

USER GUIDE

Edge Testing Tool

DRAFT

Table of Contents

1.0	OVERVIEW	4
1.1	Role of NIST	4
1.2	Edge Testing Tool.....	4
1.3	Purpose	4
1.4	Access.....	6
1.5	Testing Overview	6
2.0	TESTING CONFIGURATION FOR EDGE SYSTEM	7
2.1	Configuration Steps.....	7
2.2	Registration	7
2.3	Profile Creation.....	10
2.4	Reporting	13
2.5	Documentation.....	14
3.0	SUT SENDING	16
3.1	SMTP Test Case 14.....	16
3.1.1	Testing Steps.....	16
3.2	SMTP Test Case 18.....	20
3.2.1	Testing Steps.....	21
3.3	SMTP Test Cases 1 through 8	21
3.3.1	Testing Steps.....	23
3.4	SMTP MU2 Test Case 17	24
3.4.1	Testing Steps.....	25
3.5	SMTP MU2 Test Case 45	28
3.5.1	Testing Steps.....	29
3.6	SMTP MU2 Test Case 46	33
3.6.1	Testing Steps.....	34
3.7	SMTP MU2 Test Case 47	37
3.7.1	Testing Steps.....	38
4.0	SUT RECEIVING	43
4.1	SMTP Test Case 16.....	43
4.1.1	Testing Steps.....	44
4.2	SMTP Test Case 17.....	47
4.2.1	Testing Steps.....	48
4.3	SMTP Test Case 20.....	52
4.3.1	Testing Steps.....	52
4.4	SMTP Test Case 22.....	53
4.4.1	Testing Steps.....	53
4.5	SMTP Test Case 9.....	57
4.5.1	Testing Steps.....	58
4.6	SMTP Test Case 10.....	58
4.6.1	Testing Steps.....	59
4.7	SMTP Test Case 11	63
4.7.1	Testing Steps.....	64
4.8	SMTP Test Case 13	69
4.8.1	Testing Steps.....	70

5.0	XDR SENDING	76
5.1	XDR Test Case 6	76
5.1.1	Testing Steps.....	77
5.2	XDR Test Case 7	81
5.2.1	Testing Steps.....	81
5.3	XDR Test Case 1	85
5.3.1	Testing Steps.....	86
5.4	XDR Test Case 2	90
5.4.1	Testing Steps.....	91
6.0	XDR RECEIVING.....	96
6.1	XDR Test Case 8	96
6.1.1	Testing Steps.....	97
6.2	XDR Test Case 9	100
6.2.1	Testing Steps.....	101
6.3	XDR Test Case 3	105
6.3.1	Testing Steps.....	105
6.4	XDR Test Case 4	109
6.4.1	Testing Steps.....	110
6.5	XDR Test Case 5	113
6.5.1	Testing Steps.....	114

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 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 Criteria². 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.

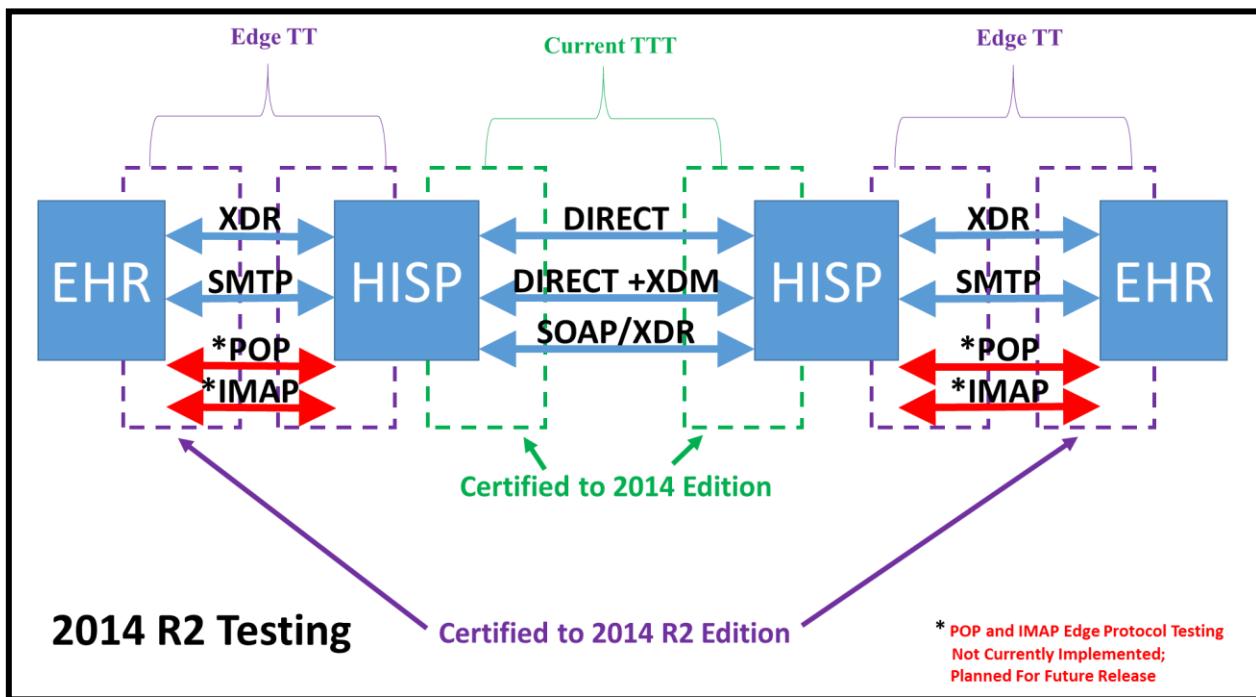


Figure 1: Testing Certification Criteria

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’ is 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 Criteria² 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 have ETT's latest code; however, documentation, content, and testing engine availability cannot be guaranteed. Thus, the development version will be updated as needed.*

1.5 Testing Overview

The ETT will allow Testers (i.e., Vendors) to send and receive messages using various transport methods to and from the SUT (acting as either a 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

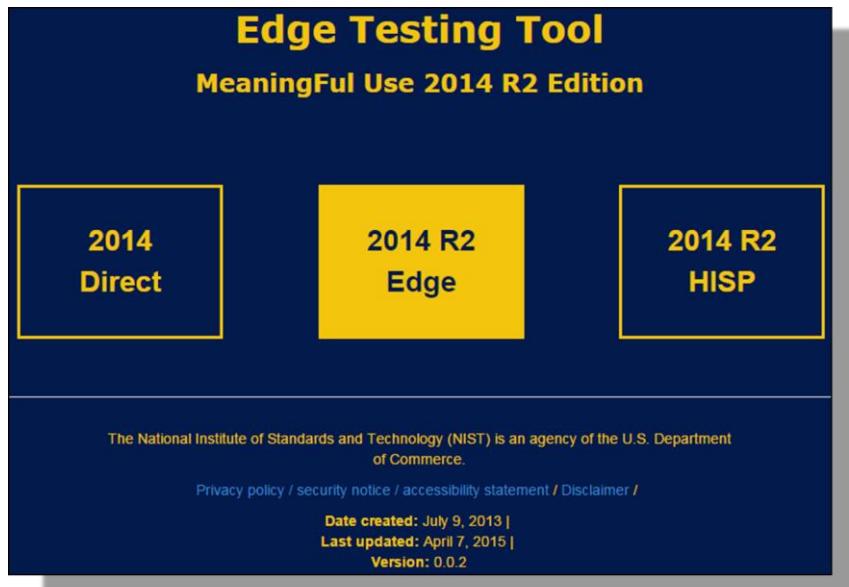
This section guides the Tester (i.e., Vendor) through the necessary configurations and preparation steps for Profile creation and Test Case execution.

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**.

★ Login

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

Username

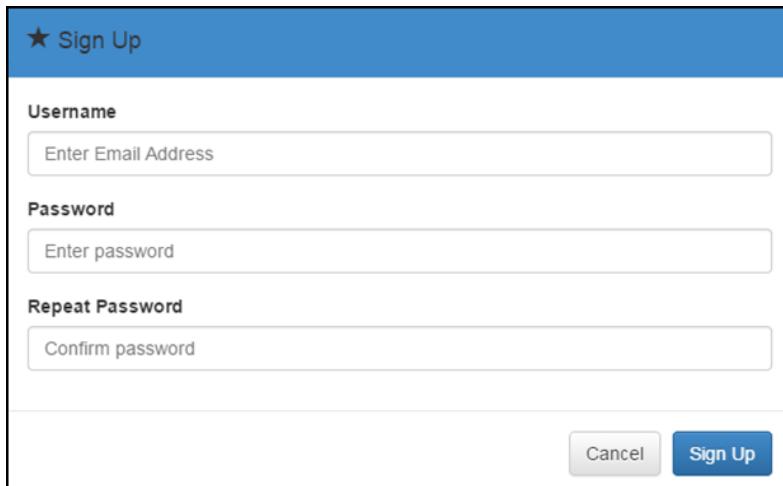
Password

[Forgot password?](#)

Remember me

Cancel Login

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



The image shows a 'Sign Up' form with a blue header bar containing the title. Below the header are three input fields: 'Username' (placeholder: 'Enter Email Address'), 'Password' (placeholder: 'Enter password'), and 'Repeat Password' (placeholder: 'Confirm password'). At the bottom right are two buttons: 'Cancel' and 'Sign Up'.

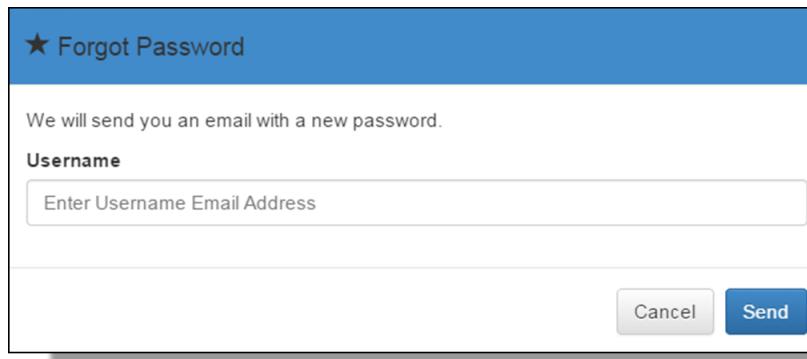


Note: The **Username** email address is used for account creation, historic testing session saves, and delivery notification of ETT specific information by NIST personnel. It is not specifically used as a component of SMTP and/or XDR testing. Testing email addresses are configured within specific **Profile**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

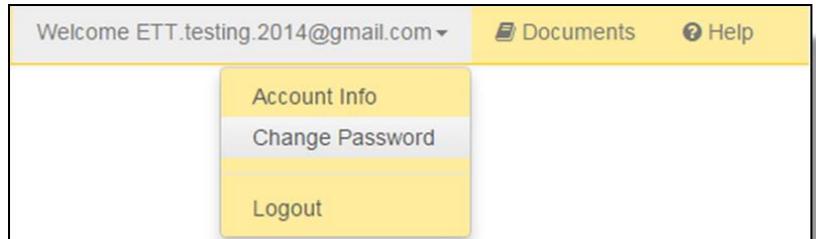


To reset an ETT account **Password**, click the **Forgot Password?** link within the **Login** prompt box. This action sends a temporary password to the Username's linked email address.



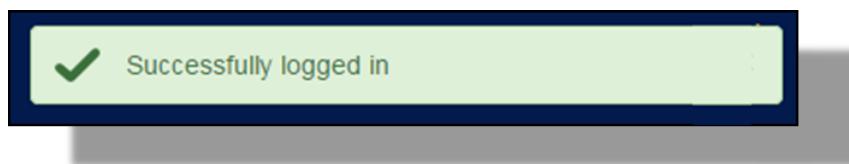
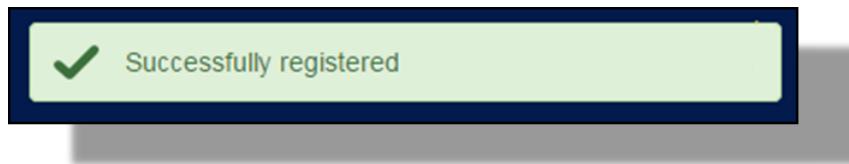
The image shows a 'Forgot Password' form with a blue header bar containing the title. Below the header is a message: 'We will send you an email with a new password.' There is one input field: 'Username' (placeholder: 'Enter Username Email Address'). At the bottom right are two buttons: 'Cancel' and 'Send'.

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**.

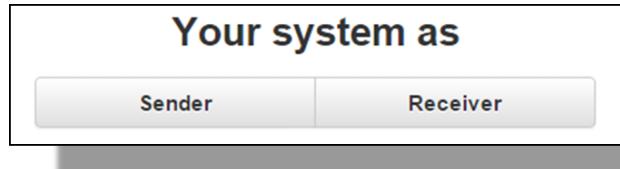


2.3 Profile Creation

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.

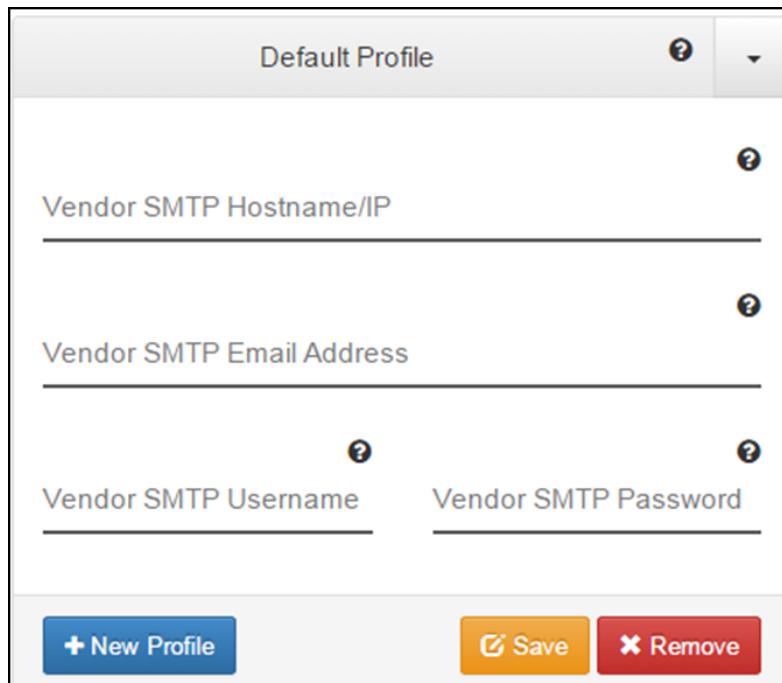
Default Profile

Vendor SMTP Hostname/IP

Vendor SMTP Email Address

Vendor SMTP Username Vendor SMTP Password

+ New Profile Save Remove



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

Default Profile

Hostname/IP address of the vendor SMTP system

Click on the text to edit profile name

Vendor SMTP Hostname/IP

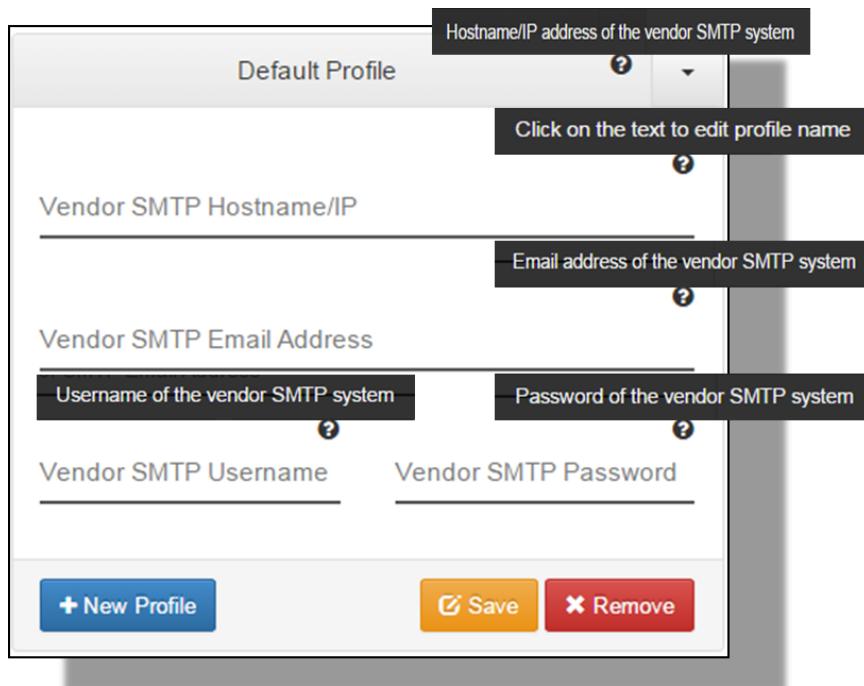
Email address of the vendor SMTP system

Vendor SMTP Email Address

Username of the vendor SMTP system Password of the vendor SMTP system

Vendor SMTP Username Vendor SMTP Password

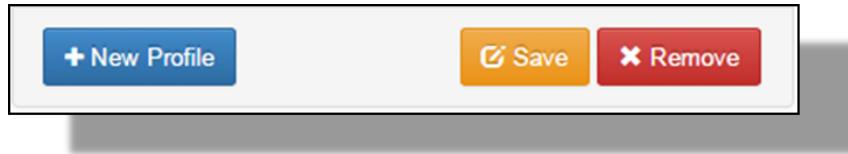
+ New Profile Save Remove



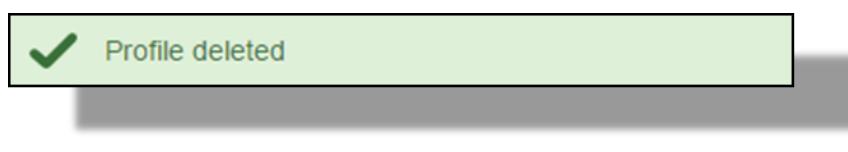
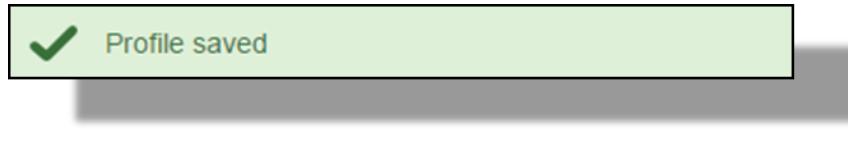


Note: For information on how to find the SMTP / IP of your email client/server, please reference vendor specific documentation or the **Help** button located on the ETT's Navigation Bar.

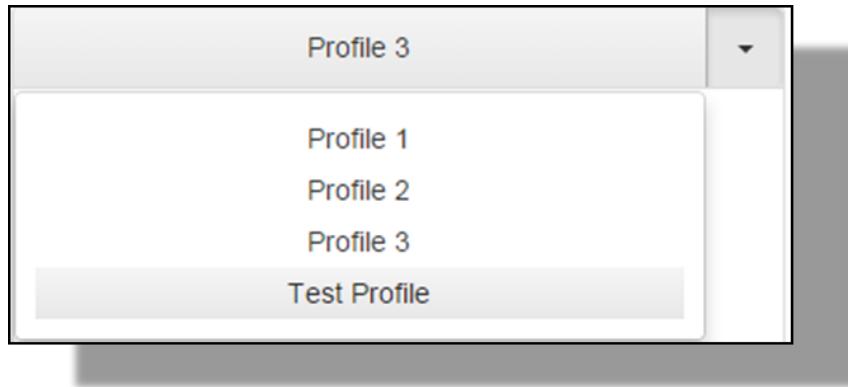
4. Before saving a Profile, assign a unique name (the default Profile name is **Default Profile**). Click the Profile name, delete the existing text, and type a new name. Upon population of the testing Profile, select **Save**. To delete a saved Profile, select **Remove**



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.

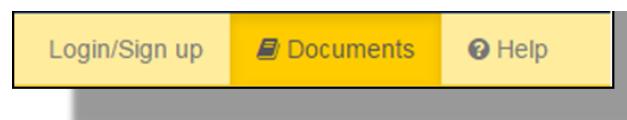
A screenshot of the Validation Reports tab from the Edge Testing Tool. It displays three test profiles: Test Profile 1, Test Profile 2, and Test Profile 3. Each profile includes the SUT SMTP Address (smtp.gmail.com) and SUT Email Address (sut.example@gmail.com), along with a "Show Report" button.

- !**
- Note: For a given testing session, the total number of ETT testing Profiles used will be displayed within the Validation Report tab.*
3. By clicking on the **Show Report** button, the Vendor is given the Test Case executed, a time ran, and Success or Failure of the test. The '**Log**' for each executed Test Case provides further detailed information concerning evidence to support Success or Failure.

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

2.5 Documentation

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



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 Test Procedure requirements document.

3.1.1 TESTING STEPS

To execute SMTP Test 14 and assess the SUT's ability to accurately form 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.

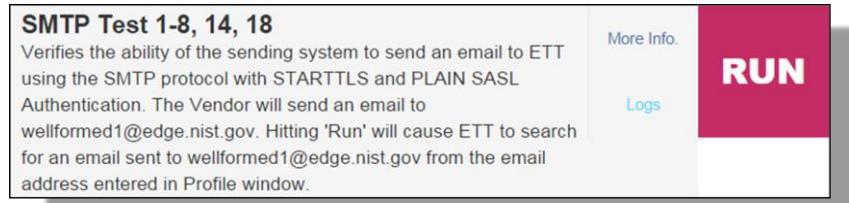


3. From the testing Profile, select ‘**Sender**’.



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. Navigate to the Test Case’s execution interface.



To gain additional information concerning a target Test Case’s intended purpose (including Description, Vendor/SUT roles), click ‘**More Info**’ link for the Test Case.

The screenshot shows a modal window titled 'SMTP Test 1-8, 14, 18'. At the top left is a back arrow icon. Below it is a 'Description:' label with the text: 'The credentials for SASL authentication is vendoraccount@hit-testing2.nist.gov / vendortesting123'. A table below shows vendor roles: 'Vendor Role' (sender), 'Vendor Edge' (green checkmark), and 'Vendor HISP' (green checkmark). At the bottom right of the modal is a blue 'Run' button.

5. With the Profile saved, More Info reviewed, and ‘**SMTP Test 1-8, 14, 18**’ selected, perform 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.
 - a. Wait at least 60 seconds from sending the message to allow successful transmission to the ETT endpoint recipient.
 - b. Click ‘**Run**’ to execute the Test.



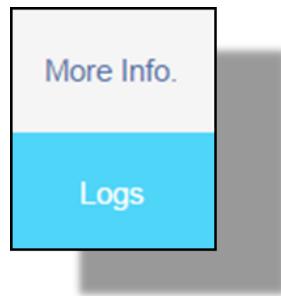
6. The test will process and render one of two results: ‘**Pass**’ or ‘**Fail**’.
 - A test Pass is indicated by a green check and a test Fail is indicated by a red X.

- 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 a particular target Test Case, click the ‘**Log**’ link.



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

The screenshot shows a test log titled "Log SMTP Test 1-8, 14, 18". It displays a summary table with four columns: Criteria Met, Request Time out, Proctored, and Time elapsed (seconds). All three rows in the table have an "X" in the first three columns and a value of 0 in the fourth column. Below the table is a section titled "Request responses" containing a large block of raw text representing an email message header and body. At the bottom is a section titled "Attachments" with a small JSON-like preview.

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

Request responses

```
Content-Type: multipart/alternative; boundary=089e01634b906425100514cb5cebDKI
M-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=gmail.com; s=20120113;
h=mime-version:date:message-id:subject:from:to:content-type;
bh=w2eRwQF6ugsEB2+yeH2W+yjZ8T+pY3Z01Cak6FT1lLE=;
b=xmhpXXAobArLM84d0jjrx4r8NXl2elmTyLB8pxGOC06VRr/m+KoumZbvbUlkEewp4
qCkFuMTVQSSi+oaUxeRP0n4TDPhgnqht3f43EJ1KKzWbHcjotA1/C2RwMMTLt9qtK08b
mfIKMvQLtthyNyle5ZdykMfjZw83H2cDMGvNhsM1270418LKeIycSg+dALF8CPbHh0
OJWqEVSQ304W5AKSh+xpP258H1R1FpjbowkIGYEJGMkn8MaJHOBDC4P/q62viuOyoAii
8lqXwIT5pM5osFKUiKGnk3xs13UraJ+TVWRsiy6OfzzAGGU33lNMOpjyBB8BYsztWgAKUT
alMw==Date: Tue, 28 Apr 2015 12:29:04 -0400Delivered-To: *****@From
m: test test <sut.example@gmail.com>MIME-Version: 1.0Message-ID: <CAJ3w=-JWM_4
D-8g23wiYTSEVsyq-jVAodgf_Q1qvPApWYjSk=g@mail.gmail.com>Received: by 10.76.14
6.4 with HTTP; Tue, 28 Apr 2015 09:29:04 -0700 (PDT)Return-Path: <sut.example@gmail.com>Subject: testTo: wellformmed1@edge.nist.govX-Received: by 10.182.13
1.130 with SMTP id om2mr15291721obb.70.1430238544535;
Tue, 28 Apr 2015 09:29:04 -0700 (PDT)
```

Attachments:

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



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

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 can 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 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 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	<ul style="list-style-type: none"> - The SUT will attempt to initiate a secure connection with the ETT and execute the correct SMTP sequence. - The ETT will receive the SMTP protocol command sequence, 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) and 4.1.1.1 (Extended HELO or EHLO).
2	<ul style="list-style-type: none"> - The SUT will attempt to send a HELO / EHLO command sequence to the ETT. - The ETT will receive the HELO / EHLO command sequence, 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 4.1.1.1 (Extended HELO or EHLO).
3	<ul style="list-style-type: none"> - The SUT will attempt to send the MAIL FROM, RCPT TO, and DATA command sequences to the ETT. - The ETT will receive the MAIL FROM, RCPT TO, and DATA command sequences, perform validation, and initiate a successful connection with the SUT.

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

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 Test Procedure requirements document.

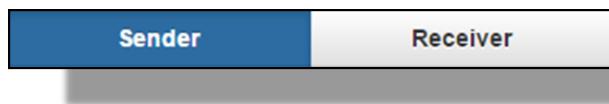
3.4.1 TESTING STEPS

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.

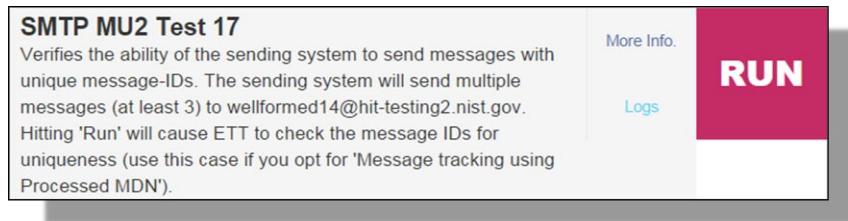


3. From the testing Profile, select ‘Sender’.



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. Navigate to the Test Case’s execution interface.



To gain additional information concerning a target Test Case’s intended purpose (including Description, Vendor/SUT roles), click ‘More Info’ link for the Test Case.

The screenshot shows the Edge Testing Tool's user interface. At the top, there are two overlapping boxes: a blue one labeled 'More Info.' and a white one labeled 'Logs'. Below them is a larger window titled 'SMTP MU2 Test 17'. The window contains the following information:

- Description:** Verifies the ability of the sending system to send messages with unique message-IDs. The sending system will send multiple messages (at least 3) to wellformed14@hit-testing2.nist.gov. Hitting 'Run' will cause ETT to check the message IDs for uniqueness (use this case if you opt for 'Message tracking using Processed MDN').
- A table with three columns: 'Vendor Role', 'Vendor Edge', and 'Vendor HISP'. The 'sender' role is listed, with a green checkmark in both the 'Vendor Edge' and 'Vendor HISP' columns.
- A large blue 'Run' button at the bottom right.

5. With the Profile saved, More Info reviewed, and 'SMTP MU2 Test 17' selected, perform the following Test Steps:
 - A. Navigate 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. Send the messages to the ETT endpoint recipient wellformed14@hit-testing2.nist.gov.
 - C. Navigate to the ETT and SMTP MU2 Test 17.
 - 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.



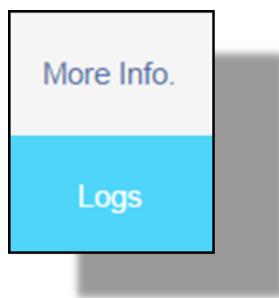
Note: SMTP MU2 Test 17 should be executed under the constraint that a Vendor/SUT opts for message tracking using processed MDNs.

6. The test will process and render one of two results: ‘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 a particular target Test Case, click the ‘Log’ link.



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

The screenshot shows a user interface titled 'Log SMTP MU2 Test 17'. At the top, it displays 'Test result #1: ✓ Pass'. Below this, there is a table with four columns: 'Criteria Met', 'Request Time out', 'Proctored', and 'Time elapsed (seconds)'. All three rows under these columns have a red 'X' mark. The 'Time elapsed (seconds)' column has a value of '0'. Under the heading 'Request responses', there is a box containing three message IDs: Message-ID 1, 2, and 3, each with a unique identifier. At the bottom, there is a section for 'Attachments' with a placeholder '(none)'.



*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 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.

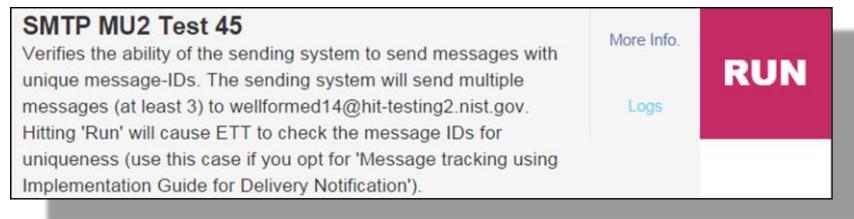


3. From the testing Profile, select ‘**Sender**’.

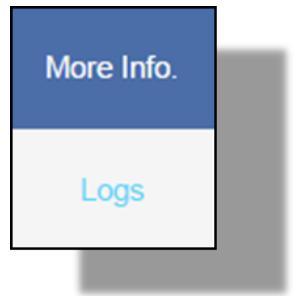


Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 Profile Creation](#).

4. Navigate to the Test Case's execution interface.



To gain additional information concerning a target Test Case'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, perform 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. Send the messages to the ETT endpoint recipient wellformed14@hit-testing2.nist.gov.
- C. Navigate to the ETT and SMTP MU2 Test 45.
 - 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: ‘**Pass**’ or ‘**Fail**’.

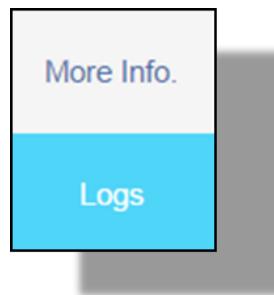
- A test Pass is indicated by a green check and a test Fail is indicated by a red X.
- A test Fail prompts the Vendor to ‘**Retry**’ the test.
- The ‘**Clear**’ button resets the test and any data input field values.





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 a particular target Test Case, click the ‘Log’ link.



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

The screenshot shows a test result for 'Log SMTP MU2 Test 45'. At the top, it displays 'Test result #1: ✓ Pass'. Below this, there is a table with four columns: 'Criteria Met', 'Request Time out', 'Proctored', and 'Time elapsed (seconds)'. All three rows under these columns contain a red 'x' symbol. Under 'Request responses', there is a box containing three message IDs: Message-ID 1, 2, and 3, each starting with <CAJ3w=-KgpPdyXf0oHVi8=y-_jM-xFAdARhhtZxsjZkKua0j6wA@mail.gmail.com>. Under 'Attachments:', there is a placeholder box with '(0)' indicating no 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 Test Procedure requirements document.

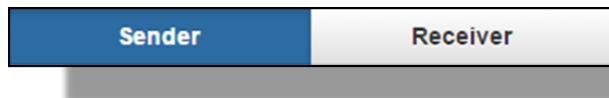
3.6.1 TESTING STEPS

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.

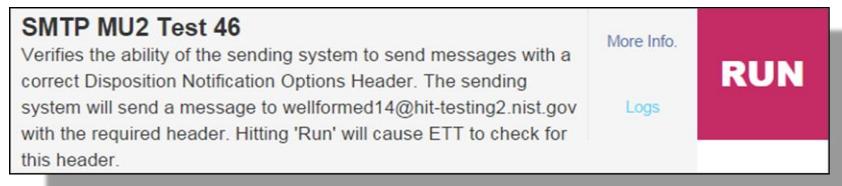


3. From the testing Profile, select ‘**Sender**’.



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. Navigate to the Test Case’s execution interface.



To gain additional information concerning a target Test Case’s intended purpose (including Description, Vendor/SUT roles), click ‘**More Info**’ link for the Test Case.

The screenshot shows the Edge Testing Tool's main interface. At the top, there are two overlapping boxes: a blue one labeled 'More Info.' and a white one labeled 'Logs'. Below them is a larger window titled 'SMTP MU2 Test 46'. The window contains the following information:

- Description:** Verifies the ability of the sending system to send messages with a correct Disposition-Notification Options Header. The sending system will send a message to wellformed14@hit-testing2.nist.gov with the required header. Hitting 'Run' will cause ETT to check for this header.
- A table with three columns: 'Vendor Role', 'Vendor Edge', and 'Vendor HISP'. The 'sender' role is listed under 'Vendor Role'. Under 'Vendor Edge', there is a green checkmark. Under 'Vendor HISP', there is also a green checkmark.
- A large blue 'Run' button at the bottom right of the window.

5. With the Profile saved, More Info reviewed, and 'SMTP MU2 Test 46' selected, perform 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. Send the messages to the ETT endpoint recipient wellformed14@hit-testing2.nist.gov.
 - C. Navigate to the ETT and SMTP MU2 Test 46.
 - 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.

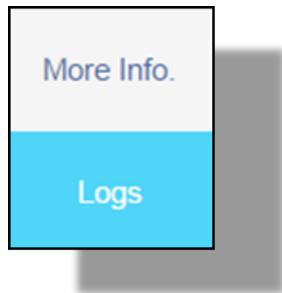


6. The test will process and render one of two results: '**Pass**' or '**Fail**'.
 - A test Pass is indicated by a green check and a test Fail is indicated by a red X.
 - A test Fail prompts the Vendor to '**Retry**' the test.
 - The '**Clear**' button resets the test and any data input field values.



*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 a particular target Test Case, click the '**Log**' link.



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

The screenshot shows a test log interface. At the top, it says "Log SMTP MU2 Test 46". Below that, it displays "Test result #1: ✓ Pass". A table follows with columns: Criteria Met, Request Time out, Proctored, and Time elapsed (seconds). All four columns have a red "x" in them, and the time elapsed is 0. Under "Request responses", there is a box containing three message IDs: Message-ID 1, 2, and 3, each with a long string of characters. Below that is a section for "Attachments:" which is currently empty.



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

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.

[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 Test Procedure requirements document.

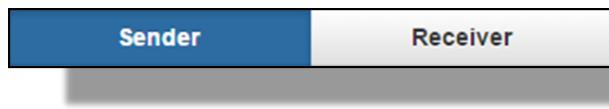
3.7.1 TESTING STEPS

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’.

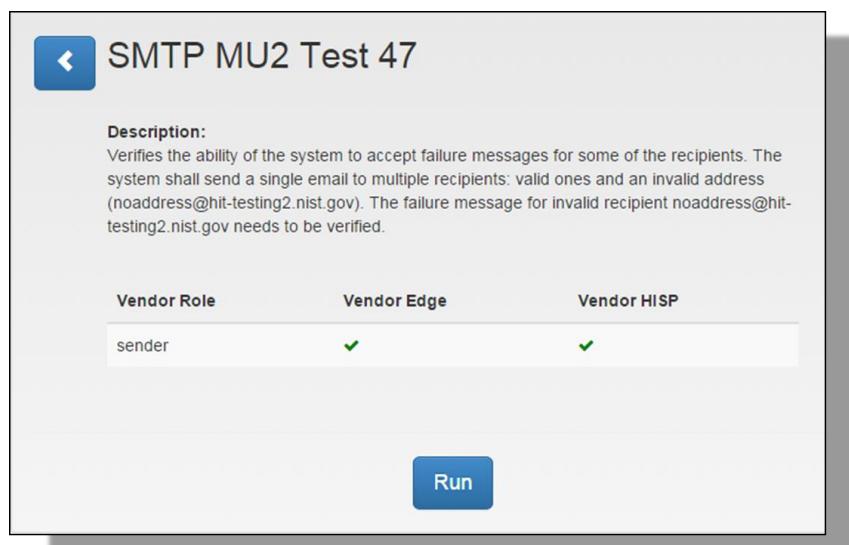
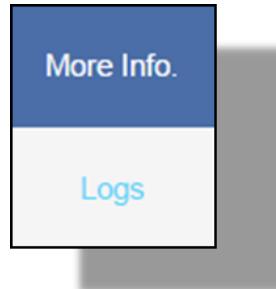


Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 Profile Creation](#).

4. Navigate to the Test Case’s execution interface.



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



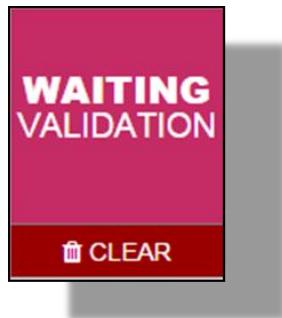
5. With the Profile saved, More Info reviewed, and 'SMTP MU2 Test 47' selected, perform the following Test Steps:
 - A. Navigate the to SUT's messaging client/interface for 'Vendor SMTP Email Address' (specified in the Profile).
 - B. Create a single new message.
 - a. Send the message to both valid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

- 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 test will process and prompt the Vendor for further interaction to complete the test. Click the ‘Waiting Validation’ button.



7. The Vendor must review the ‘Log’ and perform manual validation that the test results conformed to the testing objective(s).

Log SMTP MU2 Test 47

Test result #1:

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

Request responses

Awaiting confirmation from proctor: Proctor needs to verify the failure message from invalid recipient.

Attachments:

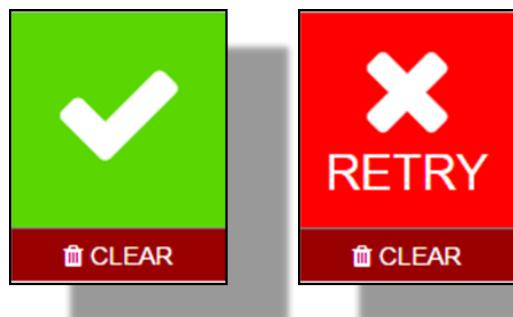
(0)

The Vendor must review the test results and confirm that the SUT successfully received a message transmission failure message from the invalid ETT endpoint recipient noaddress@hit-testing2.nist.gov.

8. ‘Accept’ or ‘Reject’ must be selected to complete the test.



9. Vendor selection will render one of two results: ‘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 Test Procedure requirements document.

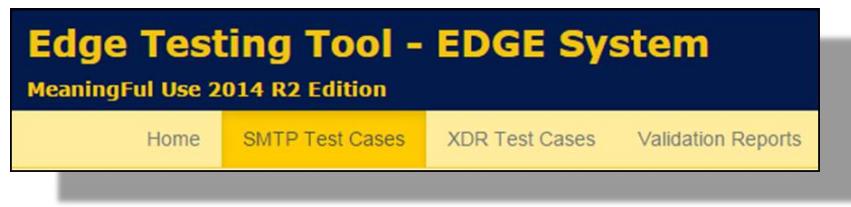
4.1.1 TESTING STEPS

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 MU2 test, select 'SMTP Test Cases' from the Navigation Bar. This enables the testing Profile feature of the tool.

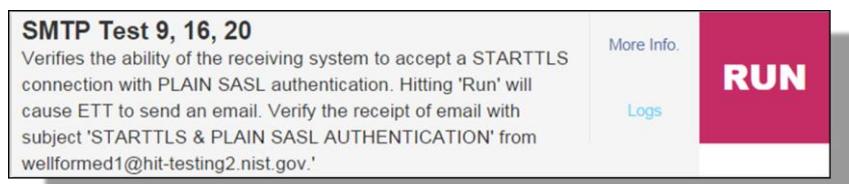


3. From the testing Profile, select 'Receiver'.

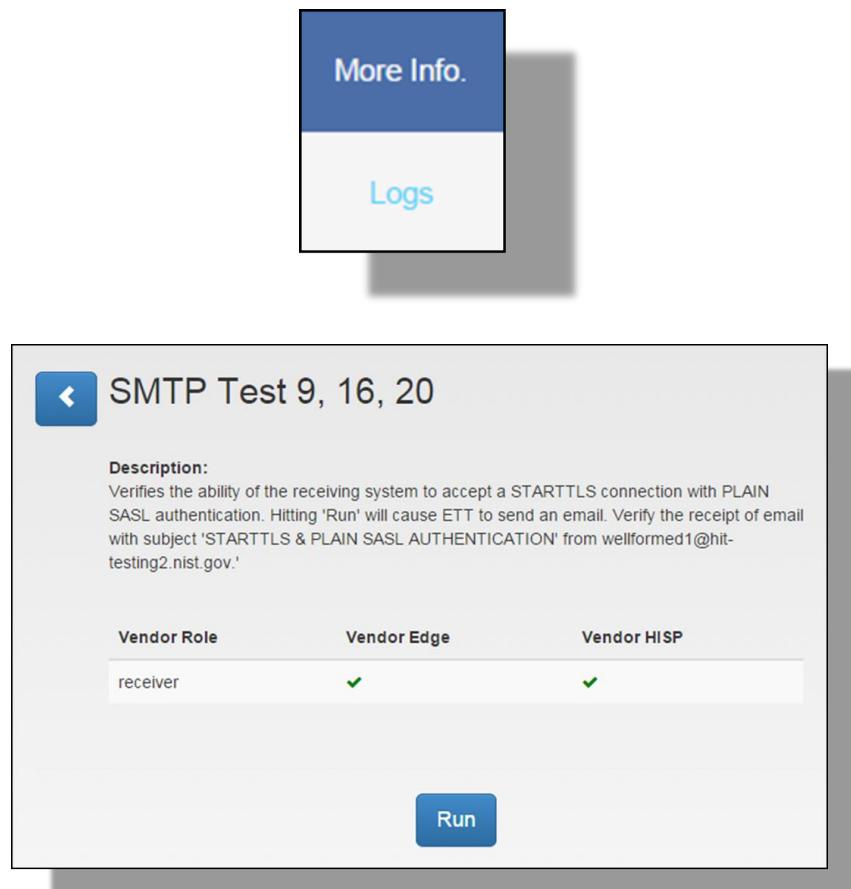


Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 Profile Creation](#).

4. Navigate to the Test Case's execution interface.



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



The screenshot shows a modal window titled 'SMTP Test 9, 16, 20'. At the top left is a back arrow icon. Below the title is a 'Description' section with the following text:
Verifies the ability of the receiving system to accept a STARTTLS connection with PLAIN SASL authentication. Hitting 'Run' will cause ETT to send an email. Verify the receipt of email with subject 'STARTTLS & PLAIN SASL AUTHENTICATION' from wellformed1@hit-testing2.nist.gov.'

Vendor Role	Vendor Edge	Vendor HISP
receiver	✓	✓

At the bottom right of the modal is a blue 'Run' button.

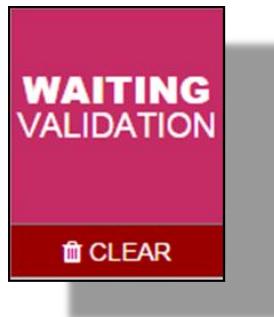
5. With the Profile saved, More Info reviewed, and 'SMTP Test 9, 16, 20' selected, perform the following Test Steps:

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).
- Wait at least 60 seconds from executing the test to allow successful transmission to the SUT.
 - 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 '**CCDA_Ambulatory**' in XML format.
6. The test will process and prompt the Vendor for further interaction to complete the test. Click the '**Waiting Validation**' button.



7. The Vendor must review the '**Log**' and perform manual validation that the test results conformed to the testing objective(s).

A screenshot of a software interface titled 'Log SMTP Test 9, 16, 20'. The title bar has a blue button with a left arrow and the text 'Log SMTP Test 9, 16, 20'. Below the title, the text 'Test result #1:' is displayed. A table follows, showing four columns: 'Criteria Met', 'Request Time out', 'Proctored', and 'Time elapsed (seconds)'. The first two columns have red 'x' marks, while the third has a green checkmark and the fourth shows '0'. Under the table, the section 'Request responses' contains the text: '1: SENDING STARTTLS & PLAIN SASL AUTHENTICATION EMAIL TO sut.example@gmail.com WITH ATTACHMENT CCDA_Ambulatory.xml' and '2: Email sent Successfully'. At the bottom, the section 'Attachments:' shows a placeholder box with the text '{}'.

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

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. '**Accept**' or '**Reject**' must be selected to complete the test.



9. Vendor selection will render one of two results: '**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 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 MU2 test, select 'SMTP Test Cases' from the Navigation Bar. This enables the testing Profile feature of the tool.

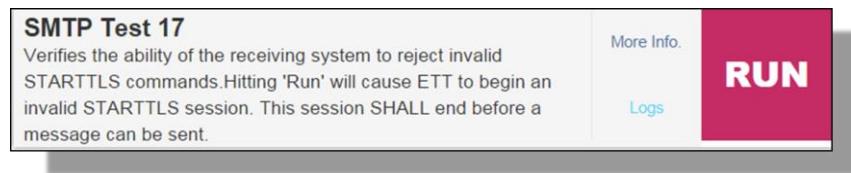


3. From the testing Profile, select 'Receiver'.

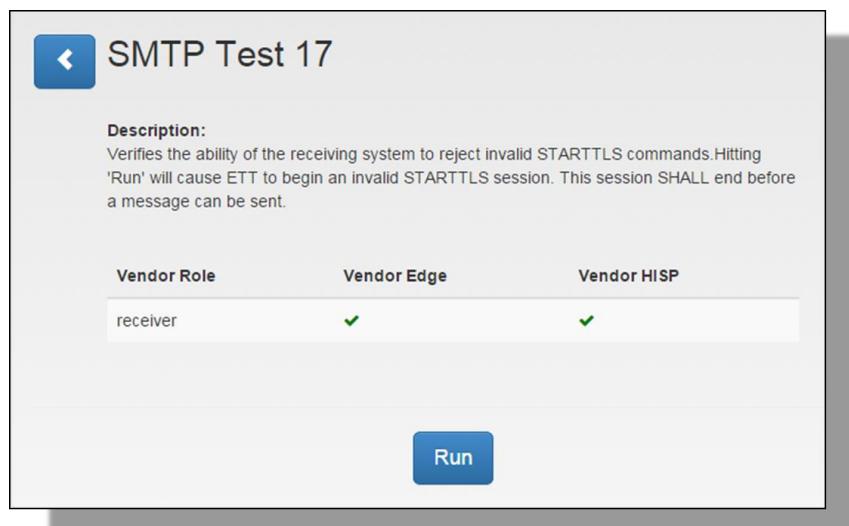
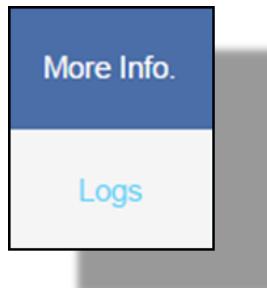


Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 Profile Creation](#).

4. Navigate to the Test Case's execution interface.



To gain additional information concerning a target Test Case'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, 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.



*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.*

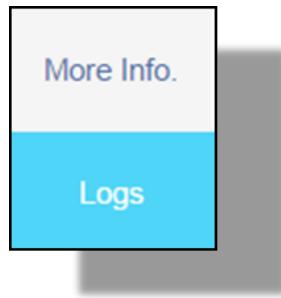
6. The test will process and render one of two results: '**Pass**' or '**Fail**'.

- 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 a particular target Test Case, click the '**Log**' link.



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

Log SMTP Test 17

Test result #1: **Pass**

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

Request responses

```
HELO testing.com
: 250 mx.google.com at your service
STARTTLS abcd
: 555 5.5.2 Syntax error. g184sm13526427qhc.6 - gsmtp
```

Attachments:

(0)



*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 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 Test Procedure requirements document.

4.4.1 TESTING STEPS

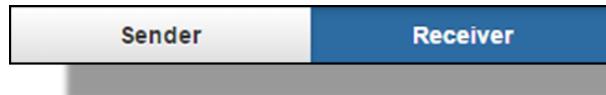
To execute SMTP Test Case 22 and assess the SUT's ability to reject an authentication connection attempt using invalid PLAIN SASL credentials, the Vendor must perform the following steps:

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 MU2 test, select ‘**SMTP Test Cases**’ from the Navigation Bar. This enables the testing Profile feature of the tool.

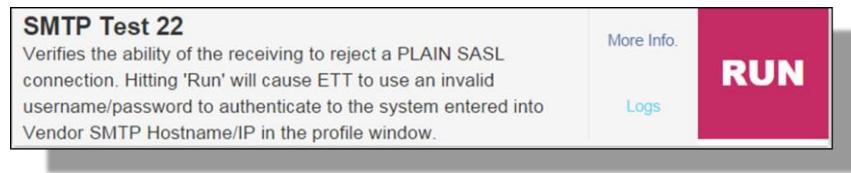


3. From the testing Profile, select ‘**Receiver**’.

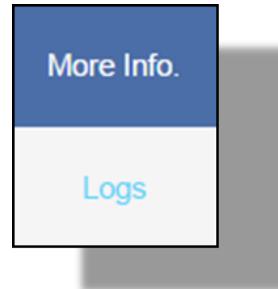


Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 Profile Creation](#).

4. Navigate to the Test Case’s execution interface.



To gain additional information concerning a target Test Case’s intended purpose (including Description, Vendor/SUT roles), click ‘**More Info**’ link for the Test Case.



The screenshot shows a test configuration window titled "SMTP Test 22". At the top left is a back arrow icon. Below the title is a section titled "Description:" which contains detailed text about the test sequence. A table below the description maps vendor roles to edge and HISp components. A large blue "Run" button is at the bottom.

Vendor Role	Vendor Edge	Vendor HISp
receiver	✓	✓

5. With the Profile saved, More Info reviewed, and ‘**SMTP Test 22**‘ 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.



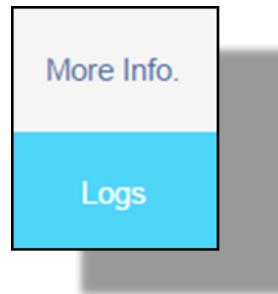
Note: The Vendor, in execution of SMTP Test Case 22, should **not** receive a message in the ‘Vendor SMTP Email Address’ from the ETT. This is a negative test attempting to assess the capability of the SUT to reject a connection attempt that uses invalid PLAIN SASL credentials. Thus, the SUT should reject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

6. The test will process and render one of two results: ‘**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 a particular target Test Case, click the ‘**Log**’ link.



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

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

Request responses

```
SUCCESS: Vendor rejects bad Username/Password combination :535-5.7.8 Username and Password not accepted. Learn more at 535 5.7.8 http://support.google.com/mail/bin/answer.py?answer=14257 j40sm13455 689qkh.46 - gsmtp
```

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 HISIP (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 can 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 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 Test Procedure requirements document.

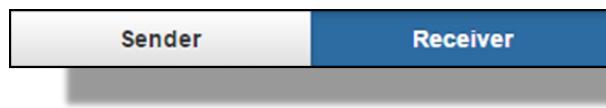
4.6.1 TESTING STEPS

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 MU2 test, select ‘**SMTP Test Cases**’ from the Navigation Bar. This enables the testing Profile feature of the tool.

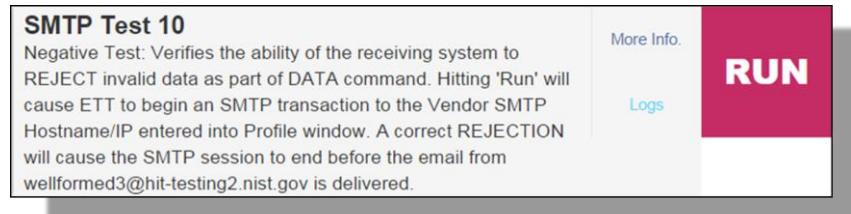


3. From the testing Profile, select ‘**Receiver**’.

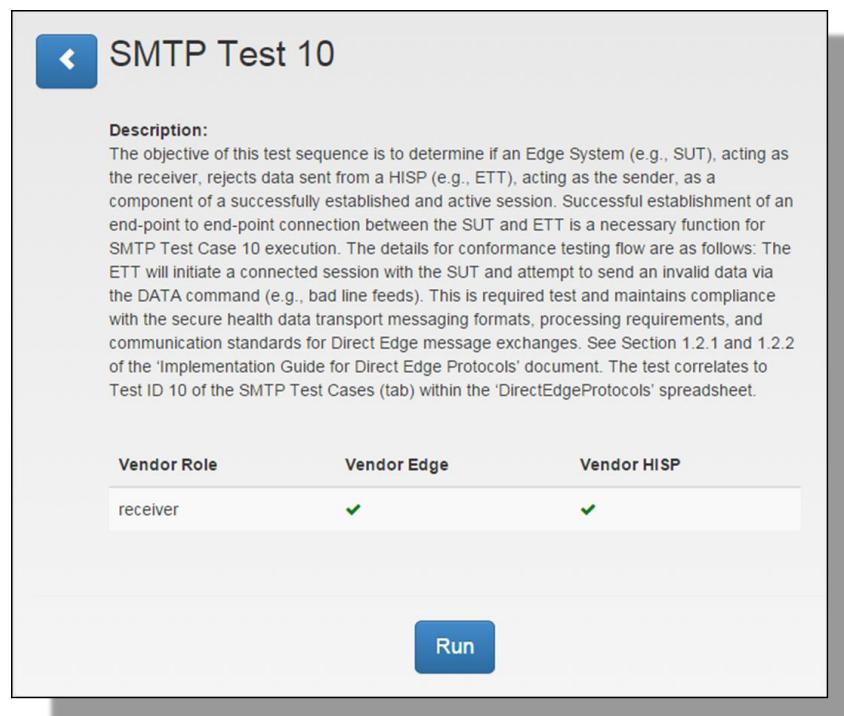


Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 Profile Creation](#).

4. Navigate to the Test Case's execution interface.



To gain additional information concerning a target Test Case'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).

- Wait at least 60 seconds from executing the test to allow successful transmission to the SUT.
- 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.



*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: ‘Pass’ or ‘Fail’.

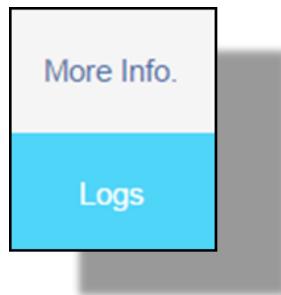
- A test Pass is indicated by a green check and a test Fail is indicated by a red X.
- A test Fail prompts the Vendor to ‘Retry’ the test.
- The ‘Clear’ button resets the test and any data input field values.





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 a particular target Test Case, click the ‘Log’ link.



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

The screenshot shows a test log titled "Log SMTP Test 10". The main header says "Test result #1: ✓ Pass". Below it is a table with four columns: "Criteria Met", "Request Time out", "Proctored", and "Time elapsed (seconds)". All three rows under these columns have an "X" mark. The "Time elapsed (seconds)" row has a value of "30". Below the table is a section titled "Request responses" containing a large block of text representing an SMTP session log. At the bottom is a section titled "Attachments:" with a placeholder "(none)".

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

Request responses

```

DATA This is sample DATA.: -02 Custom Message: Socket Timeout occurred 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
MAIL FROM:<daemon@ttt.nist.gov>
: 250 2.1.0 OK n62sm6128087qge.27 - gsmtp
RCPT TO:<daemon@ttt.nist.gov>
: 250 2.1.5 OK n62sm6128087qge.27 - gsmtp

```

Attachments:

(none)



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 HISIP (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 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.

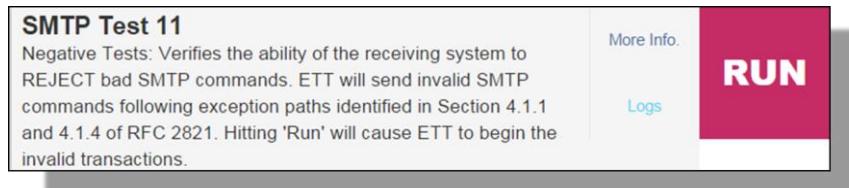


3. From the testing Profile, select ‘**Receiver**’.



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. Navigate to the Test Case's execution interface.



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

The screenshot shows the 'More Info' page for 'SMTP Test 11'. At the top left is a back arrow icon. Next to it is the title 'SMTP Test 11'. Below the title is a section titled 'Description:' containing a detailed explanation of the test's objective and flow. Underneath the description is a table with three columns: 'Vendor Role', 'Vendor Edge', and 'Vendor HISp'. The table has one row with the value 'receiver' in the 'Vendor Role' column, a green checkmark in the 'Vendor Edge' column, and another green checkmark in the 'Vendor HISp' column. At the bottom of the page is a blue 'Run' button.

Vendor Role	Vendor Edge	Vendor HISp
receiver	✓	✓

5. With the Profile saved, More Info reviewed, and ‘**SMTP Test 11**‘ 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).
- Wait at least 60 seconds from executing the test to allow successful transmission to the SUT.
 - Check the ‘**Vendor SMTP Email Address**’ to validate that a new message is not present.



*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: ‘**Pass**’ or ‘**Fail**’.

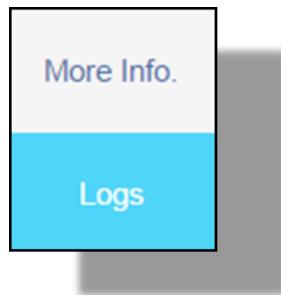
- A test Pass is indicated by a green check and a test Fail is indicated by a red X.
- A test Fail prompts the Vendor to ‘**Retry**’ the test.
- The ‘**Clear**’ button resets the test and any data input field values.





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 a particular target Test Case, click the ‘Log’ link.



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

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 Test Procedure requirements document.

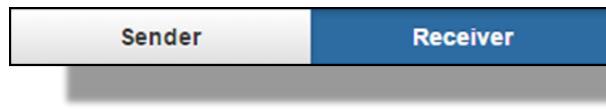
4.8.1 TESTING STEPS

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.

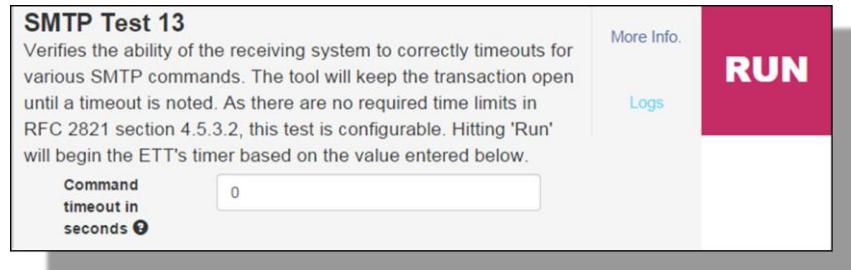


3. From the testing Profile, select 'Receiver'.

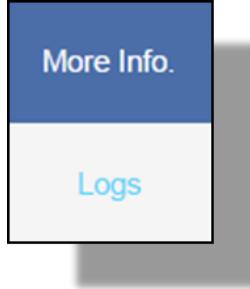


Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 5 within [2.3 Profile Creation](#).

4. Navigate to the Test Case's execution interface.



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



The screenshot shows a modal window titled "SMTP Test 13". At the top right of the modal is a "More Info." button, which is highlighted with a blue background and white text. Below it is a "Logs" button, also in blue and white. The main content area of the modal has a light gray background. It contains a "Description:" section with detailed text about the test sequence. Below the description is a table with three columns: "Vendor Role", "Vendor Edge", and "Vendor HISp". A single row in the table shows "receiver" in the first column, with a green checkmark in the second and third columns. Underneath the table is a field labeled "Command timeout in seconds" with a value of "sutCommandTimeoutInSeconds". At the bottom of the modal is a blue "Run" button.

5. With the Profile saved, More Info reviewed, and ‘**SMTP Test 13**‘ selected, perform the following Test Steps:
 - A. On the Test Case’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:

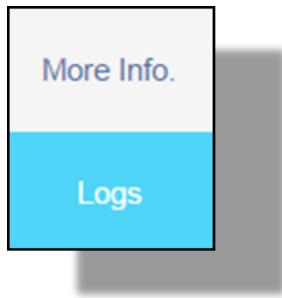
- Initial 220 Message: 5 minutes (300 seconds);
- MAIL Command: 5 minutes (300 seconds);
- RCPT Command: 5 minutes (300 seconds);
- DATA Initiation: 2 minutes (120 seconds);
- DATA Block: 3 minutes (180 seconds);
- DATA Termination: 10 minutes (600 seconds); and
- Waiting for next command from sender: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

6. The test will process and render one of two results: ‘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 a particular target Test Case, click the ‘Log’ link.



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

Log SMTP Test 13

Test result #1: ✓ Pass

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

Request responses

```
: -02 Custom Message: Socket Timeout occurredDATA
: 354 Go ahead f4sm1648122qhe.9 - 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
MAIL FROM:<daemon@ttt.nist.gov>
: 250 2.1.0 OK f4sm1648122qhe.9 - gsmtp
RCPT TO:<daemon@ttt.nist.gov>
: 250 2.1.5 OK f4sm1648122qhe.9 - gsmtp
```

Attachments:

{}

Test result #2: ✓ Pass

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

Request responses

```
: -02 Custom Message: Socket Timeout occurredEHLO ttt.nist.gov
: 250-mx.google.com at your service, [129.6.24.35]
250-SIZE 35882577
250-8BITMIME
250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN XOAUTH
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250-SMTPUTF8
MAIL FROM:<daemon@ttt.nist.gov>
: 250 2.1.0 OK 69sm13458875qkr.41 - gsmtp
RCPT TO:<daemon@ttt.nist.gov>
: 250 2.1.5 OK 69sm13458875qkr.41 - gsmtp
```

Attachments:

{}



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

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 and imported into the SUT's trust store (link located '**XDR Test Cases**' tab of ETT) before test execution.
- With the trust relationship established, the Vendor navigates to the target Test Case and populates the '**Direct From Address**' field with the SUT's accurate information (all fields should correlate so the ETT and SUT can communicate to execute this Test Case; reference [2.3 Profile Creation](#)).
- The Vendor performing this Test Case and in operation of the SUT executes first Test Step by clicking '**Run**' for the target Test Case. The ETT generates two endpoints (TLS and Non-TLS).
- The Vendor executes the second Test Step by sending the ETT generated TLS / Non-TLS endpoint a message from the SUT.
- The Vendor validates through '**Log**' review that the SUT successfully established a Mutual TLS connection with the ETT generated endpoint, the SUT authenticated with the ETT generated endpoint before transmitting data, the message met testing constraints, and testing adhered to the specified requirements within [XDR and XDM for Direct Messaging v1.0](#) and [IHE XDR Profile for Limited Metadata Document Sources](#).

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

This test correlates to Test ID 7 of the XDR Test Cases tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 2.01 within the 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 ‘**Sender**’. This will enable Test Case selection.

Your System as: Sender



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

4. To gain additional information concerning a target Test Case’s intended focus, purpose/descriptions, conditional requirements, and expected test results, Vendor role, and Metadata inclusion, click the ‘**Description**’ link for the Test Case.



5. To initiate the target Test Case (XDR Test 6), click ‘Run’. This generates a ‘TLS Endpoint’.

The screenshot shows the Edge Testing Tool interface for Test ID #6. The main panel displays the test description: "Verify that Mutual TLS session is established between the Sender and the Receiver before transmitting data." Below this, Step 1: "Hit Run to generate your endpoint" is listed. To the right, there are "Description" and "Logs" tabs. A large red box highlights the "RUN" button, which is located in a pink box. Below the main panel, Step 2: "Send XDR message to endpoint and refresh to check status" is shown, along with a red box highlighting the "Endpoint" field containing the URL "https://hit-dev.nist.gov:11080/xdstools3/sim/ETT_testing_2014@gmail.com_6_1420666723457/docrec/prb".

- !**
- Note: Instructions are labeled in sequential order (e.g., ‘Step 1’, ‘Step 2’, ‘Step 3’) in the content description of the Test Case. The ‘TLS Endpoint’ is uniquely generated and specific to the target Test Case and Tester (e.g., Vendor) ETT testing session.*
6. Once the ‘TLS Endpoint’ has been successfully created, the Vendor must then configure the SUT (their operated and managed Edge system) to execute XDR Sending Test Case 6. SUT configuration entails creating an XDR message and defining the ‘TLS Endpoint’ as the message recipient, thus establishing a mutual TLS session between the SUT and ETT. Session connection must occur before any data is transmitted.
 7. With SUT configuration complete and XDR message successfully sent to the ETT ‘TLS Endpoint’, the Vendor clicks the ‘Pending Refresh’ button for the Test Case. This enables the ETT to check the ‘TLS Endpoint’ for receipt of the XDR message.

The screenshot shows the Edge Testing Tool interface for Test ID #6. The main panel displays the test description: "Verify that Mutual TLS session is established between the Sender and the Receiver before transmitting data." Below this, Step 2: "Send XDR message to endpoint and refresh to check status" is listed, with a red box highlighting the "Endpoint" field containing the URL "https://hit-dev.nist.gov:11080/xdstools3/sim/ETT_testing_2014@gmail.com_6_1421180186561/docrec/prb". To the right, there are "Description" and "Logs" tabs. A large red box highlights the "PENDING REFRESH" button, which is located in a pink box.

- !**
- Note: For XDR Sending Test Cases, the ETT generates a unique ‘TLS Endpoint’ and listens on the specific/configured port to detect the presence of a transmitted XDR message from the SUT.*

8. Upon refresh completion, the Vendor is prompted to manually validate if the test results conformed to the testing objective. This is performed through clicking the ‘Waiting Validation’ button.



9. This will bring up the ‘Log’ screen for the Test Case. The Vendor is presented with ‘Request’ and ‘Response’ tabs. Based upon the specific testing objective for a Test Case, one of the two tabs will contain XDR message information relevant to the test. The Vendor reviews the ‘Log’ data and validates that the message content and metadata conforms to the testing objectives.



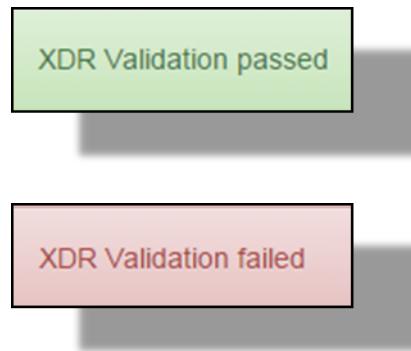
10. If the Vendor accepts the data and confirms that the XDR message content within the ‘Log’ conforms to the testing objectives for the Test Case, the ‘Accept XDR’ button is selected. However, if the XDR message content does not conform to the testing objectives for the Test Case, the ‘Reject XDR’ button 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 Vendor is given selection conformation by the ETT.



12. Acceptance or rejection of the XDR message content results in overall Test Case testing Success or Failure. This testing data is then available through the ‘Validation Report’ (reference [Section 2.4 Reporting](#)).

Test ID #6
Verify that Mutual TLS session is established between the Sender and the Receiver before transmitting data.
Step 2: Check the logs to accept/reject the response

Description: Logs

Test ID #6
Verify that Mutual TLS session is established between the Sender and the Receiver before transmitting data.
Step 2: Check the logs to accept/reject the response

Description: Logs



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

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 and imported into the SUT's trust store (link located 'XDR Test Cases' tab of ETT) before test execution.
- 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 can communicate to execute this Test Case; reference [2.3 Profile Creation](#)).
- The Vendor performing this Test Case and in operation of the SUT executes first Test Step by clicking 'Run' for the target Test Case. The ETT generates an endpoint (IP address and port).
- The Vendor executes the second Test Step by sending the ETT generated endpoint a message from the SUT.
- The Vendor validates through 'Log' review that the SUT attempted to establish a Mutual TLS connection with the ETT generated endpoint, the SUT identified during authentication invalid certificates provided by the ETT, the SUT successfully disconnected from the ETT without authenticating and/or transmitting any data, and testing adhered to the specified requirements within [XDR and XDM for Direct Messaging v1.0](#) and [IHE XDR Profile for Limited Metadata Document Sources](#).

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

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 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:

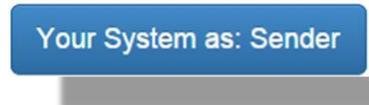
1. Reference Section [2.0 Testing Configuration for Edge System](#) of this ETT User Guide and follow Steps 1 through 7 within [2.2 Registration](#).

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

Edge Testing Tool (Beta) - EDGE System
Meaningful Use 2014 R2 Edition

[Home](#) [SMTP Test Cases](#) [XDR Test Cases](#) [Validation Reports](#)

3. From the testing options available, select '**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 a target Test Case's intended focus, purpose/descriptions, conditional requirements, and expected test results, Vendor role, and Metadata inclusion, click the '**Description**' link for the Test Case.

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

- To initiate the target Test Case (XDR Test 7), insert the SUT host name of the device that the Test Case will be executed from. Once the '**Hostname**' has been inserted, click '**Run**'. This generates a '**TLS Endpoint**'.

Test ID #7	Verify that Edge disconnects when the Server provided certificate is invalid.	Description
	<p>Step 1: Provide your hostname and hit Run to generate your endpoint</p> <p>Hostname: <input data-bbox="502 1615 771 1622" type="text" value="Hostname"/></p>	<p>Description</p> <p>Logs</p> <p>RUN</p>



Note: Instructions are labeled in sequential order (e.g., ‘Step 1’, ‘Step 2’, ‘Step 3’) in the content description of the Test Case. The ‘TLS Endpoint’ is uniquely generated and specific to the target Test Case and Tester (e.g., Vendor) ETT testing session.

6. Once the ‘TLS Endpoint’ has been successfully created, the Vendor must then configure the SUT (their operated and managed Edge system) to execute XDR Sending Test Case 7. SUT configuration entails creating an XDR message and defining the ‘TLS Endpoint’ as the message recipient, thus sending the message to the ETT.
7. With SUT configuration is complete and the XDR message has been successfully sent to the ETT ‘TLS Endpoint’, the Vendor clicks the ‘Pending Refresh’ button on for the Test Case. This enables the ETT to check the ‘TLS Endpoint’ for receipt of the XDR message.



Note: For XDR Sending Test Cases, the ETT generates a unique ‘TLS Endpoint’ and listens on the specific/configured port to detect the presence of a transmitted XDR message from the SUT.

8. Upon refresh completion, the Vendor is prompted to manually validate if the test results conformed to the testing objective. This is performed through clicking the ‘Waiting Validation’ button.



9. This will bring up the ‘Log’ screen for the Test Case. The Vendor is presented ‘Request’ and ‘Response’ tabs. Based upon the specific testing objective for a Test Case, one of the two tabs will contain XDR message information. The Vendor reviews the ‘Log’ data and validates that the message content and metadata conforms to the testing objectives.

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=MIMEBoundary112233445566778899; type="application/xop+xml"; start=<doc0@ihexds.nist.gov>; start-info="application/soap+xml"; charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Tue, 13 Jan 2015 16:41:20 GMT

35f
--MIMEBoundary112233445566778899
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <doc0@ihexds.nist.gov>

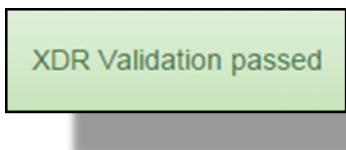
<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope">
<S:Header>
<wsa:Action s:mustUnderstand="1" xmlns:s="http://www.w3.org/2003/05/soap-envelope">
  xmlns:wsa="http://www.w3.org/2005/08/addressing">urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-bResponse</wsa:Action>
<wsa:RelatesTo xmlns:wsa="http://www.w3.org/2005/08/addressing">15dcdb7-4287-45f7-99c7-67fb778f4572</wsa:RelatesTo>
</S:Header>
<S:Body>
<r3:RegistryResponse status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
  xmlns:r3s="urn:oasis:names:tc:ebxml-regrep:xdr:rs:3.0"/>
</S:Body>
</S:Envelope>
--MIMEBoundary112233445566778899--
```

10. If the Vendor accepts the data and confirms that the XDR message content within the ‘Log’ conforms to the testing objectives for the Test Case, the ‘**Accept XDR**’ button can be selected. However, if the XDR message content does not conform to the testing objectives for the Test Case, the ‘**Reject XDR**’ button is selected. The Vendor is given conformation on selection by the ETT.



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 Vendor is given conformation on selection by the ETT.





12. Acceptance or rejection of the XDR message content results in overall Test Case testing Success or Failure. This testing data is then available through the ‘Validation Report’ (reference [Section 2.4 Reporting](#)).

Test ID #7 Verify that Edge disconnects when the Server provided certificate is invalid. Step 2: Check the logs to accept/reject the response	Description
--	---------------------

Test ID #7 Verify that Edge disconnects when the Server provided certificate is invalid. Step 2: Check the logs to accept/reject the response	Description
--	---------------------



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.

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 and imported into the SUT’s trust store (link located ‘**XDR Test Cases**’ tab of ETT) before test execution.
- 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 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 ‘**Sender**’. This will enable test case selection.

Your System as: Sender



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

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

The screenshot shows the configuration for 'Test #1'. It includes fields for 'Purpose/Description' (Verify that the Edge system can create an XDR message per the specification), 'Expected Test Results' (Edge System produces the right message and conforms to the specification), 'Vendor Role' (Sender (Edge - SUT)), and 'Metadata Included' (Limited Metadata).

5. To initiate the target Test Case (XDR Test 1), click '**Run**'. This generates a "**TLS Endpoint**".

The screenshot shows the 'Test ID #1' page. It displays the purpose ('Verify that the Edge system can create an XDR message per the specification') and the first step ('Step 1: Hit Run to generate your endpoint'). A large red box highlights the 'RUN' button.

The screenshot shows the 'Test ID #1' page again. It displays the purpose and the second step ('Step 2: Send XDR message to endpoint and refresh to check status'). A red box highlights the 'Endpoint' field, which contains the URL 'dev.nist.gov:11080/xdstools3/sim/ETT_testing_2014@gmail_com_1_1421180180776/docrec/prb'.



Note: Instructions are labeled in sequential order (e.g., '**Step 1**', '**Step 2**', '**Step 3**') in the content description of the Test Case. The '**TLS Endpoint**' is uniquely generated and specific to the target Test Case and Tester (e.g., Vendor) ETT testing session.

6. Once the '**TLS Endpoint**' has been successfully created, the Tester (e.g., Vendor) must then configure the SUT (their operated and managed Edge system) to execute XDR Sending Test Case 1. SUT configuration entails creating an XDR message and defining the '**TLS Endpoint**' as the message recipient, thus creating a path to establish a connection between the SUT and ETT.

7. With SUT configuration is complete and the XDR message has been successfully sent to the ETT ‘**TLS Endpoint**’, the Tester (e.g., Vendor) clicks the ‘**Pending Refresh**’ button on for the Test Case. This enables the ETT to check the ‘**TLS Endpoint**’ for receipt of the XDR message.



*Note: For XDR Sending Test Cases, the ETT generates a unique ‘**TLS Endpoint**’ and listens on the specific/configured port to detect the presence of a transmitted XDR message from the SUT.*

8. Upon refresh completion, the Tester (e.g., Vendor) is prompted to manually validate if the test results conformed to the testing objective. This is performed through clicking the ‘**Waiting Validation**’ button.



9. This will bring up the ‘**Log**’ screen for the Test Case. The Tester (e.g., Vendor) is presented ‘**Request**’ and ‘**Response**’ tabs. Based upon the specific testing objective for a Test Case, one of the two tabs will contain XDR message information. The Tester (e.g., Vendor) reviews the ‘**Log**’ data and validates that the message content and metadata conforms to the testing objectives.

```

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=MIMEBoundary112233445566778899; type="application/xop+xml"; start=<doc0@ihexds.nist.gov>; start-info="app
location/soap+xml"; charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Tue, 13 Jan 2015 16:41:20 GMT

35f
--MIMEBoundary112233445566778899
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <doc0@ihexds.nist.gov>

<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope">
<S:Header>
<wsa:Action s:mustUnderstand="1" xmlns:wsa="http://www.w3.org/2005/08/addressing">urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-bResponse</wsa:Action>
<wsa:RelatesTo xmlns:wsa="http://www.w3.org/2005/08/addressing">15dcdb7-4287-45f7-99c7-67fb778f4572</wsa:RelatesTo>
</S:Header>
<S:Body>
<rs:RegistryResponse status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
<rs:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"/>
</S:Body>
</S:Envelope>
--MIMEBoundary112233445566778899...

```

- If the Tester (e.g., Vendor) accepts the data and confirms that the XDR message content within the ‘Log’ conforms to the testing objectives for the Test Case, the ‘Accept XDR’ button can be selected. However, if the XDR message content does not conform to the testing objectives for the Test Case, the ‘Reject XDR’ button is selected. The Tester (e.g., Vendor) is given conformation on selection by the ETT.



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

- The Tester (e.g., Vendor) is given conformation on selection by the ETT.





12. Acceptance or rejection of the XDR message content results in overall Test Case testing Success or Failure. This testing data is then available through the ‘Validation Report’ (reference [Section 2.4 Reporting](#)).

Test ID #1
Verify that the Edge system can create an XDR message per the specification
Step 2: Check the logs to accept/reject the response
Description Logs

Test ID #1
Verify that the Edge system can create an XDR message per the specification
Step 2: Check the logs to accept/reject the response
Description Logs RETRY



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.

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 and imported into the SUT’s trust store (link located ‘**XDR Test Cases**’ tab of ETT) before test execution.
- 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 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 ‘**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 a target Test Case's intended focus, purpose/descriptions, conditional requirements, and expected test results, Tester (e.g., Vendor) role, and Metadata inclusion, click the '**Description**' link for the Test Case.

The screenshot shows the configuration for Test #2. The 'Purpose/Description' section contains the text: 'Verify that the Edge system can create an XDR message per the specification'. The 'Expected Test Results' section contains the text: 'Edge System produces the right message and conforms to the specification'. The 'Vendor Role' section shows 'Sender (Edge - SUT)'. The 'Metadata Included' section shows 'Full Metadata'.

5. To initiate the target Test Case (XDR Test 2), click '**Run**'. This generates a "**TLS Endpoint**".

The screenshot shows the Test ID #2 page. It displays the purpose: 'Verify that the Edge system can create an XDR message per the specification'. Below it, 'Step 1: Hit Run to generate your endpoint' is listed. On the right, there are 'Description' and 'Logs' tabs, and a large red-bordered 'RUN' button.

The screenshot shows the Test ID #2 page again. It displays the purpose: 'Verify that the Edge system can create an XDR message per the specification'. Below it, 'Step 2: Send XDR message to endpoint and refresh to check status' is listed. A red box highlights the 'Endpoint: http://hit-dev.nist.gov:11080/xdstools3/sim/ETT_testing_2014@gmail_com_2_1421180183192/docrec/prb' field. On the right, there are 'Description' and 'Logs' tabs, and a red-bordered status box labeled 'PENDING REFRESH'.



Note: Instructions are labeled in sequential order (e.g., '**Step 1**', '**Step 2**', '**Step 3**') in the content description of the Test Case. The '**TLS Endpoint**' is uniquely generated and specific to the target Test Case and Tester (e.g., Vendor) ETT testing session.

6. Once the '**TLS Endpoint**' has been successfully created, the Tester (e.g., Vendor) must then configure the SUT (their operated and managed Edge system) to execute XDR Sending Test Case 1. SUT configuration entails creating an XDR message and defining the '**TLS Endpoint**' as the message recipient, thus creating a path to establish a connection between the SUT and ETT.

7. With SUT configuration is complete and the XDR message has been successfully sent to the ETT ‘**TLS Endpoint**’, the Tester (e.g., Vendor) clicks the ‘**Pending Refresh**’ button on for the Test Case. This enables the ETT to check the ‘**TLS Endpoint**’ for receipt of the XDR message.



*Note: For XDR Sending Test Cases, the ETT generates a unique ‘**TLS Endpoint**’ and listens on the specific/configured port to detect the presence of a transmitted XDR message from the SUT.*

8. Upon refresh completion, the Tester (e.g., Vendor) is prompted to manually validate if the test results conformed to the testing objective. This is performed through clicking the ‘**Waiting Validation**’ button.



9. This will bring up the ‘**Log**’ screen for the Test Case. The Tester (e.g., Vendor) is presented ‘**Request**’ and ‘**Response**’ tabs. Based upon the specific testing objective for a Test Case, one of the two tabs will contain XDR message information. The Tester (e.g., Vendor) reviews the ‘**Log**’ data and validates that the message content and metadata conforms to the testing objectives.

```

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=MIMEBoundary112233445566778899; type="application/xop+xml"; start=<doc0@ihexds.nist.gov>; start-info="app
location/soap+xml"; charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Tue, 13 Jan 2015 16:41:20 GMT

35f
--MIMEBoundary112233445566778899
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <doc0@ihexds.nist.gov>

<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope">
<S:Header>
<wsa:Action s:mustUnderstand="1" xmlns:wsa="http://www.w3.org/2005/08/addressing">urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-bResponse</wsa:Action>
<wsa:RelatesTo xmlns:wsa="http://www.w3.org/2005/08/addressing">15dcdb7-4287-45f7-99c7-67fb778f4572</wsa:RelatesTo>
</S:Header>
<S:Body>
<rs:RegistryResponse status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
<rs:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"/>
</S:Body>
</S:Envelope>
--MIMEBoundary112233445566778899...

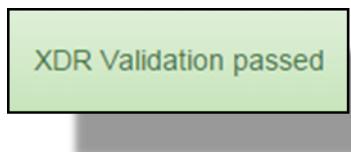
```

- If the Tester (e.g., Vendor) accepts the data and confirms that the XDR message content within the ‘Log’ conforms to the testing objectives for the Test Case, the ‘Accept XDR’ button can be selected. However, if the XDR message content does not conform to the testing objectives for the Test Case, the ‘Reject XDR’ button is selected. The Tester (e.g., Vendor) is given conformation on selection by the ETT.



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

- The Tester (e.g., Vendor) is given conformation on selection by the ETT.





12. Acceptance or rejection of the XDR message content results in overall Test Case testing Success or Failure. This testing data is then available through the ‘Validation Report’ (reference [Section 2.4 Reporting](#)).

Test ID #2 Verify that the Edge system can create an XDR message per the specification Step 2: Check the logs to accept/reject the response	Description	
--	-------------	--

Test ID #2 Verify that the Edge system can create an XDR message per the specification Step 2: Check the logs to accept/reject the response	Description	
--	-------------	--



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.

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 and imported into the SUT's trust store (link located '**XDR Test Cases**' tab of ETT) before test execution.
- With the trust relationship established, the Vendor navigates to the target Test Case and populates the '**IP Address**' and '**Port**' fields with the SUT's accurate information (all fields should correlate so the ETT and SUT can communicate to execute this Test Case; reference [2.3 Profile Creation](#)).
- The Vendor performing this Test Case and in operation of the SUT executes the first Test Step by clicking '**Run**' for the target Test Case.
- The Vendor validates through '**Log**' review that the SUT successfully received the ETT's request to establish a Mutual TLS connection, the SUT authenticated with the ETT before transmitting data, and testing adhered to the specified requirements within [XDR and XDM for Direct Messaging v1.0](#) and [IHE XDR Profile for Limited Metadata Document Sources](#).

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

This test correlates to Test ID 8 of the XDR Test Cases tab within the [DirectEdgeProtocols](#) spreadsheet and TE170.314(b)(8) – 4.01 within the 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.

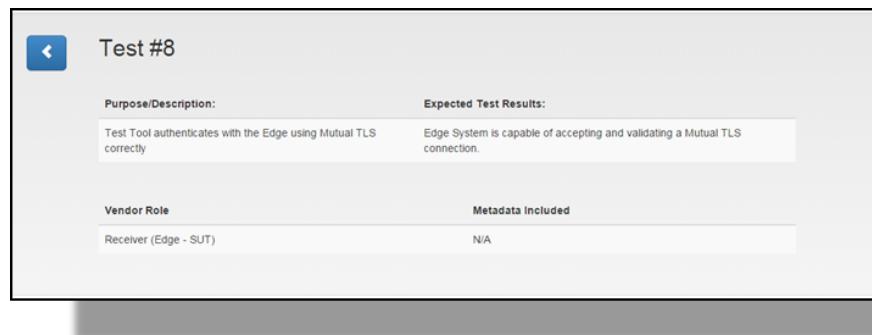


3. From the testing options available, select ‘**Receiver**’. This will enable test case selection.



! 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 Test Case’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 the target Test Case, the Tester (e.g., Vendor) must provide the SUT (their operated and managed Edge system) as a ‘**TLS Endpoint**’ for the ETT to communicate

with and send an XDR message to. The provided ‘**TLS Endpoint**’ of the SUT is the message recipient for this Test Case.



- Once the ‘TLS Endpoint’ has been inserted, ‘Run’ to transmit the XDR message.



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

- Once the XDR message has been sent, ETT will listen for the SUT’s response/conformation of the sent message. Upon receipt of the message, the Tester (e.g., Vendor) is prompted to manually validate if the test results conformed to the testing objective. This is performed through clicking the ‘Waiting Validation’ button.



- This will bring up the ‘Log’ screen for the Test Case. The Tester (e.g., Vendor) is presented ‘Request’ and ‘Response’ tabs. Based upon the specific testing objective for a Test Case, one of the two tabs will contain XDR message information. The Tester (e.g., Vendor) reviews the ‘Log’ data and validates that the message content and metadata conforms to the testing objectives.

```

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=--MIMEBoundary112233445566778899; type="application/xop+xml"; start=<doc0@ihexds.nist.gov>; start-info="application/soap+xml"; charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Tue, 13 Jan 2015 16:47:08 GMT

430
--MIMEBoundary112233445566778899
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <doc0@ihexds.nist.gov>

<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope">
  <S:Header>
    <wsa:Action s:mustUnderstand="1" xmlns:s="http://www.w3.org/2003/05/soap-envelope">
      xmlns:wsa="http://www.w3.org/2005/08/addressing">http://www.w3.org/2005/08/addressing/fault</wsa:Action>
    <wsa:RelatesTo xmlns:wsa="http://www.w3.org/2005/08/addressing">5dc0c56e-e96b-4a50-bdb4-a3ecfaf0bae</wsa:RelatesTo>
  </S:Header>
  <S:Body>
    <fault:Fault xmlns:fault="http://www.w3.org/2003/05/soap-envelope">
      <fault:Code>
        <fault:Value>fault:Sender</fault:Value>
      </fault:Code>
      <fault:Reason>
        <fault:Text xml:lang="en">Sender: Correct Header Namespace - Expected: ; Found: http://www.w3.org/2003/05/soap-envelope</fault:Text>
      </fault:Reason>
    </fault:Fault>
  </S:Body>
</S:Envelope>
--MIMEBoundary112233445566778899-

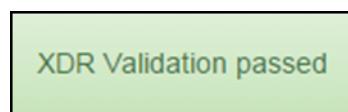
```

- If the Tester (e.g., Vendor) accepts the data and confirms that the XDR message content within the ‘Log’ conforms to the testing objectives for the Test Case, the ‘Accept XDR’ button can be selected. However, if the XDR message content does not conform to the testing objectives for the Test Case, the ‘Reject XDR’ button is selected. The Tester (e.g., Vendor) is given conformation on selection by the ETT.



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

- The Tester (e.g., Vendor) is given conformation on selection by the ETT.





11. Acceptance or rejection of the XDR message content results in overall Test Case testing Success or Failure. Rejection resets the Test Case back to ‘Step 1’. This testing data is then available through the ‘Validation Report’ (reference [Section 2.4 Reporting](#)).

The figure consists of two side-by-side screenshots of a software interface. The left screenshot shows a successful test case. It has a green checkmark icon in the top right corner. The right screenshot shows a failed test case. It has a red X icon in the top right corner and a 'RETRY' button below it. Both screenshots have a header 'Test ID #8' and a 'Logs' section.



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.

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 and imported into the SUT’s trust store (link located ‘**XDR Test Cases**’ tab of ETT) before test execution.
- With the trust relationship established, the Vendor navigates to the target Test Case and populates the ‘**IP Address**’ and ‘**Port**’ fields with the SUT’s accurate information (all fields should correlate so the ETT and SUT can communicate to execute this Test Case; reference [2.3 Profile Creation](#)).

- The Vendor performing this Test Case and in operation of the SUT executes the first Test Step by clicking ‘Run’ for the target Test Case.
- The Vendor validates through ‘Log’ review that the SUT attempted to establish a Mutual TLS connection with the ETT, the SUT identified during authentication invalid certificates provided by the ETT, the SUT successfully disconnected from the ETT without authenticating and/or transmitting any data, and testing adhered to the specified requirements within [*XDR and XDM for Direct Messaging v1.0*](#) and [*IHE XDR Profile for Limited Metadata Document Sources*](#).

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

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

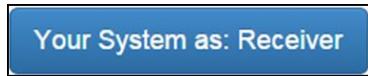
6.2.1 TESTING STEPS

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

The screenshot shows a test case summary for 'Test #9'. It includes sections for 'Purpose/Description' (Test Tool authenticates with the Edge using bad certificates), 'Expected Test Results' (Edge System rejects the connection due to the bad certificate published by the Test Tool.), 'Vendor Role' (Receiver (Edge - SUT)), and 'Metadata Included' (N/A). A back arrow is visible at the top left.

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

The screenshot shows the 'Test ID #9' screen again. The 'Endpoint' field contains 'Endpoint' and is highlighted with a red box. To the right, there are 'Description' and 'Logs' links, and a large red 'RUN' button is prominently displayed.

6. Once the '**TLS Endpoint**' has been inserted, '**Run**' to transmit the XDR message.

The screenshot shows the same 'Test ID #9' screen. The 'Endpoint' field now contains a valid URL ('Endpoint') and is no longer highlighted. The red 'RUN' button remains prominently displayed.



*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, ETT will listen for the SUT's response/conformation of the sent message. Upon receipt of the message, the Tester (e.g., Vendor) is prompted to manually validate if the test results conformed to the testing objective. This is performed through clicking the '**Waiting Validation**' button.



8. This will bring up the ‘Log’ screen for the Test Case. The Tester (e.g., Vendor) is presented ‘Request’ and ‘Response’ tabs. Based upon the specific testing objective for a Test Case, one of the two tabs will contain XDR message information. The Tester (e.g., Vendor) reviews the ‘Log’ data and validates that the message content and metadata conforms to the testing objectives.

The screenshot displays a log entry for 'Test ID #9'. At the top, there are 'Request' and 'Response' tabs, with 'Response' being the active tab. The response content is a SOAP message. It starts with an HTTP header:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=--MIMEBoundary112233445566778899; type="application/xop+xml"; start=<doc0@ihexds.nist.gov>; start-info="app
lication/soap+xml"; charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Tue, 13 Jan 2015 16:47:08 GMT
```

Following the header is an XML fault message:

```
430
--MIMEBoundary112233445566778899
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <doc0@ihexds.nist.gov>

<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope">
  <S:Header>
    <wsa:Action s:mustUnderstand="1" xmlns:wsa="http://www.w3.org/2003/05/soap-envelope"
      xmlns:wsa1="http://www.w3.org/2005/08/addressing">http://www.w3.org/2005/08/addressing/fault</wsa:Action>
    <wsa:RelatesTo xmlns:wsa="http://www.w3.org/2005/08/addressing">5dc0c56e-e96b-4a50-bdb4-ae3ecfaf0bae</wsa:RelatesTo>
  </S:Header>
  <S:Body>
    <fault:Fault xmlns:fault="http://www.w3.org/2003/05/soap-envelope">
      <fault:Code>
        <fault:Value>fault:Sender</fault:Value>
      </fault:Code>
      <fault:Reason>
        <fault:Text xml:lang="en">Sender: Correct Header Namespace - Expected: ; Found: http://www.w3.org/2003/05/soap-envelope</fault:Text>
      </fault:Reason>
    </fault:Fault>
  </S:Body>
</S:Envelope>
```

The log concludes with the closing boundary marker: '--MIMEBoundary112233445566778899--'.

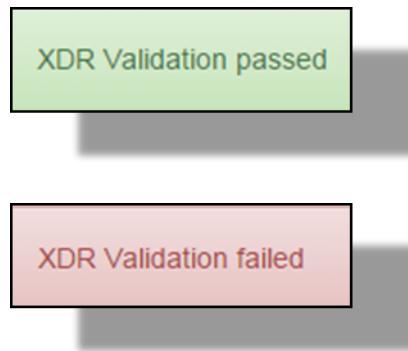
9. If the Tester (e.g., Vendor) accepts the data and confirms that the XDR message content within the ‘Log’ conforms to the testing objectives for the Test Case, the ‘Accept XDR’ button can be selected. However, if the XDR message content does not conform to the testing objectives for the Test Case, the ‘Reject XDR’ button is selected. The Tester (e.g., Vendor) is given conformation on selection by the ETT.





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 Tester (e.g., Vendor) is given conformation on selection by the ETT.



11. Acceptance or rejection of the XDR message content results in overall Test Case testing Success or Failure. Rejection resets the Test Case back to ‘Step 1’. This testing data is then available through the ‘Validation Report’ (reference [Section 2.4 Reporting](#)).

A screenshot of a software interface showing a test log entry. The entry is for 'Test ID #9' and describes the test as 'Test Tool authenticates with the Edge using bad certificates'. To the right of the text, there is a 'Description' column with a green checkmark icon and a 'Logs' column with a blue link. The entire row has a grey shadow underneath it.

A screenshot of a software interface showing a test log entry. The entry is for 'Test ID #9' and describes the test as 'Test Tool authenticates with the Edge using bad certificates'. Below the description, there is a step instruction: 'Step 1: Provide your endpoint and hit Run to send XDR'. To the right of the text, there is a 'Description' column with a red X icon and a 'Logs' column with a blue link. Below the log columns, there is a 'RETRY' button. The entire row has a grey shadow underneath it.



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

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 and imported into the SUT's trust store (link located 'XDR Test Cases' tab of ETT) before test execution.
- With the trust relationship established, the Vendor navigates to the target Test Case and populates the 'Non TLS Endpoint' field with the SUT's accurate information (all fields should correlate so the ETT and SUT can communicate to execute this Test Case; reference [2.3 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/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 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:

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 '**Receiver**'. This will enable test case selection.

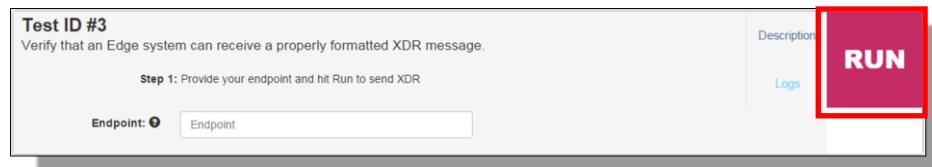
Your System as: Receiver

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

4. To gain additional information concerning a target Test Case'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.

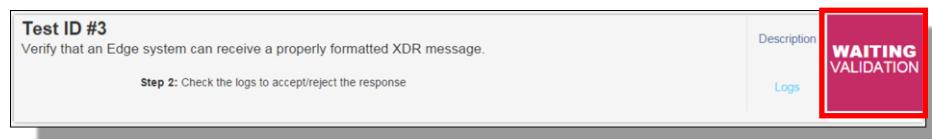
5. To initiate the target Test Case, the Tester (e.g., Vendor) must provide the SUT (their operated and managed Edge system) as a '**TLS Endpoint**' for the ETT to communicate with and send an XDR message to. The provided '**TLS Endpoint**' of the SUT is the message recipient for this Test Case.

6. Once the '**TLS Endpoint**' has been inserted, '**Run**' to transmit the XDR message.

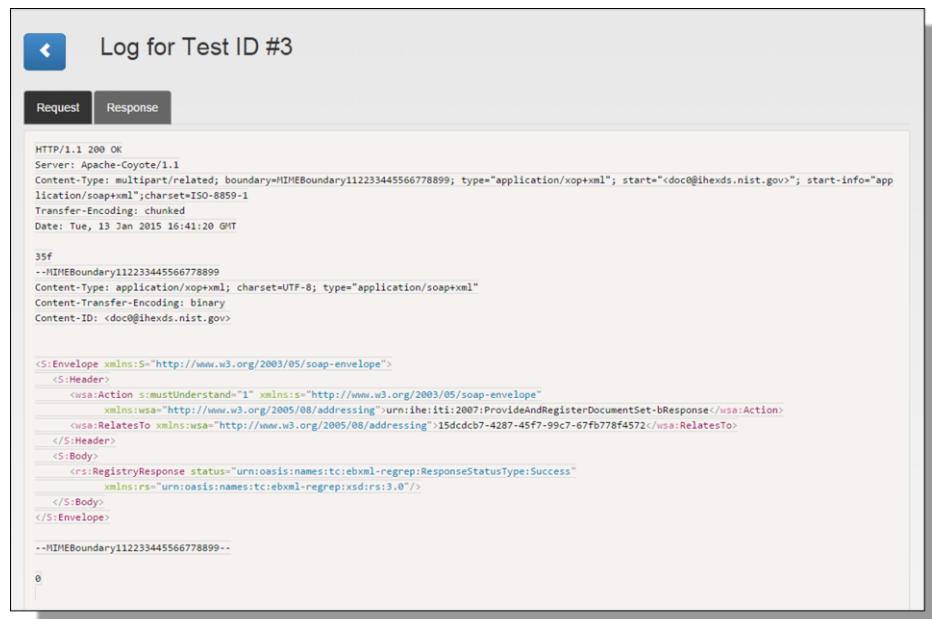


Note: Instructions are labeled in sequential order (e.g., 'Step 1', 'Step 2', 'Step 3') in the content description of the Test Case. For this Test Case, the 'TLS Endpoint' is provided by the Tester (e.g., Vendor).

- Once the XDR message has been sent, ETT will listen for the SUT's response/conformation of the sent message. Upon receipt of the message, the Tester (e.g., Vendor) is prompted to manually validate if the test results conformed to the testing objective. This is performed through clicking the 'Waiting Validation' button.



- This will bring up the 'Log' screen for the Test Case. The Tester (e.g., Vendor) is presented 'Request' and 'Response' tabs. Based upon the specific testing objective for a Test Case, one of the two tabs will contain XDR message information. The Tester (e.g., Vendor) reviews the 'Log' data and validates that the message content and metadata conforms to the testing objectives.



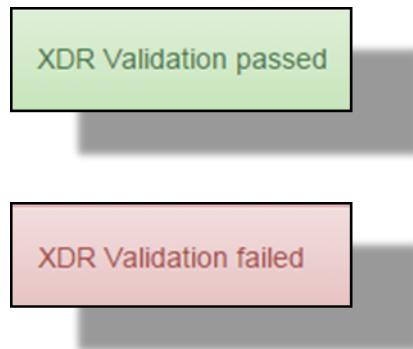
- If the Tester (e.g., Vendor) accepts the data and confirms that the XDR message content within the 'Log' conforms to the testing objectives for the Test Case, the

‘Accept XDR’ button can be selected. However, if the XDR message content does not conform to the testing objectives for the Test Case, the ‘Reject XDR’ button is selected. The Tester (e.g., Vendor) is given conformation on selection by the ETT.



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 Tester (e.g., Vendor) is given conformation on selection by the ETT.



11. Acceptance or rejection of the XDR message content results in overall Test Case testing Success or Failure. Rejection resets the Test Case back to ‘Step 1’. This testing data is then available through the ‘Validation Report’ (reference [Section 2.4 Reporting](#)).

Test ID #3 Verify that an Edge system can receive a properly formatted XDR message.	Description
---	-----------------

Test ID #3 Verify that an Edge system can receive a properly formatted XDR message. Step 1: Provide your endpoint and hit Run to send XDR Endpoint: <input type="text" value="Endpoint"/>	Description Logs RETRY
---	----------------------------------



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.

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 and imported into the SUT's trust store (link located '**XDR Test Cases**' tab of ETT) before test execution.
- 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/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 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:

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 'Receiver'. This will enable test case selection.

Your System as: Receiver

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

4. To gain additional information concerning a target Test Case'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 the target Test Case, the Tester (e.g., Vendor) must provide the SUT (their operated and managed Edge system) as a 'TLS Endpoint' for the ETT to communicate

with and send an XDR message to. The provided ‘**TLS Endpoint**’ of the SUT is the message recipient for this Test Case.

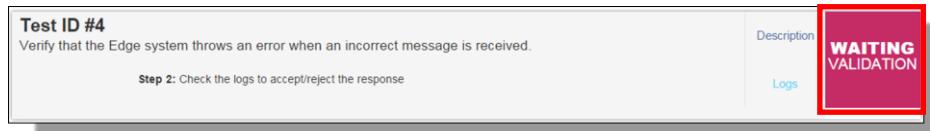


6. Once the ‘**TLS Endpoint**’ has been inserted, ‘**Run**’ to transmit the XDR message.



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, ETT will listen for the SUT’s response/conformation of the sent message. Upon receipt of the message, the Tester (e.g., Vendor) is prompted to manually validate if the test results conformed to the testing objective. This is performed through clicking the ‘**Waiting Validation**’ button.



8. This will bring up the ‘**Log**’ screen for the Test Case. The Tester (e.g., Vendor) is presented ‘**Request**’ and ‘**Response**’ tabs. Based upon the specific testing objective for a Test Case, one of the two tabs will contain XDR message information. The Tester (e.g., Vendor) reviews the ‘**Log**’ data and validates that the message content and metadata conforms to the testing objectives.

```

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=--MIMEBoundary112233445566778899; type="application/xop+xml"; start=<doc@ihexds.nist.gov>; start-info="app
lication/soap+xml"; charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Tue, 13 Jan 2015 16:47:08 GMT

430
--MIMEBoundary112233445566778899
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <doc@ihexds.nist.gov>

<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope">
  <S:Header>
    <wsa:Action s:mustUnderstand="1" xmlns:s="http://www.w3.org/2003/05/soap-envelope"
      xmlns:wsa="http://www.w3.org/2005/08/addressing">http://www.w3.org/2005/08/addressing/fault</wsa:Action>
    <wsa:RelatesTo xmlns:wsa="http://www.w3.org/2005/08/addressing">5dc0c56e-e90b-4a50-bd4-a3ecfaf0bae</wsa:RelatesTo>
  </S:Header>
  <S:Body>
    <fault:Fault xmlns:fault="http://www.w3.org/2003/05/soap-envelope">
      <fault:Code>
        <fault:Value>fault:Sender</fault:Value>
      </fault:Code>
      <fault:Reason>
        <fault:Text xml:lang="en">Sender: Correct Header Namespace - Expected: ; Found: http://www.w3.org/2003/05/soap-envelope</fault:Text>
      </fault:Reason>
    </fault:Fault>
  </S:Body>
</S:Envelope>
--MIMEBoundary112233445566778899--

```

- If the Tester (e.g., Vendor) accepts the data and confirms that the XDR message content within the ‘Log’ conforms to the testing objectives for the Test Case, the ‘Accept XDR’ button can be selected. However, if the XDR message content does not conform to the testing objectives for the Test Case, the ‘Reject XDR’ button is selected. The Tester (e.g., Vendor) is given conformation on selection by the ETT.

Accept XDR

Reject XDR



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

- The Tester (e.g., Vendor) is given conformation on selection by the ETT.

XDR Validation passed



11. Acceptance or rejection of the XDR message content results in overall Test Case testing Success or Failure. Rejection resets the Test Case back to ‘**Step 1**’. This testing data is then available through the ‘**Validation Report**’ (reference [Section 2.4 Reporting](#)).

The screenshot shows a test case entry for 'Test ID #4'. The description is 'Verify that the Edge system throws an error when an incorrect message is received.' A green checkmark icon is displayed next to the 'Logs' button, indicating success.

The screenshot shows a test case entry for 'Test ID #4'. The description is 'Verify that the Edge system throws an error when an incorrect message is received.' Below it, there is a step description: 'Step 1: Provide your endpoint and hit Run to send XDR'. An input field labeled 'Endpoint' is shown. To the right, a red 'X' icon is displayed next to the 'Logs' button, and a red 'RETRY' button is present.



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.

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 HISIP (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 and imported into the SUT’s trust store (link located ‘**XDR Test Cases**’ tab of ETT) before test execution.
- With the trust relationship established, the Vendor navigates to the target Test Case and populates the ‘**Non TLS Endpoint**’ field with the SUT’s accurate information (all fields should correlate so the ETT and SUT can communicate to execute this Test Case; reference [2.3 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 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 ‘**Receiver**’. This will enable test case selection.

Your System as: Receiver

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

4. To gain additional information concerning a target Test Case’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 the target Test Case, the Tester (e.g., Vendor) must provide the SUT (their operated and managed Edge system) as a ‘**TLS Endpoint**’ for the ETT to communicate with and send an XDR message to. The provided ‘**TLS Endpoint**’ of the SUT is the message recipient for this Test Case.

6. Once the ‘**TLS Endpoint**’ has been inserted, ‘**Run**’ to transmit the XDR message.

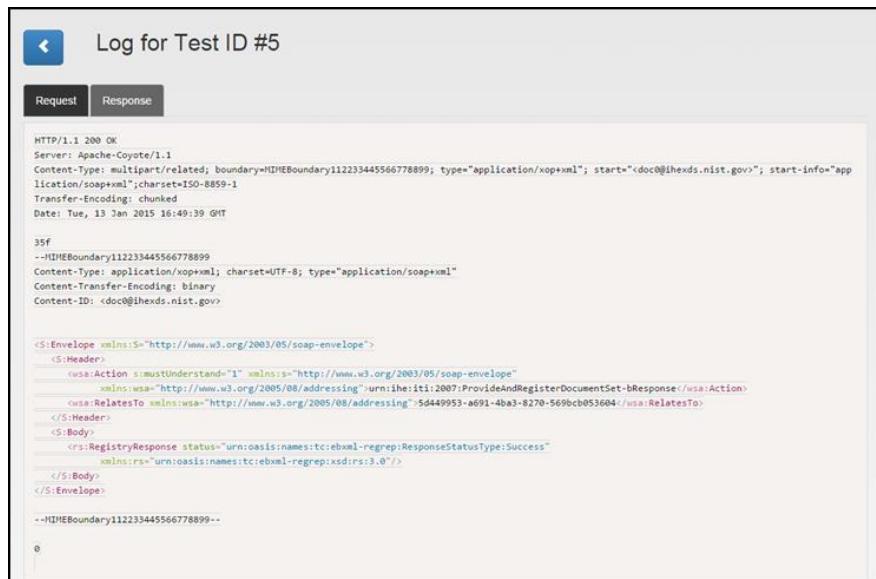


*Note: Instructions are labeled in sequential order (e.g., ‘Step 1’, ‘Step 2’, ‘Step 3’) in the content description of the Test Case. For this Test Case, the ‘**TLS Endpoint**’ is provided by the Tester (e.g., Vendor).*

7. Once the XDR message has been sent, ETT will listen for the SUT’s response/conformation of the sent message. Upon receipt of the message, the Tester (e.g., Vendor) is prompted to manually validate if the test results conformed to the testing objective. This is performed through clicking the ‘**Waiting Validation**’ button.

8. This will bring up the ‘**Log**’ screen for the Test Case. The Tester (e.g., Vendor) is presented ‘**Request**’ and ‘**Response**’ tabs. Based upon the specific testing objective for a Test Case, one of the two tabs will contain XDR message information. The

Tester (e.g., Vendor) reviews the ‘Log’ data and validates that the message content and metadata conforms to the testing objectives.



```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=-----Boundary112233445566778899; type="application/xop+xml"; start=<doc@ihexds.nist.gov>; start-info="application/soap+xml"; charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Tue, 13 Jan 2015 16:49:39 GMT
35F
-----Boundary112233445566778899
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <doc@ihexds.nist.gov>

<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope">
  <S:Header>
    <ns0:Action s:mustUnderstand="1" xmlns:ns0="http://www.w3.org/2003/05/soap-envelope">
      urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-bResponse-/ns0:Action
    </ns0:Action>
    <ns0:RelatesTo xmlns:ns0="http://www.w3.org/2005/08/addressing">5d449953-a691-4ba3-8270-569bc053604</ns0:RelatesTo>
  </S:Header>
  <S:Body>
    <ns1:RegistrationResponse status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"
      xmlns:ns1="urn:oasis:names:tc:ebxml-regrep:xsd:ns1:3.0"/>
  </S:Body>
</S:Envelope>
-----Boundary112233445566778899-
```

9. If the Tester (e.g., Vendor) accepts the data and confirms that the XDR message content within the ‘Log’ conforms to the testing objectives for the Test Case, the ‘Accept XDR’ button can be selected. However, if the XDR message content does not conform to the testing objectives for the Test Case, the ‘Reject XDR’ button is selected. The Tester (e.g., Vendor) is given conformation on selection by the ETT.



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 Tester (e.g., Vendor) is given conformation on selection by the ETT.

XDR Validation passed



11. Acceptance or rejection of the XDR message content results in overall Test Case testing Success or Failure. Rejection resets the Test Case back to ‘**Step 1**’. This testing data is then available through the ‘**Validation Report**’ (reference [Section 2.4 Reporting](#)).

Test ID #5 Verify that an Edge system can receive a properly formatted XDR message.	Description
---	-----------------

Test ID #5 Verify that an Edge system can receive a properly formatted XDR message. Step 1: Provide your endpoint and hit Run to send XDR Endpoint: <input type="text" value="Endpoint"/>	Description Logs RETRY
---	----------------------------------



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.