June 26, 2015
Revision 1.6

USER GUIDE

# Edge Testing Tool

National Institute of Standards and Technology

# Table of Contents

# 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) [1] (and forthcoming Stage 3 (MU3) [2])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 R2 Edition of the ONC Standards & Certification Criteria[3]. 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).

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 R2 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 2014 MU2 R2 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 HISP 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.

Figure 1 below depicts the high level testing objectives the ETT and TTT perform in relationship to one another and EHR / HISP interaction.

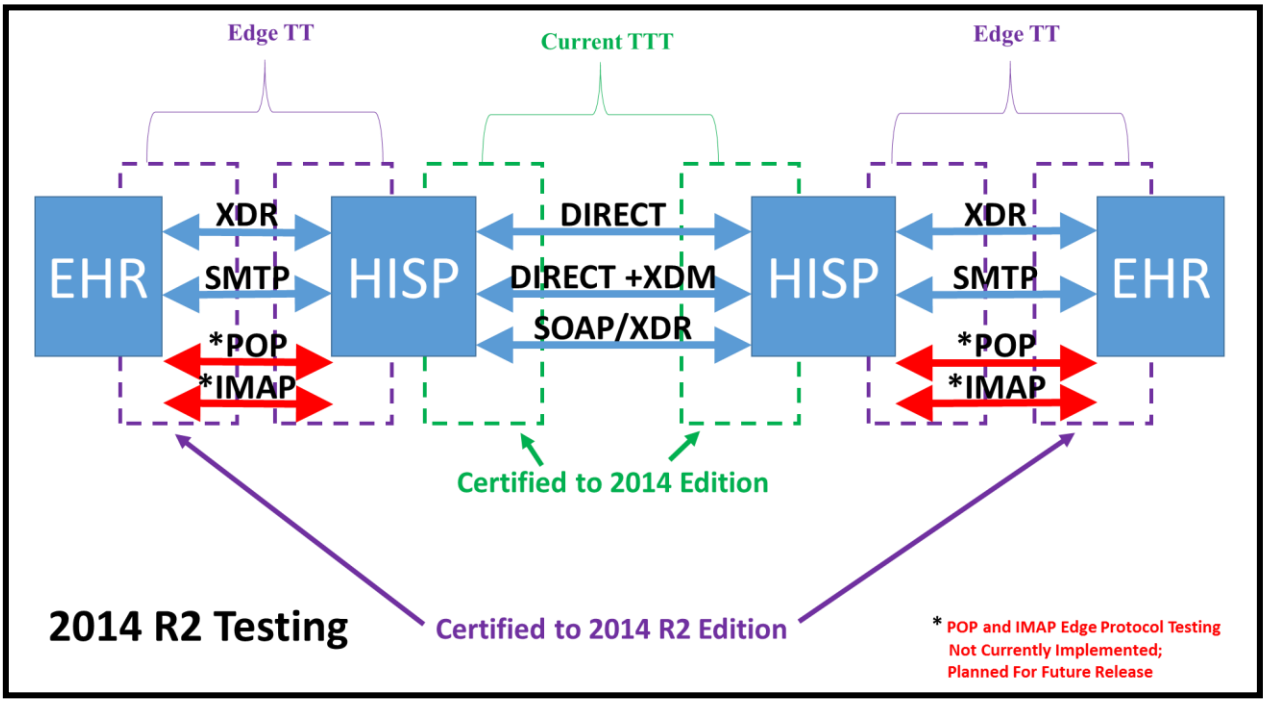



**Figure 1: Testing Certification Criteria**

An Edge System (e.g., EHR) or HISP 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.

***Note**: In the current build of the ETT, the features and capabilities for testing POP and IMAP against Edge Protocols for certification testing are not implemented. However, this is planned for the next major build/release.*

Within the scope of testing and Test Procedure context for ETT Test Cases, the term 'SUT' in commonly used in an abstract form. The SUT can act as either an Edge System (e.g., EHR) or HISP, 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 HISP 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'. The ETT User Guide describes the 2014 MU R2 Edition of the ONC Standards & Certification Criteria[2] processes.
- **Local Interface –** A downloadable and executable file (.WAR) is not currently available for the ETT. However, this functionality will be enabled in future releases of the tool.

***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 has ETT's latest code; however, documentation, content, and testing engine availability cannot be guaranteed. Thus, the development version will up 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 HISP or Edge System) dependent upon specific 2014 MU2 R2 Edge Protocol testing objectives. The identified objectives that have been selected and outlined for testing purposes are:

- **170.314(b)(8)** Transitions of Care, Optional (*Optional*); and
- **170.314(e)(1)** View, Download, Transmit to 3rd Party (*Edge Protocol Testing*).

# 2.0 TESTING CONFIGURATION FOR EDGE SYSTEM

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

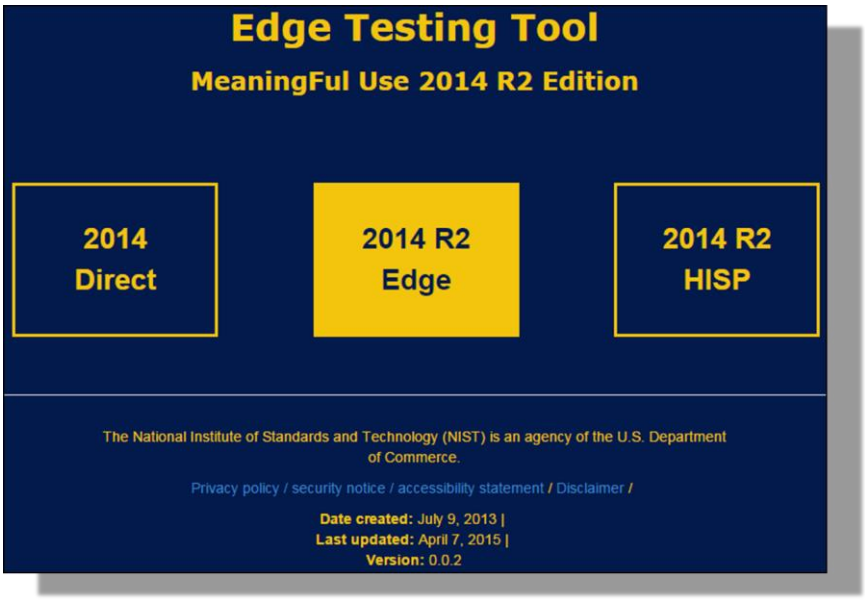
## 2.1 Configuration Steps

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 **2014 R2 Edge** option.

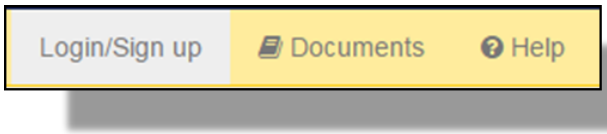


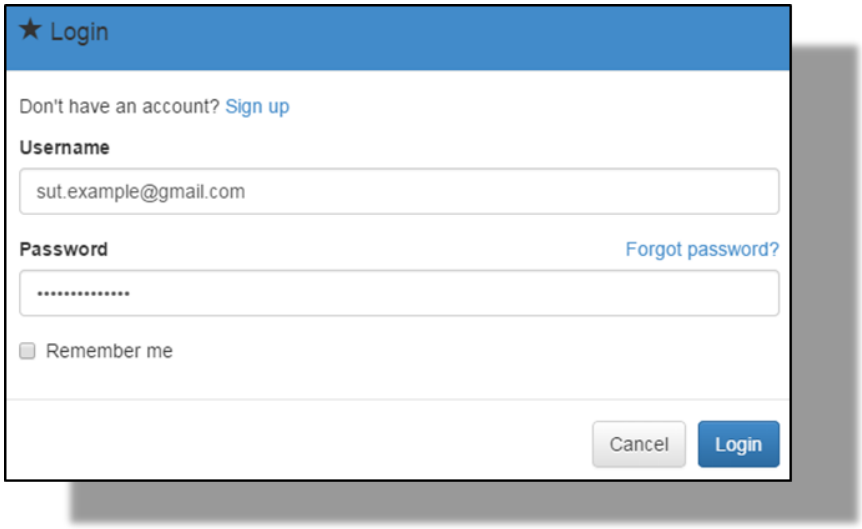

***Note**: The ETT **Date Created**, most recent and **Last Update**, and current **Version** can be found at the bottom of the ETT's Welcome Screen.*

3. Selecting the **2014 R2 Edge** option will bring up the tool's Welcome Screen. From here, the Vendor can select the intended MU2 2014 R2 Test Case(s) that will be targeted to test against.

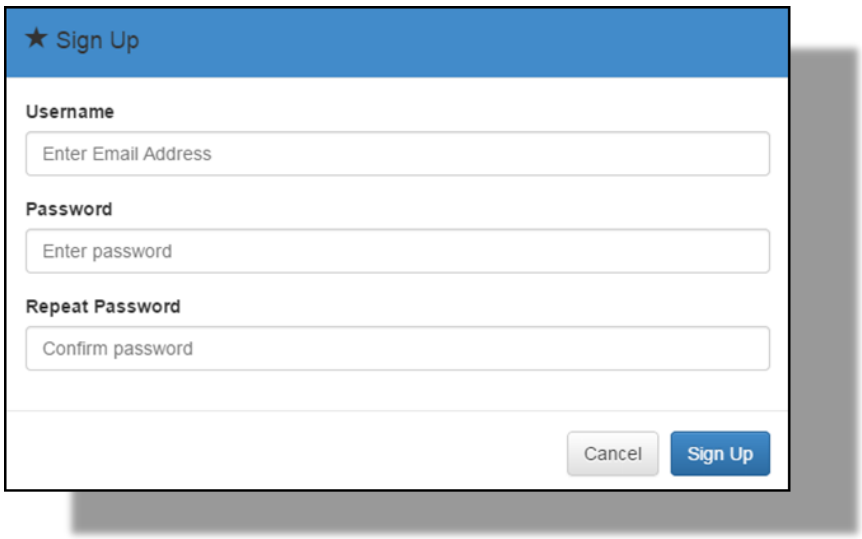
***Note**: In its current version and build, the ETT supports the functionality and feature sets to test against the loaded Simple Mail Transfer Protocol (SMTP), Cross-Enterprise Document Reliable Interchange (XDR), and tracking of Message Disposition Notifications (MDNs) using SMTP and XDR.*

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**.



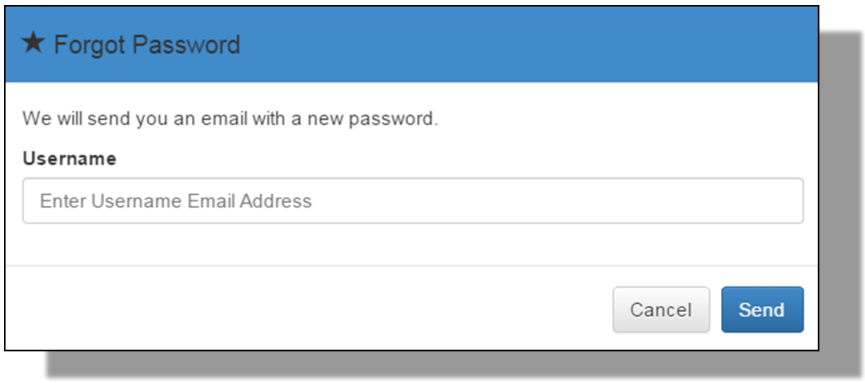

Before executing any tests within the ETT, **Login** using the credentials created during **Sign Up**.



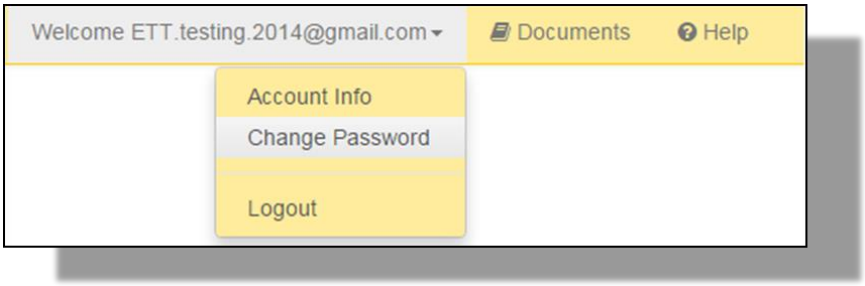

***Note**: The **Username** email address is used for account creation, historic testing session saves, and delivery notification of ETT specific information by NIST personnel. It is not specifically used as a component of SMTP and/or XDR testing. Testing email addresses are configured within specific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

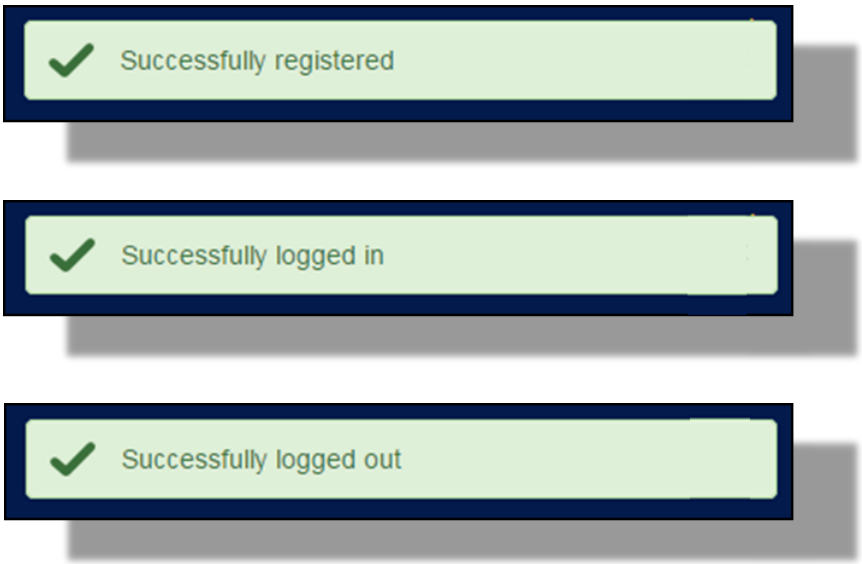


An account **Password** can also be reset through the Navigation Bar after successful **Login**.




***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.*

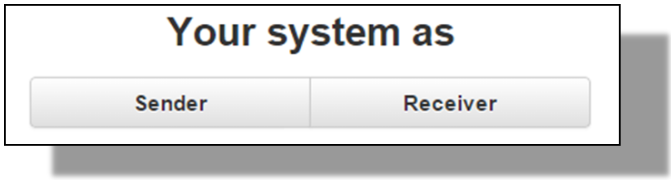
7. A success message will appear upon successful **Sign Up**, **Login**, and **Logout**.




## 2.3 Profile Creation

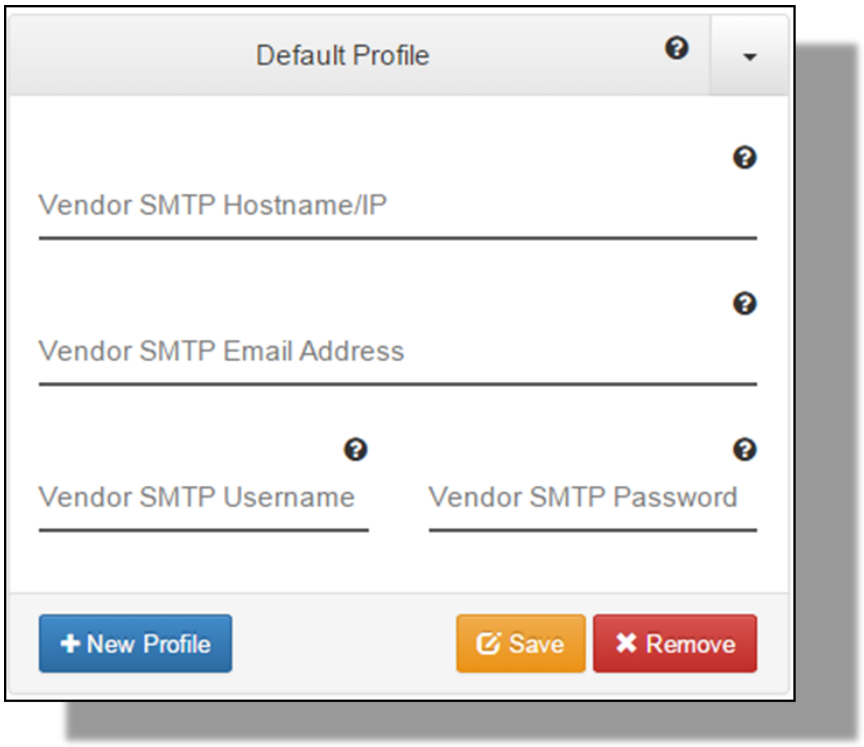
1. Select the SMTP or XDR target Test Case through the **SMTP Test Cases** or **XDR Test Cases** links on the Navigation Bar. This enables the testing Profile feature of the ETT.


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

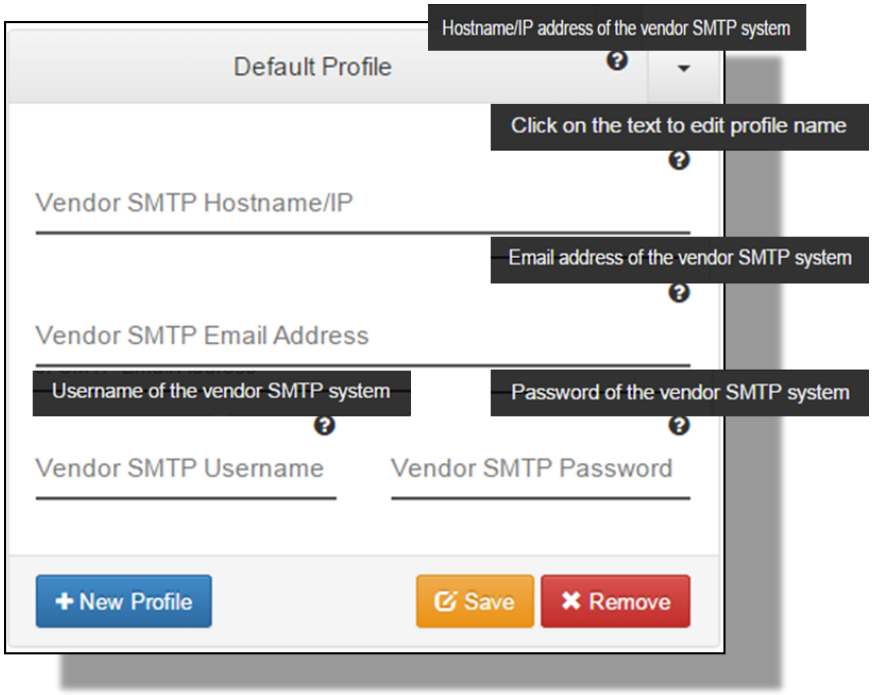



3. From the testing **Profile**, enter the:

| Profile Data Field | Description |
|---|---|
| **Profile Name** | The Profile name can be edited and customized based on testing needs by the Vendor. This feature can be accessed by clicking on the **Profile** header. Saved Profiles can be accessed from within the ETT account created during 2.2 Registration. |
| **Vendor SMTP Hostname / IP** | SMTP or IP address of the Vendor's email server. This should directly connect with the **Vendor SMTP Email Address** |
| **Vendor SMTP Email Address** | **Vendor SMTP Email Address** should correspond to the **Vendor SMTP Hostname / IP**. This email address will be used to send/receive ETT SMTP Test Case validation messages. |
| **Vendor SMTP Username and Password** | These should correspond to the **Vendor SMTP Email Address**. The Username and Password are mainly used for authentication based Test Cases so the ETT can login to the SUT. |

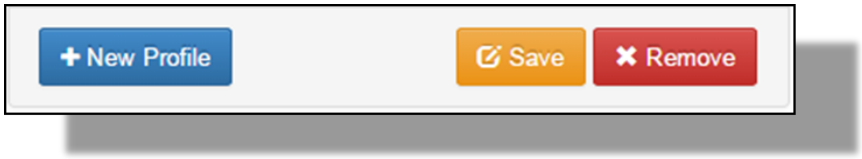



Hovering over the **?** for each **Profile** data field reveals a pop-up containing further explanation/instruction.



***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.*

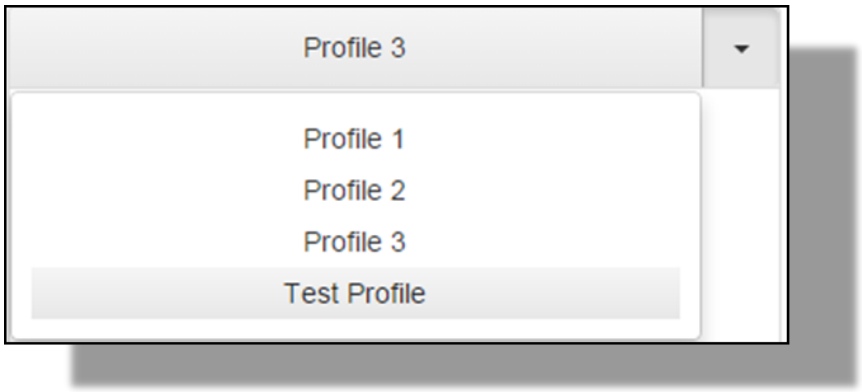
4. Before saving a Profile, assign a unique name (the default Profile name is **Default Profile**). Click the Profile name, delete the existing text, and type a new name. Upon population of the testing Profile, select **Save**. To delete a saved Profile, select **Remove**




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



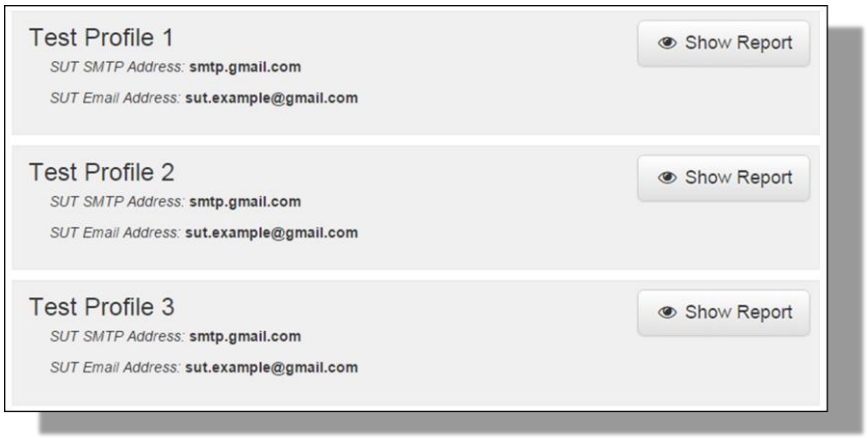
6. Saved Profiles can be retrieved and applied to subsequent/future tests by selecting the target Profile from the drop-down menu.




## 2.4 Reporting

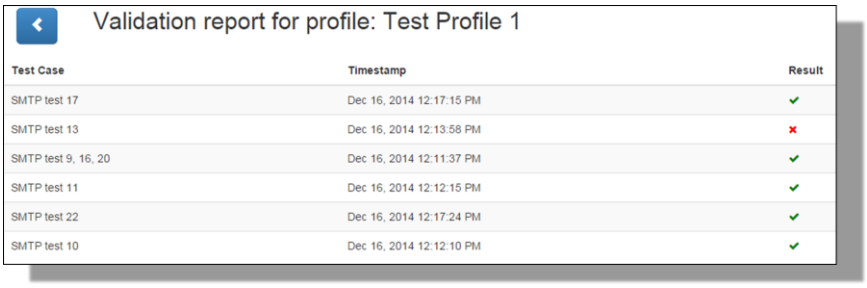
1. During a testing session, the Vendor can review a high-level synopsis of all Test Cases executed through the '**Validation Reports**' tab on the Navigation Bar.


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.



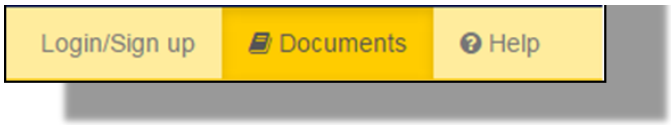

***Note**: For a given testing session, the total number of ETT testing **Profiles** used will be displayed within the **Validation Report** tab.*

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.




## 2.5 Documentation

Documentation relevant to the ETT, Test Case execution (including this ETT User Guide), Test Procedures, 2014 MU2 R2 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.


Login/Sign up
Documents
Help

# 3.0 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 |

## 3.1 SMTP Test Case 14

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. 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 2014 Edition approved Test Procedure requirements document.

### 3.1.1 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.*

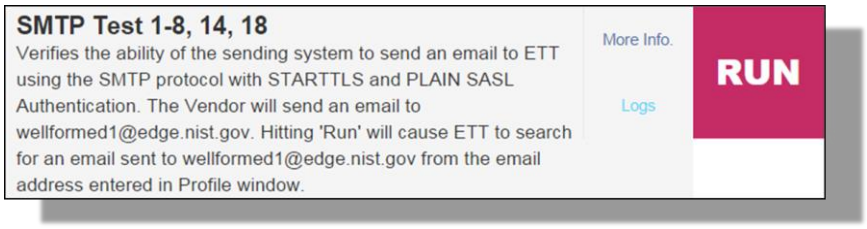
1. Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 7 within 2.2 Registration.

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

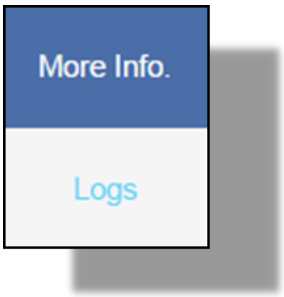

3. From the testing Profile, select **Sender**.

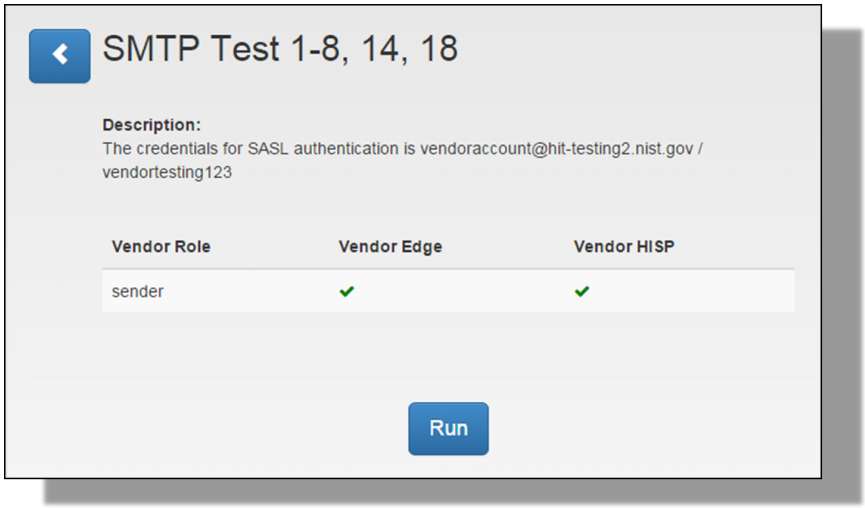

   Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 5 within 2.3 Profile Creation.

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.



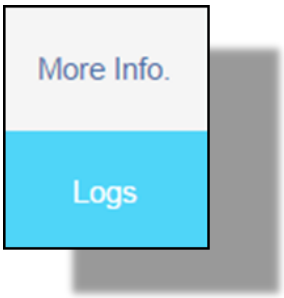

5. With the Profile saved, More Info reviewed, and **SMTP Test 1-8, 14, 18** selected, the Vendor performs the following Test Steps:
    A. Navigate the to SUT's messaging client/interface for **Vendor SMTP Email Address** (specified in the Profile).
    B. Create a single new message and send it to the ETT endpoint recipient wellformed1@edge.nist.gov.
    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**.

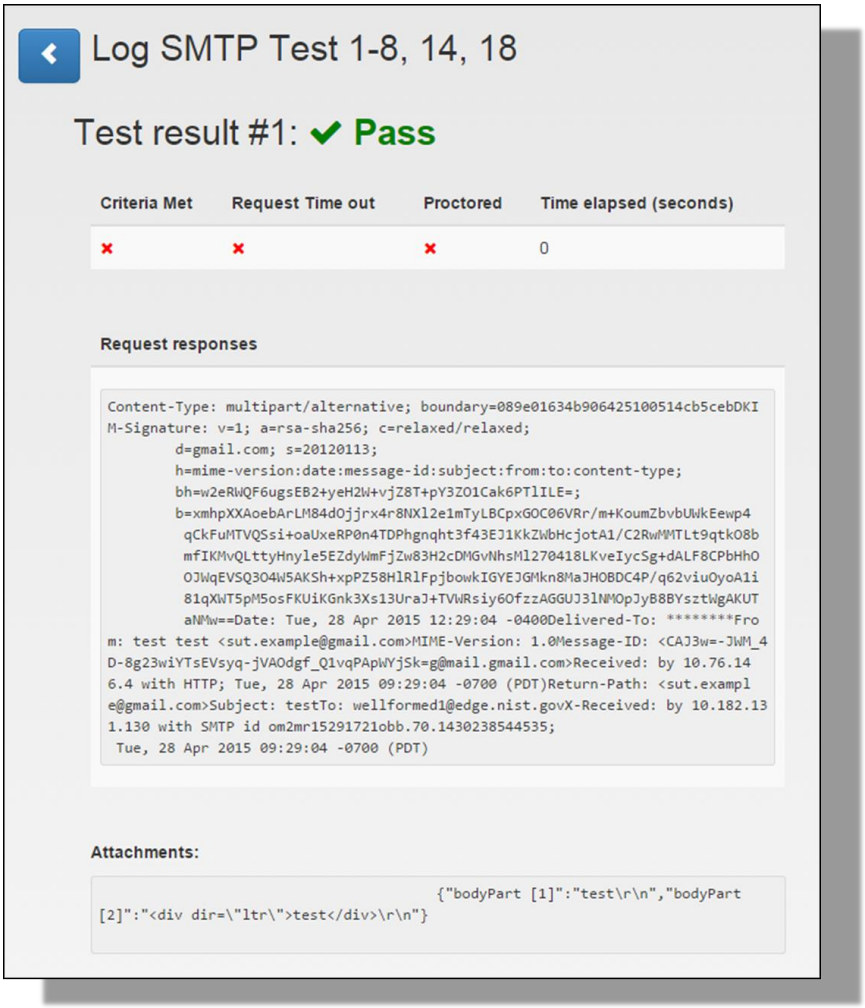
- A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
- A test Fail prompts the Vendor to **Retry** the test.
- The **Clear** button resets the test and any data input field values.


***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**.




***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.*

## 3.2 SMTP Test Case 18

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. 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 2014 Edition approved Test Procedure requirements document.

### 3.2.1 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.*

## 3.3 SMTP Test Cases 1 through 8

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. 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 2014 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.

| SMTP Test Case | Testing Objective / Conformance Test Detail |
|---|---|
| **1** | - The SUT will attempt to initiate a secure connection with the ETT and execute the correct SMTP sequence.<br>- The ETT will receive the SMTP protocol command sequence, perform validation, and initiate a successful connection with the SUT.<br>- The sequence of mail transaction connection commands will conform to the specified requirements within *RFC 2821, Section 3.1 (Session Initiation) and 4.1.1.1 (Extended HELO or EHLO)*. |
| **2** | - The SUT will attempt to send a HELO / EHLO command sequence to the ETT.<br>- The ETT will receive the HELO / EHLO command sequence, perform validation, and initiate a successful connection with the SUT.<br>- The sequence of mail transaction connection commands will conform to the specified requirements within *RFC 2821, Section 4.1.1.1 (Extended HELO or EHLO)*. |
| **3** | - The SUT will attempt to send the MAIL FROM, RCPT TO, and DATA command sequences to the ETT.<br>- The ETT will receive the MAIL FROM, RCPT TO, and DATA command sequences, perform validation, and initiate a successful connection with the SUT. |

| | |
|---|---|
| | - The sequence of mail transaction connection commands will conform to the specified requirements within *RFC 2821, Section 3.1 (Session Initiation)*. |
| **4** | - The SUT will attempt to send the MAIL command sequence to the.<br>- The ETT will receive the MAIL command sequence, perform validation, and initiate a successful connection with the SUT.<br>- The sequence of mail transaction connection commands will conform to the specified requirements within *RFC 2821, Section 4.1.1.2*. |
| **5** | - The SUT will attempt to send the RCPT TO command sequence to the ETT.<br>- The ETT will receive the RCPT TO command sequence, perform validation, and initiate a successful connection with the SUT.<br>- The sequence of mail transaction connection commands will conform to the specified requirements within *RFC 2821, Section 4.1.1.3*. |
| **6** | - The SUT will attempt to send the DATA command sequence to the ETT.<br>- The ETT will receive the DATA command sequence, perform validation, and initiate a successful connection with the SUT.<br>- The sequence of mail transaction connection commands will conform to the specified requirements within *RFC 2821, Section 2.3.7, 2.3.9, and 4.1.1.4*. |
| **7** | - The SUT will attempt to send the correctly formatted Domain Name command sequence to the ETT.<br>- The ETT will receive the correctly formatted Domain Name command sequence, perform validation, and initiate a successful connection with the SUT.<br>- The sequence of mail transaction connection commands will conform to the specified requirements within *RFC 2821, Section 2.3.5*. |
| **8** | - The SUT will attempt to send the correctly configured and formatted Mailbox and Address to the ETT.<br>- The ETT will receive the correctly configured and formatted Mailbox and Address, perform validation, and initiate a successful connection with the SUT.<br>- The sequence of mail transaction connection commands will conform to the specified requirements within *RFC 2821, Section 2.3.10 and 4.5.3.1*. |

### 3.3.1 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.*

## 3.4 SMTP MU2 Test Case 17

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 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. 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.

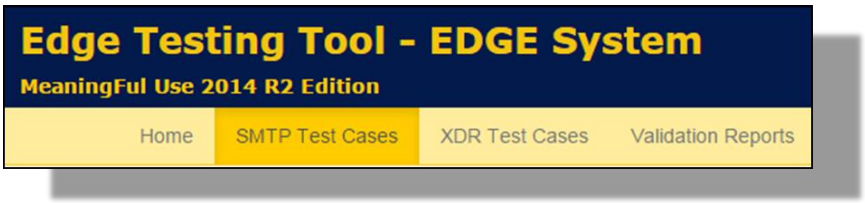
This test correlates to Test ID 17 of the MU Tracking tab within the *DirectEdgeProtocols* spreadsheet and TE170.314(b)(8) – 3.08 within the ONC 2014 Edition approved Test Procedure requirements document.

### 3.4.1 TESTING STEPS

To execute SMTP MU2 Test Case 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.

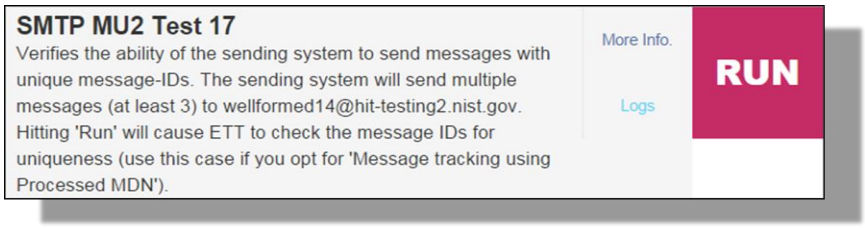
2. For this target SMTP MU2 test, select **SMTP Test Cases** from the Navigation Bar. This enables the testing Profile feature of the tool.



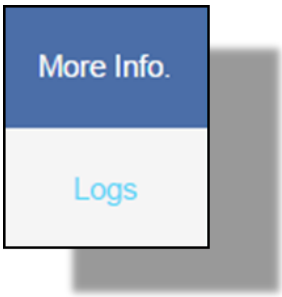

3. From the testing Profile, select **Sender**.

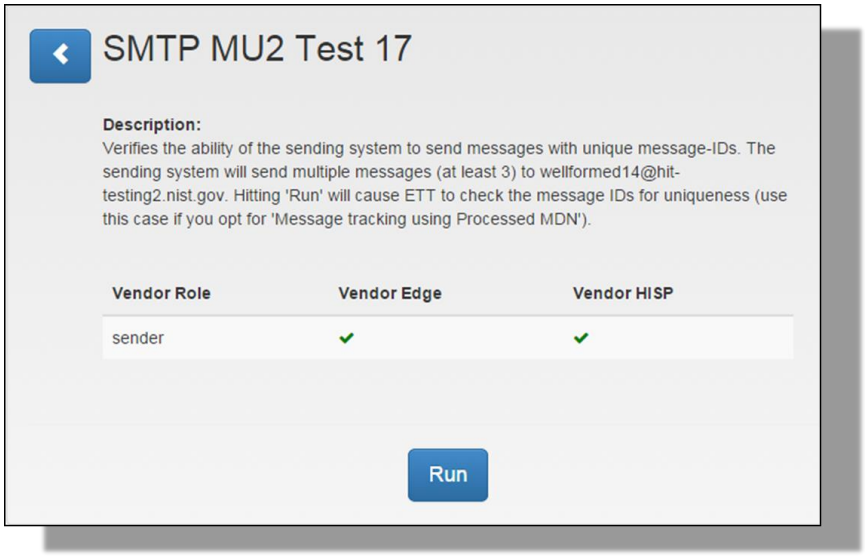

   Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 5 within 2.3 Profile Creation.

4. To initiate SMTP MU2 Test Case 17, the Vendor navigates to the Test Case's execution interface.




   To gain additional information concerning SMTP MU2 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 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.
    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.

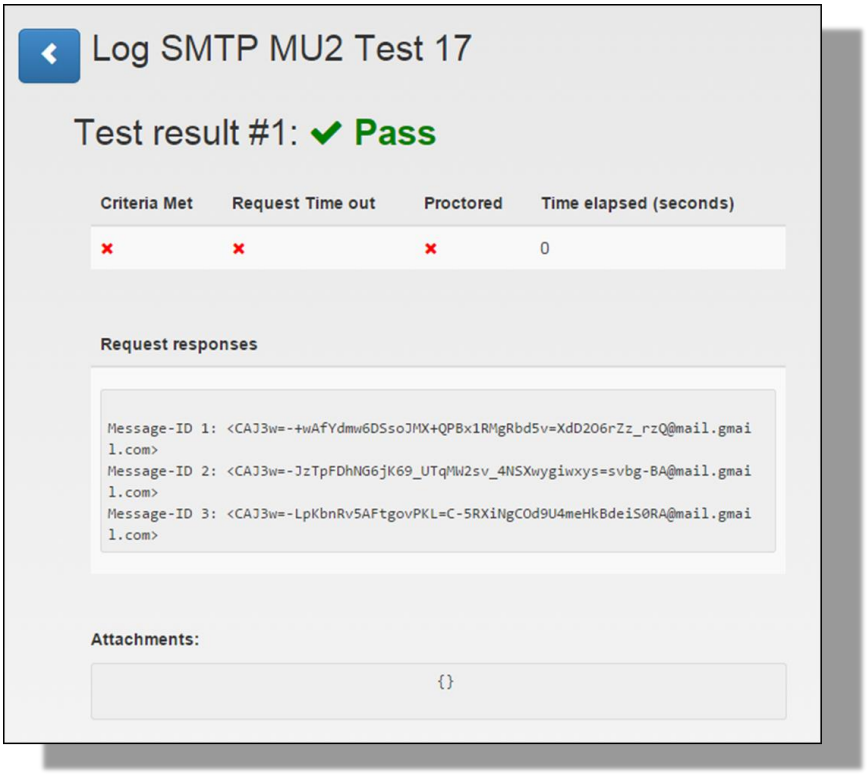

***Note**: SMTP MU2 Test 17 should be executed under the constraint that a Vendor/SUT opts for message tracking using processed MDNs.*

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**.




***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.*

## 3.5 SMTP MU2 Test Case 45

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 Delivery Notification for Direct v1.0* for delivery notification 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. 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.

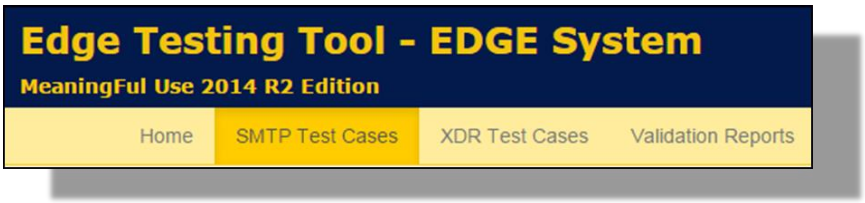
This test correlates to Test ID 45 of the MU Tracking tab within the *DirectEdgeProtocols* spreadsheet and TE170.314(b)(8) – 3.09 within the ONC 2014 Edition approved Test Procedure requirements document.

### 3.5.1 TESTING STEPS

To execute SMTP MU2 Test Case 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.

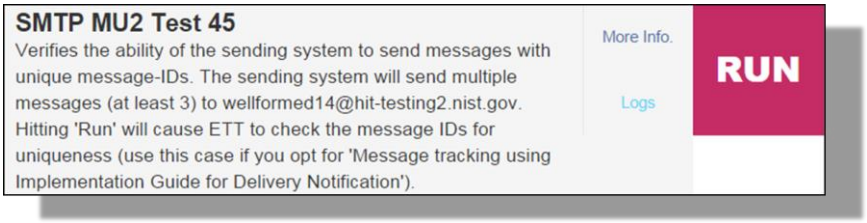
2. For this target SMTP MU2 test, select **SMTP Test Cases** from the Navigation Bar. This enables the testing Profile feature of the tool.



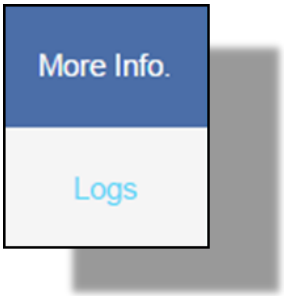
3. From the testing Profile, select **Sender**.

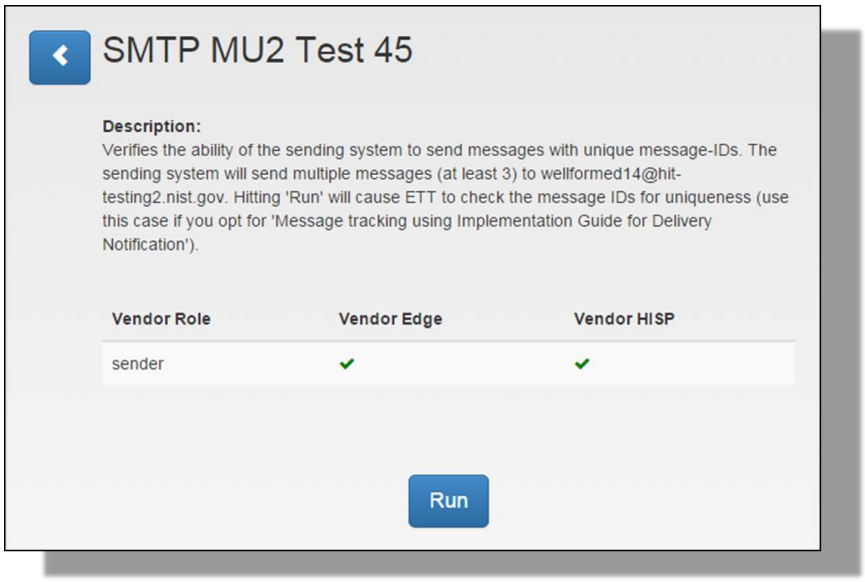

Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 5 within 2.3 Profile Creation.

4. To initiate SMTP MU2 Test Case 45, the Vendor navigates to the Test Case's execution interface.




To gain additional information concerning SMTP MU2 Test Case 45's intended purpose (including Description, Vendor/SUT roles), click **More Info** link for the Test Case.





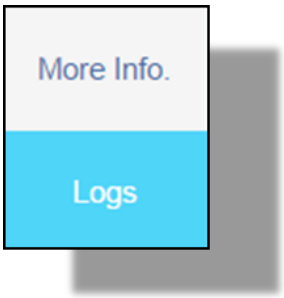

5. With the Profile saved, More Info reviewed, and **SMTP MU2 Test 45** selected, the Vendor performs the following Test Steps:
    A. Navigate the to SUT's messaging client/interface for **Vendor SMTP Email Address** (specified in the Profile).
    B. Create three (3) new messages.
        a. Each message 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.
    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.*

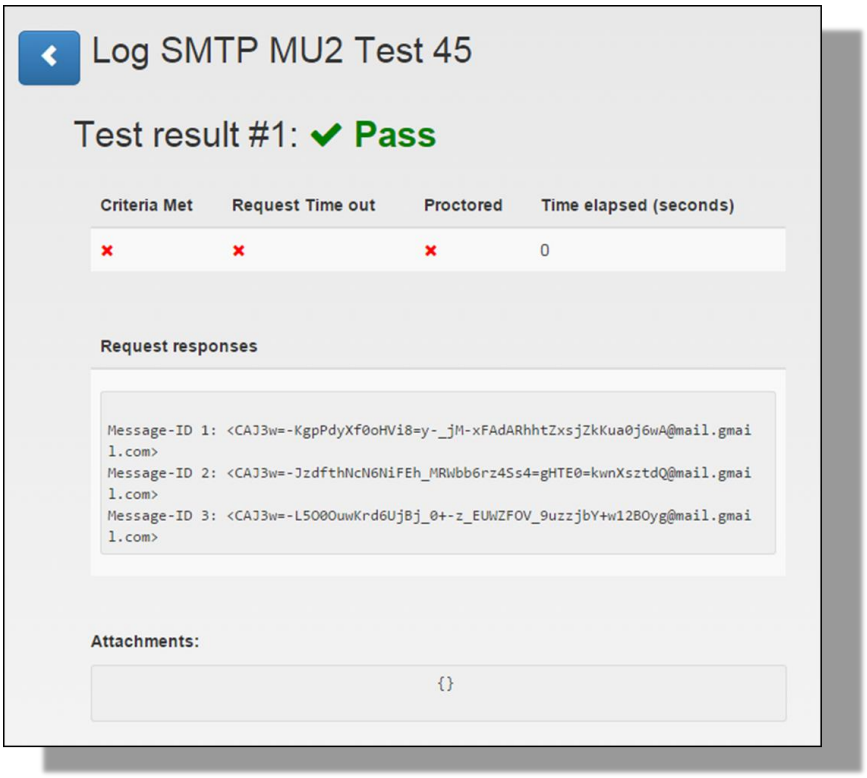
6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
   - A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
   - A test Fail prompts the Vendor to **Retry** the test.
   - The **Clear** button resets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




***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.*

## 3.6 SMTP MU2 Test Case 46

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 delivery notification 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. Upon the sending of each message, the SUT will generate and send a delivery notification message (containing the Disposition-Notification-Option header and processed MDN notification) to the ETT. The ETT will receive the 3 messages and delivery notification message (delivery notification 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 2014 Edition approved Test Procedure requirements document.

### 3.6.1 TESTING STEPS

To execute SMTP MU2 Test Case 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:

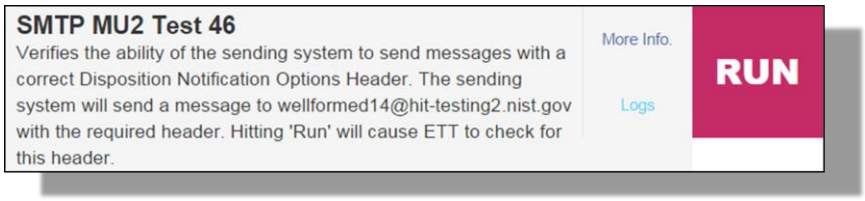
1. Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 7 within 2.2 Registration.

2. For this target SMTP MU2 test, select **SMTP Test Cases** from the Navigation Bar. This enables the testing Profile feature of the tool.

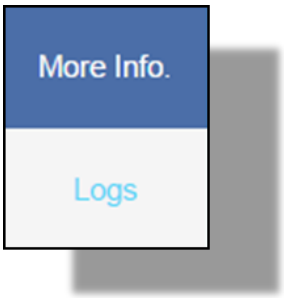

3. From the testing Profile, select **Sender**.

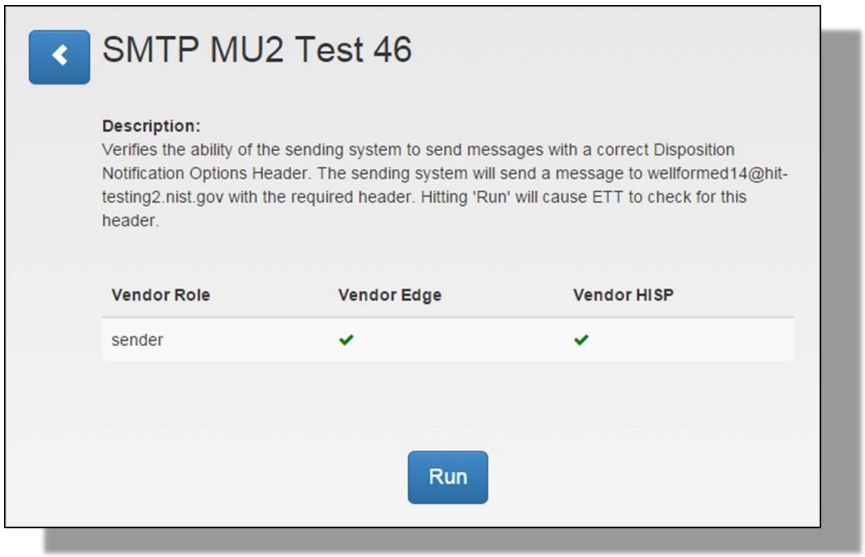

Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 5 within 2.3 Profile Creation.

4. To initiate SMTP MU2 Test Case 46, the Vendor navigates to the Test Case's execution interface.




To gain additional information concerning SMTP MU2 Test Case 46's intended purpose (including Description, Vendor/SUT roles), click **More Info** link for the Test Case.



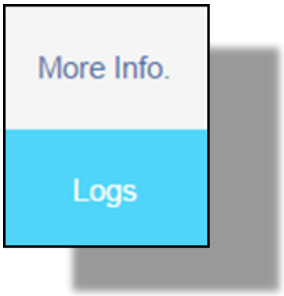



5. With the Profile saved, More Info reviewed, and **SMTP MU2 Test 46** selected, the Vendor performs the following Test Steps:
    A. Navigate the to SUT's messaging client/interface for **Vendor SMTP Email Address** (specified in the Profile).
    B. Create three (3) new messages.
        a. Each message 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.
    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.

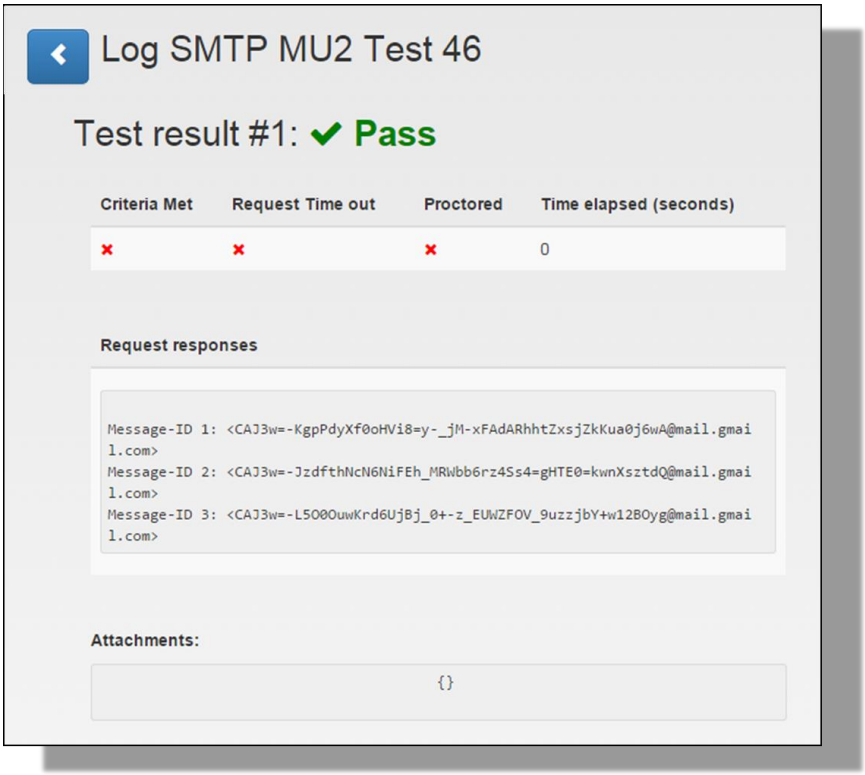

6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
    - A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
    - A test Fail prompts the Vendor to **Retry** the test.
    - The **Clear** button resets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



***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.*

## 3.7 SMTP MU2 Test Case 47

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 and wellformed14@hit-testing2.nist.gov. The available **invalid** target ETT endpoint recipient is: 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.

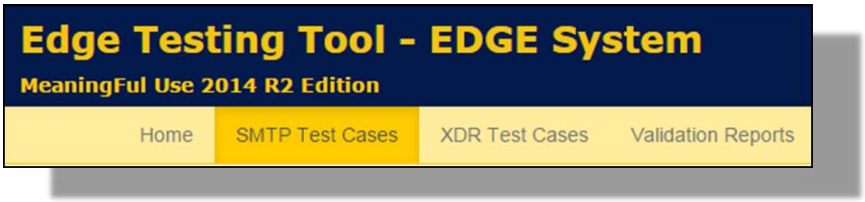
This test correlates to Test ID 47 of the MU Tracking tab within the *DirectEdgeProtocols* spreadsheet and TE170.314(b)(8) – 3.11 within the ONC 2014 Edition approved Test Procedure requirements document.

### 3.7.1 TESTING STEPS

To execute SMTP MU2 Test Case 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.

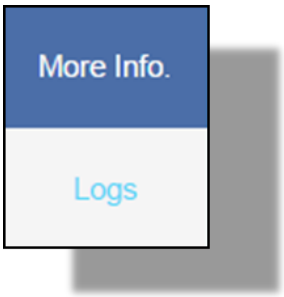


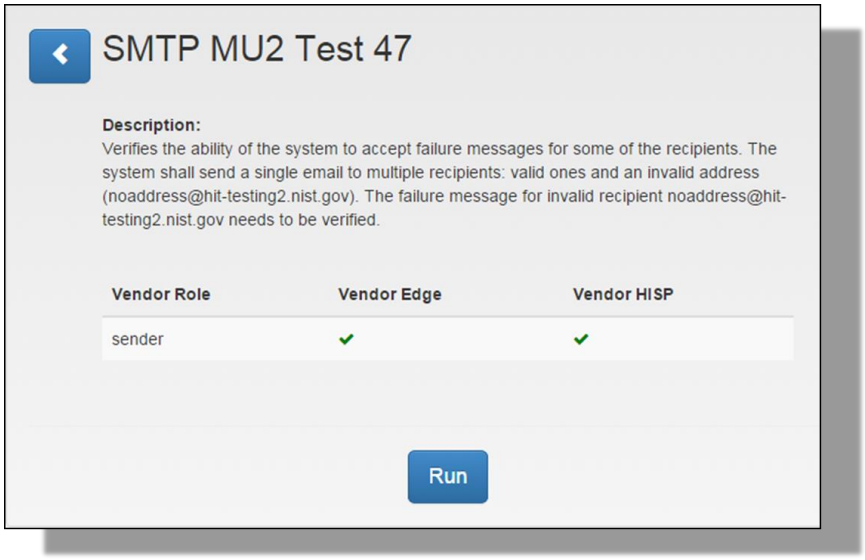

3. From the testing Profile, select **Sender**.


   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 MU2 Test Case 47, the Vendor navigates to the Test Case's execution interface.


   To gain additional information concerning SMTP MU2 Test Case 47's intended purpose (including Description, Vendor/SUT roles), click **More Info** link for the Test Case.

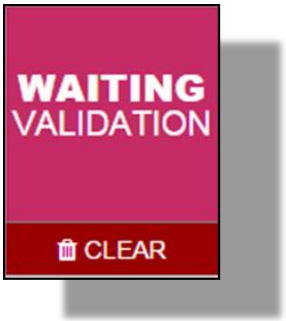


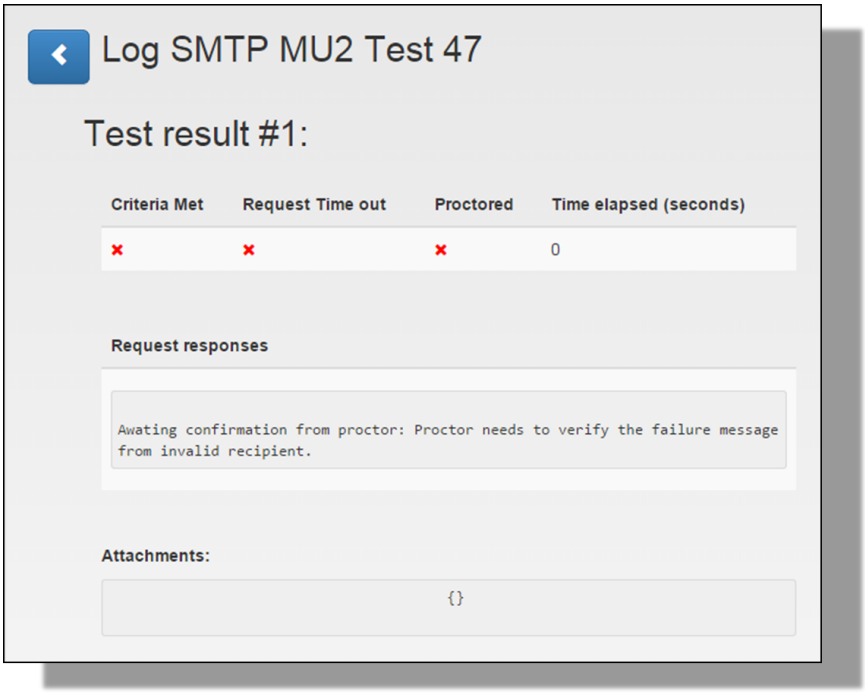

5. With the Profile saved, More Info reviewed, and **SMTP MU2 Test 47** selected, the Vendor performs the following Test Steps:
    A. Navigate the to SUT's messaging client/interface for **Vendor SMTP Email Address** (specified in the Profile).
    B. Create a single new message.
        a. Send the 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.
    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.*

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 compete this, the Vendor clicks the **Waiting Validation** button




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




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.

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.*

# 4.0 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 |

## 4.1 SMTP Test Case 16

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. 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 2014 Edition approved Test Procedure requirements document.

### 4.1.1 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.*

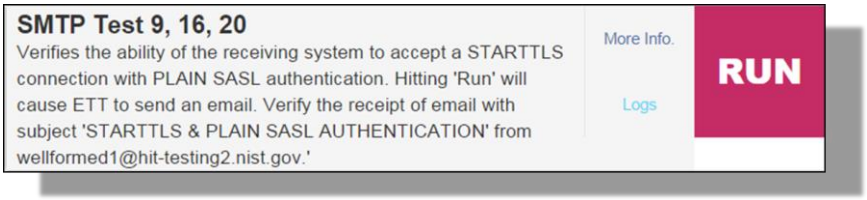
1. Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 7 within 2.2 Registration.

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

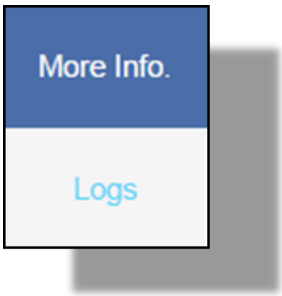

3. From the testing Profile, select **Receiver**.

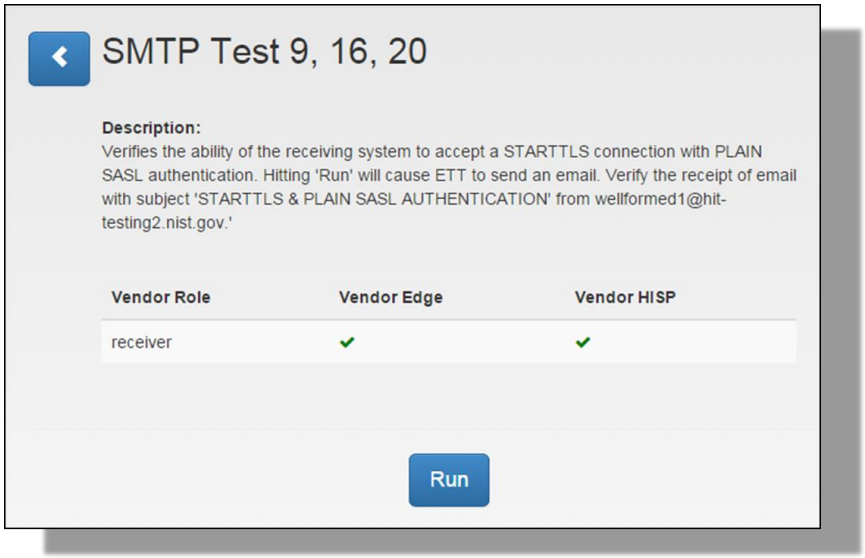

   Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 5 within 2.3 Profile Creation.

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.



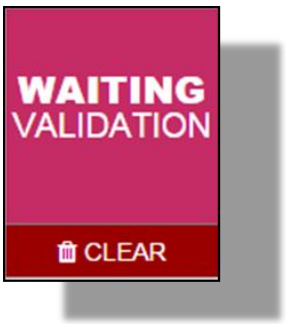




5. With the Profile saved, More Info reviewed, and **SMTP Test 9, 16, 20** selected, the Vendor performs the following Test Steps:
    A. Select the sample attachment type (**CCDA**, **CCR**, or **C32**) to be sent with the message.

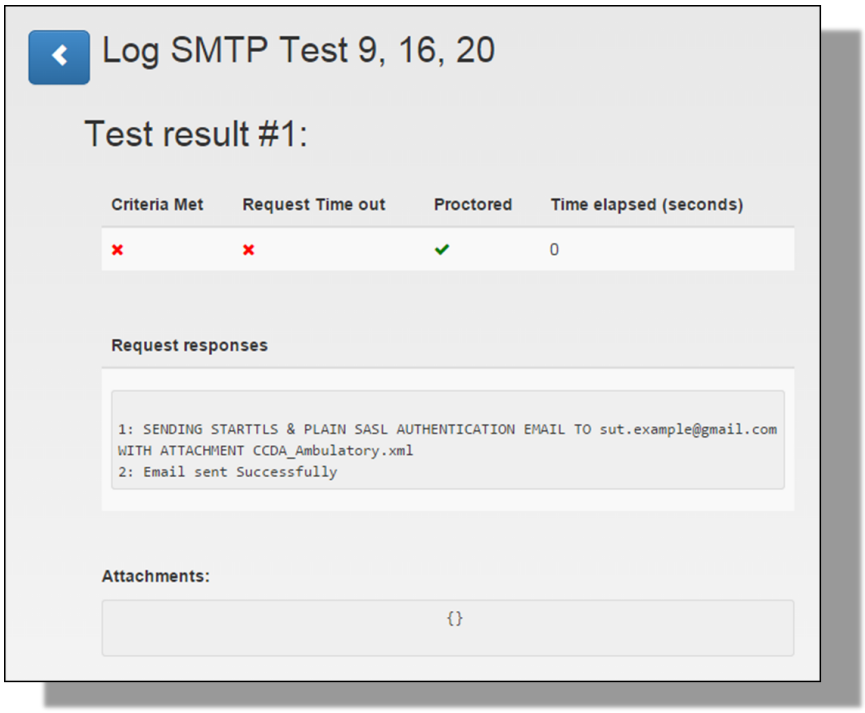

    B. Click **Run** to execute the test.


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 compete 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.




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.*

## 4.2 SMTP Test Case 17

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 2014 Edition approved Test Procedure requirements document.

### 4.2.1 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:

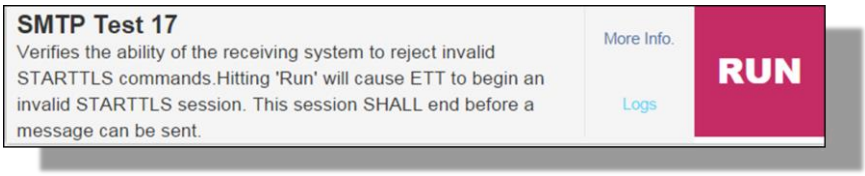
1. Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 7 within 2.2 Registration.

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

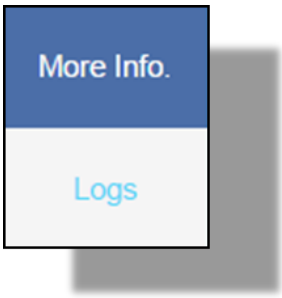

3. From the testing Profile, select **Receiver**.

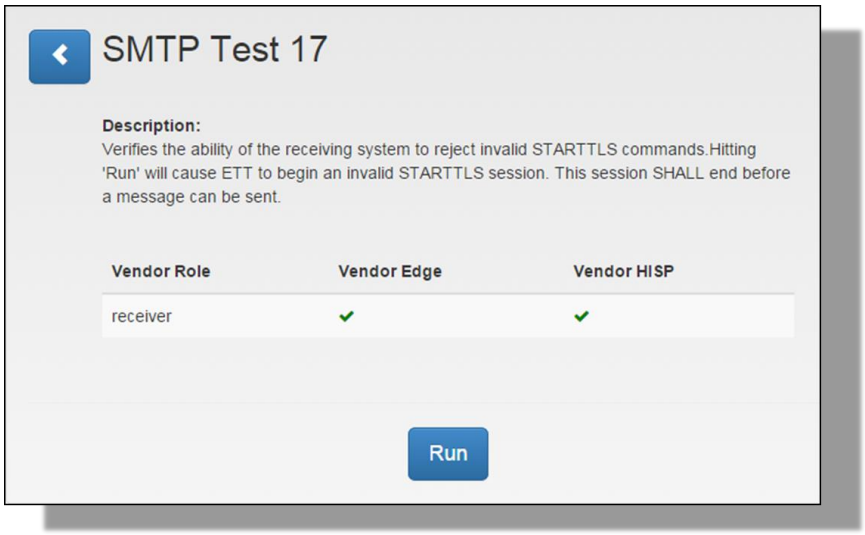

   Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 5 within 2.3 Profile Creation.

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.

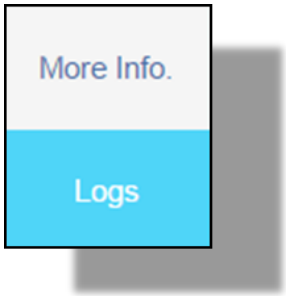

    B. Navigate the to SUT's messaging client/interface for **Vendor SMTP Email Address** (specified in the Profile).
        a. Wait at least 60 seconds from executing the test to allow successful transmission to the SUT.
        b. Check the **Vendor SMTP Email Address** to validate that a new message 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.*

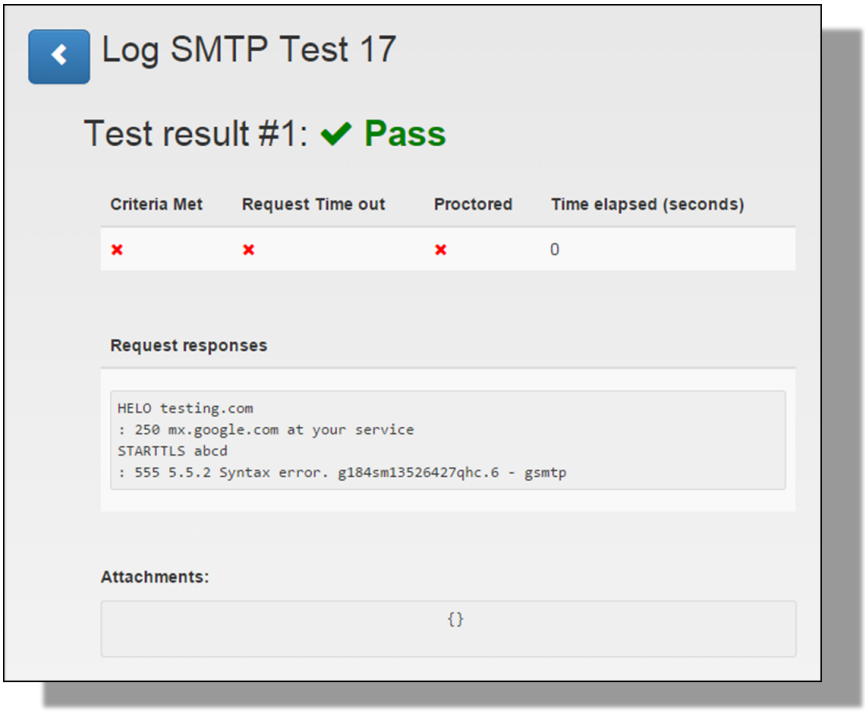
6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
   - A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
   - A test Fail prompts the Vendor to **Retry** the test.
   - The **Clear** button resets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




***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.*

## 4.3 SMTP Test Case 20

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. 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 2014 Edition approved Test Procedure requirements document.

### 4.3.1 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.*

## 4.4 SMTP Test Case 22

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 HISP (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 2014 Edition approved Test Procedure requirements document.

### 4.4.1 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:

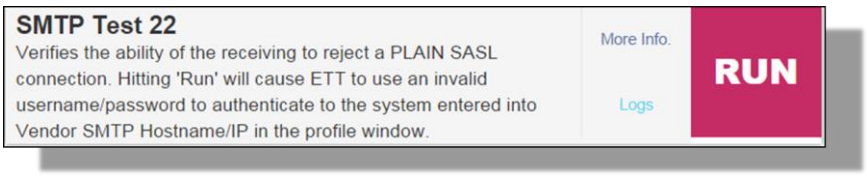
1. Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 7 within 2.2 Registration.

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

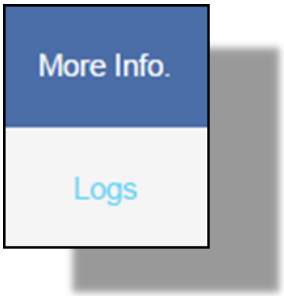

3. From the testing Profile, select **Receiver**.

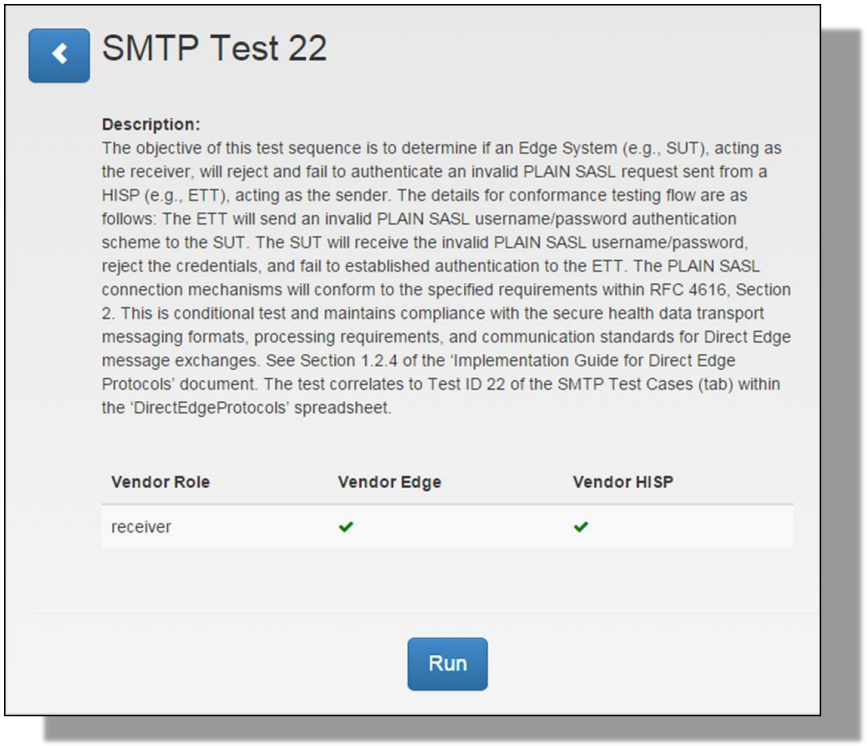

Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 5 within 2.3 Profile Creation.

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.




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.

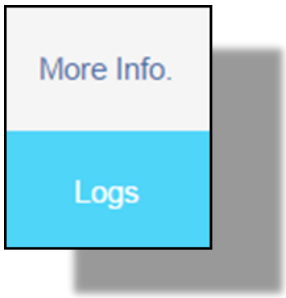

B. Navigate the to SUT's messaging client/interface for **Vendor SMTP Email Address** (specified in the Profile).
   a. Wait at least 60 seconds from executing the test to allow successful transmission to the SUT.
   b. Check the **Vendor SMTP Email Address** to validate that a new message is not present (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.*

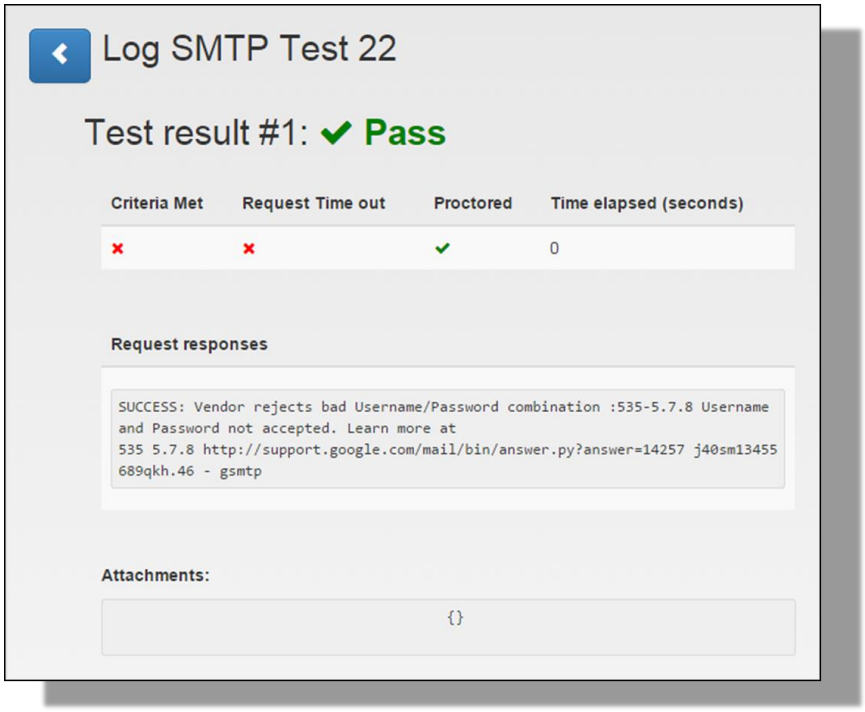
6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
   - A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
   - A test Fail prompts the Vendor to **Retry** the test.
   - The **Clear** button resets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



***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.*

## 4.5 SMTP Test Case 9

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. 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 2014 Edition approved Test Procedure requirements document.

### 4.5.1 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.*

## 4.6 SMTP Test Case 10

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 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 2014 Edition approved Test Procedure requirements document.

### 4.6.1 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:

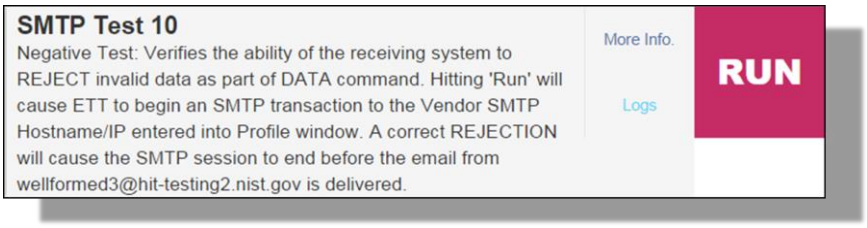
1. Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 7 within 2.2 Registration.

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

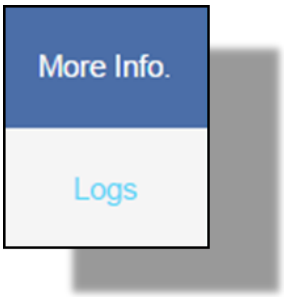

3. From the testing Profile, select **Receiver**.

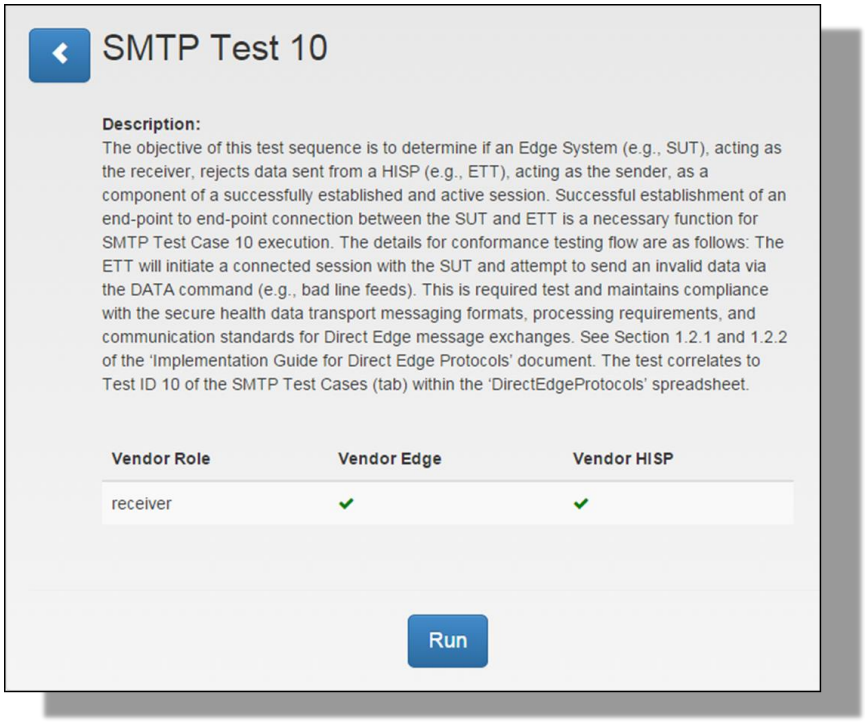

   Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 5 within 2.3 Profile Creation.

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.




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.

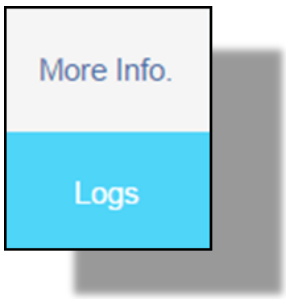
b. Check the **Vendor SMTP Email Address** to validate that a new message is not present from the ETT sending endpoint wellformed3@hit-testing.nist.gov (this is a negative test).

***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. The presence of an email from this endpoint indicates a test '**Fail**'.*

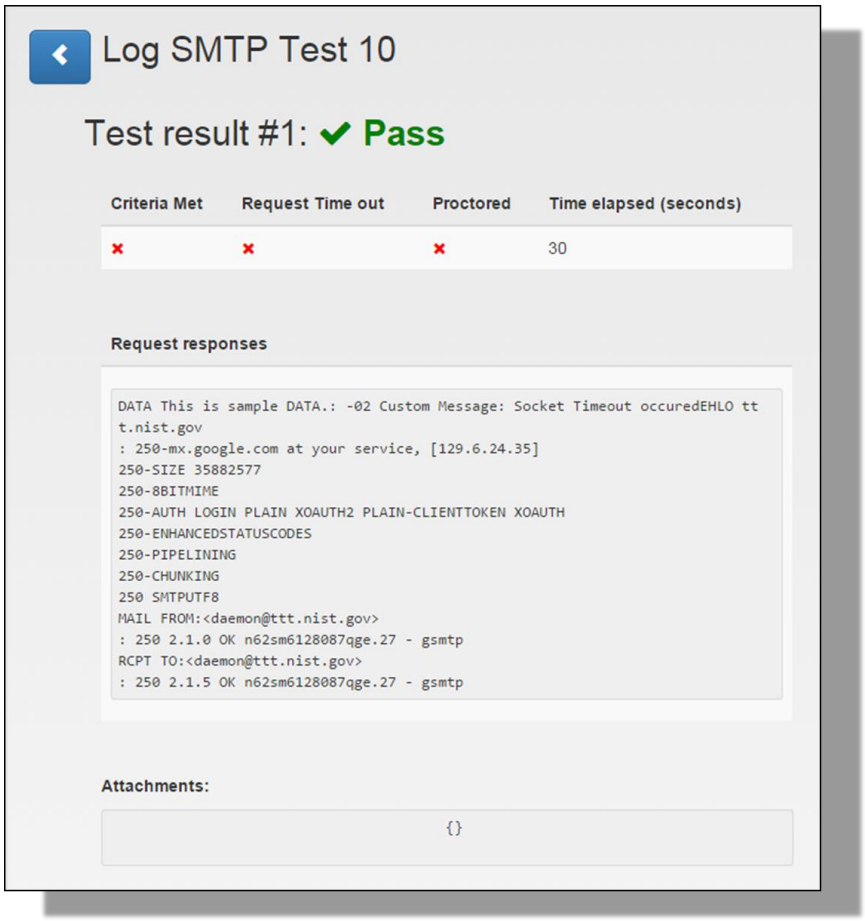
6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
   a. A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
   b. A test Fail prompts the Vendor to **Retry** the test.
   c. The **Clear** button resets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



***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.*

## 4.7 SMTP Test Case 11

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.

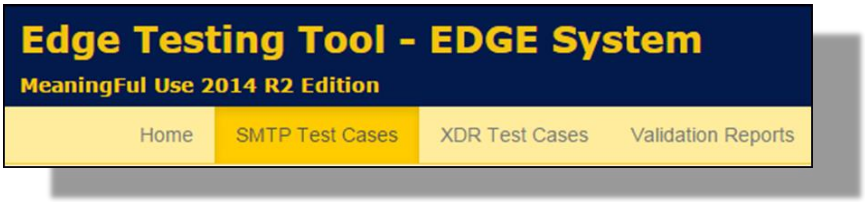
This test correlates to Test ID 11 of the SMTP Test Cases tab within the *DirectEdgeProtocols* spreadsheet TE170.314(b)(8) – 5.11 within the ONC 2014 Edition approved Test Procedure requirements document.

### 4.7.1 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.

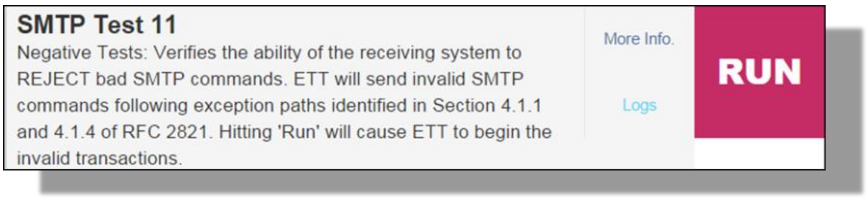
2. For this target SMTP MU2 test, select **SMTP Test Cases** from the Navigation Bar. This enables the testing Profile feature of the tool.



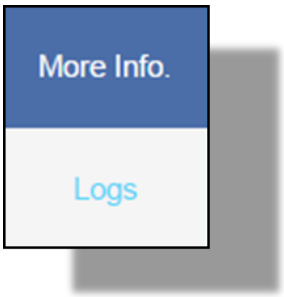

3. From the testing Profile, select **Receiver**.

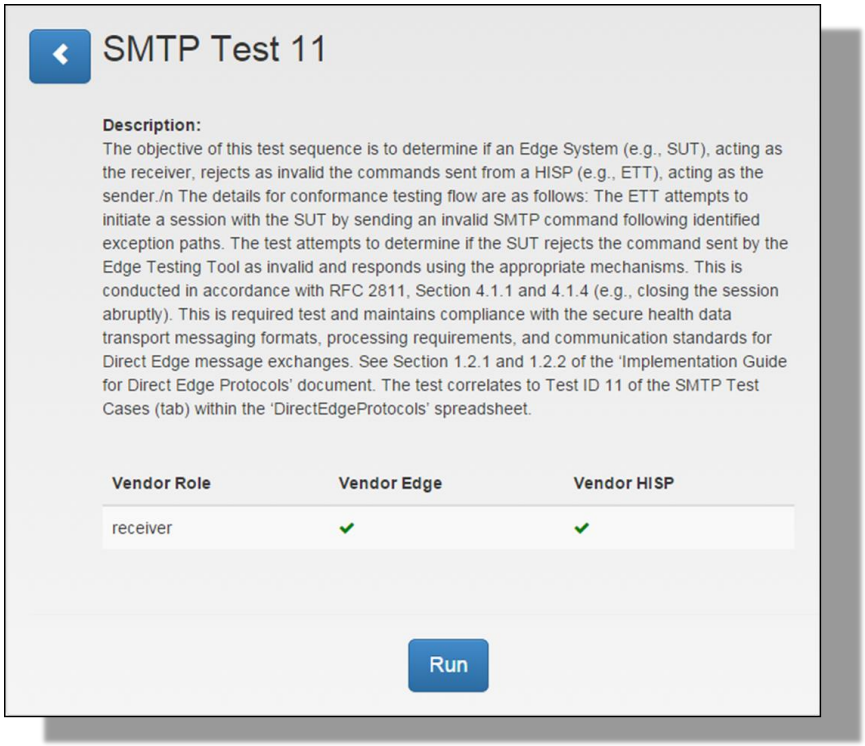

   Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 5 within 2.3 Profile Creation.

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.




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).

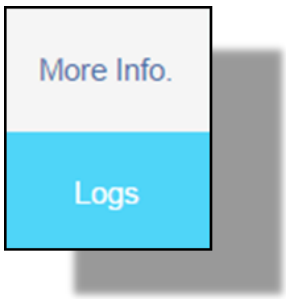
a. Wait at least 60 seconds from executing the test to allow successful transmission to the SUT.
b. Check the **Vendor SMTP Email Address** to validate that a new message is not present (this is a negative test).

***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.*

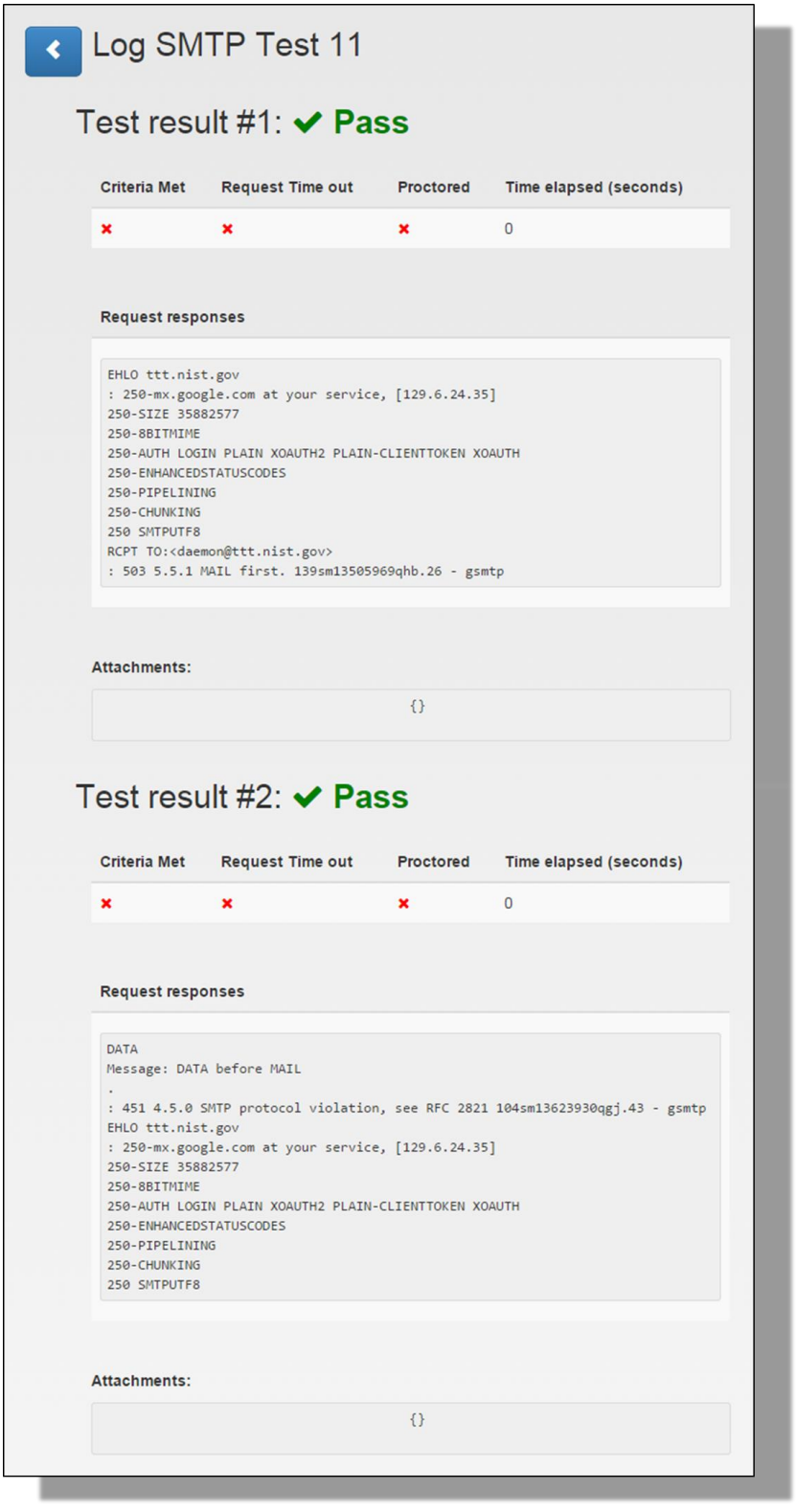
6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
   a. A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
   b. A test Fail prompts the Vendor to **Retry** the test.
   c. The **Clear** button resets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

## 4.8 SMTP Test Case 13

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 2014 Edition approved Test Procedure requirements document.

### 4.8.1 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:

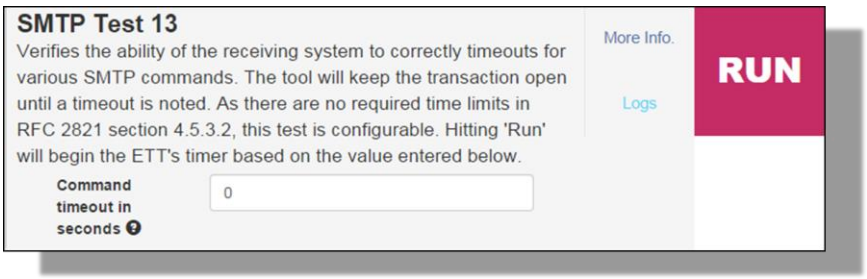
1. Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 7 within 2.2 Registration.

2. For this target SMTP MU2 test, select **SMTP Test Cases** from the Navigation Bar. This enables the testing Profile feature of the tool.

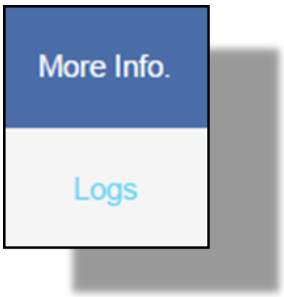

3. From the testing Profile, select **Receiver**.

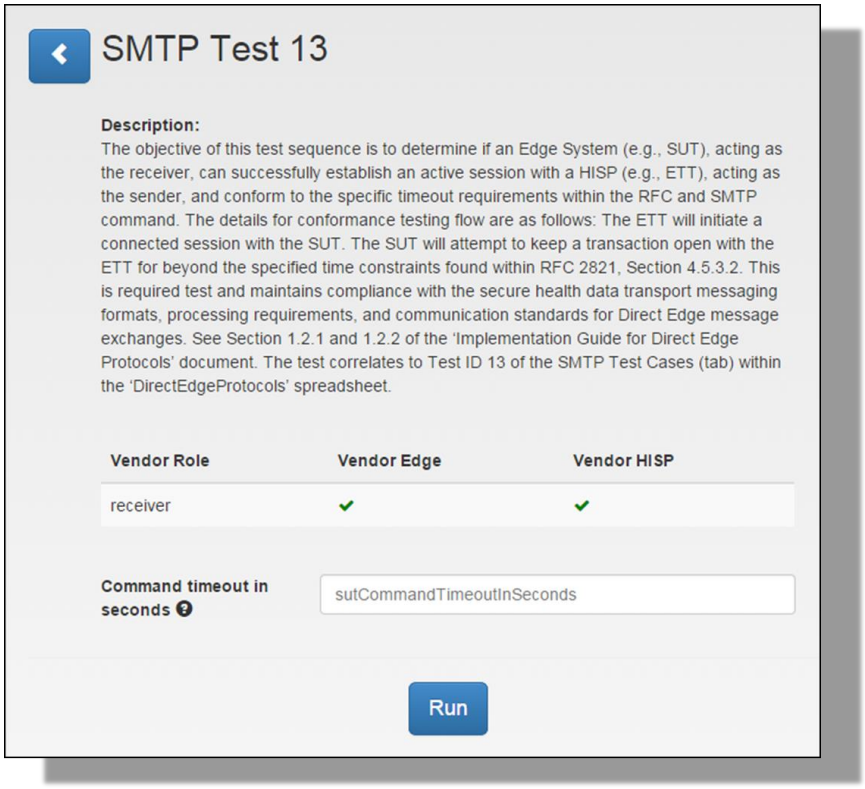

   Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 5 within 2.3 Profile Creation.

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:
    A. On the SMTP Test 13's execution interface, enter the specific timeout threshold to test the SUT against in the **Command Timeout in Seconds** field.
    B. Click **Run** to execute the test.

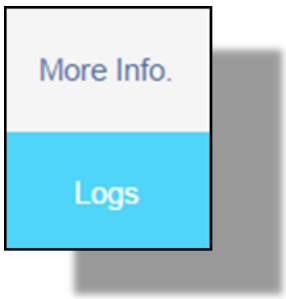
***Note**: The Vendor, in execution of SMTP Test Case 13, must enter the timeout threshold value specific to SUT testing need. RFC 2821, Section 4.5.3.2 does not require specific time dependent testing restrictions. However, examples of testable timeout constraints include:*

- *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 form sender: 5 minutes (300 seconds).*

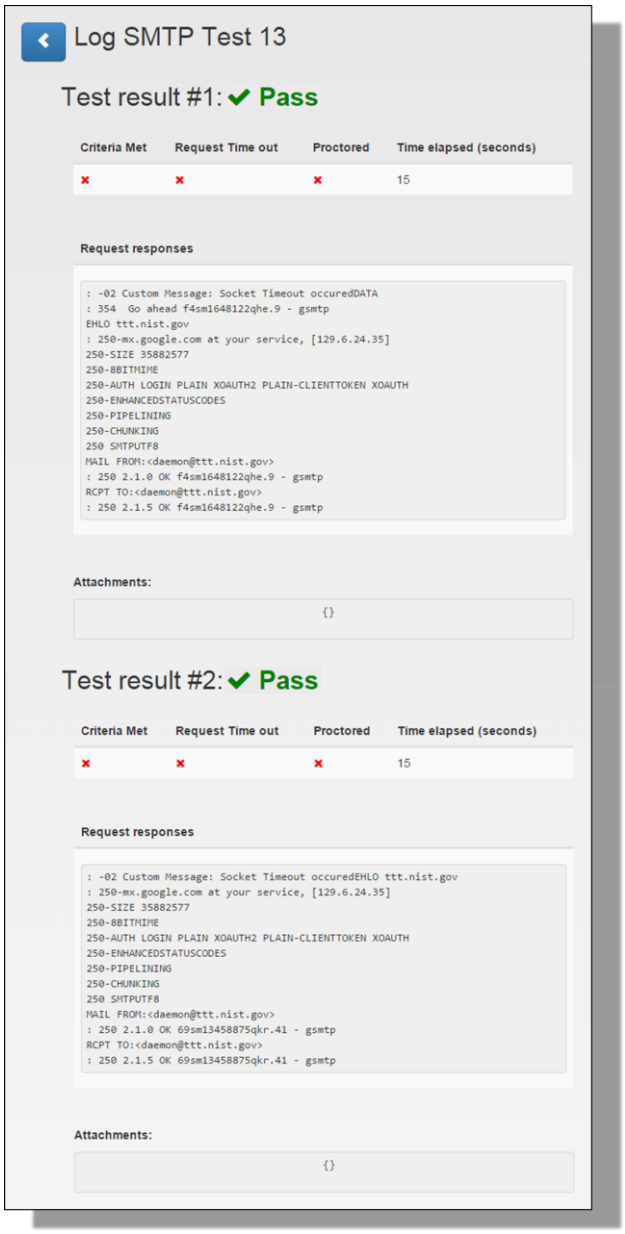
6. The test will process and render one of two results in the Test Case execution interface: **Pass** or **Fail**.
    a. A test **Pass** is indicated by a green check and a test **Fail** is indicated by a red X.
    b. A test Fail prompts the Vendor to **Retry** the test.
    c. The **Clear** button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



***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.*

# 5.0 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 |

## 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 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 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.

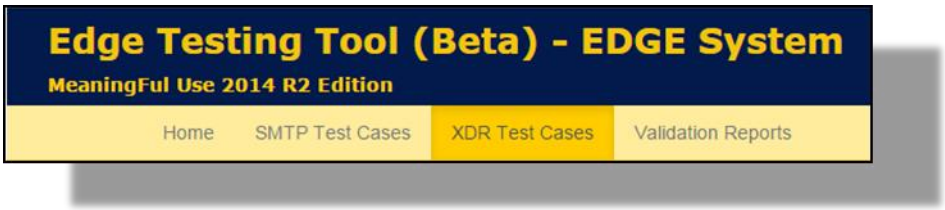
This test correlates to Test ID 7 of the XDR Test Cases tab within the *DirectEdgeProtocols* spreadsheet and TE170.314(b)(8) – 2.01 within the ONC 2014 Edition approved Test Procedure requirements document.

### 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.

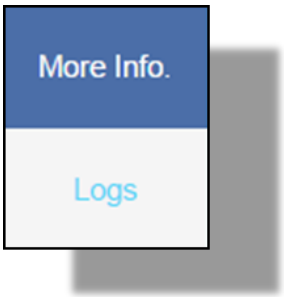
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.

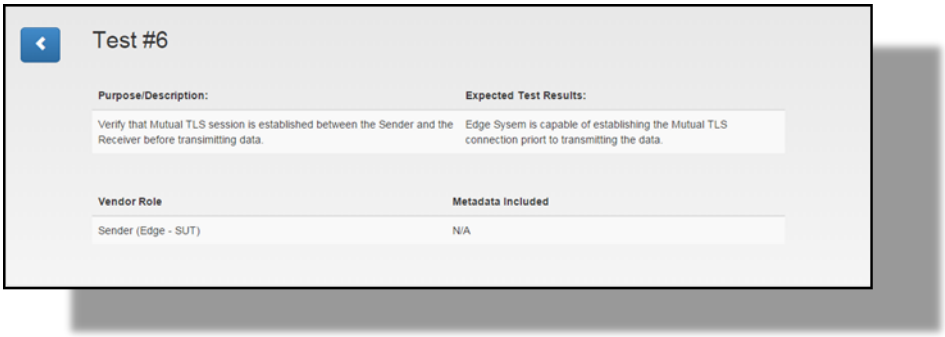



3. From the testing options available, select **Your System as: Sender**. This will enable Test Case selection.

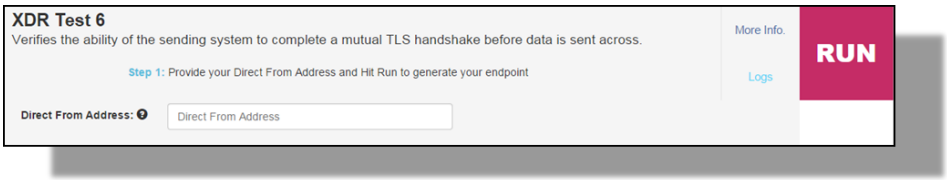

***Note**: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

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.





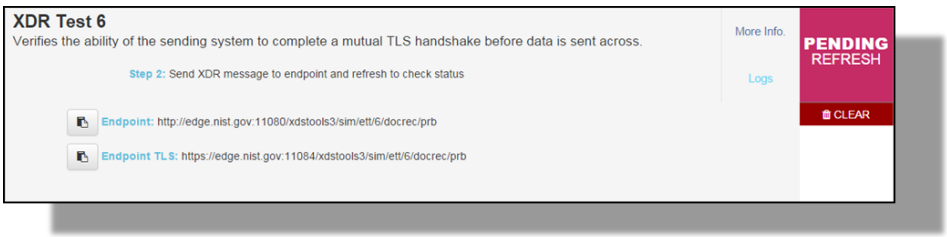

5. To initiate XDR Test 6, the Vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly.




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.



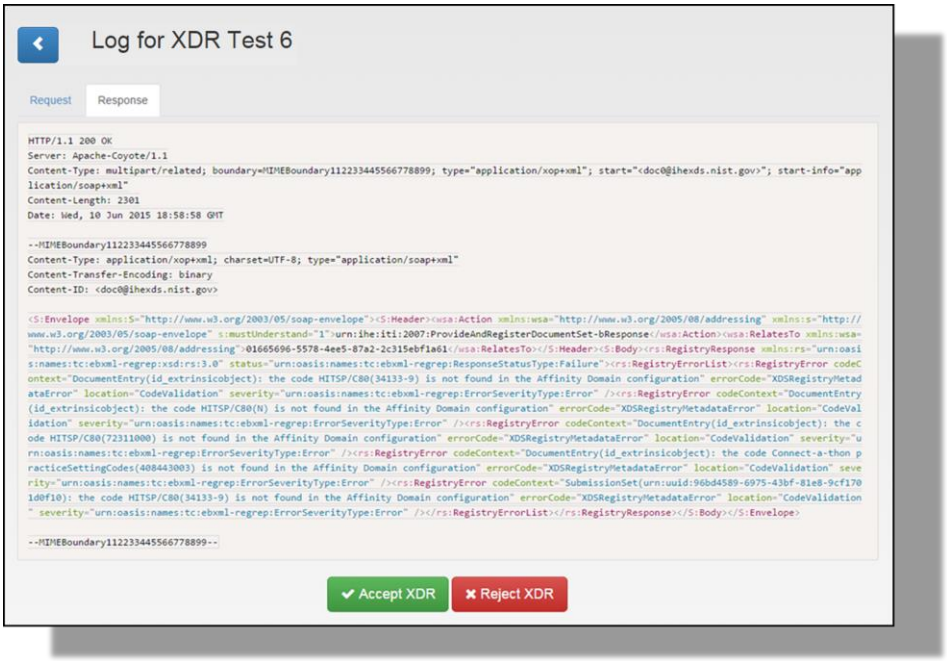

8. Once the XDR message has been transmitted from the SUT to the ETT endpoint, the Vendor clicks the **Pending Refresh** button for the Test Case.


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 compete this, the Vendor clicks the **Waiting Validation** button

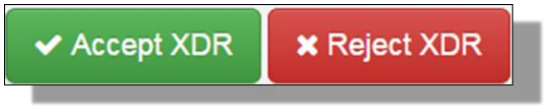

10. The Vendor is presented with the Test Case **Log** screen.


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.

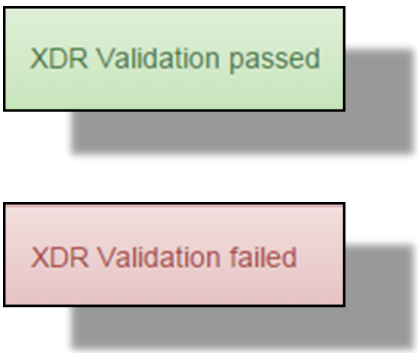



12. If the Vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata,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



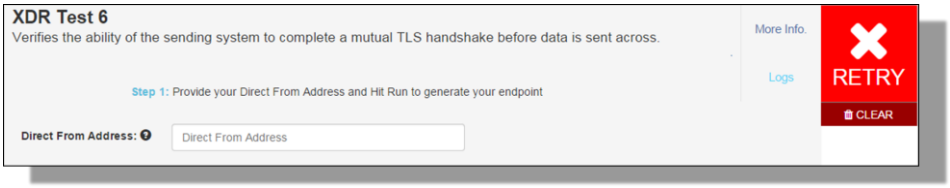

***Note**: 'Accept XDR' selections correlate with Test Case Success results (e.g., green check mark). Likewise, 'Reject XDR' selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a 'Reject XDR'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


## 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 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 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 established a Mutual TLS connection with the ETT generated endpoint, the SUT identified during authentication invalid certificates provided by the ETT, the SUT successfully disconnected from the ETT without authenticating and/or transmitting any data, and testing adhered to the specified requirements within *XDR and XDM for Direct Messaging v1.0* and *IHE XDR Profile for Limited Metadata Document Sources*.

This 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.

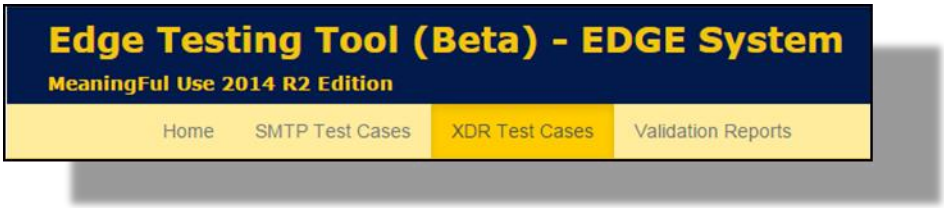
This test correlates to Test ID 7 of the XDR Test Cases tab within the *DirectEdgeProtocols* spreadsheet and TE170.314(b)(8) – 2.02 within the ONC 2014 Edition approved Test Procedure requirements document.

### 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.

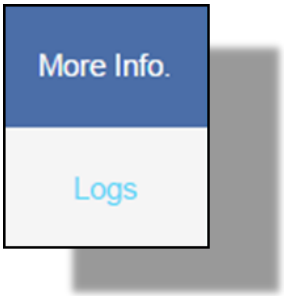
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.

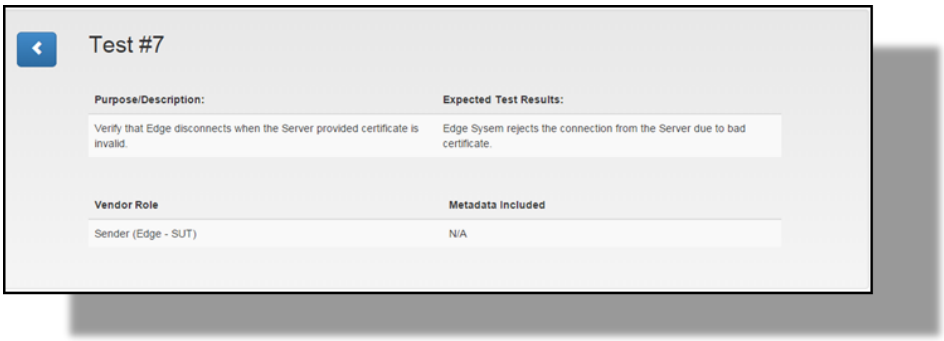



3. From the testing options available, select **Your System as: Sender**. This will enable test case selection.

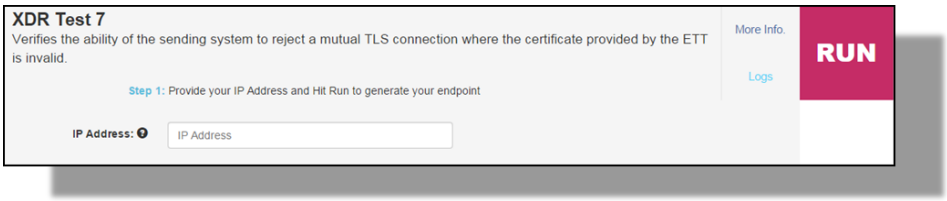

***Note**: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

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.





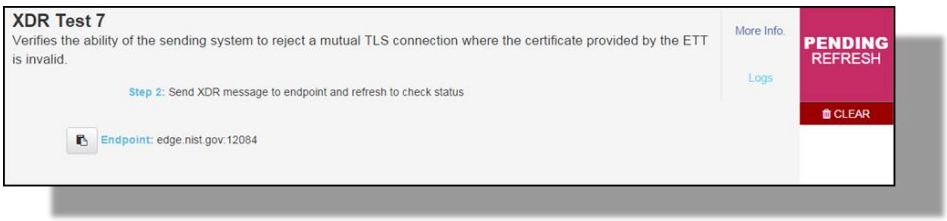

5. To initiate XDR Test 7, the Vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly.




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

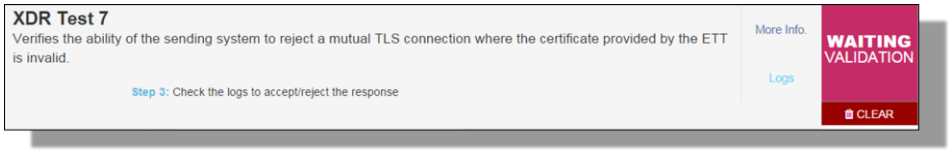

***Note**: Instructions are labeled in sequential order (e.g., '**Step 1**', '**Step 2**', '**Step 3**') in the content description of the Test Case. For this Test Case, the '**TLS Endpoint**' is provided by the Tester (e.g., Vendor).*

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.

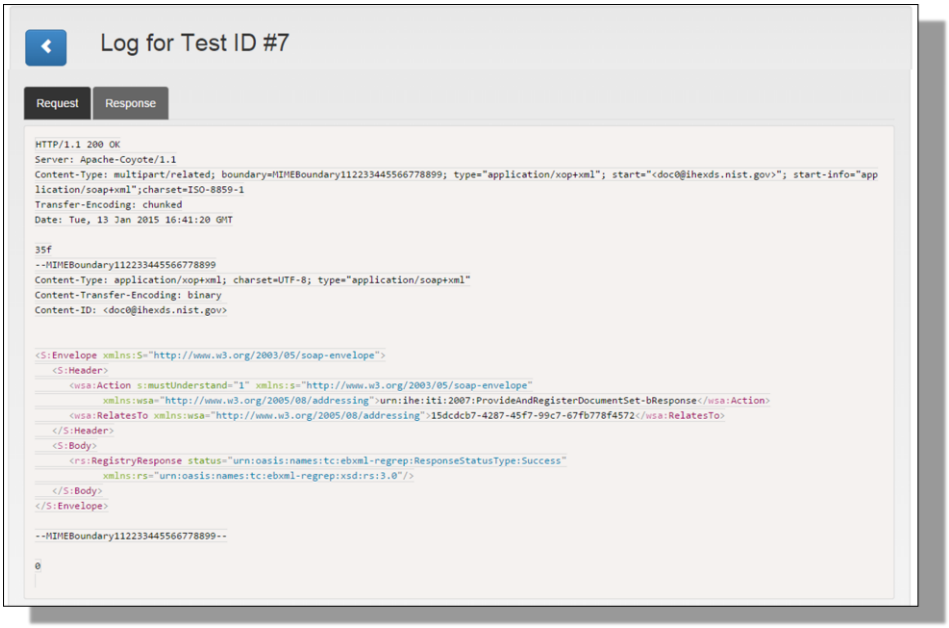

9. The ETT checks the generated endpoints for the presence of newly received XDR messages. The Vendor is prompted to manually validate if the test results conformed to the testing objectives. To compete this, the Vendor clicks the **Waiting Validation** button.



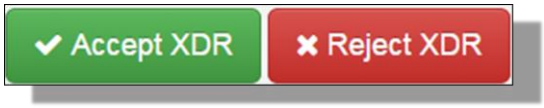

10. The Vendor is presented with the Test Case **Log** screen.


The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test 7, the Vendor will select the **Response** tab to review the ETT logged response received from the SUT after transmission of the XDR message.

11. Within the Log, the Vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
    a. Formed/transmitted the XDR message correctly;
    b. Attempted to established a connection with the ETT;
    c. Acknowledged the certificate provided by the ETT as invalid; and
    d. Successfully rejected a mutual TLS connection with the ETT.

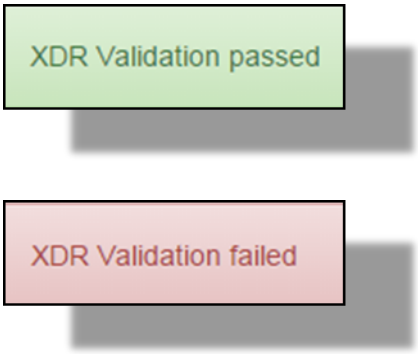



12. If the Vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata,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



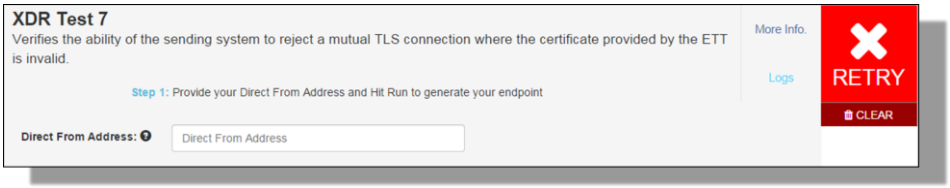

***Note**: 'Accept XDR' selections correlate with Test Case Success results (e.g., green check mark). Likewise, 'Reject XDR' selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a 'Reject XDR' 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 5.2.1 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).


## 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 2014 Edition approved Test Procedure requirements document.

### 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:

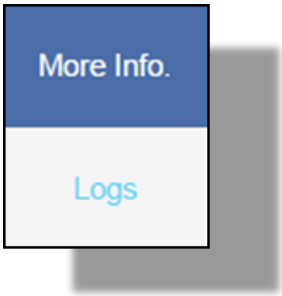
1. Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 7 within 2.2 Registration.

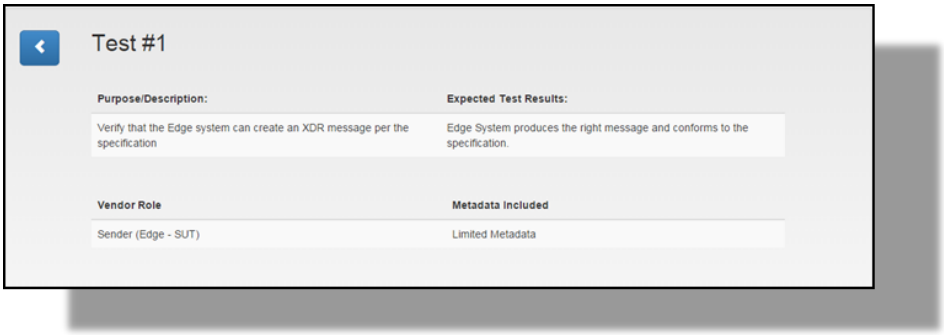
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.


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

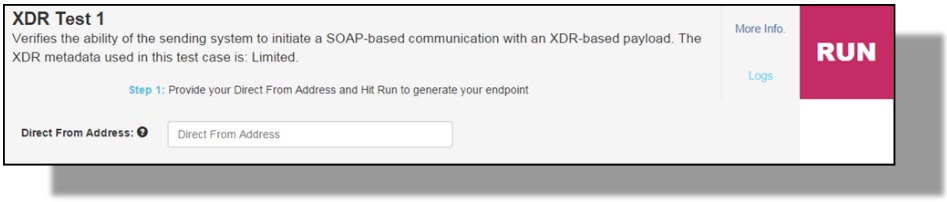

***Note**: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

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.





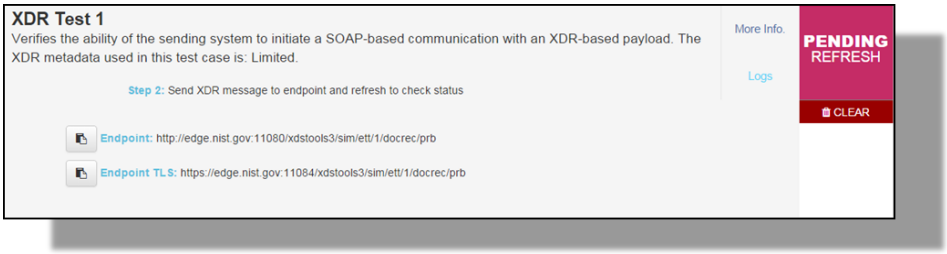

5. To initiate XDR Test 1, the Vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly.




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


***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.



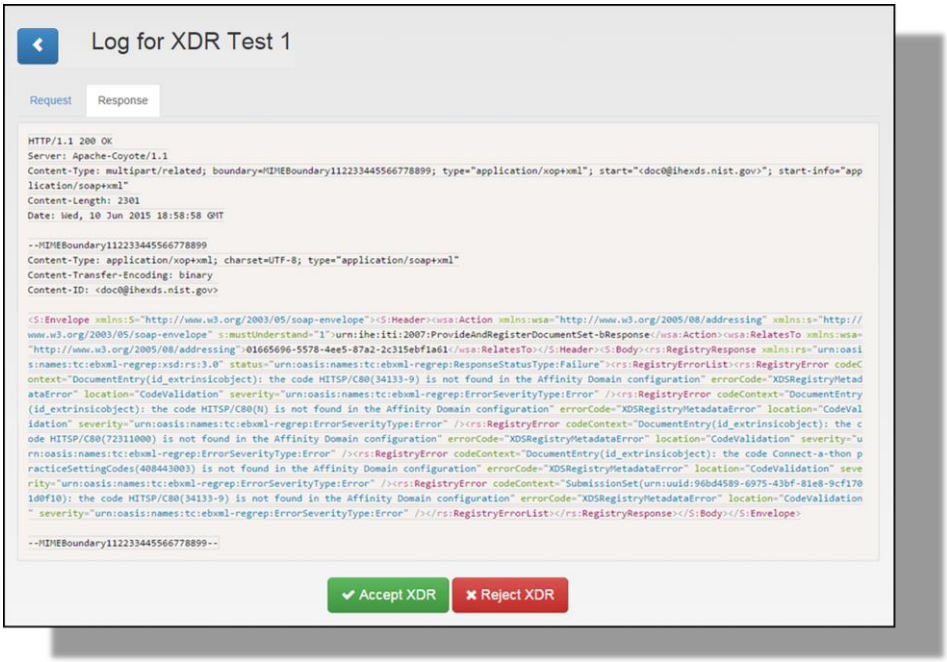

8. Once the XDR message has been transmitted from the SUT to the ETT endpoint, the Vendor clicks the **Pending Refresh** button for the Test Case.


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 compete this, the Vendor clicks the **Waiting Validation** button

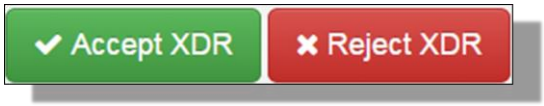

10. The Vendor is presented with the Test Case **Log** screen.


The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test 1, the Vendor will select the **Response** tab to review the ETT logged response received from the SUT after transmission of the XDR message.

11. Within the Log, the Vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
    a. Accurately attempted to established a connection with the ETT;
    b. Formed/transmitted the XDR message correctly; and
    c. Successfully initiated SOAP-based communication with the ETT;
    d. Successfully included an XDR-based payload with Limited metadata along with the message transmission.

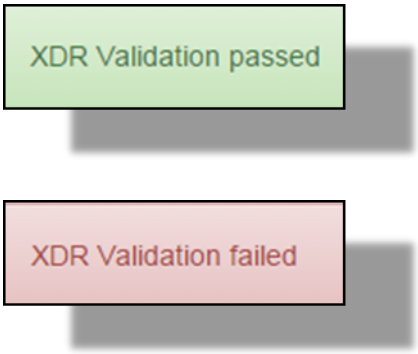



12. If the Vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata,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



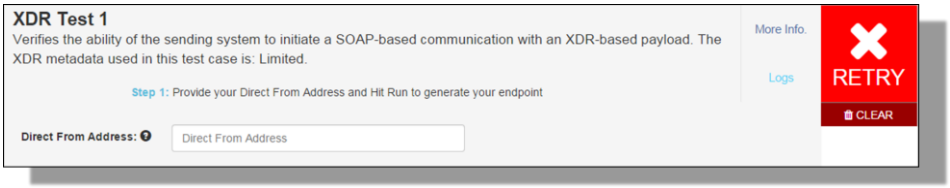

***Note**: 'Accept XDR' selections correlate with Test Case Success results (e.g., green check mark). Likewise, 'Reject XDR' selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a 'Reject XDR'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


## 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 2014 Edition approved Test Procedure requirements document.

### 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:

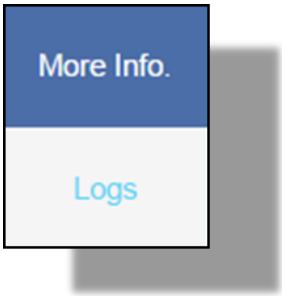
1. Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 7 within 2.2 Registration.

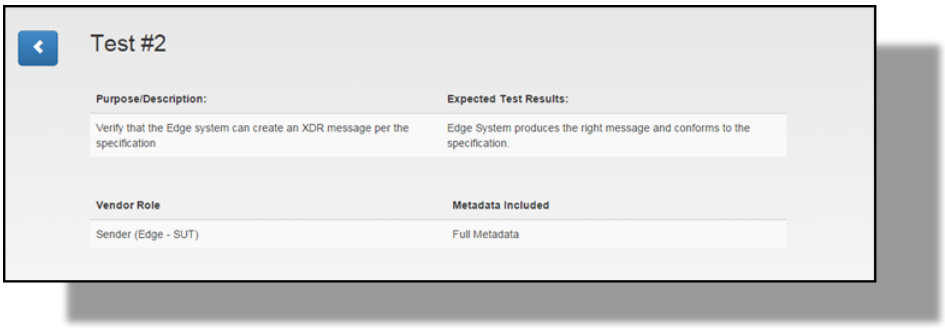
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.


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

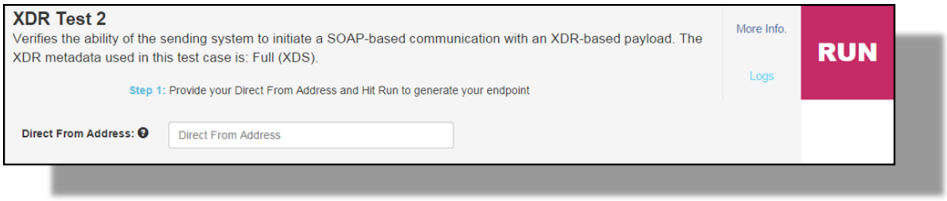

***Note**: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

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.



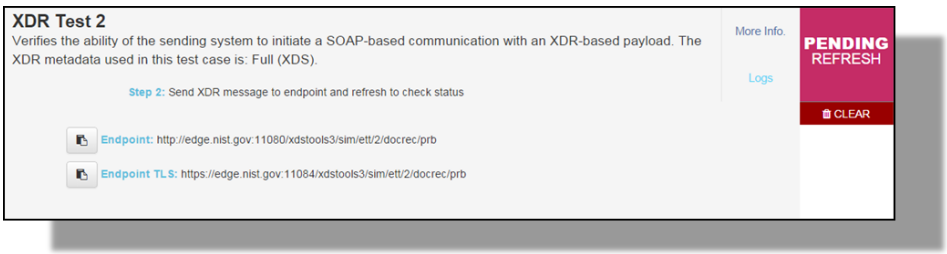



16. To initiate XDR Test 2, the Vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly.




***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.



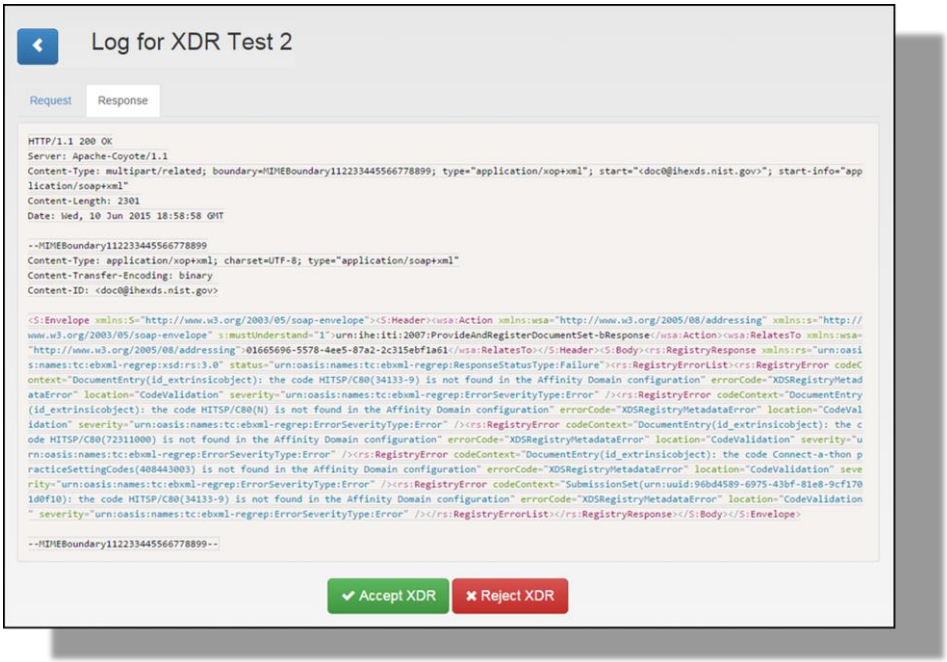

6. Once the XDR message has been transmitted from the SUT to the ETT endpoint, the Vendor clicks the **Pending Refresh** button for the Test Case.


7. 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 compete this, the Vendor clicks the **Waiting Validation** button

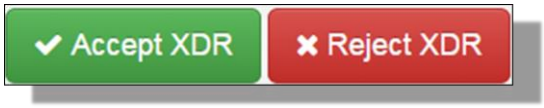

8. The Vendor is presented with the Test Case **Log** screen.


The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test 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 established a connection with the ETT;
    b. Formed/transmitted the XDR message correctly; and
    c. Successfully initiated SOAP-based communication with the ETT;
    d. Successfully included an XDR-based payload with Full XDS metadata along with the message transmission.

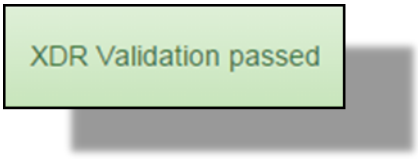


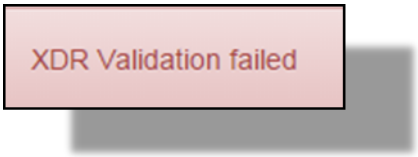

10. If the Vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata,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

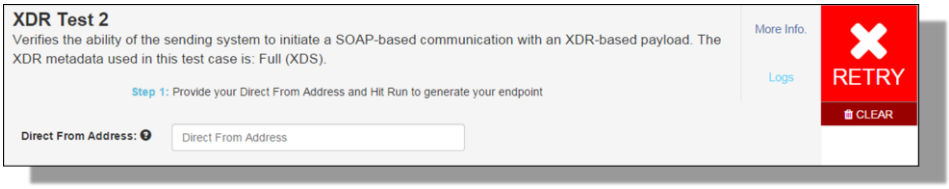
11. The ETT presents Vendor conformation based upon the selection made.






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).

## 5.5 XDR MU2 Test Case 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.

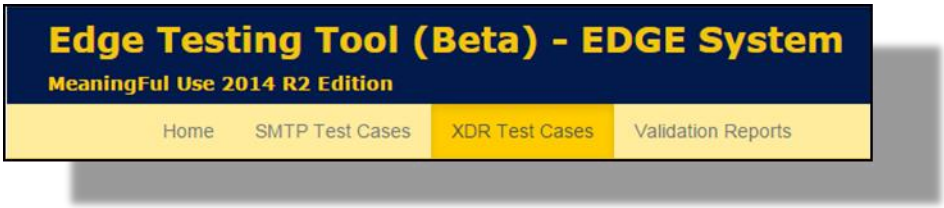
This test correlates to Test ID 19 of the MU2 Tracking tab within the *DirectEdgeProtocols* spreadsheet and TE170.314(b)(8) – 2.07 within the ONC 2014 Edition approved Test Procedure requirements document.

### 5.5.1 TESTING STEPS

To execute XDR MU2 Test Case 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.

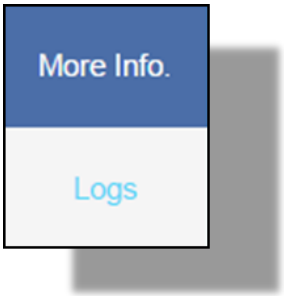
15. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.

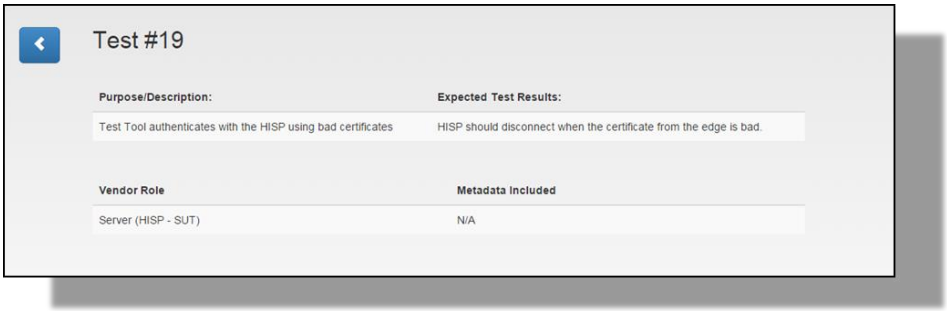



16. From the testing options available, select **Your System as: Sender**. This will enable test case selection.

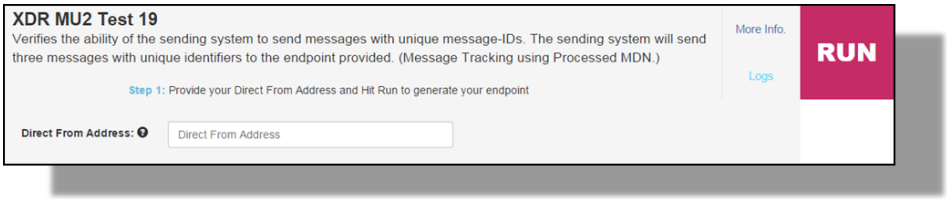

***Note**: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

17. To gain additional information concerning XDR MU2 Test Case 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.





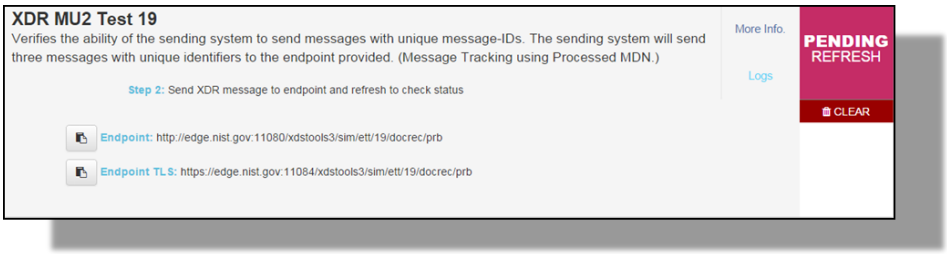

18. To initiate XDR MU2 Test Case 19, the Vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly.




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

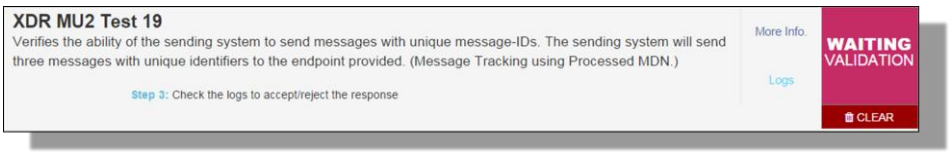

***Note**: Instructions are labeled in sequential order (e.g., '**Step 1**', '**Step 2**', '**Step 3**') in the content description of the Test Case. For this Test Case, the '**TLS Endpoint**' is provided by the Tester (e.g., Vendor).*

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.

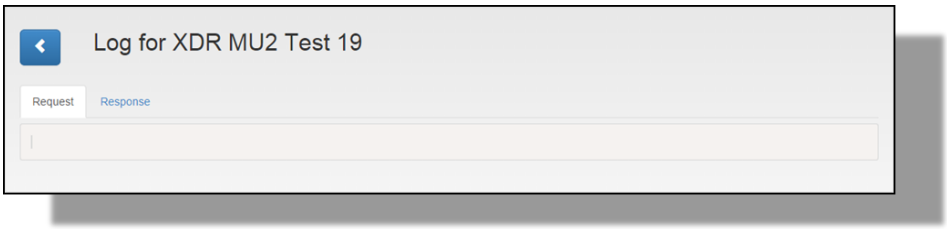



21. Once the 3 XDR messages have been transmitted from the SUT to the ETT endpoints, the Vendor clicks the **Pending Refresh** button for the Test Case.


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 compete this, the Vendor clicks the **Waiting Validation** button.

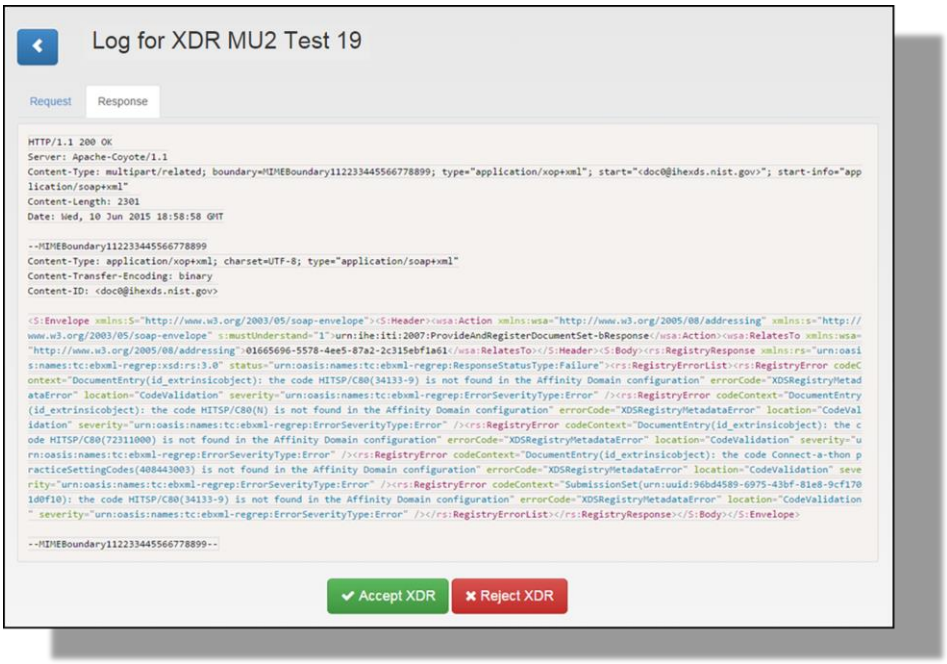



23. The Vendor is presented with the Test Case **Log** screen.

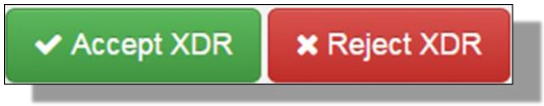



The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR MU2 Test Case 19, the Vendor will select the **Response** tab to review the ETT logged response received from the SUT after transmission of the XDR messages.

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

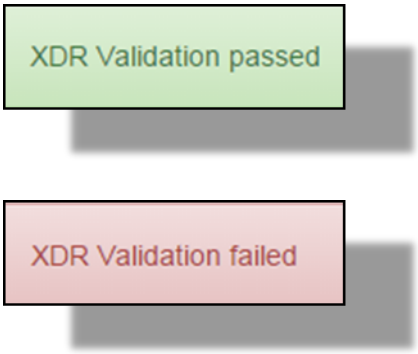



25. If the Vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata,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



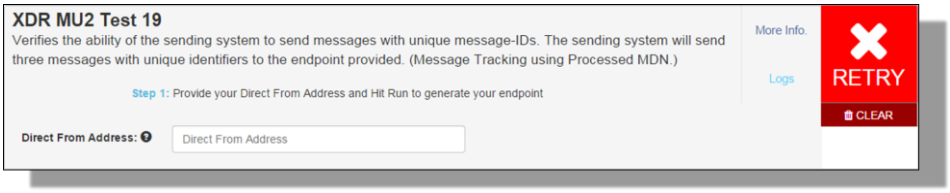

***Note**: 'Accept XDR' selections correlate with Test Case Success results (e.g., green check mark). Likewise, 'Reject XDR' selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a 'Reject XDR'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

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


## 5.6 XDR MU2 Test Case 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 an valid and invalid HISP recipient (i.e., ETT), acting as the receiver, and generate process MDNs successfully.

The testing details for conformance testing flow are as follows:

- 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 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 MU2 Tracking tab within the *DirectEdgeProtocols* spreadsheet and TE170.314(b)(8) – 2.08 within the ONC 2014 Edition approved Test Procedure requirements document.

### 5.6.1 TESTING STEPS

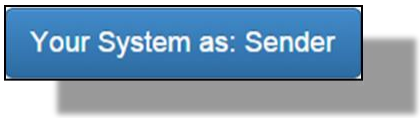
To execute XDR MU2 Test Case 20 and assess the SUT's ability to send an XDR message to both valid/invalid recipients and generate/handle process MDNs successfully, the Vendor must perform the following steps. Within the ETT, XDR MU2 Test Case 20 is broken down into two executable tests: 20a and 20b. The steps of each are described within the following steps.

#### 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.

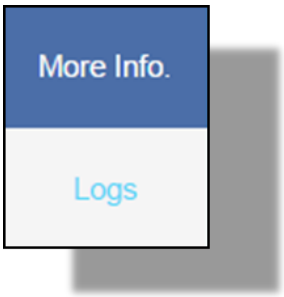
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.

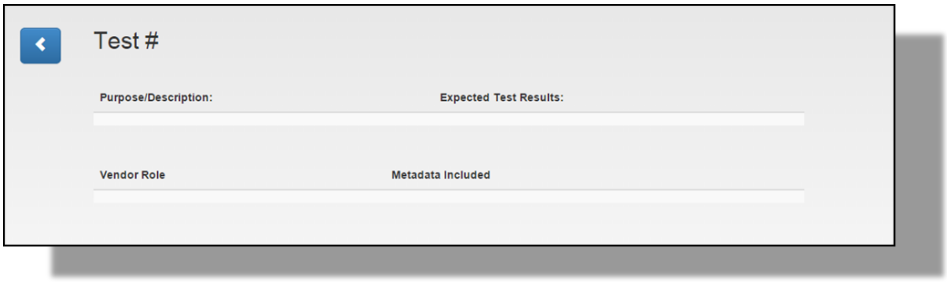

3. From the testing options available, select **Your System as: Sender**. This will enable test case selection.



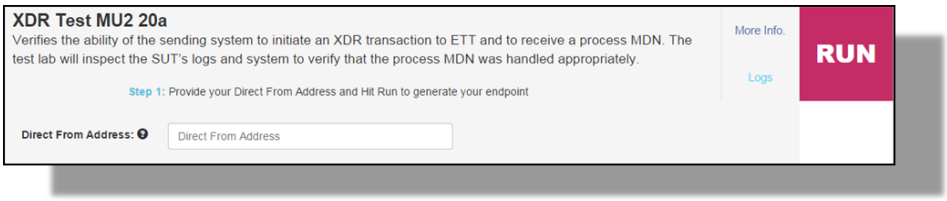

***Note**: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

4. To gain additional information concerning XDR MU2 Test Case 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.



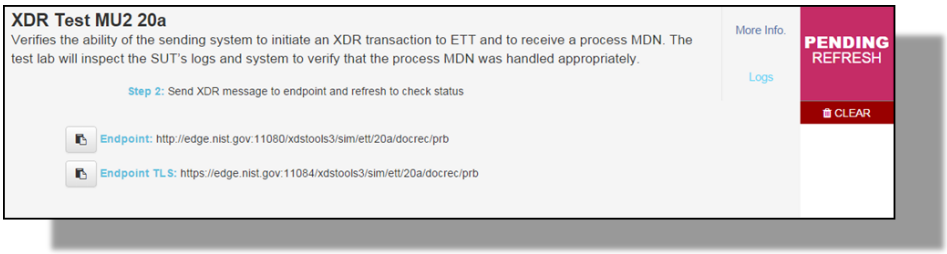

5. To initiate XDR MU2 Test Case 20a, the Vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly.




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

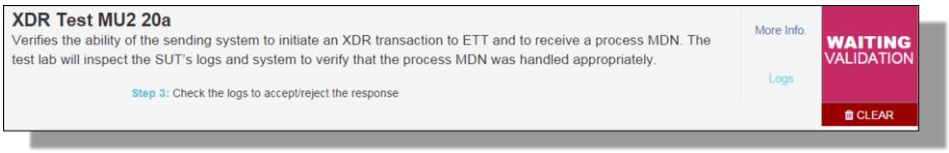

***Note**: Instructions are labeled in sequential order (e.g., '**Step 1**', '**Step 2**', '**Step 3**') in the content description of the Test Case. For this Test Case, the '**TLS Endpoint'** is provided by the Tester (e.g., Vendor).*

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 a valid recipient for the XDR messages (in addition to the ETT generated endpoint).

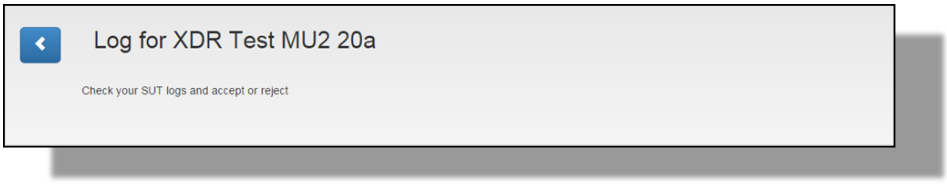



8. Once the XDR message has been transmitted from the SUT to the ETT endpoint, the Vendor clicks the **Pending Refresh** button for the Test Case.


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



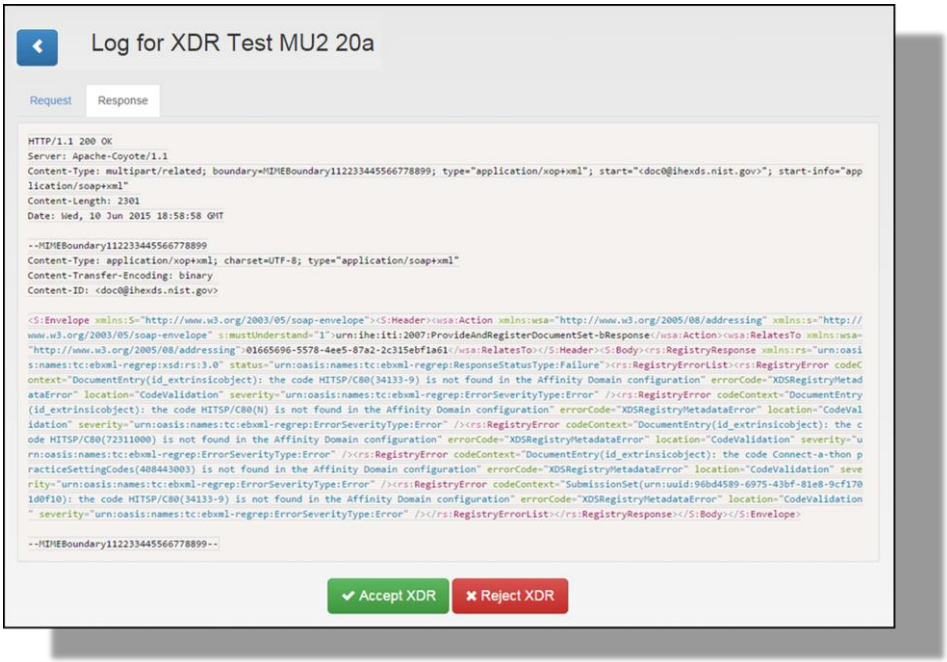

10. The Vendor is presented with the Test Case **Log** screen.



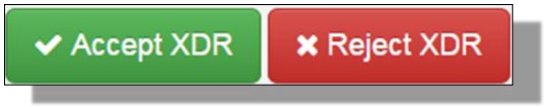

The Vendor is prompted to check the SUT's local logs and validate that the process MDNs generated as a result of sending the XDR message to both the ETT and valid recipients were handled correctly.


11. After the Vendor has reviewed and validated the SUT's log, the Vendor navigates back to the ETT's Log screen for XDR MU2 Test Case 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:
    d. Accurately established a connection with the ETT;
    e. Correctly created and transmitted the XDR message to the provided ETT endpoint recipient and additional valid message recipient;
    f. Produced conformant process MDNs for messaging tracking purposes (valid recipient); and
    g. Correctly receive and handle a process MDN notification sent from the ETT.

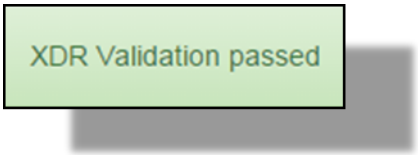


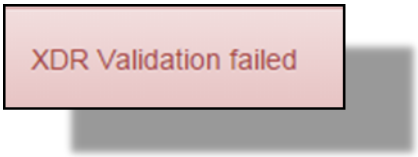

12. If the Vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata,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

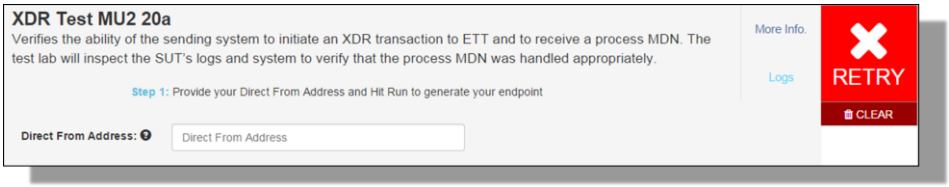
13. The ETT presents Vendor conformation based upon the selection made.



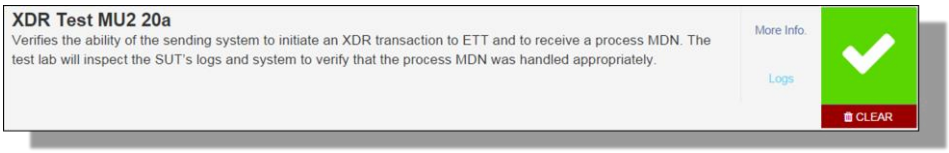



14. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case.

    XDR message rejection results in a red X and prompts the Vendor to **Retry** the test (reference Step 1 within Section 5.6.1.1 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).

#### 5.6.1.2 20b

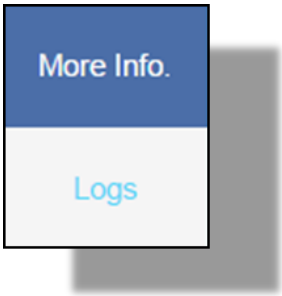
1. Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 7 within 2.2 Registration.

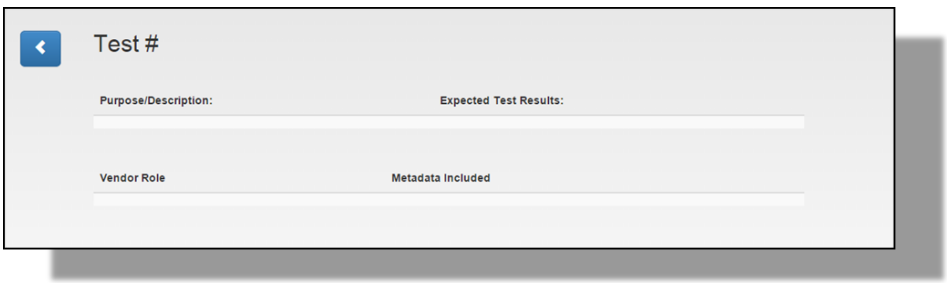
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.


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

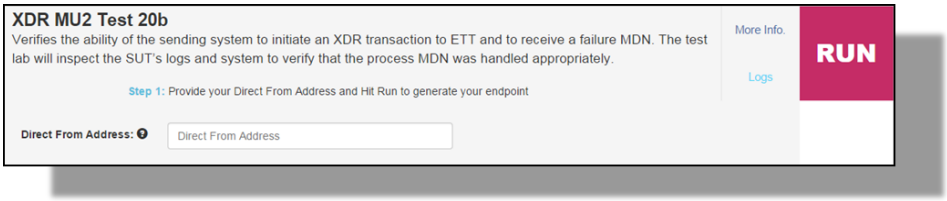

***Note**: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

4. To gain additional information concerning XDR MU2 Test Case 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.



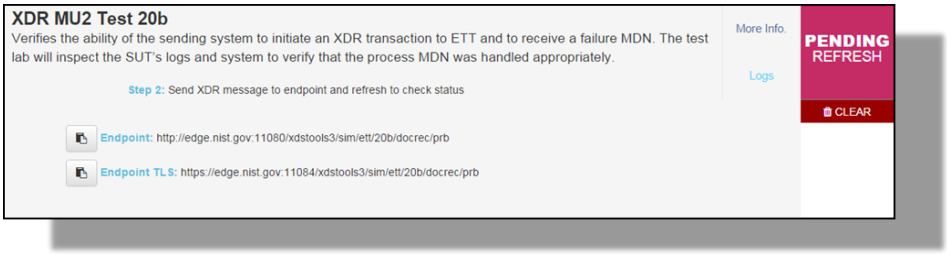
5. To initiate XDR MU2 Test Case 20b, the Vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly.




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

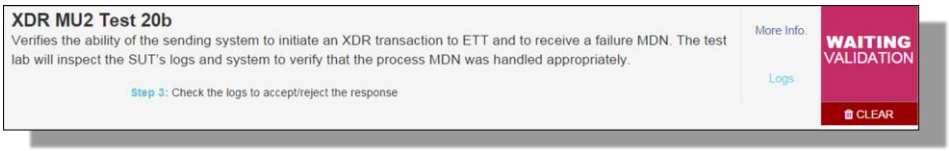

***Note**: Instructions are labeled in sequential order (e.g., '**Step 1**', '**Step 2**', '**Step 3**') in the content description of the Test Case. For this Test Case, the '**TLS Endpoint**' is provided by the Tester (e.g., Vendor).*

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).

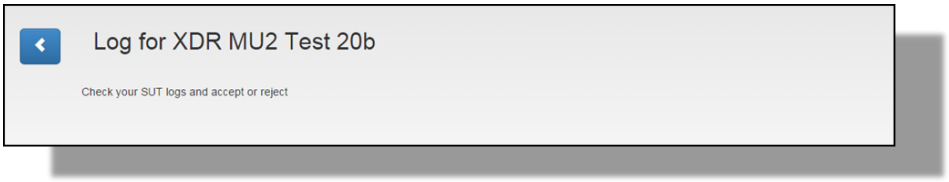



8. Once the XDR message has been transmitted from the SUT to the ETT endpoint, the Vendor clicks the **Pending Refresh** button for the Test Case.

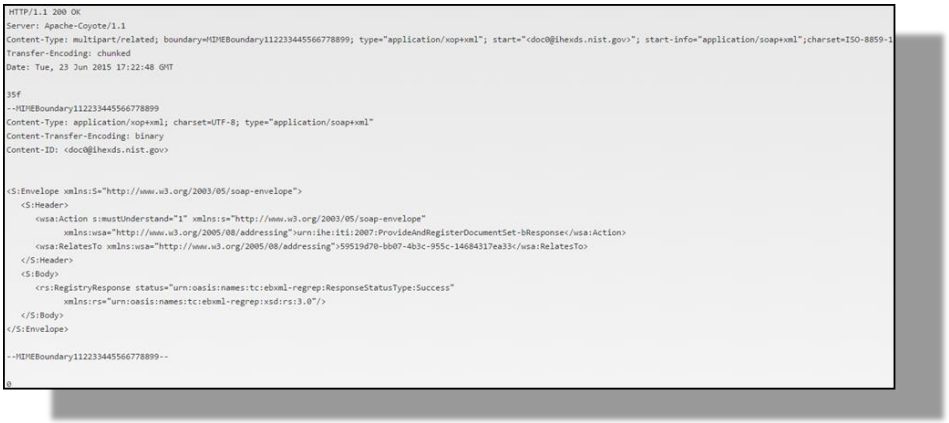

9. The ETT checks the generated endpoint(s) for the presence of a newly received XDR message. The Vendor is prompted to manually validate if the test results conformed to the testing objectives. To compete this, the Vendor clicks the **Waiting Validation** button.




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

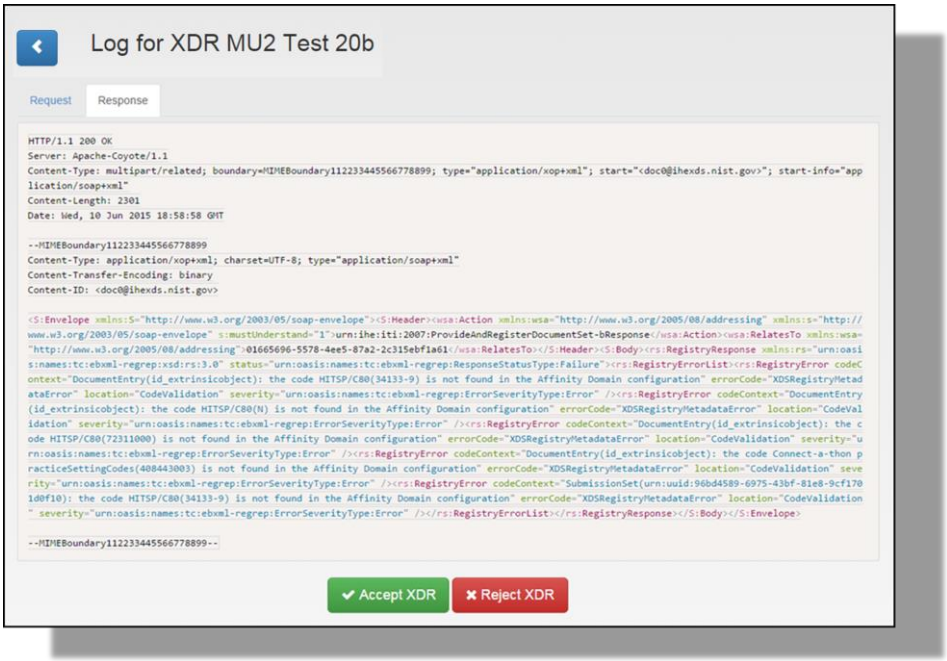



The Vendor is prompted to check the SUT's local logs and validate that the process MDNs generated as a result of sending the XDR message to both the ETT and invalid recipients were handled correctly.




11. After the Vendor has reviewed and validated the SUT's log, the Vendor navigates back to the ETT's Log screen for XDR MU2 Test Case 20b. The Vendor finalizes the review of the testing data by viewing the Log's option tabs message **Request** and **Response** data.

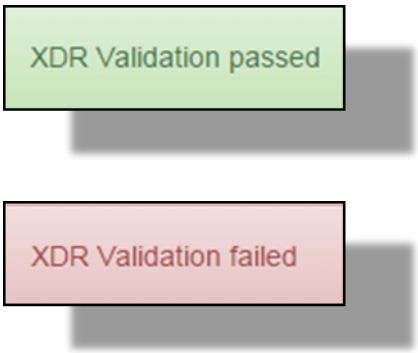

30. The Vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
    h. Accurately established a connection with the ETT;
    i. Correctly created and transmitted the XDR message to the provided ETT endpoint recipient and additional valid message recipient;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




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.

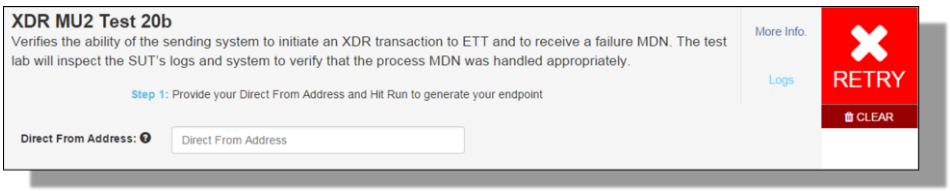
***Note**: 'Accept XDR' selections correlate with Test Case Success results (e.g., green check mark). Likewise, 'Reject XDR' selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a 'Reject XDR'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

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

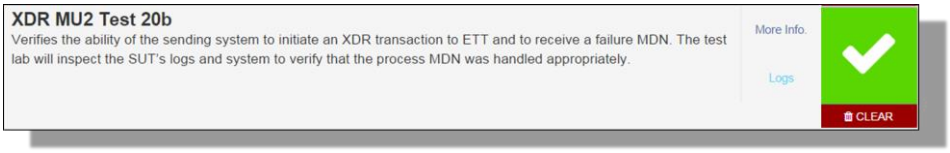



14. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case.

    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 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).


## 5.7 XDR MU2 Test Case 48

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

The testing details for conformance testing flow are as follows:

- As a precondition for this Test Case, the SUT must implement the additional constraints defined within *Implementation Guide for Delivery Notification for Direct v1.0* for delivery notification 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 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 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 MU2 Tracking tab within the *DirectEdgeProtocols* spreadsheet and TE170.314(b)(8) – 2.09 within the ONC 2014 Edition approved Test Procedure requirements document.

### 5.7.1 TESTING STEPS

To execute XDR MU2 Test Case 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 Delivery Notification requirements, the Vendor must perform the following steps:

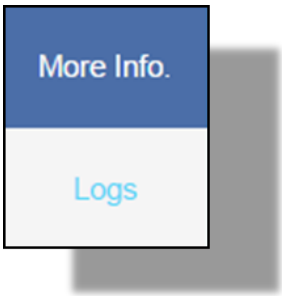
1. Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 7 within 2.2 Registration.

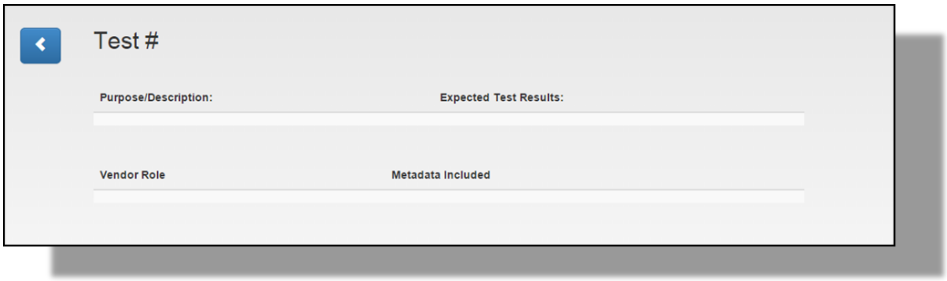
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.


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

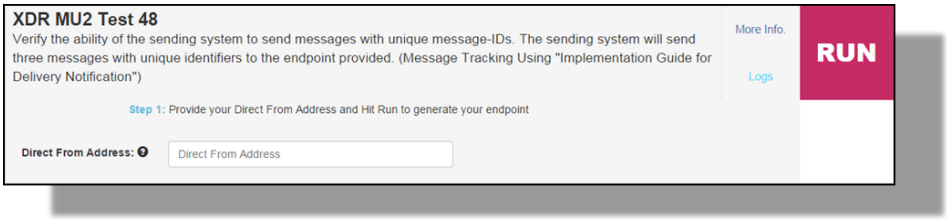
***Note**: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

4. To gain additional information concerning XDR MU2 Test Case 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 MU2 Test Case 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.



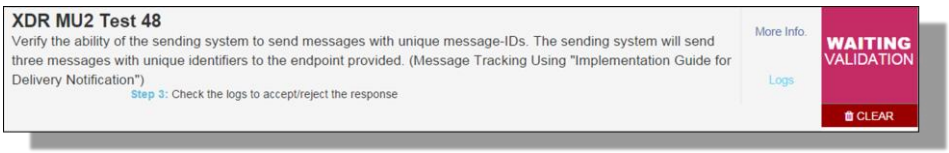

6. Once the SUT's Direct From Address has been populated in the Test Case, clicking **Run** initiates the first testing step.


***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.

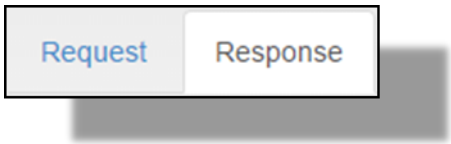

8. Once the 3 XDR messages have been transmitted from the SUT to the ETT endpoints, the Vendor clicks the **Pending Refresh** button for the Test Case.


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.

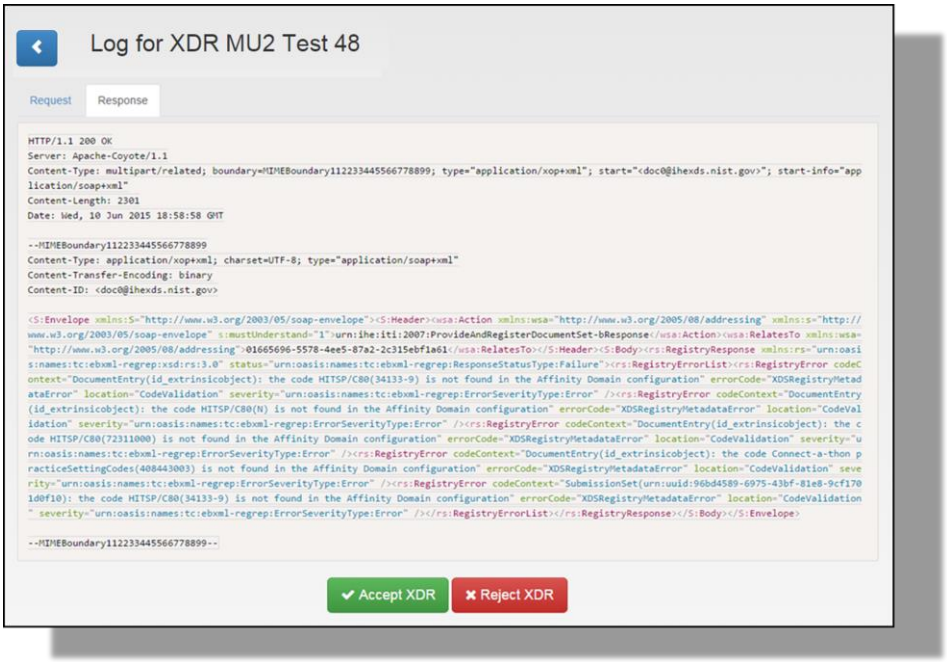



10. The Vendor is presented with the Test Case **Log** screen.

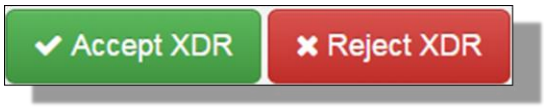

The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR MU2 Test Case 48, the Vendor will select the **Response** tab to review the ETT logged response received from the SUT after transmission of the XDR messages.




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 Delivery Notification requirements; and
    d. Generated conformant process MDNs for messaging tracking purposes.

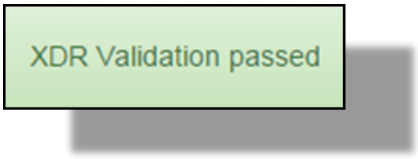


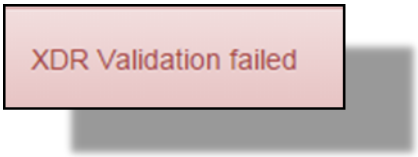

12. If the Vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata,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

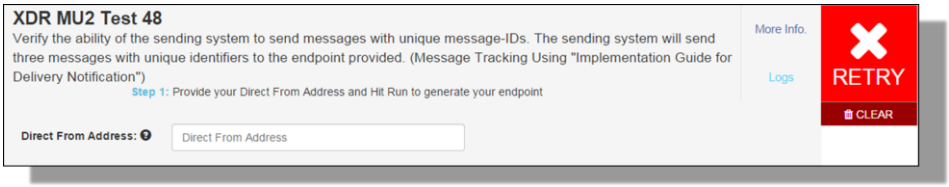
13. The ETT presents Vendor conformation based upon the selection made.






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).

## 5.8 XDR MU2 Test Case 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 delivery notification 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 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 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*.

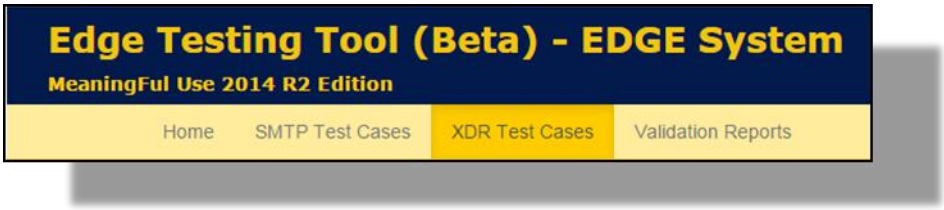
This is a required test and maintains compliance with the secure health data transport messaging formats, processing requirements, and communication standards for Direct Edge message exchanges. See Section 1.5.2.2 of the *Implementation Guide for Direct Edge Protocols* document.

This test correlates to Test ID 20 of the MU2 Tracking tab within the *DirectEdgeProtocols* spreadsheet and TE170.314(b)(8) – 2.10 within the ONC 2014 Edition approved Test Procedure requirements document.

### 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.

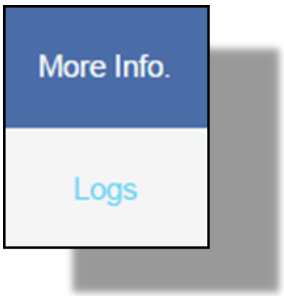
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.

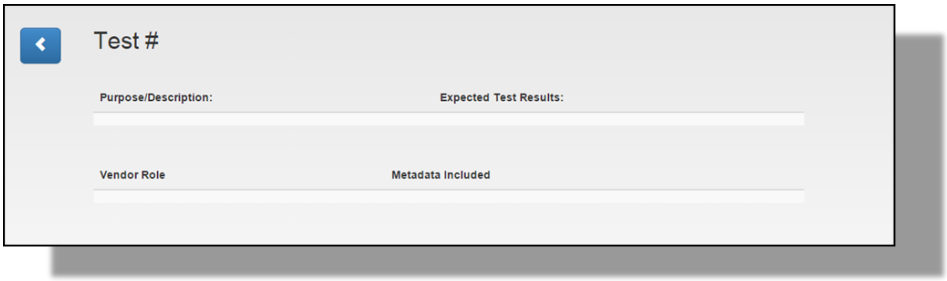



3. From the testing options available, select **Your System as: Sender**. This will enable test case selection.

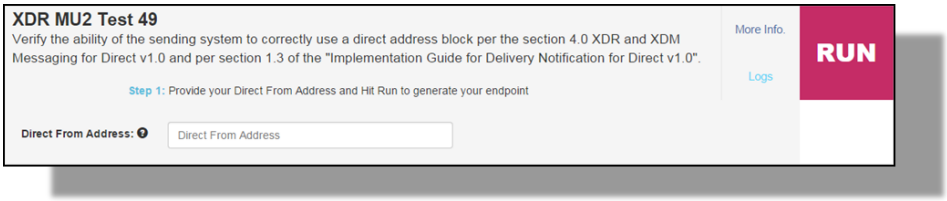

***Note**: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

4. To gain additional information concerning XDR MU2 Test Case 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.



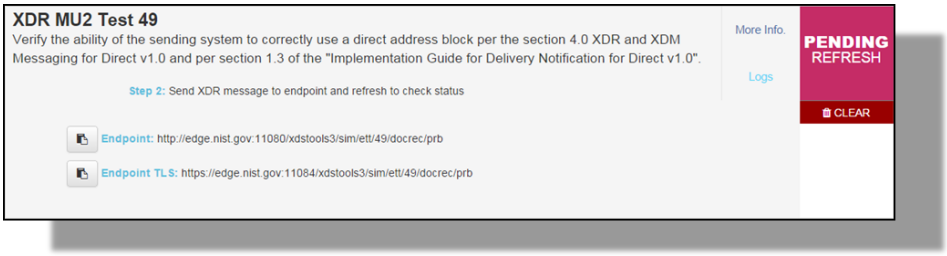
5. To initiate XDR MU2 Test Case 49, the Vendor must provide the **Direct From Address** for the SUT (e.g., operated and managed Edge system). This enables the ETT to accept sent XDR message transmissions from the SUT and process/present log data accordingly.




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

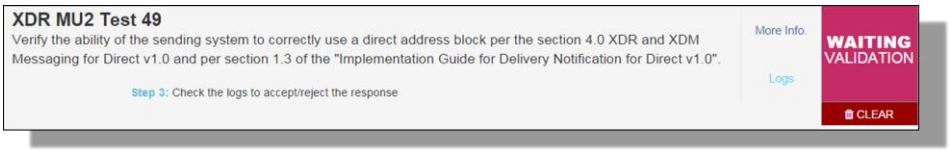

> ***Note**: Instructions are labeled in sequential order (e.g., '**Step 1**', '**Step 2**', '**Step 3**') in the content description of the Test Case. For this Test Case, the '**TLS Endpoint**' is provided by the Tester (e.g., Vendor).*

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.

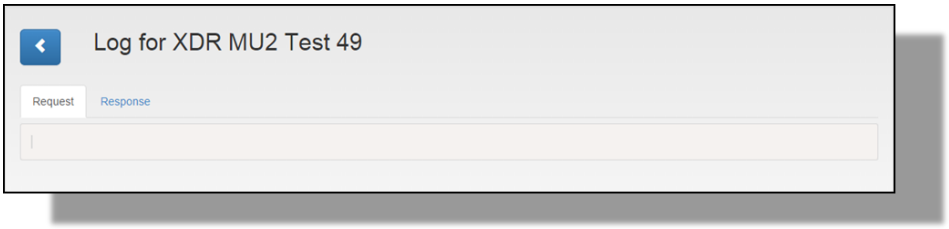



8. Once the message has been transmitted from the SUT to the ETT endpoints, the Vendor clicks the **Pending Refresh** button for the Test Case.


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

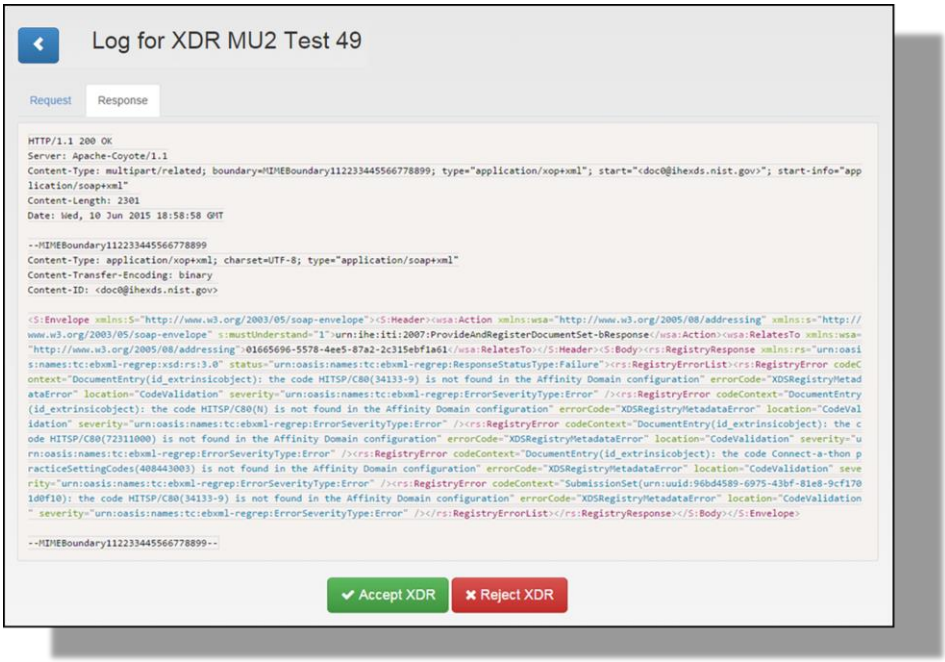



10. The Vendor is presented with the Test Case **Log** screen.




The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR MU2 Test Case 49, the Vendor will select the **Response** tab to review the ETT logged response received from the SUT after transmission of the XDR messages.

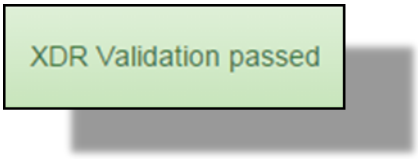

11. Within the Log, the Vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
    a. Accurately established a connection with the ETT;
    b. Formed/transmitted the XDR messages; and
    c. Upheld compliance with the Direct address block conformance requirements within Section 4.0 of the *XDR and XDM for Direct Messaging v1.0* publication and Section 1.3 of the *Implementation Guide for Direct Edge Protocols* publication.

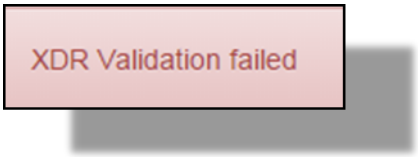



12. If the Vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata,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


***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).*

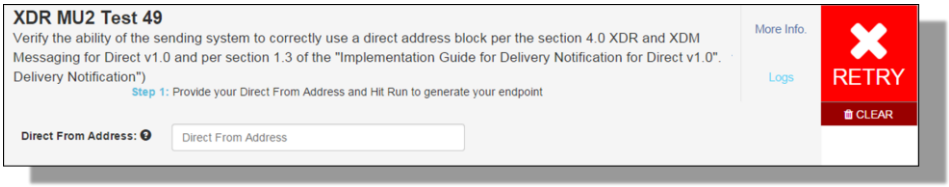
13. The ETT presents Vendor conformation based upon the selection made.






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).

## 5.9 XDR MU2 Test Case 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 MU2 Tracking tab within the *DirectEdgeProtocols* spreadsheet and TE170.314(b)(8) – 2.01 within the ONC 2014 Edition approved Test Procedure requirements document.

### 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.

#### 5.9.1.1 50a

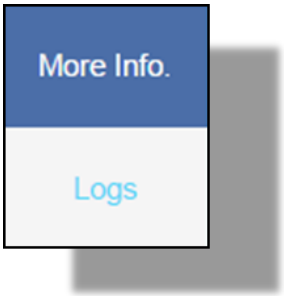
16. Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 7 within 2.2 Registration.

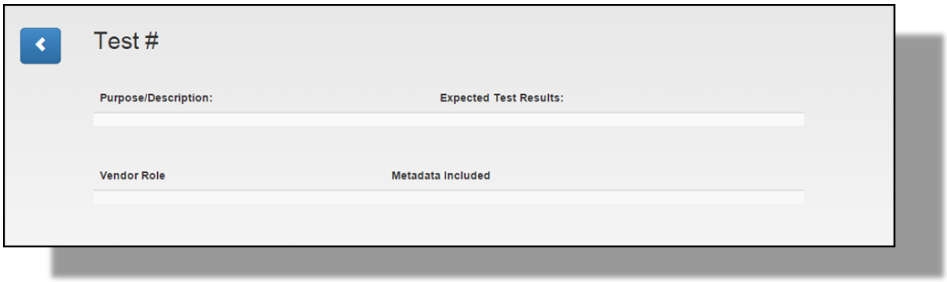
17. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.


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

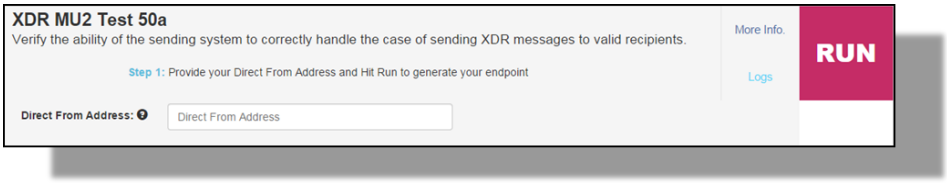

***Note**: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

19. To gain additional information concerning XDR MU2 Test Case 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.






20. To initiate XDR MU2 Test Case 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.



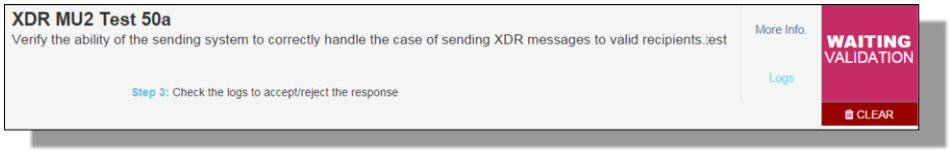

21. Once the SUT's Direct From Address has been populated in the Test Case, clicking **Run** initiates the first testing step.


***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).*

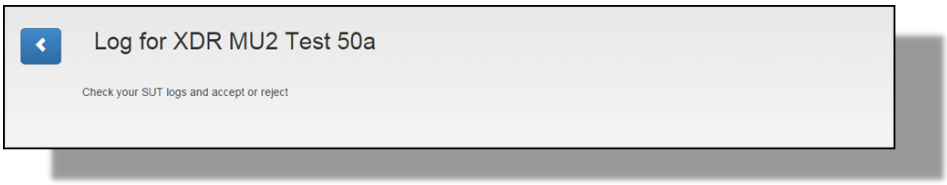
22. The Vendor is prompted to navigate to the SUT's messaging client and create a new XDR message. These new message must be accurately formed in the correct syntax. The Vendor will send the XDR message to one of the two ETT generated endpoints (TLS or non-TLS) for the Test Case. The Vendor will also 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 compete this, the Vendor clicks the **Waiting Validation** button.




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

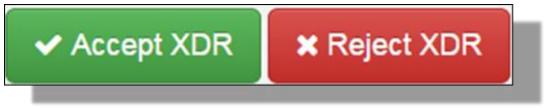



The Vendor is prompted to check the SUT's local logs and validate that the process MDNs generated as a result of sending the XDR message to both the ETT and valid recipients were handled correctly.


26. After the Vendor has reviewed and validated the SUT's log, the Vendor navigates back to the ETT's Log screen for XDR MU2 Test Case 50a. The Vendor finalizes the review of the testing data by viewing the Log's option tabs message **Request** and **Response** data.

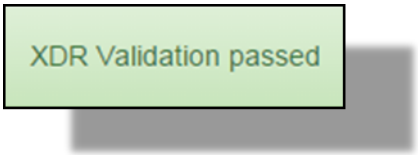

31. The Vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT:
    l. Accurately established a connection with the ETT;
    m. Correctly created and transmitted the XDR message to the provided ETT endpoint recipient and additional valid message recipient;
    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.

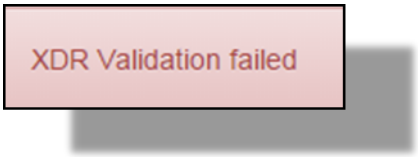

27. If the Vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata,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

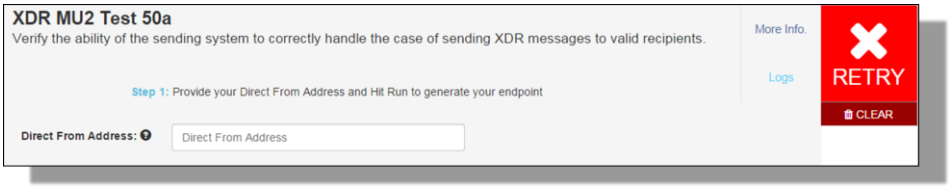
28. The ETT presents Vendor conformation based upon the selection made.



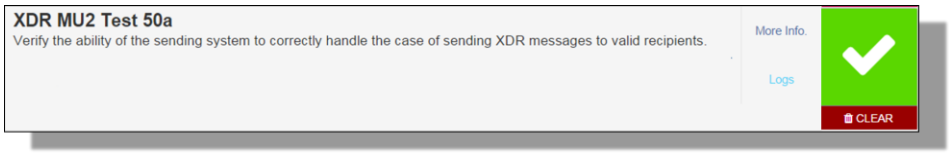



29. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case.

    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).

#### 5.9.1.2 50b

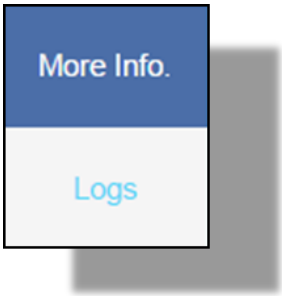
1. Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 7 within 2.2 Registration.

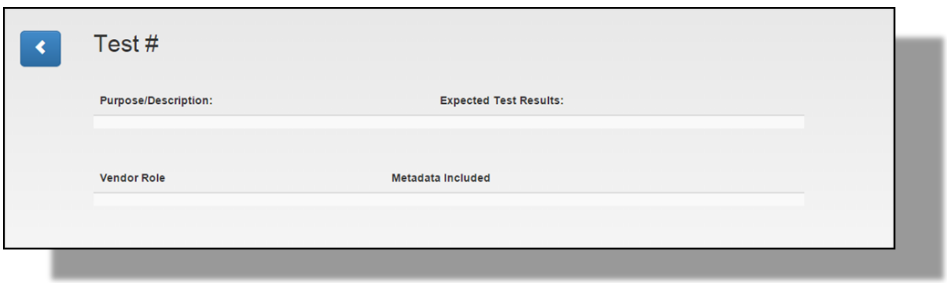
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.


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

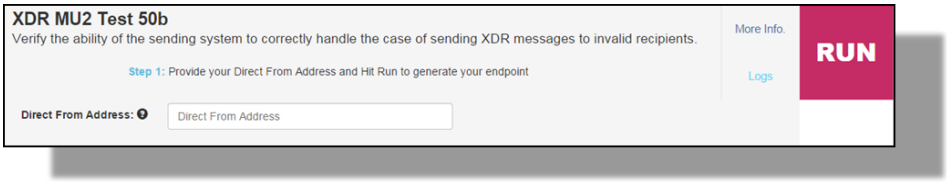

***Note**: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

4. To gain additional information concerning XDR MU2 Test 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.



5. To initiate XDR MU2 Test 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.



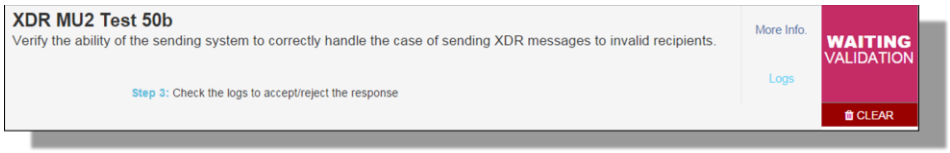

6. Once the SUT's Direct From Address has been populated in the Test Case, clicking **Run** initiates the first testing step.


***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).*

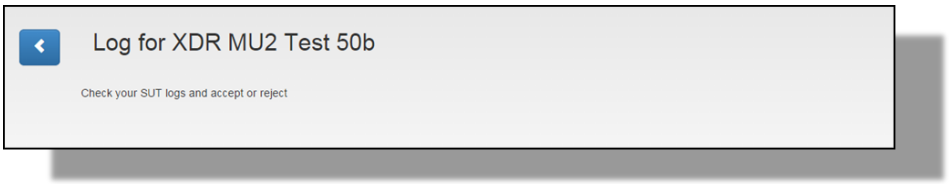
7. The Vendor is prompted to navigate to the SUT's messaging client and create two a new XDR message. These new message must be accurately formed in the correct syntax. The Vendor will send the XDR message to one of the two ETT generated endpoints (TLS or non-TLS) for the Test Case. The Vendor will also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


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

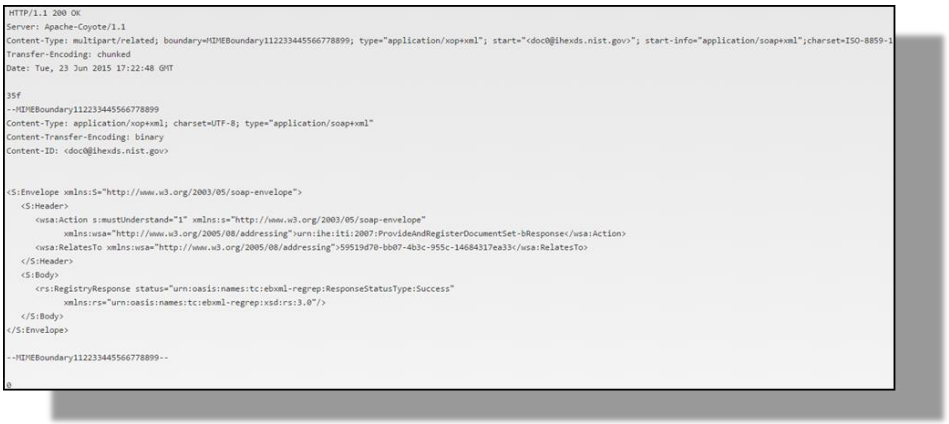

9. The ETT checks the generated endpoint(s) for the presence of a newly received XDR message. The Vendor is prompted to manually validate if the test results conformed to the testing objectives. To compete this, the Vendor clicks the **Waiting Validation** button.




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




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



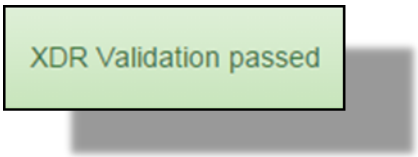

11. After the Vendor has reviewed and validated the SUT's log, the Vendor navigates back to the ETT's Log screen for XDR MU2 Test Case 50b. The Vendor finalizes the review of the testing data by viewing the Log's option tabs message **Request** and **Response** data.


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


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

***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).*

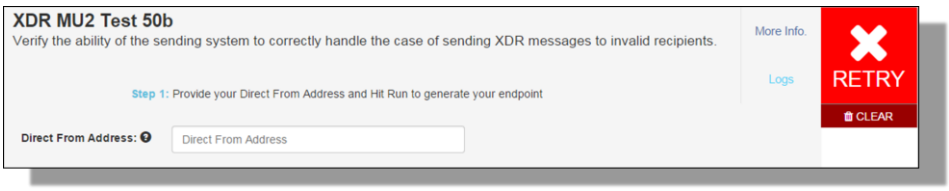
13. The ETT presents Vendor conformation based upon the selection made.



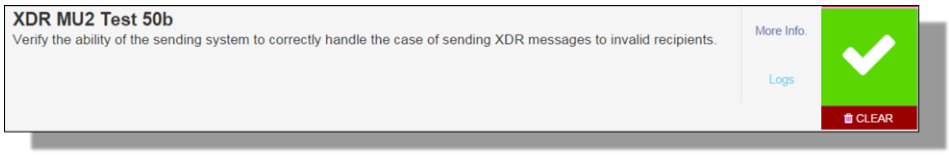


14. Acceptance or rejection of the XDR message Log content results in the overall success or failure of a Test Case.

    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 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).

# 6.0 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 |

## 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 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 Vendor validates through '**Log**' review that the SUT successfully received the ETT's request to established a Mutual TLS connection, the SUT authenticated with the ETT before transmitting data, and testing adhered to the specified requirements within *XDR and XDM for Direct Messaging v1.0* and *IHE XDR Profile for Limited Metadata Document Sources*.

This 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.

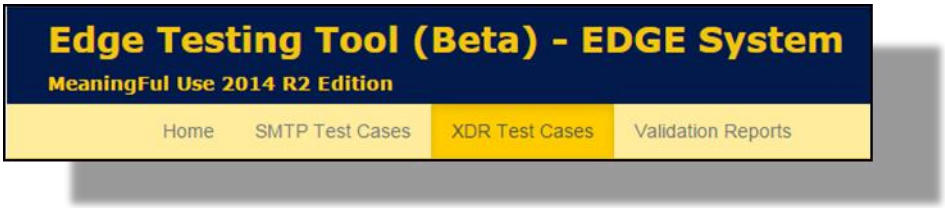
This test correlates to Test ID 8 of the XDR Test Cases tab within the *DirectEdgeProtocols* spreadsheet and TE170.314(b)(8) – 4.01 within the ONC 2014 Edition approved Test Procedure requirements document.

### 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.

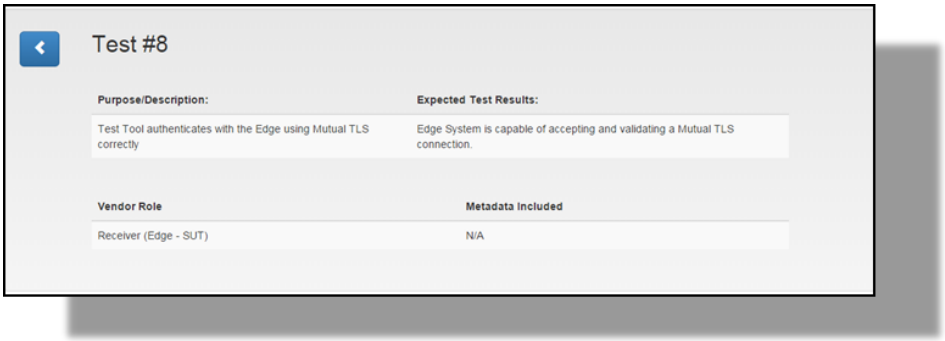
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.




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

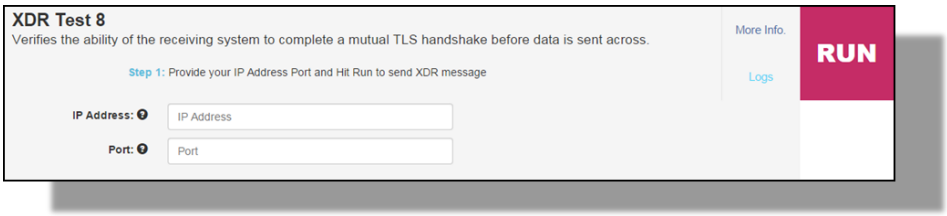

***Note**: XDR Test Cases do not implement the same testing Profile feature that the SMTP Test Cases do.*

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.




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.

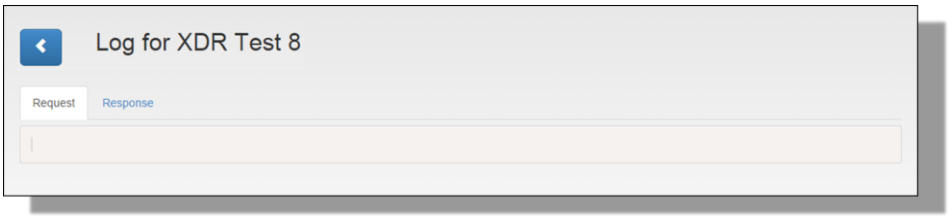



6. Once the SUT's IP Address and Port has been inserted, clicking **Run** initiates the test and XDR message transmission from the ETT to SUT.


***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 compete this, the Vendor clicks the **Waiting Validation** button.

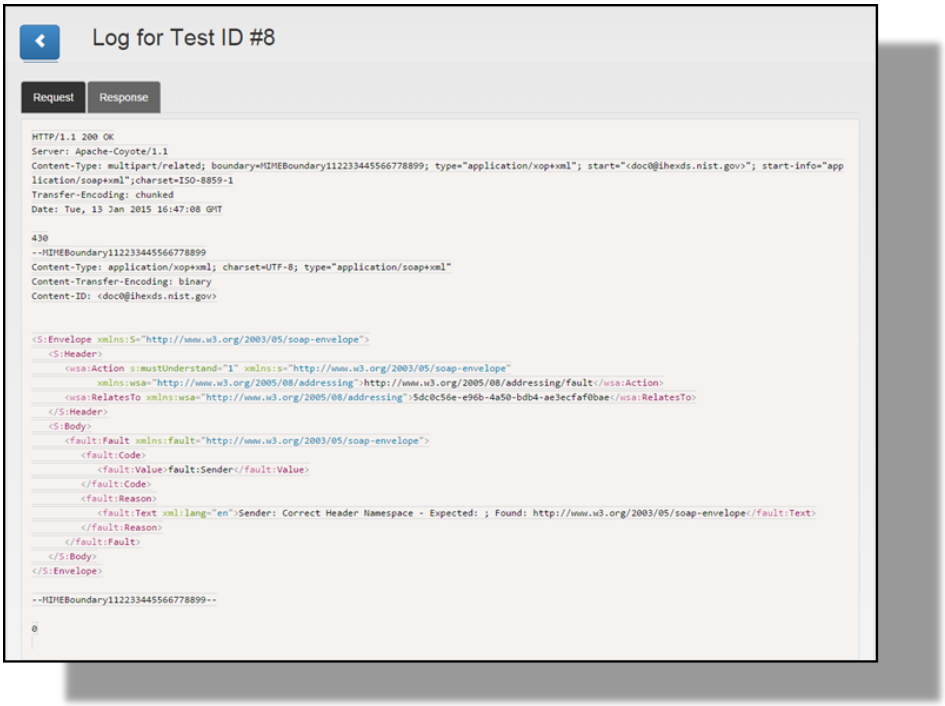

8. The Vendor is presented with the Test Case **Log** screen.



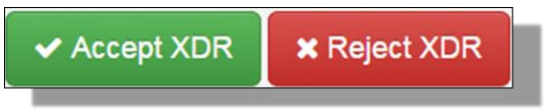

The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test Case 8, the Vendor will select the

**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.

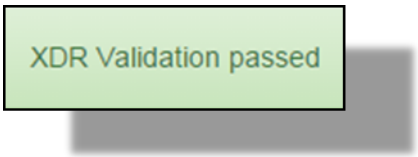



10. If the Vendor accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log data/metadata,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

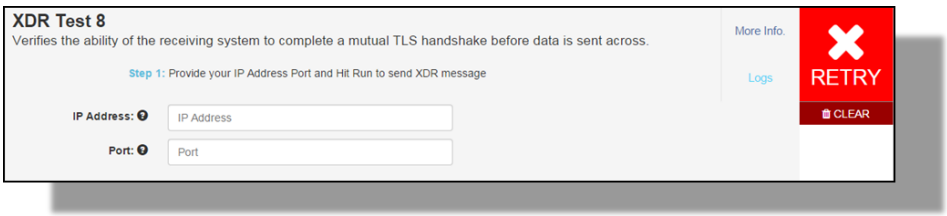
11. The ETT presents Vendor conformation based upon the selection made.



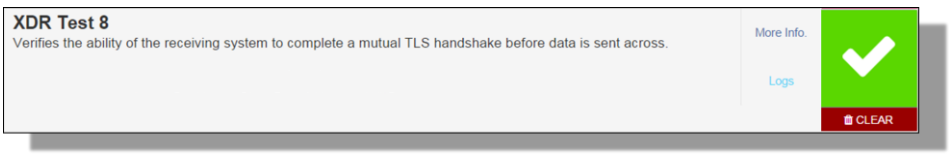


12. Acceptance or rejection of the XDR message Log content results in the overall success of failure of a Test Case.

    XDR message rejection results in a red X and prompts the Vendor to **Retry** the test (reference Step 1 within Section 6.1.1 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.*

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


## 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 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 Vendor validates through '**Log**' review that the SUT attempted to established 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 2014 Edition approved Test Procedure requirements document.

### 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.


3. From the testing options available, select **Your System as: Receiver**. 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 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.

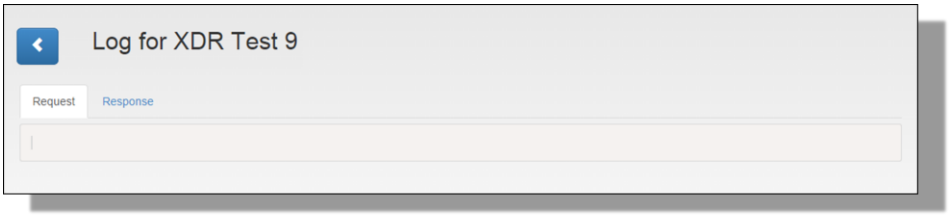

5. To initiate XDR Test Case 9, the Tester (i.e., Vendor) must provide the **IP Address** and **Port** for the SUT (e.g., operated and managed Edge system). This enables the ETT to communicate with and send an XDR message to the SUT. The provided **IP Address** and **Port** of the SUT is the message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


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 compete this, the Vendor clicks the **Waiting Validation** button.


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



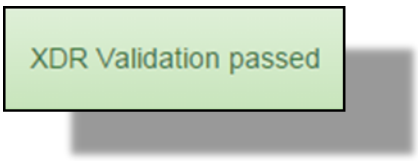

The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test Case 9, the Vendor will select the **Response** tab to review the ETT logged response received from the SUT after the XDR message has been transmitted. The Vendor validates that the SUT attempted to establish a connection to the ETT, received/detected an invalid certificate during the mutual TLS handshake process, and terminated the connection to the ETT before any data was transmitted.

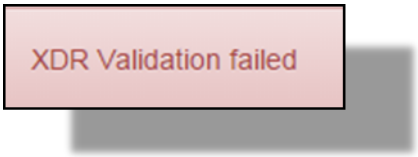

9. Within the Log, the Vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT terminated a mutual TLS connection attempt from the ETT due to an invalid certificate (this is a negative test).


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


***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.


    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).

## 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 2014 Edition approved Test Procedure requirements document.

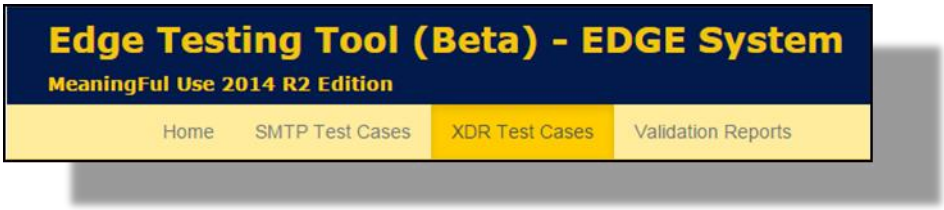
### 6.3.1 TESTING STEPS

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:

#### 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.

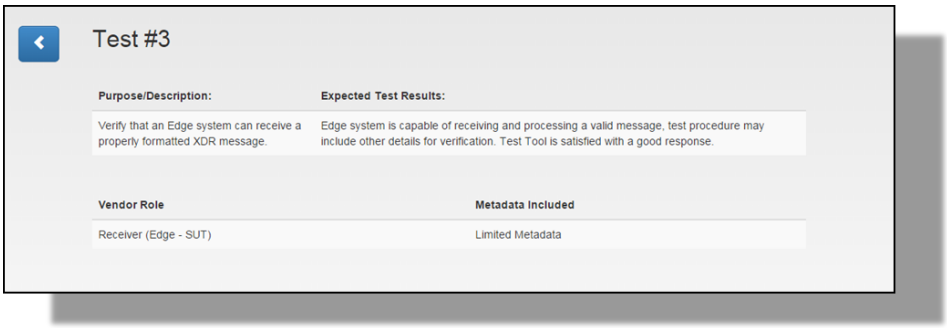
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.




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


***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.




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 compete this, the Vendor clicks the **Waiting Validation** button.

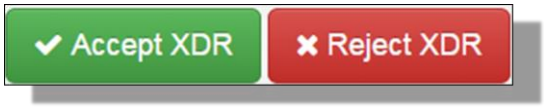

8. The Vendor is presented with the Test Case **Log** screen.


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


9. Within the Log, the Vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT provided the appropriate testing objective

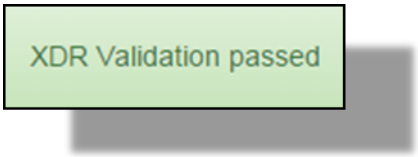
responses for receiving a properly formatted XDR message with Limited Metadata and a Consolidated CDA document attachment.

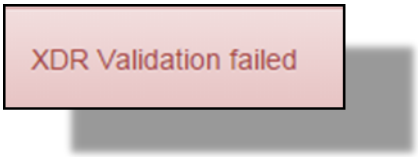

10. If the Tester (e.g., Vendor) accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log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

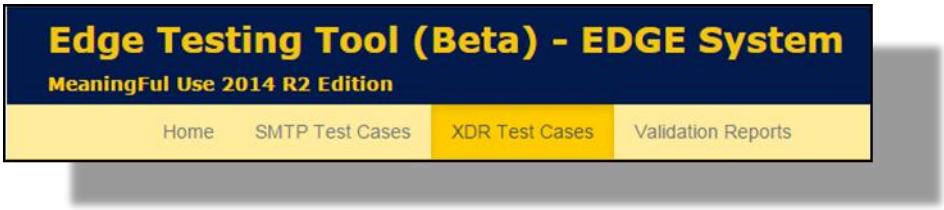

***Note**: In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The 'Validation Report' represents 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).

#### 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.

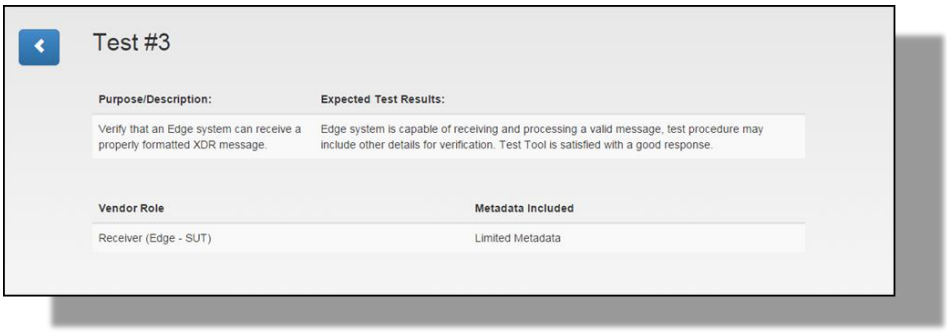
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.



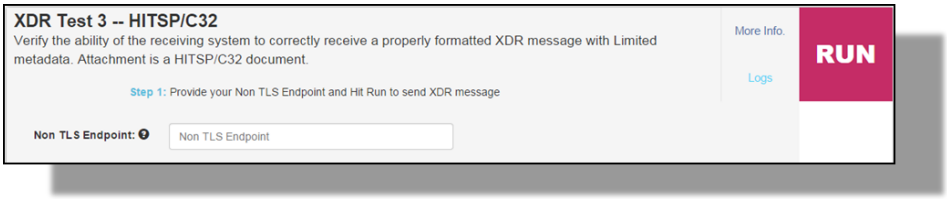

3. From the testing options available, select **Your System as: Receiver**. This will enable test case selection.


***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.



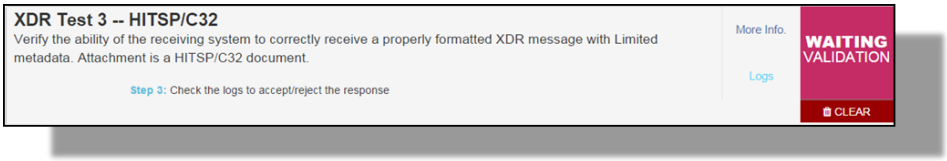

5. To initiate XDR Test Case 3 – HITSP/C32's, the Tester (i.e., Vendor) must provide the **Non TLS Endpoint** for the SUT (e.g., operated and managed Edge system). This enables the ETT to communicate with and send an XDR message to the SUT. The provided **Non TLS Endpoint** of the SUT is the message recipient for this Test Case.




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).*

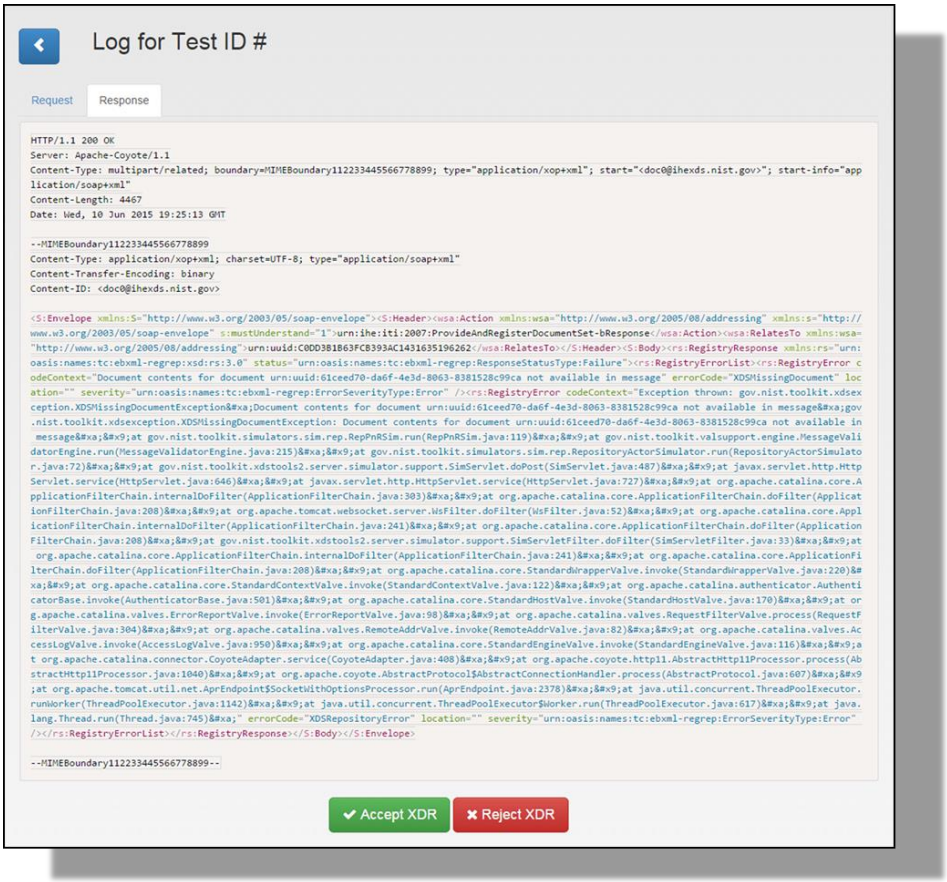
7. Once the XDR message has been sent, the Tester (e.g., Vendor) is prompted to manually validate if the test results conformed to the testing objective. To compete this, the Vendor clicks the **Waiting Validation** button.




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


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

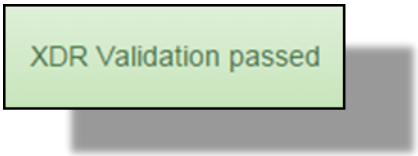

9. Within the Log, the Vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT provided the appropriate testing objective responses for receiving a properly formatted XDR message with Limited Metadata and a HITSP/C32 document attachment.

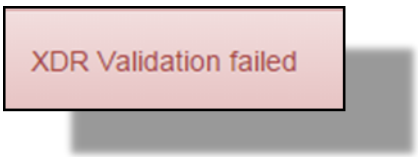



10. If the Tester (e.g., Vendor) accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log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

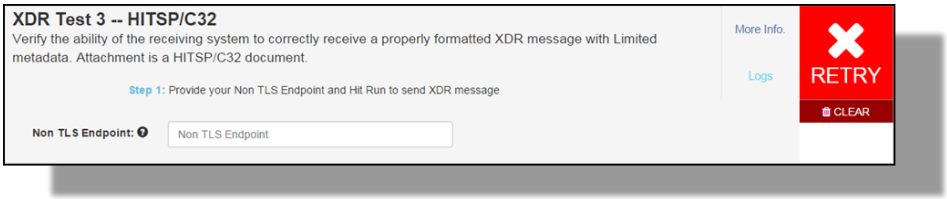
11. The ETT presents Vendor conformation based upon the selection made.




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).


#### 6.3.1.3 3 – CCR

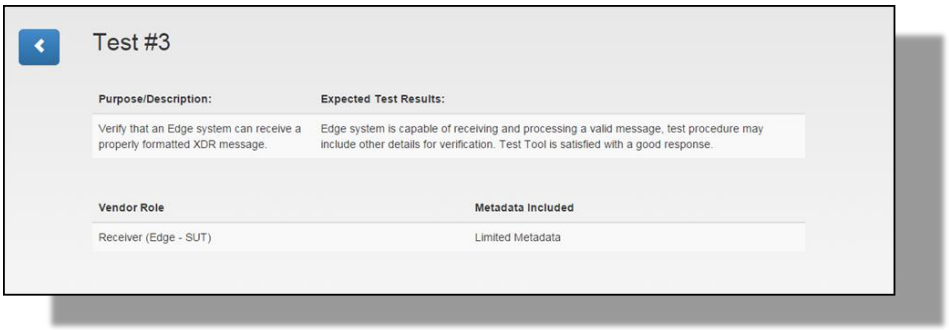
1. Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 7 within 2.2 Registration.

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

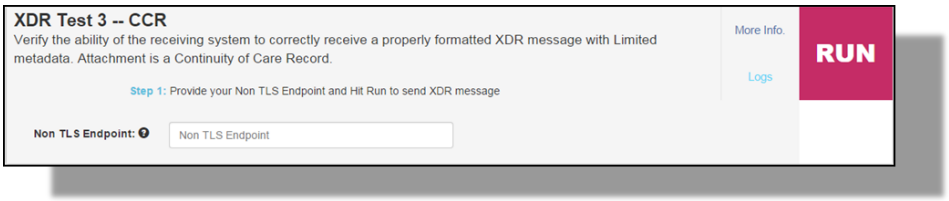

3. From the testing options available, select **Your System as: Receiver**. This will enable test case selection.


***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.




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.

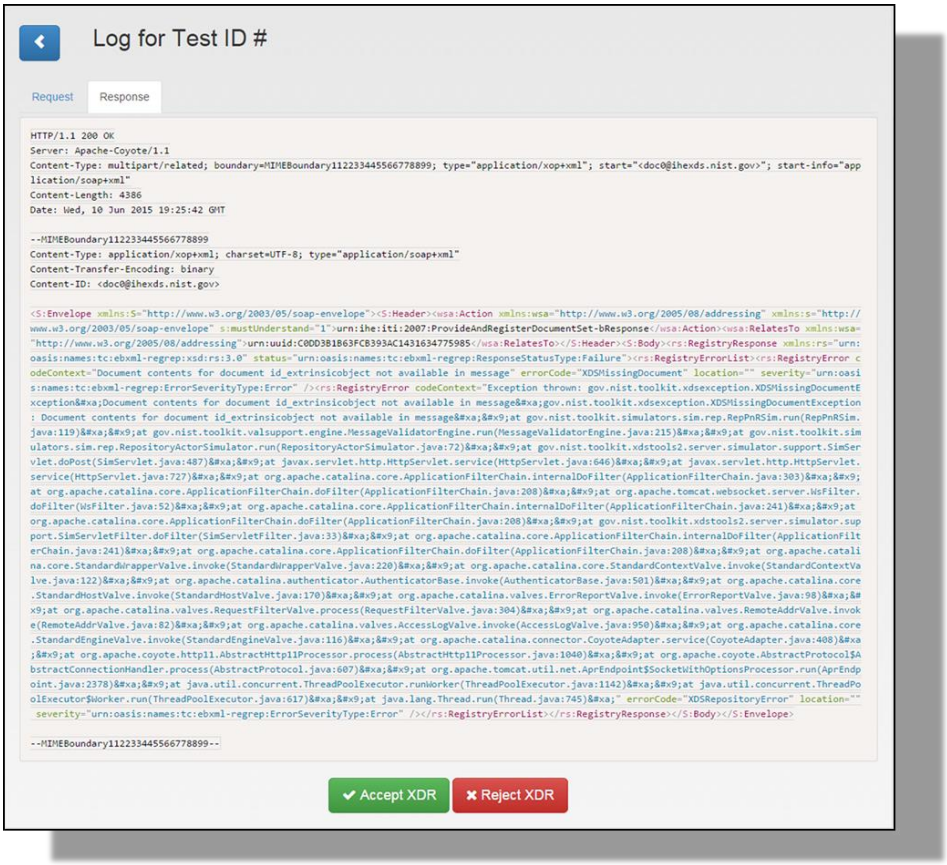

***Note**: Instructions are labeled in sequential order (e.g., '**Step 1**', '**Step 2**', '**Step 3**') in the content description of the Test Case. For this Test Case, the '**TLS Endpoint**' is provided by the Tester (e.g., Vendor).*

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 compete this, the Vendor clicks the **Waiting Validation** button.

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


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

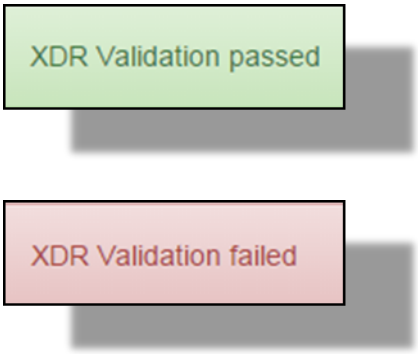

9. Within the Log, the Vendor reviews the testing data content/metadata and performs manual validation to determine if the SUT provided the appropriate testing objective responses for receiving a properly formatted XDR message with Limited Metadata and a Continuity of Care Record document attachment.




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.

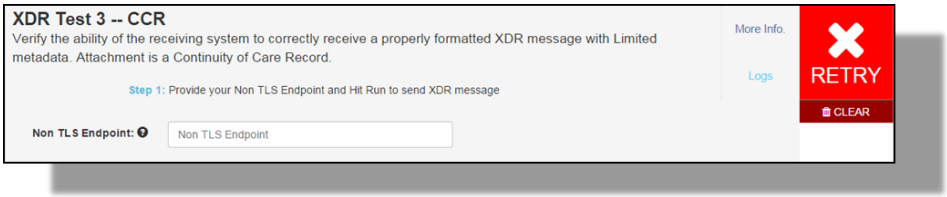

***Note**: '**Accept XDR**' selections correlate with Test Case Success results (e.g., green check mark). Likewise, '**Reject XDR**' selections correlate with Test Case Failures (e.g., red X). Only if the testing objective for a Test Case is in the negative (e.g., verify message rejection) will a '**Reject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


## 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 2014 Edition approved Test Procedure requirements document.

### 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.

#### 6.4.1.1 4a

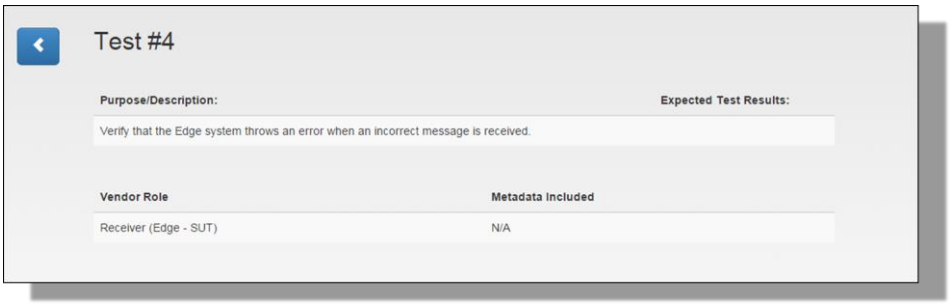
14. Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 7 within 2.2 Registration.

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.


***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).*

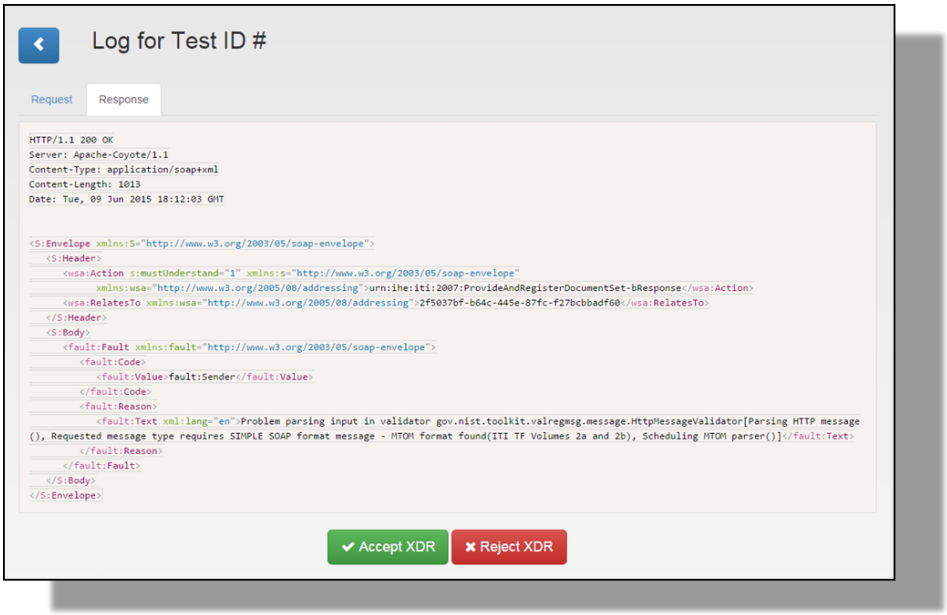
20. Once the XDR message has been sent, the Tester (e.g., Vendor) is prompted to manually validate if the test results conformed to the testing objective. To compete this, the Vendor clicks the '**Waiting Validation**' button.


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

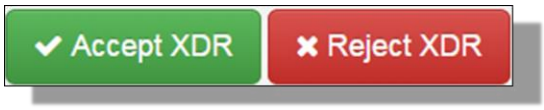

The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test Case 4a, the Vendor will select the

**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 determining if the SUT provided the appropriate testing objective responses for receiving a malformed XDR message with an invalid SOAP header.

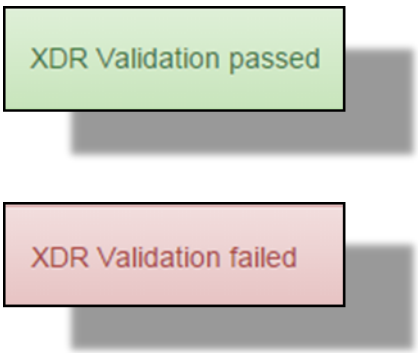



23. If the Tester (e.g., Vendor) accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log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




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.

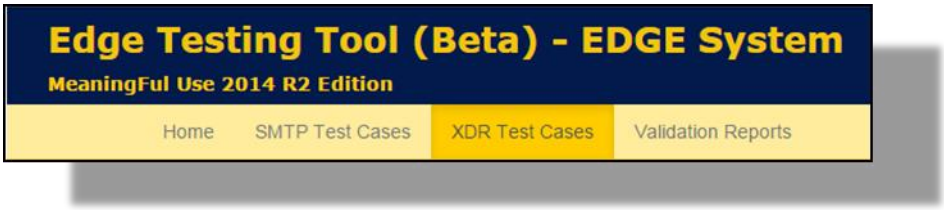

***Note**: In the test procedures, the '**Log**' directly references a single Test Case's generated result (either 'Success' or 'Fail'). The '**Log**' is geared to view individual test results details (e.g., factors for Success or Fail) and acts as a testing artifact. The 'Validation Report' represents 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).


#### 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.

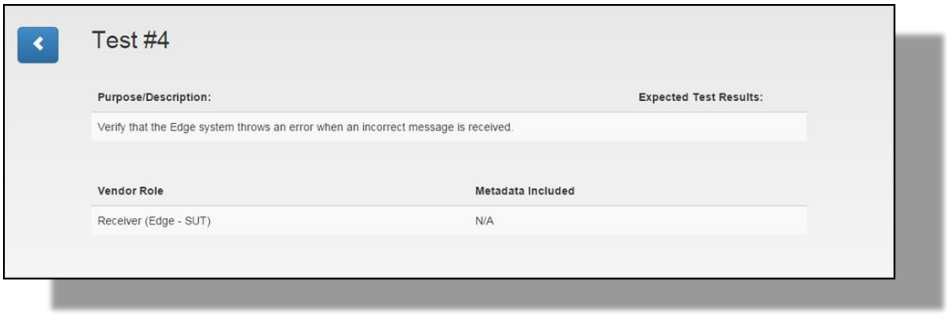
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.




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


***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.



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.

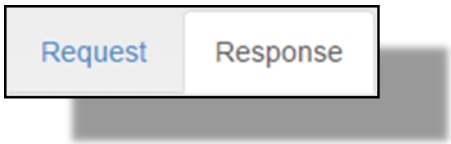

6. Once the SUT's Non TLS Endpoint has been inserted, clicking **Run** initiates the test and XDR message transmission from the ETT to SUT.


***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).*

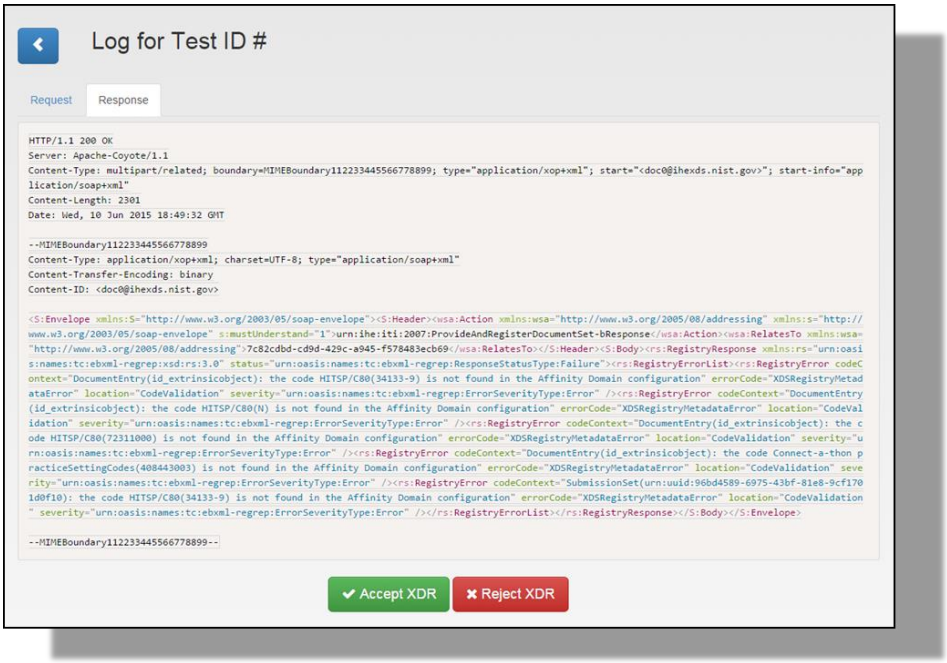
7. Once the XDR message has been sent, the Tester (e.g., Vendor) is prompted to manually validate if the test results conformed to the testing objective. To compete this, the Vendor clicks the **Waiting Validation** button.


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

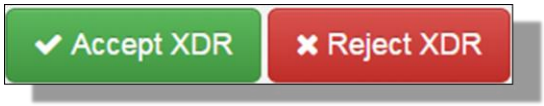
The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test Case 4b, the Vendor will select the **Response** tab to review the ETT logged response received from the SUT after the XDR message has been transmitted.




9. Within the Log, the Vendor reviews the testing data content/metadata and performs manual validation to determining if the SUT provided the appropriate testing objective responses for receiving a malformed XDR message with an invalid SOAP body.

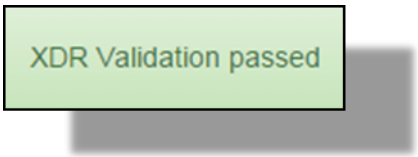



10. If the Tester (e.g., Vendor) accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log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


#### 6.4.1.3 4c

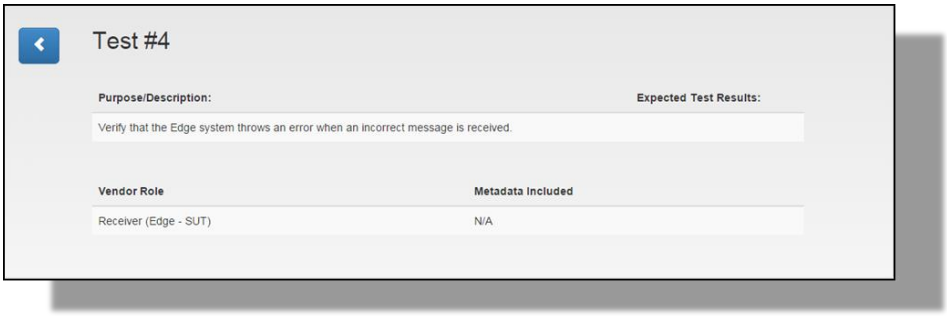
1. Reference Section 2.0 Testing Configuration for Edge System of this ETT User Guide and follow Steps 1 through 7 within 2.2 Registration.

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.


***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.




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.

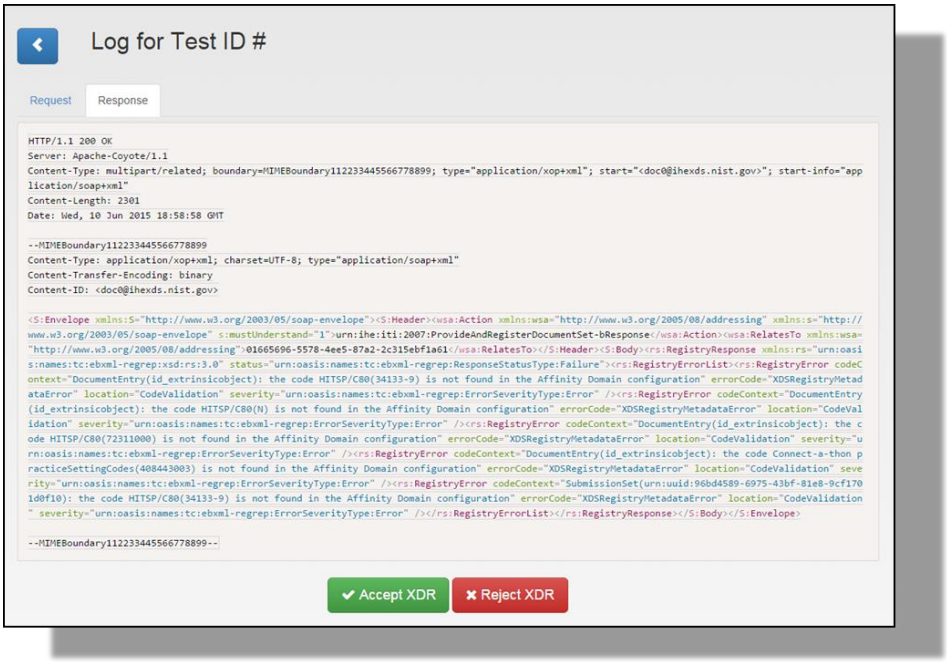

***Note**: Instructions are labeled in sequential order (e.g., '**Step 1**', '**Step 2**', '**Step 3**') in the content description of the Test Case. For this Test Case, the '**TLS Endpoint'** is provided by the Tester (e.g., Vendor).*

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 compete this, the Vendor clicks the **Waiting Validation** button.

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


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


9. Within the Log, the Vendor reviews the testing data content/metadata and performs manual validation to determining if the SUT provided the appropriate testing objective responses for receiving a malformed XDR message with a missing Direct Address Block.

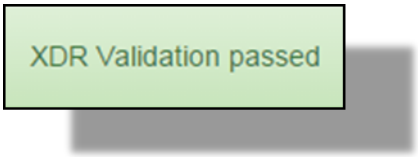



10. If the Tester (e.g., Vendor) accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the

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.





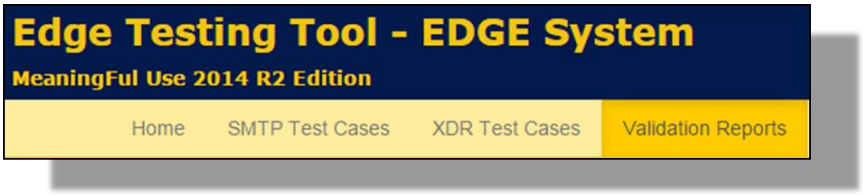
12. Acceptance or rejection of the XDR message Log content results in the overall success of failure of a Test Case.

    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).




#### 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.


***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.

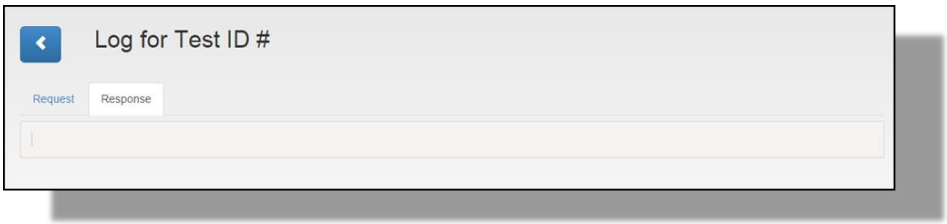

5. To initiate XDR Test Case 4d, the Tester (i.e., Vendor) must provide the **Non TLS Endpoint** for the SUT (e.g., operated and managed Edge system). This enables the ETT to communicate with and send an XDR message to the SUT. The provided **Non TLS Endpoint** of the SUT is the message recipient for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


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.

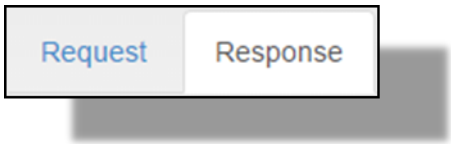

***Note**: Instructions are labeled in sequential order (e.g., '**Step 1**', '**Step 2**', '**Step 3**') in the content description of the Test Case. For this Test Case, the '**TLS Endpoint'** is provided by the Tester (e.g., Vendor).*

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 compete this the Vendor clicks the '**Waiting Validation**' button.

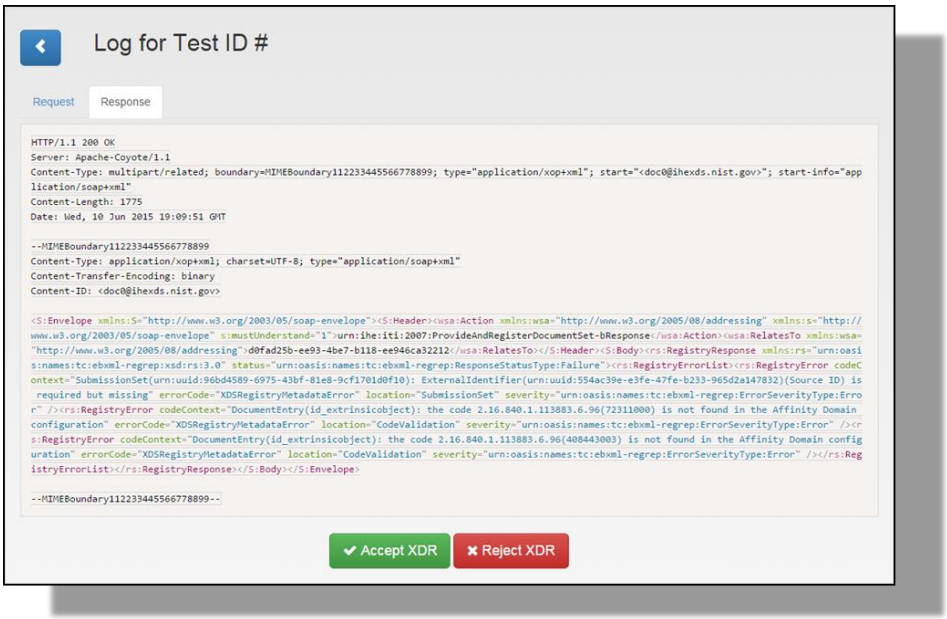

8. The Vendor is presented with the Test Case **Log** screen.




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



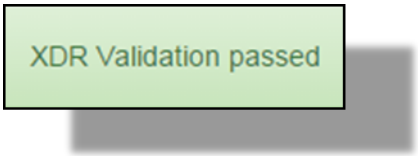

9. Within the Log, the Vendor reviews the testing data content/metadata and performs manual validation to determining if the SUT provided the appropriate testing objective responses for receiving a malformed XDR message with missing XDR metadata.

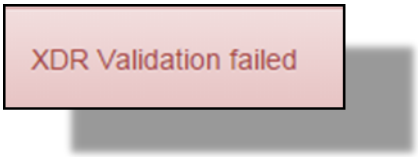


10. If the Tester (e.g., Vendor) accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log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



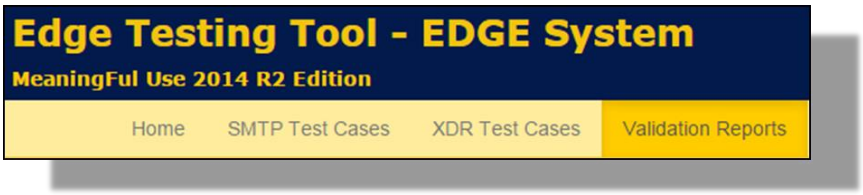

12. Acceptance or rejection of the XDR message Log content results in the overall success of failure of a Test Case.

    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).




## 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 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 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.

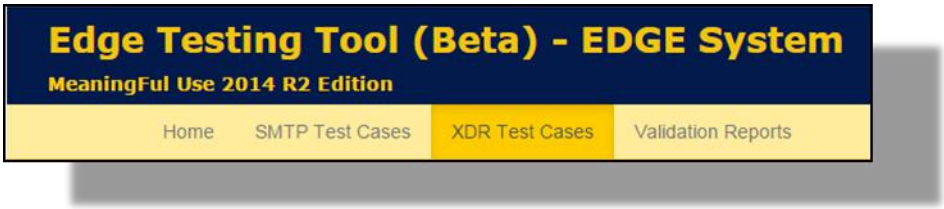
This test correlates to Test ID 5 of the XDR Test Cases tab within the *DirectEdgeProtocols* spreadsheet and TE170.314(b)(8) – 4.04 within the ONC 2014 Edition approved Test Procedure requirements document.

### 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.

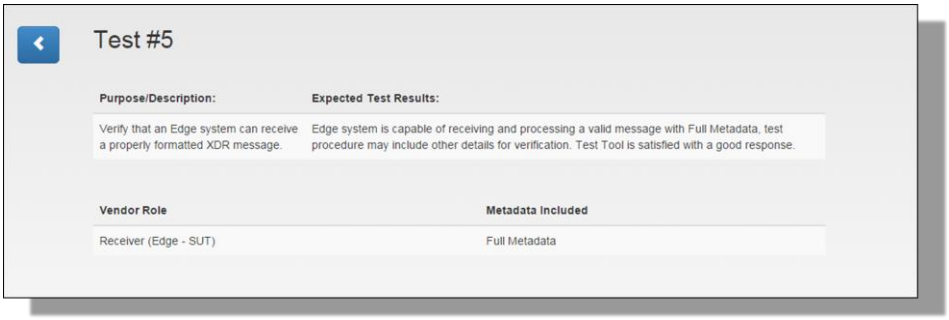
2. For this target XDR test, select **XDR Test Cases** from the Navigation Bar.



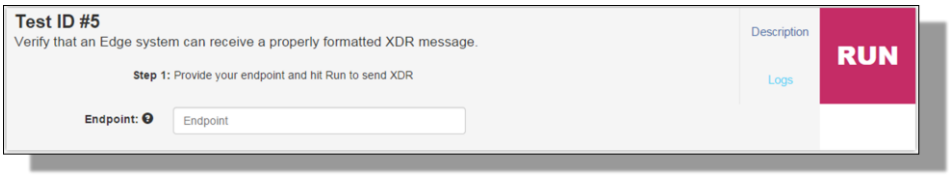

3. From the testing options available, select **Your System as: Receiver**. This will enable test case selection.


***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.



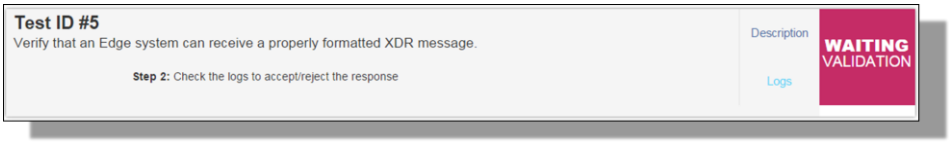

5. To initiate XDR Test 5, the Vendor must provide the **Endpoint** for the SUT (e.g., operated and managed Edge system). This enables the ETT to communicate with and send an XDR message to the SUT. The provided **Endpoint** of the SUT is the message recipient for this Test Case



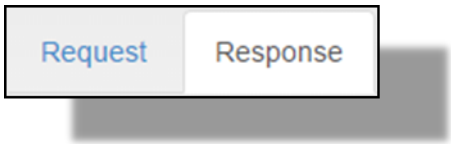

6. Once the SUT's Endpoint has been inserted, clicking **Run** initiates the test and XDR message transmission from the ETT to SUT.


***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).*

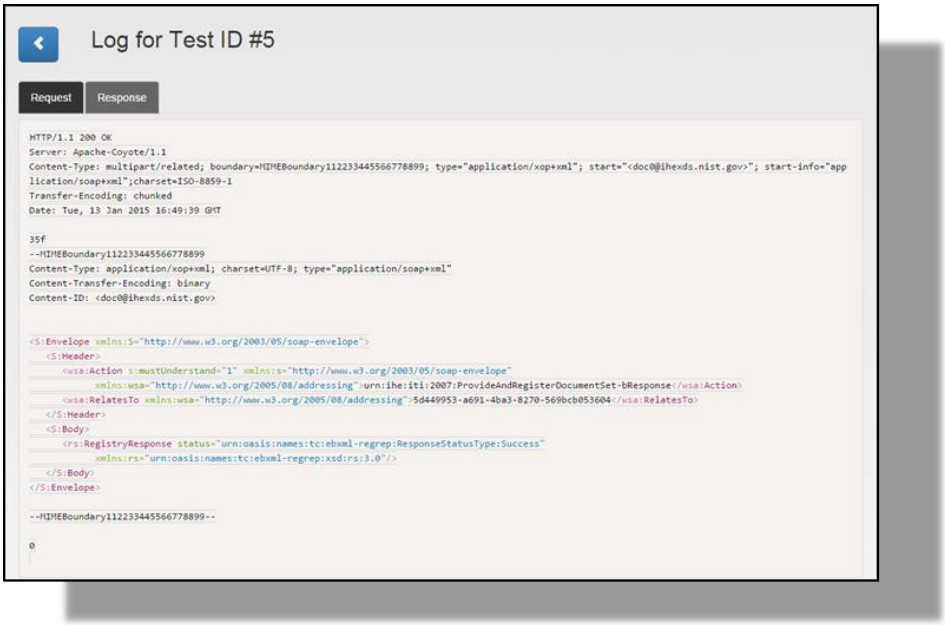
7. Once the XDR message has been sent, the Vendor is prompted to manually validate if the test results conformed to the testing objective(s). To compete this, the Vendor clicks the **Waiting Validation** button.



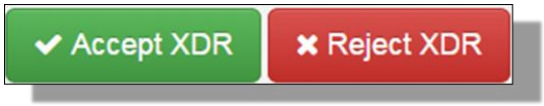
The Log contains option tabs for viewing ETT messaging **Request** and **Response** data. For the specific testing objectives for XDR Test Case 5, the Vendor will select the **Response** tab to review the ETT logged response received from the SUT after the XDR message has been transmitted.




8. Within the Log, the Vendor reviews the testing data content/metadata and performs manual validation to determining if the SUT provided the appropriate testing objective responses for receiving a properly formatted XDR message with Full XDS metadata.

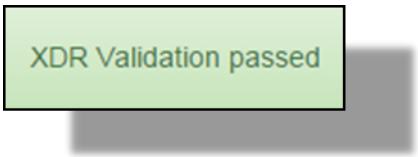



9. If the Tester (e.g., Vendor) accepts the SUT's provided response to the ETT and determines that the Log data/metadata conforms with expectations and testing objectives, then the **Accept XDR** button is selected. However, if the Vendor does not accept the SUT's provided response after review of Log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

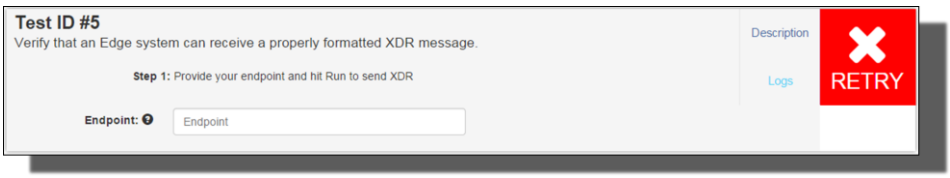
10. The ETT presents Vendor conformation based upon the selection made.





11. Acceptance or rejection of the XDR message Log content results in the overall success 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 6.5.1 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.*