Snell
Advanced
Media

SigMA

Installation and User Guide

Version History

Date	Version	Release by	Reason for changes
16/10/2015	1.0	J Metcalf	Document originated (1st proposal)
02/03/2016	1.1	G Emerson	Format update
01/06/2016	2.0	J Metcalf / J.Courtney	Update for V2.0.0.* release.
22/09/2016	2.1	J Metcalf	Updated Appendix C (Ice and Morpheus Configuration)

Table of Contents

List of Tables

1. Definitions, Acronyms and Abbreviations

Table 1: Table of Terminology

Term	Definition
Absolute Delay	Absolute latency between two MBGs
AP	Assurance Point, used to analyze and compare Media Biomtric Signatures
APL	Average Picture Level. An average picture level confidence measurement indicating video is active
BioBank	A database of Media Biometric signatures ingested from MBG XF
BioBank Connector	Connector required for SigMA to look up signatures form the BioBank
Blackish	A picture blackish detector indicating when video is black/dark
Channel Match	Confirmation two playout channels are exactly the same (same logos, captions, media essense, DVE etc…)
Confidence Monitoring	A monitoring event that provides the user confidence media is present (in a specified way), preventing the need to actually view the media. Not intended as a means of accurate measurement
Domain ID	Media Biometric signatures may be shared between equipment which uses a common Domain ID
ICE	Integrated Content Engine. SAM's playout device
Intelligent Infrastructure	Umbrella term for SAM's intelligent solutions. This includes Media Assurance and Enterprise C&M,
Lip Sync (relative delay)	Confirmation two media streams have the correct lipsync
MBG	Media Biometrics Generator
MBG Domain ID	Domain unique for signatures publication
MBG (IQ)	MBG module offering 8 x MBGs
Media Assurance	The act of automatically checking and verifying media throughout a media production chain
Media Assurance Services	A variety of licensed features for Media Assurance
Media Biometrics	SAM's unique signature technology for video, audio and metadata
Media Identification	The act of comparing a live signature with BioBank to identify media
Media Match	Confirmation two media streams contain the same media essence (video, audio and captions)

Term	Definition
Morpheus	SAMs Enterprise grade automation solution
NTP	Network Time Protocol. A Protocol used to synchronize clocks throughout a computer network. It achieves an accuracy to within a few milliseconds
PTP	Precision Time Protocol. A protocol used to schronize clocks throughout a computer netqork. It acheives an accuracy in the sub microsecond range
RollCall Control Panel	RollCall middleware application for the control and monitoring of RollCall devices
RollMap	Customizable Enterprise grade graphical control and monitoring solution
SAM (IQ)	Signal Assurance Module offering 2 x MBG’s and 1 x AP
Schedule Manager	Application used to communicate with the Morpheus 2nd screen service
Schedule Match	Confirmation the playout media matches the playout schedule (using BioBank)
SigMA	Software application enabling mulitple AP’s to run on commodity IT infrastructure
Stillish	A picture stillish detector indicating when video is still (static)

2. Introduction

One aspect of SAM's Intelligent Infrastructure is **Media Assurance**.

Media Assurance is defined as the act of automatically checking and verifying media throughout a broadcast workflow.

The benefits of implementing a Media Assurance solution are:

- More channels can be monitored per operator
- Improved quality of service
- Reduced operational costs

Our Licensed Media Assurance Services are created using a new technology we call **Media Biometrics**.

Media Biometrics is SAM's unique signature intellectual property for video, audio and metadata. Signatures are generated by MBGs (Media Biometric Generators) and are analyzed and compared by APs (Assurance Points).

The primary benefit of SAM's Media Assurance Solution is:

- It is resilient to all forms of media processing
- It is non-destructive and invisible in operation
- It offer fast detection, analysis and reporting
- It can seamlessly integrate with existing 'monitoring by exception' system
- It offers a minute payload enabling hundreds of signatures to co-exist on a single low cost IT system

SigMA is a software application that enables multiple APs to run on commodity IT infrastructure.

SigMA runs in the background on a host PC. Users interface with the SigMA via RollCall Control Panel.

This guide will take the User through the process of:

- Installing the SigMA application on the host PC.
- Integrating SigMA with the RollCall application.
- Configuring Media Biometrics Assurance Points

3. System Requirements / Prerequisites

1. **IT Network:** In order to successfully build a SAM Media Assurance system a multi-cast enabled IP network is required.
2. **RollCall Control Panel.** All SAM Media Assurance products as controlled via RollCall Control Panel. At the time of writing, the current RollCall Control Panel release version is V4.15.3. (Oct 2015). It is recommended that this software suite is kept up to date.
3. **PC/Server.** A suitable host machine is required to run SigMA. We recommend using a processor/s that offer a minimum of 2.5GHz core frequency and multiple cores. The quantity of APs that can be successfully run an any given IT platform is dictated by:
   - The quantity of APs
   - The quantity of audio channels present per AP
4. **Standard / Professional** Licenses. For successful operation MBGs for signature generation are required.
5. **Enterprise License.** In order to use some of the playout specific features of the Enterprise license such as Schedule Match, the following is required:
   - Morpheus Automation system
   - ICE playout server

   Note: Signatures from Live playout source must be time synchronized with automation system.
6. **NTP / PTP Server.** For successful operation of Schedule Match, Closed Captions (Media Match) or Absolute Delay both signatures must be generated from a source MBG that is synchronized to either a NTP or PTP server.

4. SigMA Architecture

SigMA benefits from a Service Orientated Architecture (SOA). The minimum required services are:

- **SigMA**
- **SigMA Engine**
- **License Server**

Optional Services are:

- **Schedule Manager**
- **BioBank**

SigMA is the host application responsible for managing the other Media Assurance software services. Typically one instance of SigMA would manage multiple engines.

SigMA Engine is responsible for performing the Media Assurance processing for each AP. One SigMA Engine is required for each host machine performing the processing. A single SigMA instance can manage multiple engines by ensuring the same SigMA Domain ID is the same.

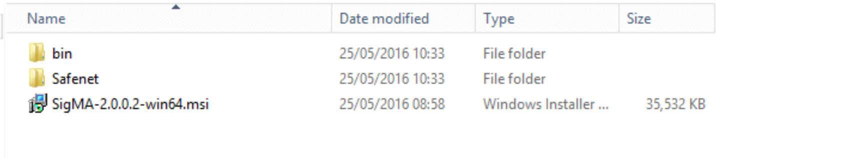
License Server is the service that manages licensing of all the SigMA services. If the license is not available, or cannot be accessed over the network, the Media Assurance Services will not be available for use.

Schedule Manager is responsible to managing the communication from the Morpheus 2nd Service to SigMA. This Service (and BioBank) is required for the successful operation of Schedule Match and Media Identification. The Signature created from the Playout device must be synchronized with the automation system system. This is achieved using NTP.

BioBank is the Media Biometrics Database. This uses the Mongo DB platform and a **BioBank Connector** license is required to enable SigMA to communicate with BioBank.

5. Installation

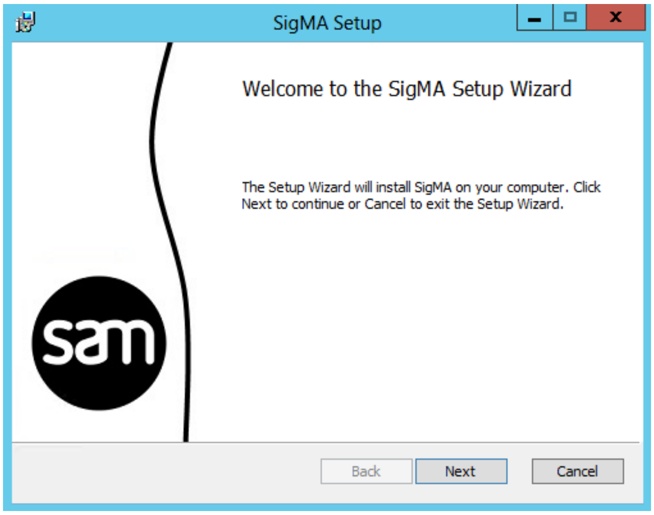
The SigMA installer package should be downloaded and moved to the host PC. SigMA will run on a 64 bit Windows platform.



Name	Date modified	Type	Size
bin	25/05/2016 10:33	File folder	
Safenet	25/05/2016 10:33	File folder	
SigMA-2.0.0.2-win64.msi	25/05/2016 08:58	Windows Installer ...	35,532 KB

5.1 Installation Procedure

1. Launch the SigMA installer program. A setup wizard will be displayed:



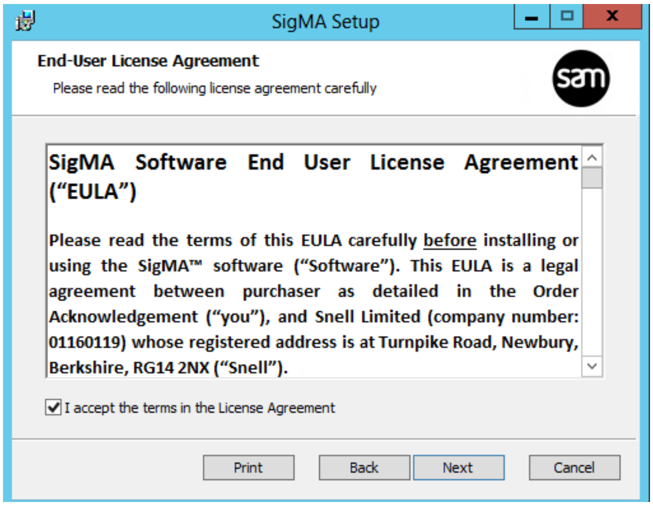
SigMA Setup

Welcome to the SigMA Setup Wizard

The Setup Wizard will install SigMA on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Select **Next.**

2. Next, the **SigMA End User Licence Agreement** widow will be displayed.



End-User License Agreement

Please read the following license agreement carefully

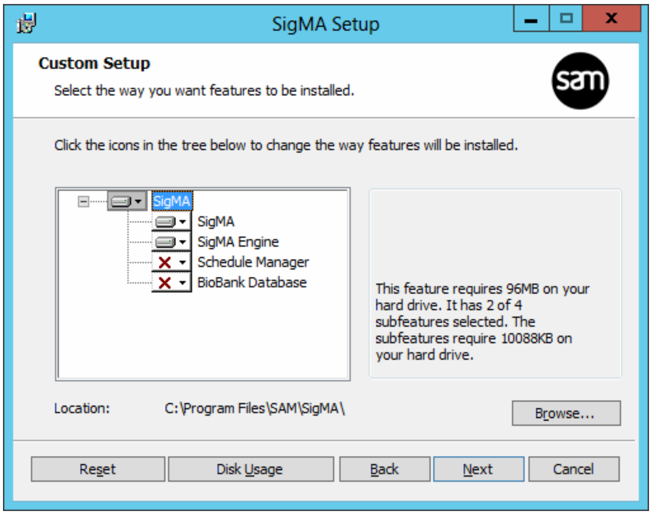
SigMA Software End User License Agreement ("EULA")

Please read the terms of this EULA carefully before installing or using the SigMA™ software ("Software"). This EULA is a legal agreement between purchaser as detailed in the Order Acknowledgement ("you"), and Snell Limited (company number: 01160119) whose registered address is at Turnpike Road, Newbury, Berkshire, RG14 2NX ("Snell").

☑ I accept the terms in the License Agreement

Check the tick-box to accept the license agreement, click **Next.**

3. The **Custom Setup** window will now be displayed.



Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

This feature requires 96MB on your hard drive. It has 2 of 4 subfeatures selected. The subfeatures require 10088KB on your hard drive.

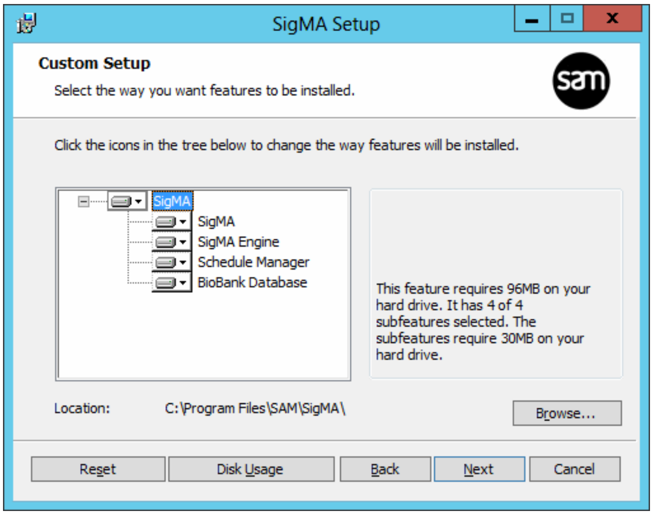
Location: C:\Program Files\SAM\SigMA\

This menu offers options to install the following Applications/Services

- **SigMA**
- **SigMA Engine**
- **Schedule Manager**
- **BioBank Database**

For a first time install, the SigMA and SigMA Engine should be enabled for installation. The Schedule Manager and the BioBank Database are optional and should only be installed if they are required.

In this example, both the **Schedule Manager** and the **BioBank Database** are enabled for installation.



SigMA Setup

Custom Setup

Select the way you want features to be installed.

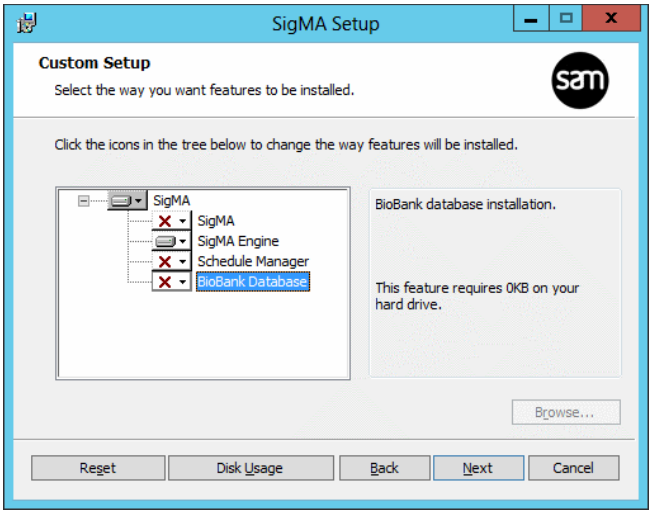
Click the icons in the tree below to change the way features will be installed.

- SigMA
  - SigMA
  - SigMA Engine
  - Schedule Manager
  - BioBank Database

This feature requires 96MB on your hard drive. It has 4 of 4 subfeatures selected. The subfeatures require 30MB on your hard drive.

Location: C:\Program Files\SAM\SigMA\

To install additional SigMA Engines the installer program should be run again and at this point the SigMA installer should be disabled.



SigMA Setup

Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

- SigMA
  - ☒ SigMA
  - SigMA Engine
  - ☒ Schedule Manager
  - ☒ BioBank Database

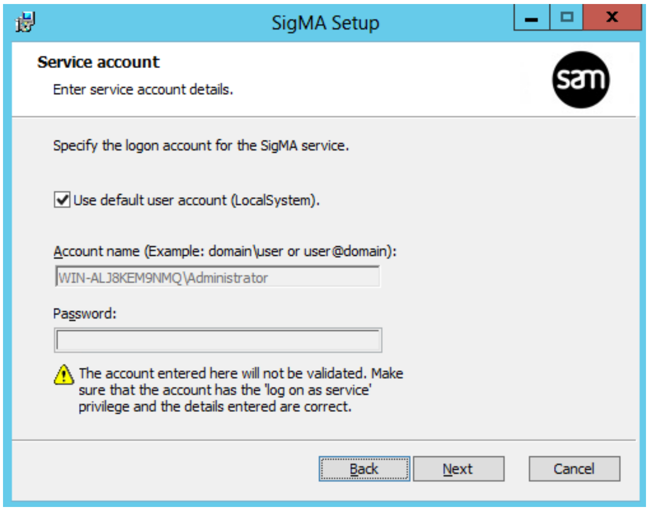
BioBank database installation.

This feature requires 0KB on your hard drive.

For more information regarding installing just a SigMA Engine, please see Appendix 1 below.

Click **Next** to continue.

4. The SigMA **Service Account** window will now appear.



Service account

Enter service account details.

Specify the logon account for the SigMA service.

☑ Use default user account (LocalSystem).

Account name (Example: domain\user or user@domain):

WIN-ALJ8KEM9NMQ\Administrator

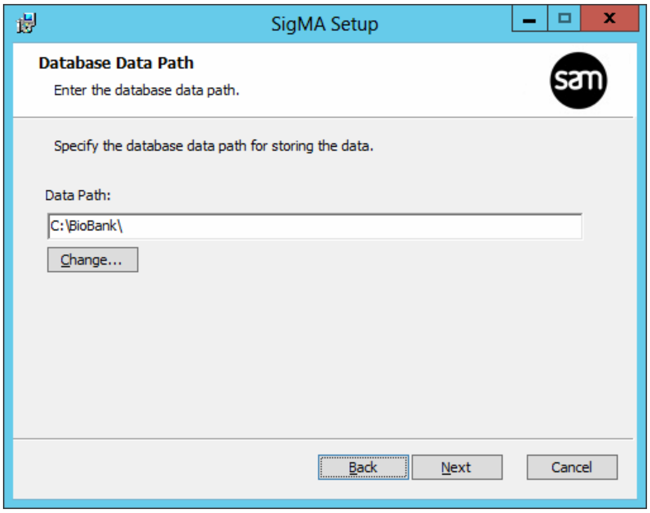
Password:

⚠ The account entered here will not be validated. Make sure that the account has the 'log on as service' privilege and the details entered are correct.

This allows SigMA Services to be configured to run for a specific User if required, but under normal circumstances the default settings for this window can be used.

Click **Next** to continue.

5. If the installation includes the BioBank Database, the SigMA **Database Data Path** window will appear.



Database Data Path

Enter the database data path.

Specify the database data path for storing the data.

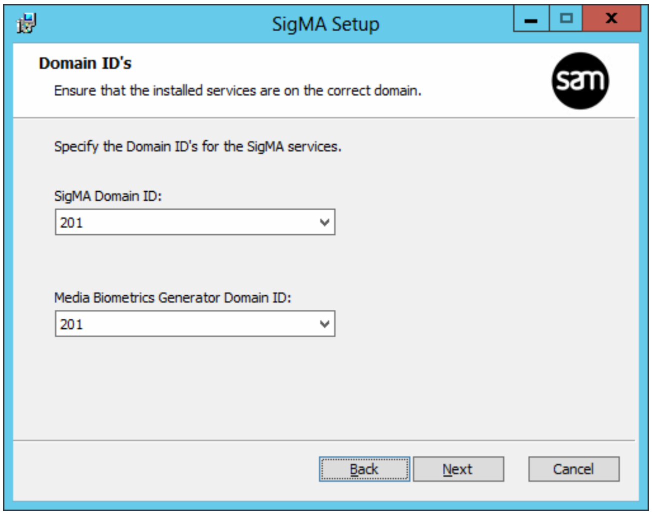
Data Path:

C:\BioBank\

An alternative path may be defined if required.

Click **Next** to continue.

6. The SigMA **Domain ID** window will now be displayed.



SigMA Setup

Domain ID's

Ensure that the installed services are on the correct domain.

Specify the Domain ID's for the SigMA services.

SigMA Domain ID: 201

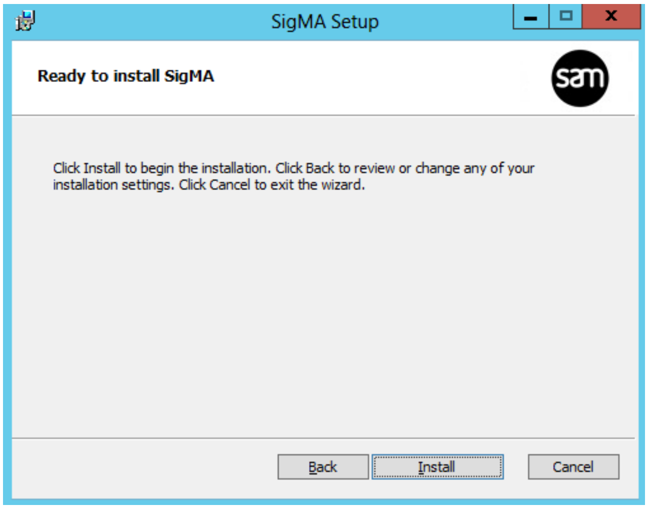
Media Biometrics Generator Domain ID: 201

Multiple SigMA's may be installed on a network, but the SigMA Engines can only communicate with one instance of SigMA.

The MBG Domain ID controls which Signatures are available on a given Domain. Multiple SigMA's may be connected to the same MBG Domain. In this case the same signatures would be available to each instance of SigMA.

Click **Next** to continue.

7. The SigMA is now ready to be installed.



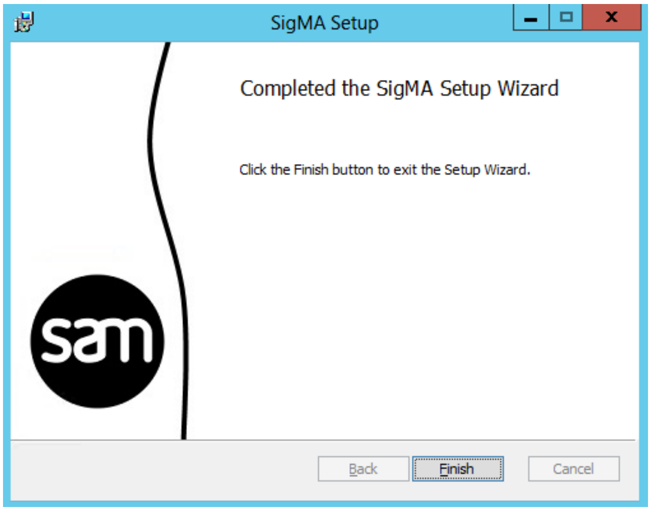
SigMA Setup

Ready to install SigMA

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Click **Install**

The SigMA application will now install. This only takes a few seconds. Once installed a confirmation window will be displayed.

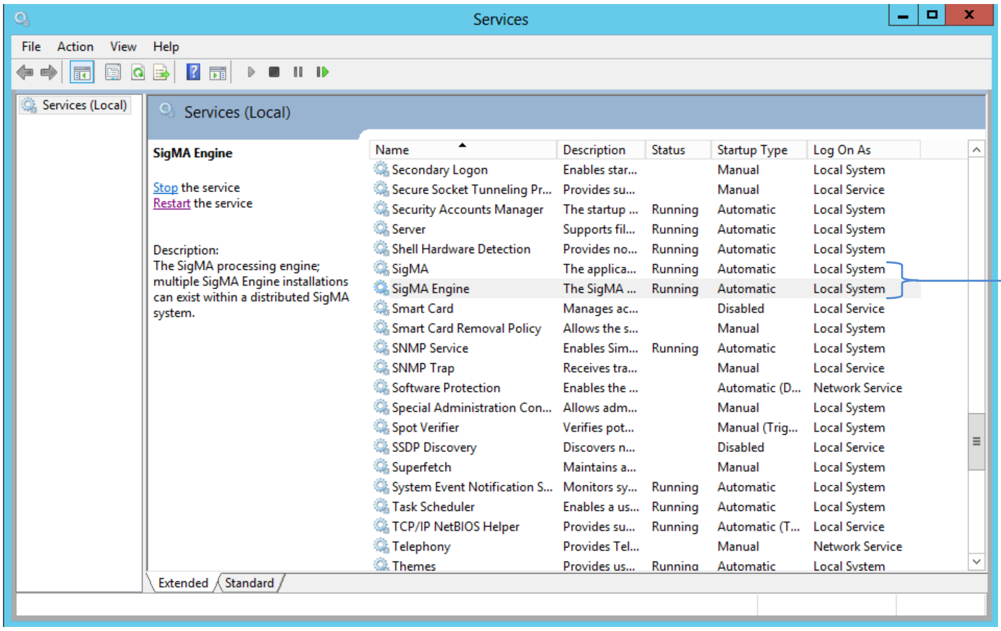


Completed the SigMA Setup Wizard

Click the Finish button to exit the Setup Wizard.

Click **Finish.**

Once the install process is completed, the SigMA and the SigMA Engine Services will start automatically and will run in the background.



SigMA Engine

Stop the service
Restart the service

Description:
The SigMA processing engine; multiple SigMA Engine installations can exist within a distributed SigMA system.

Name	Description	Status	Startup Type	Log On As
Secondary Logon	Enables star...		Manual	Local System
Secure Socket Tunneling Pr...	Provides su...		Manual	Local Service
Security Accounts Manager	The startup ...	Running	Automatic	Local System
Server	Supports fil...	Running	Automatic	Local System
Shell Hardware Detection	Provides no...	Running	Automatic	Local System
SigMA	The applica...	Running	Automatic	Local System
SigMA Engine	The SigMA ...	Running	Automatic	Local System
Smart Card	Manages ac...		Disabled	Local Service
Smart Card Removal Policy	Allows the s...		Manual	Local System
SNMP Service	Enables Sim...	Running	Automatic	Local System
SNMP Trap	Receives tra...		Manual	Local Service
Software Protection	Enables the ...		Automatic (D...	Network Service
Special Administration Con...	Allows adm...		Manual	Local System
Spot Verifier	Verifies pot...		Manual (Trig...	Local System
SSDP Discovery	Discovers n...		Disabled	Local Service
Superfetch	Maintains a...		Manual	Local System
System Event Notification S...	Monitors sy...	Running	Automatic	Local System
Task Scheduler	Enables a us...	Running	Automatic	Local System
TCP/IP NetBIOS Helper	Provides su...	Running	Automatic (T...	Local Service
Telephony	Provides Tel...		Manual	Network Service
Themes	Provides us...	Running	Automatic	Local System

SigMA Services

6. SigMA licensing

The various Media Assurance Services offer by SigMA are managed via three license tiers. All license tiers are packaged in bundles of 10 APs.

Table 2: License Types

License Type	Definition
SigMA Standard	Analysis of a single biometric signature to provide confidence monitoring
SigMA Professional	Comparison of two media biometric signatures to provide advanced media assurance and confidence monitoring. Includes Standard features
SigMA Enterprise	Playout specific Assurance Services offering integration with BioBank (Media Biometrics Database) via the BioBank Connector. Includes Standard and Professional Features
BioBank Connector	A singular license which connects a SigMA AP to the BioBank

Table 3: Assurance Services Comparison

Assurance Service	Standard	Professional	Enterprise
Average picture level	✓	✓	✓
Stillish	✓	✓	✓
Blackish	✓	✓	✓
Audio Activity	✓	✓	✓
Audio Level Meters	✓	✓	✓
Absolute Delay*	-	✓	✓
Lip Sync Match	-	✓	✓
Media Match	-	✓	✓
Quality Match	-	✓	✓
Channel Match	-	-	✓
Schedule Match	-	-	✓**
Media Identification	-	-	✓**

* Requires Signatures from an ICE or IQ MBG (devices which support PTP)

** Requires a BioBank and a BioBank Connector License

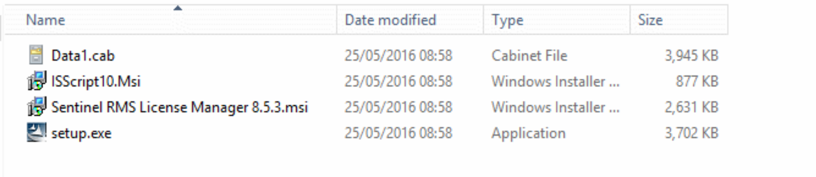
6.1 Installing the SigMA License Server

The License Server may be installed on the SigMA host machine or it can run on a separate PC/Server, on the same network that the SigMA application is running on.

The following steps are for a SigMA license service installation. The license Server installation can be found within the Safenet folder (folder within the Installer download package - see section 3 above).

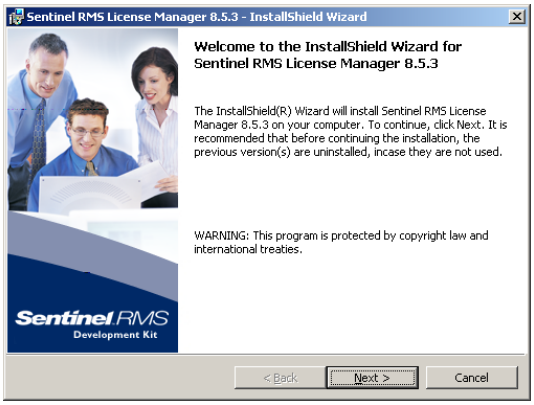
If the License Server is to be run on a separate machine, the Safenet folder should be copied and moved to the alternative PC/Server.

1. Locate the **Safenet** folder.
2. Double click on the Safenet folder.



Name	Date modified	Type	Size
Data1.cab	25/05/2016 08:58	Cabinet File	3,945 KB
ISScript10.Msi	25/05/2016 08:58	Windows Installer ...	877 KB
Sentinel RMS License Manager 8.5.3.msi	25/05/2016 08:58	Windows Installer ...	2,631 KB
setup.exe	25/05/2016 08:58	Application	3,702 KB

3. Double click on **setup.exe**,



Sentinel RMS License Manager 8.5.3 - InstallShield Wizard

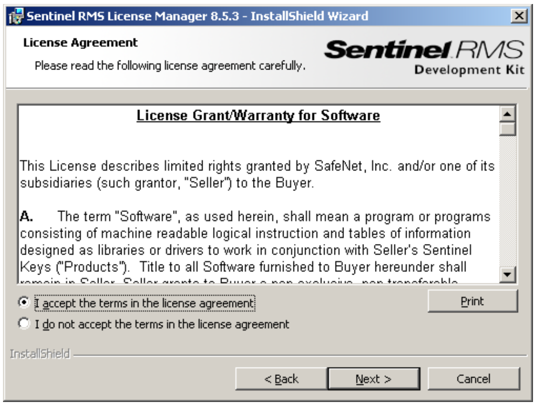
Welcome to the InstallShield Wizard for Sentinel RMS License Manager 8.5.3

The InstallShield(R) Wizard will install Sentinel RMS License Manager 8.5.3 on your computer. To continue, click Next. It is recommended that before continuing the installation, the previous version(s) are uninstalled, incase they are not used.

WARNING: This program is protected by copyright law and international treaties.

Click **Next**

4. **Accept** the license agreement.



Sentinel RMS License Manager 8.5.3 - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

License Grant/Warranty for Software

This License describes limited rights granted by SafeNet, Inc. and/or one of its subsidiaries (such grantor, "Seller") to the Buyer.

A. The term "Software", as used herein, shall mean a program or programs consisting of machine readable logical instruction and tables of information designed as libraries or drivers to work in conjunction with Seller's Sentinel Keys ("Products"). Title to all Software furnished to Buyer hereunder shall remain in Seller. Seller grants to Buyer a non-exclusive, non-transferable

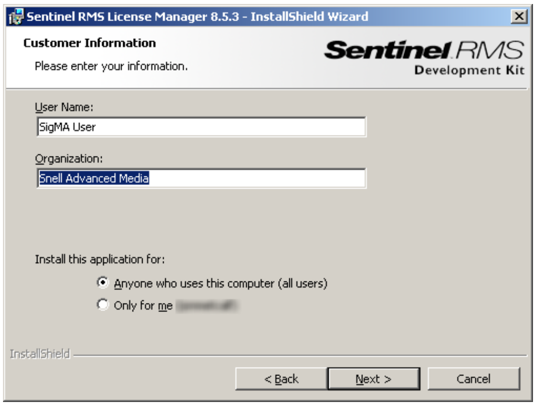
● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Click **Next**

5. When prompted add your Customer information.

   User name **SigMA User** has been used as an example.



Sentinel RMS License Manager 8.5.3 - InstallShield Wizard

Customer Information

Please enter your information.

User Name: SigMA User

Organization: Snell Advanced Media

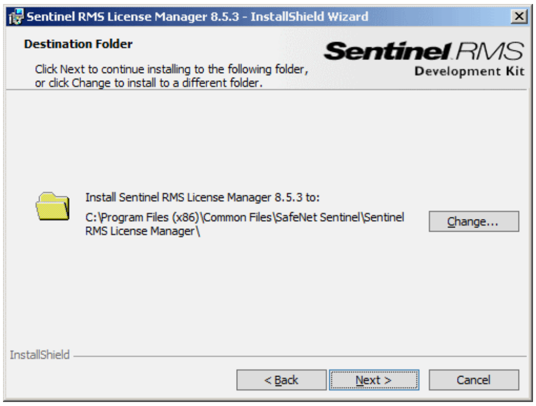
Install this application for:

● Anyone who uses this computer (all users)

○ Only for me [redacted]

   Click **Next**

6. The Installer will offer a choice of folder where Sentinel is installed.



Sentinel RMS License Manager 8.5.3 - InstallShield Wizard

Destination Folder

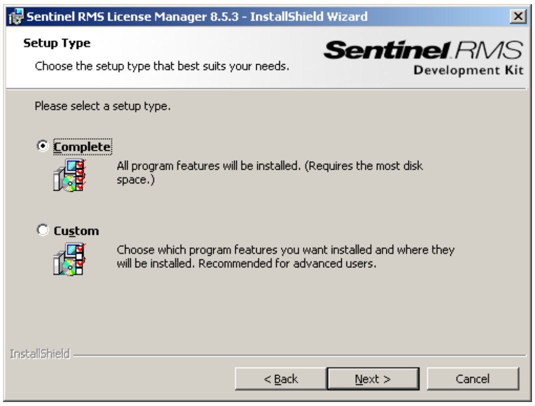
Click Next to continue installing to the following folder, or click Change to install to a different folder.

Install Sentinel RMS License Manager 8.5.3 to:
C:\Program Files (x86)\Common Files\SafeNet Sentinel\Sentinel RMS License Manager\

   Normal procedure is to use the default folder.

   Click **Next**

7. The **Setup Type** window will appear



Sentinel RMS License Manager 8.5.3 - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

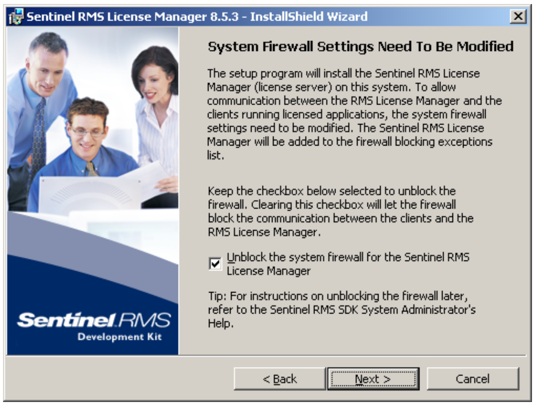
Please select a setup type.

● **Complete**
All program features will be installed. (Requires the most disk space.)

○ **Custom**
Choose which program features you want installed and where they will be installed. Recommended for advanced users.

   Leave the default setting (Complete) and click **Next**.

8. The **System Firewall Settings** windows will now appear.



System Firewall Settings Need To Be Modified

The setup program will install the Sentinel RMS License Manager (license server) on this system. To allow communication between the RMS License Manager and the clients running licensed applications, the system firewall settings need to be modified. The Sentinel RMS License Manager will be added to the firewall blocking exceptions list.

Keep the checkbox below selected to unblock the firewall. Clearing this checkbox will let the firewall block the communication between the clients and the RMS License Manager.

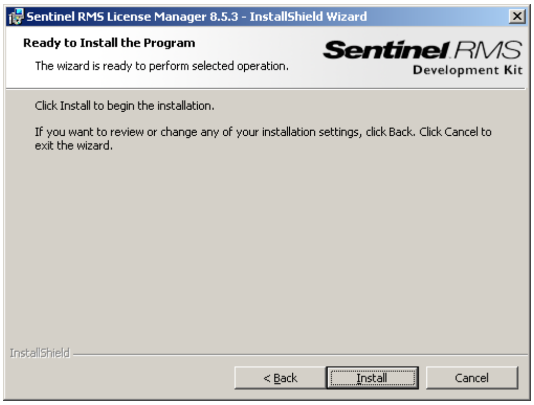
☑ Unblock the system firewall for the Sentinel RMS License Manager

Tip: For instructions on unblocking the firewall later, refer to the Sentinel RMS SDK System Administrator's Help.

By default the checkbox will be selected.

Click **Next**

9. The **Ready to Install** window will now appear.



Ready to Install the Program

The wizard is ready to perform selected operation.

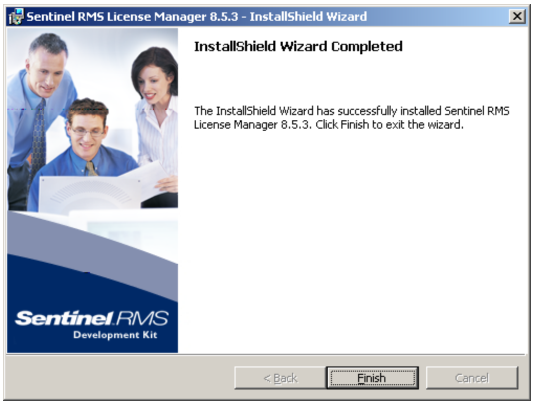
Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Click **Install.**

The Sentinel License Manager will now install.

10. When installation has completed, an **InterShield Wizard Completion** window will appear.



InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Sentinel RMS License Manager 8.5.3. Click Finish to exit the wizard.

Click **Finish** to complete the install process.

6.2 Accessing the Lock Code

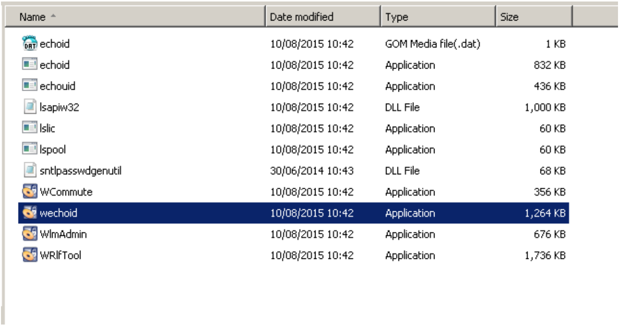
The lock code is required to activate a purchased license. The lock code is generated using unique hardware information from the host of the License Server. The License generated for this host will only work when installed on this host.

1. Log on to the host machine, where the License server is installed.

2. Navigate to the location:

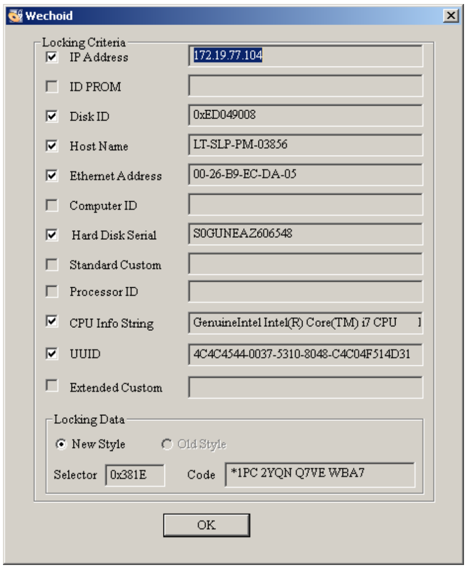
   c: > Program Files >SAM >SigMA > Licensing Tools

3. Locate and run the **wechoid** application.



Name	Date modified	Type	Size
echoid	10/08/2015 10:42	GOM Media file(.dat)	1 KB
echoid	10/08/2015 10:42	Application	832 KB
echouid	10/08/2015 10:42	Application	436 KB
lsapiw32	10/08/2015 10:42	DLL File	1,000 KB
lslic	10/08/2015 10:42	Application	60 KB
lspool	10/08/2015 10:42	Application	60 KB
sntlpasswdgenutil	30/06/2014 10:43	DLL File	68 KB
WCommute	10/08/2015 10:42	Application	356 KB
wechoid	10/08/2015 10:42	Application	1,264 KB
WlmAdmin	10/08/2015 10:42	Application	676 KB
WRlfTool	10/08/2015 10:42	Application	1,736 KB

4. The **Wechoid** window will now appear.



Wechoid

Locking Criteria

☑	IP Address	172.19.77.104
□	ID PROM	
☑	Disk ID	0xED049008
☑	Host Name	LT-SLP-PM-03856
☑	Ethernet Address	00-26-B9-EC-DA-05
□	Computer ID	
☑	Hard Disk Serial	S0GUNEAZ606548
□	Standard Custom	
□	Processor ID	
☑	CPU Info String	GenuineIntel Intel(R) Core(TM) i7 CPU I
☑	UUID	4C4C4544-0037-5310-8048-C4C04F514D31
□	Extended Custom	

Locking Data

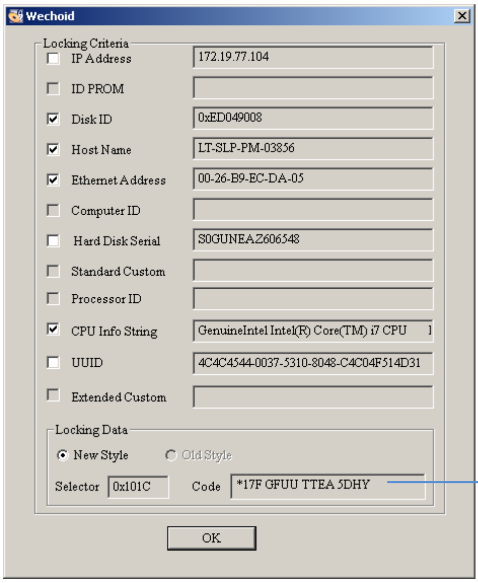
● New Style ○ Old Style

Selector 0x381E Code *1PC 2YQN Q7VE WBA7

SigMA uses four locking criteria:

- Disk ID
- Host Name
- Ethernet Address
- CPU Info String

Configure these four locking criteria:



Wechoid

Locking Criteria

□ IP Address	172.19.77.104
□ ID PROM	
☑ Disk ID	0xED049008
☑ Host Name	LT-SLP-PM-03856
☑ Ethernet Address	00-26-B9-EC-DA-05
□ Computer ID	
□ Hard Disk Serial	S0GUNEAZ606548
□ Standard Custom	
□ Processor ID	
☑ CPU Info String	GenuineIntel Intel(R) Core(TM) i7 CPU]
□ UUID	4C4C4544-0037-5310-8048-C4C04F514D31
□ Extended Custom	

Locking Data

● New Style ○ Old Style

Selector 0x101C Code *17F GFUU TTEA 5DHY

OK

Note that as each **Locking Criteria** item is selected/deselected, that the lock code is modified.

Lock Code

Select the four check boxes identified – this will create locking Data where the Selector is 0x101C and generates a Code that starts with an asterisk. The Code, including the asterisk, is the Locking Code.

The locking code needed to complete the licensing process.

Cut and paste the **License Server lock Code** into notepad, and give the file an appropriate name. This string will be used by to create your license.

Important!

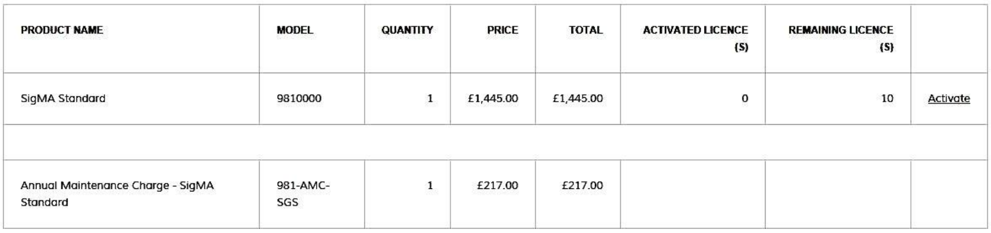
- The license will only work on the system the lock details were generated on.
- VM's (Virtual Machines) cannot be used to host the license server. For further information please contact SAM support.

6.3 Activating the License

The License can be activated via the SAM Store:

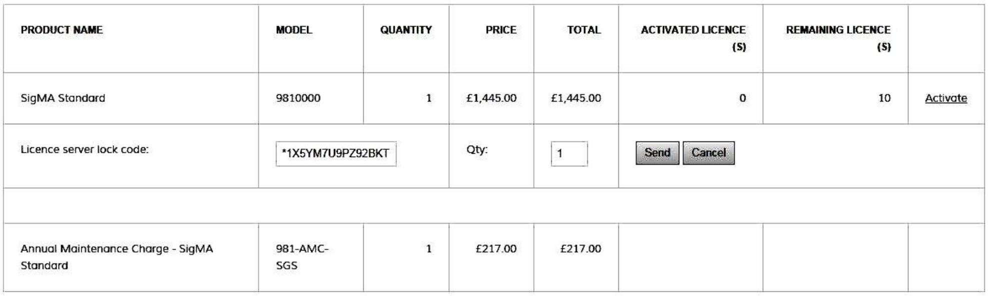
www.store.S-A-M.com

Go to your User Account area and locate the SigMA:



PRODUCT NAME	MODEL	QUANTITY	PRICE	TOTAL	ACTIVATED LICENCE (S)	REMAINING LICENCE (S)	
SigMA Standard	9810000	1	£1,445.00	£1,445.00	0	10	Activate
Annual Maintenance Charge - SigMA Standard	981-AMC-SGS	1	£217.00	£217.00			

Select **Activate.** The screen will update. Enter the lock code (generated in 4.2 above) in the appropriate field:

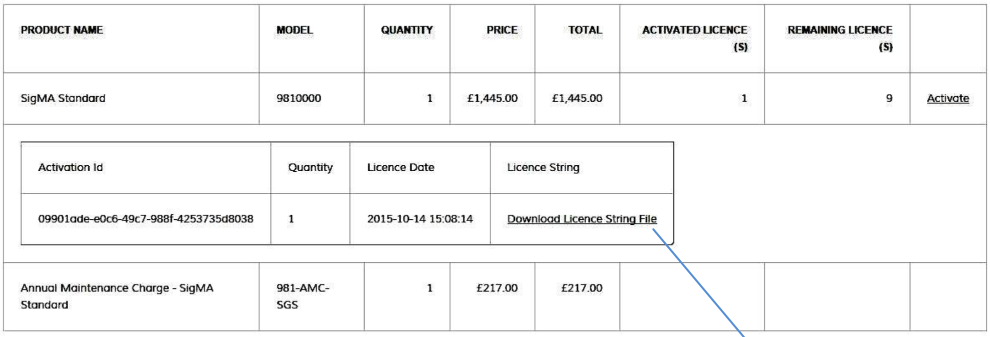


PRODUCT NAME	MODEL	QUANTITY	PRICE	TOTAL	ACTIVATED LICENCE (S)	REMAINING LICENCE (S)	
SigMA Standard	9810000	1	£1,445.00	£1,445.00	0	10	Activate
Licence server lock code:	*1X5YM7U9PZ92BKT		Qty:	1	Send Cancel		
Annual Maintenance Charge - SigMA Standard	981-AMC-SGS	1	£217.00	£217.00			

Note that licenses are issued only in batches of ten. Licenses can be activated one at a time, or if they are all relevant to a single license server, all ten will have the same lock-code and can be activated as a batch of ten.

In the above example, just one license is activated.

The screen will now update:



PRODUCT NAME	MODEL	QUANTITY	PRICE	TOTAL	ACTIVATED LICENCE (S)	REMAINING LICENCE (S)	
SigMA Standard	9810000	1	£1,445.00	£1,445.00	1	9	Activate
Annual Maintenance Charge - SigMA Standard	981-AMC-SGS	1	£217.00	£217.00			

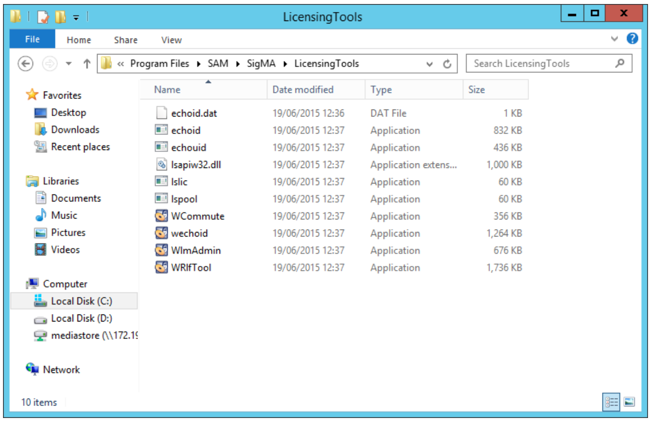
Activation Id	Quantity	Licence Date	Licence String
09901ade-e0c6-49c7-988f-4253735d8038	1	2015-10-14 15:08:14	Download Licence String File

Download License String File

Download the **License String File** and save it in an appropriate folder.

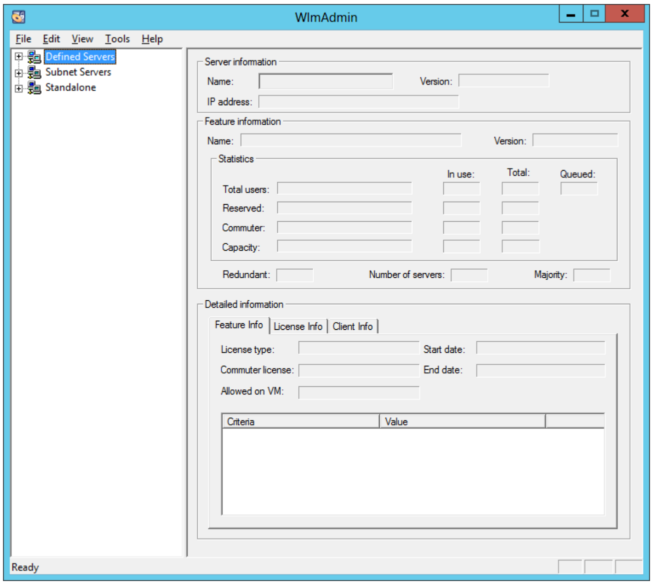
6.4 Applying License to License Server

1. Log on to the License Server host machine.
2. Using File Explorer navigate to **c: > Program Files / SAM / SigMA / Licensing Tools.**

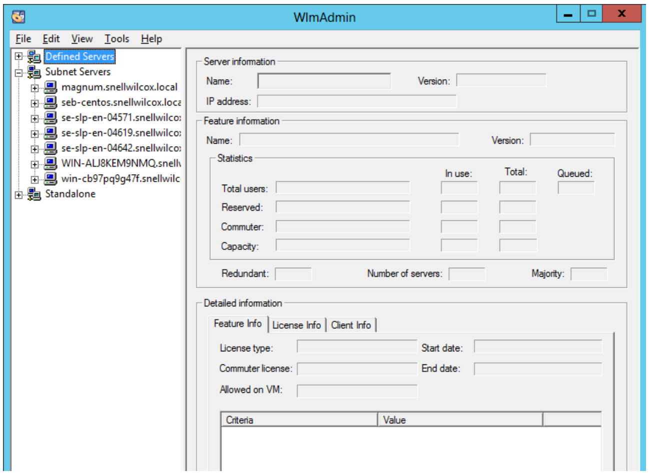


Name	Date modified	Type	Size
echoid.dat	19/06/2015 12:36	DAT File	1 KB
echoid	19/06/2015 12:37	Application	832 KB
echouid	19/06/2015 12:37	Application	436 KB
lsapiw32.dll	19/06/2015 12:37	Application extens...	1,000 KB
lslic	19/06/2015 12:37	Application	60 KB
lspool	19/06/2015 12:37	Application	60 KB
WCommute	19/06/2015 12:37	Application	356 KB
wechoid	19/06/2015 12:37	Application	1,264 KB
WlmAdmin	19/06/2015 12:37	Application	676 KB
WRlfTool	19/06/2015 12:37	Application	1,736 KB

3. Double click on the **WlmAdmin.exe.**
4. Click on the **+** icon next to **Subnet Servers** to expand the list.

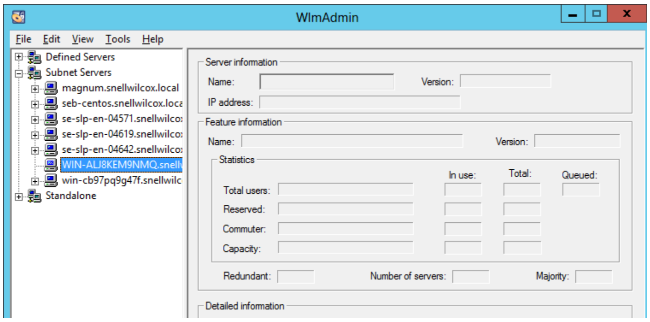


In this example there are a number of license servers running on the associated network.

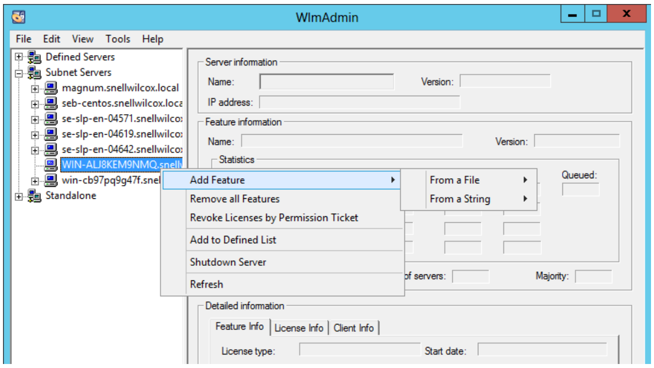


Select the appropriate Server

In this example 'WIN-ALJ8KE….' has been chosen.

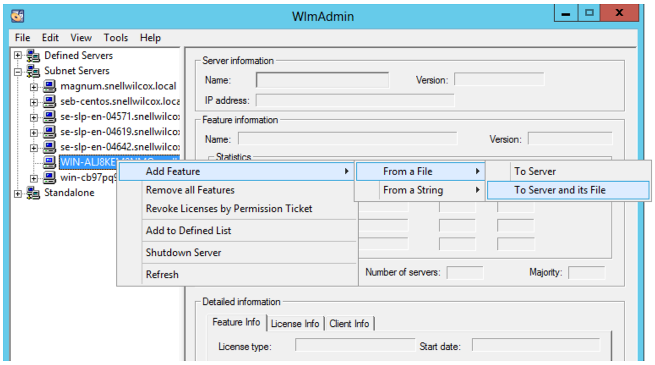


5. Right click the server then expand to **Add Feature > From a File**

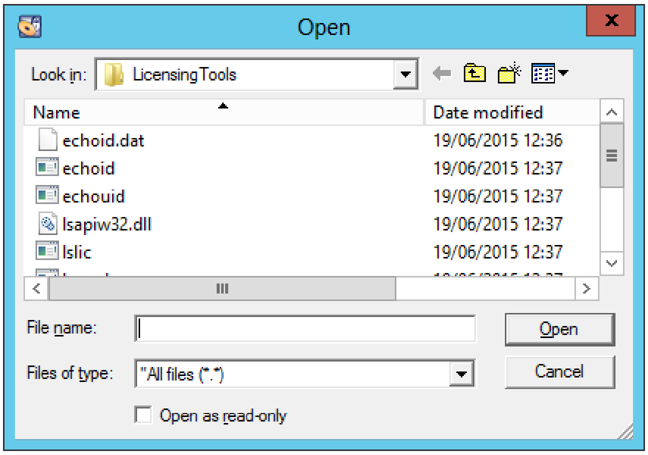


Choose the **From a File**.

Then choose **To Server and its File**



An **Open** window will now appear,



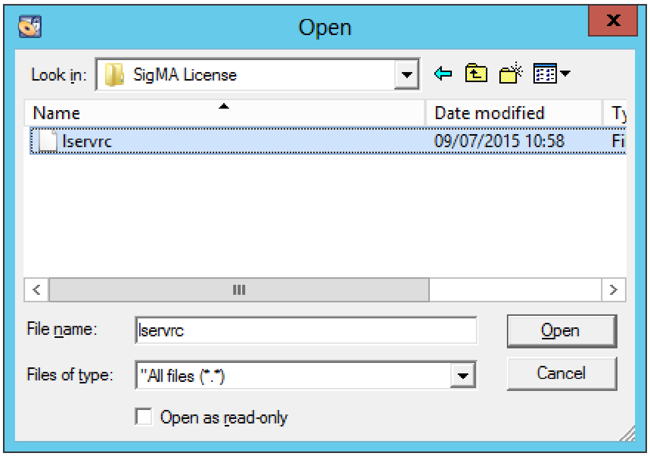
Look in: LicensingTools

Name	Date modified
echoid.dat	19/06/2015 12:36
echoid	19/06/2015 12:37
echouid	19/06/2015 12:37
lsapiw32.dll	19/06/2015 12:37
lslic	19/06/2015 12:37

File name:

Files of type: "All files (*.*)

6. Browse to the folder where the license file was downloaded to, in part 3.3 above.



Look in: SigMA License

Name	Date modified	Ty
lservrc	09/07/2015 10:58	Fi

File name: lservrc

Files of type: "All files (*.*)

Select the license file downloaded and click **Open**. A message should then be displayed stating the number of licenses successfully applied.

7. Controlling SigMA

The SigMA application does not have a dedicated control interface, but instead utilises RollCall Control Panel.

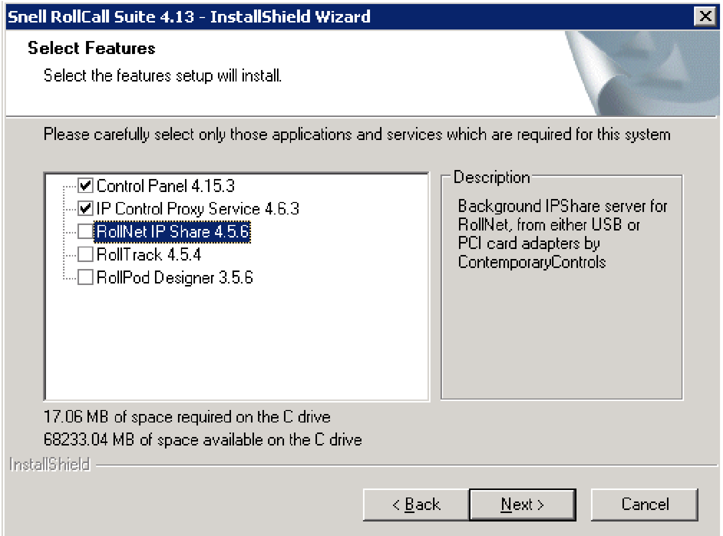
Note – this guide is not a RollCall tutorial.

Control Panel is a RollCall control application for the SAM product range and is available to SAM customers free of charge. To control SigMA it is first necessary to download and install Control Panel and associated RollCall applications.

Control Panel may be installed on the host PC, or on a remote PC with a network connection to the host machine.

Installation is very easy. Just launch the RollCall Suite Installer and follow the Install Wizard. Note that part way through the install process, you will be asked which RollCall components are to be installed. You can install all components if you wish, but from a SigMA perspective, the important components are:

- **Control Panel**
- **IP Control Proxy Service:**



Snell RollCall Suite 4.13 - InstallShield Wizard

Select Features

Select the features setup will install.

Please carefully select only those applications and services which are required for this system

☑ Control Panel 4.15.3
☑ IP Control Proxy Service 4.6.3
□ RollNet IP Share 4.5.6
□ RollTrack 4.5.4
□ RollPod Designer 3.5.6

Description

Background IPShare server for RollNet, from either USB or PCI card adapters by ContemporaryControls

17.06 MB of space required on the C drive

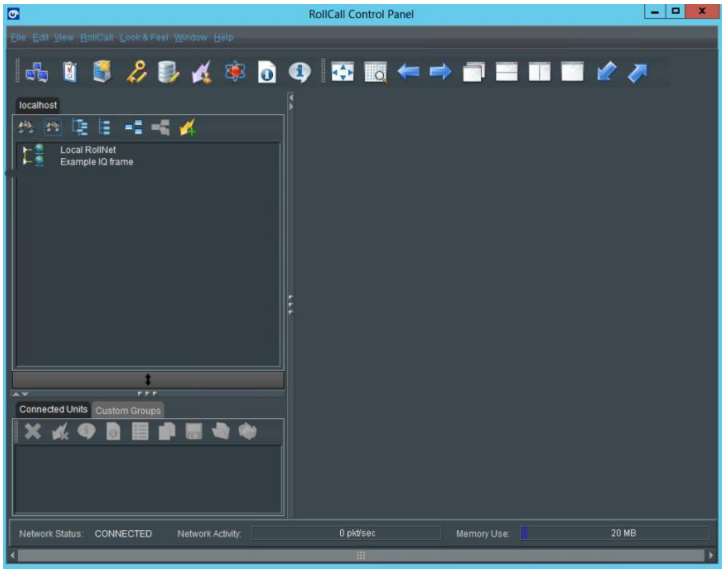
68233.04 MB of space available on the C drive

Follow the RollCall installer wizard to complete the process.

Once installed, control of SigMA is possible using either just the Control Panel or using the Control Panel via the IP Proxy Service. Just using Control Panel is a little easier to set up, but the IP Proxy service is more versatile and is the recommended method.

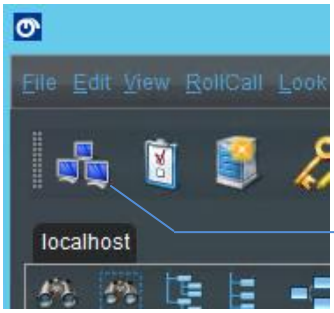
7.1 Using Control Panel Locally

1. If running Control Panel on the host PC (the PC that SigMA is running on), open RollCall Control Panel. Note that it will open connecting to ‘localhost’.



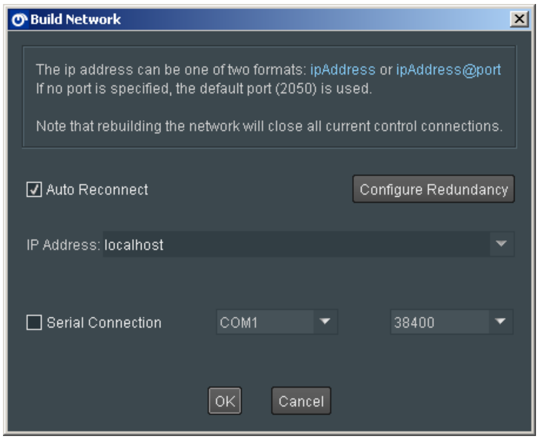
Note; there is no SigMA connection available.

2. Click on the **Connect to RollCall Network** icon.



Connect to RollCall Network

The **Build Network** window will now appear.



The ip address can be one of two formats: ipAddress or ipAddress@port
If no port is specified, the default port (2050) is used.

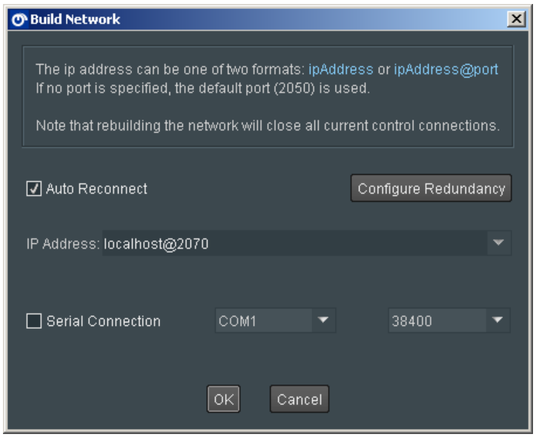
Note that rebuilding the network will close all current control connections.

☑ Auto Reconnect

IP Address: localhost

□ Serial Connection COM1 38400

3. The SigMA default port 2070 so it is necessary to edit the IP Address field accordingly.



The ip address can be one of two formats: ipAddress or ipAddress@port
If no port is specified, the default port (2050) is used.

Note that rebuilding the network will close all current control connections.

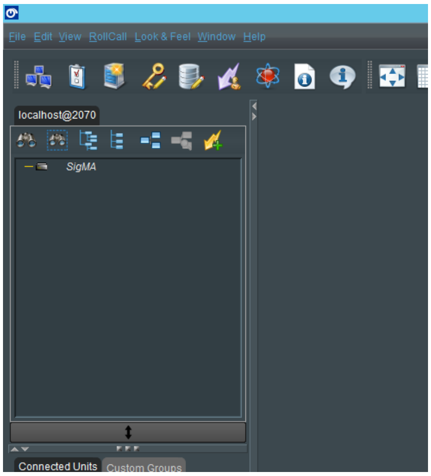
☑ Auto Reconnect

IP Address: localhost@2070

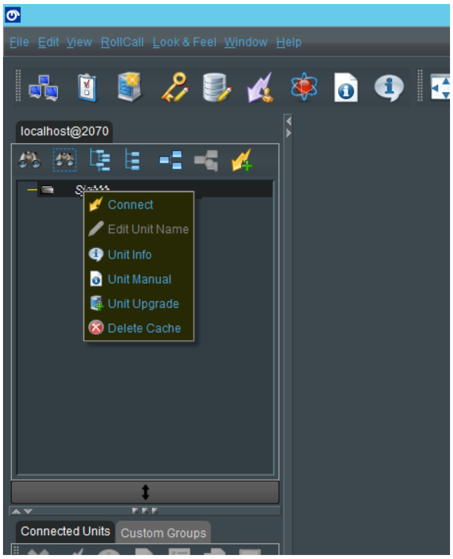
□ Serial Connection COM1 38400

Note that the port can be changed in the SigMA Setup menu. See section 7.5 below for more info

If SigMA is running as a Service on the host machine, the SigMA connection icon will be seen in the connection pane of Control Panel.

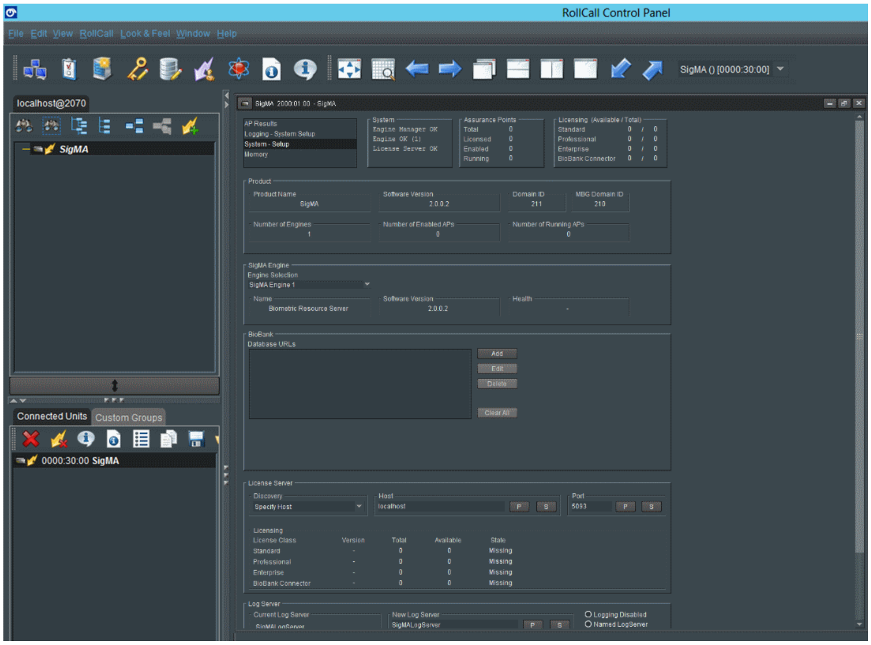


4. Right click on the SigMA icon.



A submenu will now appear. Select **Connect.**

The SigMA template will now load.



System
Engine Manager OK
Engine OK (1)
License Server OK

Assurance Points	
Total	0
Licensed	0
Enabled	0
Running	0

Licensing (Available / Total)			
Standard	0	/	0
Professional	0	/	0
Enterprise	0	/	0
BioBank Connector	0	/	0

Product

Product Name: SigMA

Software Version: 2.0.0.2

Domain ID: 211

MBG Domain ID: 210

Number of Engines: 1

Number of Enabled APs: 0

Number of Running APs: 0

SigMA Engine

Engine Selection: SigMA Engine 1

Name: Biometric Resource Server

Software Version: 2.0.0.2

Health: -

BioBank

Database URLs

License Server

Discovery: Specify Host

Host: localhost

Port: 5093

Licensing

License Class	Version	Total	Available	State
Standard	-	0	0	Missing
Professional	-	0	0	Missing
Enterprise	-	0	0	Missing
BioBank Connector	-	0	0	Missing

Log Server

Current Log Server: SigMALogServer

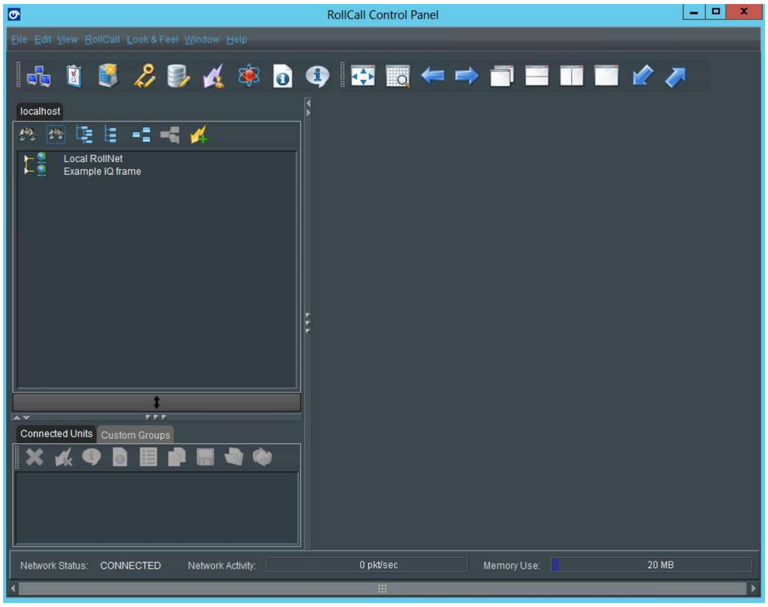
New Log Server: SigMALogServer

○ Logging Disabled

○ Named LogServer

7.2 Using Control Panel Remotely

1. If running Control Panel on a remote PC on the same network as the SigMA host machine, open RollCall Control Panel:

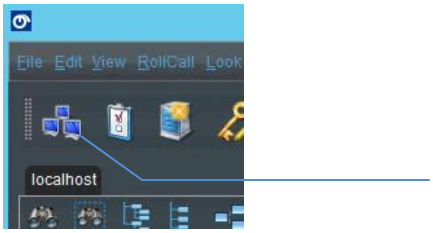


Local RollNet
Example IQ frame

Network Status: CONNECTED Network Activity: 0 pkt/sec Memory Use: 20 MB

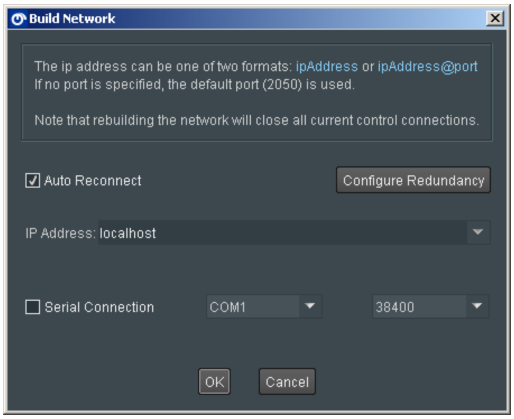
Note there is no SigMA connection in the Connection Window.

2. Click on the **Connect to RollCall Network** icon



Connect to
RollCall

The **Build Network** window will now appear



The ip address can be one of two formats: ipAddress or ipAddress@port
If no port is specified, the default port (2050) is used.

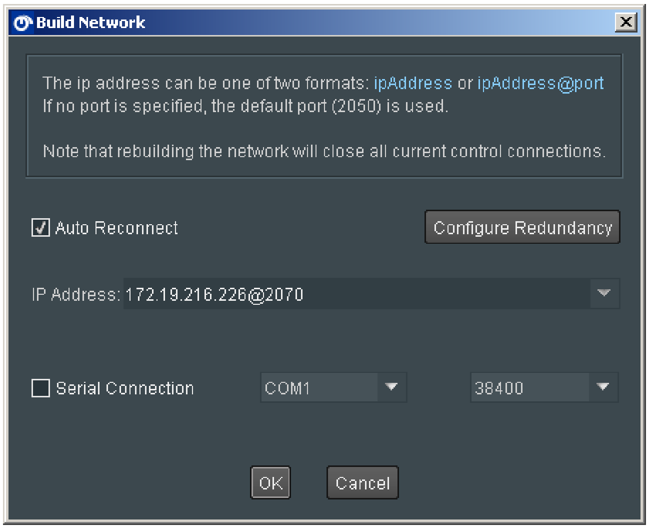
Note that rebuilding the network will close all current control connections.

☑ Auto Reconnect

IP Address: localhost

□ Serial Connection COM1 38400

3. Edit the **IP Address** box with the IP Address of the SigMA host PC.



The ip address can be one of two formats: ipAddress or ipAddress@port
If no port is specified, the default port (2050) is used.

Note that rebuilding the network will close all current control connections.

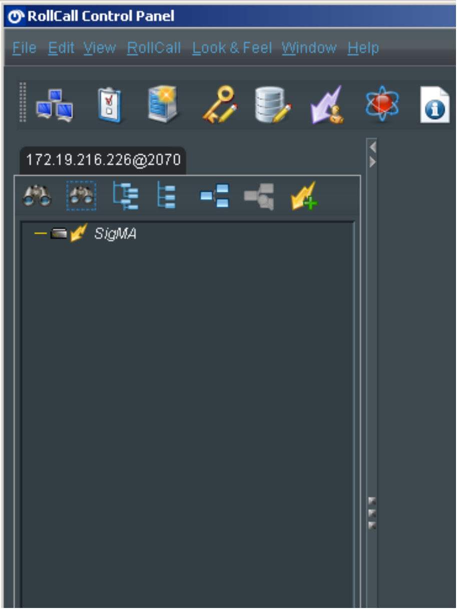
☑ Auto Reconnect

IP Address: 172.19.216.226@2070

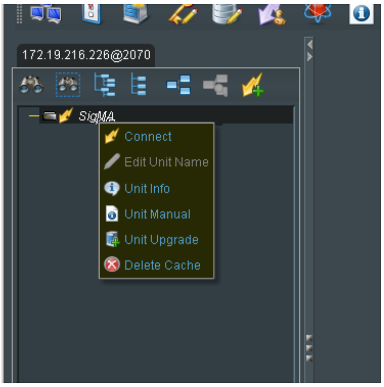
☐ Serial Connection COM1 38400

Click OK

The SigMA connection option should now appear in the connection window.

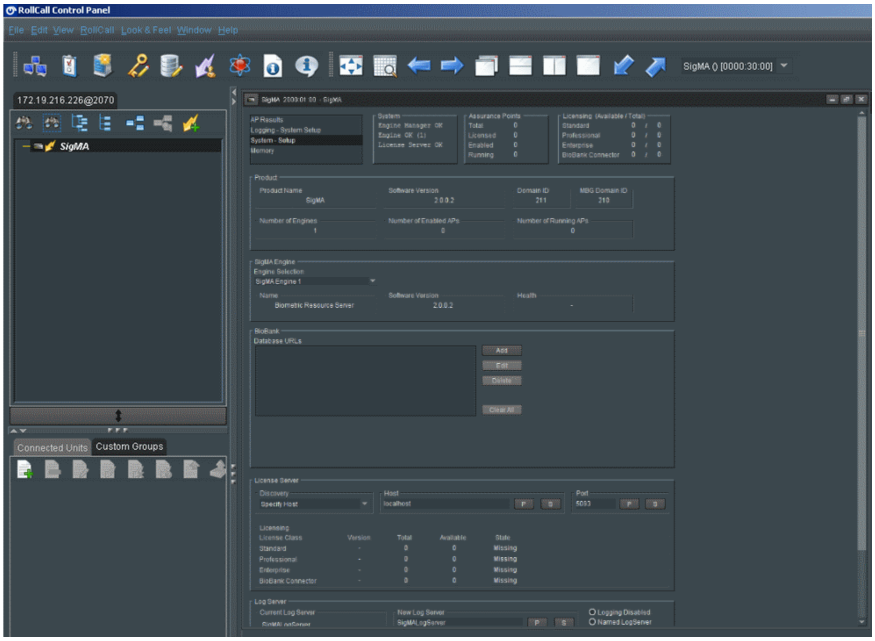


4. Right click on the SigMA icon



A submenu will now appear. Select **Connect.**

The SigMA template will now load.



System
Engine Manager OK
Engine OK (1)
License Server OK

Assurance Points	
Total	0
Licensed	0
Enabled	0
Running	0

Licensing (Available / Total)			
Standard	0	/	0
Professional	0	/	0
Enterprise	0	/	0
BioBank Connector	0	/	0

Product

Product Name	Software Version	Domain ID	MBG Domain ID
SigMA	2.0.0.2	211	210

Number of Engines	Number of Enabled APs	Number of Running APs
1	0	0

SigMA Engine
Engine Selection: SigMA Engine 1

Name	Software Version	Health
Biometric Resource Server	2.0.0.2	-

BioBank
Database URLs

License Server
Discovery: Specify Host
Host: localhost
Port: 5093

Licensing

License Class	Version	Total	Available	State
Standard	-	0	0	Missing
Professional	-	0	0	Missing
Enterprise	-	0	0	Missing
BioBank Connector	-	0	0	Missing

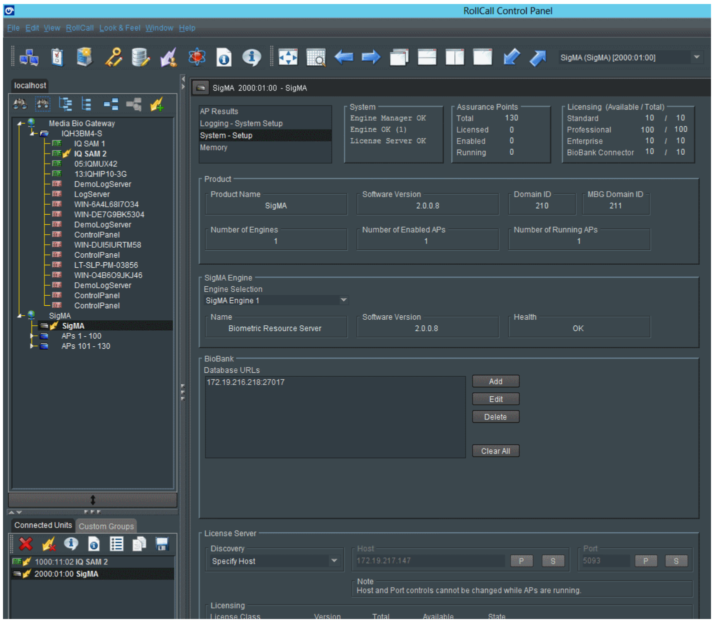
Log Server
Current Log Server: SigMALogServer
New Log Server: SigMALogServer
○ Logging Disabled
○ Named LogServer

7.3 Using Control Panel via IP Control Proxy Service

The following procedure will describe how to set up RollCall IP Control Proxy Service, on a remote PC on the same network as the SigMA host machine.

Note that the advantage of using the IP Control Proxy Service is that control of multiple SAM products can be managed from a single RollCall control panel session, without the need to keep changing the connection IP Address. By using IP Control Proxy Service, Control Panel can be set to Localhost and all devices configured in the IP Control Proxy Service will be visible in the connection pane of Control Panel.

In the following example Control Panel has connections to both a SigMA running on a remote server and an IQ frame, containing an IQSAM00 module:



System
Engine Manager OK
Engine OK (1)
License Server OK

Assurance Points

Total	130
Licensed	0
Enabled	0
Running	0

Licensing (Available / Total)

Standard	10	/	10
Professional	100	/	100
Enterprise	10	/	10
BioBank Connector	10	/	10

Product

Product Name: SigMA
Software Version: 2.0.0.8
Domain ID: 210
MBG Domain ID: 211
Number of Engines: 1
Number of Enabled APs: 1
Number of Running APs: 1

SigMA Engine

Engine Selection: SigMA Engine 1
Name: Biometric Resource Server
Software Version: 2.0.0.8
Health: OK

BioBank

Database URLs: 172.19.216.218:27017

License Server

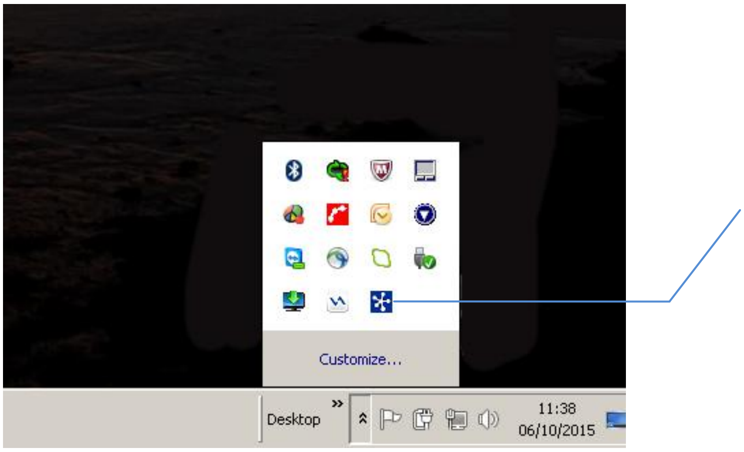
Discovery: Specify Host
Host: 172.19.217.147
Port: 5093
Note: Host and Port controls cannot be changed while APs are running.

Licensing

License Class Version Total Available State

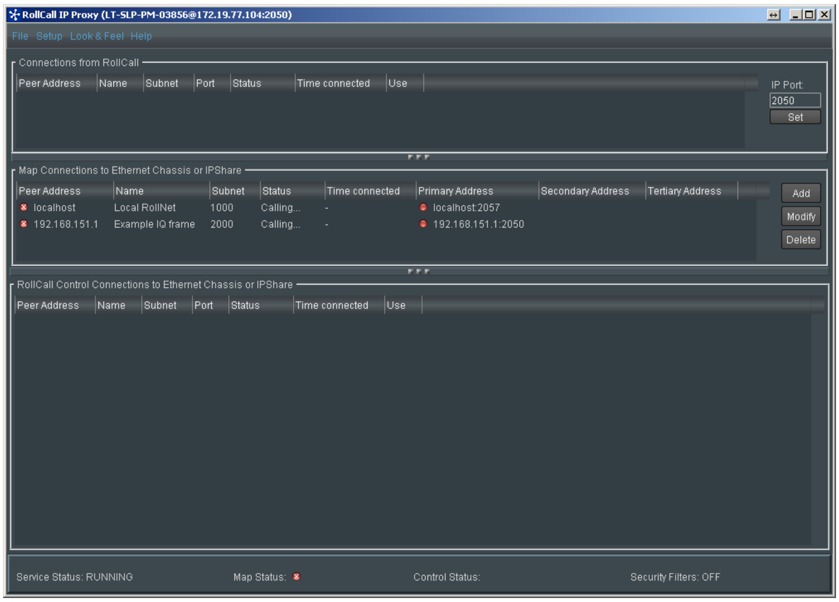
1. The RollCall IP Control Proxy Service will start automatically upon boot up of the host PC.

   Click the ‘Show Hidden Icons’ button on the task bar.



RollCall IP Control Proxy Service

Select the **RollCall IP Control Proxy Service** icon. The **RollCall IP Control Proxy Service** window will now open.



Connections from RollCall

Peer Address	Name	Subnet	Port	Status	Time connected	Use

IP Port: 2050

Map Connections to Ethernet Chassis or IPShare

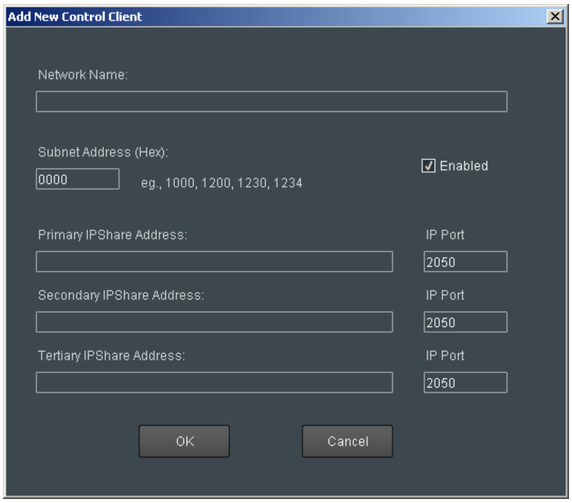
Peer Address	Name	Subnet	Status	Time connected	Primary Address	Secondary Address	Tertiary Address
☒ localhost	Local RollNet	1000	Calling...	-	● localhost:2057		
☒ 192.168.151.1	Example IQ frame	2000	Calling...	-	● 192.168.151.1:2050		

RollCall Control Connections to Ethernet Chassis or IPShare

Peer Address	Name	Subnet	Port	Status	Time connected	Use

Service Status: RUNNING Map Status: ☒ Control Status: Security Filters: OFF

2. In the **Map Connections to Ethernet Chassis or IPShare** window, click on **Add.** The **Add New Control Client** window will now appear.



Network Name:

Subnet Address (Hex): 0000 eg., 1000, 1200, 1230, 1234

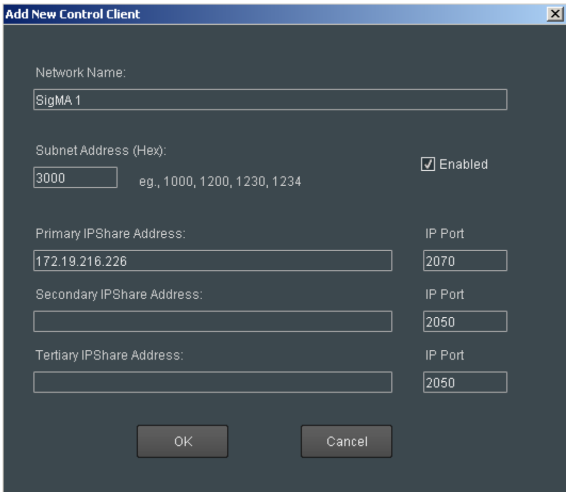
☑ Enabled

Primary IPShare Address: IP Port 2050

Secondary IPShare Address: IP Port 2050

Tertiary IPShare Address: IP Port 2050

3. Populate the **Add New Control Client** window:



Add New Control Client

Network Name: SigMA 1

Subnet Address (Hex): 3000 eg., 1000, 1200, 1230, 1234

☑ Enabled

Primary IPShare Address: 172.19.216.226 IP Port 2070

Secondary IPShare Address: IP Port 2050

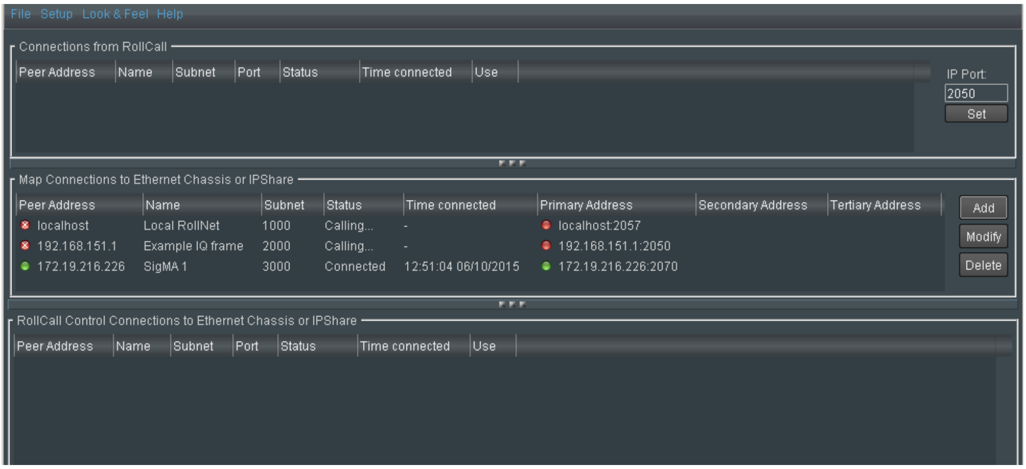
Tertiary IPShare Address: IP Port 2050

- **Network Name:** This is a unique name just for identification purposes.
- **Subset Address (Hex):** This can be anything but must be unique. In this example **3000** has been set.
- **Primary IPShare Address:** This is the IP address of the SigMA host PC.
- **IP Port** This is the port specified for SigMA. The default port is **2070.**

All other settings may be left in default.

Click **OK.**

The **Map Connections to Ethernet Chassis or IPShare** widow should now show SigMA with the status indicating **Connected.** In this example the SigMA name has been specified as SigMA 1.



Connections from RollCall

Peer Address	Name	Subnet	Port	Status	Time connected	Use

IP Port: 2050

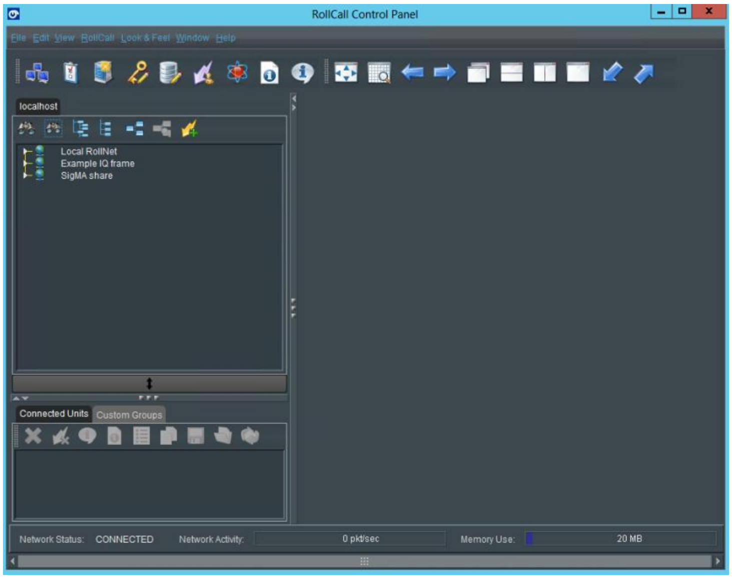
Map Connections to Ethernet Chassis or IPShare

Peer Address	Name	Subnet	Status	Time connected	Primary Address	Secondary Address	Tertiary Address
☒ localhost	Local RollNet	1000	Calling...	-	● localhost:2057		
☒ 192.168.151.1	Example IQ frame	2000	Calling...	-	● 192.168.151.1:2050		
● 172.19.216.226	SigMA 1	3000	Connected	12:51:04 06/10/2015	● 172.19.216.226:2070		

RollCall Control Connections to Ethernet Chassis or IPShare

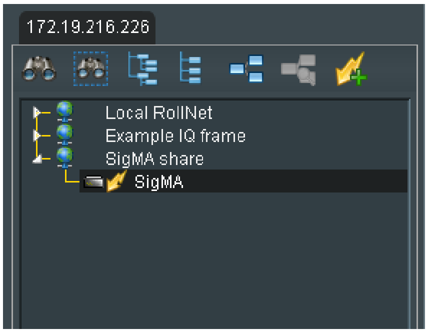
Peer Address	Name	Subnet	Port	Status	Time connected	Use

4. Open **Control Panel** on the remote PC

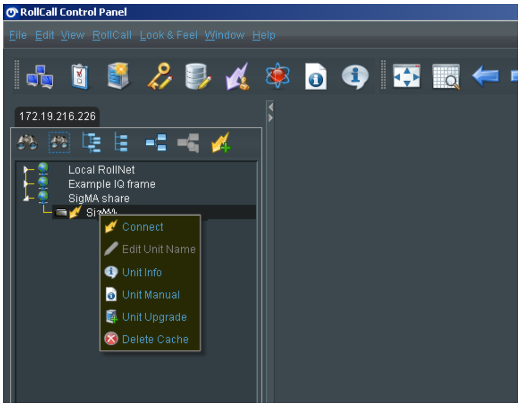


Note that **Connection** pane is connecting to **Localhost**, not a specified IP address.

5. Double click on SigMA Share and SigMA will now be shown.

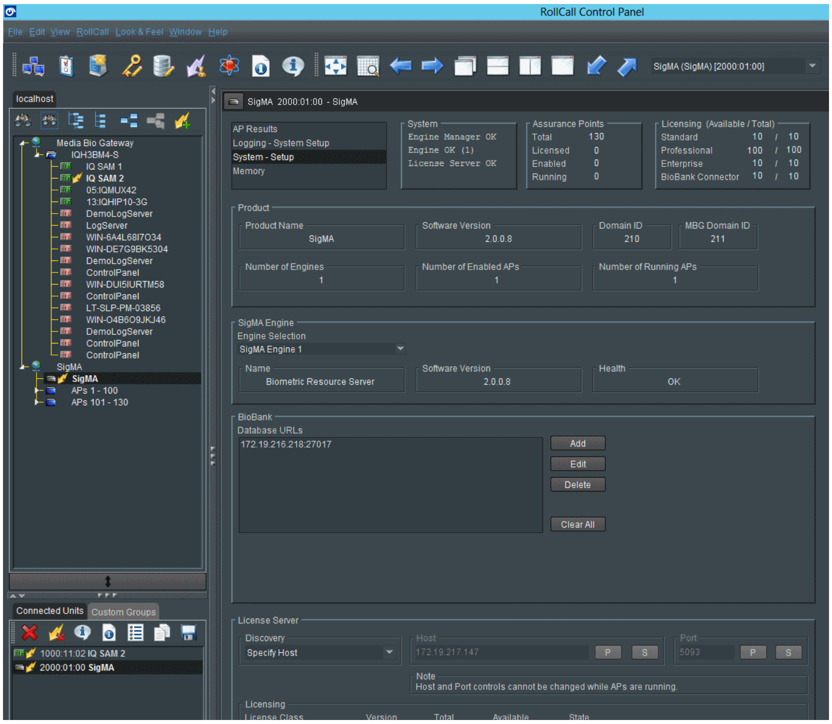


6. Right click on the SigMA icon



A submenu will now appear. Select **Connect.**

The SigMA template will now load.



Media Bio Gateway
IQH3BM4-S
IQ SAM 1
IQ SAM 2
05:IQMUX42
13:IQHIP10-3G
DemoLogServer
LogServer
WIN-6A4L68I7O34
WIN-DE7G9BK5304
DemoLogServer
ControlPanel
WIN-DUI5IURTM58
ControlPanel
LT-SLP-PM-03856
WIN-O4B6O9JKJ46
DemoLogServer
ControlPanel
ControlPanel
SigMA
SigMA
APs 1 - 100
APs 101 - 130

1000:11:02 IQ SAM 2
2000:01:00 SigMA

SigMA 2000:01:00 - SigMA

AP Results
Logging - System Setup
System - Setup
Memory

System
Engine Manager OK
Engine OK (1)
License Server OK

Assurance Points

Total	130
Licensed	0
Enabled	0
Running	0

Licensing (Available / Total)

Standard	10	/	10
Professional	100	/	100
Enterprise	10	/	10
BioBank Connector	10	/	10

Product

Product Name: SigMA
Software Version: 2.0.0.8
Domain ID: 210
MBG Domain ID: 211
Number of Engines: 1
Number of Enabled APs: 1
Number of Running APs: 1

SigMA Engine

Engine Selection: SigMA Engine 1
Name: Biometric Resource Server
Software Version: 2.0.0.8
Health: OK

BioBank

Database URLs
172.19.216.218:27017

License Server

Discovery: Specify Host
Host: 172.19.217.147
Port: 5093

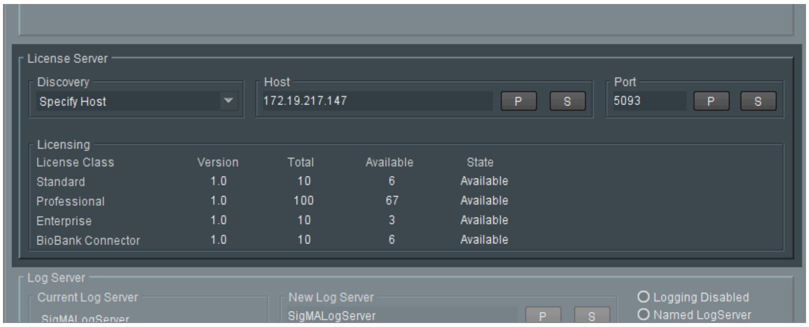
Note
Host and Port controls cannot be changed while APs are running.

Licensing

License Class	Version	Total	Available	State

8. Connecting to the SigMA License server

Once the template has been loaded SigMA can be connected to the License Server. Once connected, the **Total** and **Available** number of licenses can be reviewed within **System – Setup** menu.



License Server

Discovery: Specify Host

Host: 172.19.217.147

Port: 5093

Licensing

License Class	Version	Total	Available	State
Standard	1.0	10	6	Available
Professional	1.0	100	67	Available
Enterprise	1.0	10	3	Available
BioBank Connector	1.0	10	6	Available

Log Server

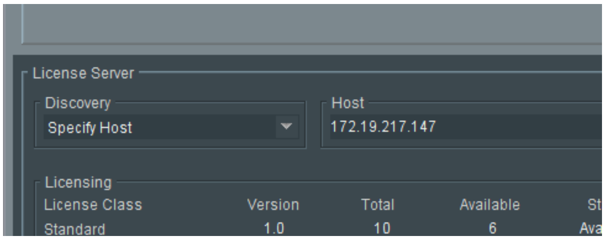
Current Log Server: SigMALogServer

New Log Server: SigMALogServer

○ Logging Disabled

○ Named LogServer

The **Discovery** field supports **Specify Host** and this is the default



License Server

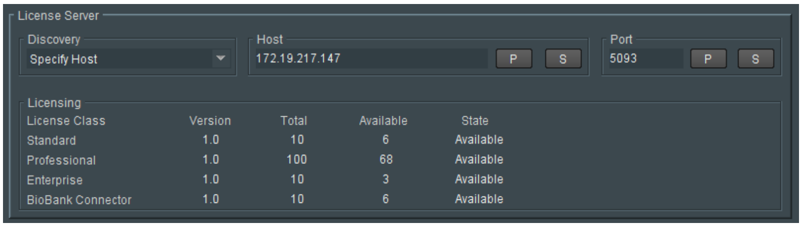
Discovery: Specify Host

Host: 172.19.217.147

Licensing

License Class	Version	Total	Available	St
Standard	1.0	10	6	Ava

Here is an example of a successfully connected License server



License Server

Discovery: Specify Host

Host: 172.19.217.147

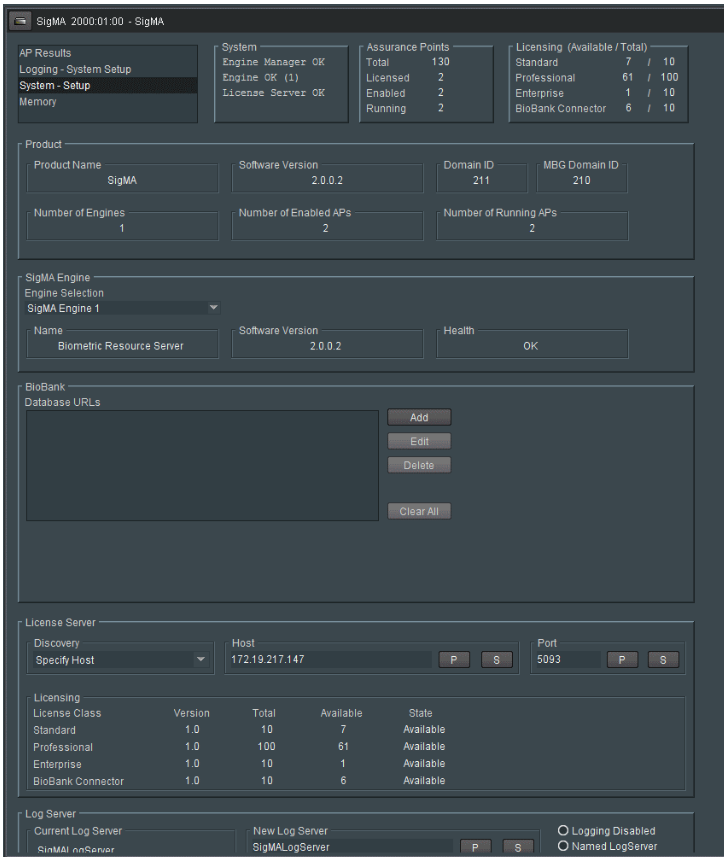
Port: 5093

Licensing

License Class	Version	Total	Available	State
Standard	1.0	10	6	Available
Professional	1.0	100	68	Available
Enterprise	1.0	10	3	Available
BioBank Connector	1.0	10	6	Available

If the License Server is running on the SigMA host machine, the **Host** can be specified as Localhost

9. SigMA System Setup



System
Engine Manager OK
Engine OK (1)
License Server OK

Assurance Points	
Total	130
Licensed	2
Enabled	2
Running	2

Licensing (Available / Total)			
Standard	7	/	10
Professional	61	/	100
Enterprise	1	/	10
BioBank Connector	6	/	10

Product
Product Name: SigMA
Software Version: 2.0.0.2
Domain ID: 211
MBG Domain ID: 210
Number of Engines: 1
Number of Enabled APs: 2
Number of Running APs: 2

SigMA Engine
Engine Selection: SigMA Engine 1
Name: Biometric Resource Server
Software Version: 2.0.0.2
Health: OK

BioBank
Database URLs

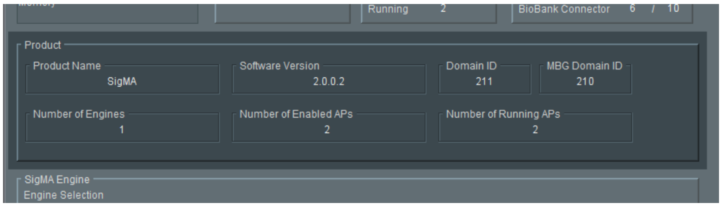
License Server
Discovery: Specify Host
Host: 172.19.217.147
Port: 5093

Licensing

License Class	Version	Total	Available	State
Standard	1.0	10	7	Available
Professional	1.0	100	61	Available
Enterprise	1.0	10	1	Available
BioBank Connector	1.0	10	6	Available

Log Server
Current Log Server: SigMALogServer
New Log Server: SigMALogServer
○ Logging Disabled
○ Named LogServer

9.1 Product



Running 2
BioBank Connector 6 / 10

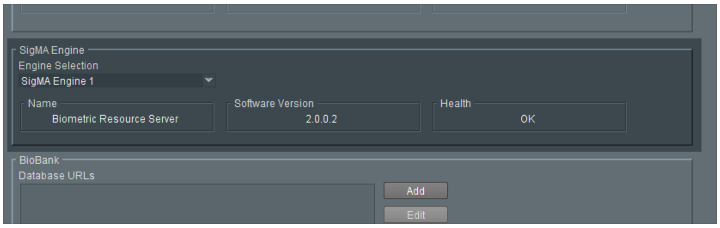
Product
Product Name: SigMA
Software Version: 2.0.0.2
Domain ID: 211
MBG Domain ID: 210
Number of Engines: 1
Number of Enabled APs: 2
Number of Running APs: 2

SigMA Engine
Engine Selection

This is just an information field. Here will be reported:

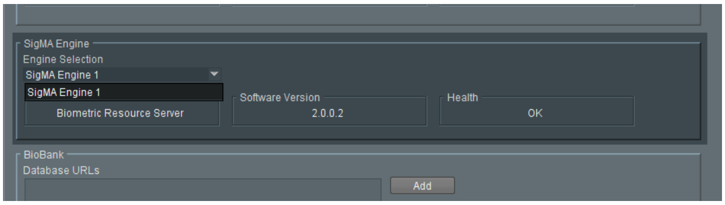
- Product Name
- Software version
- Domain ID
- Number of Engines
- Number of Enabled APs
- Number of Running APs

9.2 SigMA Engine


SigMA Engine
Engine Selection: SigMA Engine 1
Name: Biometric Resource Server
Software Version: 2.0.0.2
Health: OK
BioBank
Database URLs

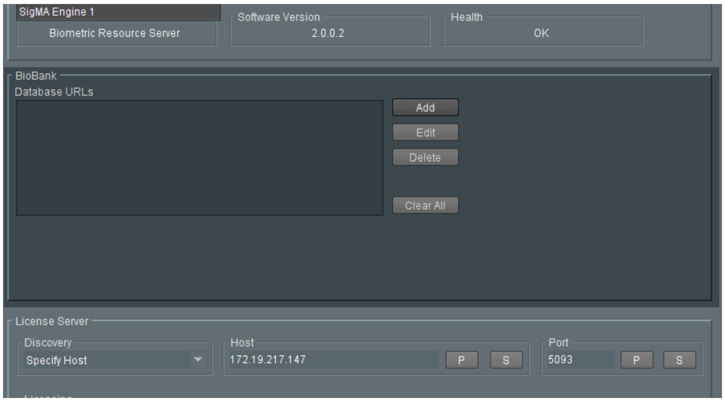
This field reports parameters of a specific SigMA Engine.

The specific SigMA Engine can be selected from a drop-down menu:


SigMA Engine
Engine Selection: SigMA Engine 1
SigMA Engine 1
Biometric Resource Server
Software Version: 2.0.0.2
Health: OK
BioBank
Database URLs

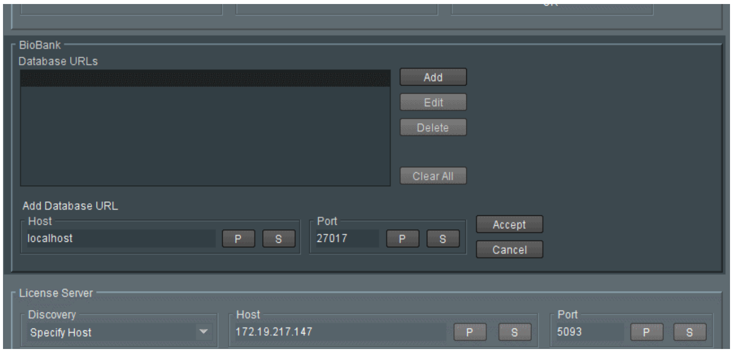
Once a specific SigMA Engine is selected, the SigMA Engine field will report the **Software Version** and the **Health** of the selected Engine.

9.3 BioBank (Media Biometrics DataBase)


SigMA Engine 1
Biometric Resource Server
Software Version: 2.0.0.2
Health: OK
BioBank
Database URLs
License Server
Discovery: Specify Host
Host: 172.19.217.147
Port: 5093

The BioBank is a Database of Media Biometric Signatures that is required for specific features such Schedule Match and Media Match. To Connect an Assurance point to a BioBank a BioBank Connector is required. This enables comparisons to be made from a live signature with Signatures which have been pre-ingested into the Database using MBG XF.

To add a BioBank click **Add.** A new field will become visible titled **Add Database URL:**



BioBank

Database URLs

Add Database URL

Host: localhost

Port: 27017

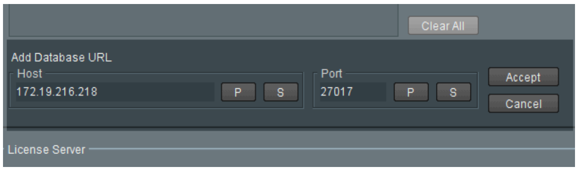
License Server

Discovery: Specify Host

Host: 172.19.217.147

Port: 5093

Enter the IP Address (or a resolved name can be used) of the host machine where the BioBank resides:



Add Database URL

Host: 172.19.216.218

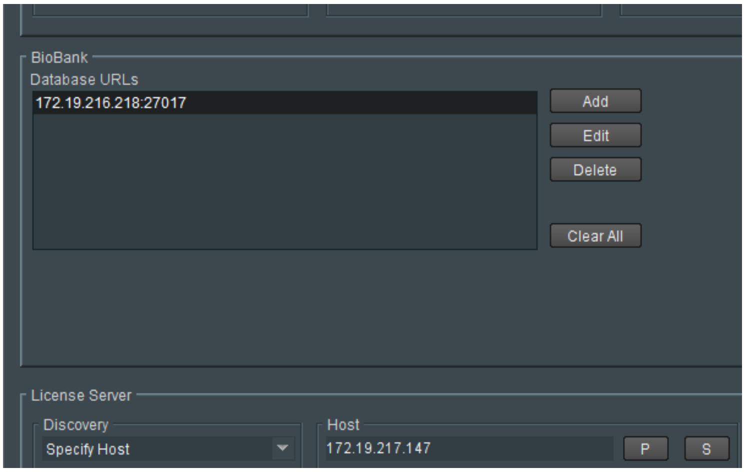
Port: 27017

License Server

Note that the **Port** is already set the default value: 27017. If the BioBank has been configured with an alternative Port, then the connection should be configured to this alternative Port.

Select **Accept.**

The BioBank Database URL should now appear in the BioBank main window:



BioBank

Database URLs

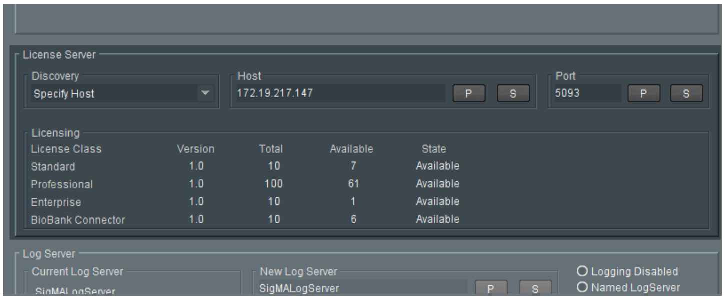
172.19.216.218:27017

License Server

Discovery: Specify Host

Host: 172.19.217.147

9.4 License Server


License Server

Discovery: Specify Host

Host: 172.19.217.147

Port: 5093

Licensing

License Class	Version	Total	Available	State
Standard	1.0	10	7	Available
Professional	1.0	100	61	Available
Enterprise	1.0	10	1	Available
BioBank Connector	1.0	10	6	Available

Log Server

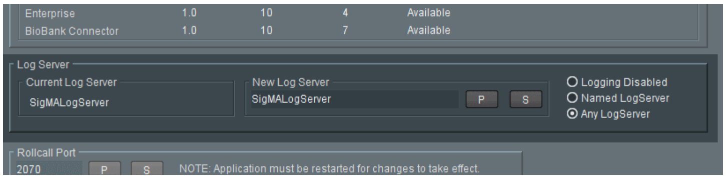
Current Log Server: SigMALogServer

New Log Server: SigMALogServer

○ Logging Disabled
○ Named LogServer

This field reports the status of the License Server.

9.5 Log Server


Enterprise	1.0	10	4	Available
BioBank Connector	1.0	10	7	Available

Log Server

Current Log Server: SigMALogServer

New Log Server: SigMALogServer

○ Logging Disabled
○ Named LogServer
● Any LogServer

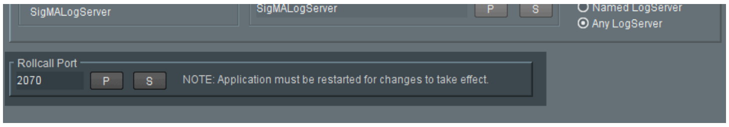
Rollcall Port: 2070

NOTE: Application must be restarted for changes to take effect.

Here the status of the Log Server is displayed.

In this field, a specific Log Server can be specified, or Logging can be disabled.

9.6 RollCall Port


SigMALogServer

SigMALogServer

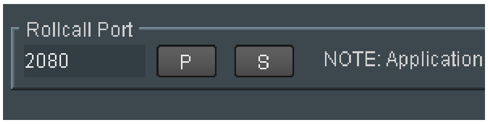
○ Named LogServer
● Any LogServer

Rollcall Port: 2070

NOTE: Application must be restarted for changes to take effect.

The default port for SigMA is 2070.

Normally the port number will be left in default. However, if there is a requirement to change the port number, this can be done here, by simple typing the desired port number in the box and pressing the **S** button.


Rollcall Port: 2080

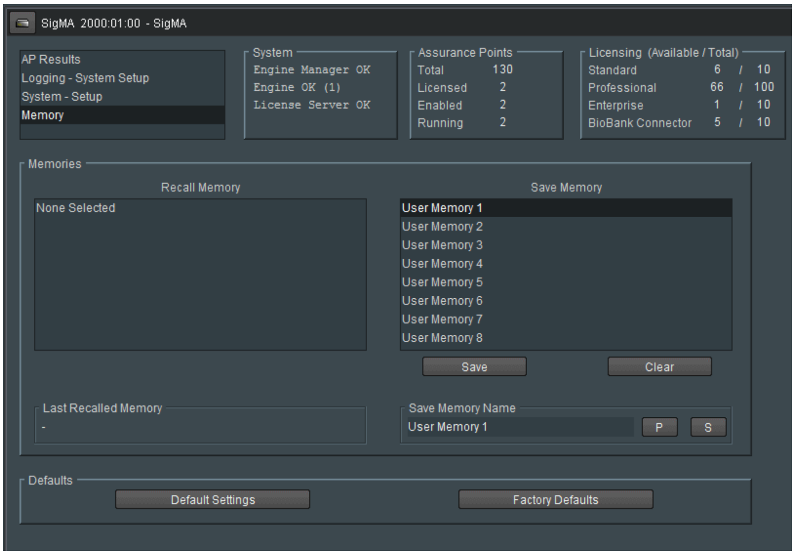
NOTE: Application

In this example, the port number has been changed to port: 2080

Pressing the P (preset) control will return the port number to default.

Note that the SigMA Service must be restarted for the port change to take effect.

10. SigMA Memory



SigMA 2000:01:00 - SigMA

AP Results
Logging - System Setup
System - Setup
Memory

System
```
Engine Manager OK
Engine OK (1)
License Server OK
```

Assurance Points	
Total	130
Licensed	2
Enabled	2
Running	2

Licensing (Available / Total)			
Standard	6	/	10
Professional	66	/	100
Enterprise	1	/	10
BioBank Connector	5	/	10

Memories

Recall Memory: None Selected

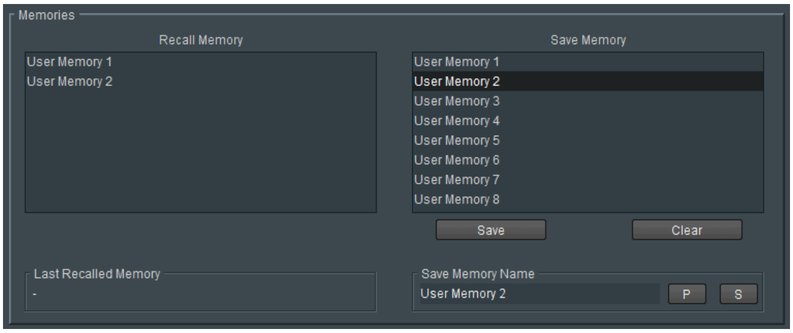
Save Memory: User Memory 1, User Memory 2, User Memory 3, User Memory 4, User Memory 5, User Memory 6, User Memory 7, User Memory 8

Last Recalled Memory: -

Save Memory Name: User Memory 1

SigMA configurations may be stored using the Memory feature. Up to eight configurations may be saved. Each memory save stores the SigMA configuration and the configuration of all Assurance Points.

To save a SigMA configuration, select one of the eight available memories and click on **Save.** Note that the saved memory will then appear in the **Recall Memory** window.



Memories

Recall Memory: User Memory 1, User Memory 2

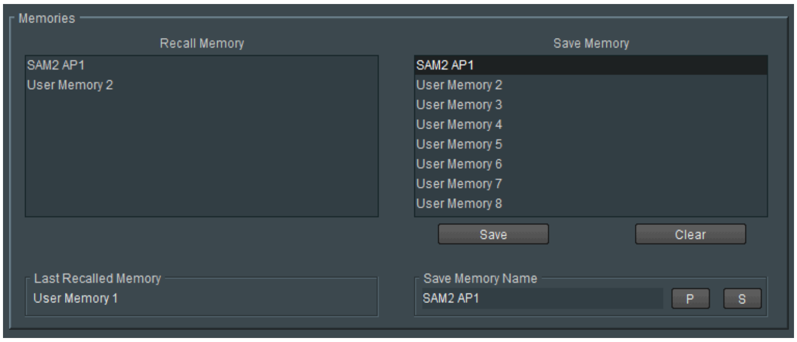
Save Memory: User Memory 1, User Memory 2, User Memory 3, User Memory 4, User Memory 5, User Memory 6, User Memory 7, User Memory 8

Last Recalled Memory: -

Save Memory Name: User Memory 2

In this example, two memory configurations have been saved; **User Memory 1** and **User Memory 2.**

Any memory listed in the **Save Memory** field can have its name changed, by selecting it and using the **Save Memory Name** feature.



Memories

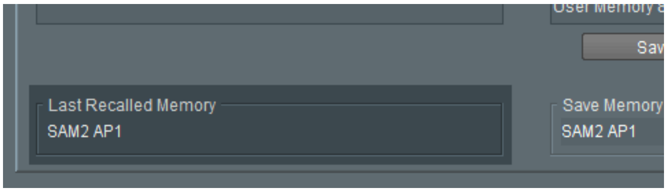
Recall Memory: SAM2 AP1, User Memory 2

Save Memory: SAM2 AP1, User Memory 2, User Memory 3, User Memory 4, User Memory 5, User Memory 6, User Memory 7, User Memory 8

Last Recalled Memory: User Memory 1

Save Memory Name: SAM2 AP1

Note that the last Memory recalled is listed in the **Last Recalled Memory** field.

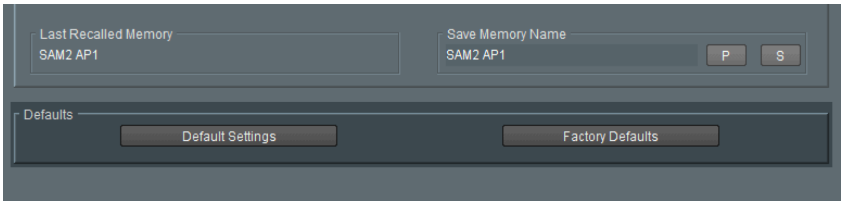


Last Recalled Memory
SAM2 AP1

Save Memory
SAM2 AP1

This feature allows a User to easily see what the current configuration is.

Defaults (Memory)



Last Recalled Memory
SAM2 AP1

Save Memory Name
SAM2 AP1

- **Default Settings:** When selected, all User controls will be returned their default value. User Memories will not be deleted. Configured IP Addresses will remain.

- **Factory Defaults:** When selected, the SigMA system will be returned to Factory condition. All User controls will be returned to default. Memories, including defined names, will be cleared. Configured IP Addresses will be reset.

All SigMA memory saves are located in C:\ProgramData\SAM (hidden directory by default).

For each saved memory there will be a *mymemorysave*.ini file present.

11. Configuring Assurance Points

SigMA offers a variety of Media Assurance Services. Some services derive results from analyzing a single signature, others require the comparison of a **known good** signature against a **processed** signature.

The state of all Media Assurance Services is reported via RollCall log fields.

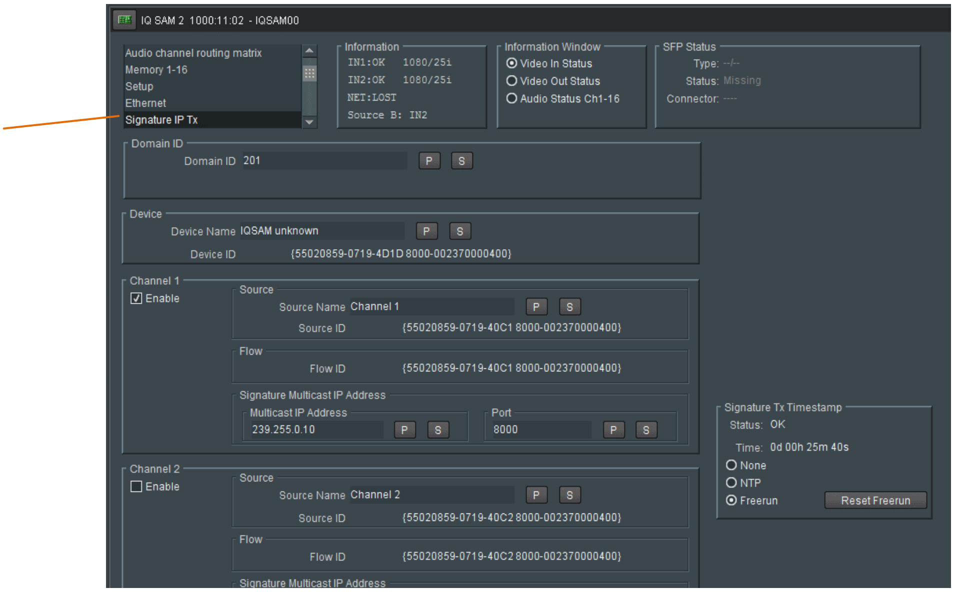
The following example will explain how to configure SigMA to monitor and compare two signatures generated from an IQSAM module.

It is assumed that a RollCall connection to the:

- IQSAM is configured in RollCall Control Panel and the IQSAM template has been loaded.
- SigMA is configured in Control Panel and the SigMA template is loaded.

11.1 Configuring IQSAM Domain ID

In the IQSAM00 RollCall template in Control Panel, scroll down the IQSAM menu and select **Signature IP Tx.**



Select

Signature IP Tx

IQ SAM 2 1000:11:02 - IQSAM00

Information
IN1:OK 1080/25i
IN2:OK 1080/25i
NET:LOST
Source B: IN2

Information Window
● Video In Status
○ Video Out Status
○ Audio Status Ch1-16

SFP Status
Type: --/--
Status: Missing
Connector: ----

Domain ID
Domain ID 201

Device
Device Name IQSAM unknown
Device ID {55020859-0719-4D1D 8000-002370000400}

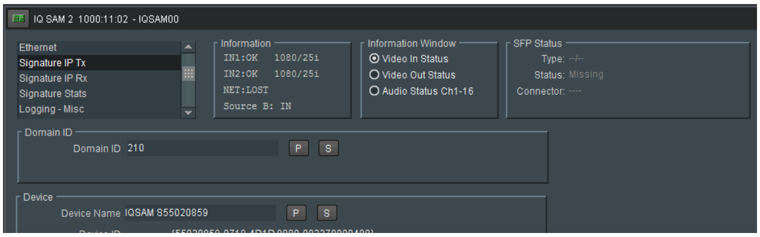
Channel 1
☑ Enable
Source
Source Name Channel 1
Source ID {55020859-0719-40C1 8000-002370000400}
Flow
Flow ID {55020859-0719-40C1 8000-002370000400}
Signature Multicast IP Address
Multicast IP Address 239.255.0.10
Port 8000

Channel 2
□ Enable
Source
Source Name Channel 2
Source ID {55020859-0719-40C2 8000-002370000400}
Flow
Flow ID {55020859-0719-40C2 8000-002370000400}
Signature Multicast IP Address

Signature Tx Timestamp
Status: OK
Time: 0d 00h 25m 40s
○ None
○ NTP
● Freerun

Note that in this example that the Domain ID of the IQSAM module is set to **201.** This is the default SigMA MBG Domain ID**.** In order for the SigMA to communicate with the IQSAM module (or any other form of MBG) these two Domain IDs must be the same.

In this example, the IQSAM Domain ID will be changed to match the SigMA MBG Domain ID of **210.**



IQ SAM 2 1000:11:02 - IQSAM00

Ethernet
Signature IP Tx
Signature IP Rx
Signature Stats
Logging - Misc

Information
```
IN1:OK   1080/25i
IN2:OK   1080/25i
NET:LOST
Source B: IN
```

Information Window
● Video In Status
○ Video Out Status
○ Audio Status Ch1-16

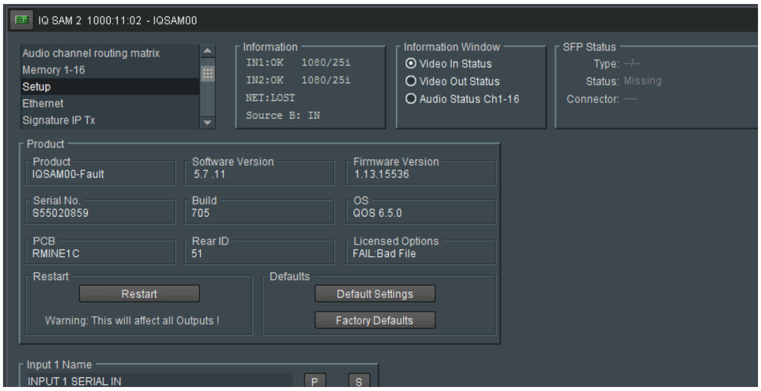
SFP Status
Type: --/--
Status: Missing
Connector: ----

Domain ID
Domain ID 210 P S

Device
Device Name IQSAM S55020859 P S

To change, simply type the new Domain ID address in the box and press the **'S'** button (S = select).

To implement the change it is necessary to restart the module. The **Restart** feature is located in the **Setup** menu.



IQ SAM 2 1000:11:02 - IQSAM00

Audio channel routing matrix
Memory 1-16
Setup
Ethernet
Signature IP Tx

Information
```
IN1:OK   1080/25i
IN2:OK   1080/25i
NET:LOST
Source B: IN
```

Information Window
● Video In Status
○ Video Out Status
○ Audio Status Ch1-16

SFP Status
Type: --/--
Status: Missing
Connector: ----

Product

Product	Software Version	Firmware Version
IQSAM00-Fault	5.7 .11	1.13.15536

Serial No.	Build	OS
S55020859	705	QOS 6.5.0

PCB	Rear ID	Licensed Options
RMINE1C	51	FAIL:Bad File

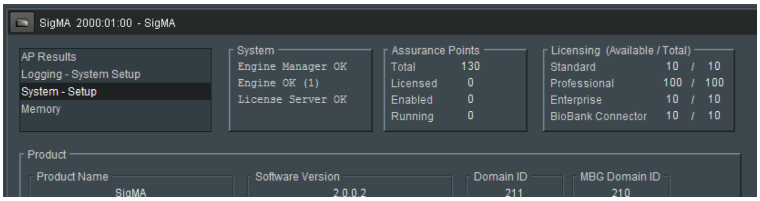
Restart
Restart
Warning: This will affect all Outputs !

Defaults
Default Settings
Factory Defaults

Input 1 Name
INPUT 1 SERIAL IN P S

11.2 Allocating Licenses

The number of APs available is defined by the number of Licenses available.



SigMA 2000:01:00 - SigMA

AP Results
Logging - System Setup
System - Setup
Memory

System
```
Engine Manager OK
Engine OK (1)
License Server OK
```

Assurance Points	
Total	130
Licensed	0
Enabled	0
Running	0

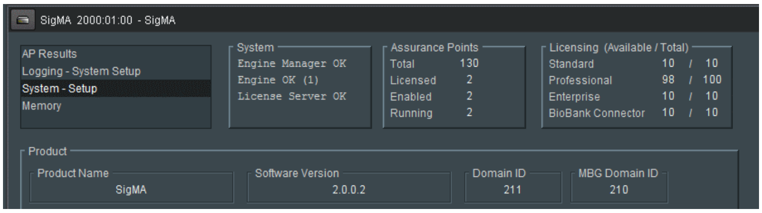
Licensing (Available / Total)			
Standard	10	/	10
Professional	100	/	100
Enterprise	10	/	10
BioBank Connector	10	/	10

Product

Product Name	Software Version	Domain ID	MBG Domain ID
SigMA	2.0.0.2	211	210

In this example it can be seen that there are a total of 130 licenses available. No licenses have been consumed. Note the correlation between the number of APs and the number of available licenses.

As licenses are consumed, by the process of configuring APs, so the available licenses will be reduces accordingly.



SigMA 2000:01:00 - SigMA

AP Results
Logging - System Setup
System - Setup
Memory

System
```
Engine Manager OK
Engine OK (1)
License Server OK
```

Assurance Points	
Total	130
Licensed	2
Enabled	2
Running	2

Licensing (Available / Total)			
Standard	10	/	10
Professional	98	/	100
Enterprise	10	/	10
BioBank Connector	10	/	10

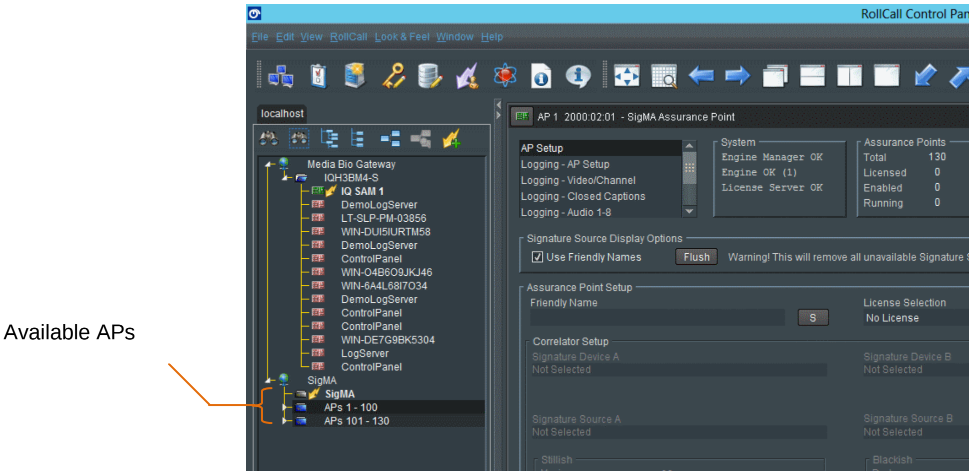
Product

Product Name	Software Version	Domain ID	MBG Domain ID
SigMA	2.0.0.2	211	210

In this example, two Professional licenses have been consumed as two APs have been configured.

11.3 Assurance Point Selection

In the RollCall connection window expand the SigMA tree to reveal the available APs .



Available APs

Media Bio Gateway
IQH3BM4-S
IQ SAM 1
DemoLogServer
LT-SLP-PM-03856
WIN-DUI5IURTM58
DemoLogServer
ControlPanel
WIN-O4B6O9JKJ46
WIN-6A4L68I7O34
DemoLogServer
ControlPanel
ControlPanel
WIN-DE7G9BK5304
LogServer
ControlPanel
SigMA
SigMA
APs 1 - 100
APs 101 - 130

AP 1 2000:02:01 - SigMA Assurance Point

AP Setup
Logging - AP Setup
Logging - Video/Channel
Logging - Closed Captions
Logging - Audio 1-8

System
Engine Manager OK
Engine OK (1)
License Server OK

Assurance Points
Total 130
Licensed 0
Enabled 0
Running 0

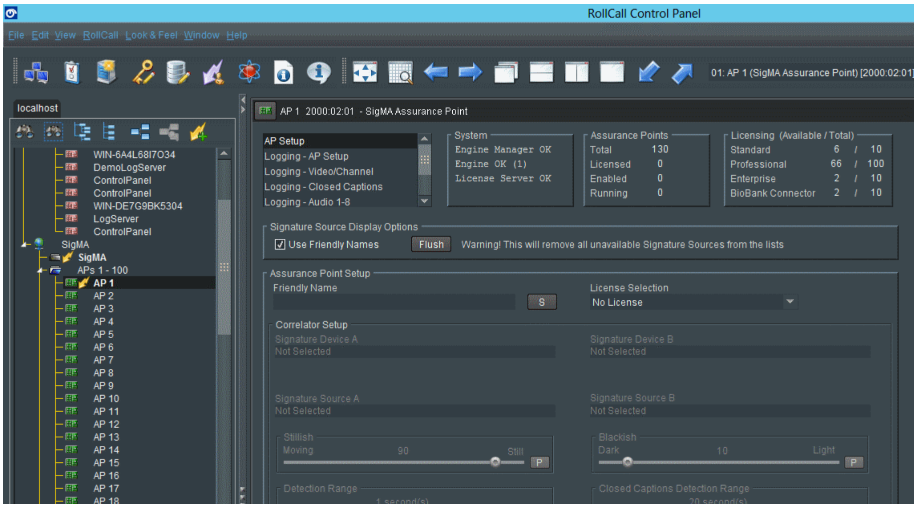
Signature Source Display Options
☑ Use Friendly Names Flush Warning! This will remove all unavailable Signature

Assurance Point Setup
Friendly Name S
License Selection: No License

Correlator Setup
Signature Device A: Not Selected
Signature Device B: Not Selected
Signature Source A: Not Selected
Signature Source B: Not Selected
Stillish
Blackish

Note that the available APs are arranged in groups of 100 APs. In the above example, there are 130 APs available, so there is one group of 100 AP’s and a second group of 30 APs.

Each group can be expanded enabling single APs to be selected:


RollCall Control Panel
File Edit View RollCall Look & Feel Window Help
01: AP 1 (SigMA Assurance Point) [2000:02:01]
localhost

WIN-6A4L68I7O34
DemoLogServer
ControlPanel
ControlPanel
WIN-DE7G9BK5304
LogServer
ControlPanel
SigMA
SigMA
APs 1 - 100
AP 1
AP 2
AP 3
AP 4
AP 5
AP 6
AP 7
AP 8
AP 9
AP 10
AP 11
AP 12
AP 13
AP 14
AP 15
AP 16
AP 17
AP 18

AP 1 2000:02:01 - SigMA Assurance Point

AP Setup
Logging - AP Setup
Logging - Video/Channel
Logging - Closed Captions
Logging - Audio 1-8

System
Engine Manager OK
Engine OK (1)
License Server OK

Assurance Points
Total 130
Licensed 0
Enabled 0
Running 0

Licensing (Available / Total)			
Standard	6	/	10
Professional	66	/	100
Enterprise	2	/	10
BioBank Connector	2	/	10

Signature Source Display Options
☑ Use Friendly Names Flush Warning! This will remove all unavailable Signature Sources from the lists

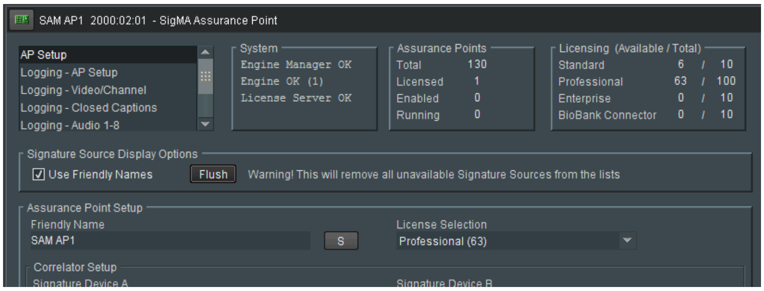
Assurance Point Setup
Friendly Name S
License Selection: No License

Correlator Setup
Signature Device A: Not Selected
Signature Device B: Not Selected
Signature Source A: Not Selected
Signature Source B: Not Selected
Stillish: Moving 90 Still P
Blackish: Dark 10 Light P
Detection Range: 1 second(s)
Closed Captions Detection Range: 20 second(s)

In the above example, AP1 has been selected and can be configured.

11.4 Assurance Point Setup

In the RollCall template for the selected AP (in this case AP1), select **AP Setup**.



SAM AP1 2000:02:01 - SigMA Assurance Point

AP Setup
Logging - AP Setup
Logging - Video/Channel
Logging - Closed Captions
Logging - Audio 1-8

System
```
Engine Manager OK
Engine OK (1)
License Server OK
```

Assurance Points	
Total	130
Licensed	1
Enabled	0
Running	0

Licensing (Available / Total)			
Standard	6	/	10
Professional	63	/	100
Enterprise	0	/	10
BioBank Connector	0	/	10

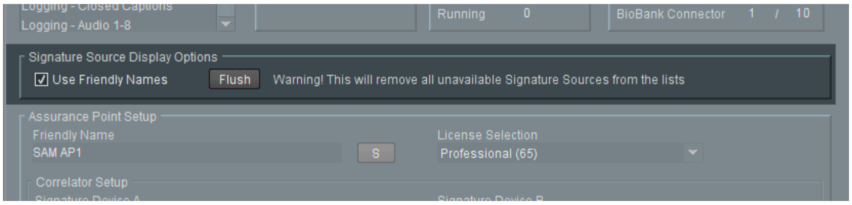
Signature Source Display Options
☑ Use Friendly Names   Flush   Warning! This will remove all unavailable Signature Sources from the lists

Assurance Point Setup
Friendly Name: SAM AP1   S
License Selection: Professional (63)

Correlator Setup
Signature Device A
Signature Device B

11.4.1 Signature Source Display Option

Friendly Names Enable



Logging - Closed Captions
Logging - Audio 1-8
Running 0
BioBank Connector 1 / 10

Signature Source Display Options
☑ Use Friendly Names   Flush   Warning! This will remove all unavailable Signature Sources from the lists

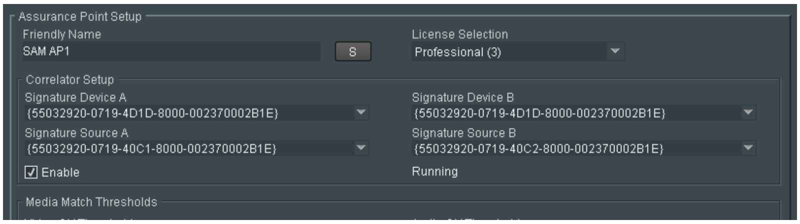
Assurance Point Setup
Friendly Name: SAM AP1   S
License Selection: Professional (65)

Correlator Setup
Signature Device A
Signature Device B

This menu allows the User to enable or disable the use of **Friendly Names**.

The **Flush** control updates the network and removes from the list of sources any which are off-line.

Internally SigMA uses UUIDs (Universal Unique Identifiers). These tend to be long strings of text:



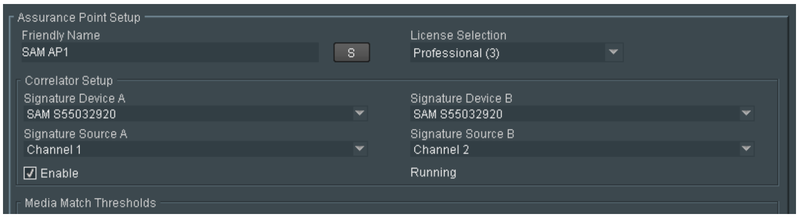
Assurance Point Setup
Friendly Name: SAM AP1   S
License Selection: Professional (3)

Correlator Setup
Signature Device A: {55032920-0719-4D1D-8000-002370002B1E}
Signature Device B: {55032920-0719-4D1D-8000-002370002B1E}
Signature Source A: {55032920-0719-40C1-8000-002370002B1E}
Signature Source B: {55032920-0719-40C2-8000-002370002B1E}
☑ Enable
Running

Media Match Thresholds

In this example, friendly Names have not been configured. Each field displays the relevant UUID.

The **Friendly Names** feature just makes the displayed information easier to comprehend, from a human perspective.

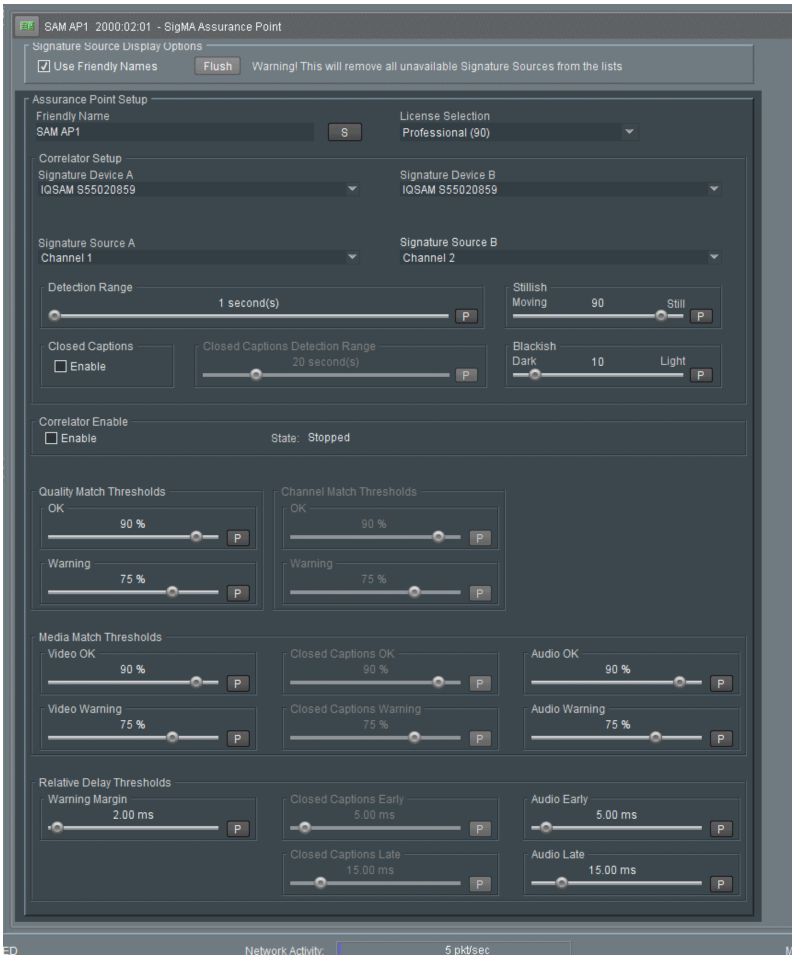


Assurance Point Setup
Friendly Name: SAM AP1   S
License Selection: Professional (3)

Correlator Setup
Signature Device A: SAM S55032920
Signature Device B: SAM S55032920
Signature Source A: Channel 1
Signature Source B: Channel 2
☑ Enable
Running

Media Match Thresholds

Here we can see all the AP configuration parameters at a glance.



SAM AP1 2000:02:01 - SigMA Assurance Point

Signature Source Display Options

☑ Use Friendly Names

Warning! This will remove all unavailable Signature Sources from the lists

Assurance Point Setup

Friendly Name: SAM AP1

License Selection: Professional (90)

Correlator Setup

Signature Device A: IQSAM S55020859

Signature Device B: IQSAM S55020859

Signature Source A: Channel 1

Signature Source B: Channel 2

Detection Range: 1 second(s)

Stillish: Moving 90 Still

Closed Captions: □ Enable

Closed Captions Detection Range: 20 second(s)

Blackish: Dark 10 Light

Correlator Enable: □ Enable

State: Stopped

Quality Match Thresholds: OK 90 %; Warning 75 %

Channel Match Thresholds: OK 90 %; Warning 75 %

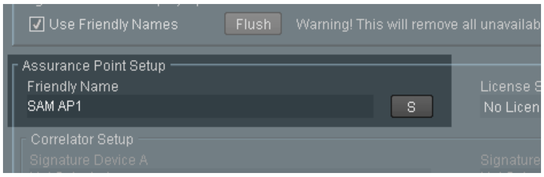
Media Match Thresholds: Video OK 90 %; Video Warning 75 %; Closed Captions OK 90 %; Closed Captions Warning 75 %; Audio OK 90 %; Audio Warning 75 %

Relative Delay Thresholds: Warning Margin 2.00 ms; Closed Captions Early 5.00 ms; Closed Captions Late 15.00 ms; Audio Early 5.00 ms; Audio Late 15.00 ms

Network Activity: 5 pkt/sec

11.4.2 Friendly Name

Here a User can give the assurance point a Friendly Name. The User simply types a ‘friendly’ name in the box and click on the **S** icon to initiate the change.



☑ Use Friendly Names

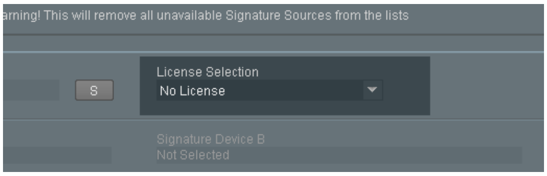
Warning! This will remove all unavailab

Assurance Point Setup

Friendly Name: SAM AP1

In this example the **Friendly Name** ‘SAM AP1’ has been set.

11.4.3 License Selection

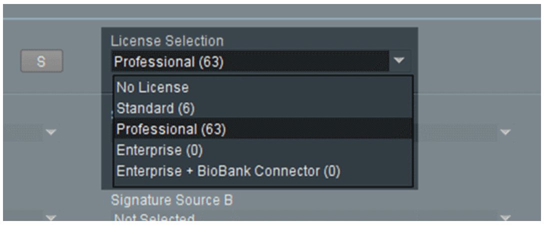


arning! This will remove all unavailable Signature Sources from the lists

License Selection: No License

Signature Device B: Not Selected

Here, the User can apply an available license to the new AP. The available licenses can be displayed by using the associated down-arrow.

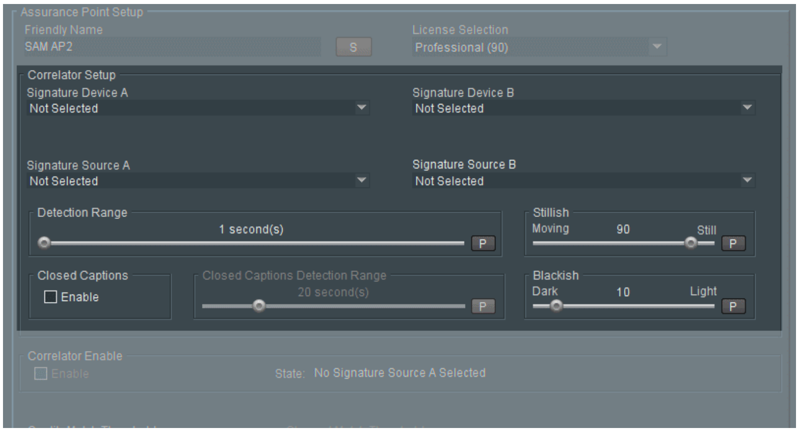


License Selection: Professional (63)

Signature Source B: Not Selected

The User can select the type of license from the drop-down list.

11.4.4 Correlator Setup



Assurance Point Setup

Friendly Name: SAM AP2

License Selection: Professional (90)

Correlator Setup

Signature Device A: Not Selected

Signature Device B: Not Selected

Signature Source A: Not Selected

Signature Source B: Not Selected

Detection Range: 1 second(s)

Stillish: Moving 90 Still

Closed Captions: □ Enable

Closed Captions Detection Range: 20 second(s)

Blackish: Dark 10 Light

Correlator Enable: □ Enable

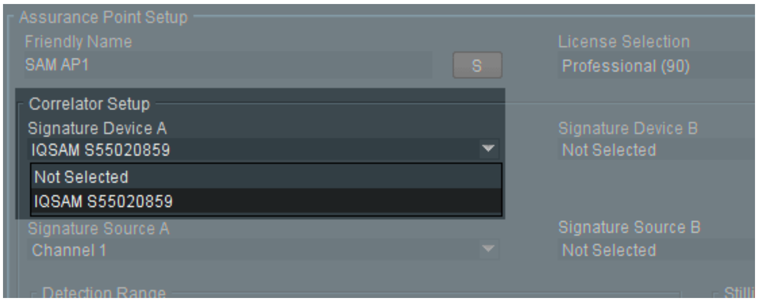
State: No Signature Source A Selected

Here the parameters of the AP are configured.

In the following example, the two inputs of an IQSAM00 module are being used for Signature generation.

Note that the IQSAM00 module has an MBG (Media Biometric Generator) on each Input.

First it is necessary to select the **Signature Device A** from the drop-down menu.



Assurance Point Setup

Friendly Name: SAM AP1

License Selection: Professional (90)

Correlator Setup

Signature Device A: IQSAM S55020859

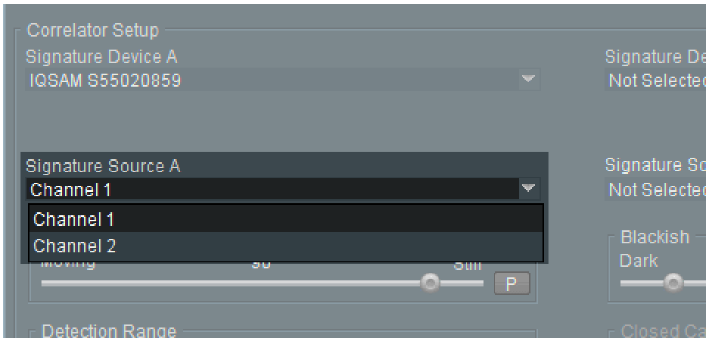
Signature Device B: Not Selected

Signature Source A: Channel 1

Signature Source B: Not Selected

In this particular example there is only one device that can be selected as a signature generation device; the IQSAM00 s/n s55020859.

It is then necessary to define the **Signature Source A** (this is because a device, in this case an IQSAM00, may have multiple Signature sources. The IQSAM00 has two).



Correlator Setup

Signature Device A: IQSAM S55020859

Signature De: Not Selecte

Signature Source A: Channel 1

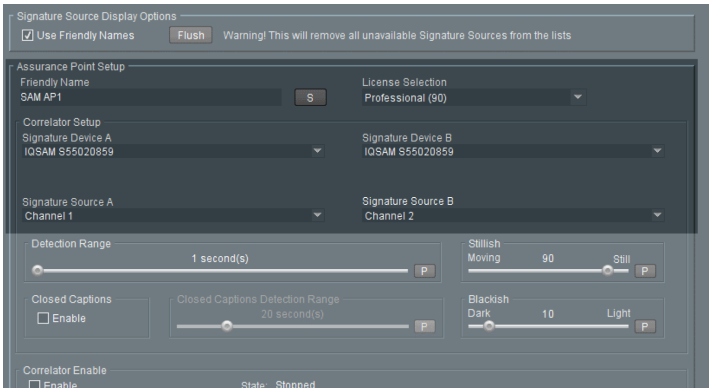
Channel 1
Channel 2

Signature So: Not Selecte

There are two options available. Channel 1 is chosen.

The process is then repeated for **Signature Device B**

In the example shown, the **Signature Device** is the same IQSAM00 and the **Signature Source** is channel 2.



Signature Source Display Options

☑ Use Friendly Names [Flush] Warning! This will remove all unavailable Signature Sources from the lists

Assurance Point Setup

Friendly Name: SAM AP1 [S]

License Selection: Professional (90)

Correlator Setup

Signature Device A: IQSAM S55020859

Signature Device B: IQSAM S55020859

Signature Source A: Channel 1

Signature Source B: Channel 2

Detection Range: 1 second(s) [P]

Stillish: Moving 90 Still [P]

Closed Captions: □ Enable

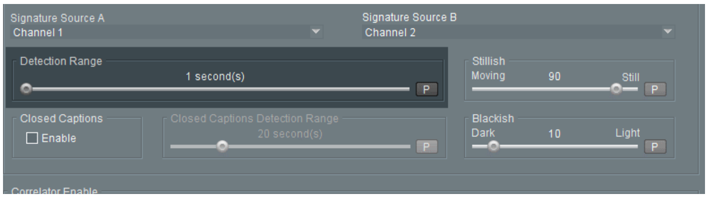
Closed Captions Detection Range: 20 second(s) [P]

Blackish: Dark 10 Light [P]

Correlator Enable

□ Enable State: Stopped

11.4.5 Detection Range



Signature Source A: Channel 1

Signature Source B: Channel 2

Detection Range: 1 second(s) [P]

Stillish: Moving 90 Still [P]

Closed Captions: □ Enable

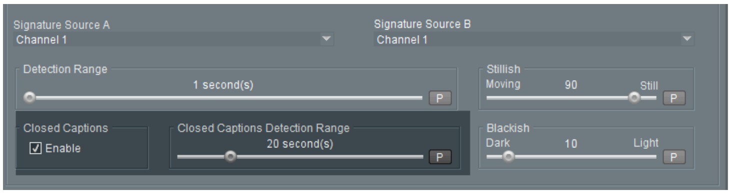
Closed Captions Detection Range: 20 second(s) [P]

Blackish: Dark 10 Light [P]

Correlator Enable

Where an AP is configured to compare two video streams in a system, it is unlikely that the two streams will not be exactly co-timed. The **Detection Range** allows the User to set a limit on how separated in time the two streams can be. The default value is 1 second, but the user can increase this up to 5 seconds.

11.4.6 Closed Captions Detection Range



Signature Source A: Channel 1

Signature Source B: Channel 1

Detection Range: 1 second(s)

Stillish: Moving 90 Still

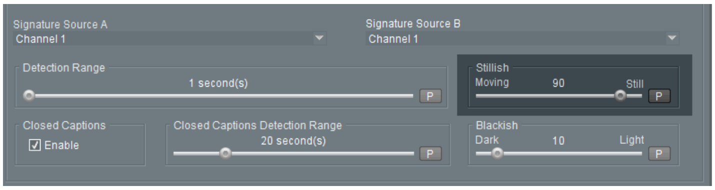
Closed Captions: ☑ Enable

Closed Captions Detection Range: 20 second(s)

Blackish: Dark 10 Light

This control is similar to **Detection Range** above, but it only applies to any closed captions within the streams being compared. Closed Captions, by their very nature, are prone to drift temporally and so a longer detection range will probably need to be configured. Default setting is 20 seconds, but the control allows any time between 10 and 60 seconds to be configured.

11.4.7 Stillish



Signature Source A: Channel 1

Signature Source B: Channel 1

Detection Range: 1 second(s)

Stillish: Moving 90 Still

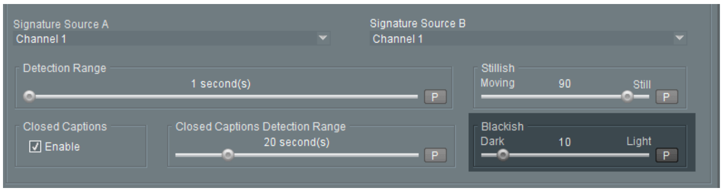
Closed Captions: ☑ Enable

Closed Captions Detection Range: 20 second(s)

Blackish: Dark 10 Light

Here the Operator can adjust the Stillish threshold if required. The default settings represent a good starting point for the majority of applications, but the User does have the ability to increase or decrease the sensitivity.

11.4.8 Blackish



Signature Source A: Channel 1

Signature Source B: Channel 1

Detection Range: 1 second(s)

Stillish: Moving 90 Still

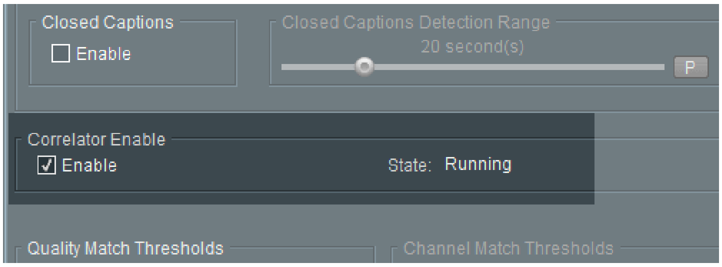
Closed Captions: ☑ Enable

Closed Captions Detection Range: 20 second(s)

Blackish: Dark 10 Light

Here the Operator can adjust the Blackish threshold if required. The default settings represent a good starting point for the majority of applications, but the User does have the ability to increase or decrease the sensitivity.

11.4.9 Correlator Enable



Closed Captions: ☐ Enable

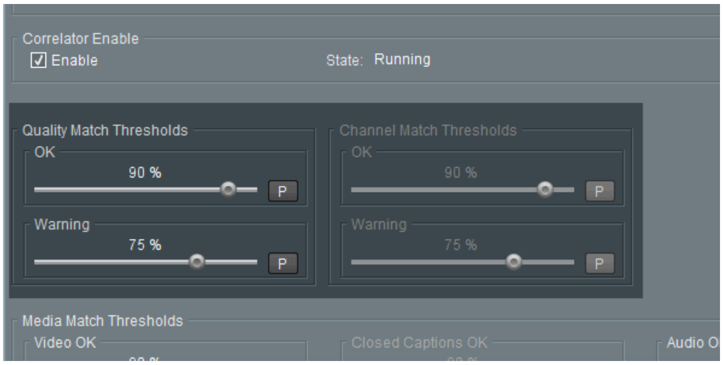
Closed Captions Detection Range: 20 second(s)

Correlator Enable: ☑ Enable State: Running

For the Correlator (used in an AP) to be operational and process/transmit results it must be **Enabled.**

11.5 Quality Match Thresholds

Here the thresholds of Quality Match can be set using the slider controls. The default settings represent a good starting point for the majority of applications, but the User does have the ability to increase or decrease the Quality Match sensitivity. Sensitivity describes when a state changes from Ok, Warning & Error.



Correlator Enable
☑ Enable
State: Running

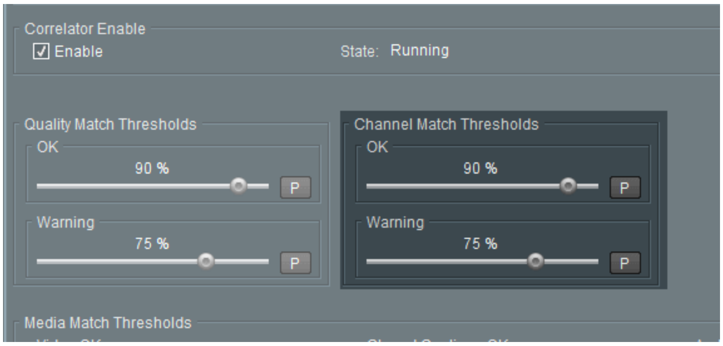
Quality Match Thresholds
OK 90 %
Warning 75 %

Channel Match Thresholds
OK 90 %
Warning 75 %

Media Match Thresholds
Video OK
Closed Captions OK
Audio O

11.6 Channel Match Thresholds

Here the thresholds of **Channel Match** can be set using the slider controls. The default settings represent a good starting point for the majority of applications, but the User does have the ability to increase or decrease the Channel Match sensitivity. Sensitivity describes when a state changes from Ok, Warning & Error.



Correlator Enable
☑ Enable
State: Running

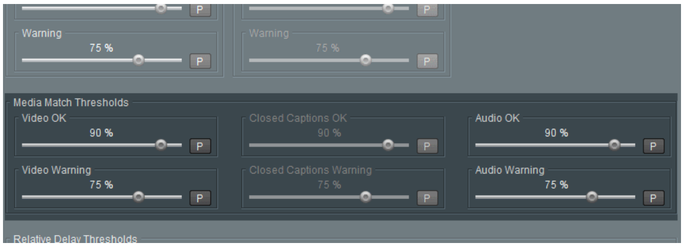
Quality Match Thresholds
OK 90 %
Warning 75 %

Channel Match Thresholds
OK 90 %
Warning 75 %

Media Match Thresholds

Note that the Channel Match feature is only available when the AP has an Enterprise License. When the AP is licensed with either a Standard License, or a Professional License, then the Channel Match controls will be greyed out.

11.7 Media Match Thresholds



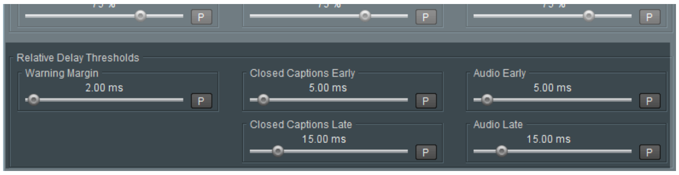
Warning 75 %
Warning 75 %

Media Match Thresholds
Video OK 90 %
Closed Captions OK 90 %
Audio OK 90 %
Video Warning 75 %
Closed Captions Warning 75 %
Audio Warning 75 %

Relative Delay Thresholds

Here the thresholds of **Media Match** can be set using the slider controls. The default settings represent a good starting point for the majority of applications, but the User does have the ability to increase or decrease the Media Match sensitivity. Sensitivity describes when a state changes from Ok, Warning & Error.

11.8 Relative Delay Thresholds



Relative Delay Thresholds

Warning Margin 2.00 ms

Closed Captions Early 5.00 ms

Closed Captions Late 15.00 ms

Audio Early 5.00 ms

Audio Late 15.00 ms

Here the thresholds for **Relative Audio Delay** (also referred to as **Lip Sync**) and **Relative Closed Caption Delay** can be set using the slider controls. The default settings represent a good starting point for the majority of applications, but the User does have the ability to increase or decrease the Relative Delay sensitivity for each. Sensitivity describes when a state changes from Ok, Warning & Error.

The **Warning Margin** applies to both Audio and Captions.

Closed Captions (Early / Late):

These controls allow a User to define the threshold of what relative delay error is deemed **Ok** for Closed Captions.

It is normally deemed a worse condition that Closed Captions are early, hence a tighter tolerance is usually configured at default.

If default values are configured, this will result in a **Warning** being issued if Closed Captions are between 5ms and 7ms early, and an **Error** issued if Closed Captions are more that 7ms early.

Similarly, if Closed Captions are between 15ms and 17ms late, this will result in a **Warning**, and Closed Captions more than 17ms late will issue an ‘error’.

Note that it is important for a relative delay measurement for the us the User to understand which is the **known good** signature and which signature is under test. This is because this will influence the sign of the value.

Audio (Early/Late):

These controls allow a User to define the threshold of what relative delay error is deemed acceptable for Audio.

It is normally deemed a worse condition that Audio is early, hence a tighter tolerance is usually configured at default.

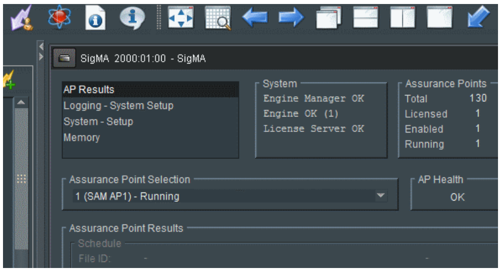
If default values are configured, this will result in a **Warning** being issued if Closed Captions are between 5ms and 7ms early, and an **Error** issued if Closed Captions are more that 7ms early.

Similarly, if Closed Captions are between 15ms and 17ms late, this will result in a **Warning**, and Closed Captions more than 17ms late will issue an **Error**.

Note that it is important for a relative delay measurement, for the User to understand which is the known *good* signature and which signature is under test. This is because this will influence the sign of the value.

11.9 AP Results

In the **SigMA** main menu, select **AP Results**.



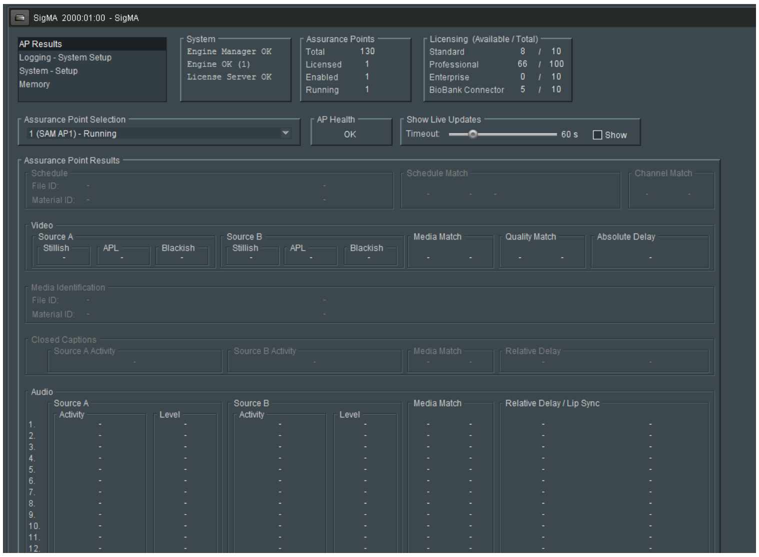
System: Engine Manager OK, Engine OK (1), License Server OK

Assurance Points: Total 130, Licensed 1, Enabled 1, Running 1

Assurance Point Selection: 1 (SAM AP1) - Running

AP Health: OK

The AP Results template will now load.



System: Engine Manager OK, Engine OK (1), License Server OK

Assurance Points: Total 130, Licensed 1, Enabled 1, Running 1

Licensing (Available / Total): Standard 8 / 10, Professional 66 / 100, Enterprise 0 / 10, BioBank Connector 5 / 10

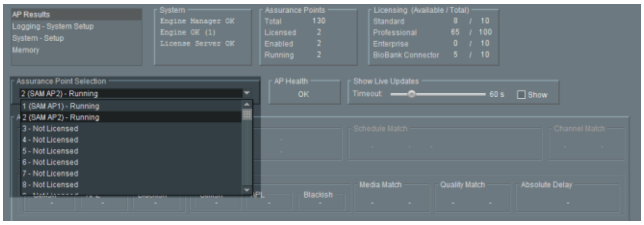
Assurance Point Selection: 1 (SAM AP1) - Running

AP Health: OK

Show Live Updates: Timeout: 60 s □ Show

11.9.1 Assurance Point Selection

In the **Assurance Point Selection** field, the User can select the specific AP, for which results are to be observed, using the associated drop-down menu.



System: Engine Manager OK, Engine OK (1), License Server OK

Assurance Points: Total 130, Licensed 2, Enabled 2, Running 2

Licensing (Available / Total): Standard 8 / 10, Professional 65 / 100, Enterprise 0 / 10, BioBank Connector 5 / 10

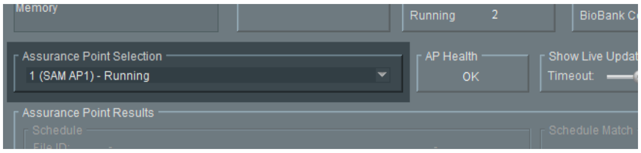
Assurance Point Selection: 2 (SAM AP2) - Running

AP Health: OK

Show Live Updates: Timeout: 60 s □ Show

In the above example, there are only two AP configured (SAM AP1 & SAM AP2).

AP1 will be selected by default.



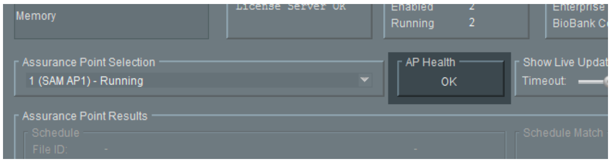
Assurance Point Selection: 1 (SAM AP1) - Running

AP Health: OK

Show Live Updat
Timeout:

11.9.2 AP Health

The **AP Heath** feature gives assurance that the IT infrastructure supporting the SigMA installation has enough resource to support all the APs configured. In circumstances where resource is running short, this field will flag a warning.



Memory

License Server OK

Enabled 2
Running 2

Enterprise
BioBank C

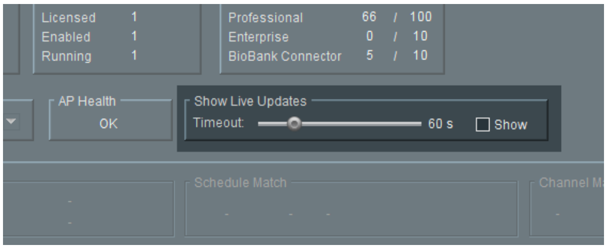
Assurance Point Selection: 1 (SAM AP1) - Running

AP Health: OK

Show Live Updat
Timeout:

Assurance Point Results
Schedule
File ID: - -
Schedule Match

11.9.3 Show Live Updates



Licensed 1
Enabled 1
Running 1

Professional 66 / 100
Enterprise 0 / 10
BioBank Connector 5 / 10

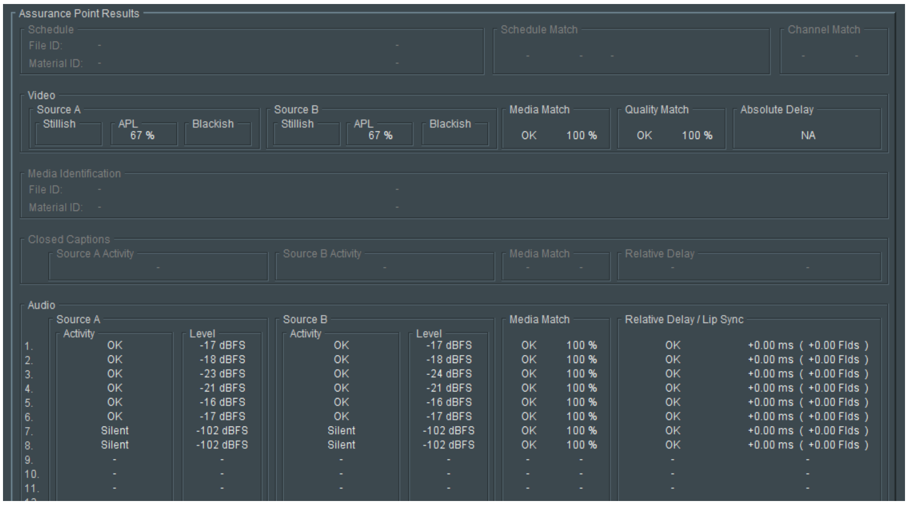
AP Health: OK

Show Live Updates
Timeout: 60 s ☐ Show

Schedule Match: - - -
Channel M: -

The **Show Live Updates** field allow the User to view, in real time, the parameters being reported by the AP. The duration that the results are displayed in the Assurance Point Results field can be controlled using the **Timeout** slider. Default value is 60 seconds.

When the Show button is selected, the live results for the selected AP will be displayed.



Assurance Point Results

Schedule
File ID: - -
Material ID: - -

Schedule Match: - - -

Channel Match: - -

Video
Source A: Stillish; APL 67 %; Blackish
Source B: Stillish; APL 67 %; Blackish
Media Match: OK 100 %
Quality Match: OK 100 %
Absolute Delay: NA

Media Identification
File ID: - -
Material ID: - -

Closed Captions
Source A Activity: -
Source B Activity: -
Media Match: - -
Relative Delay: - -

Audio

	Source A		Source B		Media Match		Relative Delay / Lip Sync	
	Activity	Level	Activity	Level				
1.	OK	-17 dBFS	OK	-17 dBFS	OK	100 %	OK	+0.00 ms (+0.00 Flds)
2.	OK	-18 dBFS	OK	-18 dBFS	OK	100 %	OK	+0.00 ms (+0.00 Flds)
3.	OK	-23 dBFS	OK	-24 dBFS	OK	100 %	OK	+0.00 ms (+0.00 Flds)
4.	OK	-21 dBFS	OK	-21 dBFS	OK	100 %	OK	+0.00 ms (+0.00 Flds)
5.	OK	-16 dBFS	OK	-16 dBFS	OK	100 %	OK	+0.00 ms (+0.00 Flds)
6.	OK	-17 dBFS	OK	-17 dBFS	OK	100 %	OK	+0.00 ms (+0.00 Flds)
7.	Silent	-102 dBFS	Silent	-102 dBFS	OK	100 %	OK	+0.00 ms (+0.00 Flds)
8.	Silent	-102 dBFS	Silent	-102 dBFS	OK	100 %	OK	+0.00 ms (+0.00 Flds)
9.	-	-	-	-	-	-	-	-
10.	-	-	-	-	-	-	-	-
11.	-	-	-	-	-	-	-	-

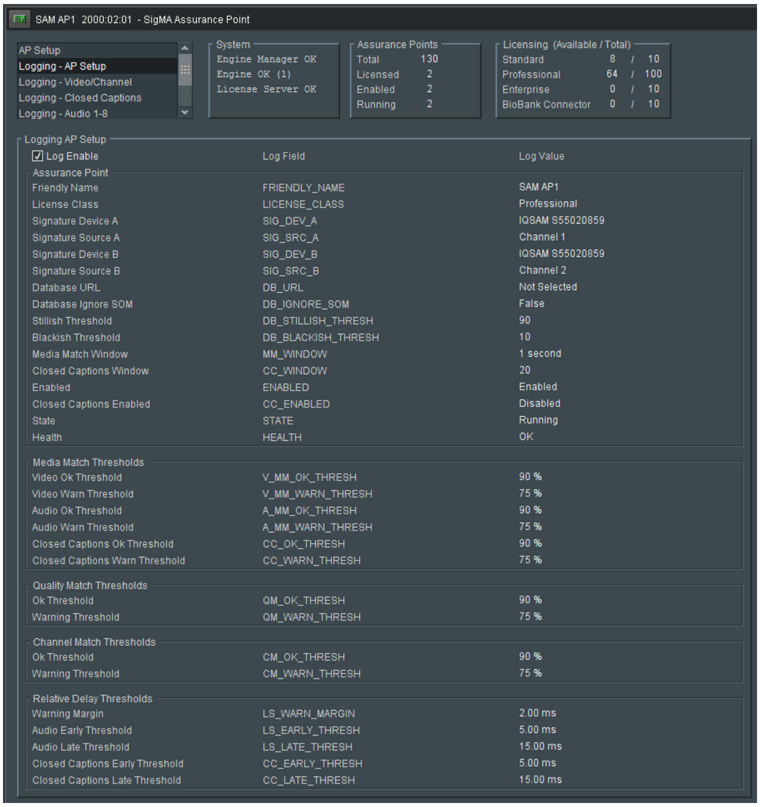
12. SigMA Logging

In a Media Assurance System, the part played by the SigMA is to monitor and report to status of Media Assurance Points.

Logged items are reported to a RollMap Log Server and it is the configuration of RollMap that dictates what the system does with the information SigMA is supplying.

Note: This document is not a RollMap help guide.

12.1 Logging AP Setup



System
Engine Manager OK
Engine OK (1)
License Server OK

Assurance Points	
Total	130
Licensed	2
Enabled	2
Running	2

Licensing (Available / Total)			
Standard	8	/	10
Professional	64	/	100
Enterprise	0	/	10
BioBank Connector	0	/	10

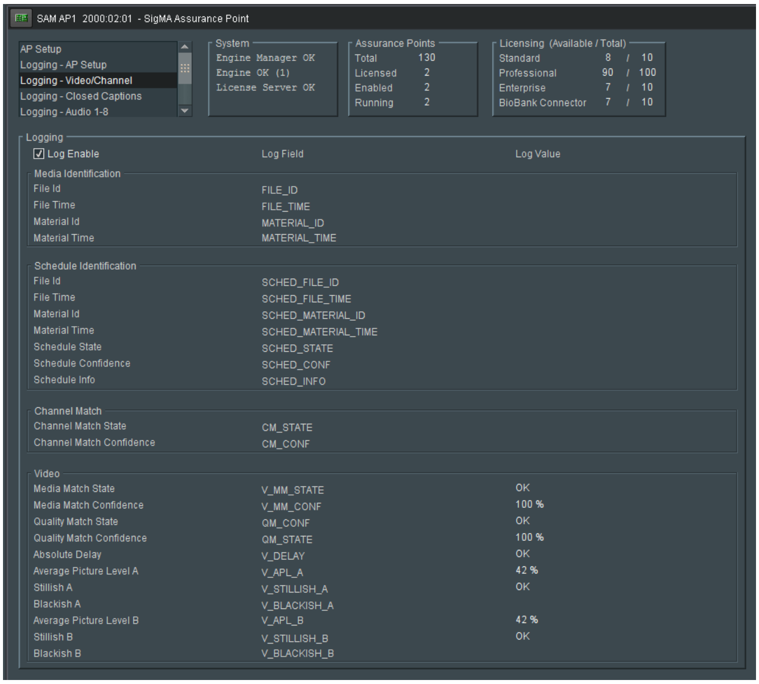
Logging AP Setup

☑ Log Enable	Log Field	Log Value
Assurance Point		
Friendly Name	FRIENDLY_NAME	SAM AP1
License Class	LICENSE_CLASS	Professional
Signature Device A	SIG_DEV_A	IQSAM S55020859
Signature Source A	SIG_SRC_A	Channel 1
Signature Device B	SIG_DEV_B	IQSAM S55020859
Signature Source B	SIG_SRC_B	Channel 2
Database URL	DB_URL	Not Selected
Database Ignore SOM	DB_IGNORE_SOM	False
Stillish Threshold	DB_STILLISH_THRESH	90
Blackish Threshold	DB_BLACKISH_THRESH	10
Media Match Window	MM_WINDOW	1 second
Closed Captions Window	CC_WINDOW	20
Enabled	ENABLED	Enabled
Closed Captions Enabled	CC_ENABLED	Disabled
State	STATE	Running
Health	HEALTH	OK
Media Match Thresholds		
Video Ok Threshold	V_MM_OK_THRESH	90 %
Video Warn Threshold	V_MM_WARN_THRESH	75 %
Audio Ok Threshold	A_MM_OK_THRESH	90 %
Audio Warn Threshold	A_MM_WARN_THRESH	75 %
Closed Captions Ok Threshold	CC_OK_THRESH	90 %
Closed Captions Warn Threshold	CC_WARN_THRESH	75 %
Quality Match Thresholds		
Ok Threshold	QM_OK_THRESH	90 %
Warning Threshold	QM_WARN_THRESH	75 %
Channel Match Thresholds		
Ok Threshold	CM_OK_THRESH	90 %
Warning Threshold	CM_WARN_THRESH	75 %
Relative Delay Thresholds		
Warning Margin	LS_WARN_MARGIN	2.00 ms
Audio Early Threshold	LS_EARLY_THRESH	5.00 ms
Audio Late Threshold	LS_LATE_THRESH	15.00 ms
Closed Captions Early Threshold	CC_EARLY_THRESH	5.00 ms
Closed Captions Late Threshold	CC_LATE_THRESH	15.00 ms

Here the AP Setup is logged and reported to the Log Server.

The **Log Enable** control allows the User to configure whether the parameters of a particular AP, in this example AP1, are logged.

12.2 Logging Video Channel



System
Engine Manager OK
Engine OK (1)
License Server OK

Assurance Points	
Total	130
Licensed	2
Enabled	2
Running	2

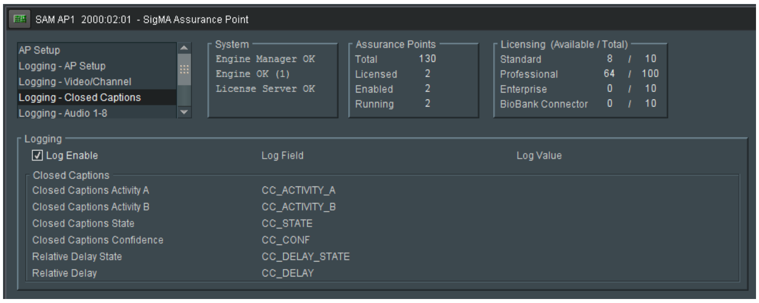
Licensing (Available / Total)			
Standard	8	/	10
Professional	90	/	100
Enterprise	7	/	10
BioBank Connector	7	/	10

Logging

☑ Log Enable	Log Field	Log Value
Media Identification		
File Id	FILE_ID	
File Time	FILE_TIME	
Material Id	MATERIAL_ID	
Material Time	MATERIAL_TIME	
Schedule Identification		
File Id	SCHED_FILE_ID	
File Time	SCHED_FILE_TIME	
Material Id	SCHED_MATERIAL_ID	
Material Time	SCHED_MATERIAL_TIME	
Schedule State	SCHED_STATE	
Schedule Confidence	SCHED_CONF	
Schedule Info	SCHED_INFO	
Channel Match		
Channel Match State	CM_STATE	
Channel Match Confidence	CM_CONF	
Video		
Media Match State	V_MM_STATE	OK
Media Match Confidence	V_MM_CONF	100 %
Quality Match State	QM_CONF	OK
Quality Match Confidence	QM_STATE	100 %
Absolute Delay	V_DELAY	OK
Average Picture Level A	V_APL_A	42 %
Stillish A	V_STILLISH_A	OK
Blackish A	V_BLACKISH_A	
Average Picture Level B	V_APL_B	42 %
Stillish B	V_STILLISH_B	OK
Blackish B	V_BLACKISH_B	

The **Logging – Video/Channel** menu will detail what video items are being logged, and will allow the User to Enable or Disable logging for any particular AP.

12.3 Logging – Closed Captions



System
Engine Manager OK
Engine OK (1)
License Server OK

Assurance Points	
Total	130
Licensed	2
Enabled	2
Running	2

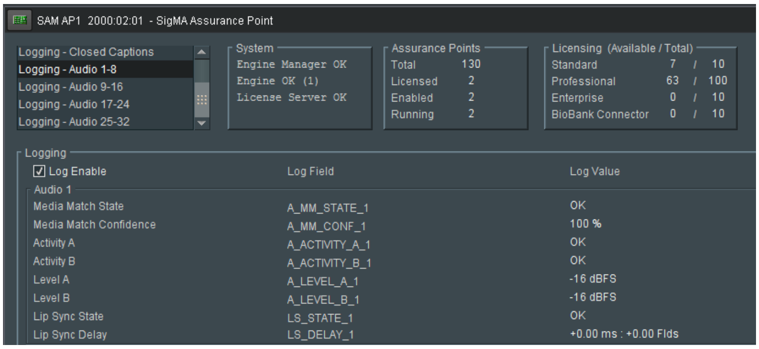
Licensing (Available / Total)			
Standard	8	/	10
Professional	64	/	100
Enterprise	0	/	10
BioBank Connector	0	/	10

Logging

☑ Log Enable	Log Field	Log Value
Closed Captions		
Closed Captions Activity A	CC_ACTIVITY_A	
Closed Captions Activity B	CC_ACTIVITY_B	
Closed Captions State	CC_STATE	
Closed Captions Confidence	CC_CONF	
Relative Delay State	CC_DELAY_STATE	
Relative Delay	CC_DELAY	

The **Logging – Closed Caption** menu will allow the User to Enable or Disable logging of Closed Captions for any particular AP.

12.4 Logging – Audio



System

```
Engine Manager OK
Engine OK (1)
License Server OK
```

Assurance Points

Total	130
Licensed	2
Enabled	2
Running	2

Licensing (Available / Total)

Standard	7	/	10
Professional	63	/	100
Enterprise	0	/	10
BioBank Connector	0	/	10

Logging

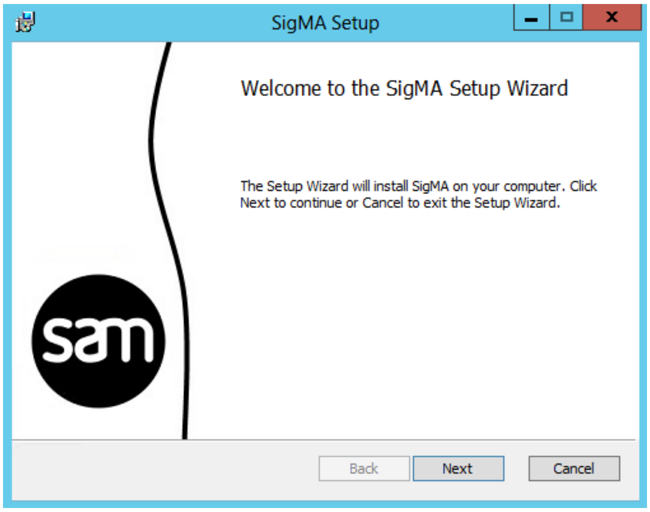
☑ Log Enable	Log Field	Log Value
Audio 1		
Media Match State	A_MM_STATE_1	OK
Media Match Confidence	A_MM_CONF_1	100 %
Activity A	A_ACTIVITY_A_1	OK
Activity B	A_ACTIVITY_B_1	OK
Level A	A_LEVEL_A_1	-16 dBFS
Level B	A_LEVEL_B_1	-16 dBFS
Lip Sync State	LS_STATE_1	OK
Lip Sync Delay	LS_DELAY_1	+0.00 ms : +0.00 Flds

Up to 32 channels of audio can be logged for each AP. The menus are split into groups of 8 audio channels, allow the User to select multiple groups of 8 to be logged.

Appendix A. Installing multiple SigMA Engines

Assuming a **SigMA** and **SigMA Engine** have been installed on a particular server, as per section 2, additional SigMA Engines can be installed on other Hardware Servers on the same network, using the following procedure:

1. Launch the SigMA installer program. A setup wizard will be displayed:

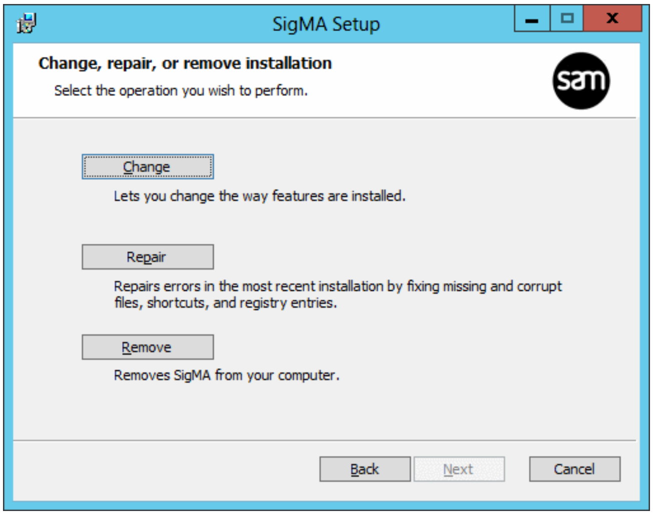


Welcome to the SigMA Setup Wizard

The Setup Wizard will install SigMA on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Select **Next.**

2. Next, the **Change, repair or remove installation** widow will be displayed.



Change, repair, or remove installation

Select the operation you wish to perform.

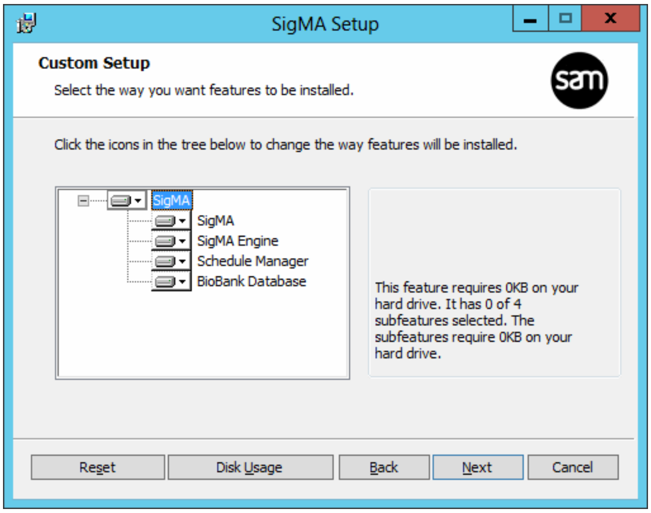
Lets you change the way features are installed.

Repairs errors in the most recent installation by fixing missing and corrupt files, shortcuts, and registry entries.

Removes SigMA from your computer.

Select **Change**, then click **Next.**

3. The **Custom Setup** window will now be displayed.



SigMA Setup

Custom Setup

Select the way you want features to be installed.

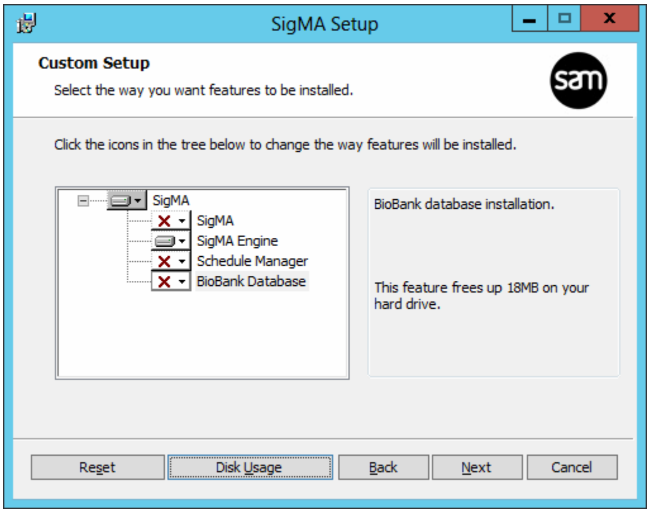
Click the icons in the tree below to change the way features will be installed.

- SigMA
  - SigMA
  - SigMA Engine
  - Schedule Manager
  - BioBank Database

This feature requires 0KB on your hard drive. It has 0 of 4 subfeatures selected. The subfeatures require 0KB on your hard drive.

This menu offers options to select which SigMA components to install.

4. Ensure that only the SigMA engine is selected for install.



SigMA Setup

Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

- SigMA
  - ✗ SigMA
  - SigMA Engine
  - ✗ Schedule Manager
  - ✗ BioBank Database

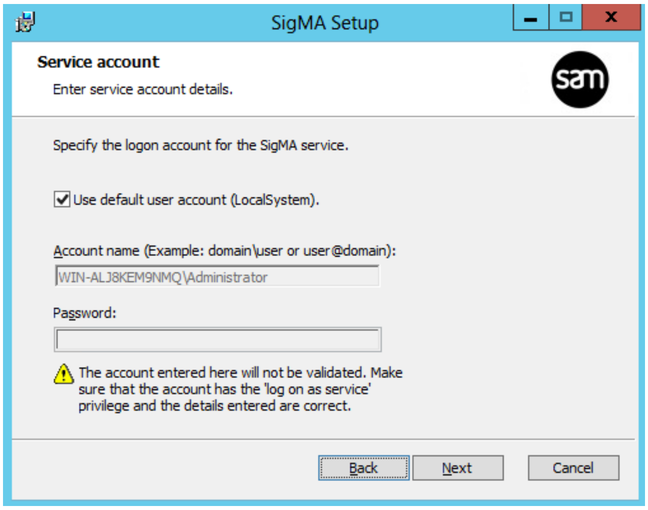
BioBank database installation.

This feature frees up 18MB on your hard drive.

This will ensure that only the SigMA Engine is installed.

Click **Next.**

5. The **Service account** window will now appear.



SigMA Setup

Service account

Enter service account details.

Specify the logon account for the SigMA service.

☑ Use default user account (LocalSystem).

Account name (Example: domain\user or user@domain):

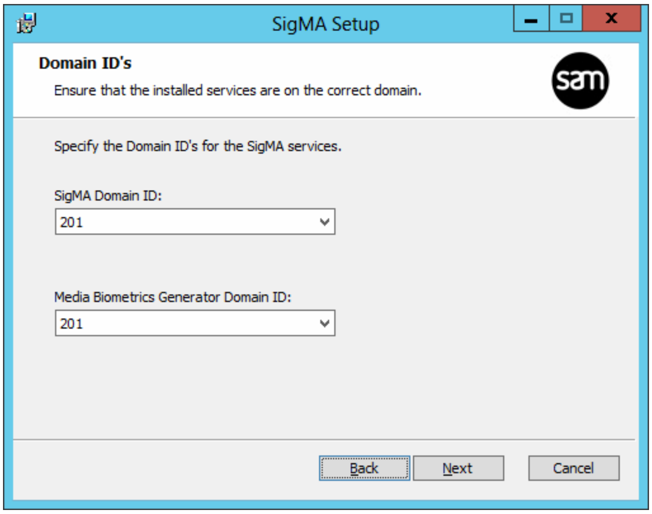
WIN-ALJ8KEM9NMQ\Administrator

Password:

The account entered here will not be validated. Make sure that the account has the 'log on as service' privilege and the details entered are correct.

As with the main install procedure, this window should be left with the default settings. Select **Next.**

6. The SigMA **Domain ID** window will now be displayed.



SigMA Setup

Domain ID's

Ensure that the installed services are on the correct domain.

Specify the Domain ID's for the SigMA services.

SigMA Domain ID:

201

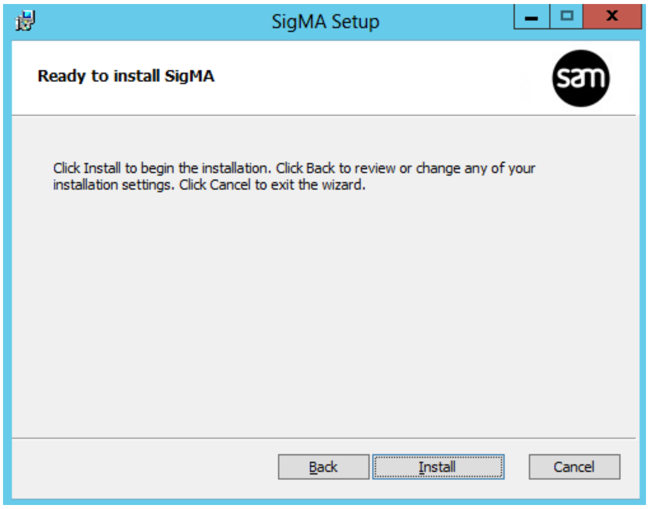
Media Biometrics Generator Domain ID:

201

As previously, under normal circumstances there will only ever be one SigMA installed on a network. Therefore the Domain ID is unimportant and the default setting should be used.

Click **Next** to continue.

7. The **Ready to change SigMA** window will appear.



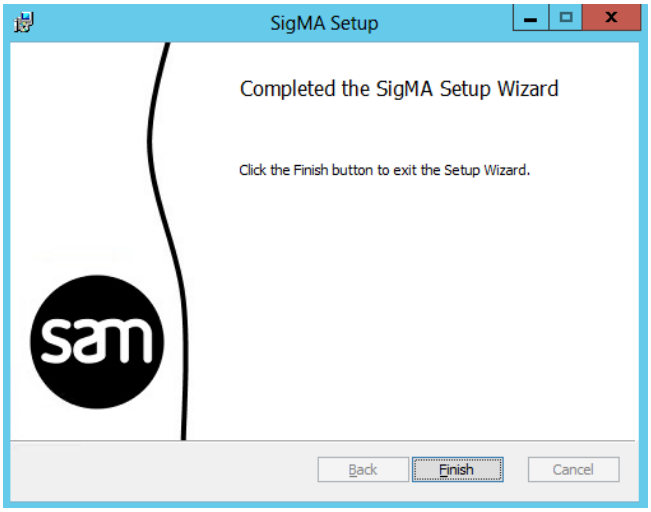
SigMA Setup

Ready to install SigMA

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Click **Install.**

The SigMA Engine will now install. This only takes a few seconds. Once installed a confirmation window will be displayed.



SigMA Setup

Completed the SigMA Setup Wizard

Click the Finish button to exit the Setup Wizard.

Click **Finish.**

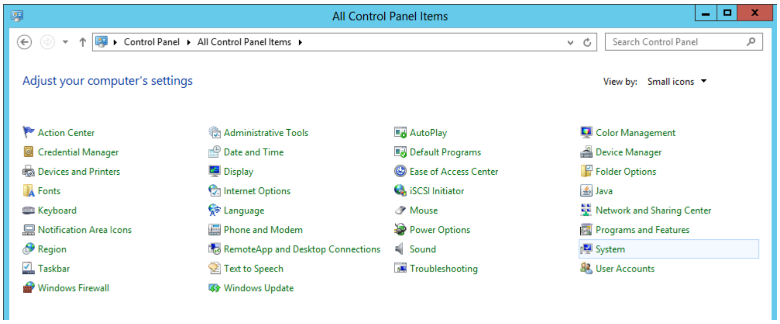
Appendix B. Changing the Domain ID of the SigMA

The **Domain ID** of the SigMA is set during the installation process (as described in section 2 (part 5) above.

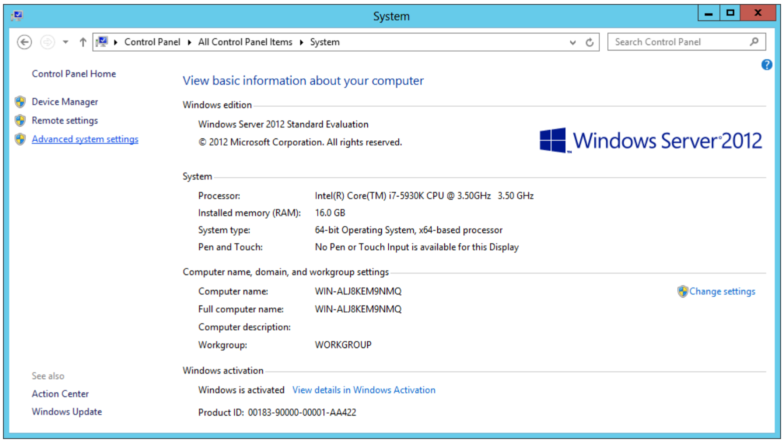
Note that the Domain ID of the SigMA cannot be changed in the RollCall template. If there is a need to change the Domain ID of the SigMA at any time, the following procedure should be applied.

Procedure to change the SigMA Domain ID

1. On the SigMA host PC/Server, open Control Panel, and select **System**



2. Select Advanced System Settings



View basic information about your computer

Windows edition

Windows Server 2012 Standard Evaluation
© 2012 Microsoft Corporation. All rights reserved.

System

Processor: Intel(R) Core(TM) i7-5930K CPU @ 3.50GHz 3.50 GHz
Installed memory (RAM): 16.0 GB
System type: 64-bit Operating System, x64-based processor
Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

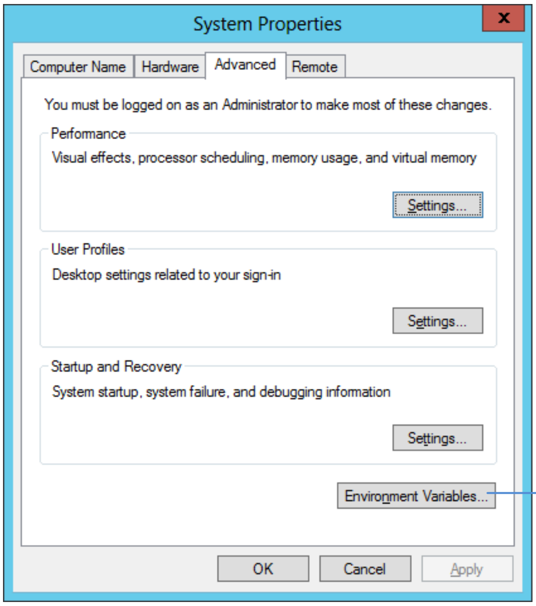
Computer name: WIN-ALJ8KEM9NMQ
Full computer name: WIN-ALJ8KEM9NMQ
Computer description:
Workgroup: WORKGROUP

Windows activation

Windows is activated View details in Windows Activation
Product ID: 00183-90000-00001-AA422

A new window will open titled **System Properties.**

3. In **System Properties,** select **Environmental Variables**, located at the bottom of the Advanced tab.



You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles

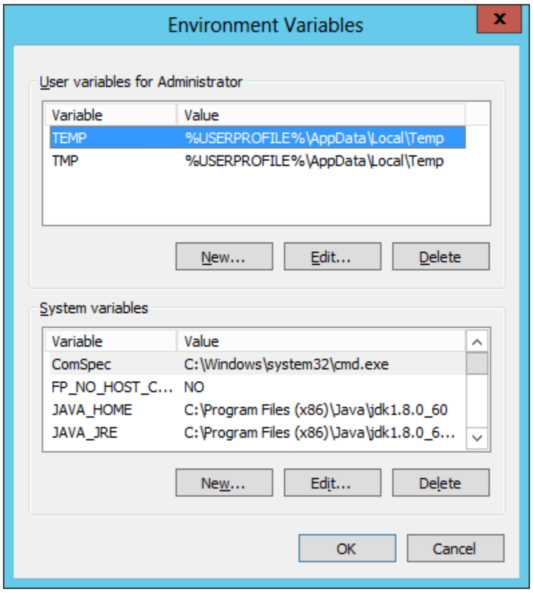
Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information

Select

4. The **Environmental Variables** windows will now appear.



User variables for Administrator

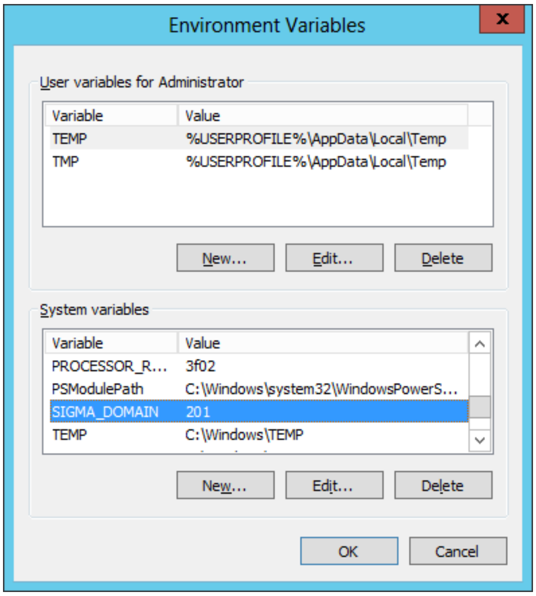
Variable	Value
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

System variables

Variable	Value
ComSpec	C:\Windows\system32\cmd.exe
FP_NO_HOST_C...	NO
JAVA_HOME	C:\Program Files (x86)\Java\jdk1.8.0_60
JAVA_JRE	C:\Program Files (x86)\Java\jdk1.8.0_6...

Within this window the **System Variables** are listed.

5. Scroll down the list of **System Variables** and locate the **SIGMA_DOMAIN.**
   Select **SIGMA_DOMAIN** to highlight it.



User variables for Administrator

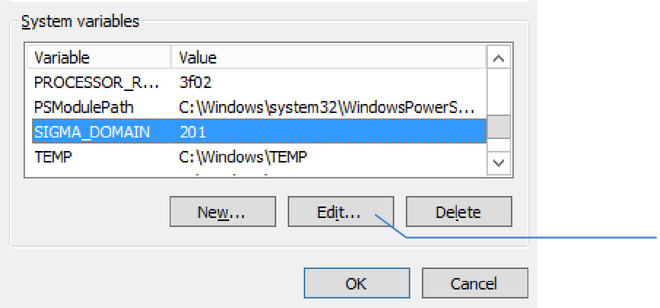
Variable	Value
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

System variables

Variable	Value
PROCESSOR_R...	3f02
PSModulePath	C:\Windows\system32\WindowsPowerS...
SIGMA_DOMAIN	201
TEMP	C:\Windows\TEMP

Note, in this example, the **Domain ID** is currently set to default i.e. 201.

6. In the System Variables field, select **Edit.**

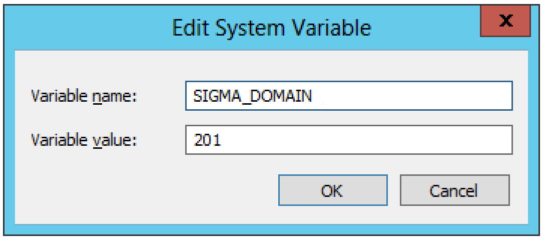


System variables

Variable	Value
PROCESSOR_R...	3f02
PSModulePath	C:\Windows\system32\WindowsPowerS...
SIGMA_DOMAIN	201
TEMP	C:\Windows\TEMP

Select

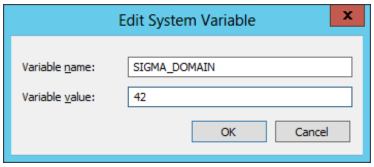
This will bring up the Edit System Variable window.



Variable name: SIGMA_DOMAIN

Variable value: 201

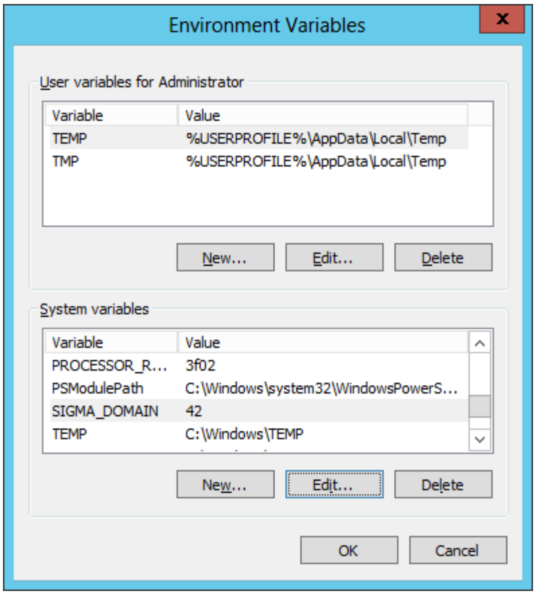
7. Now edit the **Variable value:** field, entering the new Domain Id value.



Variable name: SIGMA_DOMAIN

Variable value: 42

Click OK **to complete the** editing process.



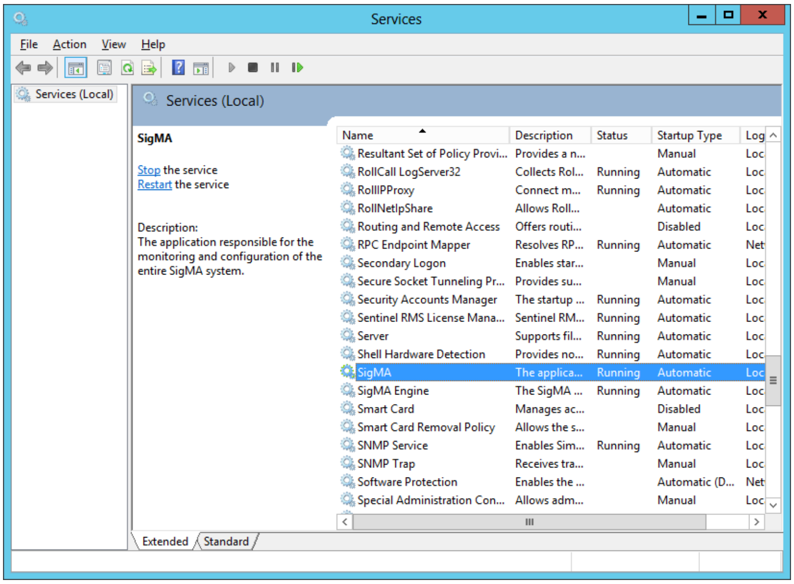
User variables for Administrator

Variable	Value
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

System variables

Variable	Value
PROCESSOR_R…	3f02
PSModulePath	C:\Windows\system32\WindowsPowerS…
SIGMA_DOMAIN	42
TEMP	C:\Windows\TEMP

To make the change of Domain Id take effect, the SigMA Services must be stopped and restarted:



SigMA

Stop the service
Restart the service

Description:
The application responsible for the monitoring and configuration of the entire SigMA system.

Name	Description	Status	Startup Type	Log
Resultant Set of Policy Provi…	Provides a n…		Manual	Loc
RollCall LogServer32	Collects Rol…	Running	Automatic	Loc
RollIPProxy	Connect m…	Running	Automatic	Loc
RollNetIpShare	Allows Roll…		Automatic	Loc
Routing and Remote Access	Offers routi…		Disabled	Loc
RPC Endpoint Mapper	Resolves RP…	Running	Automatic	Net
Secondary Logon	Enables star…		Manual	Loc
Secure Socket Tunneling Pr…	Provides su…		Manual	Loc
Security Accounts Manager	The startup …	Running	Automatic	Loc
Sentinel RMS License Mana…	Sentinel RM…	Running	Automatic	Loc
Server	Supports fil…	Running	Automatic	Loc
Shell Hardware Detection	Provides no…	Running	Automatic	Loc
SigMA	The applica…	Running	Automatic	Loc
SigMA Engine	The SigMA …	Running	Automatic	Loc
Smart Card	Manages ac…		Disabled	Loc
Smart Card Removal Policy	Allows the s…		Manual	Loc
SNMP Service	Enables Sim…	Running	Automatic	Loc
SNMP Trap	Receives tra…		Manual	Loc
Software Protection	Enables the …		Automatic (D…	Net
Special Administration Con…	Allows adm…		Manual	Loc

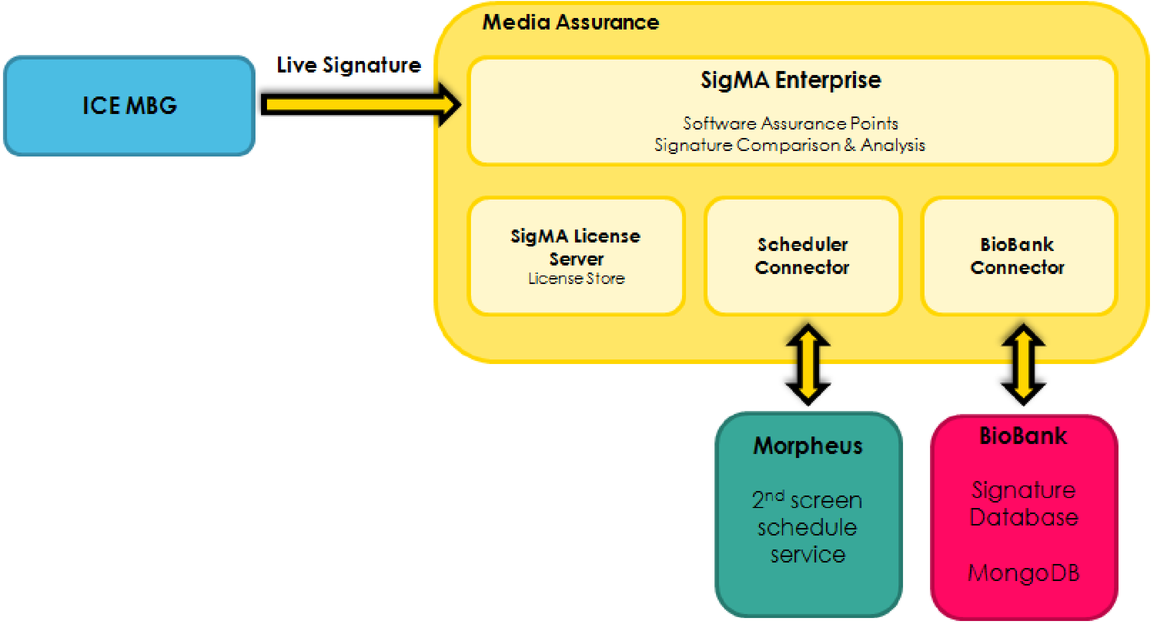
Restart both the SigMA and the SigMA Engine services.

Appendix C. Ice and Morpheus Configuration

Schedule Match is a specific playout Media Assurance service that confirms the live playout media (from ICE) matches the Scheduled ingested media (from Morpheus). Media is ingested into the database using MBG XF.

SigMA communicates with Morpheus using the Second Screen service. This provides the required Material ID to perform a lookup in the database. The pre-ingested signature is then compared with the live signature.

This Appendix describes how to configure ICE and Morpheus.



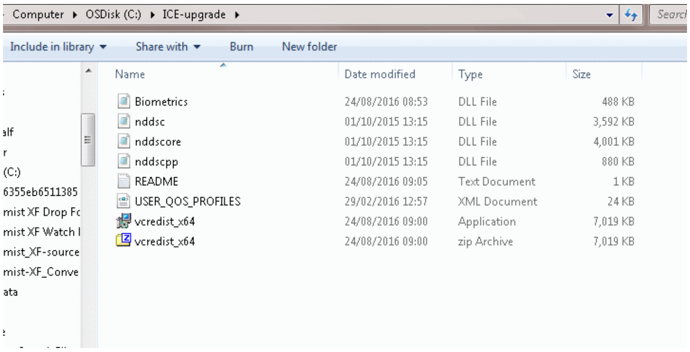
Prerequisites

- ICE needs to be upgraded to version 5.0.0.5146 and the Morpheus and ICE must on the same network as SigMA
- ICE Biometrics.dll needs updating as per the following instruction.

ICE Biometrics.dll updating procedure:

Setting up ICE for Biometrics.

1. Unzip the Upgrade.zip file to a location local to the ICE.



Name	Date modified	Type	Size
Biometrics	24/08/2016 08:53	DLL File	488 KB
nddsc	01/10/2015 13:15	DLL File	3,592 KB
nddscore	01/10/2015 13:15	DLL File	4,001 KB
nddscpp	01/10/2015 13:15	DLL File	880 KB
README	24/08/2016 09:05	Text Document	1 KB
USER_QOS_PROFILES	29/02/2016 12:57	XML Document	24 KB
vcredist_x64	24/08/2016 09:00	Application	7,019 KB
vcredist_x64	24/08/2016 09:00	zip Archive	7,019 KB

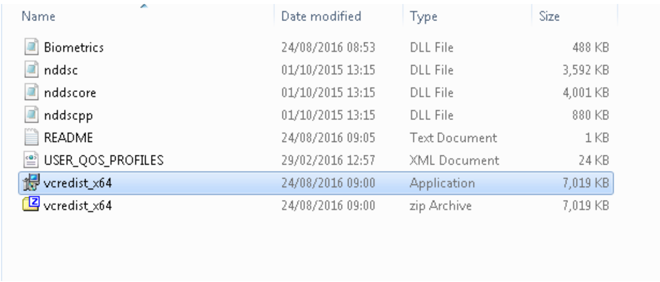
2. Copy the files:
   - Biometrics.dll
   - nddsc.dll
   - nddscore.dll
   - nddscpp.dll

   to the directory: C:\Program Files\Snell\Snell ICE

3. Copy the file:
   - USER_QOS_PROFILES.xml

   to directory C:\Users\snell\AppData\Local\Snell\Morpheus ICE

4. Run the executable ***vcredist_x64.exe*** to install msvc2012 runtime distributable



Name	Date modified	Type	Size
Biometrics	24/08/2016 08:53	DLL File	488 KB
nddsc	01/10/2015 13:15	DLL File	3,592 KB
nddscore	01/10/2015 13:15	DLL File	4,001 KB
nddscpp	01/10/2015 13:15	DLL File	880 KB
README	24/08/2016 09:05	Text Document	1 KB
USER_QOS_PROFILES	29/02/2016 12:57	XML Document	24 KB
vcredist_x64	24/08/2016 09:00	Application	7,019 KB
vcredist_x64	24/08/2016 09:00	zip Archive	7,019 KB

5. Set the environment variable

   NDDSHOME=C:\Program Files\rti_connext_dds-5.2.0

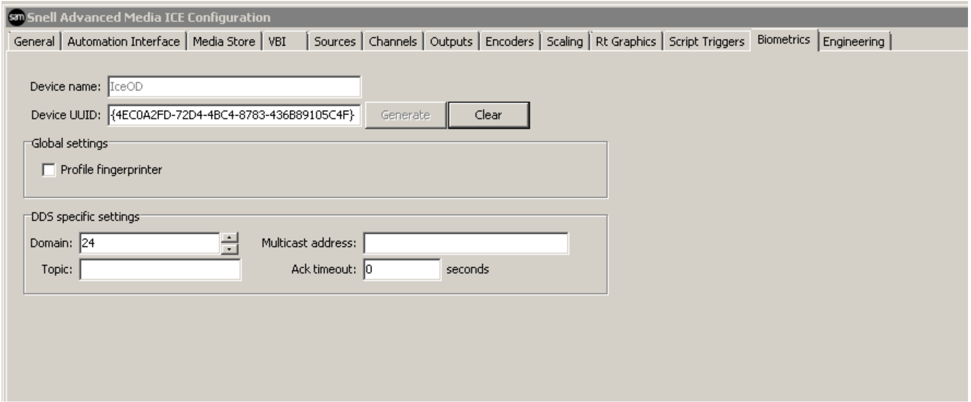
   I don't believe you actually need Rti 5.2 installed.

   But you do need this environment variable to be defined as ICE code checks for it.

ICE Configuration

To set the ICE configuration, launch the configuration app on the desktop (this writes settings to the registry). After making a change you have to click Apply and restart ICE.

Biometrics tab:



Device name: IceOD

Device UUID: {4EC0A2FD-72D4-4BC4-8783-436B89105C4F}

Global settings

☐ Profile fingerprinter

DDS specific settings

Domain: 24

Multicast address:

Topic:

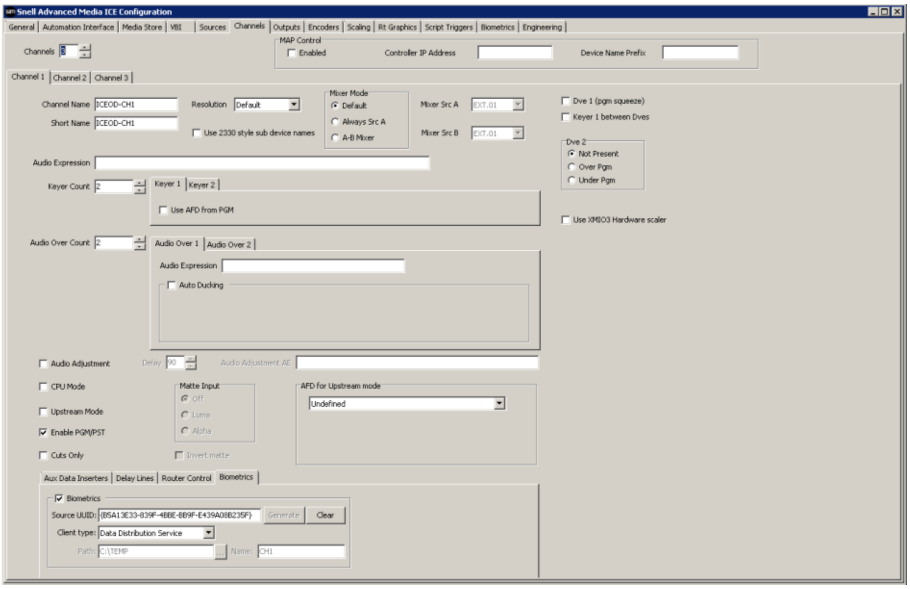
Ack timeout: 0 seconds

- If necessary, generate a Device UUID and enter a friendly name.
- Make sure **Profile fingerprinter** is not set.
- Set the DDS domain that you want the fingerprints generated on.
- Leave **Topic** blank and set **Ack timeout** to 0.
- Leave the multicast address blank. This automatically engages the use of **unicast** (current requirement of the system).

Channels Tab

This allows you to enable fingerprint generation for a given channel by ticking ‘Biometrics’ for that channel.

Note: this should be done on the Channels tab not the Outputs tab to ensure a clean video source for the fingerprints if you are doing a database match.



Channels: 3

MAP Control: □ Enabled; Controller IP Address: ; Device Name Prefix:

Channel Name: ICEOD-CH1

Short Name: ICEOD-CH1

Resolution: Default

□ Use 2330 style sub device names

Mixer Mode: ● Default ○ Always Src A ○ A-B Mixer

Mixer Src A: EXT.01

Mixer Src B: EXT.01

□ Dve 1 (pgm squeeze)

□ Keyer 1 between Dves

Dve 2: ● Not Present ○ Over Pgm ○ Under Pgm

Audio Expression:

Keyer Count: 2

□ Use AFD from PGM

□ Use XMIO3 Hardware scaler

Audio Over Count: 2

Audio Expression:

□ Auto Ducking

□ Audio Adjustment; Delay: 90; Audio Adjustment AE:

□ CPU Mode

Matte Input: ● Off ○ Luma ○ Alpha

AFD for Upstream mode: Undefined

□ Upstream Mode

☑ Enable PGM/PST

□ Cuts Only

□ Invert matte

☑ Biometrics

Source UUID: {B5A13E33-839F-4BBE-BB9F-E439A08B235F}

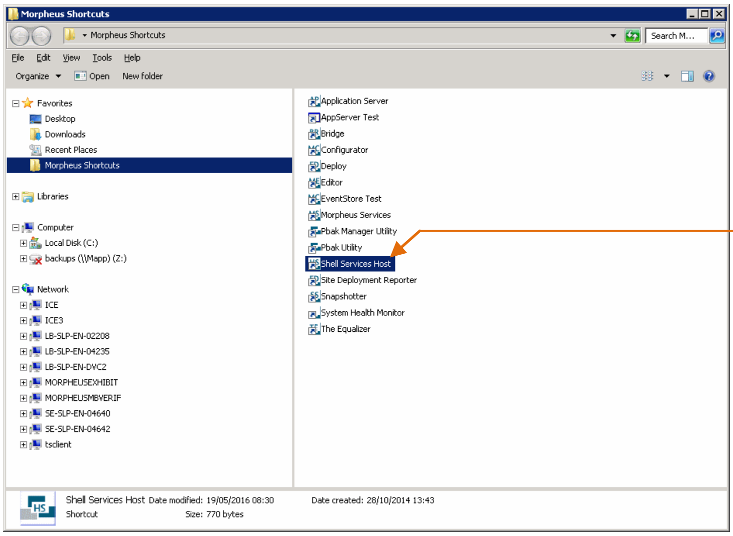
Client type: Data Distribution Service

Path: C:\TEMP; Name: CH1

- If necessary, generate a Source UUID, the friendly name will match the channel name.
- Set the **Client Type** to **Data Distribution Service** (DDS)

Morpheus Configuration

On the Morpheus machine, locate the folder: Morpheus Shortcuts.



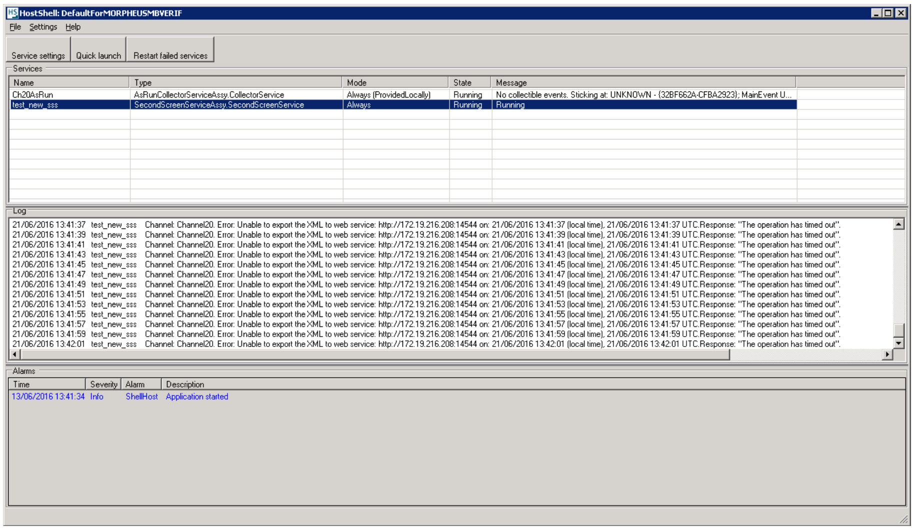
Shell Services Host Date modified: 19/05/2016 08:30 Date created: 28/10/2014 13:43
Shortcut Size: 770 bytes

Start:

Shall Services Host

Start the **Shell Services Host** application.

A new window will appear called **Host Shall Default for MORPHEUSMBVERIF**

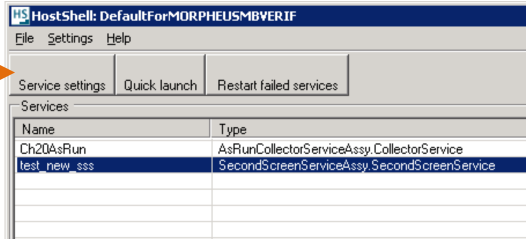


Name	Type	Mode	State	Message
Ch20AsRun	AsRunCollectorServiceAssy.CollectorService	Always (ProvidedLocally)	Running	No collectible events. Sticking at: UNKNOWN - {32BF662A-CFBA2923}; MainEvent U...
test_new_sss	SecondScreenServiceAssy.SecondScreenService	Always	Running	Running

```
21/06/2016 13:41:37  test_new_sss  Channel: Channel20. Error: Unable to export the XML to web service: http://172.19.216.208:14544 on: 21/06/2016 13:41:37 (local time), 21/06/2016 13:41:37 UTC.Response: "The operation has timed out".
21/06/2016 13:41:39  test_new_sss  Channel: Channel20. Error: Unable to export the XML to web service: http://172.19.216.208:14544 on: 21/06/2016 13:41:39 (local time), 21/06/2016 13:41:39 UTC.Response: "The operation has timed out".
21/06/2016 13:41:41  test_new_sss  Channel: Channel20. Error: Unable to export the XML to web service: http://172.19.216.208:14544 on: 21/06/2016 13:41:41 (local time), 21/06/2016 13:41:41 UTC.Response: "The operation has timed out".
21/06/2016 13:41:43  test_new_sss  Channel: Channel20. Error: Unable to export the XML to web service: http://172.19.216.208:14544 on: 21/06/2016 13:41:43 (local time), 21/06/2016 13:41:43 UTC.Response: "The operation has timed out".
21/06/2016 13:41:45  test_new_sss  Channel: Channel20. Error: Unable to export the XML to web service: http://172.19.216.208:14544 on: 21/06/2016 13:41:45 (local time), 21/06/2016 13:41:45 UTC.Response: "The operation has timed out".
21/06/2016 13:41:47  test_new_sss  Channel: Channel20. Error: Unable to export the XML to web service: http://172.19.216.208:14544 on: 21/06/2016 13:41:47 (local time), 21/06/2016 13:41:47 UTC.Response: "The operation has timed out".
21/06/2016 13:41:49  test_new_sss  Channel: Channel20. Error: Unable to export the XML to web service: http://172.19.216.208:14544 on: 21/06/2016 13:41:49 (local time), 21/06/2016 13:41:49 UTC.Response: "The operation has timed out".
21/06/2016 13:41:51  test_new_sss  Channel: Channel20. Error: Unable to export the XML to web service: http://172.19.216.208:14544 on: 21/06/2016 13:41:51 (local time), 21/06/2016 13:41:51 UTC.Response: "The operation has timed out".
21/06/2016 13:41:53  test_new_sss  Channel: Channel20. Error: Unable to export the XML to web service: http://172.19.216.208:14544 on: 21/06/2016 13:41:53 (local time), 21/06/2016 13:41:53 UTC.Response: "The operation has timed out".
21/06/2016 13:41:55  test_new_sss  Channel: Channel20. Error: Unable to export the XML to web service: http://172.19.216.208:14544 on: 21/06/2016 13:41:55 (local time), 21/06/2016 13:41:55 UTC.Response: "The operation has timed out".
21/06/2016 13:41:57  test_new_sss  Channel: Channel20. Error: Unable to export the XML to web service: http://172.19.216.208:14544 on: 21/06/2016 13:41:57 (local time), 21/06/2016 13:41:57 UTC.Response: "The operation has timed out".
21/06/2016 13:41:59  test_new_sss  Channel: Channel20. Error: Unable to export the XML to web service: http://172.19.216.208:14544 on: 21/06/2016 13:41:59 (local time), 21/06/2016 13:41:59 UTC.Response: "The operation has timed out".
21/06/2016 13:42:01  test_new_sss  Channel: Channel20. Error: Unable to export the XML to web service: http://172.19.216.208:14544 on: 21/06/2016 13:42:01 (local time), 21/06/2016 13:42:01 UTC.Response: "The operation has timed out".
```

Time	Severity	Alarm	Description
13/06/2016 13:41:34	Info	ShellHost	Application started

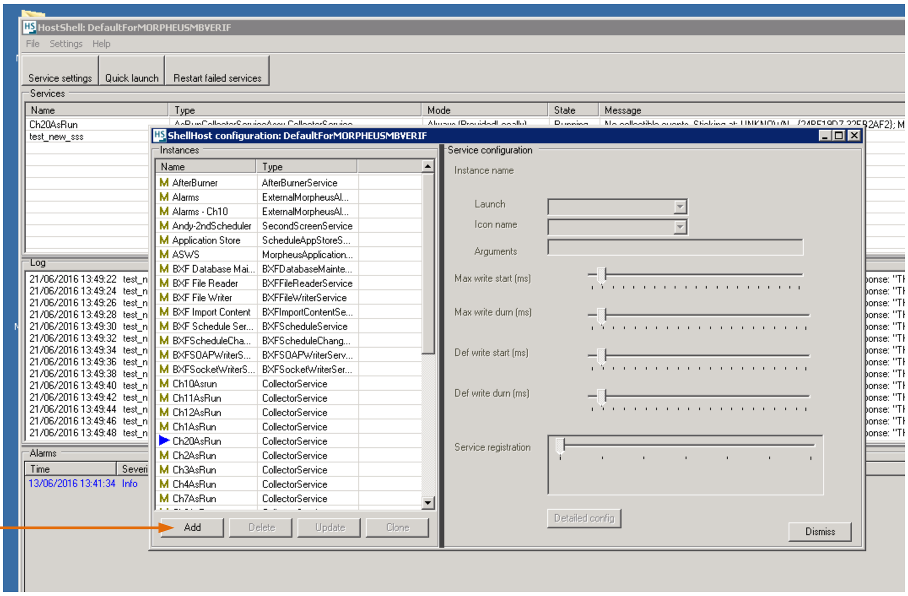
Click Service settings



Name	Type
Ch20AsRun	AsRunCollectorServiceAssy.CollectorService
test_new_sss	SecondScreenServiceAssy.SecondScreenService

Select

A new window will appear titled: **ShallHost configuration**



Name	Type	Mode	State	Message
Ch20AsRun				
test_new_sss				

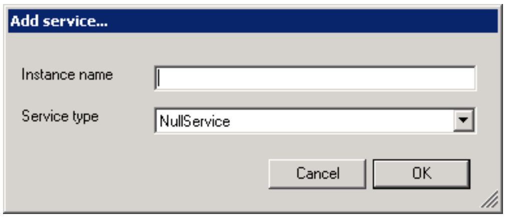
```
21/06/2016 13:49:22  test_n
21/06/2016 13:49:24  test_n
21/06/2016 13:49:26  test_n
21/06/2016 13:49:28  test_n
21/06/2016 13:49:30  test_n
21/06/2016 13:49:32  test_n
21/06/2016 13:49:34  test_n
21/06/2016 13:49:36  test_n
21/06/2016 13:49:38  test_n
21/06/2016 13:49:40  test_n
21/06/2016 13:49:42  test_n
21/06/2016 13:49:44  test_n
21/06/2016 13:49:46  test_n
21/06/2016 13:49:48  test_n
```

Time	Severi
13/06/2016 13:41:34	Info

Name	Type
AfterBurner	AfterBurnerService
Alarms	ExternalMorpheusAl...
Alarms - Ch10	ExternalMorpheusAl...
Andy-2ndScheduler	SecondScreenService
Application Store	ScheduleAppStoreS...
ASWS	MorpheusApplication...
BXF Database Mai...	BXFDatabaseMainte...
BXF File Reader	BXFFileReaderService
BXF File Writer	BXFFileWriterService
BXF Import Content	BXFImportContentSe...
BXF Schedule Ser...	BXFScheduleService
BXFScheduleCha...	BXFScheduleChang...
BXFSOAPWriterS...	BXFSOAPWriterServ...
BXFSocketWriterS...	BXFSocketWriterSer...
Ch10Asrun	CollectorService
Ch11AsRun	CollectorService
Ch12AsRun	CollectorService
Ch1AsRun	CollectorService
Ch20AsRun	CollectorService
Ch2AsRun	CollectorService
Ch3AsRun	CollectorService
Ch4AsRun	CollectorService
Ch7AsRun	CollectorService

Select

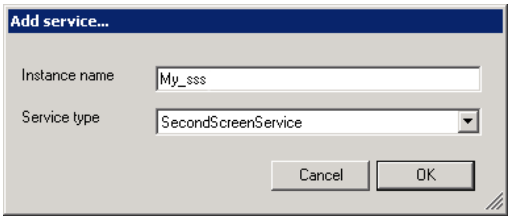
Select **Add** and the **Add service…** window will appear



Instance name

Service type: NullService

Enter the **Instance name** and select **Service type** as below:



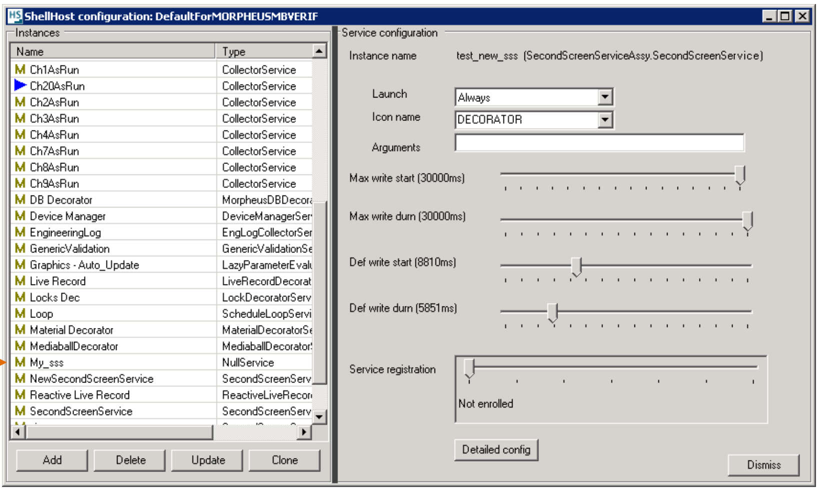
Instance name: My_sss

Service type: SecondScreenService

In this example the **Instance name** has been entered as: ***My_sss***

Note: **Service type (SecondScreenService)**, is selected from the drop down menu.

The new **instance** now appears in the Instances window:



New Instance

ShellHost configuration: DefaultForMORPHEUSMBVERIF

Instances

Name	Type
Ch1AsRun	CollectorService
Ch20AsRun	CollectorService
Ch2AsRun	CollectorService
Ch3AsRun	CollectorService
Ch4AsRun	CollectorService
Ch7AsRun	CollectorService
Ch8AsRun	CollectorService
Ch9AsRun	CollectorService
DB Decorator	MorpheusDBDecora
Device Manager	DeviceManagerSer
EngineeringLog	EngLogCollectorSer
GenericValidation	GenericValidationSe
Graphics - Auto_Update	LazyParameterEvalu
Live Record	LiveRecordDecorat
Locks Dec	LockDecoratorServ
Loop	ScheduleLoopServi
Material Decorator	MaterialDecoratorSe
MediaballDecorator	MediaballDecorator
My_sss	NullService
NewSecondScreenService	SecondScreenServ
Reactive Live Record	ReactiveLiveRecor
SecondScreenService	SecondScreenServ

Service configuration

Instance name: test_new_sss (SecondScreenServiceAssy.SecondScreenService)

Launch: Always

Icon name: DECORATOR

Arguments:

Max write start (30000ms)

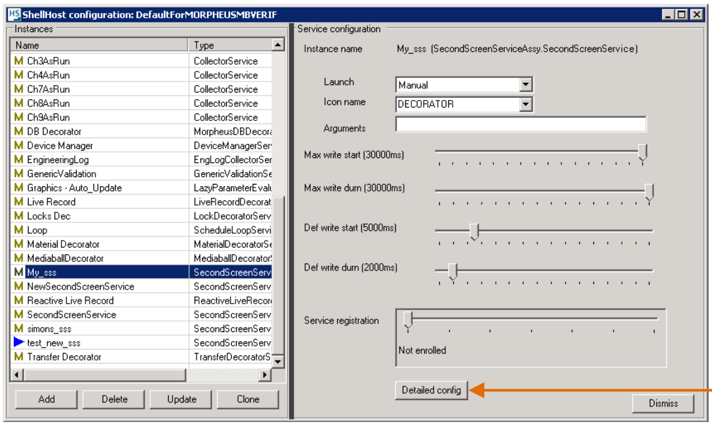
Max write durn (30000ms)

Def write start (8810ms)

Def write durn (5851ms)

Service registration: Not enrolled

Click on the New Instance to highlight it, then select **Detailed config** in the right hand pane:



Select

ShellHost configuration: DefaultForMORPHEUSMBVERIF

Instances

Name	Type
Ch3AsRun	CollectorService
Ch4AsRun	CollectorService
Ch7AsRun	CollectorService
Ch8AsRun	CollectorService
Ch9AsRun	CollectorService
DB Decorator	MorpheusDBDecora
Device Manager	DeviceManagerSer
EngineeringLog	EngLogCollectorSer
GenericValidation	GenericValidationSe
Graphics - Auto_Update	LazyParameterEvalu
Live Record	LiveRecordDecorat
Locks Dec	LockDecoratorServ
Loop	ScheduleLoopServi
Material Decorator	MaterialDecoratorSe
MediaballDecorator	MediaballDecorator
My_sss	SecondScreenServ
NewSecondScreenService	SecondScreenServ
Reactive Live Record	ReactiveLiveRecor
SecondScreenService	SecondScreenServ
simons_sss	SecondScreenServ
test_new_sss	SecondScreenServ
Transfer Decorator	TransferDecoratorS

Service configuration

Instance name: My_sss (SecondScreenServiceAssy.SecondScreenService)

Launch: Manual

Icon name: DECORATOR

Arguments:

Max write start (30000ms)

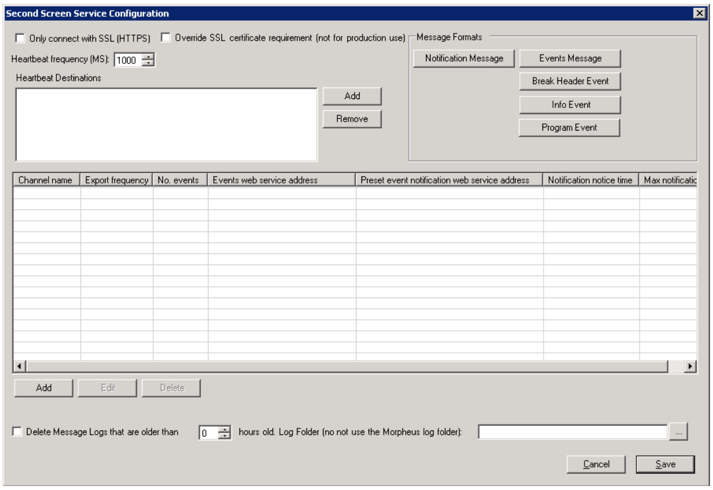
Max write durn (30000ms)

Def write start (5000ms)

Def write durn (2000ms)

Service registration: Not enrolled

A new window will appear called **Second Screen service Configuration**



Second Screen Service Configuration

☐ Only connect with SSL (HTTPS) ☐ Override SSL certificate requirement (not for production use)

Heartbeat frequency (MS): 1000

Heartbeat Destinations

Message Formats

Channel name	Export frequency	No. events	Events web service address	Preset event notification web service address	Notification notice time	Max notificatic

☐ Delete Message Logs that are older than 0 hours old. Log Folder (no not use the Morpheus log folder):

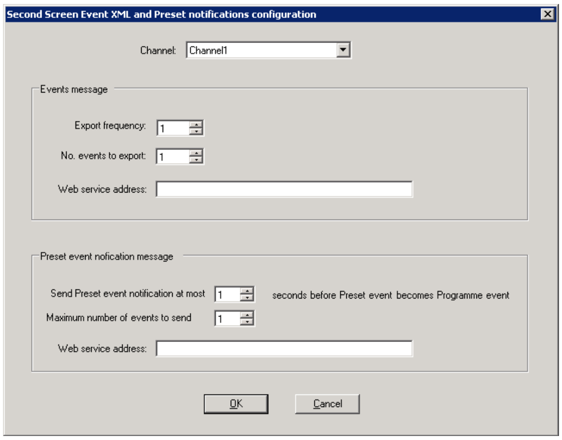
Note: the **Channel Name** needs to be the name of the channel of the associated Biometrics ICE.

Click Add, and enter

http://<IP address of machine running ScheduleManager>:14544
for both the Events web service address and the preset event notification web service address.

Select **Add** at the bottom of the window. A new window will appear called:

Second Screen Event XML and Preset notification configuration



Second Screen Event XML and Preset notifications configuration

Channel: Channel1

Events message

Export frequency: 1

No. events to export: 1

Web service address:

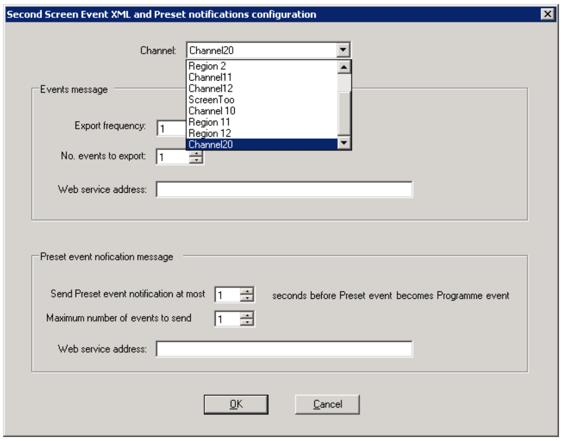
Preset event nofication message

Send Preset event notification at most 1 seconds before Preset event becomes Programme event

Maximum number of events to send 1

Web service address:

Choose the appropriate channel from the dropdown list.



Second Screen Event XML and Preset notifications configuration

Channel: Channel20

- Region 2
- Channel11
- Channel12
- ScreenToo
- Channel 10
- Region 11
- Region 12
- Channel20

Events message

Export frequency: 1

No. events to export: 1

Web service address:

Preset event nofication message

Send Preset event notification at most 1 seconds before Preset event becomes Programme event

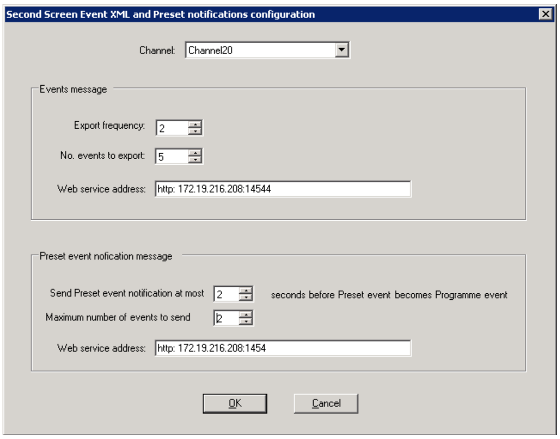
Maximum number of events to send 1

Web service address:

Note: for settings of the fields; **Export frequency** and **No. events to export,** consult the Morpheus User manual.

Enter the web service addresses:

http://<IP address of machine running ScheduleManager>:14544 for both the **Events** web service address and the **Preset** event notification web service address.



Second Screen Event XML and Preset notifications configuration

Channel: Channel20

Events message

Export frequency: 2

No. events to export: 5

Web service address: http: 172.19.216.208:14544

Preset event nofication message

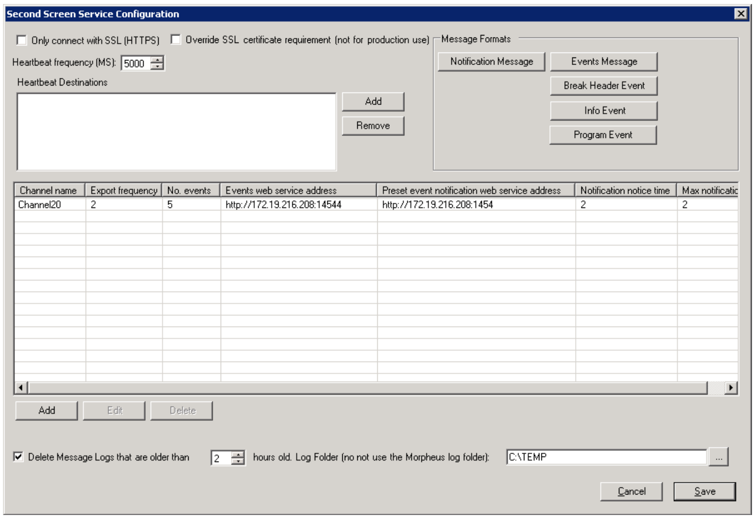
Send Preset event notification at most 2 seconds before Preset event becomes Programme event

Maximum number of events to send 2

Web service address: http: 172.19.216.208:1454

Click OK

The new Second Screen Service will now appear in the **Second Screen Service Configuration** window:



Second Screen Service Configuration

☐ Only connect with SSL (HTTPS) ☐ Override SSL certificate requirement (not for production use)

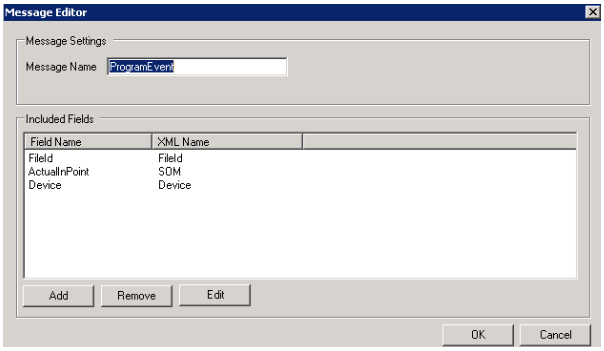
Heartbeat frequency (MS): 5000

Heartbeat Destinations

Channel name	Export frequency	No. events	Events web service address	Preset event notification web service address	Notification notice time	Max notificatic
Channel20	2	5	http://172.19.216.208:14544	http://172.19.216.208:1454	2	2

☑ Delete Message Logs that are older than 2 hours old. Log Folder (no not use the Morpheus log folder): C:\TEMP

Click, **Program Event** and add the following (copy these strings exactly):



Message Editor

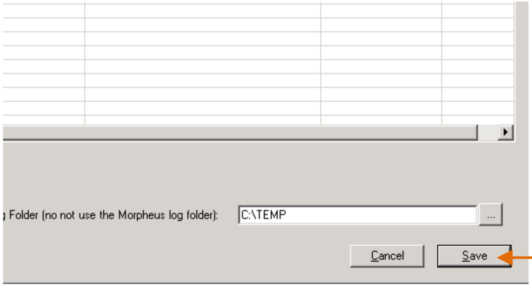
Message Settings

Message Name ProgramEvent

Included Fields

Field Name	XML Name
FileId	FileId
ActualInPoint	SOM
Device	Device

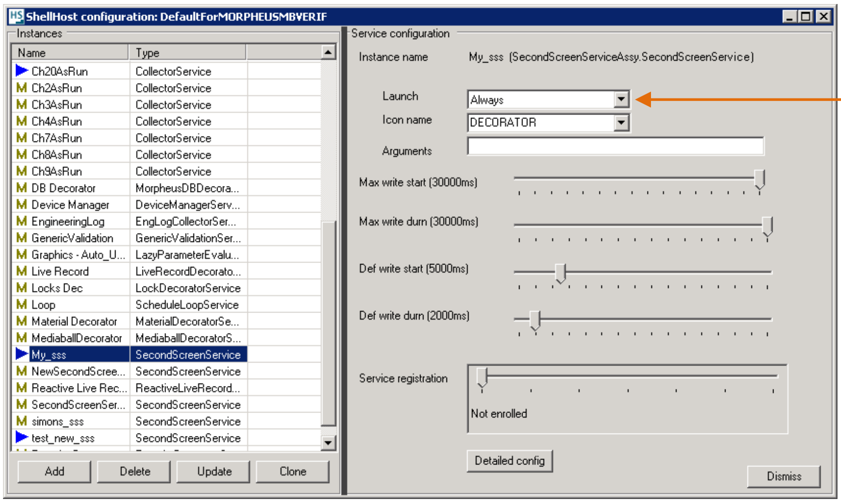
Save this configuration:



Folder (no not use the Morpheus log folder): C:\TEMP

Save config

Then in the main Shell Host services app, make sure the new Host Service is always running.



ShellHost configuration: DefaultForMORPHEUSMBVERIF

Instances

Name	Type
▶ Ch20AsRun	CollectorService
M Ch2AsRun	CollectorService
M Ch3AsRun	CollectorService
M Ch4AsRun	CollectorService
M Ch7AsRun	CollectorService
M Ch8AsRun	CollectorService
M Ch9AsRun	CollectorService
M DB Decorator	MorpheusDBDecora...
M Device Manager	DeviceManagerServ...
M EngineeringLog	EngLogCollectorSer...
M GenericValidation	GenericValidationSer...
M Graphics - Auto_U...	LazyParameterEvalu...
M Live Record	LiveRecordDecorato...
M Locks Dec	LockDecoratorService
M Loop	ScheduleLoopService
M Material Decorator	MaterialDecoratorSe...
M MediaballDecorator	MediaballDecoratorS...
▶ My_sss	SecondScreenService
M NewSecondScree...	SecondScreenService
M Reactive Live Rec...	ReactiveLiveRecord...
M SecondScreenSer...	SecondScreenService
M simons_sss	SecondScreenService
▶ test_new_sss	SecondScreenService

Service configuration

Instance name: My_sss (SecondScreenServiceAssy.SecondScreenService)

Launch: Always

Icon name: DECORATOR

Arguments:

Max write start (30000ms)

Max write durn (30000ms)

Def write start (5000ms)

Def write durn (2000ms)

Service registration: Not enrolled

Set to: **Always**

The **Schedule Manager** (and therefore) SigMA should get the channel information.