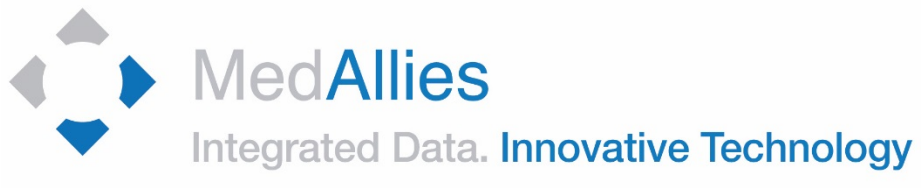


MedAllies General Support Training Guide

Version 1.2

Rev. 1/27/2017

Table of Contents

1. Overview

(Dependent on support model) provides first / second line **(Dependent on support model)** support for Direct. First line support generally documents the reported issue and assigns an initial priority. Sedond line support also attempts to resolve questions and minor issues through the use of available knowledge management tools.

The purpose of this document is to introduce the learner to the basic elements used in Direct, basic troubleshooting tools, and the support data template required to request MedAllies support.

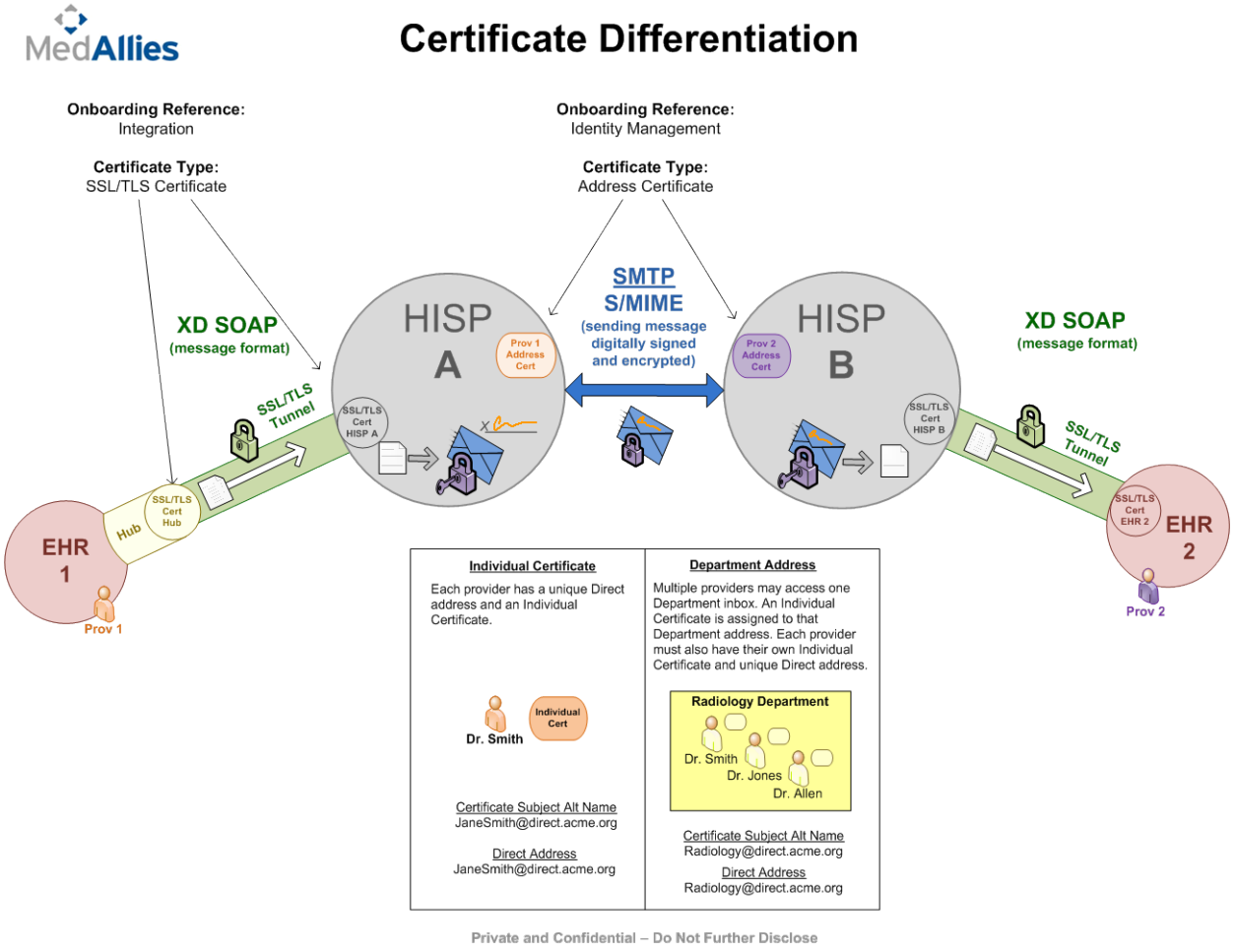
2. Learning Objective

The learning objective is to be able to provide the user a basic understanding of the following:

- Direct Messaging Flows
- Components Related to Direct Messaging
- Troubleshooting Tools
- Support Requests

3. Direct Messaging Flows

The diagram below outlines the flow of Direct messages between edge systems and their respective HISPs.



- Direct communications can be a 1:1 exchange or a 1:many
- Certified EHRs connect to accredited HISPs in the Direct Trust Trust Bundle
- Direct Accounts are provisioned by the HISP and recorded in the EHR
- Direct Messages are sent/received using validly provisioned Direct Accounts
- A secure SSL/TLS Tunnel transmits unencrypted messages between the EHR and the MedAllies HISP

4. Components Related to Direct Messaging

4.1. Direct Address Structure

There are 2 parts to a Direct address:

- **Name part**
- **Domain part**

Format: Name@Domain

Example: johnsmith@Direct.acme.org

4.1.1. Name Part

Allowable characters:

- A-Z
- a-z
- 0-9
- Underscore (_)
- Hyphen (-)
- Period (.)

4.1.2. Domain Part

- Domain Name: a unique internet namespace
  - medalliesdirect.net
  - acme.org
- Direct addresses must belong to a valid domain
- Purpose of domain name: to have a segregated namespace for Direct addressing
- Domain name must be used explicitly for Direct messaging
  - Cannot be same as corporate email address

4.2. IP Addresses

- Public vs private
  - In a typical organization servers exist on a private network behind a firewall
  - A firewall is a network security system that controls the incoming and outgoing network traffic based on an applied rule set.
    - Servers are assigned private IP addresses such as 192.168.100.10
    - Private address ranges
      - 10.0.0.1 – 10.255.255.255
      - 172.16.0.1 – 172.31.255.255
      - 192.168.0.1 – 192.168.255.255
    - Private addresses are not reachable from the internet
    - Firewalls separate the private network from the internet
    - Firewalls can have one or more public IP addresses which can be translated to private server addresses for the purpose of publishing resources

- Whitelisting: a list or register of those that are being provided a particular privilege, service, mobility, access, or recognition. Those on the list will be accepted, approved, or recognized.
  - By default inbound firewalled connections are blocked
  - Selected public IP addresses can be permitted access based on firewall rules (whitelisting)
  - Private IP addresses may not be whitelisted

4.3. Certificates

- Video (located at *http://www.youtube.com/watch?v=LRMBZhdFjDI*)

4.4. TLS

- Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet.
- TLS ensures no third parties may tamper with or eavesdrop on message
- TLS is the successor to Secure Sockets Layer (SSL)

5. Troubleshooting Steps

5.1. Request Recent Transaction

Is this a recurring issue?

In order to effectively troubleshoot issues, the message failures should be actively occurring. "One off" messages are difficult to troubleshoot as they cannot be replicated. If the message that failed is older than 2 hours, have the user send a more recent message. If the message fails once again, continue below. Otherwise, please document and advise customer to report if it should happen again. Report patterned, or recurring issues to MedAllies for further investigation.

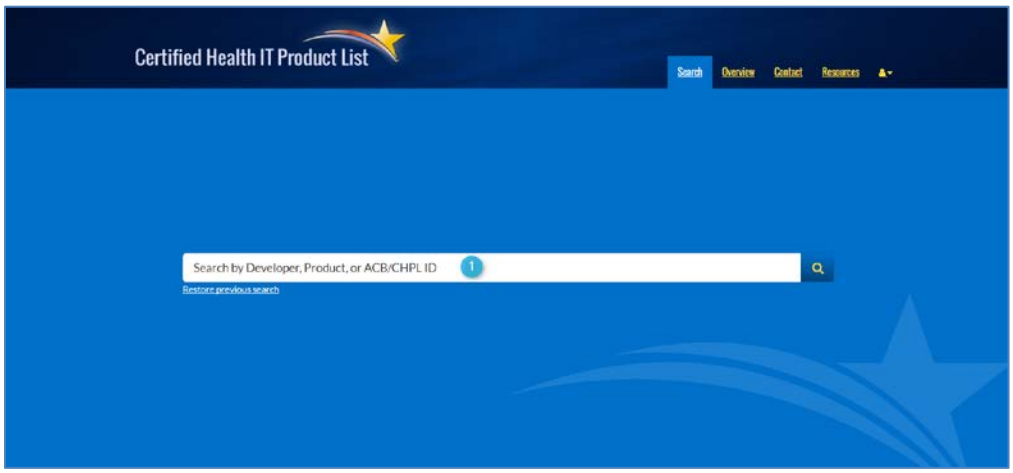
5.2. Check for Certified Products

Are both sender and receiver using certified EHR products?

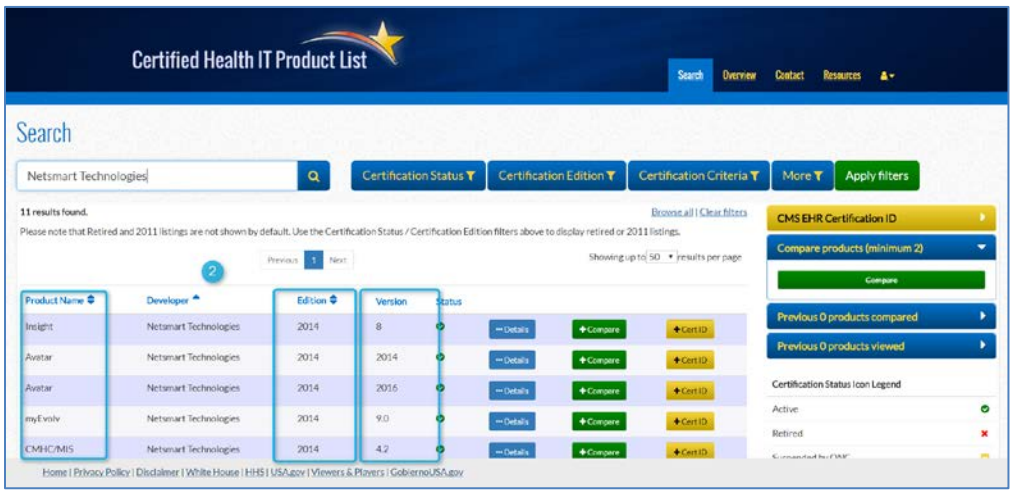
CMS and the ONC have established standards and other criteria for structured data that EHRs must meet in order to qualify for use in the Medicare and Medicaid EHR Incentive Programs. Messages must originate from these certified products. This site can be accessed to confirm an EHR is accredited and can be used to exchange Direct messages:

https://chpl.healthit.gov/#/search

1) Enter Product or Developer name in search bar



2) Confirm the product version is on the list of certified editions



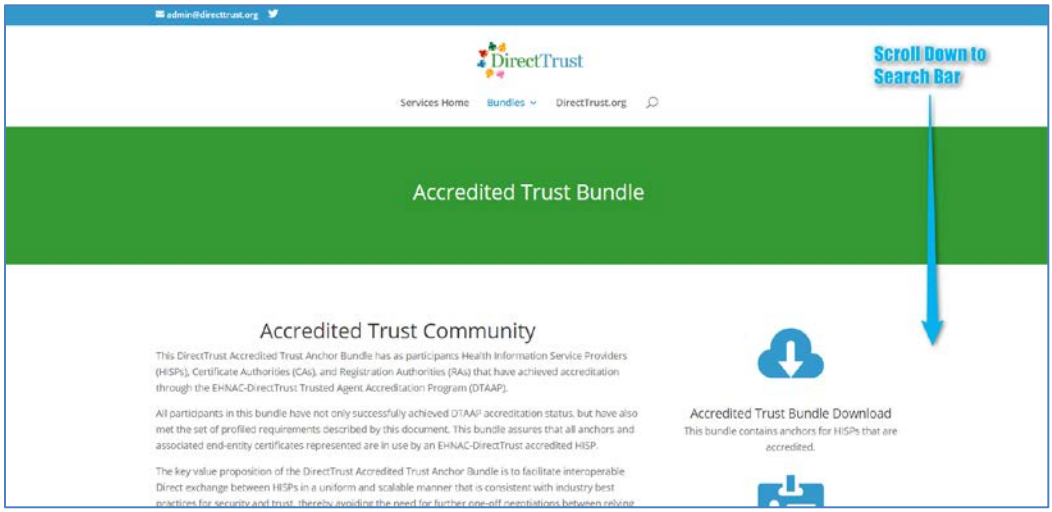
5.3. Confirm Trust

Are both sender and receiver using HISPs in the Direct Trust Trust Bundle?

The HISPs for both sending and receiving entities must be in the Direct Trust Trust Bundle to ensure successful Direct Message exchange. The Direct Trust (DT) website provides visibility to the HISPs in the DT Trust Bundle. This site can be accessed to verify the DT status of the third party HISP:

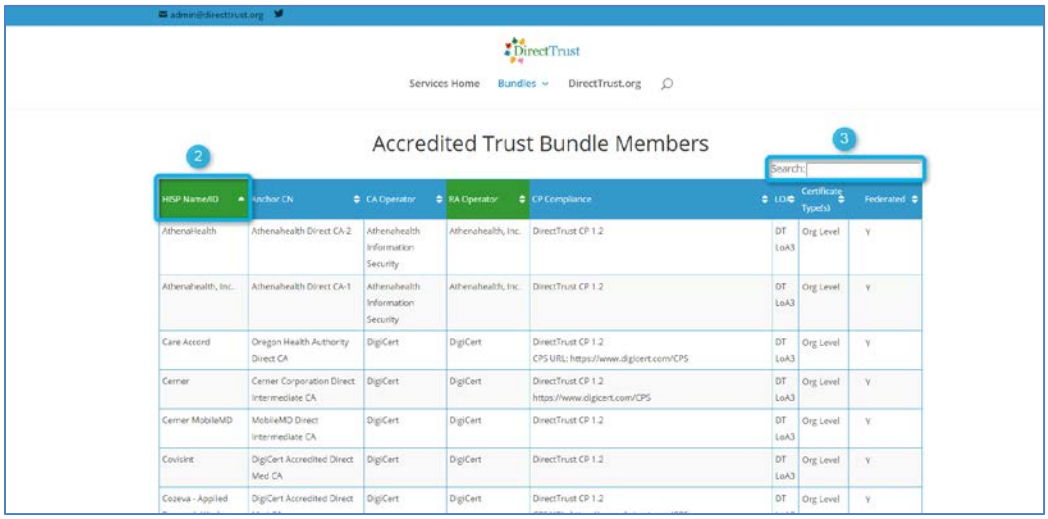
https://services.directtrust.org/about_accredited_bundle/

1) Scroll down the page until you arrive at the Search Bar



2) Sort by HISP name or

3) Search by HISP name



5.4. Validate Direct Addresses

Are both the sending and receiving Direct Addresses valid?

Direct Addresses must be valid, provisioned by an accredited HISP in the DT Trust Bundle, and active to ensure successful Direct Message exchange.

Validate addresses by:

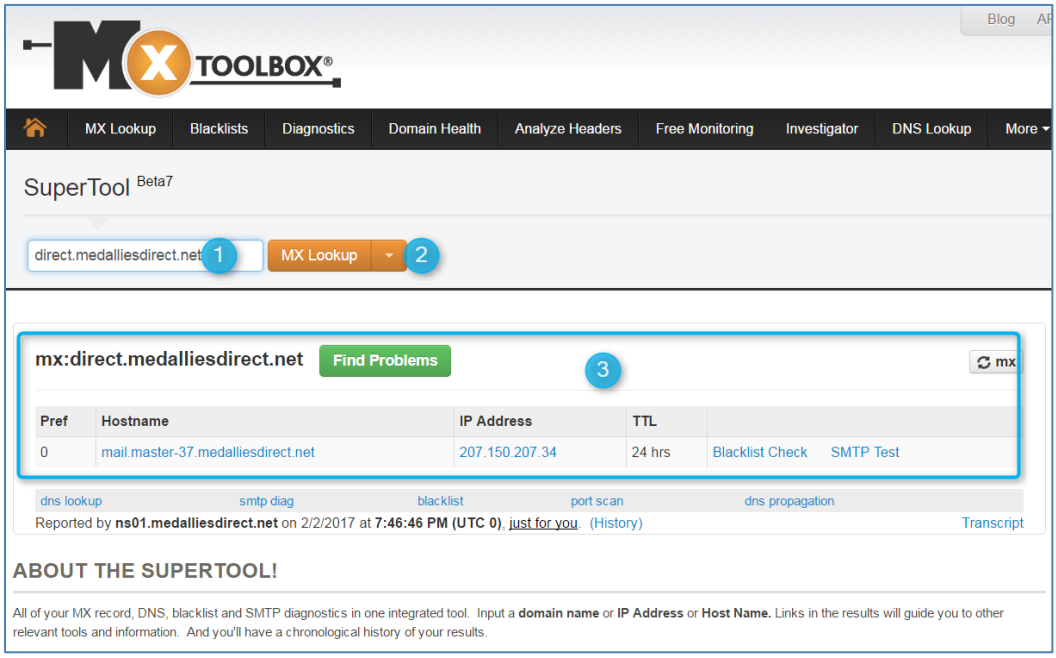
- Checking for typos and “active” status in the Directory
- Confirm only allowable characters are used.

5.5. Validate Domain

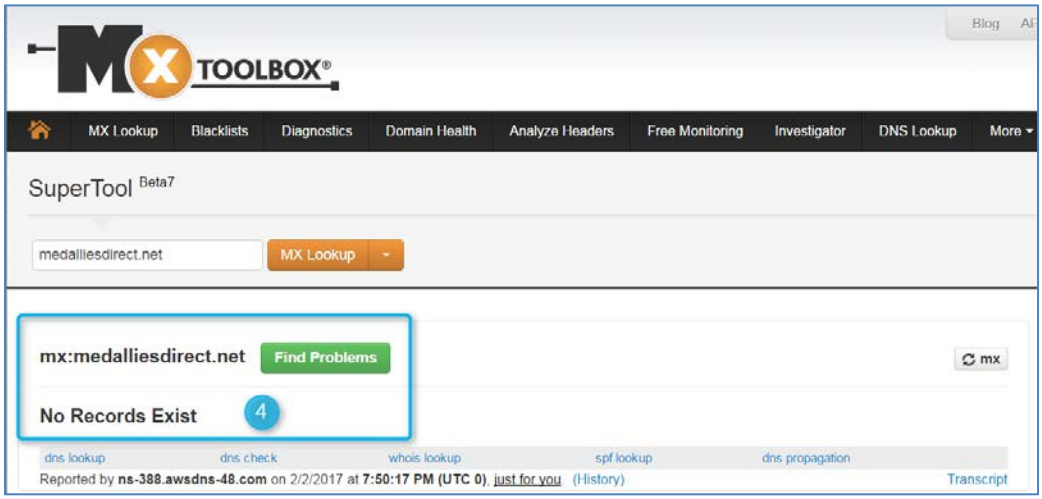
Are the domains behind the Direct Address valid domains?

Validate domains using: http://mxtoolbox.com

1) Enter domain name to search
2) Select MX Lookup
3) Confirm domain validity



4) "No Records Exist" will display if there is an issue with the domain name entered



5.6. Confirm Certificate Discoverability

Are the certificates discoverable?

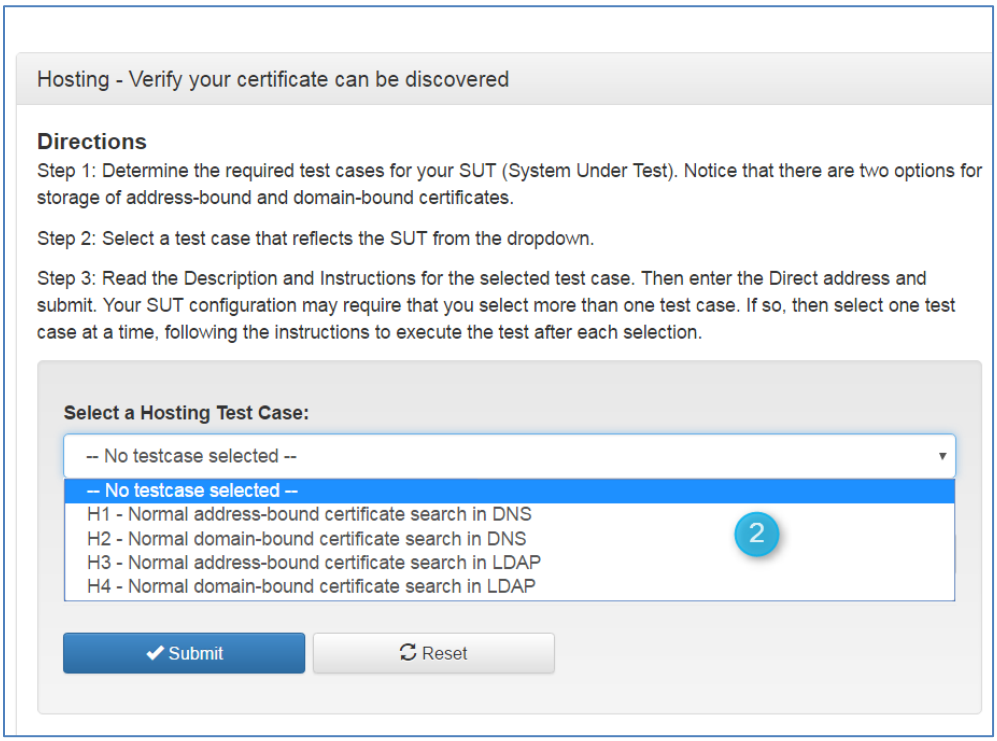
Direct certificates must be hosted correctly and discoverable by other Direct implementations in order for messaging to succeed. Messages will not be delivered

if the Direct addresses do not have valid certificates. You can validate certificates for any of four test cases at this site:

Validate certificate discoverability using: https://sitenv.org/web/site/direct-certificate-discovery-tool-2015

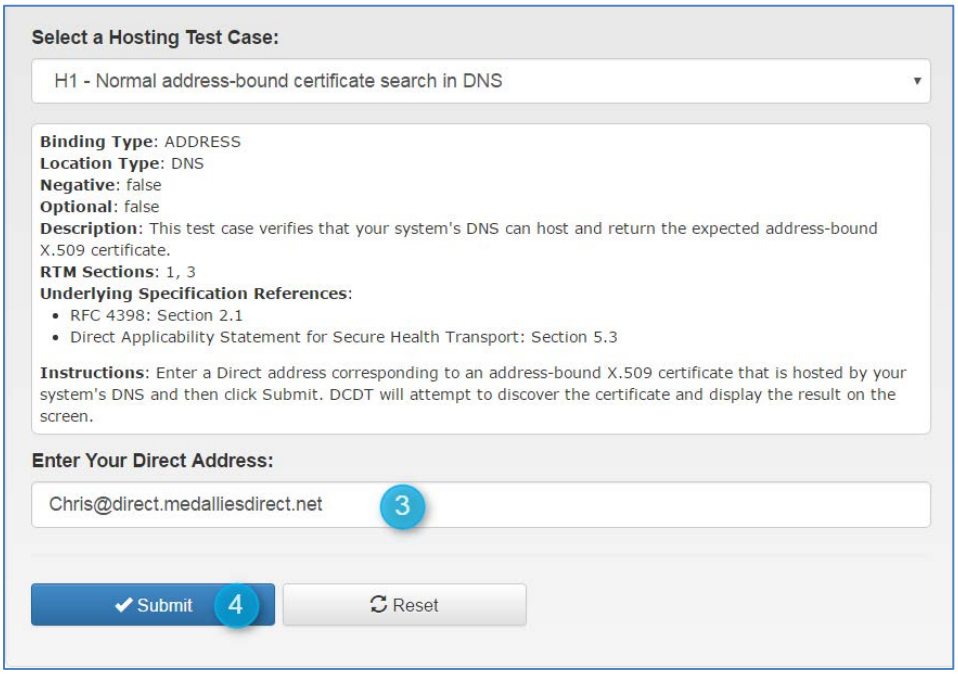
1) Scroll down to the discovery tool

2) Select each of a test case from the drop down.

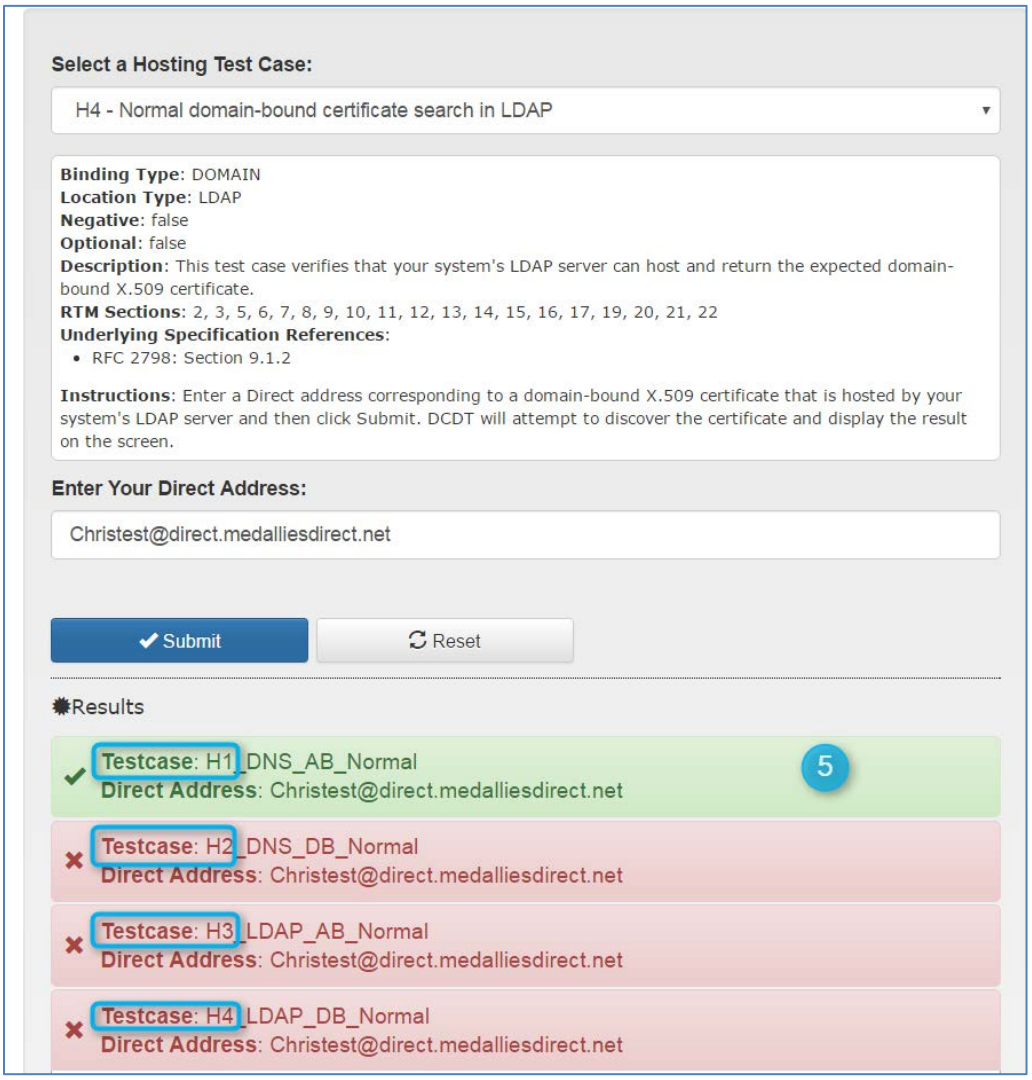


3) Enter Direct Address to check for certificate discoverability

4) Select Submit



5) Results appear below - The certificate must be able to be discoverable (green) under 1 of 4 use cases. Please test each until a certificate is discoverable (green result). If none are discoverable, please open a support request for further investigation.



5.7. Confirm Production Environment Exchanges

Are the users sending / receiving from production environments?

MedAllies supports only the connection of Production environments to the MedAllies Production HISP. Both addresses used to exchange messages must be in Production environments.

5.8. Other Environment Changes

Questions to explore if message exchanges have been previously successful:

- What has changed in the environment?
  - New system versions?
    - MedAllies should be made aware of application upgrades. New versions should be tested prior to deployment to ensure continuity in Direct message exchanges.
    - New servers?
  - Have IP addresses been mutually whitelisted?
    - Have there been changes to the Firewall?

6. Support Requests

Direct support requests are to be reported to the MedAllies Support Center. The required support template information may be submitted through various support channels.

6.1. Support Template

The following template is used to capture the required data necessary to request support.

MedAllies Support Requests – Required Data

Sending Organization Info:

1. Sending Organization Name:
2. Organization Vendor Product:
3. Sending HISP:
4. Sending Direct Address:

Receiving Organization Info:

1. Receiving Organization Name:
2. Organization Vendor Product:
3. Receiving HISP:
4. Receiving Direct Address:

Message Timestamp and Time zone:

Issue / Error Encountered (secure any PHI, if applicable):

Is this affecting MU calculation for the client?

6.2. Support Channels

Support requests may be submitted either by email or phone.

- Email: DirectSupport@MedAllies.com
- Telephone: 855-250-7867, Option 1

6.3. Support Hours

The MedAllies Support Center is available during standard support hours.

6.3.1. Standard Support Hours

Standard support hours are 8:30am – 5pm Eastern, Monday through Friday.

6.3.2. Afterhours Support

The MedAllies Support Center is available 24/7 for emergency afterhours support.

6.4. Support Processes

6.4.1. Case Creation

Support requests are acknowledged and cases created within one hour of receipt of the request.

6.4.2. Troubleshooting Process

- Troubleshooting begins upon receipt of required information
- Cases are escalated timely
- Customer is kept updated