OCTO CONSULTING GROUP

Forensic advantage Installation Instructions

Version 1

March, 25 2016



Prepared by:

Octo Consulting Group

1600 International Drive, 5th Floor

McLean, VA 22102

Change Description Form

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Revision** | **Change Description** | **Changed By** | **Date** | **Approved By** |
| 1.0 | Initial Draft | Erik Hosler | 03/25/2016 |  |
| 1.1 | Minor updates for Sentinel Submission Type | Erik Hosler | 03/30/2016 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

1 Introduction 3

1.1 Sentinel Prelog API 3

1.2 Pre-requisites 3

2 Prelog API v1.0 Installation 3

3 Configure FAS.Prelog Service 3

Sentinel Submission Type 4

Associate New Submission to Criminal Lab 4

3.1 Database Strings 5

Database Configuration 5

3.2 Application Settings - <appSettings> 5

Required Information 5

appSettings Configuration 5

FAS Task Manager Configuration Settings 6

3.3 Application Settings - <applicationSettings> 6

Submission\_XP Extended Data 6

<applicationSettings> Configuration 7

3.4 Remaining Configuration File Settings 8

4 SQL Installation 9

5 Create Cluster Instance and Test Service 10

5.1 Pre-requisites 10

52 HA Service Configuration 10

5.3 Test Prelog API Availability 12

6 Enable SSL for Sentinel Connectivity 13

6.1 Pre-requisites 13

6.2 Certificates Installation 13

6.3 Configure the Prelog API for SSL 16

6.4 Add IIS to the FA Application Server 17

6.5 Add HTTPS Binding and SSL to IIS 18

# 1 Introduction

## 1.1 Sentinel Prelog API

The Sentinel Prelog API (Prelog) is an application integration interface between The Forensic Advantage® Laboratory Information Management System (FA LIMS) and the FBI Sentinel Record Management System (Sentinel). The Prelog accepts the content of the FBI form FD-1121 Laboratory Examination Request, and delivers the data elements to the FA LIMS for import as new FA LIMS submissions. The information includes general case information, detailed evidence inventories and PDF documents. Each Sentinel request received by Prelog is tracked and status showing the current state of the submission can be displayed in the Sentinel User Interface (UI).

## 1.2 Pre-requisites

Before proceeding with the upgrade, the following conditions must be met:

 FA LIMS Installed and Configured

 FA Service Account and Password (ex. svc\_fa)

 Server administrative privileges

 Knowledge of MS Clustering and installation environment cluster configuration

 IP address for setting up clustered service for Prelog

 Appropriate SSL certificate for the installation environment

# 2 Prelog API v1.0 Installation

Prelog operates as a Windows Service under the “Trusted Subsystem Security model”. The service runs in the same security context as the other FAS application services. The software is installed via an MSI installer, which needs to be completed on all application servers in environments that utilize a cluster architecture.

1. From the installation media, copy the FAS.Prelog.Setup.msi to the local server.
2. Run the Prelog API installer as an administrator.
3. If a Security Warning window appears, click “Run” to continue.
4. Click the check box to accept the license agreement and click the “Advanced” button to enter the Advanced Configuration screen.

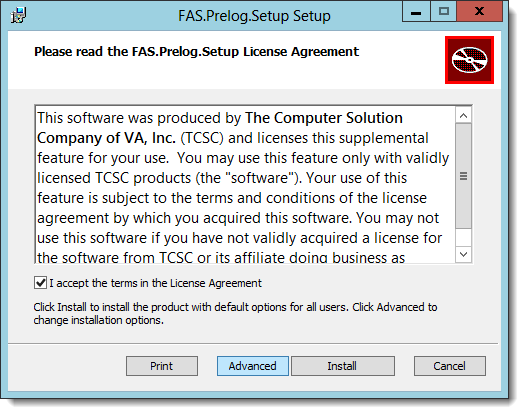


Figure 1 - Prelog License Acceptance

1. Select the radial button for “Install for all Users of this Machine”, and click the “Next” button.
2. In the “Install FAS Sentinel Prelog to:” field enter the following.
   1. C:\Program Files\TCSC\<environment>\FAS.Prelog\

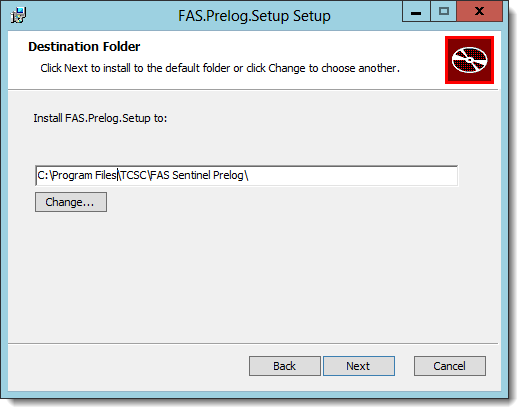


Figure 2 - Select Installation Location

1. Click “Next” and allow for the installation process to complete.

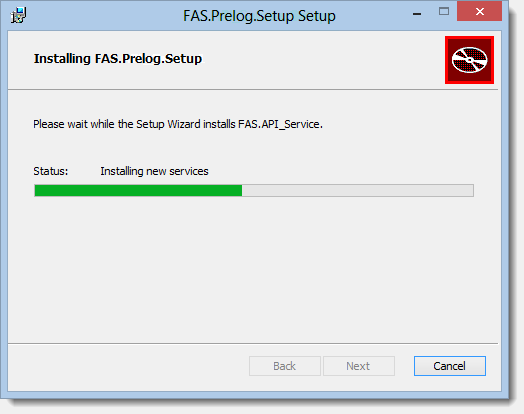


Figure 3 - FAS.Prelog Installation Progress

1. Click “Install” to accept defaults on the “Product Features” screen.
2. Click “Finish” to close the installation window.

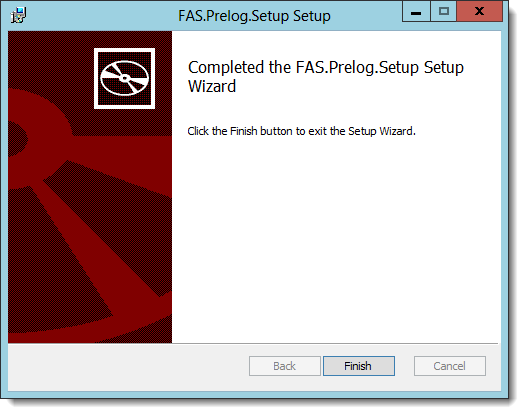


Figure 4 - FAS.Prelog Installation Finalization

1. DO NOT START THE SERVICE.
2. **If installing the Prelog API in a clustered environment**, complete the API installation on the remainder of the FAS application servers.

# 3 Configure FAS.Prelog Service

After successful installation of the Prelog software, a default configuration file is available in the installation directory. The file name is FAS.Prelog.Sentinel.WindowsService.exe.config and contains all of the available settings for the API. A second configuration file is provided as part of the Gold Disk that distinctly marks with brackets (< >) what value need to change per installation environment. It is encouraged that the configuration file supplied on the Gold Disk is used to replace the configuration file in the default Prelog installation directory. In using either of the supplied configuration files,the settings must be changed so that environment specific configurations, and client configurations are captured and implemented.

In addition to the configuration file, a new submission type in the FA application must be created to allow submissions from Sentinel with zero evidence items. To create the submission type, follow the directions below.

### Sentinel Submission Type

1. Open the FA Application.
2. Navigate to Admin Console | Cases and Evidence | Submission Type.
3. Create a new submission with the following attributes.
   1. Description = Sentinel
   2. All Exams = Checked
   3. FA Web Visible = Not Checked
   4. Require Exams = Not Checked
   5. Require Evidence = Not Checked
   6. Require Offense = Not Checked
   7. Allow Historical = Checked
   8. Allow Subsequent = Checked
   9. Allow New Submission = Checked
   10. Require Inv Officers = Checked
   11. Retain Agencies = Checked
   12. Retain Sub Officers = Checked
   13. Retain All Officers = Not Checked
   14. Retain Delivery Return Methods = Checked
   15. Retain Primary Section = Checked
   16. Retain SOF Comments = Not Checked
   17. Retain Jurisdiction Offense Court = Not Checked
   18. Retain Exams = Not Checked
   19. Retain Evidence = Not Checked
   20. Require Jurisdiction = Not Checked
   21. Auto Increment Case Disc Num = Not Checked
   22. Require Agency = Checked
   23. Case Num Mask = YYYY-SSSSS
   24. Min Year = 1900
   25. Max Year = 2050
   26. Is Active = Checked

### Associate New Submission to Criminal Lab

1. From the Admin console navigate to Cases and Evidence | Submission Configuration | Lab / Submission Type.
2. Create a new entry with the following attributes.
   1. Lab = Criminal
   2. Submission Type = Sentinel
   3. Is Active = Checked
3. Click “Save Changes” icon in the ribbon bar.

## 3.1 Database Strings

The Prelog API needs to connect to supporting databases in order to present and record data to/from Sentinel appropriately. Using an advanced text editing tool similar to NotePad++ will make the editing of the configuration file easier and is recommended for the following steps. The instructions to configure the database follows.

### Database Configuration

1. Open the configuration file.
2. Navigate to the <connectionStrings> element.
   1. There are 3 connection strings that must be modified.
3. Modify the connection strings as follows.
4. Name = “PrelogContext”
   1. Data Source = <SQL SERVER>
   2. Catalog= <FA CORE DB>
5. Name = “FaContext”
   1. Data Source = <SQL SERVER>
   2. Catalog= <FA CORE DB>
6. Name = “SubmissionEmployeeDataContext”
   1. Data Source = <SQL SERVER>
   2. Catalog= <FA CORE DB>

## 3.2 Application Settings - <appSettings>

The “General Application Settings” below specify how the Prelog API handles data both inbound and outbound to/from Sentinel. These settings are client and environment specific. Careful attention is needed to ensure the API functions as required per user specifications.

### Required Information

The following FA settings are required to complete this section. FA Settings are environment specific and will need to be addressed for each installation location.

 Core Repository Name

 External Repository Name

 FBI Headquarters Agency ID

 FBI Headquarters Agency Location ID

 Criminal Lab ID

 Evidence Control Section ID

 Federal Express Submission Method Code

 FBI Organization Prefix

 Sentinel Submission Type ID

 FA Task Manager Connection String

 The “UPDATE VIOLATION” Offense ID

### appSettings Configuration

1. Open the configuration file (if not already open).
2. Navigate to the <appSettings> element.
3. Check and or modify the keys identify below.
4. key="AddDefaultEvidenceIfEmpty"
   1. value="false"
5. key="AgencyNumberStringFormat"
   1. value="{0}, {1}"
   2. **NOTE:** There is a space between the comma and open curly bracket.
6. key="CoreObjectRepositoryName"
   1. value="Core"
7. key="ExternalObjectRepositoryName"
   1. value="External"
8. key="DefaultAgencyId”
   1. value="<FBI Headquarters Agency ID>"
9. key="DefaultAgencyLocationId"
   1. value="<FBI Headquarters Agency Location ID>"
10. key="DefaultEvidenceTypeCode"
    1. value="I"
11. key="DefaultLabId"
    1. value="<Criminal Lab ID>"
12. key="DefaultLabSectionId"
    1. value="<Evidence Control Section ID"
13. key="DeliveryMethodCode"
    1. value="<Federal Express Delivery Method Code>"
14. key="OrganizationPrefix"
    1. value="<FBI Organization Prefix>"
15. key="SubmissionType"
    1. value="<Sentinel Submission Type>"

### FAS Task Manager Configuration Settings

The Prelog API relies on the FAS Task Manager Service, not to be confused with the scheduled tasks utilized for the 1A packet, to complete jobs and interact with the FA application. The following keys in the appSettings element provide the connection strings required for the communication channel.

1. key="DefaultServiceAddress\_CaseManager"
   1. value="net.tcp://<clustered\_machine\_name:Port#>/fa/api/1.0/CaseManager"
2. key="DefaultServiceAddress\_GatewayManager"
   1. value="net.tcp:// <clustered\_machine\_name:Port#>/fa/api/1.0/GatewayManager"
3. key="DefaultServiceAddress\_LookupsManager"
   1. value="net.tcp:// <clustered\_machine\_name:Port#>/api/1.0/LookupsManager"
4. key="DefaultServiceAddress\_SequenceManager"
   1. value="net.tcp:// <clustered\_machine\_name:Port#>/fa/api/1.0/SequenceManager"

## 3.3 Application Settings - <applicationSettings>

The configuration file is sectioned into two “settings” sections. The second section, noted by the element <applicationSettings>, controls how information is presented to Sentinel. This section also controls how extended data is handled.

### Submission\_XP Extended Data

Extended data must be collapsed into a flat structure in order to support submissions from Sentinel. Migration of pre-existing Sumbission\_XP extended data to the newly created properties below is required, but is outside the scope of these instructions.

1. Open the FA application (if not opened already).
2. Navigate to Admin Tab | Extended Data Designer | Submission\_XP.
3. Click the Add Button.
4. Use the following values for the first new XD element.
   1. Definition | Name: DocumentSerial
   2. Definition | Property Type: StringData
   3. Presentation | Display Name: DocumentSerial
   4. Presentation | Order: 2
5. Use the following values for the second new XD element.
   1. Definition | Name: DocumentType
   2. Definition | Property Type: StringData
   3. Presentation | Display Name: DocumentType
   4. Presentation | Order: 3
6. Use the following for the third new XD element.
   1. Definition | Name: DocumentDate
   2. Definition | Property Type: StringData
   3. Presentation | Display Name: DocumentDate
   4. Presentation | Order: 4
7. Use the following for the fourth new XD element.
   1. Definition | Name: DocumentUniqueId
   2. Definition | Property Type: StringData
   3. Presentation | Display Name: DocumentUniqueId
   4. Presentation | Order: 5
8. Confirm the following XD elements exist for Submission\_XP.
   1. Case ID
   2. Lead
   3. DocumentSerial
   4. DocumentType
   5. DocumentDate
   6. DocumentUniqueId

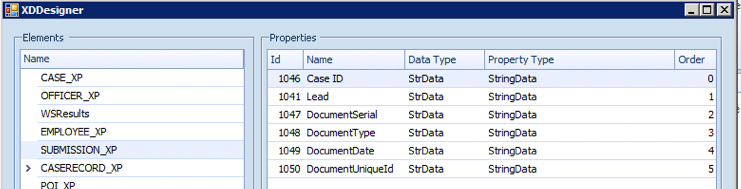


Figure 5 Submission\_XP Extended Data

1. Document the Extended Data Property Ids.
   1. **Note:** The Id column may need to be added to the grid from the “Column Chooser” pop-up menu option.

### <applicationSettings> Configuration

1. Within the Prelog configuration file, locate the <applicationSettings> element
2. For each of the below items, confirm or modify the setting’s <value> tag.
3. name="RecordStatusFilter"
   1. Value = T
4. name="RecordStatusMaps"
   1. Value = A|A,C|C,B|E,D|E,E|E,F|E,L|E,M|E,R|E,V|E,1|E,W|W
5. name="SubmissionAgencyRelationshipCodes"
   1. Value = “INV”
6. name="DefaultOffenseIds"
   1. Value = <use the UPDATE VIOLATION Offense Id from Admin Console | Cases and Evidence | Submission Configuration | Offense>
7. name="DocumentUniqueIdExtendedProperty"
   1. Definition = <Extended Data Property Id>
   2. Name = DocumentUniqueId
   3. Leave the remaining 2 settings as the default
8. name="DocumentSerialExtendedProperty"
   1. Definition = <Extended Data Property Id>
   2. Name = DocumentSerial
   3. Leave the remaining 2 settings as the default
9. name="DocumentDateExtendedProperty"
   1. Definition = <Extended Data Property Id>
   2. Name = DocumentDate
   3. Leave the remaining 2 settings as the default
10. name="LeadNumberExtendedProperty"
    1. Definition = <Extended Data Property Id>
    2. Name = Lead
    3. Leave the remaining 2 settings as the default
11. name="DocumentTypeExtendedProperty"
    1. Definition = <Extended Data Property Id>
    2. Name = DocumentType
    3. Leave the remaining 2 settings as the default

## 3.4 Remaining Configuration File Settings

The remainder of the configuration file will be similar to the other FAS application services. Reference to the other FAS service configuration files would be helpful in completing this section.

1. repositoryClient
   1. Points to the environment temp directory, most commonly C:\FATemp
2. TCSCLogging
   1. Configure the service log directory, and log file name
3. baseAddress
   1. Configure the base address to the IP address for the clustered service and port number
   2. Recommended port number is 5170, but can be any unused port for the application server
4. Client (OR and OR\_LOCAL)
   1. Configure the TCP endpoint addresses for the OR service.
5. Save the configuration file, and copy it to the remaining FA application servers if a clustered environment exists.
6. **DO NOT START THE PRELOG SERVICE.**

# 4 SQL Installation

SQL tables and stored procedures required to support the Prelog API are installed into the CORE database under the custom schema. Utilizing this method enables the Prelog backend and software to be installed and utilized independently of the core FA application.

The installation of the SQL databases requires the person conducting the installation to have administrative privileges to the SQL database server, and CORE database. The MSI for Prelog saves the SQL scripts under the service installation folder in the SQL\_Installation directory. The default install location for the MSI is %ProgramFiles%\TCSC\<environment>\FAS.Prelog\SQL\_Installation.

1. Log into the environment’s SQL server.
2. Copy the SQL\_Installation folder from the FA Application server to the SQL Server.
3. Open the SQL\_Installation folder.
4. For each of the following SQL files, change the USE [FAS.PRELOG] statement to the correct CORE database for the environment. Ex. USE [FA\_Stage\_Core]
   1. FAS.PrelogExamTypeFilters\_Data.sql
   2. FAS.Prelog.OrgUnitAgencyLocationMaps\_Data.sql
   3. FAS.Prelog\_CommandScript.sql
5. Open PowerShell as an administrator, and change the directory to the SQL\_Installation folder location.
   1. Ex. cd c:\users\<username>\desktop\SQL\_Installation
6. Run the following command.
   1. substitute <Server> with the SQL Server name
   2. Substitute <Database> with the FA Core database

sqlcmd –E -S <Server> -d <database> -i  FA.PrelogOfficer\_View.sql -m10 -r1

1. In the PowerShell windows, change the directory to the .\Script\_Components folder.
   1. Ex. cd c:\users\<username>\desktop\SQL\_Installation\SQL\_Components
2. Run the following commands.
   1. substitute <Server> with the SQL Server name

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

sqlcmd -E -S <Server> -i ..\FAS.Prelog.OrgUnitAgencyLocationMaps\_Data.sql -m10 -r1

sqlcmd -E -S <Server> -i ..\ FAS.Prelog.Prelog.ExamTypeFilters\_Data.sql -m10 -r1

1. Once all scripts have completed, open SQL Server Management Studio, and confirm the following tables exists.
   1. Custom.Prelog\_BusinessesOfInterest
   2. Custom.Prelog\_Evidence
   3. Custom.Prelog\_ExamTypeFilters
   4. Custom.Prelog\_ForensicCases
   5. Custom.Prelog\_Leads
   6. Custom.Prelog\_Officers
   7. Custom.Prelog\_OrgUnitAgencyLocationMaps
   8. Custom.Prelog\_PersonsOfInterest
   9. Custom.Prelog\_RelatedCaseNumbers
   10. Custom.Prelog\_RelatedDocuments
   11. Custom.Prelog\_SubmissionRelatedDocuments
   12. Custom.Prelog\_Submissions
2. Select all rows from Custom.Prelog\_ExamTypeFilters.
   1. Total row count should equal 148
3. Select all rows from Custom.Prelog\_OrgUnitAgencyLocationMaps.
   1. Total row count should equal 5,958

# 5 Create Cluster Instance and Test Service

For service high availability (HA), the Prelog API will be configured as a HA Service in Microsoft Failover Cluster Manager. After the configuration is complete, and the previous section of this installation and configuration document have been completed successfully, the Prelog service can be tested by the Prelog Test Client.

## 5.1 Pre-requisites

 The Prelog Service (FAS Sentinel Prelog Service) is configured to run with the svc\_fa account.

 The Prelog Service is set to a start type of “Automatic”.

## 52 HA Service Configuration

1. On the FA Application Server, open the Failover Cluster Manager console.
2. Expand the cluster node, and highlight “Services and applications”.

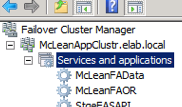


Figure 6 Cluster Manager

1. In the Actions Pane, click on “Configure a Service or Application…”.

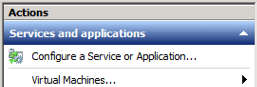


Figure 7 Action Pane Selection

1. Click “Next” on the High Availability Wizard “Welcome” page.
2. From the selection screen, choose “Generic Service” and click “Next”.

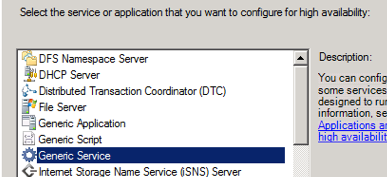


Figure 8 Generic Service Selection

1. From the service list, select “FAS Sentinel Prelog Service” and click “Next”.

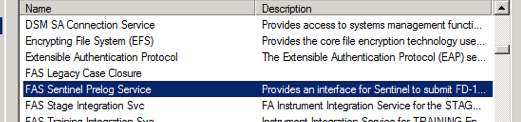


Figure 9 Prelog API Service Selection

1. On the “Client Access Point” screen enter the Name and IP address for the clustered service and click “Next”.

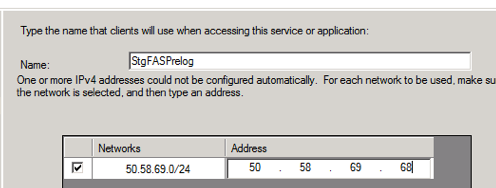


Figure 10 Client Access Point

1. Click “Next” on the “Select Storage screen”.
2. Click “Next” on the “Replicate Registry Settings” screen.
3. Click “Next” on the “Confirmation” screen.
4. Allow the configuration process to finish then click “Finish”.

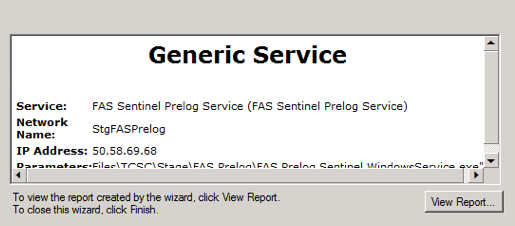


Figure 11 Finish Screen

1. In the Failover Cluster Manager console, confirm the newly created HA service is running.



Figure 12 Service Confirmation

1. Navigate to the FALog directory for the Prelog API.
2. Open the Prelog API log and confirm that the service is running.
   1. That log entry should resemble the following graphic.

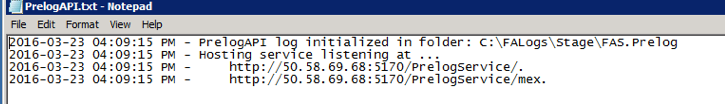


Figure 13 API Log File Confirmation

## 5.3 Test Prelog API Availability

In addition to the baseline Prelog API software, the installation directory also contains a rudimentary Prelog Test Client that can be used to ensure the service is operational and available to accept incoming Sentinel Submissions.

The client was developed as a developer/tester tool and does not contain the refinement of a production application. There is no support for issues or defects with the test client, and should only be used to ensure the Prelog API is operational. Instructions for the use of the client, as well as, any other supporting documentation are outside the scope of the Prelog API functionality and delivery. The instructions below are provided only to confirm the Prelog API was successfully installed and it is not intended for use in GAT/UAT testing.

1. Navigate to the Prelog API installation directory.
2. With an text editor (ex. NotePad++) open the Test Client configuration file.
   1. FAS.Prelog.TestClient.exe.config
3. In the <client> section of the configuration file, change the endpoint address to point to the IP address and port for the Prelog Service.



Figure 14 Test Client Configuration

1. In the Prelog API installation directory, double click the test client application executable.
   1. FAS.Prelog.TestClient.exe
2. Once loaded, click the “Ping” button on the “Ping” tab in the Test Client.
3. A successful ping result resembles the following graphic and indicates that the Prelog API service is properly configured and running.

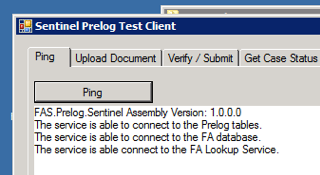


Figure 15 Success Confirmation

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**STOP AND READ THE FOLLOWING:** *For the GAT environment testing to commence, a connection to the Sentinel HS3 Integration environment is required. The work, infrastructure and code may not be available at the time that the FAS Prelog API is successfully installed into the GAT environment. If the HS3 Integration environment is not setup, the installation process of the API is complete. Only after the time that the HS3 Integration environment is ready should the remainder of these instructions be followed and completed.*

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

# 6 Enable SSL for Sentinel Connectivity

The service connection between the Prelog API and Sentinel needs to occur over a secure communication channels. The connection for the Low to High (L>H) channel is secured with machine certificates and TCP port 443. The section below details how to implement the changes required to secure the Prelog API endpoint address and communicate over HTTPS/443.

## 6.1 Pre-requisites

 SSL Certificate with a 2048 bit cypher key. Public and Private Key is required.

 Sec-D Low-side DataPower SSL certificate and root certificate.

## 6.2 Certificates Installation

1. Open a Microsoft Management Console (MMC) as an Administrator.
2. Navigate to File | Add/Remove Snap-in…
3. From the Add or Remove Snap-ins screen, highlight “Certificates” and click the “Add >” button.

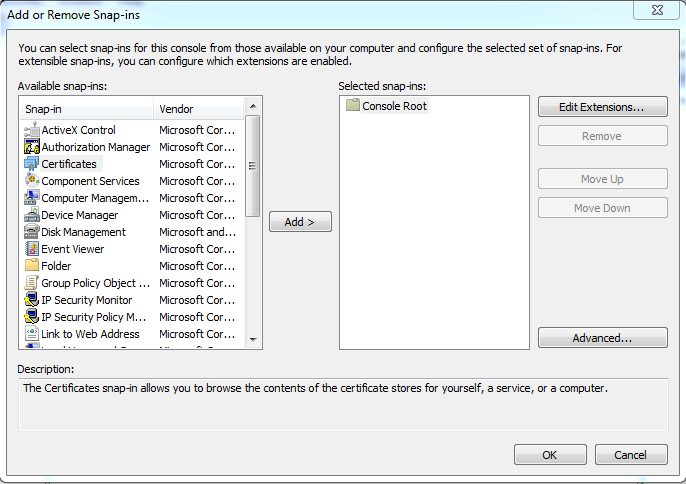


Figure 16 - Add Certificate Snap-in

1. From the Certificates snap-in window, select the radial button for “Computer account”.

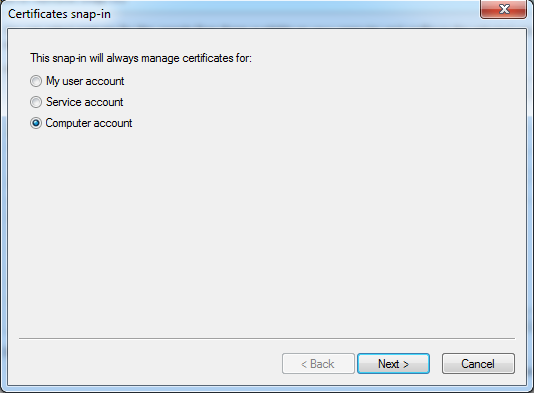


Figure 17 Computer Account Selection

1. On the “Select Computer” screen, select the “Local Computer…” radial button.

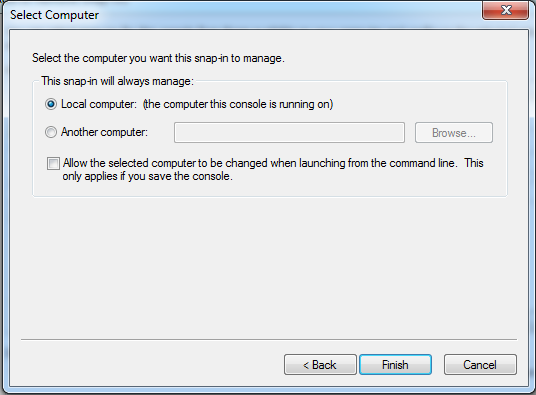


Figure 18 Local Computer Selection

1. Click on the “Finish” button.
2. Confirm “Certificates” is displayed in the “Selected snap-ins” window, and click the “OK” button.

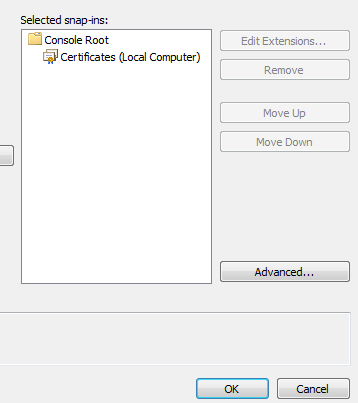


Figure 19 Certificate Confirmation

1. If not already completed, install the “eLAB” certificate that will secure the Prelog API.
2. Within the MMC Console, confirm that the certificate is displayed in the correct certificate store.
   1. Most commonly this certificate will appear in the “Personal” certificate store.
3. Install the SEC-D Low-Side Data Power Root Certificate into the “Trusted Root Certification Authorities” certificate store.
   1. Within the MMC Console, confirm that the certificate is displayed in the correct store.
4. Install the SEC-D Low-Side Data Power certificate into the “Personal” certificate store.
   1. Within the MMC Console, confirm that the certificate is displayed in the correct store.
5. If operating in a clustered environment, the steps above must be completed on all FA Application servers.

## 6.3 Configure the Prelog API for SSL

1. From the Failover Cluster Management console, stop the Prelog API service.
2. Navigate to the Prelog installation directory.
   1. Default installation path is %ProgramFiles%\TCSC\<environment>\FAS.Prelog\
3. With a text editor (ex. NotePad++) open the Prelog API configuration file.
   1. FAS.Prelog.Sentinel.WindowsService.exe.conf
4. In the <baseAddresses> element, add a second base address for SSL communication.
   1. <add baseAddress=”https://<IP\_Address>/PrelogService/” />



Figure 20 Add baseAddress

1. In the <bindings> section of the configuration file, find the element <basicHttpBinding>.
2. After the <binding> element, add the following elements.
   1. <security mode=”Transport”>  
       <transport clientCredentialType=”None” />  
      </security>

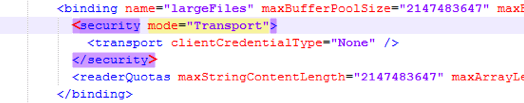


Figure 21 Security Settings

## 6.4 Add IIS to the FA Application Server

1. Open the Server Management Console.
2. Highlight Roles.
3. In the middle pane, click on “Add Role Services”.

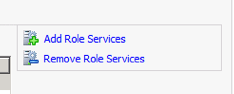


Figure 22 Add Role Services

1. Under Application Server, add “Web Server (IIS) Support”.

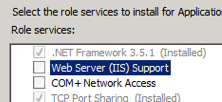


Figure 23 Select HTTP Activation

1. On the “Add Role Services” pop-up window, click “Add Required Role Services”.

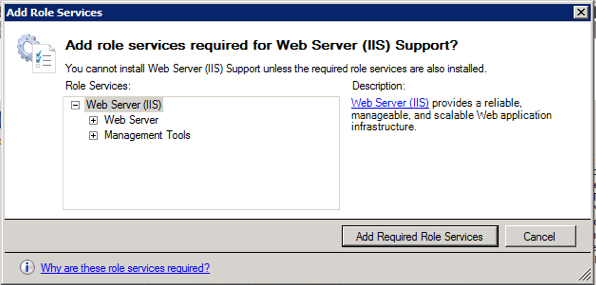


Figure 24 Required Role Services

1. Click “Next” until Installation Ready, then click the “Install” button.

## 6.5 Add HTTPS Binding and SSL to IIS

1. Open IIS Management console.
2. Click the “Plus” sign next to the server name to expand.
3. Click the “Plus” sign on the “Sites” node.
4. Select “Default Website”.

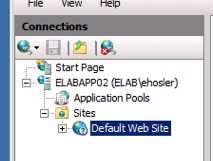


Figure 25 Default Website Selection

1. In the “Actions” pane, click on the “Bindings” link.

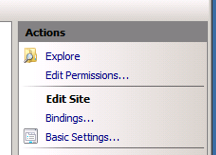


Figure 26 Actions Pane - Bindings

1. Click “Add” on the Site Bindings screen.

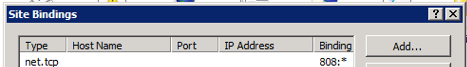


Figure 27 Site Bindings

1. Configure the new site binding with these values.
   1. Type: https
   2. IP Address: All Unassigned
   3. Port: 443
   4. SSL certificate: <select the FBI certificate for the environment

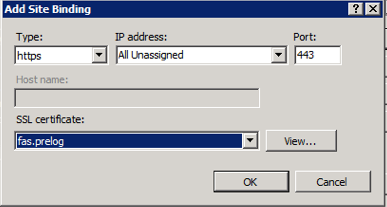


Figure 28 Binding Configuration

1. Click “OK”.
2. Click “Close”.