Configuring ETT using AMIs

**Introduction**

The document explains the process on how to use ONC provided AMIs to install and configure a local instantiation of the Edge Testing Tool.

**Note:** The ETT AMIs is currently available as private images. An organization would have to provide their AWS account id so that ONC team can authorize the organization to access and implement the AMI’s in their account space.

**ETT Deployment Architecture and Instances**

The diagram below shows a high level overview of the ETT deployment architecture



The ETT architecture requires three registered domains for running all the components, we will refer to these three domains as:

* Edgedomain: top-level domain for user access (user interface), Direct, and XDR testing
* Jamesdomain: SMTP, IMAP, POP protocol testing and C-CDA Validator
* Directdomain: Direct testing

The provided AMI’s are functional with these pre-configured parameters for the above three domains:

* ttpedgedev.sitenv.org (Edgedomain), SITEAMI-TTPEDGE
* ttpdsdev.sitenv.org, (Jamesdomain), SITEAMI-TTPDS1
* ttpds2dev.sitenv.org. (Directdomain), SITEAMI-TTPDS2

After instantiating, you will have to follow the outlined steps below to point the pre-configured settings to your own domain names and your own corresponding certificates.

**Port, Domain Configuration, and Certificate Creation**

|  |  |  |
| --- | --- | --- |
| **Server** | **Ports - Inbound** | **Outbound** |
| Edge Test Tool | - 25 (SMTP)  - 53 TCP/UDP (DNS)  - 11080/11084/8888 (toolkit)  - 80/443 | - 25/53/10389/11389/12389/  110/143/SUT’s XDR ports |
| James Server | - 25 (SMTP)  - 110 (POP3)  - 143(IMAP4)  - 8080 (tomcat – C-CDA validator service) | - 25/110/143 |
| Direct Server | - 25 (SMTP)  - 110 (POP3)  - 143(IMAP4)  - 53 TCP/UDP (DNS)  - 10389/11389/12389 (LDAP) | - 25/53/10389/11389/ 12389/110/143 |

To create new, self-signed certificates for XDR using TLS follow these steps:

1. Create a key pair using **keytool**; set the alias to “1” in the keystore, password to “changeit” (you could use a different password – corresponding references in the configuration needs to be updated)
   * 1. *keytool -genkey -alias 1 -keyalg RSA -keystore /opt/ttp/certificates/xdr/keystore*
     2. *if you want to use a truststore different from the keystore, duplicating this file and referencing in the step 2.i below would be a start. This separation allows importing the trusted keys to the truststore without modifying the keystore. See Note 2 below.*
2. Update the config file as necessary.
   * 1. *Connector for port 11080 in /opt/tomcat7/conf/server.xml if the password or the key/store file names are changed*
     2. Xdstoolkit configuration – if the environment/filenames/password need to be changed.

Note 1: If you want to use existing CA certs for this purpose, create (or import) the keystore with alias “1”/password “changeit” and update the certs using the same steps as above skipping the creation step 1.

Note 2: For the ETT to communicate with SUT’s using different certs, the SUT keys needs to be imported into the trust store using these commands:

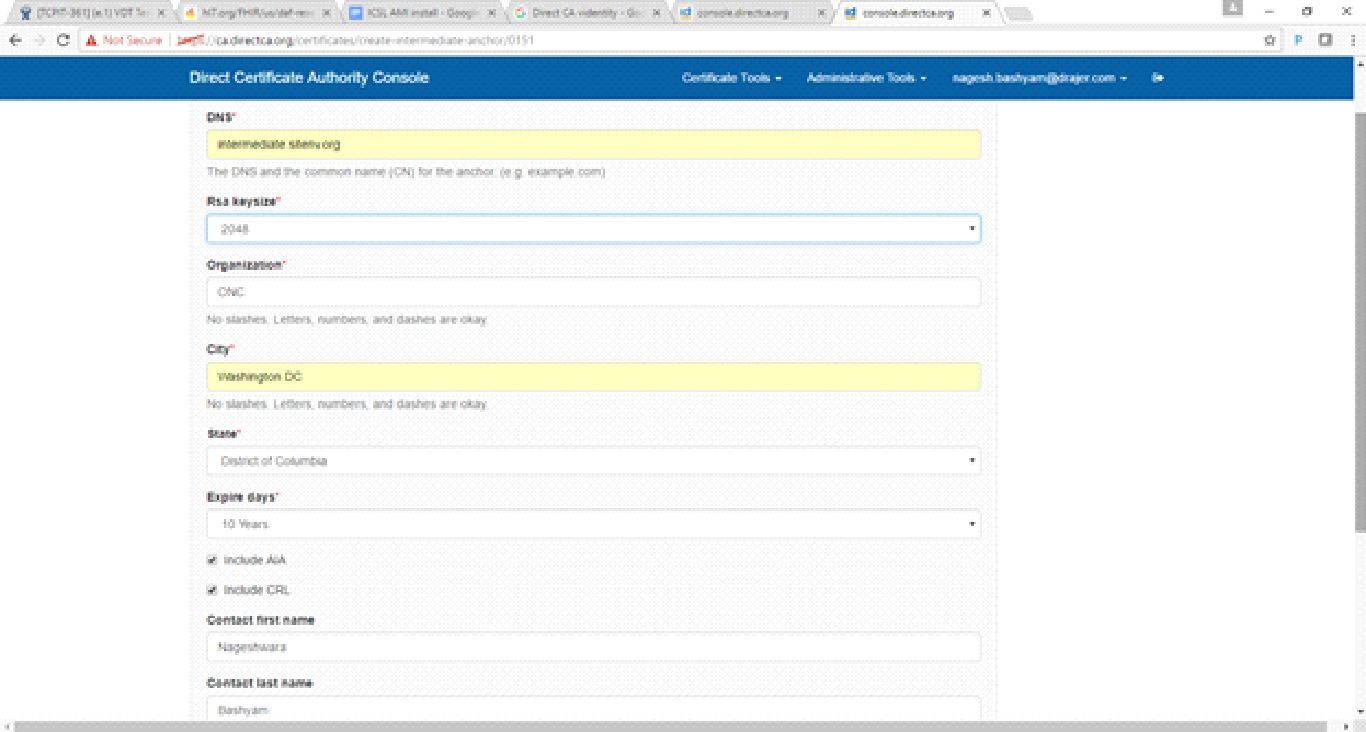
1. keytool -importcert -alias any-name -file cer-file-path -keystore */opt/ttp/certificates/xdr/truststore*

To create new, self-signed certificates for Direct follow these steps:

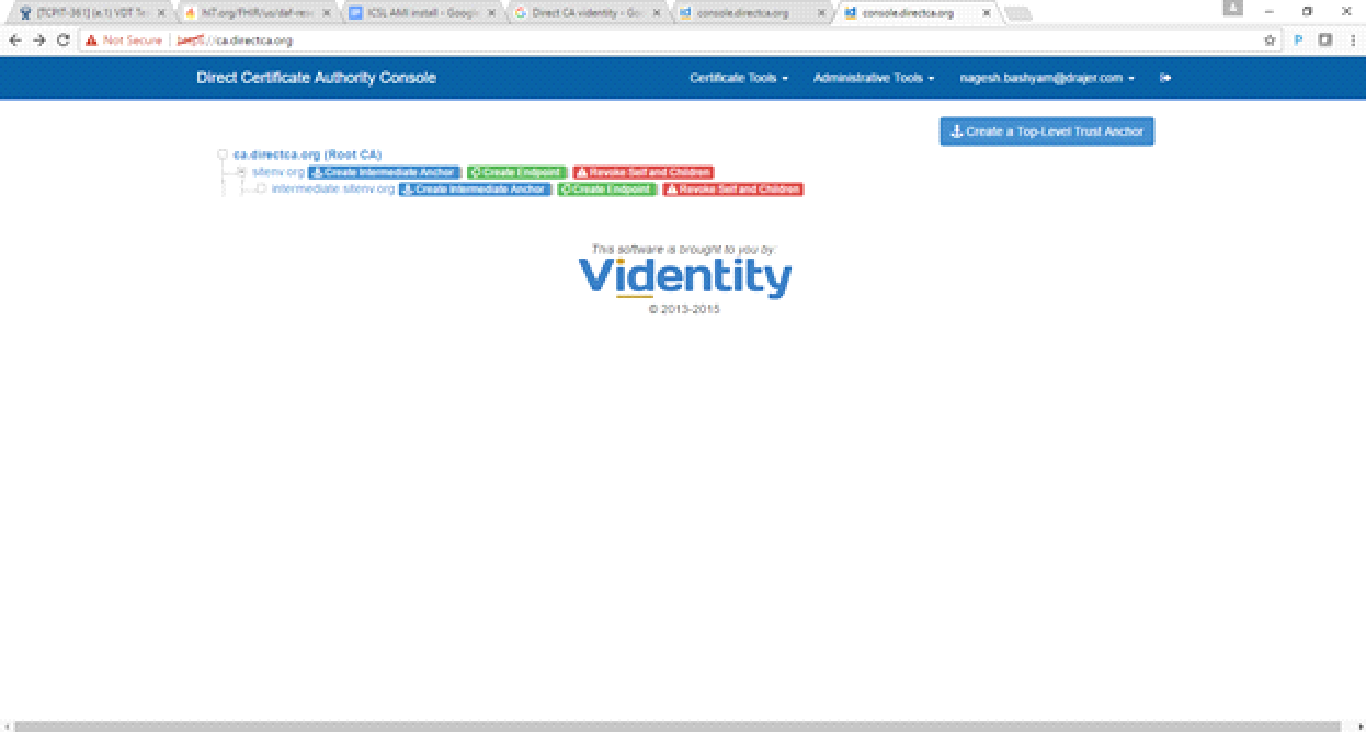
1. Sign up for an account at: https://ca.directca.org/

2. Create a **Top Level Trust Anchor** for the primary domain from which the direct subdomain will be created. (For example, if the top level domain is sitenv.org and the subdomain for direct is ttpedge.sitenv.org then you should create the top level trust anchor for sitenv.org.)

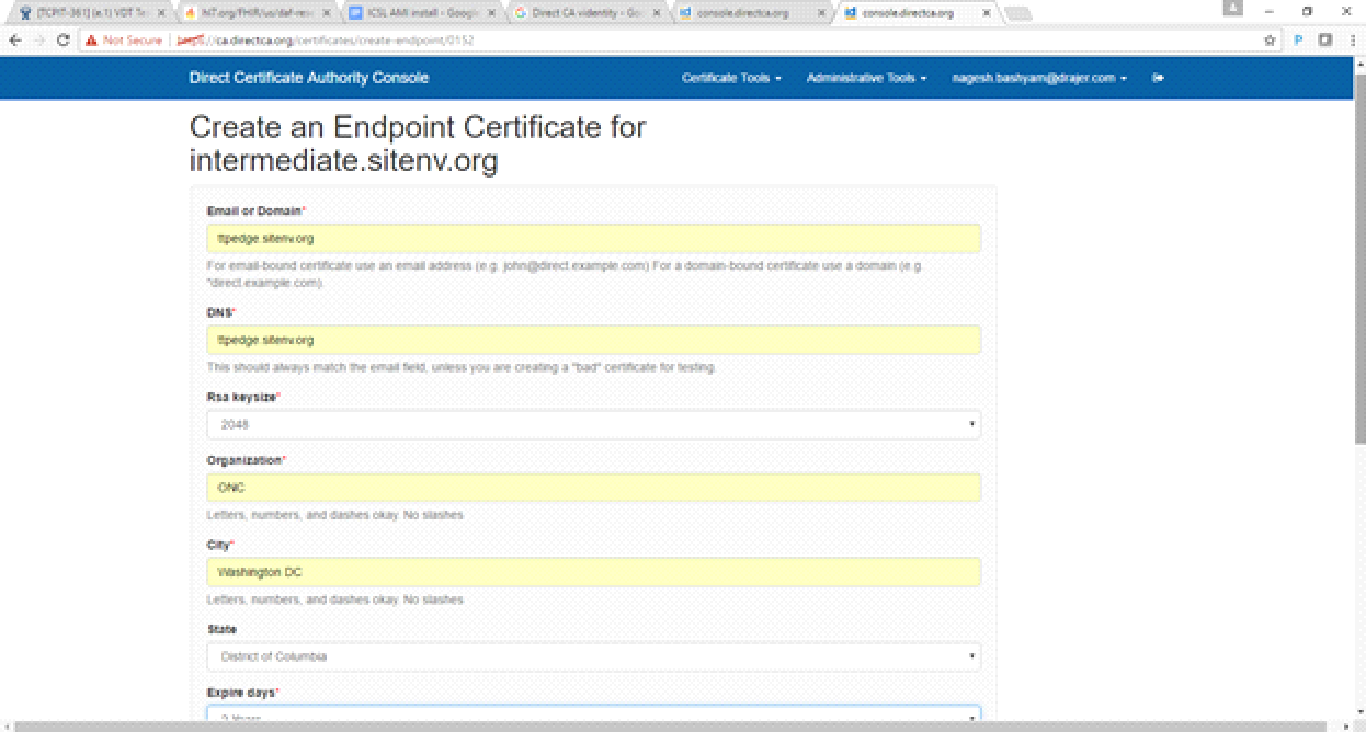
3. Once you have done the top level trust anchor, then click on **Create Intermediate Anchor** and enter the details and create the intermediate as shown.



After successful creation you should see the screen below (using sitenv.org as an example.)



4. Next click on your <intermediate.domain.name>, Select **Create an EndPoint Certificate** as shown below

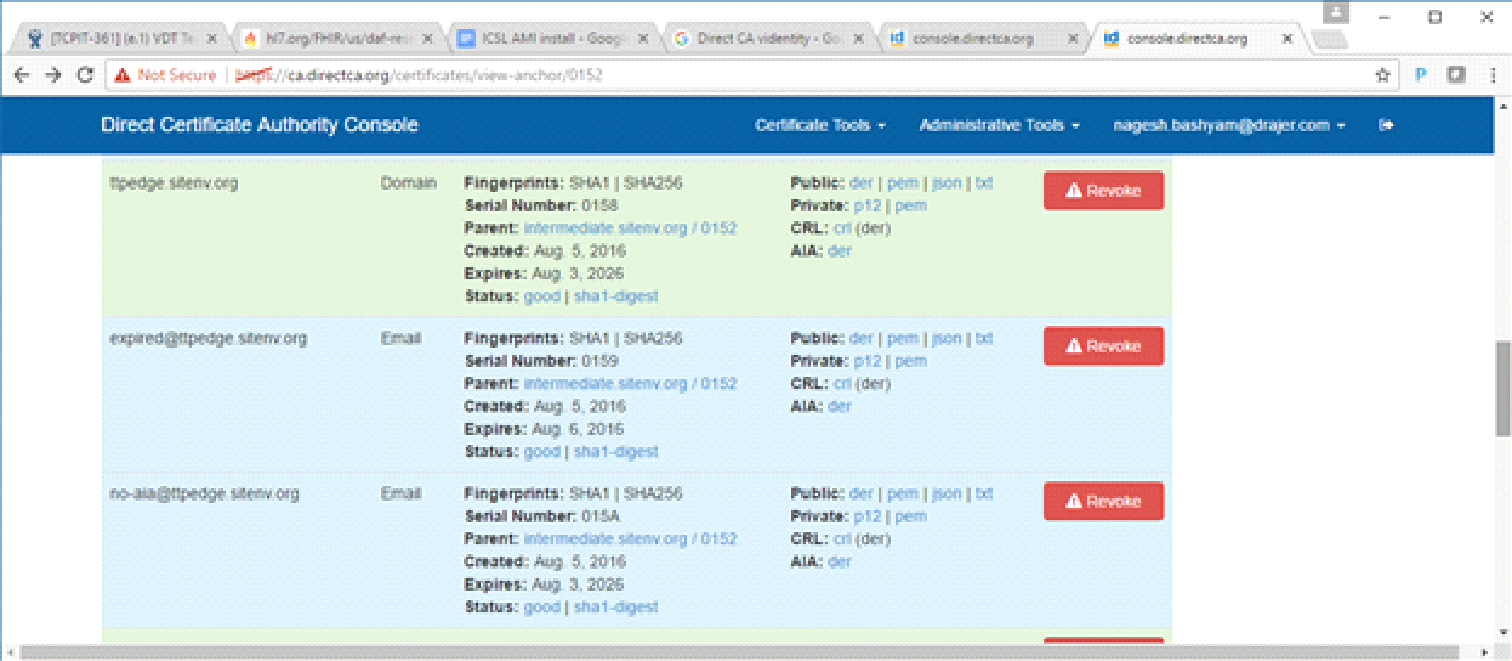


5. Create another **Endpoint Certificate** and this time creates it for an email address, this is for an expired certificate test. For example, "expired@ttpedge.sitenv.org"

Select the expiration date to be the **1 day** after the creation date, so it will expire within a day.

6. Create another endpoint certificate and this time create it for an email address, but **do not include the AIA** (Unclick the checkbox for AIA). For example, "no-aia@ttpedge.sitenv.org"

Now you should have **3 certificates** as shown below which would be visible when you click on the intermediate.sitenv.org



7. Create another **Endpoint Certificate** and this time for an email address. For example, " revoked@ttpedge.sitenv.org"

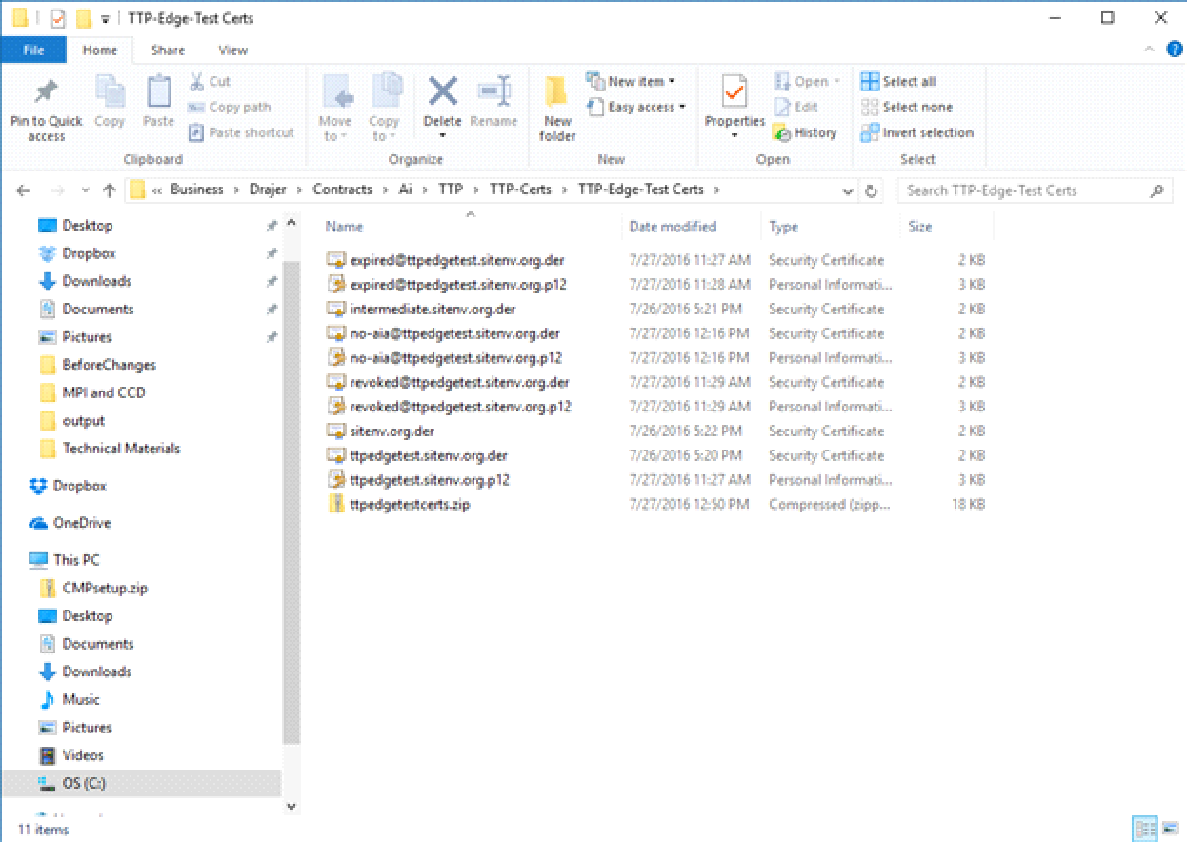
After the certificate is created, select the revoke button which is next to it and revoke it.

8. Go to **Administrative Tools** and click **Re-Generate Root CRL**

9. Download the certificates

* + DER file for the root domain (sitenv.org)
  + DER file for the Intermediate domain (intermediate.sitenv.org)
  + DER file and .p12 file for all the endpoint certificates.

For example, you should have the following once you download all certificates.



10. The above process has to be done for every domain. In ETT there are two domains for example:

* + ttpedge.sitenv.org (Edge Instance)
  + ttpds2.sitenv.org (Direct RI Instance)

So for each domain the above steps have to be followed.

Add these certificates to the Direct DNS server so that they can be published to the DNS for DIRECT to work.

**Note:** In addition to pointing DNS A records for the corresponding domain names to these servers; since, edgedomain and directdomain also run their own name servers (due to the fact that the certificates need to be published in the DNS for direct), you may have to add NS (glue) records for these two domains as well pointing to the corresponding ips.

**Configuring Edge Test Tool Instance**

ETT is packaged as a springboot jar application. All the parameters to the ETT UI can be configured in these three files (listed below) by replacing all the occurrences of the preconfigured "ttp" domain references to your domain settings (with a few exceptions.)

1) /opt/ttp/application.properties,

2) */opt/ttp/smtptestcases.json, and*

*3) /opt/ttp/direct\_certificates\_links.json*

To assist with that configuration, we've provided the three files with some placeholder configurations that will need to be revised. Replace the application.properties the smtptestcases.json and the *direct\_certificates\_links.json* provided in the AMI's with the files located in the installation-resources.

The application.properties is used by the application during the startup to reference the validator, toolkit, james, direct components. The json files are used by the user interface to display the endpoints.

**Direct certificate settings for your domain**

The /opt/certificates folder contains the certificates used by the ETT direct.

1. good/aia folders with appropriate certificates for your domain for the Direct Send component. Populate the good folder with the security cert (PKCS#12) for edgedomain. Use the same certs for the next step in creating the edgeserver domain which publishes the certs to DNS. If you want to update the downloadable URLs shown in the in the ETT Direct page, you have to update the /opt/ttp/direct\_certificates\_links.json correspondingly.

#### To validate the configuration, perform the following steps:

Test if the ETT starts up without errors (detecting any config, environment issues) and perform basic SMTP receive (Edge SUT) tests. Since the DNS steps may not have been completed, you may have to use the IP address in the browser to access the ETT.

1. Start the ETT. $ sudo service ttpservice start
2. Access the instance in your browser: <http://ip-address-of-the-edge-testing-tool-server/ttp>
3. Use valid SMTP account information (an example of an Edge SUT requires a gmail account) in the profile for SMTP Test 9, 16, 20.

In case of any issues, looking into the logs (/opt/ttp/logs/catalina.out) will reveal the issues (or the SUT logs).

Configure the Direct DNS using Appendix A.

Configuring the XDS Toolkit using Appendix B

**XDS toolkit Mutual-TLS**

These certificates are used by the mutual TLS for XDR testcases: /opt/certificates/xdr files: keystore, keystore.p12, key.pem, cert.pem.

**Optional: SSL configuration for HTTPS**

SSL can be enabled through apache and/or springboot combination. Update /opt/ttp/application.properties, /opt/certificates/private and/or /etc/apache2 conf files.

**Configuring ETT James Instance**

The ETT James instance is preconfigured with users and mailboxes for the ttpds.sitenv.org domain. You will have to create your corresponding domain and users using the provided script: addusers.sh. This script can be found at:

https://github.com/siteadmin/ett/blob/resources/installation-resources/james/addusers.sh

Populate the corresponding mailboxes using the contents located at:

https://github.com/siteadmin/ett/tree/resources/installation-resources/james/mailbox-testmessages

Configure an MX record with the name of the James domain, as in the following example:

ttpds.sitenv.org. IN MX 1 ttpds.sitenv.org.

#### Validate the James server configuration by using Thunderbird to send an email from one of the email accounts.

**Configuring ETT Direct Instance**

The Direct instance is used as a Sending HISP for SMTP message tracking test cases. The instance is configured with an address bound certificate to this domain ttpds2dev.sitenv.org. Configuring the instance involves adding your domain using the UI for the direct web application.

Note that you may need to use the IP address to access the application until all the name services are configured fully. The Direct web application can be accessed using: <http://directserver-ip:8081/config-ui>.

To accomplish this configuration, perform the following startup commands:

cd /opt/tomcat7/bin

sudo ./startup.sh

cd /opt/direct/DirectDNSServices/DirectDNSServer/bin

sudo ./DirectDNSServer start

cd /opt/direct/apache-james-3.0-beta4/bin

sudo ./james start

The instructions to create a domain and import your certificate are in Appendix A.

**Startup**

Edge server: Name services

cd /opt/tomcat7/bin

sudo ./startup.sh

cd /opt/direct/DirectDNSServices/DirectDNSServer/bin

sudo ./DirectDNSServer start

James server:

cd /opt/james/bin

sudo ./james start

This server also runs the ccda-validator:

cd /opt/tomcat7/bin

sudo ./startup.sh

Direct services:

cd /opt/tomcat7/bin

sudo ./startup.sh

cd /opt/direct/DirectDNSServices/DirectDNSServer/bin

sudo ./DirectDNSServer start

cd /opt/direct/apache-james-3.0-beta4/bin

sudo ./james start

**Validation of the Servers**

Direct Validation: Perform a send from ETT to the Direct server and return a message from Direct server using Thunderbird back to ETT.

Edge Protocol Validation: Send from ETT to the James server and return a message from the James server back to ETT.

C-CDA Validator: Run a few sample files through the Validator using the ETT UI.

XDR Validation: Send a message from ETT to SITE and from SITE back to ETT.

**Update to Current Builds**

Get and install the most recent builds from these locations (check the current ETT releases here:

<https://github.com/siteadmin/ett/releases>

<https://github.com/siteadmin/referenceccdavalidator/releases>

<https://github.com/usnistgov/iheos-toolkit2/releases>

**Maintenance notes**

1. Remove /opt/ttp/ccda\_objectives.txt to reflect the refresh github resources periodically.
2. Review these logs for troubleshooting the ett - /opt/ttp/logs/catalina.out @edgeserver

toolkit - /opt/tomcat7/logs/catalina.out @edgeserver

DNS issues for edgeserver - /opt/tomcat7/logs/catalina.out @edgeserver

james issues - /opt/james/logs @jamesserver

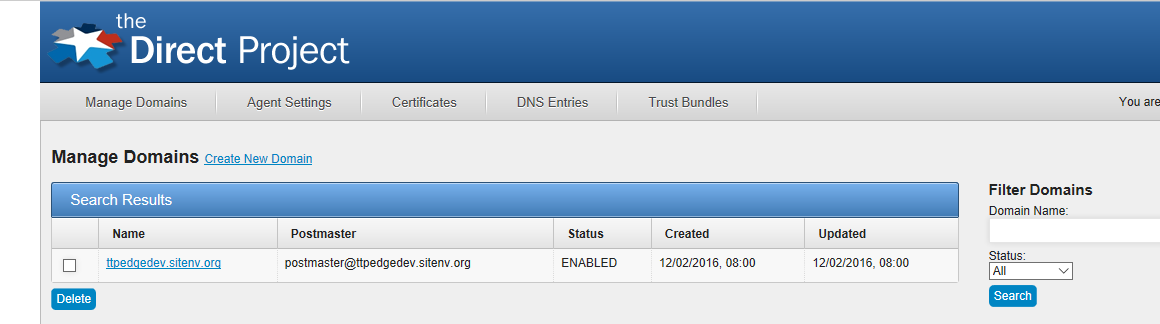
validator - /opt/tomcat7/logs/catalina.out @jamesserver

1. The toolkit may need periodic updates; more info can be found at <https://github.com/usnistgov/iheos-toolkit2>. Also the C-CDA validator updates are available at <https://github.com/siteadmin/referenceccdavalidator/releases> and the Technical Support <https://groups.google.com/d/forum/edge-test-tool> or [edge-testing-tool@googlegroups.com](mailto:edge-testing-tool@googlegroups.com)

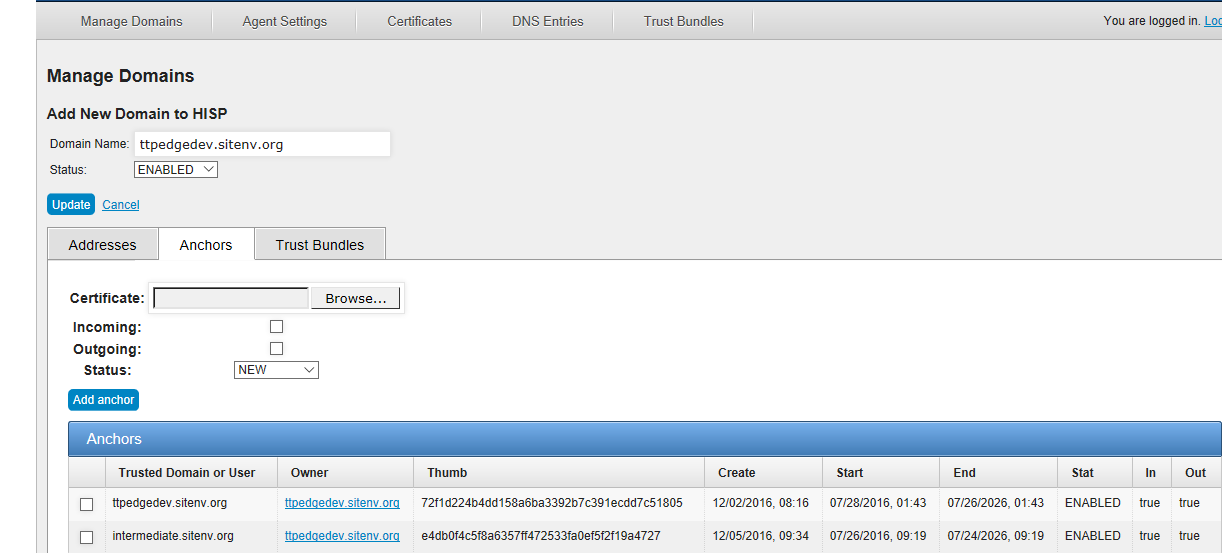
**Appendix A: Configuring Direct and Name Services**

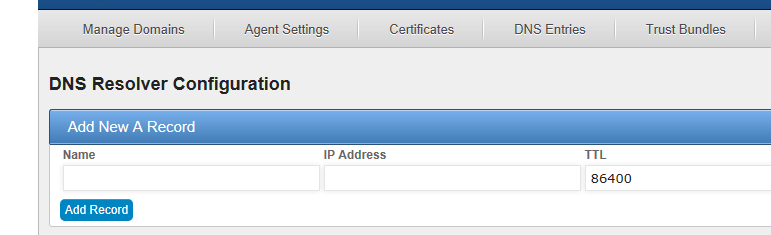
This document contains the necessary steps for setting up a complete direct server and hence will be used a reference for some of the steps below: <https://github.com/meaningfuluse/mu2/blob/master/transport/direct-hello-world.md>

* Since the AMI has already has been bundled with the Direct components using the above steps, only steps that need to be achieved are creating your own domain and configuring the DNS entries, Trust Anchors/bundles and Address bound/User certificates. These steps need to be performed once in the Edge Test Tool server and once in the Direct Server - in each server using its own unique domain name/certificate combination.
* You will have to use the IP-address (as explained above) due to the fact DNS settings are still being worked upon.
* Access the configuration in the browser: <http://ip-addressttpedgedev.sitenv.org:8081/config-ui/>
* Credentials: admin/adm1nD1r3ct.
* The Edge Testing Tool comes with a preconfigured direct domain: ttpedgedev.sitenv.org with all the relevant DNS/certificate/Trust Anchor settings. You will have to create “your own domain” using “Create Domain” and configure the DNS settings, upload the trust anchor and the certificates.



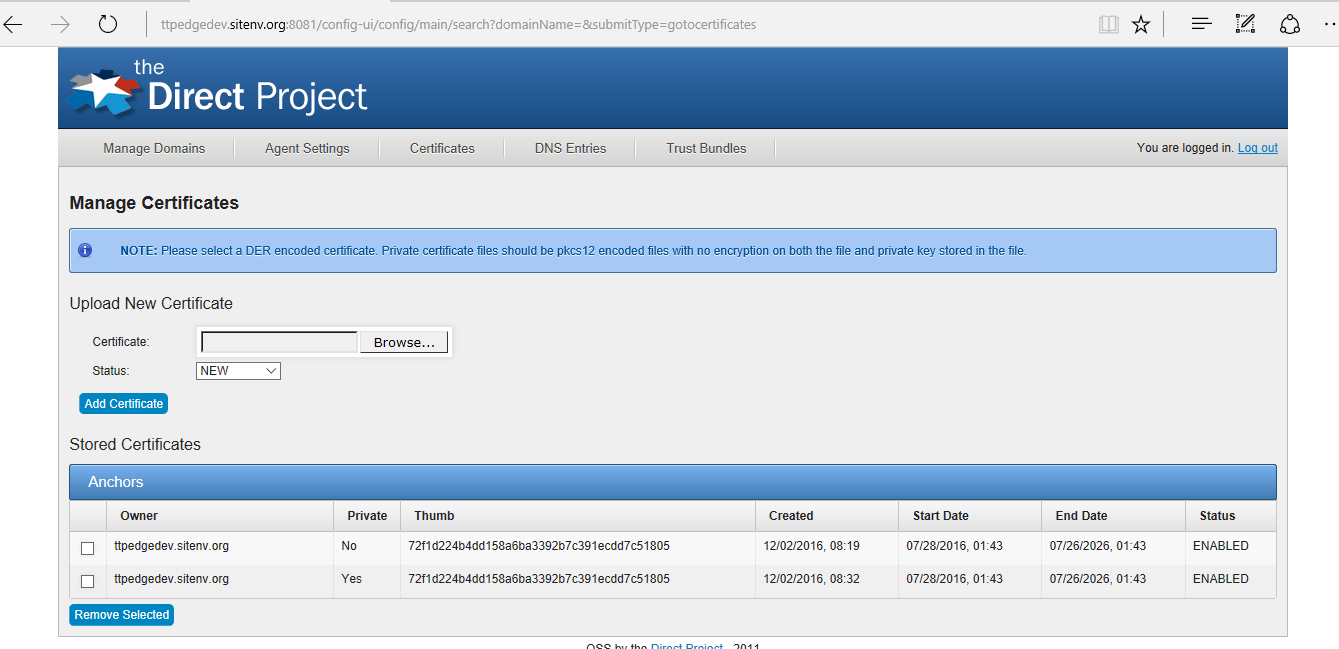
Upload your trust anchors to the created domain:





Using the above guide, add all the DNS records to your domain.

Finally add the address bound certificate and if necessary, user certificates in the “Certificates” screen:



* After you complete the above steps successfully, you should be able to view their certs by querying the DNS

$ dig directserver CERT

In addition, follow the instructions from the above guide to create a user called *hisp-testing@jamesdomain* in the directserver James - this is the account from which ETT communicates to the Receiving HISP test cases. If you are using address bound certificate for this domain, you may need to create a certificate and upload that as well to the DirectDNS using the above web interface.

**Appendix B: Configuring XDS toolkit**

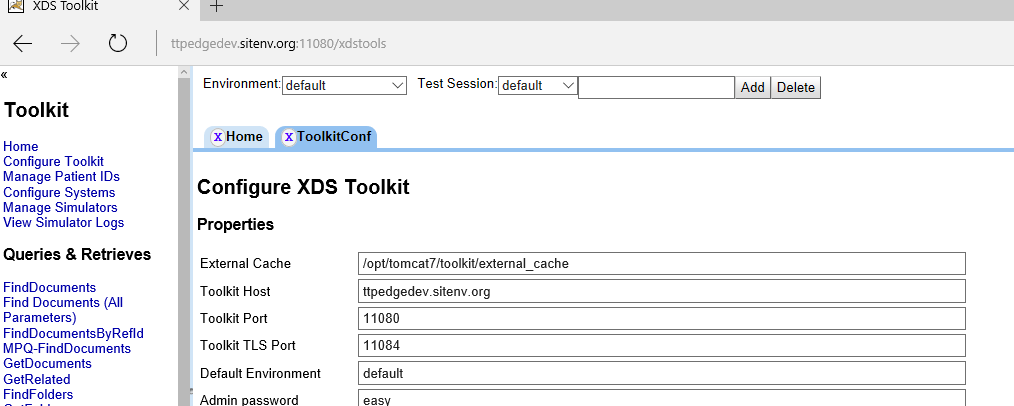
Prerequisite: The DNS configuration needs to have been completed on Edge Testing Tool instance.

1. Starting the XDS toolkit – the tomcat container needs to be started if it is not already running:

cd /opt/tomcat7/bin

sudo ./startup.sh

1. Access the configuration web application for XDS toolkit using a browser: <http://edgedomain:11080/xdstools/>
2. Select “Configure toolkit” (admin password: “easy”) and update the server name. Any changes to the environment/port (should not be necessary) needs to be updated here.



For troubleshooting startup or any other XDR issues, the tomcat7 logs (/opt/tomcat7/logs/catalina.out) should have the necessary information.