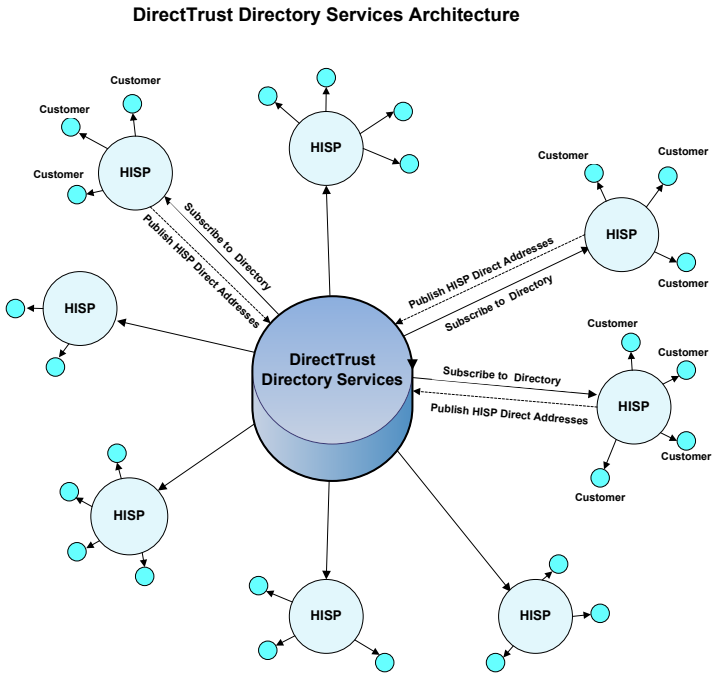
Directory Services Users Guide

Version: V2.5

Executive Summary

DirectTrust provides a Directory Service for HISPs that choose to participate in he service. Every DirectTrust HISP in good standing may elect to participate in the Directory Service provided that they agree to follow the requirements outlined in the Directory Data Services Agreement and the requirements defined in this User Guide. Each participating HISP may submit Direct Addresses and other related information that they have authoritative control over. In return for submitting their data, they may receive the aggregation of all of the other contributing HISPs' Directory data.

The architecture for the Directory Services application is a hub and spoke model where DirectTrust is the hub and is responsible for securely accepting and aggregating data contributed from each HISP that is represented as a spoke around the hub. The following diagram represents the system's technical architecture:



This document describes the process and procedures for HISPs to Contribute (upload) and Download DirectTrust Directory Services Data.

Overview of Version 2 Changes

The Directory Service Version 2 software has several new features. The V2 software is backwards compatible with the older V1 format CSV files.

File Version Number and Column Order

One of the important new features in V2 is that reliance of the order of the columns has been eliminated with the exception that the first column must always be the HISP ID.

The new V2 features are described in more detail below. The system will automatically detect the version of the file by examining the first column header. If the column header label = HISP ID then the file will be considered to be Version 1 and all of the Version 1 rules for column headings apply. In Version 1, the column heading positions were fixed and were order dependent.

If the first column heading is equal to the string "V2.0" then the file will be considered to be in Version 2 format. In Version 2, with the exception of the first column heading every other column is order independent and the names of the columns are fixed and are treated as named tags. In Version 2, the name of each column heading is significant and must be followed or an error will be generated.

Note: If the first column contains a version number that the software does not recognize the file version format and parsing behavior will default to Version 1 format.

To migrate to Version 2, the HISP simply uploads a CSV file in the new Version 2 format. The system will automatically remember the uploaded version number and output the CSV file according to the version number rules. If a HISP decides to revert back to Version 1 after upgrading to Version 2, they should upload a Version 1 format file and the system will automatically revert back to Version 1. To upgrade to Version 2, simply upload a Version 2 file.

Edit Checking

In Version 2, the edit checks for the values of each column is strictly enforced. If the format is incorrect or a mandatory field is not present then an error will be generated.

Note: This edit checking behavior is different than Version 1, where the edit checks were defined in the documentation but not strictly enforced by the edit checks for each column.

New Preview Feature

There is a new V2.0 "Preview" feature. The Preview feature allows HISPs to inspect the output of their uploaded CSV file after it has been parsed. The output of the parsing operation is a CSV file in the format that it will appear as in the aggregated

production file. The purpose of the Preview function is to allow developers to see how the data they submit in an upload will actually appear in the aggregated file.

Changed Org UID Behavior

In Version 1, the use of the column Org UID field was not universally understood and in some cases caused confusion.

The purpose of this field is to allow multiple Providers to be hierarchically listed under an Organization. The Org UID column had to be unique within each HISP's submission for each Organization being represented.

To allow for simpler implementations this field may be left blank in Version 2 and the system will automatically synthesize a value based on the HISP ID, the Organization Name and Geographic Address.

Note: if a HISP chooses to leave this field blank then it must be blank for every submission. If a HISP chooses to supply its own Org UID then it must do so for every organization.

Error Handling

In Version 1, there have been cases where HISPs have upgraded their Directory Service software and at times inadvertently caused an error to occur for each line of their CSV file submission.

This had the effect of removing the HISP's data from the aggregated file.

In Version 2, there is now a Max Errors value that is set system wide for every HISP. The current value is equal to 100.

If a HISP's CSV file encounters errors while it is being parsed during the upload and the error would cause the line not to be included in the aggregated CSV file, the error count is incremented. Once the error count exceeds Max Errors, the entire file is rejected and the previous upload is used instead.

All of the errors and other messages related to the upload and parsing of a HISP's CSV file can be found in the HISP's error report available from the interactive web page.

Data Schema Changes

There have been several changes to the Directory Service Data Schema. Please see the section in this document that defines the new schema.

DirectTrust Directory Data Security and Trust Model

The DirectTrust Directory Data Application (DDA) security is based on Mutual Authentication carried out by Transport Layer Security (TLS).

A HISP must perform certain steps before they can begin to contribute and download Directory Data.

A HISP must:

- Execute the DirectTrust Federated Services Agreement
- Be a member of DirectTrust
- Be included in the DirectTrust Accredited Anchor Trust Bundle
- Submit their organizations .PEM Certificate file and other enrollment information to the DDA System Administrator as part of the HISP DDA Enrollment Process

Note: A HISP must Contribute (upload) Directory Data to be able to Download Directory Data from other HISPs.

HISP DDA Enrollment Process

As part of the enrollment process, the HISP must provide DirectTrust with enrollment information. The following information is required:

- **Organization .PEM** Certificate File
- **HISP Name** – the full name of the HISP being added
- **Technical Contact Name** – this is the name of the person at the HISP that will be contacted for technical issues.
- **Contact Phone** – this is the phone number for the Contact Name.
- **Contact Email** – this is the email address for the Contact Name.

This information may be emailed to: admin@directtrust.org

After DirectTrust has completed the enrollment, your HISP will be assigned a HISP ID. The HISP ID is an identifier that must be included in every row of your directory submission data. **Note: The HISP ID** is case sensitive. The HISP ID will be all upper case and 10 characters or less. Please see the example CSV File named: Annotated V2 Example CSV File for the layout of the data elements being contributed and used for submitting data to the DDA system.

Enabling The HISP User's Browser

Before a User can access the DDA via a web browser, they must add their certificates to the Browser that they will use to connect to the Server.

At present, two Browsers are supported: Chrome and Firefox. Adding Certificates to each Browser varies according to the individual Browser's software. Please refer to your Browser's Help for instructions on adding your Certificates. The following Certificates are required to be added:

- *certificateName.*PEM file
- *certificateName.*PKS12 file

Note: It is possible to access the DDA's REST API via an automated processes, e.g., using cURL. The implementer should be well versed in how to use digital certificates with their chosen API client. See this document section titled "Contributing (Uploading) Directory Data via RESTful API" for additional details.

Organization Certificate File

Note: The Organization Certificate should NOT be the one submitted by the HISP for inclusion in the DirectTrust Anchor Trust Bundle. For security reasons, a separate self-signed certificate should be created by the HISP for accessing the Directory Services Application.

The HISP has to provide the DDA Administrator with an organizational certificate that meets the requirements of the Certificate Profile described below.

In addition, the HISP must also supply any intermediate and root certificates to establish the chain of trust for the organizational certificate. This includes the organization's root CA certificate if provided by an external Certificate Authority"

Certificate Profile

The Certificate for the mutual TLS Security should have the following profile:

Cryptographic properties
Signature Algorithm: sha256WithRSAEncryption
Key length: 2048 bits

Maximum interval for a self signed CA Certificate:

5 Years

Other Certificate constraints:

For a self signed CA certificate:

X509v3 Basic Constraint: CA = true
X509v3 Key Usage(s): Certificate Sign

For a TLS client certificate:

X509v3 Key Usage(s): Digital Signature, Key Agreement

Optionally, specify "TLS Web Client Authentication" as an additional extended key usage

Creating Directory Service Certificate Pairs

The Directory Service uses mutual TLS for authentication. In addition, as part of the on-boarding process, the Directory Service Administrator uses an Administrative Tool to add the participating HISP which includes adding the Client Certificate. The on-boarding Administrative Tool adds the thumbprint of the Client Certificate to the Directory Services Database. The thumbprint stored in the database is compared with the Client Certificate being used to authenticate to the Directory Service.

If the thumbprints don't match access is denied.

This following is a sample script that can be used to create the Certificate Pair (CA and Client) that is required for a participating HISP to be added to the Directory Service.

Direct Trust will need the ca.crt and the client.crt files and no other files. The client.crt and and client.key files are used to connect to the Directory service. The client.p12 file may loaded into a browser to access the Directory website and perform testing.

Note: the Client Certificate must be supplied to DirectTrust as a .PEM file.

Sample openssl Script:

```
openssl genrsa -aes256 -out ca.key -passout pass:PASSWORD 4096

openssl req -new -x509 -days 3650 -key ca.key -out ca.crt -subj
"/CN=HISPName CA" -passin pass:PASSWORD -passout pass:PASSWORD

openssl genrsa -aes256 -out client.key -passout pass:PASSWORD 4096

openssl req -new -key client.key -out client.csr -subj "/CN=HISPName Client"
-passin pass:PASSWORD

openssl x509 -req -days 1825 -in client.csr -CA ca.crt -CAkey ca.key -
set_serial 01 -out client.crt -passin pass:PASSWORD

openssl pkcs12 -export -clcerts -in client.crt -inkey client.key -out
client.p12 -passin pass:PASSWORD -passout pass:PASSWORD
```

HISP On Boarding Process

Each HISP will work with the DDA Administrator to be on boarded (enrolled) within the service. During the enrollment part of the process the HISP will have provided the

DDA Administrator with the HISP's information and received a HISP ID at the completion of the enrollment process in return.

When a HISP is first enrolled, it is set up in the Directory Service Test System (directory-test.directtrust.org) in Active mode for testing purposes.

Note: Any HISP that was already on-boarded in the Version 1 of the Directory Service has automatically been on boarded in the new Directory Service Test System. Your existing TLS authentication credentials have been ported to the new Test System and can be used to access it.

During the testing process, the HISP will be able to upload their CSV files for testing and analysis. As the CSV file is uploaded, the system will parse it and report any errors that it encounters.

The results of the parsing operation are available to the HISP in a log file for each CSV file upload it performs.

The testing process may consist of multiple iterations of CSV file upload and parsing report review to eliminate errors.

After the HISP has completed its testing it will notify the DDA Administrator via email that it has completed its testing process. If a HISP has already been on boarded using Version 1 then the next step is to use the Production URL for publishing their Version 2 CSV File into production.

If a HISP on boards for the first time into the Test System post Version 1 then the DDA Administrator will add their security credentials and other information to the Production System and let the HISP know that they may upload to the Production System using the Production System URL directory.directtrust.org.

Once a HISP uploads their CSV Files to the Production System their data will be aggregated and incorporated into the production DirectTrust Directory Data database.

The HISP may download the aggregated Directory from all of the HISPs that are participating in the Directory Data Sharing Service.

Note: It is expected that any HISP that on boards for the first time after the release of the Test System will only use the Version 2 Format or later formats as they become available.

HISP Directory Data Publishing

A HISP may publish their Directory Data using one of the following procedures:

- Upload a CSV File via a Web Page
- Use a RESTful API to submit a CSV File

When publishing Directory Data, there are data elements that are required and other elements that are optional.

CSV File Notes

Please note: Due to the size of the aggregated data file, in Version 2, the raw CSV file format is no longer supported as an output file format for downloading.

The uploaded CSV files may have one of two forms:

1.) gzip: a CSV file compressed using GNU gzip or equivalent.

2.) zip: the CSV file may be compressed into a traditional PKZIP archive: the file name of the data must be DATA.csv in the "root" of the archive (no sub-folder.)

Due to the text content and inherently high redundancy found in these CSV files compression algorithms tend to be very effective and will greatly reduce the file size.


DirectTrust
The most trusted names
in healthcare exchange.

DirectTrust Directory Version 2 Data Elements

The Version 2 Directory Data Elements are defined below.

Note: This table below describes the OUPUT FILE format. As a reminder, in Version 2 the column order of the INPUT CSV FILE is no longer dependent on any particular order except that the first column must always be the HISP ID.

Field Name	Field Description	Required	Column (v1)	Column (v2)
HISP	This identifier is assigned to the HISP during the onboarding process. It must be present in every row of data submitted. Assigned by Directory Aggregator operator. (See Note 5 below.)	**R**	A	A
SERV_DIRECT_ADDR	The Direct Address	**R**	B	B
SERV_DESC	URL pointer to additional information (e.g., pointer to web page or FHIR resource)	**O**	C	C
Describing Individuals				
PROV_UID	Internal HISP supplied Provider identifier. This is meant for HISP use. (When combined with HISP ID, forms a globally unique record identifier.)	**R**	D	D
PROV_NPI	Provider NPI Number (Type 1 only)	**R2**	E	E
PROV_FIRST_NAME	Provider First Name See, Note 1 below	**R**	F	F
PROV_MID_NAME	Provider Middle Name or Initial	**O**	G	G
PROV_LAST_NAME	Provider Last Name, See Note 1 below	**R**	H	H
PROV_SUFFIX	Provider Suffix (e.g., Jr, Sr, III)	**O**	I	I
PROV_HCSC		**O**	J	
PROV_SPEC_CODE	NUCC Code: required when NPIN is present, otherwise optional. (See Note 2 for NUCC URL.)	**R2**		J
PROV_SPEC_TEXT	(Free-form text describing provider's healthcare specialty)	**R2**	K	K
PROV_ROLE	(not described in User Guide)	**O**	L	
PROV_FAX	Provider FAX number (to be used for searching only)	**O**		L or Y
Describing Organizations				
ORG_UID	Internal HISP supplied identifier. This is meant for HISP use. See section title "ORG_UID Column" in this document for a discussion of automatic population by the DDA.	**R**	M	M
ORG_NPI	Organization NPI Number (Type 2 only)	**R2**	N	N

ORG_NAME	Name of the Organization	**R**	O	O
ORG_GEO_ADDR_TYPE	Primary service offered at the geographic address. Enumerated values: Billing; Mailing; Practice; Test?	**R**	P	P
ORG_ADDR_1	Address Line 1 (Patient service address if type is “Practice”)	**R**	Q	Q
ORG_ADDR_2	Address Line 2	**R2**	R	R
ORG_CITY	City	**R**	S	S
ORG_STATE	State	**R**	T	T
ORG_ZIP	Zip Code (Postal Code)	**R**	U	U
ORG_PHONE	Phone number	**O**	V	V
ORG_HCSC	(no described in User's Guide)	**O**	W	
ORG_SPEC_CODE	NUCC Code: required when NPIN is present, otherwise optional. (See Note 2 for NUCC URL.)	**R2**		W
ORG_SPEC_TEXT	(Free-form text)	**R2**	X	X
ORG_FAX	Organization FAX number (to be used for searching only)	**O**		Y
PUBLISHABILITY	1=publish to providers only; 2=publish to patients only; 3=publish to both providers and patients (default value is 1)	**R**		Z

Note 1:
For role-based or department addresses, the first name shall be the department or role and the last name the organizational name (e.g. firstName="Radiology" lastName="Mercy Hospital")

Note 2:
For Specialty Code, please refer to:
http://www.nucc.org/index.php?option=com_wrapper&view=wrapper&Itemid=126

Note 3:
All data must be represented in UTF-8 Format. No other characters are supported. Any data not in this format is automatically rejected and increases the submission’s error count.

Note 4:
For additional information, please consult the User's Guide at:
https://www.directtrust.org/wp-content/uploads/2015/12/Directory-Services-Users-Guide-August-20-2015.pdf

Note 5:
Version number of the submission will be set in Cell A1. For v1 the cell says "Hisp ID" Otherwise the version number will be present.

Required Column Values

R = Required: a value SHALL be supplied
R2 = Required if Known: a value SHALL be supplied unless the submitting HISP does not have/know the value
O = Optional

Column Heading Names

In the Table above containing the V2 Data Schema, the first column "Field Name" contains the specific label for the column.

In Version 2, this label is used as a Tag to reference the column as the order of each Tag is not important. The first column must always be the HISP ID and the column name is used to determine the version that the HISP wishes to operate under. If the first column name is "HISP ID" then the file is assumed to be in Version 1 format. If the first column name is "V2.0" then the file is assumed to be in Version 2 format. If the first column name is not recognized, the system will default to and use the Version 1 format.

ORG_UID Column

This column is used to allow multiple Providers to be nested under a single organization. When the Parser reads the CSV file, it will read and associate the first occurrence of a unique ORG_UID with an organizations demographic information e.g. organization name, address etc. Thereafter when the file is being parsed every time the Parser encounters a previously processed ORG_UID it will use the demographic information associated with it.

The ORG_UID must be unique within the CSV file for a particular HISP.

This mechanism has not been well understood and in Version 2 another method exists for using this column. In Version 2, a HISP may leave this column blank and the system will synthesize an ORG_UID from concatenating HISP + ORG_NAME + ORG_ADDR_1. The strings are concatenated, spaces are removed and the string is changed to all uppercase before computing a hash value to be used as the ORG_UID.

In Version 2, a HISP may now leave this field blank or may populate it, but it may not do both; i.e. supply a value for one ORG_UID and leave another row ORG_UID value blank. In other words, the ORG_UID value for *all* rows must be blank to activate auto-computation and auto-population by the DDA.

Directory Data Element Relationships

The CSV File supports a relationship between Providers and Organizations. A Provider can belong to one or more Organizations by having a membership.

For example, a Provider: Dr. Smith may have a relationship (member of) three organizations: City Hospital, County Hospital and Drs Practice. Dr. Smith has a separate Direct Address associated with each of the Organizations that has been issued from a single HISP.

The following diagram illustrates the relationship between Providers and Organizations.

Provider Organization Relationship

Establishing an Organization Entry in the CSV File

To establish an organization entry during processing of CSV records two things must be present; a unique Org UID and an Org Name. Once the organization entry is established the Org UID may appear in subsequent records without the Org Name.

What happens if an Org UID is provided without the Org Name?

If an Org UID without an Org Name appears among the records prior to having been established by a previous record, the system will report "Organization name attribute required for Org UID X; Organization Entry not created" where "X" will report the Org UID that was not created.

In practice the best policy is to simply provide both the Org UID and Org Name for every record that contains either; the ability to omit the Org Name on subsequent records doesn't convey any real value.

The Org Name need not be unique; the same Org Name may be assigned to different Org UID values.

Example Annotated CSV File

Please see the companion Annotated V2 Example CSV File spreadsheet that provides different illustrations on how to create rows in the upload CSV file. For example: the Annotated V2 Example CSV File contains many examples for adding data such as

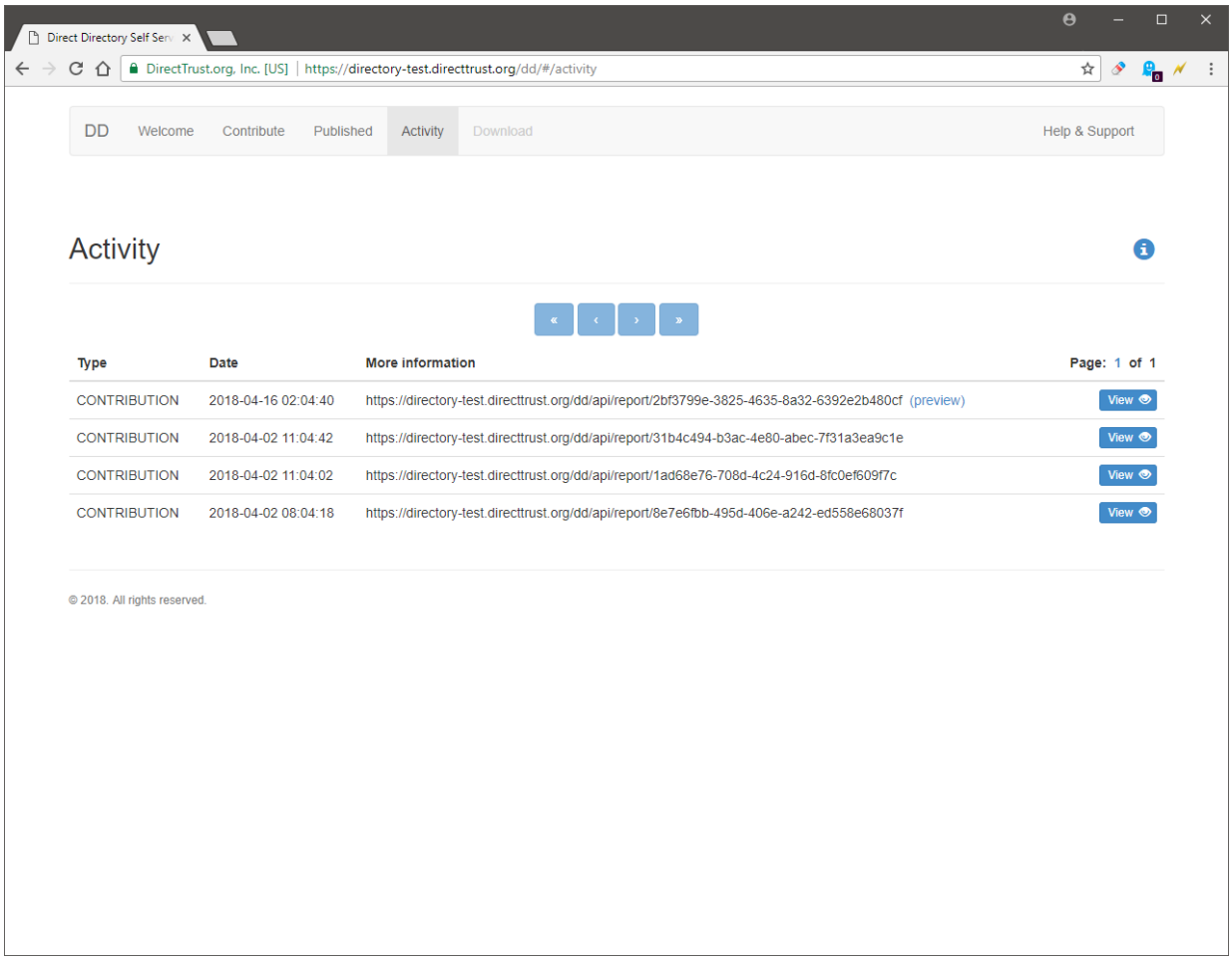
Providers that practice at multiple practice locations or an Organization with multiple addresses.

CSV Output File Preview Function

In Version 2, a new feature called "Preview" is available for developers to inspect the actual results of the Directory Service parsing and aggregation functions on the CSV files that they upload.

The V2 software now writes out the contents of the uploaded CSV file in the format as it will appear in the aggregated file. The developer may select the Preview function to download and review the contents of the file after it has been processed.

The following illustrates the new function:



The developer may select the file they have uploaded (referred to here as a "contribution") by clicking on the View button.

Error Definitions

The Version 2 software now enforces the rules in the data schema and a specific list of errors is defined and used by the Parser to write errors into the Parsing Log file report.

The following is a list of errors and what they mean:

UTF8_ERROR Encoding error: invalid UTF-8 character(s); line skipped

BAD_RECORDCSV Record not understood; skipping

MISSING_EMAIL The SERV_DIRECT_ADDR value missing; service entry not created

BAD_EMAIL Invalid SERV_DIRECT_ADDR value; service entry not created

MISSING_PROV_UID Provider UID missing; provider entry not created

MISSING_LAST_NAME Provider last name missing; provider entry not created

MISSING_ORG_UID Organization UID missing; organization not created. This can occur when the submitter populates at least one ORG_UID value, but fails to populate all ORG_UID values.

MISSING_ORG_NAME Organization name missing; organization not created

BAD_PUBLISHABILITY Publishability flag missing

MISSING_FIRST_NAME Provider first name missing; provider entry not created

MISSING_GEO_ADDR_TYPE Organization Geo Address Type missing; organization not created

BAD_GEO_ADDR_TYPE Organization Geo Address Type invalid; organization not created

MISSING_ADDRESS Organization address missing; organization not created

MISSING_CITY Organization city missing; organization not created

MISSING_STATE Organization state missing; organization not created

MISSING_ZIP Organization postal code missing; organization not created

V2_ORG_UID_POLICY_VIOLATION Organization UID policy violation; all input rejected

MAX_ERRORS Error exceeded threshold; all input rejected

Note: MAX_ERRORS occurs when the threshold for the maximum number of errors encountered by the Parser is exceeded. This value is set system wide and is used for

each HISP's submission. It is currently set to 100. If this error occurs the submitted file is ignored and the last previous good file is used instead.

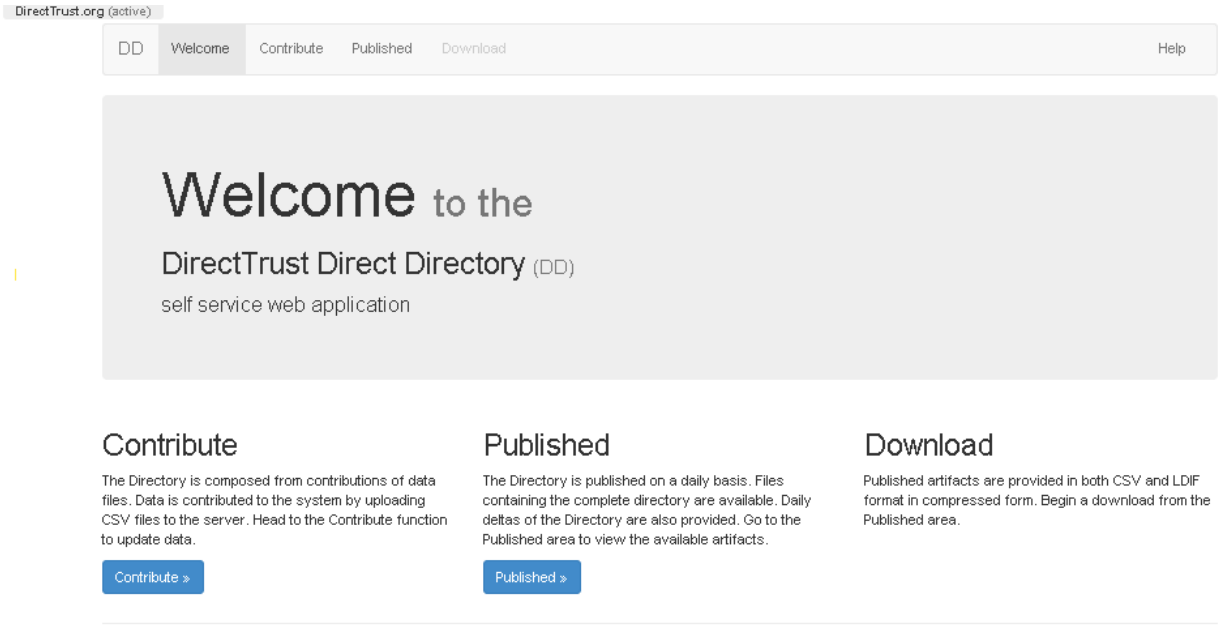
Publishing Directory Data via A Web Page

A HISP may interactively Publish (upload) their Directory Data via the following Web Page URL:

https://directory.directtrust.org

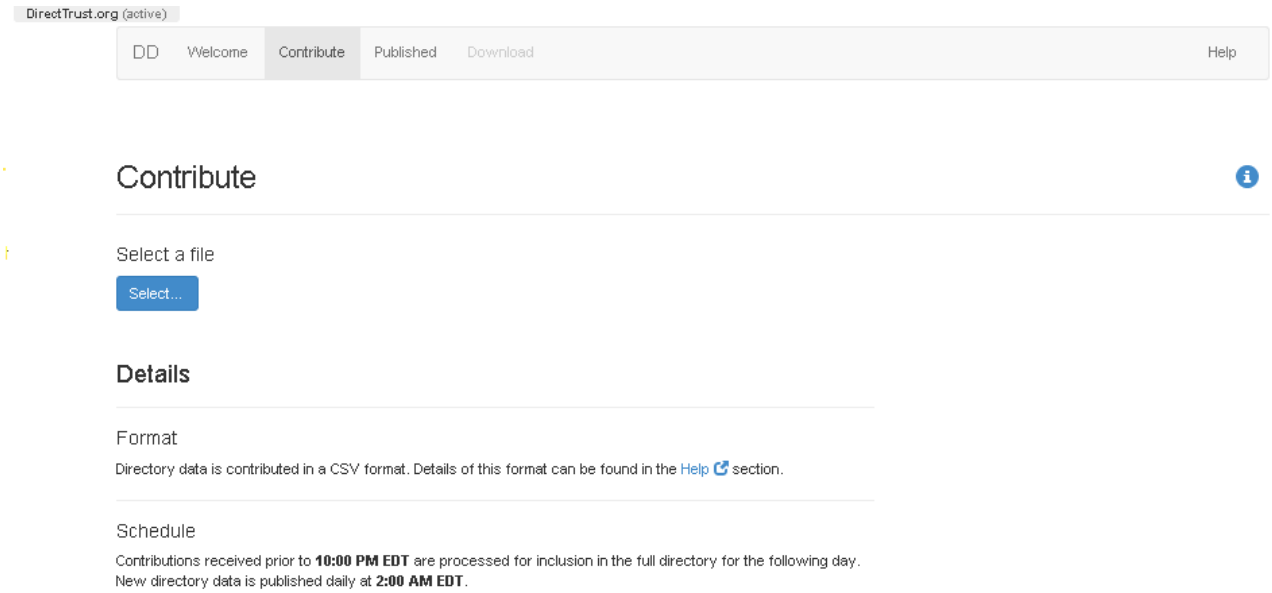
Your Browser may prompt you to select a Certificate to use to Authenticate to the Server; select the appropriate Certificate.

You will then be presented with the following Web Page:

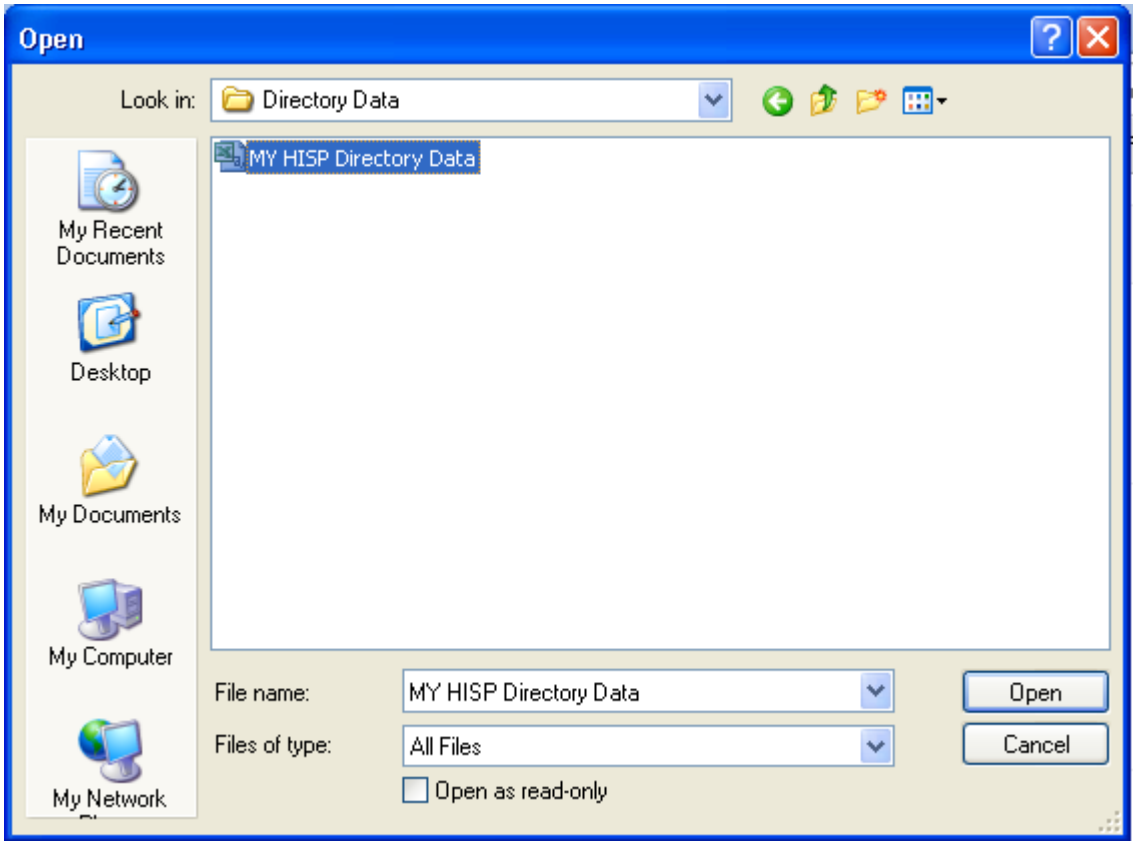


To Contribute (upload) your Directory Data, Click on the Contribute button.

You will then be presented with the Contribute Web Page:

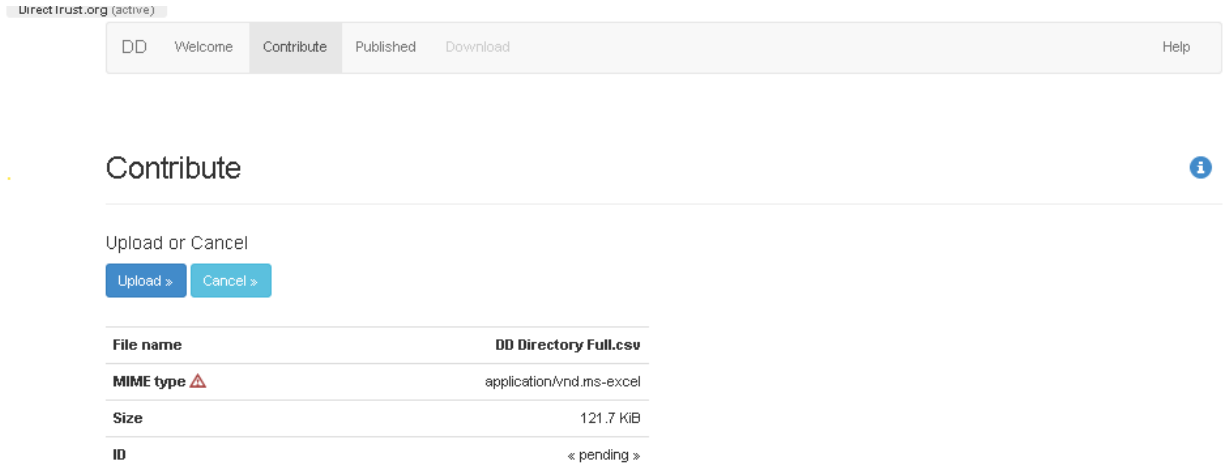


Next, click on the Select button to browse for the file to upload.



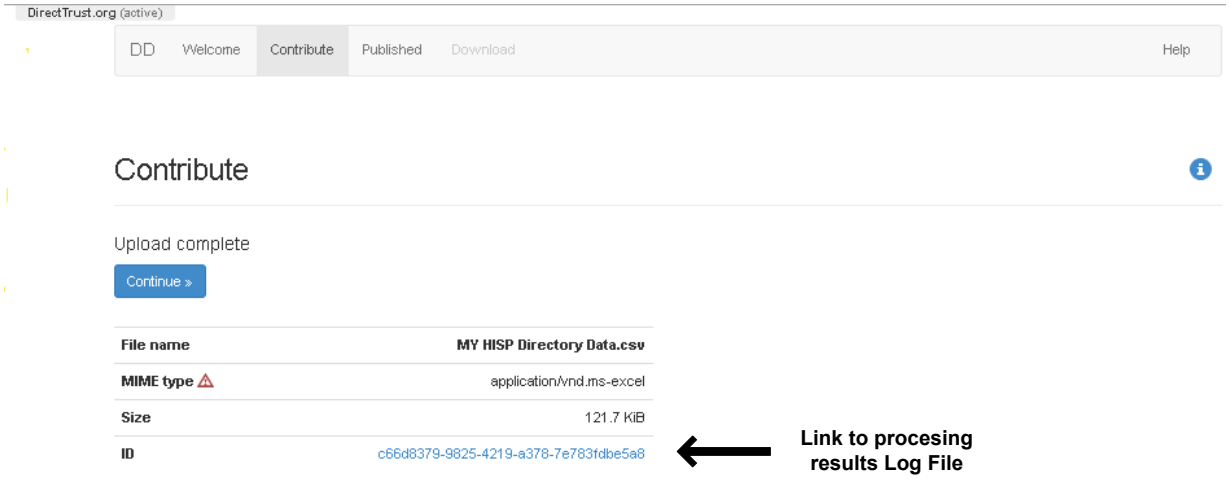
Select the file for upload and click Open. Note: this is a Windows Dialog Box, other operating systems i.e. Linux will appear differently.

Next you will be prompted to confirm the upload of the file in the following Web Page:



Click on the Upload button to confirm the upload.

After the DDA system has processed the uploaded file, the following Web Page will be displayed:



Please note that the Web Page displays a message: "Upload complete", this verifies that the processing has been completed.

As the DDA system processes the uploaded file it creates a Log File of the Processing results. The Log File can be accessed by clicking on the Link that is labeled "ID" and has been annotated in the diagram above with an arrow pointing to it.

Note: the arrow and text are for documentation purposes only and do not appear in the actual Web Page.

Contributing (Uploading) Directory Data via RESTful API

HISPs that wish to automatically Contribute their Directory Data as CSV files may upload them the DDA Server via the POST method API. POST may be implemented in several ways, curl is used below to illustrate how POST would be used to upload the file:

To upload (Contribute) a CSV file:

```
curl --cert client.crt --key client.key --data-binary @data.csv
https://directory.directtrust.org/dd/api/contribute
```

After the uploaded (Contributed) CSV file has been processed, the HISP may access the processing log file using the GET method API. The following example uses curl to illustrate how to retrieve the report.

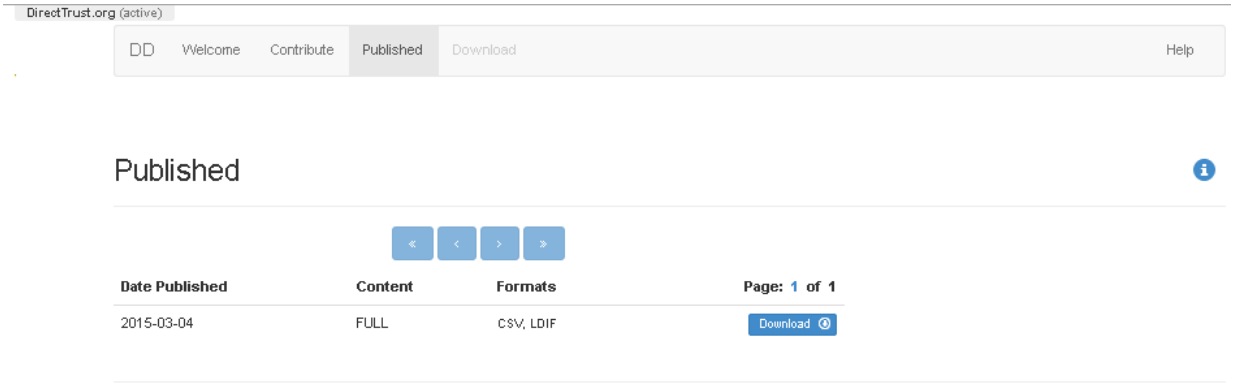
Retrieve a contribution report:

```
curl --cert client.crt --key
client.key https://directory.directtrust.org/dd/api/report/<contribution-id>
```

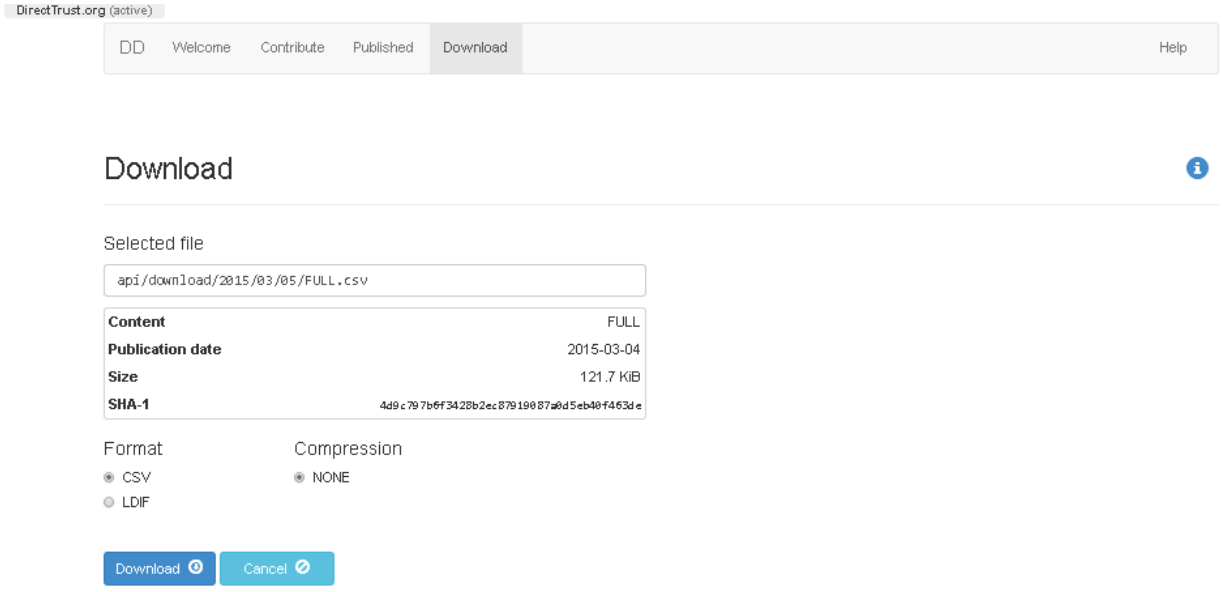
Subscribing To Directory Data via a Web Page

From the DDA main screen (see above) click on the Published button to download and download a complete copy of the DirectTrust Directory Data. This file contains all of the Direct Addresses that have been contributed by your HISP and all of the other member's addresses that are participating in the Directory Data service.

When you click on the Published button you will be presented with the following Web Page:



Next, click on the Download button. You will be presented with the following Web Page:



Click on the Download button to confirm the download.

Note: You may select a complete file or a file with Deltas, changes since the last full file was processed.

Downloading Directory Data via Restful API

HISPs that wish to automatically Download consolidated Directory Data as a CSV files may download them from the DDA Server via the GET method API. GET may be implemented in several ways, curl is used below to illustrate how POST would be used to upload the file:

curl --cert client.crt --key client.key https://directory.directtrust.org/dd/api/download/2015/03/05/FULL.csv.zip
Where:

Notes: The date components (2015/03/05 above) reflect the desired date. Please note: the Month (MM) and the Day (DD) must be right justified and zero padded. In the above example: March is 03 and the fifth day is 05

The file name syntax is one of the of following:

FULL.csv
FULL.csv.zip
FULL.csv.gz

The published API returns a JSON data structure that enumerates all of the published documents.

```
{
    "files": [
        {
            "path": "/2014/09/20/FULL.ldif.gz",
            "size": 15093021,
            "sha1": "a272e7acff61ddb7569671e751d97e3691691636",
            "date": "2014-09-20",
            "content": "FULL",
            "format": "LDIF",
            "compression": "GZIP"
        },
        ...
    ]
}
```

Retrieve a contribution report:

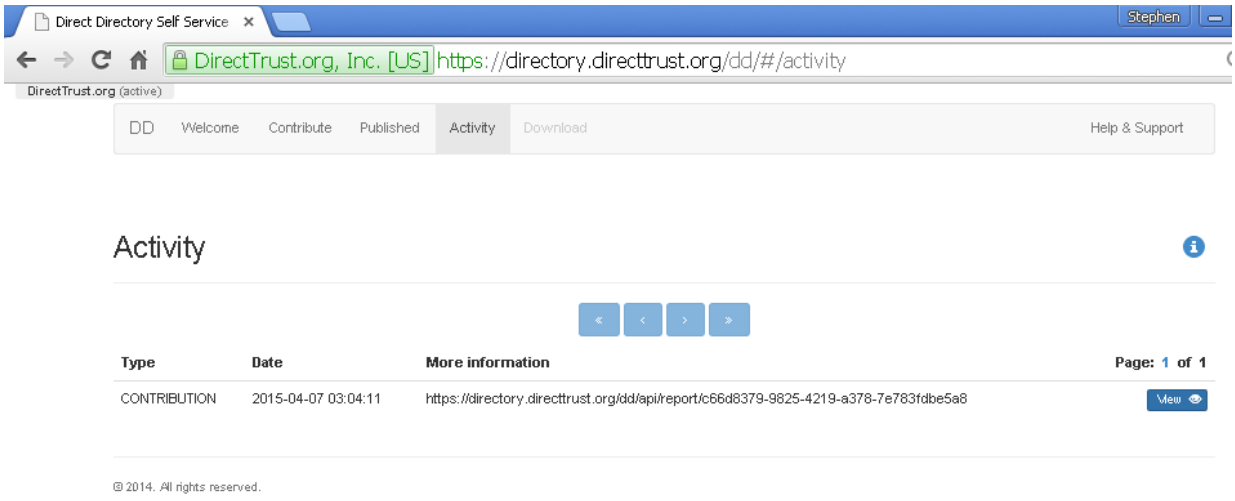
```
curl --cert client.crt --key
client.key https://directory.directtrust.org/dd/api/report/<contribution-id>
```

Viewing Activity

You may view the activities that your HISP has performed by clicking on the Activity option in the Menu Bar.

This function displays the activity logs from each operation that your HISP has performed.

A HISP may now see a Preview of how the data will appear in the aggregated file by selecting a file in the Activity Tab.



Appendix A Document Version Control

Note: This section is for internal use by DirectTrust only.

Document Version	Document Date	Version Notes
1.0	8/20/2015	Final V1 User Guide, SMW
2.0 Draft	4/16/2018	Draft V2.0 User Guide, SMW
2.1 Draft	4/21/2018	Draft V2.1 User Guide, JF, SMW changes
2.2 Draft	4/22/2018	Add Preview function documentation
2.3 V2 Final	7/25/2018	Version 2 Final Version
2.4	8/14/2018	Minor change re; zero padding in download requests and added example script for creating Certificate Pairs
2.5	10/15/2018	Minor update to specify Purpose of the Certificate is for TLS Client Authentication