# Purpose

This document briefly outlines the steps to install the latest build of the Sentinel Serialization services and client application.

# Scope

This build is the latest work of the development team. Serialization operations are complete. SQL Prelog and Serialization tables have been migrated into the FA database Custom schema. Initial work to handle Leads submitted via Prelog has been added to the table designs. The automatic Lead handling service is operational. The Serialization and Lead client application functions primarily as a status viewer.

Serialization services are provided as Windows Service-hosted WCF services. To facilitate testing with minimum installation, we have provided console hosts applications for all services. The Sentinel mock services are provided only in a console-hosted form.

Installation using the Windows installer is now supported as noted in the following section.

# Installation

The Serialization feature is installed from a single MSI installation file. Advanced options provide for selecting components for installation. This includes selection of the Serialization services, console hosts for testing, mock services and data, installation of SQL scripts, Serialization and administration client applications. The installer can install individual components or all components at once.

## Service Installation

If Serialization has previously been installed on the target server, stop the service and uninstall it using the Windows Control Panel > Programs and Features applet.

The single, installer file FAS.Sentinel.Serialization.Setup.msi contains all of the Serialization components. Perform the installation with administrator privilege.

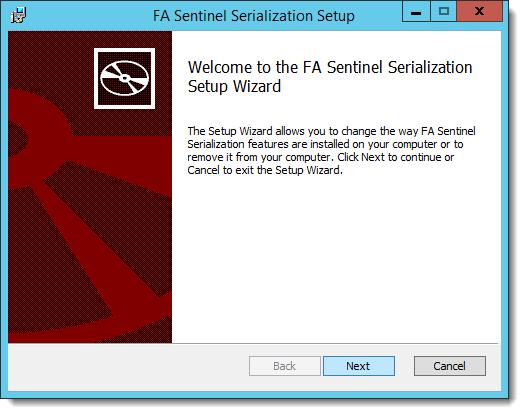


Figure 1 - Serialization Feature Installation

After extracting the installer, the setup requests that you acknowledge the TCSC license agreement.

After reading the agreement, check the box indicating your acceptance and click the Advanced button to permit changing the installation folder.

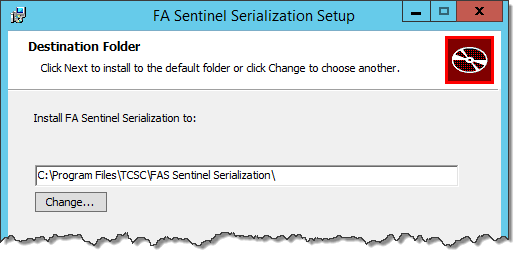


Figure 2 - Select Installation Location

The Serialization services run as 64-bit services. It is customary to install the service under the “Program Files” folder. Click Next to select the installation components.

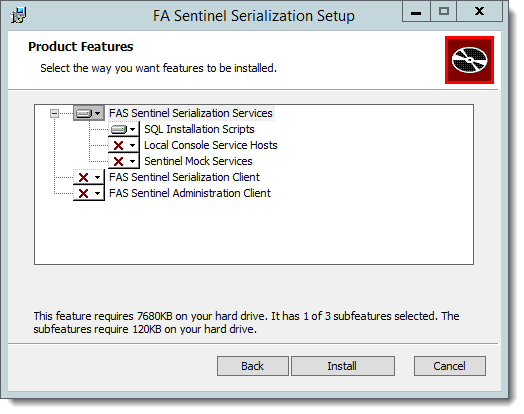


Figure 3 - Installation Feature Selection

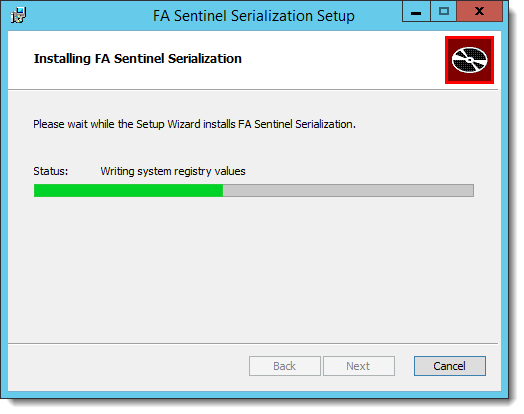


Figure 4 ‑ FAS Serialization Installation Progress

When the installation process completes, if problems occurred during the installation, preserve the Windows Installer log file to assist problem determination.

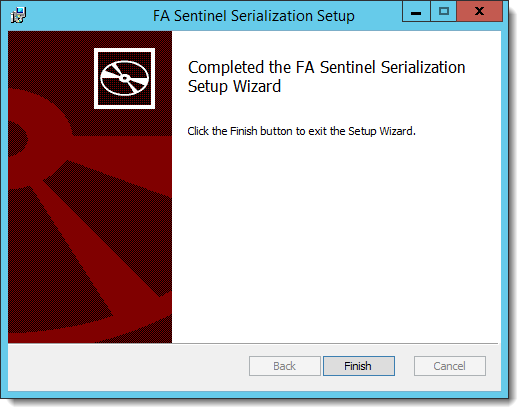


Figure 5 - FAS Serialization Installation Finalization

DO NOT START THE SERVICE until you have completed the remaining configuration steps.

Subsequent installations may add or remove selected components. Using the Windows Control Panel Programs and Features applet, the FAS Sentinel Serialization feature can be removed, repaired or individual components added or removed.

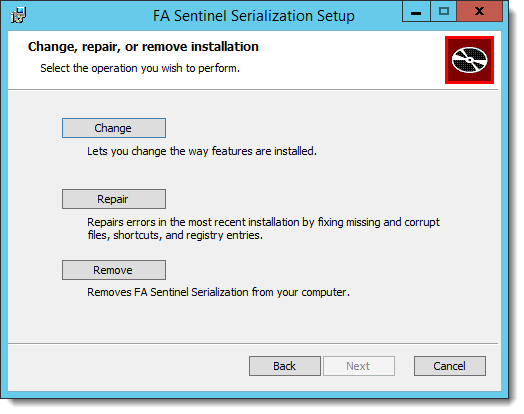


Figure 6 - Change, Repair or Remove Feature

## Installing Components

Serialization operates as a collection of Windows services under the Trusted Subsystem security model. It runs in the same security context as the other FAS application services.

The installation process requires carefully following these steps:

### Using local console hosts

1. Install FAS.Sentinel.Serialization.Setup.msi according to the Service Installation instructions below.
2. Modify the specified SQL installation scripts according to local infrastructure.
3. Use the SQLCMD utility to run the SQL installation script FAS.Sentinel.Serialization\_CommandScript.sql.
4. Configure each console host configuration file according to the local infrastructure.
5. Start each of the console service hosts.
6. Start the Sentinel Mock services console host.

### Using Windows service hosts

1. Install FAS.Sentinel.Serialization.Setup.msi according to the Service Installation instructions below.
2. Use the SQLCMD utility to run the SQL installation script FAS.Sentinel.Serialization\_CommandScript.sql.
3. Configure each service configuration file according to the local infrastructure.
4. Using the sc.exe utility, install and configure each service and configure its Log On and Startup type.
5. Start FAS Sentinel Configuration, Serialization Manager and Request Queue Services.
6. Start the Sentinel Mock services console host.

Failure to complete the above steps may lead to unpredictable and likely undesirable results.

The SQL script Sentinel\_CommandScript.sql is installed in the SQL\_Installation folder under the service folder (the default install location is %ProgramFiles%\TCSC\FAS Sentinel Serialization Services). This script invokes a number of SQL scripts to create tables in the ‘custom’ schema and adds several stored procedures in the target database.

The MSI installer installs the Serialization services but does not register them with the Windows Service Control Manager (SCM).

# SQL Database Provisioning

Installing stored procedures into the FA database requires that the user is logged in with administrator permission for the target database. During MSI installation, if you selected the “SQL Installation Scripts”, the installer copied the SQL installation scripts under the service installation folder (the default install location is %ProgramFiles%\TCSC\FAS Sentinel Serialization Services\SQL\_Installation).

## Modify SQL Installation Scripts

Modify the USE statement in Sentinel\_CommandScript.sql to specify the name of the FA Core database that is to support operation of the Serialization services.

Modify the SQL scripts Sentinel\_RepositoryObjectContentChunk\_Synonym.sql and Sentinel\_RepositoryObjectVersion\_Synonym.sql, replacing [yourORdatabase] with the name of the FA Object Repository database that is to support operation of the Serialization services.

## Provision FAS.Serialization Tables

After modifying the command script, change to the SQL\_Installation\Script\_Components folder and run the following command to add the Serialization tables to the FA Core database.

sqlcmd –E -S <Server> -i ..\Sentinel\_CommandScript.sql -m10 -r1

Sentinel\_CommandScript.sql is the name of the SQLCMD script that invokes other SQL scripts in the folder in which it is run. These scripts install views, synonyms and stored procedures into the Custom database schema.

When the SQLCMD utility runs, it displays its progress to the console.

**Note:** the installation script Sentinel\_CommandScript.sql is not a SQL query. It contains instructions for the SQLCMD utility to run individual SQL scripts in the SQL\_Installation\Script\_Components folder. The SQLCMD utility must be run in the folder containing the SQL scripts that were installed by the Serialization\_Setup process. These are idempotent scripts that and not remove existing data.

## Load Mock Data

To support testing of the client and services when actual data is not readily available, the installation process optionally provides mock data in the SQL\_Installation\Script\_Components\MockData folder. This script is not idempotent and simply adds a set of sample data in support of the Serialization services.

# Service Configuration

After Serialization software is installed, the service must be configured to the local infrastructure. For initial testing, the installer (optionally) provides console host applications to run the services without requiring that they be installed and enabled in the Windows Service Control Manager.

## Service Security

The FA Serialization services operate in compliance with the Trusted Subsystem security model. As such, they must run in the security context of the FA Services service account. If using the console hosts option, starting the console host in the administrator security context usually is sufficient.

Use the PowerShell script FASSentinelService-Install.ps1 from a PowerShell command prompt with Administrator rights. DO NOT START THE SERVICE until you have updated the application configuration files.

## Service Configuration Files

Ensure that each service configuration file contains settings compatible with the target environment. If using the console host option, configure the appropriate Console.exe.config file. If using the Windows service host option, configure the appropriate WindowsService.exe.config file.

|  |  |
| --- | --- |
| File name | Setting |
| FAS.Configuration.Console.exe.config | connectionStrings |
|  | TCSCLogging logPath |
| FAS.Sentinel.Serialization.Console.exe.config | connectionStrings |
|  | TCSCLogging logPath |
|  | LabReportPacketTypeId |
|  | ServiceSecurityAccountName |
| FAS.Sentinel.Serialization.RequestQueueConsole.exe.config | connectionStrings |
|  | TCSCLogging logPath |
|  | LabReportPacketTypeId |
|  | ServiceSecurityAccountName |
| FAS.Sentinel.Serialization.MockServices.Console.exe.config | TCSCLogging logPath |

Review the following settings and make the appropriate changes.

### TCSCLogging logPath

Serialization records its actions in a log file to assist with problem determination. The configuration file specifies the log file location, the amount and type of information recorded, and the maximum size of each log file segment. Serialization obtains configuration settings from the FAS.Serialization.Sentinel.WindowsService.exe.config file in the configuration/TCSCLogging element.

1. Specify the location of the log files as the value of the logPath attribute.
2. Set the log file name with the logName attribute
3. Control the type and volume of logging detail using the level attribute. The level set during installation is “Verbose”. This setting generates the greatest, most detailed amount of logged data. Upon completion of testing, the recommended operational level is “Error.”

By default, each service’s log file is configured to output to the C:\Logs folder.

### connectionStrings

The serialization services noted need to connect to the FA Core database. Inspect each configuration file and locate the configuration/connectionStrings element. Change the SERVER and DATABASE properties of the ConfigurationDbContext, and FaContext settings to correspond to the local installation. Your changes should match the following pattern:

<connectionStrings>  
 <add name="FaContext"  
 connectionString="Data Source=**<SERVER>**;Initial Catalog=**<DATABASE>**;Integrated Security=True"  
 providerName="System.Data.SqlClient" />  
 . . .  
</connectionStrings>

### General Application Settings

The following settings are found in the configuration/appSettings element and configure the FA edge of the Serialization service interface.

LabReportPacketTypeId value="<Guid>" This setting is the unique identifier of the lab report Packet Type. The following SQL script extracts the value from the FA Core database.

SELECT [Id]

,[Name]

,[Description]

FROM .[pkt].[PacketType] PT

WHERE PT.Name = 'Lab Report'

ServiceSecurityAccountName value="FBI UID" This setting is the default value to be used as the UsernameToken when a valid FBI UID is not provided in the Position Code field of the FA employee details.

## AutoDiscovery Configuration

Refer to the Sentinel Serialization AutoDiscovery Configuration document.

# Service Installation

Install the three (3) serialization services using the accompanying FASSentinelService-Install.ps1 PowerShell script. If one or more of the services have not been shut down or uninstalled, this script will attempt to shut down and remove the service before configuring the newly installed release. However, it is best if the existing release is uninstalled using the control panel applet before attempting to install a new release.

Open a PowerShell command window with Administrator rights. Figure 4 below shows entry of the installation script FASSentinelService-Install.ps1 in a PowerShell window with Administrator rights.

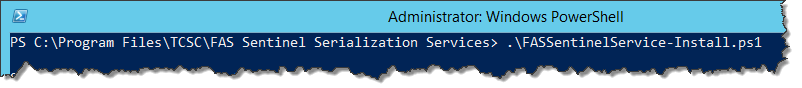


Figure 4 - Start Install Script

Upon starting, the installation script requests the service account name and password to be used with all of the Serialization services as illustrated in Figure 5 - Service Account Entry.

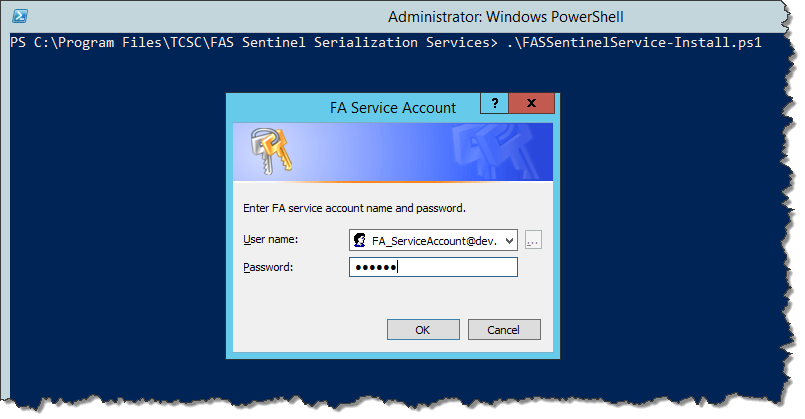


Figure 5 - Service Account Entry

The PowerShell script installs each of the services into Windows and records its progress.

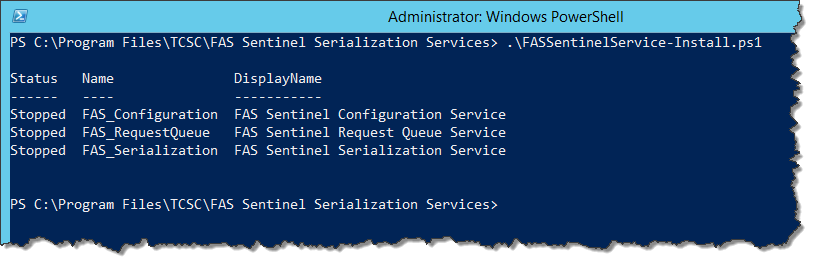


Figure 6 - Service Installation Completed

Note that each of the services is installed in the Stopped state. Update each of the service configuration files to correspond to local infrastructure requirements.

The Request Queue service must have the proper certificate installed for it to interoperate with the Mock Sentinel services. Test the Mock Sentinel services using a browser before starting the Request Queue service.

Use the Windows Services applet or the PowerShell Start-Service cmdlet to start each of the services.

## Sentinel Mock Service for Testing

The Sentinel Mock service is not configured to run as an installed Windows service. Rather, it is intended to run under the console host found in the Mock Services folder. To provide support for local testing, modify the configuration file for the local infrastructure before starting the mock service console host.

## Install the Sentinel Cross-Domain Certificate

The Sentinel cross-domain solution requires a WS-Security Username token to be supplied with each web service connection initiated by services running on the Quantico LabNet. Data Power and Sentinel services operate according to the SOAP v1.1, WS-SecurityPolicy v1.1 and Basic Security Profile v1.0. To authenticate initiation of the FA to Data Power service connection, communication must be encrypted using the Https scheme and contain a WS-Security UsernameToken element.

* Create (or purchase) an appropriate SSL certificate.
* Install the certificate on the system hosting the Sentinel (or Mock) services.
* Copy the certificate thumbprint and secure the port used by the client to communicate with the Sentinel services. Use the value ‘{b4996e50-9894-446a-888c-997cd532c37b}’ as the appid.

# Application Folder Structure

The FAS Sentinel Serialization Setup MSI creates a folder structure under the Program Files folder according to the selections made during installation. The installer places the files required to operate all services and their Windows and console hosts in the FAS Sentinel Serialization Services folder. Under this folder, the installer places the SQL\_Installation files and the Mock data source files.

Selecting the Serialization Client during installation places the files required to run the client in the FAS Sentinel Serialization folder. The installer also creates the registry entries required to install the controls and libraries used in the user interface. The Serialization Client may be tested on a machine other than the one running the services.

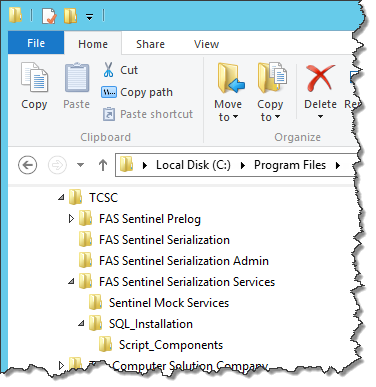


Figure 7 - Installed Folder Structure

# Ports in use

The four (4) serialization services are configured to listen on the following ports. These port assignments may be changed to meet local requirements.

| Scheme | Port | Service |
| --- | --- | --- |
| netTCP | 8755 | Configuration service |
| netTCP | 8001 | Sentinel.SerializationManagement service |
| https | 8733 | Sentinel.Mock Case service |
| https | 8733 | Sentinel.Mock Lead service |
| https | 8733 | Sentinel.Mock Serialize service |
| https | 8733 | Sentinel.Mock Search service |
| https | 8733 | Sentinel.Mock CreateFD1057 service |

The Request Queue service client endpoints must be configured to use the same addresses exposed by the Mock services. In addition, the Request Queue service and Mock services must be configured to use the SentinelWSSecurityBinding custom binding that supports the Data Power WS-Security UsernameToken authentication mode.

# Running the application

The FA – Sentinel Serialization services communicate among themselves and with the Sentinel Cross-Domain services as illustrated in Figure 8 - Serialization Service Communication.

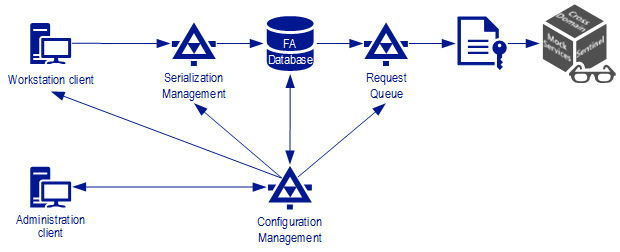


Figure 8 - Serialization Service Communication

Although the services are resilient to communication failures, it is best to start the services in order to minimize such failures.

Start the console hosts in the following order:

1. Mock Services
2. Configuration
3. Serialization
4. Request Queue

Following startup of the service command hosts you can start the Serialization client application.

During startup the Serialization client application requests the FA Employee entry for the currently logged in Windows user. If the FAS Serialization service cannot be accessed or the FA Employee entry cannot be accessed or if the Windows user name is not in the table, the Serialization client raises a message and shuts down.

If the Mock Services have not been installed with the proper SSL certificates the FAS.Sentinel.Serialization.RequestQueueService will start properly but fail when attempting to communicate with the Sentinel Mock service. Test the Sentinel Mock services using a normal browser before attempting to run the Request Queue service.

# Configuration Service

The Configuration Service provides methods that automate management of the service and client configurations. FBI requested elimination of configuration files for both the Serialization Client and Administration Client applications. This requires the capability for applications to store configuration information in the FA database to minimize content stored in the configuration file deployed with the application.

The Domain Name System (DNS) provides a name to address mapping technology that already is available within the client environment. While DNS generally is used to store predefined types of information (e.g. host addresses, mail servers, etc.) in resource records (RR) it also is possible to use this technology to store application configuration information.

This design provides a simple means to associate locally defined string information with attributes that are accommodated but not defined by the formal DNS naming process. It leverages DNS TXT resource records to store the relationship between a database context and a service offering. DNS SRV resource records provide the endpoint definition attributes required to access the required service. This design requires no change to the current DNS implementation and abides by the applicable IETF[[1]](#footnote-1) RFC[[2]](#footnote-2)s – [RFC1464](http://tools.ietf.org/html/rfc1464)[[3]](#footnote-3) and [RFC2782](http://tools.ietf.org/html/rfc2782)[[4]](#footnote-4).

The following sections identify how to configure DNS TXT records to point to one or more SRV resource records that define available WCF endpoints.

## TXT Record

The DNS TXT resource record provides the ability to associate arbitrary text with attributes not otherwise defined by the DNS. The TXT record has a structured format in its TXT-Data field that consists of an attribute name followed by the value of the attribute. The name and value are separated by an equal sign (=). Multiple name – value pairs may be quoted, separated by a space and enclosed within parentheses. The general syntax of the TXT resource record is:

<service> <class> <ttl> <RR Type> <TXT-Data>

### Service

The symbolic name of the desired service, as defined locally. The Service name is case insensitive.

### Class

Standard DNS meaning according to [RFC 1035](http://tools.ietf.org/html/rfc1035)[[5]](#footnote-5). TXT records occur in the IN class.

### TTL

Standard DNS meaning according to [RFC 1035](http://tools.ietf.org/html/rfc1035). A 32 bit signed integer that specifies the time interval that the resource record may be cached before the source of the information should again be consulted. A zero value means that the RR can only be used for the transaction in progress and should not be cached.

### RR Type

DNS resource record type of literal ‘TXT’.

## Txt Data

TXT RRs hold descriptive text. The program that consumes the content determines the semantics of the text. The Configuration Service expects the following format.

("<name>=<value>" "<name>=<value>")

Use double quotes around name – value pairs, separate with a space and enclose within parentheses.

### Name

Specifies the name of the database context e.g. STAGE.

### Value

Specifies the service prefix of one or more service (SRV) records.

### Example

TXT records to support configuration discovery for the Lead and Serialization service might be expressed as shown in Table 1 - TXT Record Example.

Table 1 – Example TXT Records

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Service | Class | TTL | Id | Txt data |
| lead | IN | 0 | TXT | (“STAGE=\_fa-stage” “PROD=\_fa-prod” “TEST=\_fa-test”) |
| serialize | IN | 0 | TXT | (“STAGE=\_fa-stage” “PROD=\_fa-prod” “TEST=\_fa-test”) |

Note that the example shows TXT records containing the same data for both the Lead and Serialization services. This is coincidental and does not imply that the services must be provided by the same server.

## SRV Record

The SRV DNS resource record specifies the location of the server(s) for a specific protocol and domain. The format of the SRV record is:

<symbolic name> <ttl> <class> <RR Type> <priority> <weight> <port> <target>

### Symbolic Name

The symbolic name of the service consists of the Service, Protocol, and Name components, separated by a period (.).

#### Service

The name of the desired service, as locally defined. An underscore (\_) is prepended to the service name to avoid collisions with other DNS labels. The Service is case insensitive. For configuration discovery, the service identifier must match the value portion of the TXT record for the desired implementation of the service and operation context.

#### Protocol

The symbolic name of the desired protocol, with an underscore (\_) prepended to prevent collisions with DNS labels already defined. \_http and \_tcp are the most useful values for this field, though any name defined locally or by Assigned Numbers may be used. Protocol is case insensitive.

#### Name

The domain to which this RR refers (e.g. eLAB.gov).

### TTL

Standard DNS meaning according to [RFC 1035](http://tools.ietf.org/html/rfc1035). A 32 bit signed integer that specifies the time interval that the resource record may be cached before the source of the information should again be consulted. Zero is interpreted to mean that the RR can only be used for the transaction in progress, and should not be cached.

### Class

Standard DNS meaning. SRV records occur in the ‘IN’ class.

### RR Type

DNS resource record type of literal ‘SRV’.

### Priority

The priority of this target host. For configuration discovery, the value is 0.

### Weight

A server selection mechanism. The weight field specifies a relative weight for entries with the same priority. For configuration discovery, the value is 0.

### Port

The port on the target host that provides this service. The range is 0-65535. This is a 16 bit unsigned integer in network byte order.

### Target

The domain name of the target host. There must be one or more DNS address records for this name. The name must not be an alias (in the sense of RFC 1034 or RFC 2181). A Target with the value of "." means that the service is NOT available in this domain. It provides a convenient way to temporarily disable configuration discovery for a service.

### Example

TXT records to support configuration discovery for the Lead and Serialization service might be expressed as shown in Table 2 - Example SRV Records.

Table 2 - Example SRV Records

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Symbolic name | TTL | Class | RR | Pri | Wt | Port | Target |
| \_fa-stage-lead.\_http.elab.gov | 0 | IN | SRV | 0 | 0 | 8080 | Test123 |
| \_fa-stage-lead.\_tcp.elab.gov | 0 | IN | SRV | 0 | 0 | 5200 | Test123 |
| \_fa-stage-serialize.\_tcp.elab.gov | 0 | IN | SRV | 0 | 0 | 5200 | Test123 |

This example indicates that in the Stage context the Lead service is available at two endpoints on the server named “Test123”. One endpoint via http on port 8080 and the other via netTcp on port 5200. The Serialize service is available on the server named “Test123” via netTcp on port 5200.

# Configuration Service Implementation

A single Configuration service in each operation context provides access to the FA Configuration table. The DNS records denoted in the previous section allow both the Sentinel Serialization client and the Sentinel Administrator Console to discover the server and endpoint for the service in the proper operational context. The service value of the TXT and SRV records correspond to the value of the Name column in the FA Configuration table. The Settings column contains the Xml configuration data for the Sentinel Serialization client.

Refer to the Sentinel Serialization Administration Guide for a discussion of using the Sentinel Administrator Console.

1. IETF - The Internet Engineering Task Force <http://www.ietf.org/> [↑](#footnote-ref-1)
2. A Request for Comments (RFC) is a type of publication from the Internet Engineering Task Force (IETF) and the Internet Society, the principal technical development and standards-setting bodies for the Internet. [↑](#footnote-ref-2)
3. RFC1464 - Using the Domain Name System To Store Arbitrary String Attributes http://tools.ietf.org/html/rfc1464 [↑](#footnote-ref-3)
4. RFC2782 - A DNS RR for specifying the location of services (DNS SRV) http://tools.ietf.org/html/rfc2782 [↑](#footnote-ref-4)
5. RFC1035 - Domain names - implementation and specification http://tools.ietf.org/html/rfc1035 [↑](#footnote-ref-5)