

DSM Edge Implementation Guides: SMTP Edge Protocol



Last Modified on 03/28/2023 4:24 pm EDT

Overview

The intention of this document is to provide instructions for integrating with Updox's Direct Secure Messaging service via secure SMTP. This document contains no instructions for certifying Edge via the Edge Testing Tool.

Unless otherwise noted, the instructions below apply for both XDM and non-XDM messages.

Definitions

- **Edge System** - Customer system using Updox to send and receive Direct Secure Messages. In the scenario outlined in this document, this integration is via secure SMTP.
- **Edge SMTP Client** - The customer system that will relay SMTP messages to Updox for forwarding as Direct Secure Messages.
- **Edge SMTP Server** - The customer system that Updox will relay decrypted Direct Secure Messages to via secure SMTP. This may or may not be the same system as the Edge SMTP Client.
- **Message Disposition Notification (MDN)** - a special email that functions as a machine-readable receipt document for an email. The MDN contains the original message ID of a message and status information about the original message.

Prerequisites

The Edge System requires an SMTP client and an SMTP server (which might be the same SMTP agent) that support

- TLS via the SMTP STARTTLS extension
- Authentication via PLAIN SASL

NOTE: Currently, Updox supports only TLS 1.2

Sending Messages from the Edge into Updox/DSM

In order to relay messages TO Updox, the Edge system will require the following:

1. The Edge SMTP client must be configured for Transport Layer Security via the SMTP STARTTLS extension.
2. The Edge SMTP client must be configured to send authentication credentials via PLAIN SASL.
3. Contact Updox for the SMTP endpoint (host/port) information for the environment (QA/Production) you're

integrating with. It may also be necessary for Updox Operations to whitelist the Edge system, depending on the environment.

4. For each message sent to Updox by the Edge system:

1. The credentials sent via PLAIN SASL must be the valid username/password of an active Direct Secure Messaging user within the Updox system.
2. The MAIL FROM address in the SMTP envelope of the outgoing message and the FROM address in the payload will both be **ignored** by Updox. When the message is relayed as a Direct Secure Message, the Direct address of the SASL-authenticated user above will be used as the FROM address.
3. The Edge system will need to save the original `Message-Id` header for outgoing message, in order to handle the MDNs for the outgoing message.

NOTE: DIFFERENCES WITH THE EDGE TESTING TOOL

- Unlike the Edge Testing Tool, Updox DOES NOT require the Edge Client to send the `Disposition-Notification-Options` header when sending, and Updox will **ignore** this header when sent by the Edge Client. Instead, when forwarding messages via DSM, Updox will *always* request a `dispatched` MDN via creating its own `Disposition-Notification-Options` header and `X-DIRECT-FINAL-DESTINATION-DELIVERY` parameter.
- Unlike the Edge Testing Tool, Updox DOES NOT currently require a client certificate (Mutual TLS) in order for the Edge system to connect and send messages. However, if the Edge system requires use of Mutual TLS when receiving messages from Updox, Updox can and will generate and install the necessary client certificate (see Receiving section, below).

Receiving Messages / MDNs from Updox/DSM at the Edge

In order to receive Direct Secure Messages and MDNs from Updox via SMTP, the Edge system will require the following:

1. The Edge SMTP server must be configured for Transport Layer Security via the SMTP STARTTLS extension.
2. The Edge SMTP server must be configured to accept authentication credentials via PLAIN SASL (often disabled by default).
3. If Mutual TLS is to be used for Updox to connect to the Edge, Updox's public client certificate will have to be installed on the Edge system.
4. Updox will need the following information in order to begin relaying Direct Messages to the Edge:
 1. Public host / port of the Edge SMTP server
 2. Username/password (must be furnished via secure channel).
 3. (optional)
5. For each message sent to the Edge:
 1. The MAIL FROM address in the SMTP envelope and the FROM address in the mail header will both be set to the Direct address of the sender. (ex. jeff@direct.notupdox.com)

2. The RCPT TO address in the SMTP envelope and the TO address in the mail will header will both be set to the Direct address of the recipient (ex. jessica@direct.updoxcustomer.com)

NOTE: Updox supports Edge configurations at either the Partner (ie. EHR) or Account (ie. individual practice) level. This means that individual accounts can have their own credentials on the Edge system, or even their own endpoints.

However, Updox does not support authenticating to the Edge system at any finer granularity than at the account level (ie at the individual user level). This is, of course, inconsistent with how the Edge system must authenticate to Updox, which requires individual user credentials.

MDN Processing

For each message sent from the Edge, Updox will send a single MDN back to the Edge.

- In the case of a failure to send the corresponding Direct Secure Message, an MDN will be sent back to the Edge immediately
- In all other cases the MDN will be sent after a 1-hour timeout.
- The MDNs sent to the Edge conform to [RFC 2298](#). Importantly, this means:
 - Can be identified as an MDN by the top-level `Content-Type` header, that begins
 - `Content-Type: multipart/report; report-type=disposition-notification;`
 - The `Original-Message-ID` header of the MDN is set to the value of the `Message-ID` header from the original message sent to the Edge.

Supported Dispositions / Cases:

Disposition	Human-Readable Message
dispatched	Original message successfully delivered
failed	We were unable to deliver your message.
failed	We attempted to deliver your message but did not receive timely confirmation of receipt.
failed	Your message was sent to the recipient but no final delivery confirmation was received