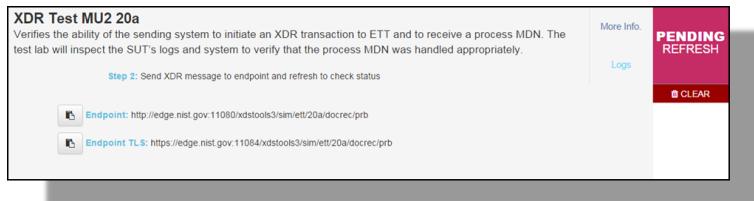
Direct From Address:  Direct From Address

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



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the **TLS Endpoint** is provided by the Tester (e.g., Vendor).*

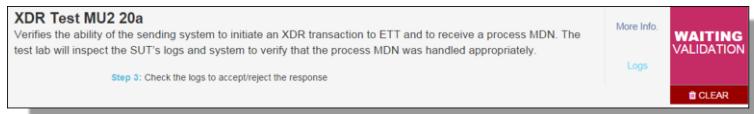
- The Vendor is prompted to navigate to the SUT's messaging client and create two a new XDR message. These new message must be accurately formed in the correct syntax. The Vendor will send the XDR message to one of the two ETT generated endpoints (TLS or non-TLS) for the Test Case. The Vendor will also specify a valid recipient for the XDR messages (in addition to the ETT generated endpoint).



- 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.



- 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.

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=IDEBoundary112233445566778899; type="application/xop+xml"; start=<doc@hexds.nist.gov>; start-info="application/soap+xml"; charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Tue, 23 Jun 2015 17:22:48 GMT
X-FW:
--IDEBoundary112233445566778899
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <doc@hexds.nist.gov>

<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope">
<S:Header>
  <S:Action s:mustUnderstand="1" xmlns:S="http://www.w3.org/2003/05/soap-envelope">
    xmlns:wsa="http://www.w3.org/2005/08/addressing">urn:be:111:2007:ProvideAndRegisterDocumentSet-&Response</S:Action>
  <S:RelatesTo> xmlns:wsa="http://www.w3.org/2005/08/addressing">99519d70-3b87-4b3c-995c-14684317a323</S:RelatesTo>
</S:Header>
<S:Body>
  <S:RegistryResponse status="urn: oasis:names:tc:ebml-regrep:ResponseStatusType:Success">
    xmlns:rsw="urn:oasis:names:tc:ebml-regrep:xsd:rsw:3.0"/>
</S:Body>
</S:Envelope>
--IDEBoundary112233445566778899--
```

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.



29. The Vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:

- Accurately established a connection with the ETT;
- 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.

The screenshot shows the 'Log for XDR Test MU2 20a' window. The 'Response' tab is selected. The log content is a large XML document. At the bottom of the window are two buttons: a green 'Accept XDR' button and a red 'Reject XDR' button.

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.



*Note: 'Accept XDR' selections correlate with Test Case Success results (e.g., green check mark). Likewise, 'Reject XDR' selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a 'Reject XDR' selection correlate with a Test Success).*

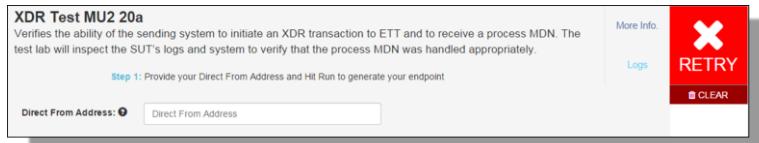
13. The ETT presents Vendor conformation based upon the selection made.

XDR Validation passed



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 (reference Step 1 within [Section 5.6.1.1](#) to perform further retesting). The Vendor can select the **Clear** button to reset the test.

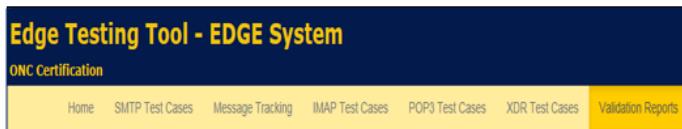


XDR message acceptance results in a green check. The Vendor can select the **Clear** button to reset the test.



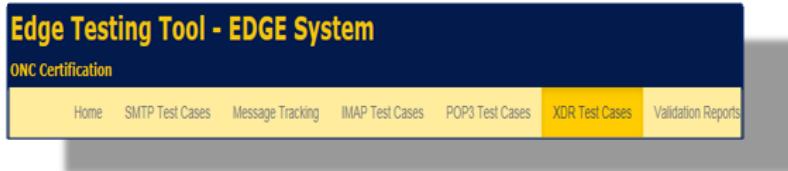
**Note:** In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The '**Validation Report**' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., 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 (reference [Section 2.4 Reporting](#)).



#### 7.5.6.1.2 20b

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 7 within [2.2 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.



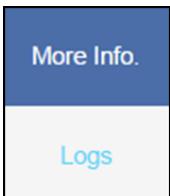
3. From the testing options available, select **Your System as: Sender**. This will enable test case selection.

**Your System as: Sender**



*Note: 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/descriptions, conditional requirements, and expected test results, Vendor role, and Metadata inclusion, click the **More Information** link for the Test Case.

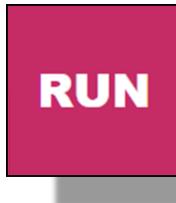


A screenshot of a form titled "Test #". It has fields for "Purpose/Description" and "Expected Test Results". Below these are sections for "Vendor Role" and "Metadata Included".

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 MU2 Test 20b' configuration screen. It includes a description of the test, a 'More Info.' link, a 'Logs' link, and a large red 'RUN' button. A text input field for 'Direct From Address' is present, with a placeholder 'Direct From Address' and a help icon.

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



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the 'TLS Endpoint' is provided by the Tester (e.g., 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).

The screenshot shows the 'XDR MU2 Test 20b' configuration screen, specifically Step 2. It includes a description of the test, a 'More Info.' link, a 'Logs' link, and a large red 'PENDING REFRESH' button. Two input fields for 'Endpoint' and 'Endpoint TLS' are shown, each with a help icon and a dropdown arrow.

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.



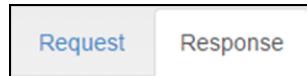
The Vendor is prompted to check the SUT's local logs and validate that the process MDNs generated as a result of sending the XDR message to both the ETT and invalid recipients were handled correctly.

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=IDEBoundary112233445566778899; type="application/xop+xml"; start="cid@hexds.nist.gov"; start-info="application/soap+xml"; charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Tue, 23 Jun 2015 17:22:48 GMT
X-FW
--IDEBoundary112233445566778899
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <cid@hexds.nist.gov>

<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope">
  <S:Header>
    <wsa:Action s:mustUnderstand="1" xmlns:wsa="http://www.w3.org/2005/08/addressing">urn:be111:2007:ProvideAndRegisterDocumentSet->Response</wsa:Action>
    <wsa:RelatesTo xmlns:wsa="http://www.w3.org/2005/08/addressing">urn:be111:2007:4b3c-995c-14684317ea32</wsa:RelatesTo>
  </S:Header>
  <S:Body>
    <rs:RegistryResponse status="urn: oasis:names:tc:ebml-regrep:ResponseStatusType:Success"
      xmlns:rs="urn:oasis:names:tc:ebml-regrep:xsdr:s13:0"/>
  </S:Body>
</S:Envelope>
--IDEBoundary112233445566778899--
```

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.



30. The Vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
- Accurately established a connection with the ETT;
  - Correctly created and transmitted the XDR message to the provided ETT endpoint recipient and additional valid message recipient;
  - Produced conformant process MDNs for messaging tracking purposes (valid recipient); and
  - Correctly received and handled a process MDN failure notification sent from the ETT.

A screenshot of a web-based log viewer titled "Log for XDR MU2 Test 20b". It shows a "Request" tab and a "Response" tab. The "Response" tab is active, displaying a large block of XML code representing the XDR message. At the bottom of the response pane are two buttons: a green "Accept XDR" button with a checkmark icon and a red "Reject XDR" button with a cross icon.

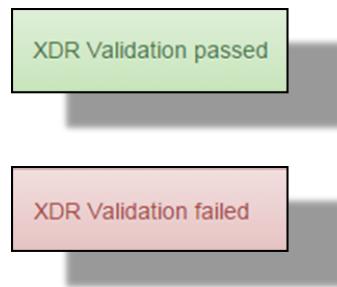
12. If the Vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected.





**Note:** ‘Accept XDR’ selections correlate with Test Case Success results (e.g., green check mark). Likewise, ‘Reject XDR’ selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a ‘Reject XDR’ selection correlate with a Test Success).

13. The ETT presents Vendor conformation 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 (reference Step 1 within [Section 5.6.1.2](#) to perform further retesting). The Vendor can select the **Clear** button to reset the test.

**XDR MU2 Test 20b**  
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 process MDN was handled appropriately.  
More Info  
Logs  
Step 1: Provide your Direct From Address and Hit Run to generate your endpoint  
Direct From Address:  Direct From Address  
RETRY  
CLEAR

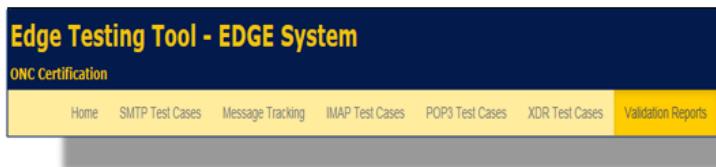
XDR message acceptance results in a green check. The Vendor can select the **Clear** button to reset the test.

**XDR MU2 Test 20b**  
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 process MDN was handled appropriately.  
More Info  
Logs  
X  
CLEAR



**Note:** In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The '**Validation Report**' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., 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 (reference [Section 2.4 Reporting](#)).



### 7.5.7 XDR MESSAGE TRACKING (MT) 48

The objective of this test sequence is to determine if an Edge System (i.e., SUT), acting as the sender, can 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:

- 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.
- The Tester (i.e., 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.
- 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 communicate to execute this Test Case; reference [2.3 Profile Creation](#)).
- 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).

- 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.
- 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 is a **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 1.5.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

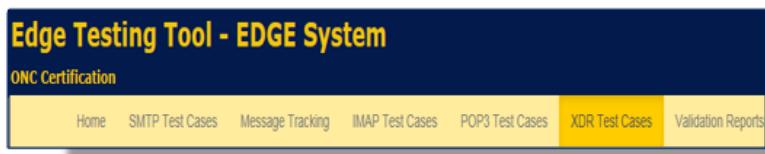
This test correlates to Test ID 19 of the Message Tracking (MT) tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 2.09 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

**Comment [a7]:** Need link

#### 7.5.7.1 Testing Steps

To execute XDR Message Tracking (MT) 48and 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 7 within [2.2 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.

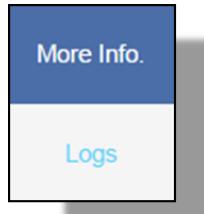


3. From the testing options available, select **Your System as: Sender**. This will enable test case selection.



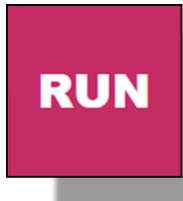
*Note: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

4. To gain additional information concerning XDR Message Tracking (MT) 48's intended focus, purpose/descriptions, conditional requirements, and expected test results, Vendor role, and Metadata inclusion, click the **More Information** link for the Test Case.



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.

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

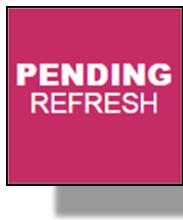


*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the **TLS Endpoint** is provided by the Tester (e.g., Vendor).*

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.



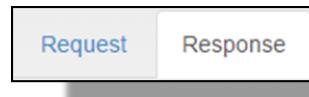
9. The ETT checks the generated endpoints for the presence of newly received XDR messages. The Vendor is prompted to manually validate if the test results conformed to the testing objectives. To compete this, the Vendor clicks the **Waiting Validation** button.



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) 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.

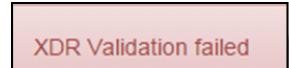
12. If the Vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected.



**Note:** ‘Accept XDR’ selections correlate with Test Case Success results (e.g., green check mark). Likewise, ‘Reject XDR’ selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a ‘Reject XDR’ selection correlate with a Test Success).

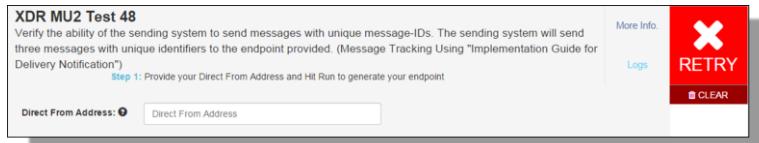
13. The ETT presents Vendor conformation based upon the selection made.





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 (reference Step 1 within [Section 5.7.1](#) to perform further retesting). The Vendor can select the **Clear** button to reset the test.

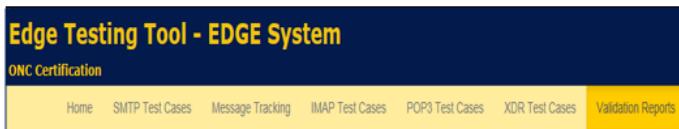


XDR message acceptance results in a green check. The Vendor can select the **Clear** button to reset the test.



**Note:** In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The '**Validation Report**' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., 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 (reference [Section 2.4 Reporting](#)).



### 7.5.8 XDR MESSAGE TRACKING (MT) 49

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:

- The Tester (i.e., 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.
- 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 communicate to execute this Test Case; reference [2.3 Profile Creation](#)).
- 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).
- 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.
- 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](#).

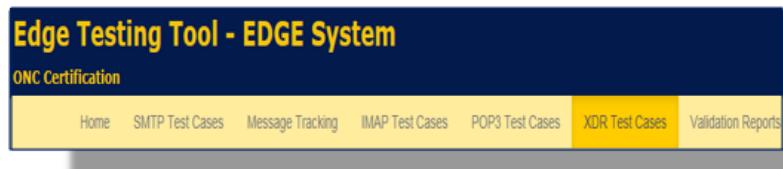
This is a **required test** and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.5.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 20 of the Message Tracking (MT) tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 2.10 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

Comment [a8]: Need link

### 7.5.8.1 Testing Steps

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 7 within [2.2 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.



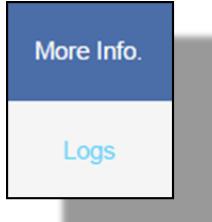
3. From the testing options available, select **Your System as: Sender**. This will enable test case selection.

Your System as: Sender



*Note: 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, conditional requirements, and expected test results, Vendor role, and Metadata inclusion, click the **More Information** link for the Test Case.



The screenshot shows a "Test #>" button, fields for "Purpose/Description:" and "Expected Test Results:", and sections for "Vendor Role" and "Metadata Included".

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.

The screenshot shows a "XDR MU2 Test 49" step with instructions to provide a Direct From Address. It includes a "More Info." link, a "Log in" button, 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.



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the **TLS Endpoint** is provided by the Tester (e.g., Vendor).*

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.



- Once the message has been transmitted from the SUT to the ETT endpoints, the Vendor clicks the **Pending Refresh** button for the Test Case.



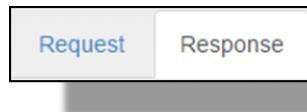
- The ETT checks the generated endpoints for the presence of newly received XDR messages. The Vendor is prompted to manually validate if the test results conformed to the testing objectives. To complete this, the Vendor clicks the **Waiting Validation** button.



- 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:

  - Accurately established a connection with the ETT;
  - Formed/transmitted the XDR messages; and
  - 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.



**Note:** ‘Accept XDR’ selections correlate with Test Case Success results (e.g., green check mark). Likewise, ‘Reject XDR’ selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a ‘Reject XDR’ selection correlate with a Test Success).

13. The ETT presents Vendor conformation 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 (reference Step 1 within [Section 5.8.1](#) to perform further retesting). 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:** In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The '**Validation Report**' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., 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 (reference [Section 2.4 Reporting](#)).



### 7.5.9 XDR MESSAGE TRACKING (MT) 50

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:

- The Tester (i.e., 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.
- 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 [2.3 Profile Creation](#)).
- 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).
- 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).
- 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 is a **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 1.5.2.2 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 50 of the Message Tracking (MT) tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 2.01 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

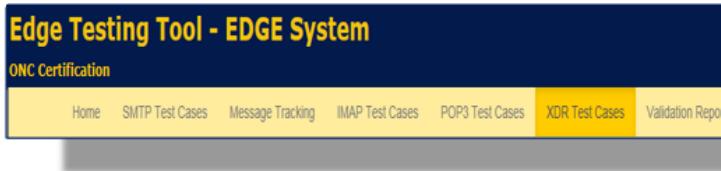
Comment [a9]: Need link

### 7.5.9.1 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.

#### 7.5.9.1.1 50a

16. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 7 within [2.2 Registration](#).
17. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.



18. From the testing options available, select **Your System as: Sender**. This will enable test case selection.

Your System as: Sender



*Note: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

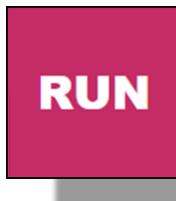
19. To gain additional information concerning XDR Message Tracking (MT) 50a's intended focus, purpose/descriptions, conditional requirements, and expected test results, Vendor role, and Metadata inclusion, click the **More Information** link for the Test Case.

The screenshot shows a web-based testing tool. At the top left is a blue button labeled "More Info.". Below it is a white button labeled "Logs". The main area is a form titled "Test #". It has two input fields: "Purpose/Description:" and "Expected Test Results:". Below these are two more input fields: "Vendor Role" and "Metadata Included". A small "Logs" link is located at the bottom right of the form area.

20. 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.

The screenshot shows a configuration screen for "XDR MU2 Test 50a". The title is "XDR MU2 Test 50a" and the subtitle is "Verify the ability of the sending system to correctly handle the case of sending XDR messages to valid recipients.". Below this is a note: "Step 1: Provide your Direct From Address and Hit Run to generate your endpoint". On the right side, there are three buttons: "More Info.", "Logs", and a large red "RUN" button. At the bottom left, there is a "Direct From Address:" field with a placeholder "Direct From Address" and a "Logs" link.

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



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the 'TLS Endpoint' is provided by the Tester (e.g., Vendor).*

22. 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).



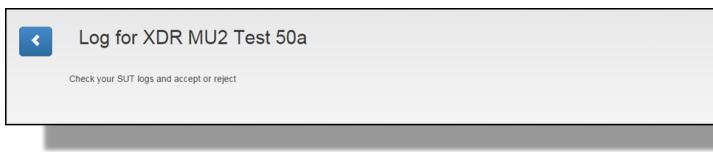
23. Once the XDR message has been transmitted from the SUT to the ETT endpoint, the Vendor clicks the **Pending Refresh** button for the Test Case.



24. 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.



25. 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.

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=IDEBoundary112233445566778899; type="application/xop+xml"; start=<doc0@iheds.nist.gov>; start-info="application/soap+xml"; charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Tue, 23 Jun 2015 17:22:48 GMT

35F
--IDEBoundary112233445566778899
Content-Type: application/soap+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <doc0@iheds.nist.gov>

<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope">
  <S:Header>
    <S:Action i:mustUnderstand="1" xmlns:i="http://www.w3.org/2003/05/soap-envelope">
      urn:use:<http://www.w3.org/2005/08/addressing>urn:hei:iti:2007:ProvideAndRegisterDocumentSet-bResponse</S:Action>
      <S:RelatesTo xmlns:use="http://www.w3.org/2005/08/addressing">59919d7b-b074b3c-959c-1468a017ea33</S:RelatesTo>
    </S:Header>
  <S:Body>
    <S:RegistryResponse status="urn: oasis:names:tc:ebml-regrep:ResponseStatusType:Success"
      xmlns:rsrc="urn: oasis:names:tc:ebml-regrep:xsdris3.0"/>
  </S:Body>
</S:Envelope>
--IDEBoundary112233445566778899--
```

26. 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.



31. The Vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
- i. Accurately established a connection with the ETT;
  - m. Correctly created and transmitted the XDR message to the provided ETT endpoint recipient and additional valid message recipient;
  - n. Produced conformant process MDNs for messaging tracking purposes (valid recipient); and
  - o. Correctly receive and handle a process MDN notification sent from the ETT.

27. 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.



**Note:** ‘Accept XDR’ selections correlate with Test Case Success results (e.g., green check mark). Likewise, ‘Reject XDR’ selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a ‘Reject XDR’ selection correlate with a Test Success).

28. The ETT presents Vendor conformation based upon the selection made.





29. 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 (reference Step 1 within [Section 5.9.1.1](#) to perform further retesting). 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.



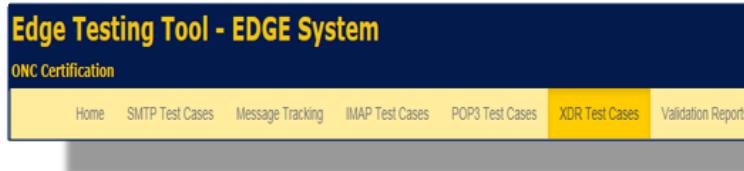
*Note: In the test procedures, the 'Log' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The 'Log' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The 'Validation Report' represents the aggregation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

30. All completed test session data is then available through the ETT's **Validation Report** tab (reference [Section 2.4 Reporting](#)).



#### 7.5.9.1.2 50b

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 7 within [2.2 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.



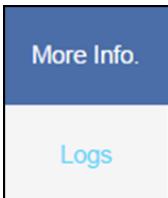
3. From the testing options available, select **Your System as: Sender**. This will enable test case selection.

Your System as: Sender



*Note: 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) Case 50b's intended focus, purpose/descriptions, conditional requirements, and expected test results, Vendor role, and Metadata inclusion, click the **More Information** link for the Test Case.

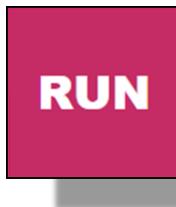


A screenshot of a form titled "Test #". It has fields for "Purpose/Description:" and "Expected Test Results:". Below these are sections for "Vendor Role" and "Metadata Included".

5. 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.

XDR MU2 Test 50b  
Verify the ability of the sending system to correctly handle the case of sending XDR messages to invalid recipients.  
Step 1: Provide your Direct From Address and Hit Run to generate your endpoint.  
More Info. [Logs](#) **RUN**  
Direct From Address:  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.



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the 'TLS Endpoint' is provided by the Tester (e.g., 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).

XDR MU2 Test 50b  
Verify the ability of the sending system to correctly handle the case of sending XDR messages to invalid recipients.  
Step 2: Send XDR message to endpoint and refresh to check status.  
More Info. [Logs](#) **PENDING REFRESH**  
Endpoint: <http://edge.nist.gov:11080/xdstools3/sim/ett/50b/docrec/prb>  
Endpoint TLS: <https://edge.nist.gov:11084/xdstools3/sim/ett/50b/docrec/prb>  
 CLEAR

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.



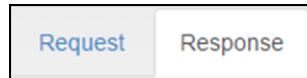
The Vendor is prompted to check the SUT's local logs and validate that the process MDNs generated as a result of sending the XDR message to both the ETT and invalid recipients were handled correctly.

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=----Boundary112233445566778899; type="application/xop+xml"; start=<doc@ihexds.nist.gov>; start-info="application/soap+xml"; charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Tue, 23 Jun 2015 17:22:48 GMT
...
----Boundary112233445566778899
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <doc@ihexds.nist.gov>

<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope">
<S:Header>
<S:Action s:mustUnderstand="1" xmlns:s="http://www.w3.org/2003/05/soap-envelope">
<ns1:use href="http://www.w3.org/2005/08/addressing/urn:he:11112007:ProvideAndRegisterDocumentSet-bResponse/>
<ns1:relatesTo href="http://www.w3.org/2005/08/addressing/55913d7f-6e07-4b3c-951c-14084317ea33"/>
</S:Header>
<S:Body>
<ns1:RegistryResponse status="urn:osais:names:tc:ebml-regrep:ResponseStatusType:Success">
<ns1:nsr><urn:osais:names:tc:ebml-regrep:xsdr13:0/>
</S:Body>
</S:Envelope>
----Boundary112233445566778899--
```

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.



32. The Vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
- Accurately established a connection with the ETT;
  - Correctly created and transmitted the XDR message to the provided ETT endpoint recipient and additional valid message recipient;
  - Produced conformant process MDNs for messaging tracking purposes (valid recipient); and
  - Correctly received and handled a process MDN failure notification sent from the ETT.

A screenshot of a web-based log viewer titled "Log for XDR MU2 Test 50b". It shows a "Request" tab and a "Response" tab. The "Response" tab is active, displaying a large block of XML log data. At the bottom of the page are two buttons: a green "Accept XDR" button with a checkmark icon and a red "Reject XDR" button with a cross icon.

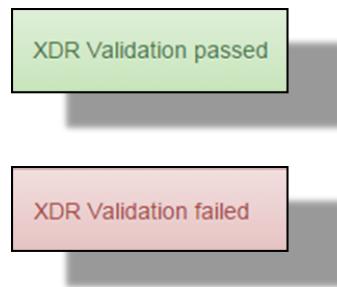
12. If the Vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected.





**Note:** ‘Accept XDR’ selections correlate with Test Case Success results (e.g., green check mark). Likewise, ‘Reject XDR’ selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a ‘Reject XDR’ selection correlate with a Test Success).

13. The ETT presents Vendor conformation 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 (reference Step 1 within [Section 5.9.1.2](#) to perform further retesting). The Vendor can select the **Clear** button to reset the test.

**XDR MU2 Test 50b**  
Verify the ability of the sending system to correctly handle the case of sending XDR messages to invalid recipients.

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

More Info Logs

Direct From Address:  Direct From Address

RETRY

CLEAR

XDR message acceptance results in a green check. The Vendor can select the **Clear** button to reset the test.

**XDR MU2 Test 50b**  
Verify the ability of the sending system to correctly handle the case of sending XDR messages to invalid recipients.

More Info Logs

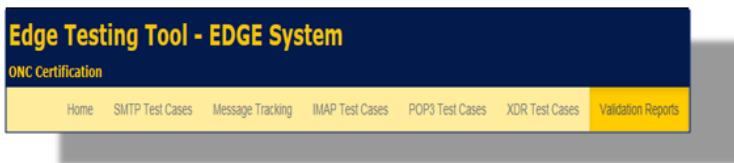
Direct From Address:  Direct From Address

CLEAR



**Note:** In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The '**Validation Report**' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., 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 (reference [Section 2.4 Reporting](#)).



## 7.6 XDR Receiving

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

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

### 7.6.1 XDR TEST CASE 8

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:

- The Tester (i.e., 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.
- 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 [2.3 Profile Creation](#)).

- 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 Vendor validates through ‘Log’ review that the SUT successfully received the ETT’s request to establish 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 is a **required test** and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.

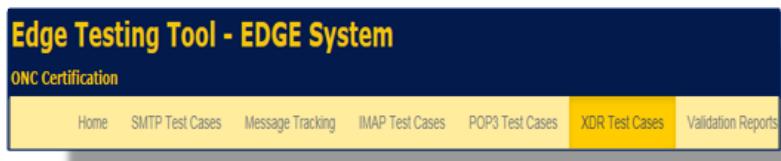
This test correlates to Test ID 8 of the XDR Test Cases tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 4.01 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

Comment [a10]: Need link

#### 7.6.1.1 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 7 within [2.2 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.

Your System as: Receiver



*Note: 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, conditional requirements, and expected test results, Tester (e.g., Vendor) role, and Metadata inclusion, click the **Description** link for the Test Case.

The screenshot shows a test case summary for 'Test #8'. It includes the following details:

Purpose/Description:	Expected Test Results:
Test Tool authenticates with the Edge using Mutual TLS correctly	Edge System is capable of accepting and validating a Mutual TLS connection.

Vendor Role	Metadata Included
Receiver (Edge - SUT)	N/A

5. To initiate XDR Test Case 8, the Tester (i.e., 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.

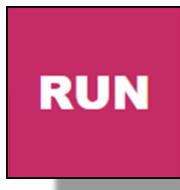
The screenshot shows the configuration interface for 'XDR Test 8'. It includes the following fields:

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

IP Address:  More Info. Log

Port:  RUN

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.



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the 'TLS Endpoint' is provided by the Tester (e.g., Vendor).*

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 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.



9. 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.

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=IDEBoundary112233445566778899; type="application/xop+xml"; start=<doc0@hexds.nist.gov>; start-info="application/xop+xml"; charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Tue, 13 Jan 2015 10:47:08 GMT

430
--IDEBoundary112233445566778899
Content-Type: application/xop+xml; charset=UTF-8; type="application/xop+xml"
Content-Transfer-Encoding: binary
Content-ID: <doc0@hexds.nist.gov>

<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Header>
    <wsa:Action s:mustUnderstand="1" xmlns:s="http://www.w3.org/2003/05/soap-envelope">
      http://www.w3.org/2005/08/addressing
    </wsa:Action>
    <wsa:RelatesTo xmlns:wsa="http://www.w3.org/2005/08/addressing" >d4c054e-e9d9-d450-bd84-aecfcfa0bae</wsa:RelatesTo>
  </env:Header>
  <env:Body>
    <fault:Fault xmlns:fault="http://www.w3.org/2003/05/soap-envelope">
      <fault:Code>
        <fault:value>fault:Sender</fault:value>
      </fault:Code>
      <fault:Reason>
        <fault:Text xml:lang="en">Sender: Correct Header Namespace - Expected: ; Found: http://www.w3.org/2003/05/soap-envelope/fault:Text</fault:Text>
      </fault:Reason>
    </fault:Fault>
  </env:Body>
</env:Envelope>
--IDEBoundary112233445566778899--
```

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.



*Note: 'Accept XDR' selections correlate with Test Case Success results (e.g., green check mark). Likewise, 'Reject XDR' selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a 'Reject XDR' selection correlate with a Test Success).*

11. The ETT presents Vendor conformation based upon the selection made.

XDR Validation passed



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 (reference Step 1 within [Section 6.1.1](#) to perform further retesting). The Vendor can select the **Clear** button to reset the test.

The screenshot shows the 'XDR Test 8' interface. It includes fields for 'IP Address' and 'Port', and buttons for 'Logs', 'RETRY', and 'CLEAR'. A red 'X' icon is displayed next to the 'RETRY' button, indicating a failure.

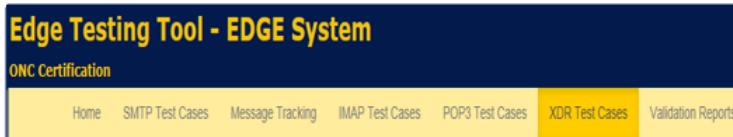
XDR message acceptance results in a green check. The Vendor can select the **Clear** button to reset the test.

The screenshot shows the same 'XDR Test 8' interface as above, but with a green checkmark icon next to the 'RETRY' button, indicating success.



**Note:** In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The '**Validation Report**' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., 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 (reference [Section 2.4 Reporting](#)).



### 7.6.2 XDR TEST CASE 9

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:

- The Tester (i.e., 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.
- 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 [2.3 Profile Creation](#)).
- 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 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 is a **required test** and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 9 of the XDR Test Cases tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 4.02 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

#### 7.6.2.1 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 7 within [2.2 Registration](#).
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.

The screenshot shows the main navigation bar of the Edge Testing Tool. The title "Edge Testing Tool - EDGE System" is at the top in yellow. Below it is a sub-header "ONC Certification". The navigation menu includes "Home", "SMTP Test Cases", "Message Tracking", "IMAP Test Cases", "POP3 Test Cases", "XDR Test Cases" (which is highlighted in yellow), and "Validation Reports".

3. From the testing options available, select **Your System as: Receiver**. This will enable test case selection.

**Your System as: Receiver**



*Note: 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, conditional requirements, and expected test results, Tester (e.g., Vendor) role, and Metadata inclusion, click the **Description** link for the Test Case.

The screenshot shows the "Test #9" details page. It includes sections for "Purpose/Description" (Test Tool authenticates with the Edge using bad certificates) and "Expected Test Results" (Edge System rejects the connection due to the bad certificate published by the Test Tool). Below this are sections for "Vendor Role" (Receiver (Edge - SUT)) and "Metadata Included" (N/A).

5. To initiate XDR Test Case 9, the Tester (i.e., 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.

The screenshot shows the "XDR Test 9" configuration page. It has a "Step 1: Provide your IP Address Port and Hit Run to send XDR message" section with fields for "IP Address" and "Port". A "RUN" button is prominently displayed in red. Other buttons include "More Info" and "Logs".

- 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.



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the **TLS Endpoint** is provided by the Tester (e.g., Vendor).*

- 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.



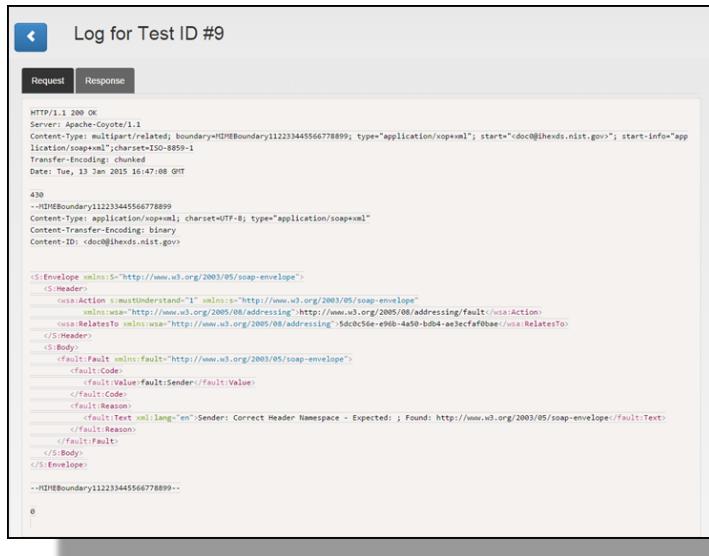
- The Vendor is presented with the Test Case **Log** screen.



The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test Case 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).



The screenshot shows a log entry for Test ID #9. The log details a failed TLS connection attempt. The response header includes a SOAP fault message indicating a 'fault:Reason' where the 'Text' field contains the message 'Correct Header Namespace - Expected: ; Found: http://www.w3.org/2003/05/soap-envelope/fault:Text'. The log concludes with a closing boundary marker.

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=IDMEBoundary112233445566778899; type="application/xop+xml"; start=<doc@iheds.nist.gov>; start-info="app
lication/soap+xml"; charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Tue, 13 Jan 2015 16:47:08 GMT

--IDMEBoundary112233445566778899
Content-Type: application/soap+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <doc@iheds.nist.gov>

<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Header>
    <wsa:Action s:mustUnderstand="1" xmlns:wsa="http://www.w3.org/2005/08/addressing">http://www.w3.org/2005/08/addressing/fault</wsa:Action>
    <wsa:RelatesTo xmlns:wsa="http://www.w3.org/2005/08/addressing">5dc0c56e-e9eb-4a50-bd4-a3ecfaf0bae</wsa:RelatesTo>
  </env:Header>
  <env:Body>
    <fault:Fault xmlns:fault="http://www.w3.org/2003/05/soap-envelope">
      <fault:Code>
        <fault:Value>fault:Sender</fault:Value>
      </fault:Code>
      <fault:Reason>
        <fault:Text enLang="en">Sender: Correct Header Namespace - Expected: ; Found: http://www.w3.org/2003/05/soap-envelope/fault:Text</fault:Text>
      </fault:Reason>
    </fault:Fault>
  </env:Body>
</env:Envelope>
--IDMEBoundary112233445566778899--
```

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.



*Note: 'Accept XDR' selections correlate with Test Case Success results (e.g., green check mark). Likewise, 'Reject XDR' selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify 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 of failure of a Test Case.

XDR message rejection results in a red X and prompts the Vendor to **Retry** the test (reference Step 1 within [Section 6.2.1](#) to perform further retesting). The Vendor can select the **Clear** button to reset the test.

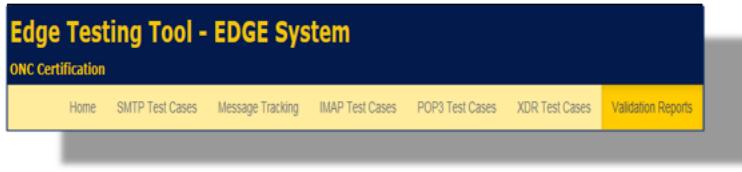
A screenshot of the Edge Testing Tool interface. On the left, a panel titled "XDR Test 9" with the subtitle "Verifies the ability of the receiving system to reject a mutual TLS connection where the certificate provided by the ETT is invalid." contains fields for "IP Address" and "Port". On the right, there are "More Info" and "Logs" buttons, and a large red button labeled "RETRY" with a white X icon. Below the red button is a "CLEAR" button.

XDR message acceptance results in a green check. The Vendor can select the **Clear** button to reset the test.

A screenshot of the Edge Testing Tool interface, similar to the previous one but with a green checkmark icon instead of a red X. The "RETRY" button is still present below it.

**Note:** In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The '**Validation Report**' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., 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 (reference [Section 2.4 Reporting](#)).



### 7.6.3 XDR TEST CASE 3

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:

- The Tester (i.e., 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.
- 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 2.3 Profile Creation](#) of this ETT User Guide).
- 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 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 is a **required test** and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 3 of the XDR Test Cases tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 4.03 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

#### 7.6.3.1 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:

#### 7.6.3.1.1 3

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 7 within [2.2 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.

**Your System as: Receiver**



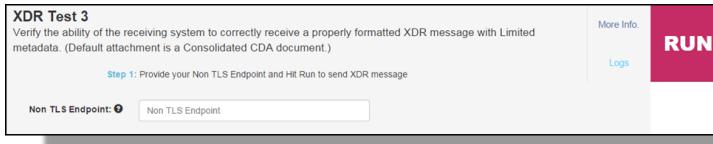
*Note: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

4. To gain additional information concerning a target XDR Test Case 3's intended focus, purpose/descriptions, conditional requirements, and expected test results, Tester (e.g., Vendor) role, and Metadata inclusion, click the **Description** link for the Test Case.

A screenshot of a test case details page. At the top left is a back arrow and the text "Test #3". Below that is a table with two columns: "Purpose/Description:" and "Expected Test Results:". The "Purpose/Description:" row contains the text "Verify that an Edge system can receive a properly formatted XDR message.". The "Expected Test Results:" row contains the text "Edge system is capable of receiving and processing a valid message. Test procedure may include other details for verification. Test Tool is satisfied with a good response.". Below the table are two sections: "Vendor Role" (Receiver (Edge - SUT)) and "Metadata Included" (Limited Metadata).

5. To initiate XDR Test Case 3, the Tester (i.e., 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.



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the **TLS Endpoint** is provided by the Tester (e.g., Vendor).*

7. Once the XDR message has been sent, the Tester (e.g., 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.

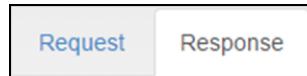


8. The Vendor is presented with the Test Case **Log** screen.



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

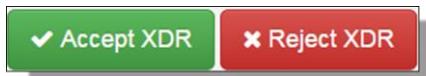
**Response** tab to review the ETT logged response received from the SUT after the XDR message has been transmitted.



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.

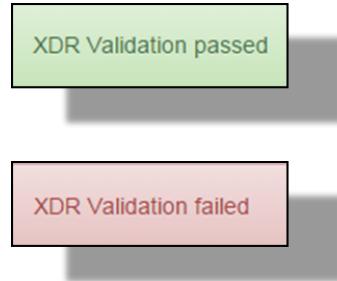
The screenshot shows a mobile application interface titled "Log for Test ID #". At the top, there are "Request" and "Response" tabs. The "Response" tab is selected, showing a detailed log entry. The log entry includes a timestamp, HTTP headers, and a large block of XML response data. At the bottom of the screen are two buttons: a green "Accept XDR" button and a red "Reject XDR" button.

10. If the Tester (e.g., 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.



*Note: 'Accept XDR' selections correlate with Test Case Success results (e.g., green check mark). Likewise, 'Reject XDR' selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify 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 of failure of a Test Case.

XDR message rejection results in a red X and prompts the Vendor to **Retry** the test (reference Step 1 within [Section 6.4.1.1 4a](#) to perform further retesting). The Vendor can select the **Clear** button to reset the test.

The screenshot shows the ETT interface for an XDR Test. The test name is 'XDR Test 3'. The description states: 'Verify the ability of the receiving system to correctly receive a properly formatted XDR message with Limited metadata. (Default attachment is a Consolidated CDA document.)'. Below this, there is a note: 'Step 1: Provide your Non TLS Endpoint and Hit Run to send XDR message'. A 'Non TLS Endpoint' input field contains the value 'Non TLS Endpoint'. To the right of the input field are two buttons: 'More Info.' and 'Logs'. At the bottom right of the interface is a large red button labeled 'RETRY' with a white X icon. Below the 'RETRY' button is a smaller red button labeled 'CLEAR' with a white 'X' icon.

XDR message acceptance results in a green check. The Vendor can select the **Clear** button to reset the test.

The screenshot shows the ETT interface for an XDR Test. The test name is 'XDR Test 3'. The description is identical to the previous screenshot. Below the description, there is a note: 'Step 1: Provide your Non TLS Endpoint and Hit Run to send XDR message'. A 'Non TLS Endpoint' input field contains the value 'Non TLS Endpoint'. To the right of the input field are two buttons: 'More Info.' and 'Logs'. At the bottom right of the interface is a large green button labeled 'CLEAR' with a white checkmark icon.



*Note: In the test procedures, the 'Log' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The 'Log' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The 'Validation Report' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., 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 (reference [Section 2.4 Reporting](#)).



#### 7.6.3.1.2 3 – HITSP/C32

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 7 within [2.2 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.

**Your System as: Receiver**



*Note: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

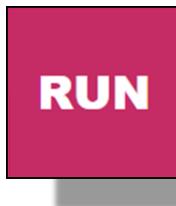
4. To gain additional information concerning a target XDR Test Case 3 – HITSP/C32's intended focus, purpose/descriptions, conditional requirements, and expected test results, Tester (e.g., Vendor) role, and Metadata inclusion, click the **Description** link for the Test Case.

The screenshot shows the 'Test #3' configuration page. It includes fields for 'Purpose/Description' (Verify that an Edge system can receive a properly formatted XDR message) and 'Expected Test Results' (Edge system is capable of receiving and processing a valid message, test procedure may include other details for verification. Test Tool is satisfied with a good response). There are also sections for 'Vendor Role' (Receiver (Edge - SUT)) and 'Metadata Included' (Limited Metadata).

5. To initiate XDR Test Case 3 – HITSP/C32's, the Tester (i.e., 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 3 -- HITSP/C32' step 1 interface. It displays the test purpose ('Verify the ability of the receiving system to correctly receive a properly formatted XDR message with Limited metadata. Attachment is a HITSP/C32 document.') and a 'Non TLS Endpoint' input field. A large red 'RUN' button is prominently displayed.

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.



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the 'TLS Endpoint' is provided by the Tester (e.g., Vendor).*

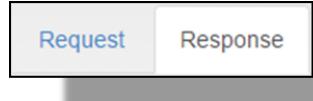
7. Once the XDR message has been sent, the Tester (e.g., Vendor) is prompted to manually validate if the test results conformed to the testing objective. To complete this, the Vendor clicks the **Waiting Validation** button.

The screenshot shows the 'XDR Test 3 -- HITSP/C32' step 3 interface. It displays the test purpose and a 'Logs' link. A large red 'WAITING VALIDATION' button is prominently displayed.

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 – HITSP/C32's, 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 HITSP/C32 document attachment.

```

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=H1#Boundary112233445566778899; type="application/xop+xml"; start="<doc0@ihexds.nist.gov>"; start-info="application/soap+xml"
Content-Length: 4467
Date: Wed, 10 Jun 2015 19:25:13 GMT

--H1#Boundary112233445566778899
Content-Type: application/soap+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <doc0@ihexds.nist.gov>

<Envelope xmlns="http://www.w3.org/2005/08/soap-envelope"><Header><action xmlns="http://www.w3.org/2005/08/soap-envelope">/s:Header</action><messageID>1-urn:uuid:112233445566778899</messageID><lastUpdated>2005-08-10T19:25:13Z</lastUpdated><uri>/s:Header</uri><Body><s:RegistryResponse xmlns="urn: oasisnames:tc:ebml-regrep:xsd:r3_0" status="urn:oasis:names:tc:ebml-regrep:ResponseStatusType:Failure"><s:RegistryErrorList><s:RegistryError codeContext="Document contents for document urn:uuid:8iced70-dae7-4e3d-8003-8381528c99ce not available in message" errorCode="XDSMissingDocument" location="" severity="urn:oasis:names:tc:ebml-regrep:ErrorSeverityType:Error" /></s:RegistryErrorList></s:RegistryResponse></Body></Envelope>

```

**Accept XDR**   **Reject XDR**

10. If the Tester (e.g., 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.



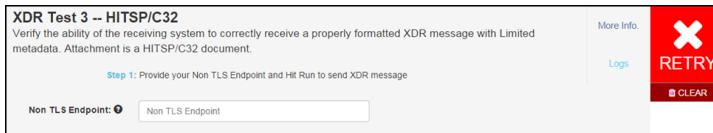
*Note: 'Accept XDR' selections correlate with Test Case Success results (e.g., green check mark). Likewise, 'Reject XDR' selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a 'Reject XDR' selection 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 of failure of a Test Case.

XDR message rejection results in a red X and prompts the Vendor to **Retry** the test (reference Step 1 within [Section 6.4.1.1 4a](#) to perform further retesting). 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.



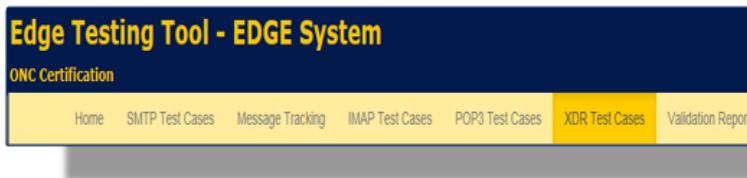
**Note:** In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The '**Validation Report**' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., 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 (reference [Section 2.4 Reporting](#)).



#### 7.6.3.1.3 3 – CCR

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 7 within [2.2 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.

Your System as: Receiver



*Note: 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 – CCR's intended focus, purpose/descriptions, conditional requirements, and expected test results, Tester (e.g., Vendor) role, and Metadata inclusion, click the **Description** link for the Test Case.

The screenshot shows a "Test #3" page. At the top left is a back arrow. The main content area has two columns: "Purpose/Description:" and "Expected Test Results:". Under "Purpose/Description:", there is a table with two rows. The first row contains the text "Verify that an Edge system can receive a properly formatted XDR message.". The second row contains the text "Edge system is capable of receiving and processing a valid message, test procedure may include other details for verification. Test Tool is satisfied with a good response.". Below this is a "Vendor Role" section with a table: "Receiver (Edge - SUT)" under "Role" and "Limited Metadata" under "Metadata Included".

5. To initiate XDR Test Case 3 – CCR, the Tester (i.e., 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.



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the **TLS Endpoint** is provided by the Tester (e.g., Vendor).*

7. Once the XDR message has been sent, the Tester (e.g., 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.



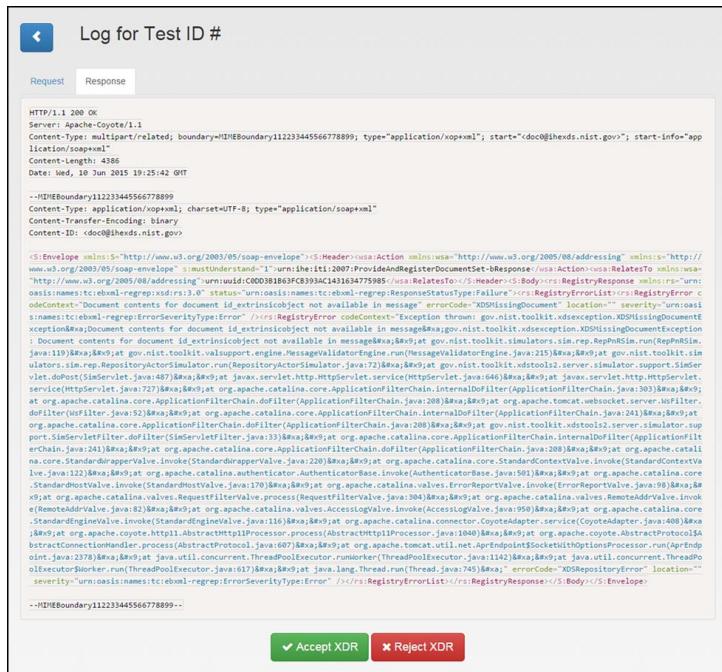
8. The Vendor is presented with the Test Case **Log** screen.



The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test Case 3 – CCR, the Vendor will select the **Response** tab to review the ETT logged response received from the SUT after the XDR message has been transmitted.



- 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 Continuity of Care Record document attachment.

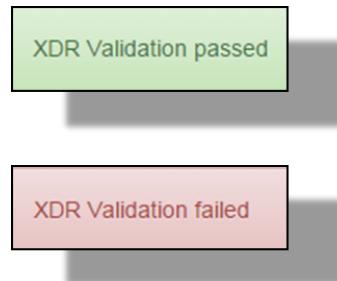


10. If the Tester (e.g., Vendor) accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected.



*Note: 'Accept XDR' selections correlate with Test Case Success results (e.g., green check mark). Likewise, 'Reject XDR' selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify 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 of failure of a Test Case.

XDR message rejection results in a red X and prompts the Vendor to **Retry** the test (reference Step 1 within [Section 6.4.1.1 4a](#) to perform further retesting). The Vendor can select the **Clear** button to reset the test.

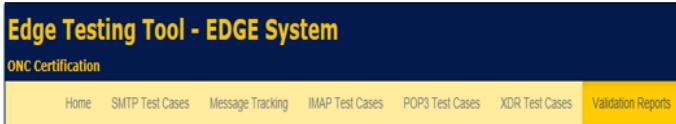
XDR Test 3 -- CCR  
Verify the ability of the receiving system to correctly receive a properly formatted XDR message with Limited metadata. Attachment is a Continuity of Care Record.  
Step 1: Provide your Non TLS Endpoint and Hit Run to send XDR message  
Non TLS Endpoint:  Non TLS Endpoint  
More Info. [Log in](#) RETRY

XDR message acceptance results in a green check. The Vendor can select the **Clear** button to reset the test.



**Note:** In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The '**Validation Report**' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., 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 (reference [Section 2.4 Reporting](#)).



#### 7.6.4 XDR TEST CASE 4

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:

- The Tester (i.e., 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.
- 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 2.3 Profile Creation](#) of this ETT User Guide).
- 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 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 is a **required test** and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.

This test correlates to Test ID 4 of the XDR Test Cases tab within the [DirectEdgeProtocols](#) 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 2015 Edition approved Test Procedure requirements document](#).

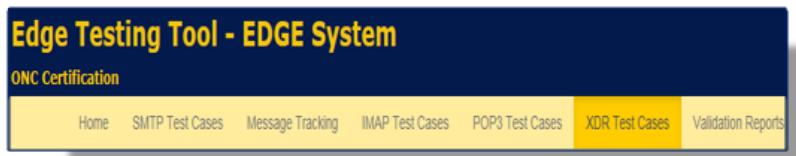
Comment [a11]: Need Link

#### 7.6.4.1 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.

##### 7.6.4.1.1 4a

14. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 7 within [2.2 Registration](#).
15. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.



16. From the testing options available, select **Your System as: Receiver**. This will enable test case selection.

Your System as: Receiver



*Note: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

17. To gain additional information concerning a target XDR Test Case 4a's intended focus, purpose/descriptions, conditional requirements, and expected test results, Tester (e.g., Vendor) role, and Metadata inclusion, click the **Description** link for the Test Case.

18. To initiate XDR Test Case 4a, the Tester (i.e., 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.

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



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the **'TLS Endpoint'** is provided by the Tester (e.g., Vendor).*

20. Once the XDR message has been sent, the Tester (e.g., 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.



21. 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.



22. 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 header.

Log for Test ID #

Request Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/soap+xml
Content-Length: 1013
Date: Tue, 09 Jun 2015 18:12:03 GMT

<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope">
  <S:Header>
    <wsa:Action s:mustUnderstand="1" xmlns:wsa="http://www.w3.org/2005/08/addressing">urn:sheiti:2007:ProvideAndRegisterDocumentSet-bResponse:/wsa:Action</wsa:Action>
    <wsa:RelatesTo xmlns:wsa="http://www.w3.org/2005/08/addressing">2f5037bf-b64c-445e-87fc-f27bcbbad60</wsa:RelatesTo>
  </S:Header>
  <S:Body>
    <fault:Fault xmlns:fault="http://www.w3.org/2003/05/soap-envelope">
      <fault:Code>
        <fault:Value>fault:Sender</fault:Value>
      </fault:Code>
      <fault:Reason>
        <fault:Text>calllangs.en</fault:Text>Problem parsing input in validator gov.nist.toolkit.valregmsg.message.HttpMessageValidator[Parsing HTTP message ()], Requested message type requires SIMPLE SOAP format message - HTOM format found[ITI TF Volumes 2a and 2b], Scheduling HTOM parser().</fault:Text>
      </fault:Reason>
    </fault:Fault>
  </S:Body>
</S:Envelope>
```

Accept XDR    Reject XDR

23. If the Tester (e.g., 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.



*Note: 'Accept XDR' selections correlate with Test Case Success results (e.g., green check mark). Likewise, 'Reject XDR' selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a 'Reject XDR' selection correlate with a Test Success).*

24. The ETT presents Vendor conformation based upon the selection made.

XDR Validation passed



25. 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 (reference Step 1 within [Section 6.4.1.1 4a](#) to perform further retesting). 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:** In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The '**Validation Report**' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., Vendor) to validate the acceptance of the message received by the SUT.

26. All completed testing session data is then available through the ETT's **Validation Report** tab (reference [Section 2.4 Reporting](#)).



#### 7.6.4.1.2 4b

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 7 within [2.2 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.

**Your System as: Receiver**



*Note: 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, conditional requirements, and expected test results, Tester (e.g., Vendor) role, and Metadata inclusion, click the **Description** link for the Test Case.

Purpose/Description:	Expected Test Results:
Verify that the Edge system throws an error when an incorrect message is received.	

Vendor Role	Metadata Included
Receiver (Edge - SUT)	N/A

5. To initiate XDR Test Case 4b, the Tester (i.e., 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.



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the 'TLS Endpoint' is provided by the Tester (e.g., Vendor).*

7. Once the XDR message has been sent, the Tester (e.g., 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.



- 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.

The screenshot shows a "Log for Test ID #" interface. It has tabs for "Request" and "Response". The "Request" tab is selected, displaying a SOAP message log entry. The "Response" tab is also visible. At the bottom are "Accept XDR" and "Reject XDR" buttons.

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=HMEBoundary112233445566778899; type="application/xop+xml"; start=<doc@ihexds.nist.gov>; start-info=<app
location/soap+xml>
Content-Length: 2301
Date: Wed, 10 Jun 2015 18:49:32 GMT

--HMEBoundary112233445566778899
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <doc@ihexds.nist.gov>

<Envelope xmlns="http://www.w3.org/2005/08/soap-envelope"><Header><action>urn:oasis:names:tc:ebms:metadata:1:urn:ibm:it1:2007:ProviderMetadataDocument</action><messageID>urn:ibm:it1:2007:ProviderMetadataDocument</messageID><to>http://www.oa3.org/2005/08/addressing/><relatesTo>/S:Header</relatesTo></Header><Body><rs:RegistryResponse xmlns:rs="urn:oasis
names:tc:ebms:regrp:xs:rs:1.0" status="urn:oasis:names:tc:ebms:regrp:ResponseStatusType:failure"><rs:RegistryErrorList><rs:RegistryError codeC
ontext="DocumentEntry(id extrinsicObject): the code HTTPS/CB0(CB0|34133-9) is not found in the Affinity Domain configuration" errorCode="XDSRegistryMetad
ataError" location="CodeValidation" severity="urn:oasis:names:tc:ebms:regrp:ErrorSeverityType:Error" /><rs:RegistryError codeContext="DocumentEntry
(id extrinsicObject): the code HTTPS/CB0(N) is not found in the Affinity Domain configuration" errorCode="XDSRegistryMetadataError" location="CodeVal
idation" severity="urn:oasis:names:tc:ebms:regrp:ErrorSeverityType:Error" /><rs:RegistryError codeContext="DocumentEntry(id extrinsicObject): the c
ode HTTPS/CB0(CB0|34133-9) is not found in the Affinity Domain configuration" errorCode="XDSRegistryMetadataError" location="CodeValidation" seve
rity="urn:oasis:names:tc:ebms:regrp:ErrorSeverityType:Error" /><rs:RegistryError codeContext="DocumentEntry(id extrinsicObject): the code Connect-a-thon p
racticeSettingCodes(4088439003) is not found in the Affinity Domain configuration" errorCode="XDSRegistryMetadataError" location="CodeValidation" seve
rity="urn:oasis:names:tc:ebms:regrp:ErrorSeverityType:Error" /><rs:RegistryError codeContext="SubmissionSeturnuuid:9b0d4590-6975-43bf-81e8-9cf170
1d0f10": the code HTTPS/CB0(CB0|34133-9) is not found in the Affinity Domain configuration" errorCode="XDSRegistryMetadataError" location="CodeValidation"
severity="urn:oasis:names:tc:ebms:regrp:ErrorSeverityType:Error" /></rs:RegistryErrorList></rs:RegistryResponse></Body></Envelope>
```

- If the Tester (e.g., 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.



*Note: 'Accept XDR' selections correlate with Test Case Success results (e.g., green check mark). Likewise, 'Reject XDR' selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a 'Reject XDR' selection correlate with a Test Success).*

- 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 of failure of a Test Case.

XDR message rejection results in a red X and prompts the Vendor to **Retry** the test (reference Step 1 within [Section 6.4.1.1 4a](#) to perform further retesting). 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:** In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The '**Validation Report**' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., 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 (reference [Section 2.4 Reporting](#)).



#### 7.6.4.1.3 4c

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 7 within [2.2 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.

Your System as: Receiver



*Note: 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 4c's intended focus, purpose/descriptions, conditional requirements, and expected test results, Tester (e.g., Vendor) role, and Metadata inclusion, click the **Description** link for the Test Case.

The screenshot shows a "Test #4" page. At the top left is a back arrow. The title "Test #4" is centered. Below the title are two input fields: "Purpose/Description:" containing "Verify that the Edge system throws an error when an incorrect message is received" and "Expected Test Results:" which is empty. At the bottom are two tables: "Vendor Role" with "Receiver (Edge - SUT)" and "Metadata Included" with "N/A".

5. To initiate XDR Test Case 4c, the Tester (i.e., 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.



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the 'TLS Endpoint' is provided by the Tester (e.g., Vendor).*

7. Once the XDR message has been sent, the Tester (e.g., 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 4c, the Vendor will select the **Response** tab to review the ETT logged response received from the SUT after the XDR message has been transmitted.



- 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 a missing Direct Address Block.

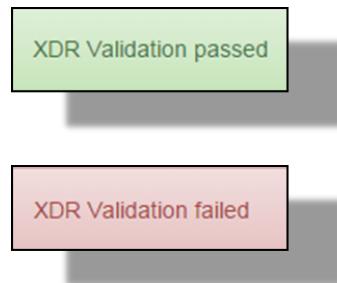


- If the Tester (e.g., Vendor) accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected.



**Note:** ‘Accept XDR’ selections correlate with Test Case Success results (e.g., green check mark). Likewise, ‘Reject XDR’ selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify 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 (reference Step 1 within [Section 6.4.1.1 4a](#) to perform further retesting). The Vendor can select the **Clear** button to reset the test.

XDR Test 4c  
Verify the ability of the receiving system to appropriately respond to a malformed message. This case is of a missing Direct Address Block.  
Step 1: Provide your Non TLS Endpoint and Hit Run to send XDR message  
Non TLS Endpoint:  More Info. Logos RETRY CLEAR

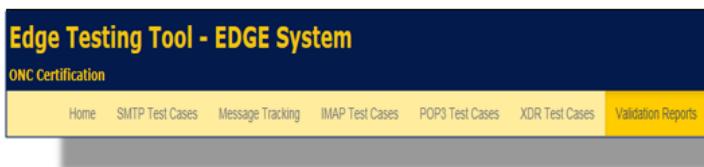
XDR message acceptance results in a green check. The Vendor can select the **Clear** button to reset the test.

XDR Test 4c  
Verify the ability of the receiving system to appropriately respond to a malformed message. This case is of a missing Direct Address Block.  
More Info. Logos  CLEAR



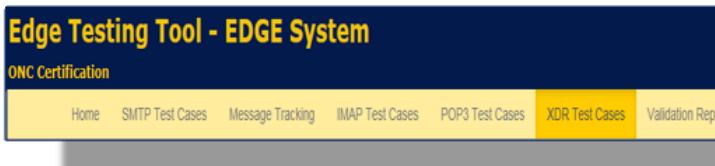
**Note:** In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The '**Validation Report**' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., 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 (reference [Section 2.4 Reporting](#)).



#### 7.6.4.1.4 4d

1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 7 within [2.2 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.

Your System as: Receiver



**Note:** 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 4d's intended focus, purpose/descriptions, conditional requirements, and expected test results, Tester (e.g., Vendor) role, and Metadata inclusion, click the **Description** link for the Test Case.

The screenshot shows a test configuration page for 'Test #4'. It includes fields for 'Purpose/Description' (Verify that the Edge system throws an error when an incorrect message is received), 'Expected Test Results' (a text area), 'Vendor Role' (Receiver (Edge - SUT)), and 'Metadata Included' (N/A). A back arrow is visible at the top left.

5. To initiate XDR Test Case 4d, the Tester (i.e., 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 initial step of running the test. It displays the test description, a 'Step 1' instruction to provide a Non TLS Endpoint, and a large red 'RUN' button. A 'More Info.' link and a 'Logout' button are also present.

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.

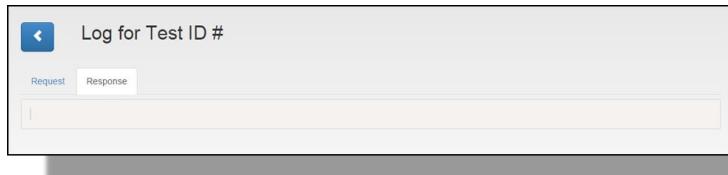


*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the 'TLS Endpoint' is provided by the Tester (e.g., Vendor).*

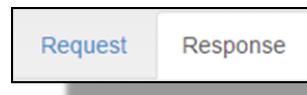
7. Once the XDR message has been sent, the Tester (e.g., Vendor) is prompted to manually validate if the test results conformed to the testing objective. To complete this the Vendor clicks the '**Waiting Validation**' button.



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 4d, 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 missing XDR metadata.

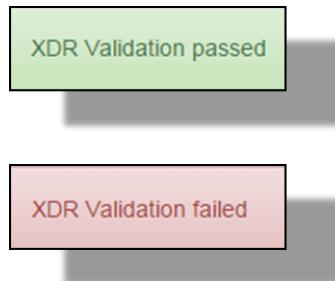


10. If the Tester (e.g., Vendor) accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected.



*Note: 'Accept XDR' selections correlate with Test Case Success results (e.g., green check mark). Likewise, 'Reject XDR' selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify 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 of failure of a Test Case.

XDR message rejection results in a red X and prompts the Vendor to **Retry** the test (reference Step 1 within [Section 6.4.1.1 4a](#) to perform further retesting). The Vendor can select the **Clear** button to reset the test.

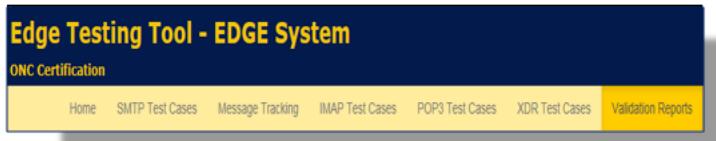


XDR message acceptance results in a green check. The Vendor can select the **Clear** button to reset the test.



**Note:** In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The '**Validation Report**' represents the aggregation of all Test Cases executed and result outcomes. This enables the Tester (e.g., 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 (reference [Section 2.4 Reporting](#)).



### 7.6.5 XDR TEST CASE 5

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:

- The Tester (i.e., 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.
- 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 communicate to execute this Test Case; reference [2.3 Profile Creation](#)).
- 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 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 is a **required test** and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Sections 1.1 of the [Implementation Guide for Direct Edge Protocols](#) document.

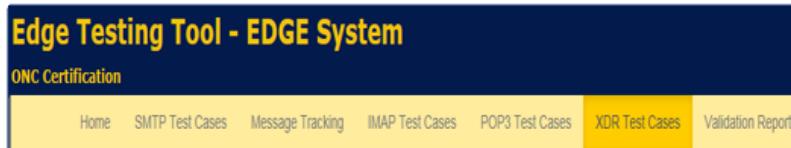
This test correlates to Test ID 5 of the XDR Test Cases tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 4.04 within the [ONC 2015 Edition approved Test Procedure requirements document](#).

Comment [a12]: Need link

#### 7.6.5.1 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 7 within [2.2 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.

Your System as: Receiver



*Note: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

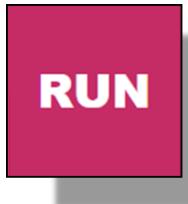
4. To gain additional information concerning XDR Test 5’s intended focus, purpose/descriptions, conditional requirements, and expected test results, Tester (e.g., Vendor) role, and Metadata inclusion, click the **Description** link for the Test Case.

The screenshot shows the configuration for Test #5. It includes fields for Purpose/Description (Verify that an Edge system can receive a properly formatted XDR message) and Expected Test Results (Edge system is capable of receiving and processing a valid message with Full Metadata, test procedure may include other details for verification. Test Tool is satisfied with a good response). It also lists Vendor Role (Receiver (Edge - SUT)) and Metadata Included (Full Metadata).

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 Test ID #5 screen with the 'Run' button highlighted in red.

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



*Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the 'TLS Endpoint' is provided by the Tester (e.g., Vendor).*

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 screenshot shows the Test ID #5 screen with the 'Waiting Validation' button highlighted in red.

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 determine if the SUT provided the appropriate testing objective responses for receiving a properly formatted XDR message with Full XDS metadata.

A screenshot of a web-based log viewer titled "Log for Test ID #5". At the top, there are two tabs: "Request" (which is dark grey) and "Response" (which is light grey). The main area displays a detailed log entry. The log starts with a header:

HTTP/1.1 200 OK  
Server: Apache-Coyote/1.1  
Content-Type: multipart/related; boundary=-----Boundary112233445566778899; type="application/xop+xml"; start=<doc@ihxds.nist.gov>; start-info=<application/soap+xml>  
Content-Security-Policy: default-src='self'; frame-src='https://www.nist.gov'; script-src='self' https://www.nist.gov'; object-src='none'; style-src='self' https://www.nist.gov'; font-src='self' https://www.nist.gov'; img-src='self' https://www.nist.gov'; media-src='self' https://www.nist.gov';  
Content-Transfer-Encoding: chunked  
Date: Tue, 13 Jan 2015 16:49:39 GMT  
35F  
-----Boundary112233445566778899  
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"  
Content-Transfer-Encoding: binary  
Content-ID: <doc@ihxds.nist.gov>

Below the header is the XML content of the SOAP envelope:

```
<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope">  
  <S:Header>  
    <ns1:Action ns1="http://www.w3.org/2003/05/soap-envelope">  
      <ns1:mustUnderstand>1</ns1:mustUnderstand>  
      <ns1:uri>urn:uuid:5d449953-a691-4ba3-8270-569bc053604</ns1:uri>  
    </S:Header>  
  <S:Body>  
    <ns1:RegistryResponse status="urn:oasis:names:tc:ebml-regrep:ResponseStatusType:Success"  
      <ns1:uri>urn:oasis:names:tc:ebml-regrep:xdris:3.0</ns1:uri>  
    </S:Body>  
</S:Envelope>
```

-----Boundary112233445566778899--

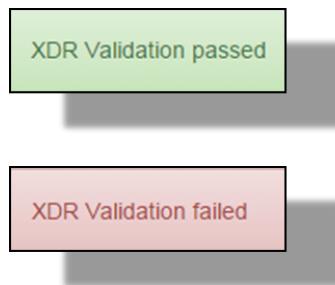
9. If the Tester (e.g., Vendor) accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata, then the **Reject XDR** button is selected.





**Note:** ‘Accept XDR’ selections correlate with Test Case Success results (e.g., green check mark). Likewise, ‘Reject XDR’ selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a ‘Reject XDR’ selection correlate with a Test Success).

10. The ETT presents Vendor conformation 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 (reference Step 1 within [Section 6.5.1](#) to perform further retesting). The Vendor can select the **Clear** button to reset the test

Test ID #5  
Verify that an Edge system can receive a properly formatted XDR message.  
Step 1: Provide your endpoint and hit Run to send XDR  
Logs **RETRY**  
Endpoint:

XDR message acceptance results in a green check. The Vendor can select the **Clear** button to reset the test.

Test ID #5  
Verify that an Edge system can receive a properly formatted XDR message.  
Logs **✓**



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