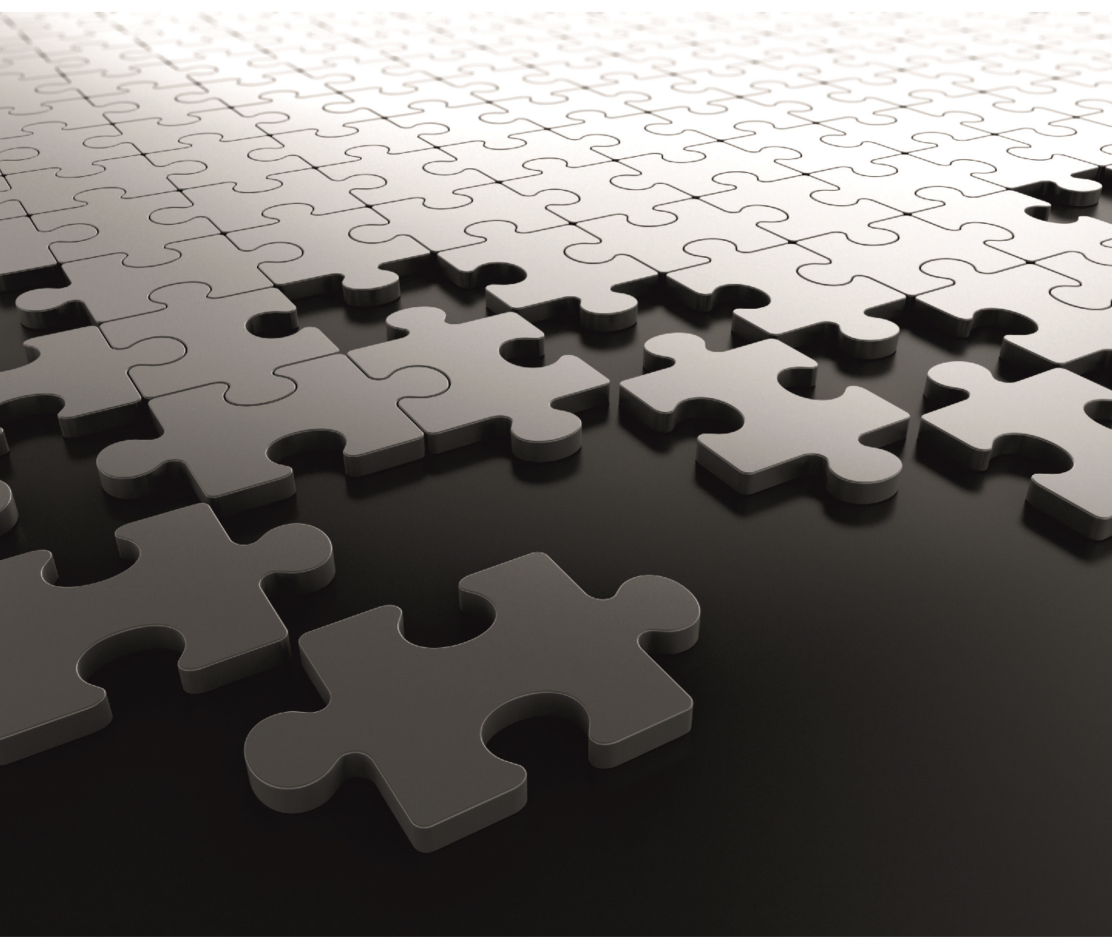


SATATYA SAMAS

Installation Guide



Matrix SATATYA SAMAS

Video Management System

Installation Guide



Documentation Disclaimer

Matrix Comsec reserves the right to change, at any time, without prior notice, the product design, specifications, components, as engineering and manufacturing may warrant.

This is a general documentation for all models of the product. The product may not support some of the features and facilities described in the documentation.

Information in this documentation may change from time to time. Matrix Comsec reserves the right to revise information in this publication for any reason without prior notice. Matrix Comsec makes no warranties with respect to this documentation and disclaims any implied warranties. While every precaution has been taken in the preparation of this quick start, Matrix Comsec assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Neither Matrix Comsec nor its affiliates shall be liable to the buyer of this product or third parties for damages, losses, costs or expenses incurred by the buyer or third parties as a result of: accident, misuse or abuse of this product or unauthorized modifications, repairs or alterations to this product or failure to strictly comply with Matrix Comsec's operating and maintenance instructions.

Copyright

All rights reserved. No part of this quick start may be copied or reproduced in any form or by any means without the prior written consent of Matrix Comsec.

Warranty

For product registration and warranty related details visit us at.

<https://www.matrixcomsec.com/warranty/#IP-video-surveillance>

Version 6

Release date: May 28, 2025

Contents

Getting Started	1
<i>Introduction</i>	<i>1</i>
<i>System Requirements</i>	<i>1</i>
Software Installation	5
<i>System Pre-requisites</i>	<i>5</i>
<i>SATATYA SAMAS Installer Utility</i>	<i>6</i>
<i>Create/Upgrade/Backup Database</i>	<i>20</i>
<i>Create GPU Model</i>	<i>28</i>
<i>Uninstallation and Reinstallation</i>	<i>32</i>
<i>Installing SAMAS Components at Different Sites</i>	<i>34</i>
<i>Service Installation</i>	<i>36</i>
<i>SSL Configurations</i>	<i>89</i>
<i>Port Forwarding</i>	<i>94</i>
Licensing of SATATYA SAMAS	99

Getting Started

Introduction

This document provides the information about installation of Matrix SATATYA SAMAS. Please read this document carefully to get acquainted with the product before installing and operating it.

System Requirements

The SATATYA SAMAS has the following components:

- Management Server
- Recording Server
- License Server
- IVA Server
- Notification Server
- Failover Server
- Transcoding Server
- ONVIF Server
- Smart Client
- Admin Client
- Media Player

For Installation of SATATYA SAMAS components in different computers, following specifications are required.



Make sure the date and time of all the PCs on which the various Servers and Clients are installed are same, to ensure smooth functionality of SAMAS. If not, it may impact features like Recording and Playback.

Management Server

Hardware/Software	Minimum	Recommended
CPU	Intel Core i3	Intel Core i5 or higher
RAM	4 GB	8 GB
Network	100 Mbps	1 Gbps

Hardware/Software	Minimum	Recommended
Hard disk Space	10 GB	50 GB free space
Operating System	Windows10	Windows10 or above Windows Server 2019 Standard or higher (if adding 400 cameras or more).

Recording Server/Failover Server

Hardware/Software	Minimum	Recommended
CPU	Intel Core i5	Intel Core i7 or higher
RAM	4 GB	8 GB
Network	100 Mbps	1 Gbps
Hard disk Space	10 GB free space	100 GB free space
Operating System	Windows10	Windows10 or above Windows Server 2019 Standard or higher (if adding 400 cameras or more).

Smart Client

Hardware/Software	Minimum	Recommended
CPU	Intel Core i3	Intel Core i5 or higher
RAM	4 GB	8 GB
Network	100 Mbps	1 Gbps
Hard disk Space	10 GB free space	50 GB free space
Operating System	Windows10	Windows10 or above
Graphics Accelerator	1 GB Memory (Inbuilt)	4GB- NVIDIA Graphics card (Inbuilt/External Card)

Admin Client

Hardware/Software	Minimum	Recommended
CPU	Intel Core i3	Intel Core i5 or higher
RAM	4 GB	8 GB
Network	100 Mbps	1 Gbps
Hard disk Space	10 GB free space	10 GB free space
Operating System	Windows10	Windows10 or above

IVA Server

Hardware/Software	Minimum	Recommended
CPU	Intel Core i5	Intel Core i7 or higher
RAM	8 GB	8-12 GB or higher
Network	100 Mbps	1 Gbps
Hard disk Space	10 GB free space	100 GB free space
Operating System	Windows10	Windows10 or above
Graphics Accelerator	1 GB Memory (Inbuilt)	4GB- NVIDIA Graphics card (Inbuilt/External Card)
Frequency Clock	2.5 GHz	3.4 GHz or higher

Transcoding Server

Hardware/Software	Minimum	Recommended
CPU	Intel Core i5	Intel Core i7 or higher
RAM	4 GB	8 GB
Network	100 Mbps	1 Gbps
Hard disk Space	10 GB free space	100 GB free space
Operating System	Windows10	Windows10 or above

ONVIF Server

Hardware/Software	Minimum	Recommended
CPU	Intel Core i5	Intel Core i7 or higher
RAM	4 GB	8 GB
Network	1 Gbps	1 Gbps
Hard disk Space	10 GB free space	100 GB free space
Operating System	Windows10	Windows10 or above

Software Installation

System Pre-requisites

Make sure the following are installed in your computer before you begin with the installation:

- Microsoft .NET Framework 4.5 and above
- Windows Installer 3.1
- Microsoft SQL Server 2008 R2 SP2
- Microsoft Visual C++ 2015-2019 Redistributable - 14.24.28127
- Access DB Engine 14.0.6119.5000

Make sure the following pre-requisites are fulfilled to configure **Object Detection**¹ and **Face Detection**²:

- GPU is affixed in the PC where IVA Server and Smart Client are installed. The required GPU is NVIDIA GTX³.
- If you have multiple GPU affixed in your PC, make sure NVIDIA GTX is affixed at the first position.
- GPU Model is created using the SATATYA SAMAS GPU Model Creator Utility. For detailed GPU Model creation process, refer to [“Create GPU Model”](#).

Along with this, make sure you activate the **Object Classification** license along with the desired module license to configure the same in the Admin Client. For details, refer to the SATATYA SAMAS Admin Client Manual, General Settings > License Management Settings.

1. *Object Detection, Object Type in all the IVA Events and Object Classification License are not available in the current Software Release. These will be included in the upcoming release.*
2. *This feature is not available in the current Software Release. It will be included in the upcoming release.*
3. *Recommended GPU is NVIDIA GTX-1050/1650.*



For SAMAS V2R1 to V3R8, .NET framework 4.0 or higher is recommended and from V4R1 and later .NET Framework 4.5 and above is recommended.

To enhance security from SAMAS V6R1 and onwards, we have introduced data security for data at rest as well as in transit. Hence, if you are upgrading SAMAS to V6R1, then make sure all the components are also upgraded to the same version to ensure smooth functioning.

If you have already enabled SSL in the software version you have installed and you are upgrading the same to V6R1, then after the re-installation process completes, you will have to manually configure all the Server Managers in order to retain the SSL communication between different entities of SAMAS.

SATATYA SAMAS Installer Utility

The SATATYA SAMAS Software Installation setup is available on the Portal. The URL of the portal is:

<ftp://matrixtelecomsolutions.com/SecurityProducts/SATATYA/SATATYA%20SAMAS/>

In the Windows PC, double-click on **This PC** option on the desktop and paste the above link in the Location bar to access the setup.



For credentials, contact Matrix Channel Partners or Matrix Tech Team at Techcommunity@MatrixComSec.com

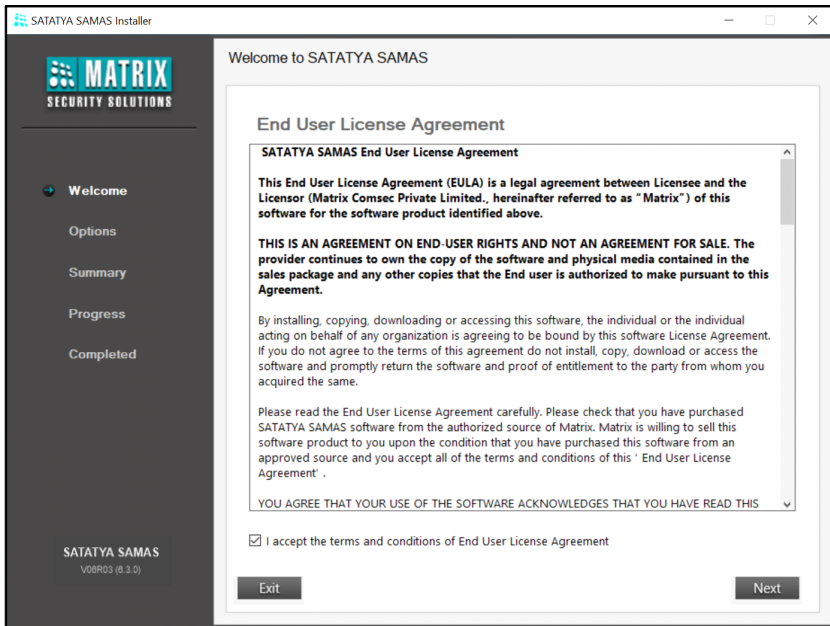
To start with the software installation, follow the steps given below:

1. Right-click on **SATATYA_SAMAS_Installer** and click **Run as administrator**.

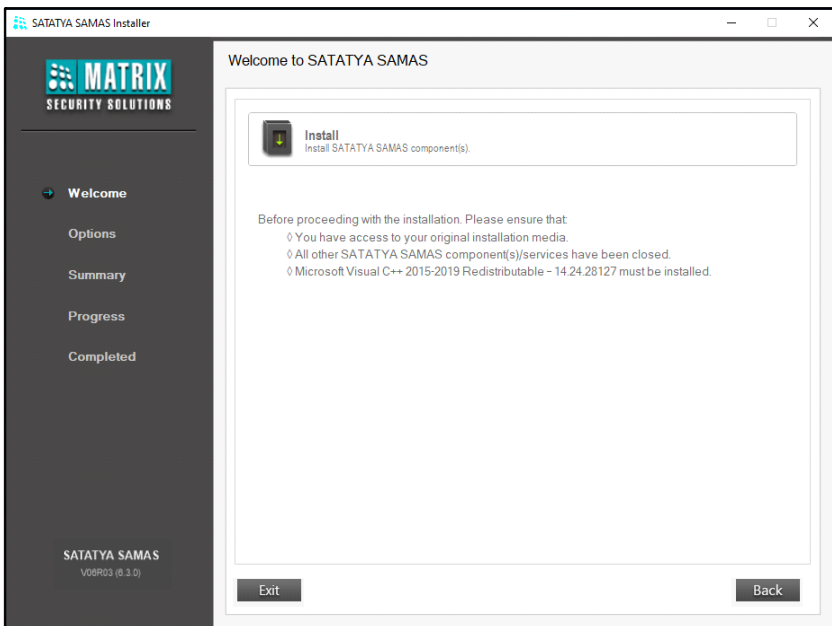
Name	Date modified	Type	Size
Help	17-Apr-18 6:29 PM	File folder	
Setup	17-Apr-18 6:29 PM	File folder	
F-R&D-SWD-09 (Software Release to SWQA)_...	15-Dec-16 6:47 PM	Microsoft Word 9...	209 KB
SAMASInstallerNew	23-Nov-15 6:39 PM	XML Document	8 KB
SATATYA_SAMAS_Installer	29-Nov-16 11:50 A...	Application	1,204 KB

Administrator rights are required for installing the SATATYA setup.

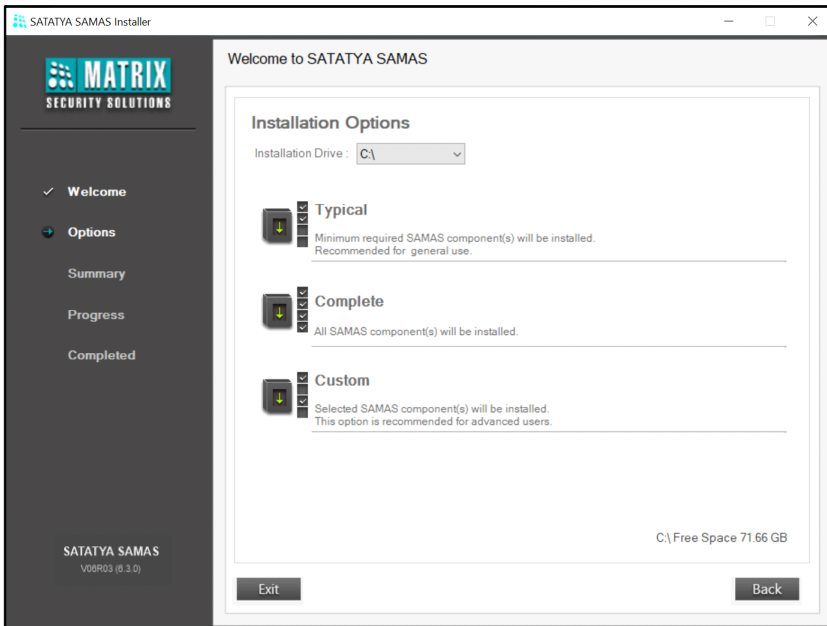
2. The **License Agreement** screen appears. Select the check box to accept the terms and conditions. Click **Next** to continue the installation process.



3. Click **Install** to initiate the installation process.



- Now select the **Installation Drive** from the drop-down list.



Choose the type of installation from the following options:

- **Typical:** Minimum required SAMAS component(s) will be installed. Refer to [“Typical Installation”](#).
- **Complete:** All the SAMAS components will be installed. Refer to [“Complete Installation”](#).
- **Custom:** For the users who may wish to install the components like Management Server, Recording Server and Admin Client at different locations on different computers. Refer to [“Custom Installation”](#).

The GPU Model Creator Utility will be installed automatically in Typical and Complete installation. In Custom installation, the GPU Model Creator Utility will be installed automatically if either Smart Client or IVA Server is selected for installation. For details, refer to [“Create GPU Model”](#).

The SAMAS Default Certificate (Digital Certificate) will be installed automatically irrespective of the type of Installation. You can upload a custom SSL Certificate, if required or use the SAMAS Default Certificate to enable secure communication between all the SAMAS Components. For details, refer to respective Server Manager in [“Service Installation”](#).

Typical Installation

- If you choose Typical installation, follow **Steps 1-4** explained above and select **Typical** option.

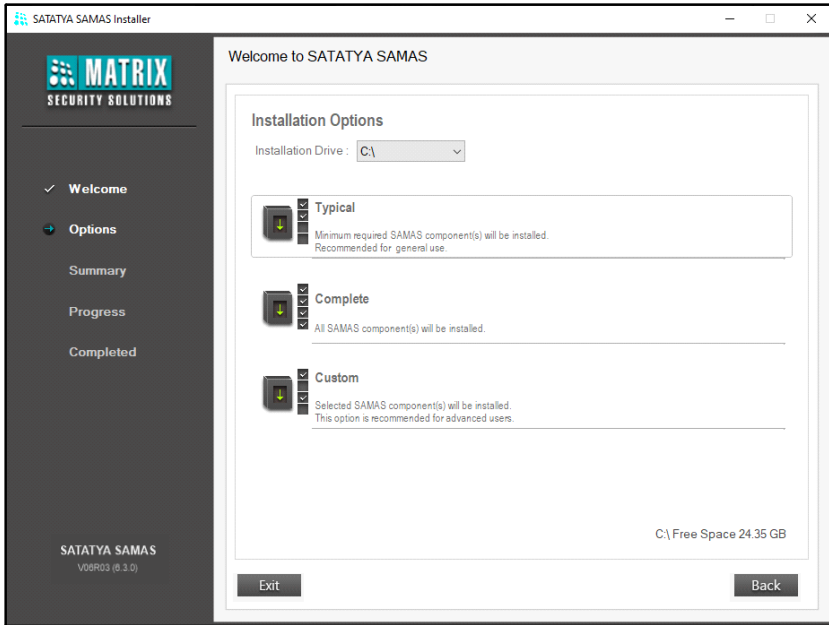


Image Storage Drive

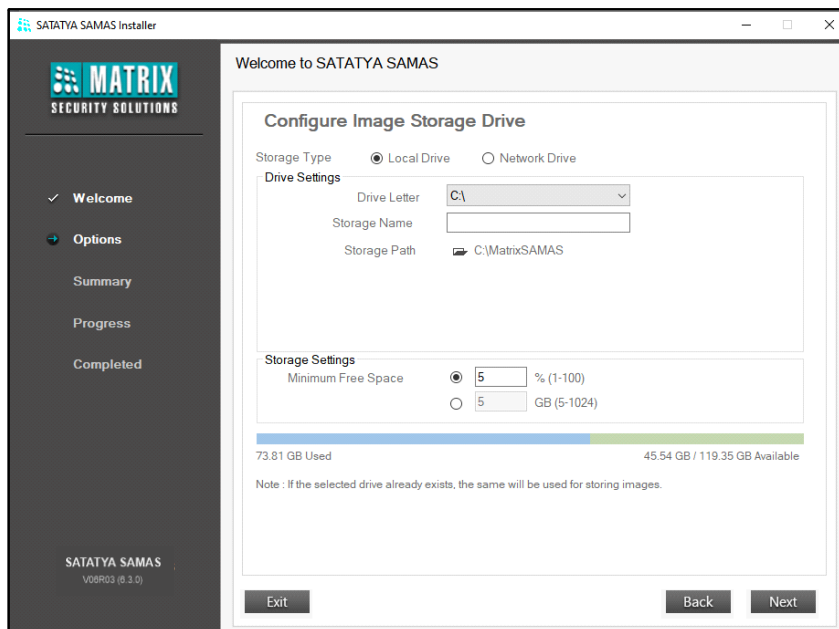
- You need to configure the Image Storage Drive as shown below.



The Image Storage option will appear only during the first installation process. Once configured, you will not be asked to configure this option again.

*If you wish to change the configurations you can do the same from **Admin Client > Servers & Devices > System Components > Management Server > Storage.***

For the Storage Type = Local Drive,



- **Drive Settings**

- Select the required **Drive Letter** of the Local Drive from the drop-down list. For Example: C:\
- Enter the desired **Storage Name**. For Example: Image Drive. In Storage Name, you can enter upto 50 characters. Default: Blank.
- Browse to select the **Storage Path** (folder) in which the images will be stored. Default: Blank.

- **Storage Settings**

- Select the desired option for **Minimum Free Space** — Percentage (Valid Range: 1-100, Default: 5) or GB (Valid Range: 5-1024, Default: 5). Enter the value which is to be maintained in the selected storage drive.

For Storage Type = Network Drive,

The screenshot shows the 'Configure Image Storage Drive' window in the SATATYA SAMAS installer. The 'Storage Type' is set to 'Network Drive'. Under 'Drive Settings', the 'Drive Letter' is 'A:\', 'Storage Name' is empty, 'Storage Path' has a folder icon, 'Username' is empty, and 'Password' is empty. A 'Connect' button is below these fields. Under 'Storage Settings', 'Minimum Free Space' is set to '5 % (1-100)'. A note at the bottom says: 'Note : If the selected drive already exists, the same will be used for storing images.' At the bottom of the window are 'Exit', 'Back', and 'Next' buttons.

- **Drive Settings**

- Select the required **Drive Letter** of the Local Drive from the drop-down list. For Example: F:\
- Enter the desired **Storage Name**. For Example: Image Drive. In Storage Name, you can enter upto 50 characters. Default: Blank.
- Browse to select the **Storage Path** (folder) in which the images will be stored or enter the location of the server manually. For example: \\192.168.103.54. In Storage Path, you can enter upto 255 characters. Default: Blank.



Storage Path supports both IPv4/IPv6 Address of a system or Server Name where you wish to create Network Drive.

- *If you wish to configure IPv6 Address, make sure you enclose the IPv6 Address in square brackets, for example, [2001:db8::1].*
- *If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.*
- Provide the **Username** and **Password** of the computer/server to which the (network) drive belongs. In Username and Password, you can enter upto 50 characters. Default: Blank.

- **Storage Settings**

- Select the desired option for **Minimum Free Space** — Percentage (Range: 1-100%, Default: 5) or GB (Range: 5-1024, Default: 5). Enter the value which is to be maintained in the selected storage drive.

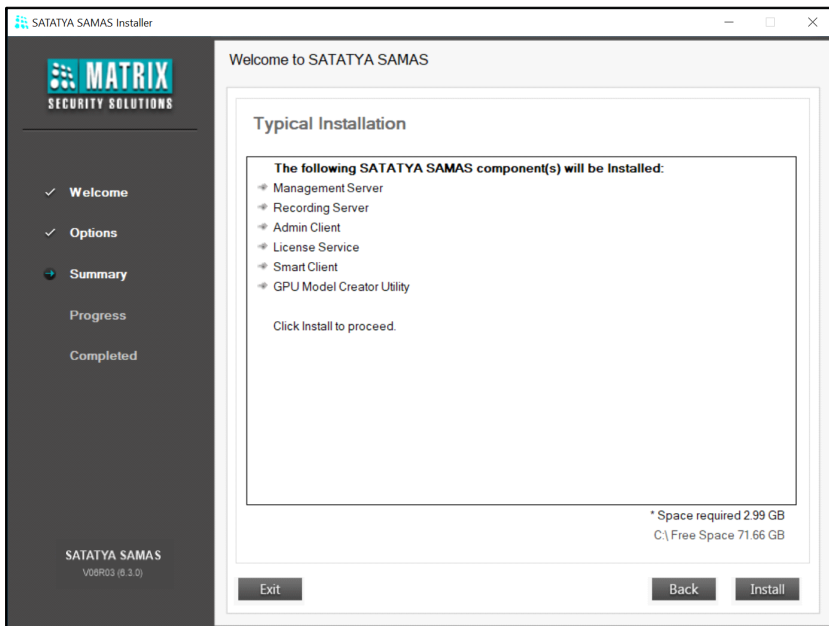
Click **Connect** to connect with the configured Network Drive.

- Once the drive is connected successfully, click **Next** to proceed with the component installation.



If you are upgrading MS from any lower version to V04R03 or later then, the image transfer process will take place once the MS starts. This is a one time process in which the current images present in the database will be transferred to the configured Image Storage Drive.

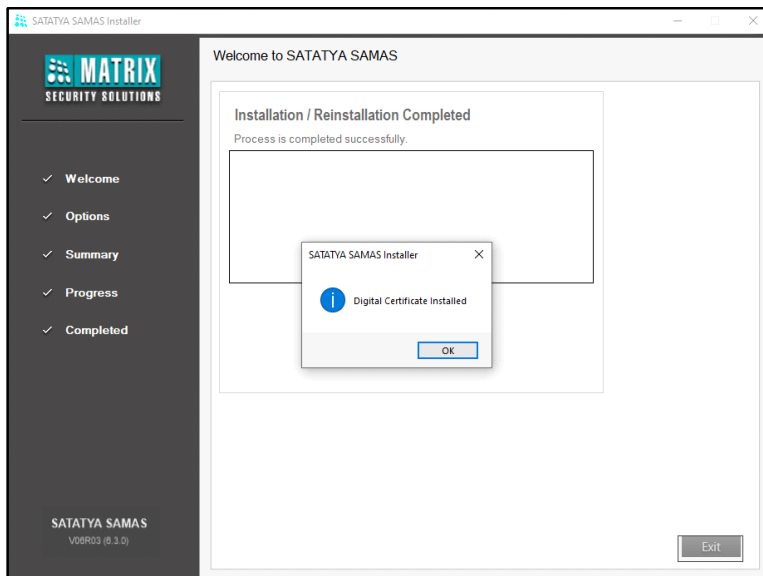
- The components to be installed will be listed as shown below. Click **Install**.



For the Management Service and Notification Service to function, Microsoft SQL Express 2008 R2 SP2 is required.

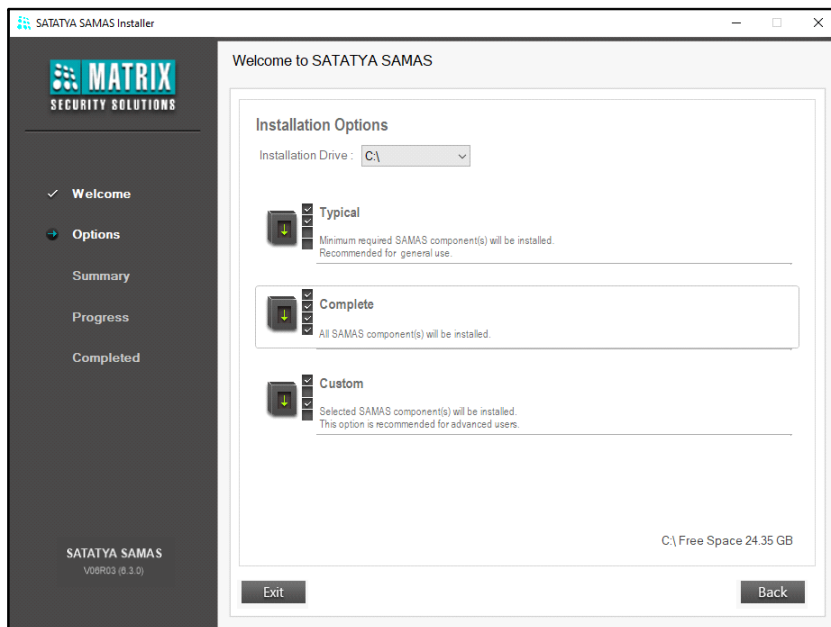
The system will start installing the SAMAS components.

- Click **Exit** to exit from the installation window or click the **Click Here** link to create, upgrade or take backup of the SATATYA SAMAS database. For more information, refer to [“Creating/Upgrading Database”](#).



Complete Installation

- If you choose Complete Installation, follow **Steps 1-4** explained above and select **Complete**.

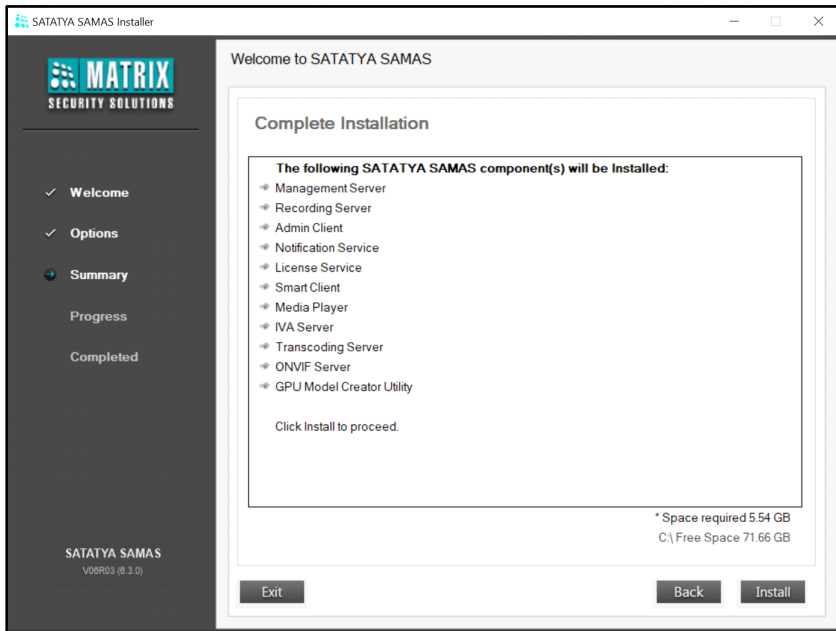


- Configure the Image Storage Drive. Refer [“Image Storage Drive”](#) for more information.
- Once the Storage Drive is configured, click **Next** to proceed further with the installation.



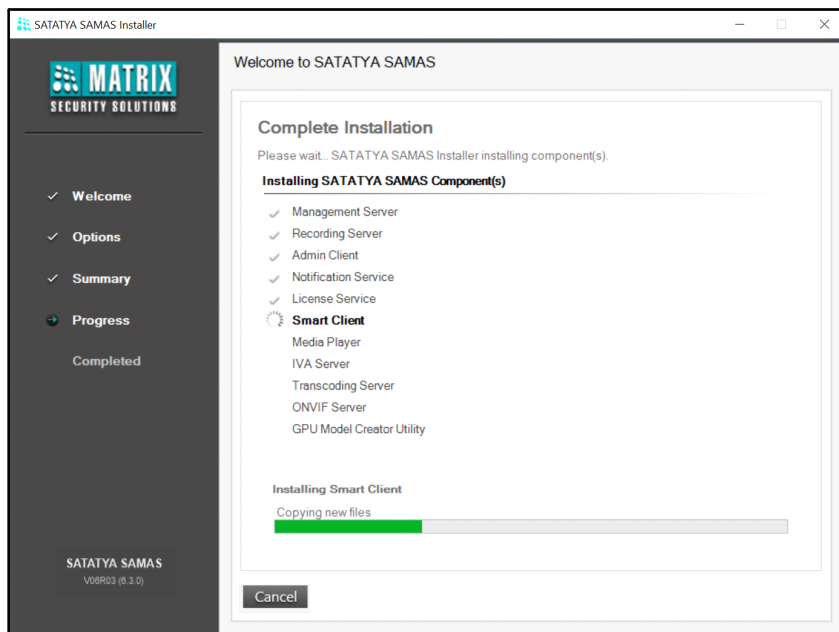
In case you have installed any component before then, the list of the following will be displayed:

- *components that will be installed*
 - *components that are already installed*
 - *components that will not be installed*
- Click **Install**.

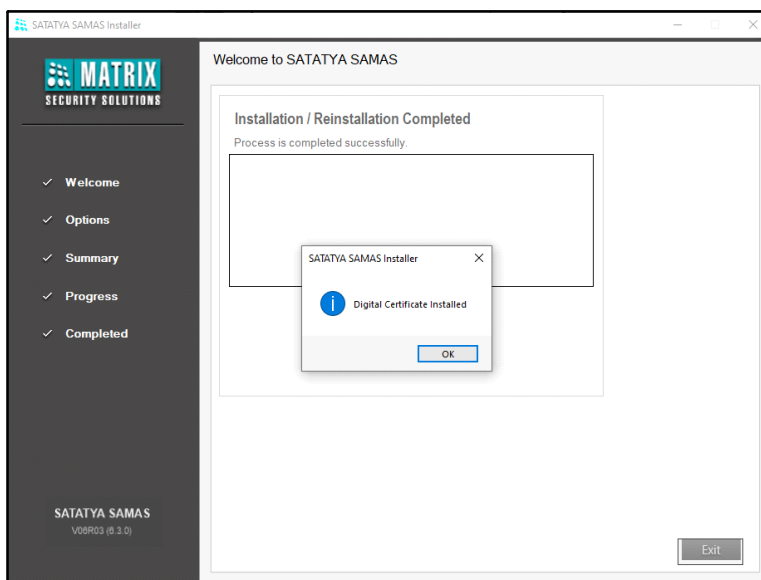


For the Management Service and Notification Service to function, Microsoft SQL Express 2008 R2 SP2 is required.

The system will start installing all the SAMAS components.

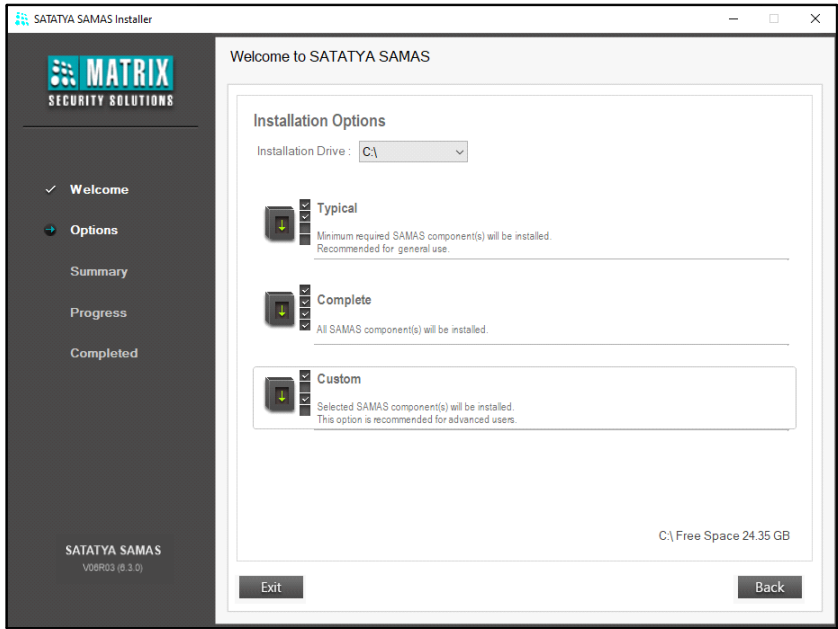


- Click **Exit** to exit from the installation window or click on the **Click Here** link to create, upgrade or take backup of the SATATYA SAMAS database. For more information, refer to “[Creating/Upgrading Database](#)”.

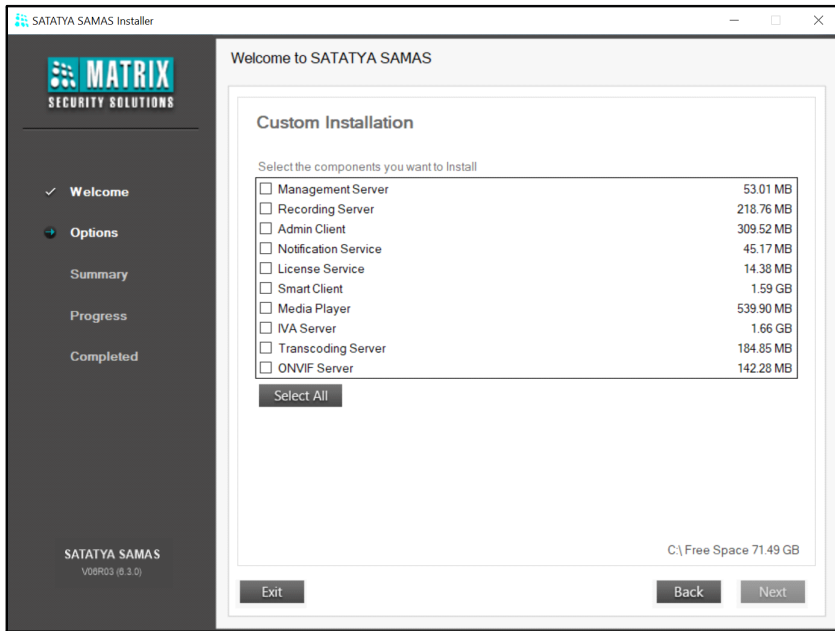


Custom Installation

- If you choose Custom Installation, follow **Steps 1-4** explained above and select **Custom**.



- Select check boxes of the desired components from the list that you wish to install. Click **Next** to continue.

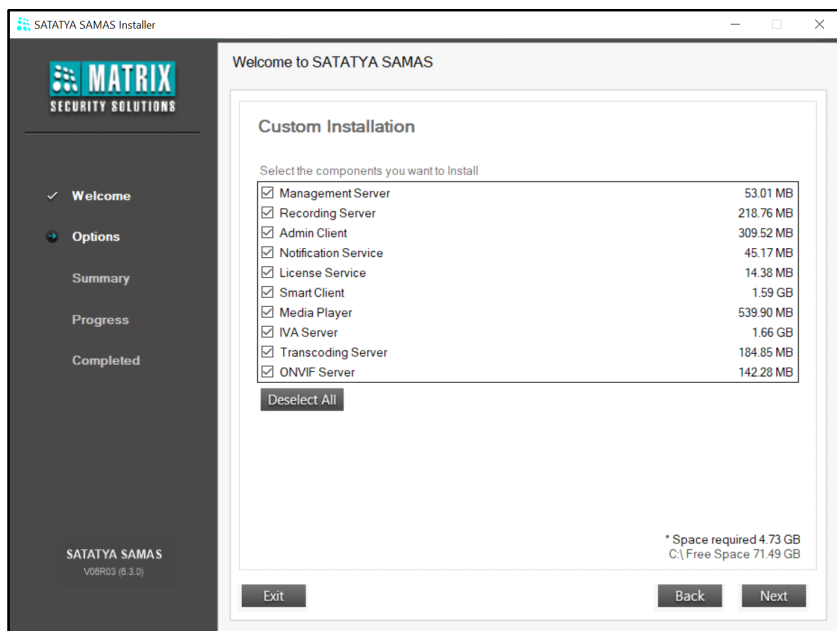


- If the 'Management Server' is selected in the list to be installed, the 'Image Storage Drive configuration' page appears. Refer "[Image Storage Drive](#)" for the detailed configuration.
- If the "Smart Client" or "IVA Server" is selected in the list to be installed, the GPU Model Creator Utility will be installed automatically.
- Once the Drive is configured, click **Next** to proceed further with the installation.

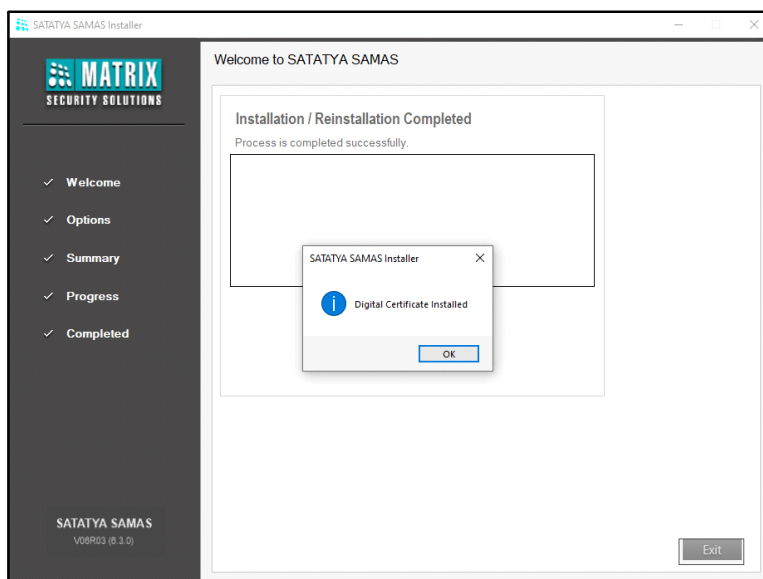


In case you have installed any component before then, the list of the following will be displayed:

- *components that will be installed*
- *components that are already installed*
- *components that will not be installed*



- Click **Install**. The system will start installing the selected SAMAS components.
- Click **Exit** to exit from the installation window or click on the **Click Here** link to create, upgrade or take backup of the SATATYA SAMAS database. For more information, refer to "[Creating/Upgrading Database](#)".



After completing the Installation, you need to:

- [“Create/Upgrade/Backup Database”](#)
- [“Create GPU Model”](#)

If you are installing/upgrading SATATYA SAMAS and your system does not support GPU(NVIDIA GTX) or does not have any GPU, the application will abort the model creation process. However, the installation will be completed successfully and the functionality of the SATATYA SAMAS can be resumed.

Create/Upgrade/Backup Database

The SATATYA SAMAS allows the you to create a new database and upgrade or take the backup of the existing one. Click on the desired link for detailed information.

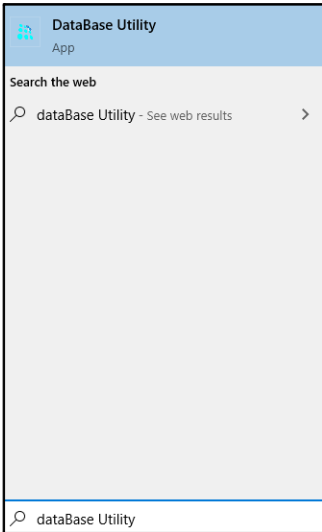
[“Creating/Upgrading Database”](#)

[“Taking Database Backup”](#)

Creating/Upgrading Database

You can create and upgrade the SAMAS Database using Database (DB) Utility.

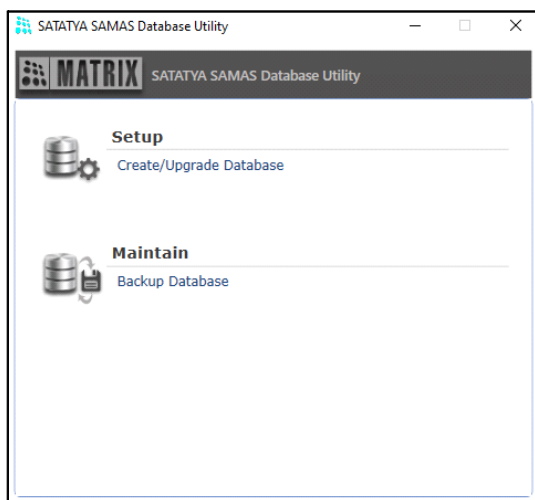
The DB Utility can be opened either by clicking on the **Click Here** link just after completion of the installation or click on your PC Search option and enter **Database Utility**. Click the same.



The SATATYA SAMAS Database Utility window appears.



Make sure you have MS SQL Server 2008 on which the SAMAS database can be created.



Click **Setup** to create or upgrade an existing database.

The Database Utility Setup page appears. Click **Change Setting** and select the **New Database** check box. Configure the Database Connection Settings.

- **Database Type:** The database type supported is MS SQL Server.

- **Server:** Specify the Database Server Name in the following format:- Database Server Name\Instance Name e.g. dbserver\squlexpress. In Server Name, you can enter upto 200 characters. Default: Blank.



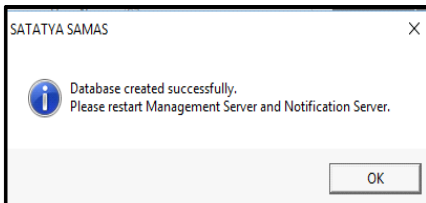
The Server Name is the Name/IP of the system where the MS SQL Server (DB Server) is installed. Server Name supports both IPv4 and IPv6 Address.

- **Authentication Mode:** Select the desired option from the drop-down list— SQL Server Authentication or Windows Authentication.

If you select SQL Server Authentication,

- **User Name:** Specify the User Name of the SQL Server user. Default: Blank.
- **Password:** Enter the Password of the SQL Server user. Default: Blank.
- **Database Name:** Specify the Database Name of the SAMAS application. By default the application creates a database by the name of “SATATYA_SAMAS”. Default: Blank.

Click **Create** to start the creation of the database.



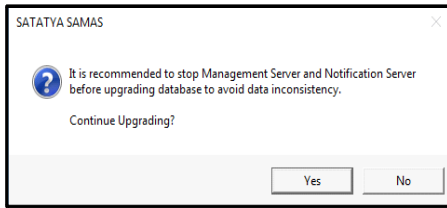
Click **Test Connection** to test the connection with the Database Server. The connection will be successful only if all the parameters have been configured correctly.

Click **Save Setting** to save the settings.

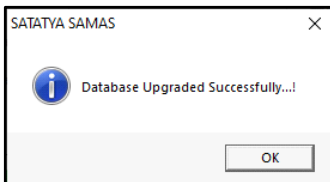
You can now start using the SAMAS applications installed on the computer.

Once the SAMAS database has been created using the above procedure, the Administrator needs to subsequently only use the **Upgrade** option as and when required. Do not select **New Database**.

Click **Upgrade** to upgrade the database.



Click **Yes** to start the database upgrade process. Once the database upgrade process is completed successfully, the following pop-up appears.



Click **OK**.

Taking Database Backup

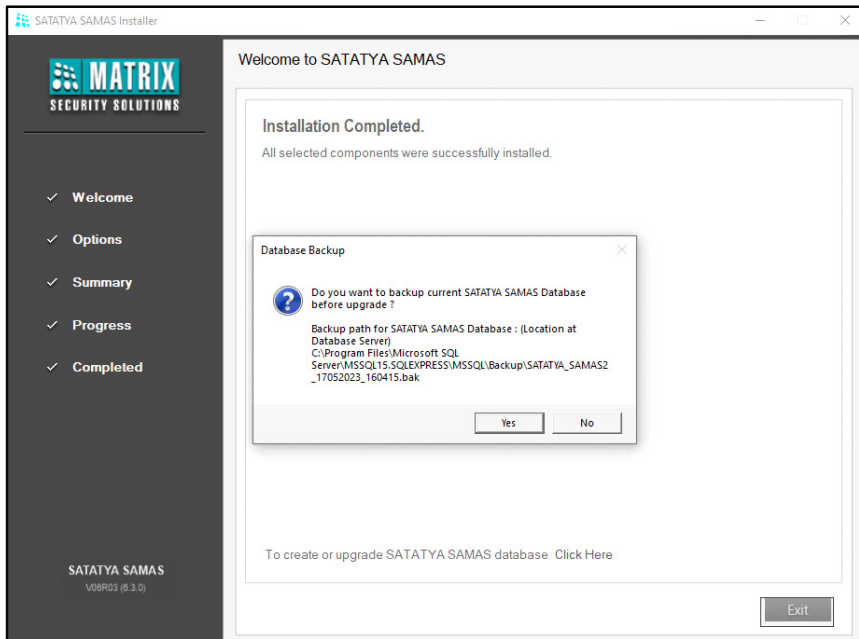
In the event of software or hardware problems, it is always a good idea to have a recent copy of your database files. The **Backup** option allows the Administrator to take the backup of the database at regular intervals.

Backup of the database can be taken in two ways. For the detailed process click the desired link below.

- [“Soon After Installation Process”](#)
- [“Using Database Utility”](#)

Soon After Installation Process

After the completion of installation process, the SAMAS searches for the existing Database, if the database is found then, a pop-up appears, to confirm if you wish to take the Backup of the current database before upgradation as shown below.

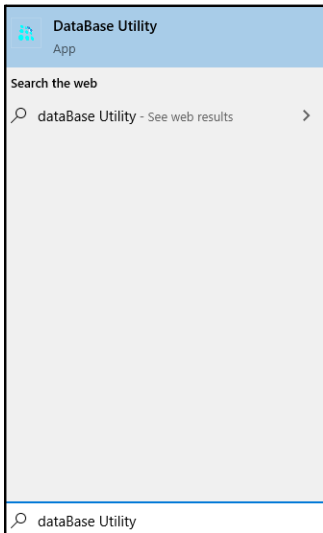


Click **Yes**, to take the Backup of the current database.

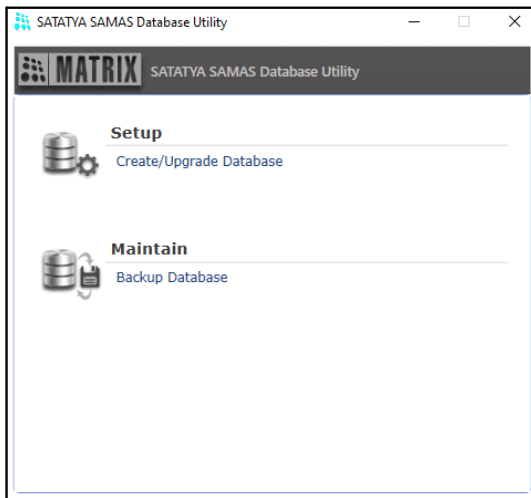
Using Database Utility

You can also take the backup of the SAMAS Database using Database Utility.

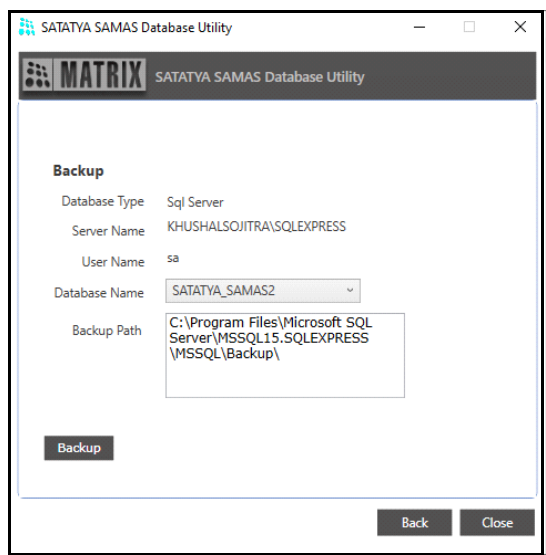
The Database Utility can be opened either by clicking on the **Click Here** link just after completion of the installation or click on your PC Search option and enter **Database Utility**. Click the same.



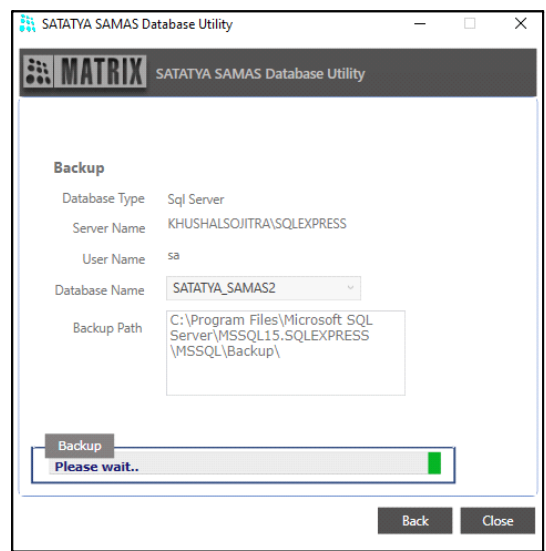
The SATATYA SAMAS Database Utility window appears.



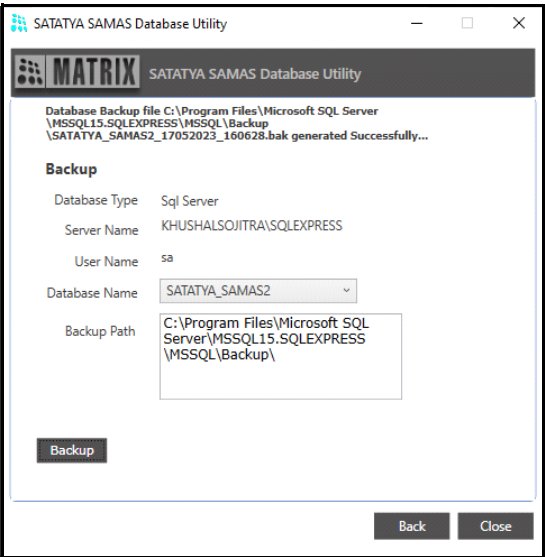
Click **Maintain** to take the backup of the database and the following window appears.



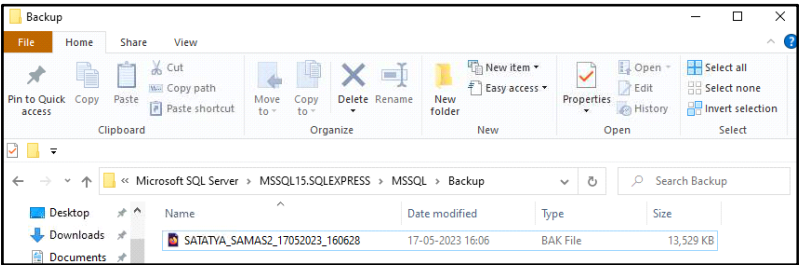
- Select the **Database Name** from the drop-down list.
- In **Backup Path**, the path of the backup file is displayed where the MS SQL has been installed. This path cannot be edited.
- Click **Backup**. The system will start the backup process.



On successful completion of the process, the system displays the path as well as the name of the backup file.



The database backup file is created at the specified location as shown below:



Create GPU Model

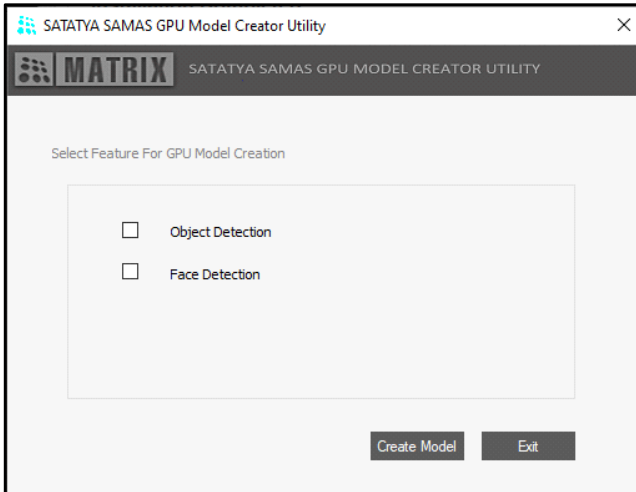
For configuring Object Type, detecting Objects in various events and detecting Faces in Face Detection Event, it is necessary to create a GPU Model. The GPU Model can be created in two ways. Click the desired link for detailed information.

[“Soon after Installation”](#)

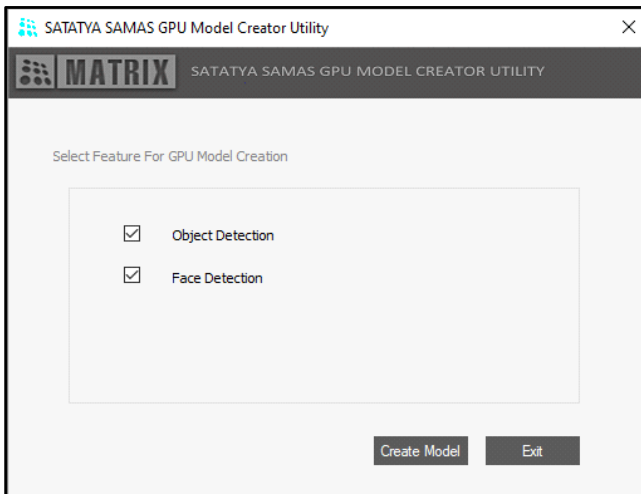
[“Using GPU Model Creator Utility”](#)

Soon after Installation

After the completion of installation process and Database backup, the SAMAS searches for GPU Card affixed in the system. If GPU Card is found, then the **SATATYA SAMAS GPU Model Creator Utility** pop-up appears.

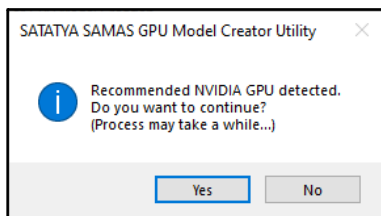


- Select the desired check box for the feature you wish to create the GPU Model.

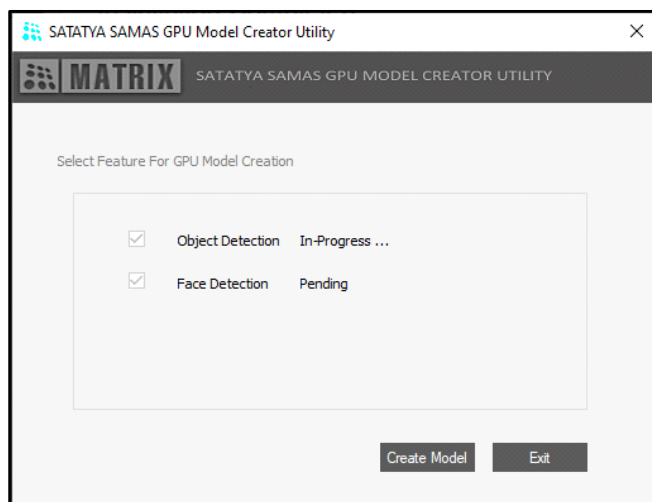


- Click **Create Model**. The SAMAS will search for the GPU NVIDIA GTX in the system.

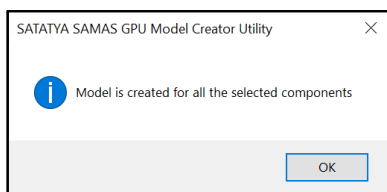
The GPU Model will be created only if the recommended GPU is detected. Once the recommended GPU is detected, the following pop-up appears.



- Click **Yes**. The status of model creation is displayed. If multiple features are selected, then the GPU Models for the same will be created sequentially.



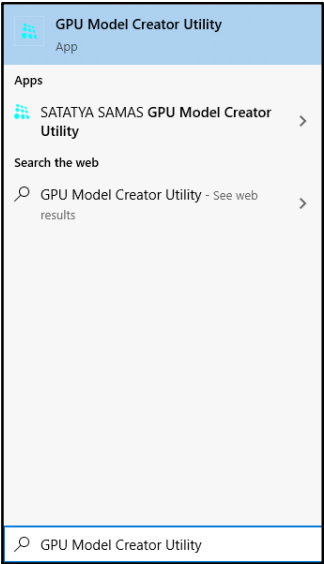
- Once the model is created successfully, the following pop-up appears.



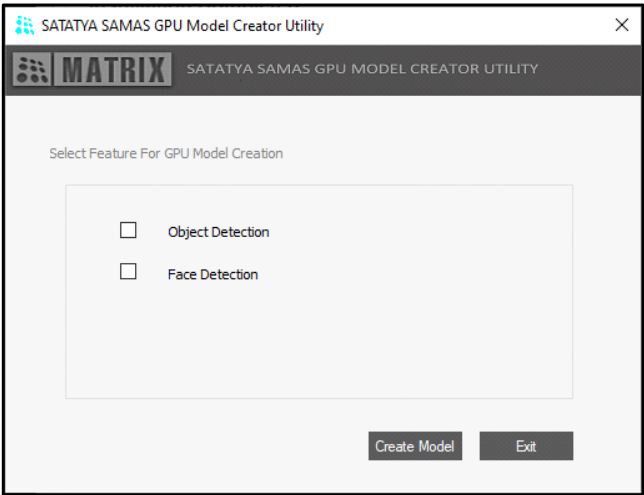
- Click **OK**.

Using GPU Model Creator Utility

You can also create the GPU Model using the GPU Model Creator Utility. Click on your PC Search option and enter GPU Model Creator Utility. Click the same.



The **SATATYA SAMAS GPU Model Creator Utility** pop-up appears.



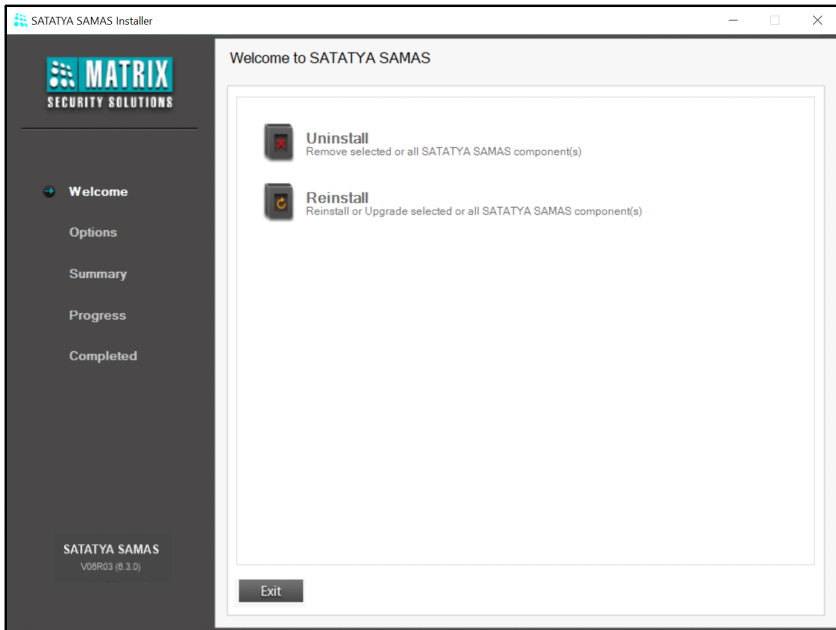
The model creation process is same as explained above. For details, refer to [“Soon after Installation”](#).

Uninstallation and Reinstallation

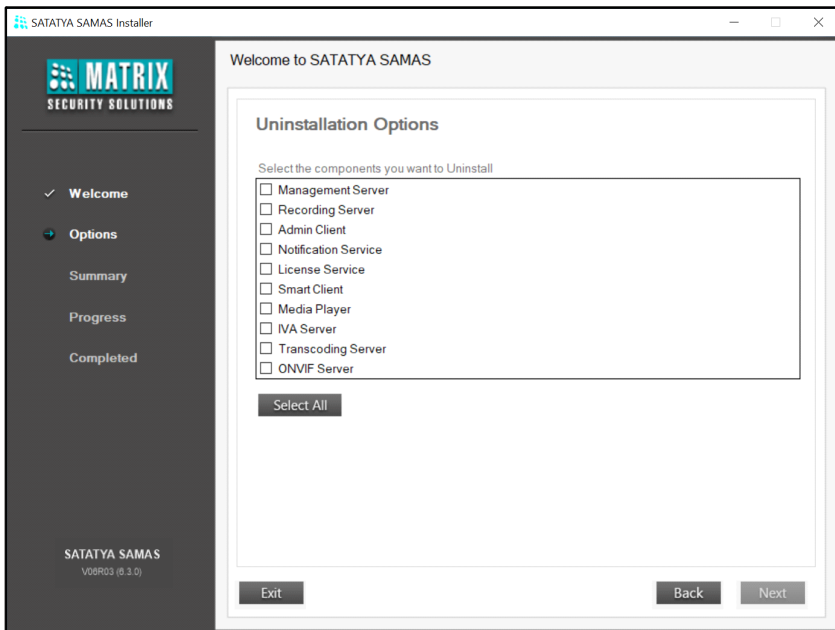
To Uninstall or Reinstall the SATATYA SAMAS components, click SATATYA_SAMAS_Installer. The setup window appears.



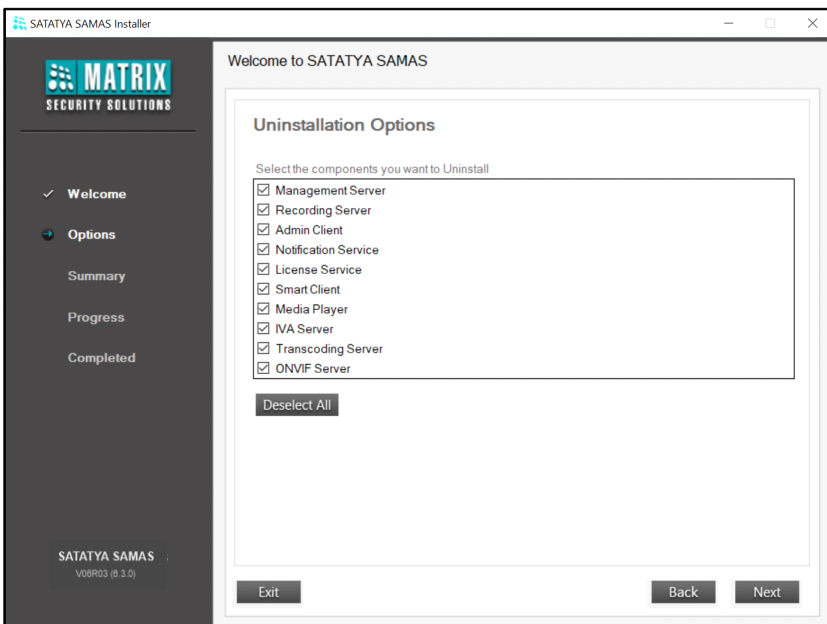
For successful uninstallation or reinstallation of SATATYA SAMAS, it is recommended that all the services are stopped before performing these tasks.



- To Uninstall the SAMAS components, Click **Uninstall**. Then select the check boxes of the desired components or click **Select All** to uninstall all the components.



- Click **Next** and then click **Uninstall**. The selected components will be uninstalled.



Similarly, the desired components can be reinstalled by selecting the **Reinstall** option from the setup window.

Installing SAMAS Components at Different Sites

SATATYA SAMAS has a distributed architecture. Hence, different components of SAMAS can be installed at different geographical locations based on monitoring requirement.

For example, an organization ABC has its head quarters in Delhi where the Management Server is set up and Recording Servers have been set up at Delhi, Mumbai and Ahmedabad. Now the Smart Client is to be installed only in Ahmedabad while the Admin Client has to be set up at the Administrator's station in Delhi. For such a situation, sending the Installation setup across to all these locations for individual installations can become tedious and time-consuming. This problem can be resolved using the SAMAS Downloader.

SAMAS Downloader



SAMAS Downloader is supported till Software Release V5R6 as well as from Software Release V6R2 and onwards.

The SAMAS Downloader provides a simple solution for multi-site installations. It enables the users to download different components of SAMAS at diverse locations using a simple Web URL from any standard Web Browser.

Open your Web Browser, enter the URL in the following format:

`http://<Management Server IPv4/IPv6 Address>:<Admin Client_Port>/downloader.html`

(For example, "http://192.168.x.y:8711/downloader.html")



If you wish to configure IPv6 Address, make sure you enclose the IPv6 Address in square brackets, for example, [2001:db8::1].

The SATATYA SAMAS Downloader appears.

SATATYA SAMAS Downloader	
Components	Product Manuals
SAMAS Smart Client	SAMAS Smart Client
SAMAS Media Player	SAMAS Media Player
SAMAS Admin Client	SAMAS Admin Client
SAMAS Recording Server	SAMAS Installation Guide
SAMAS Notification Server	SAMAS API
SAMAS IVA Server	SAMAS ONVIF Server
SAMAS Transcoding Server	
SAMAS ONVIF Server	

Select a Component from the **Components** section to initiate the download and follow the instructions to complete the installation. User can also download all Product Manuals if required.

Service Installation

Once the SAMAS setup installation is successfully completed, the Administrator must perform the following steps to start the Management Server, before configuring the *Admin Client*.



The Management Server, License Server and Database must be in the same network.

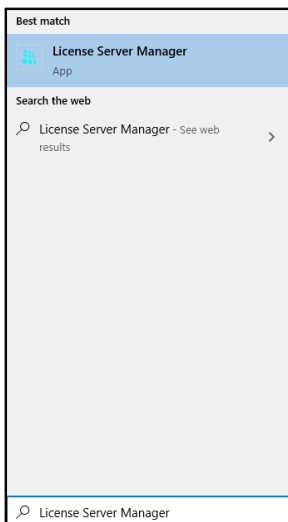
If Management Server is running on SSL Mode, then it is mandatory that all the other Servers and Clients are also configured to communicate on SSL Port of the Management Server.

If you wish to also use IPv6 Addresses in SATATYA SAMAS, make sure IPv6 network settings are configured on the PC where Management Server and License Server are installed.

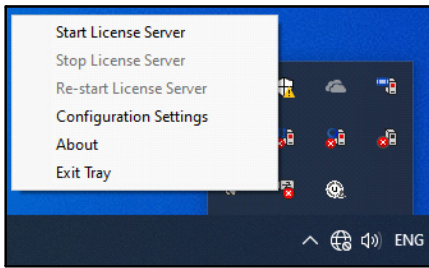
Step-1: Configure License Server Settings using the License Server Manager Utility.

The License Server Settings helps to configure the Listening Port of the installed License Server.

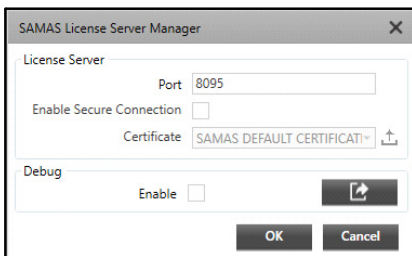
- Ensure that you have the License Dongle with you. The License Server and Dongle must be in the same PC. For Licensing details see "[Licensing of SATATYA SAMAS](#)".
- Click on your PC Search option and enter **License Server Manager**. Click the same.



- The License Server icon appears in the Tray. Right-click on the **License Server** icon.




- Select **Configuration Settings**. The **SAMAS Server License Manager** window appears.



License Server

- **Port:** Specify the Listening **Port** on which License Server communicates with the Management Server. Valid Range: 1024-65535. Default: 8095.
- **Enable Secure Connection:** Select the check box for License Server to communicate with the Management Server securely.
- **Certificate:** By default, the SAMAS Default Certificate is selected. The **Certificate** drop-down list displays the certificates fetched from the Windows Certificate Store (In PC Search option, enter Manage User Certificates to view all the certificates). From the list, select the desired certificate and click **OK**. To place the certificates in the folder manually, refer to [“Uploading SSL Certificate”](#).

OR

If you wish to upload a new certificate automatically, select the **select** option from the list and click **Upload** . The **SSL Settings** window appears to upload the SSL Certificate as well as configure the SSL Settings. For details, refer to [“SSL Settings”](#). This uploaded certificate will now appear in the Certificate drop-down list. Select the same.




*Make sure you have logged in as administrator to view the list of certificates in the **Certificate** drop-down list.*

Make sure the desired SSL Certificates are placed in the Window Certificate Store to enable the system to fetch the same.

In case the custom SSL Certificate uploaded is not available, then the system will continue functioning with the SAMAS Default Certificate.

Debug

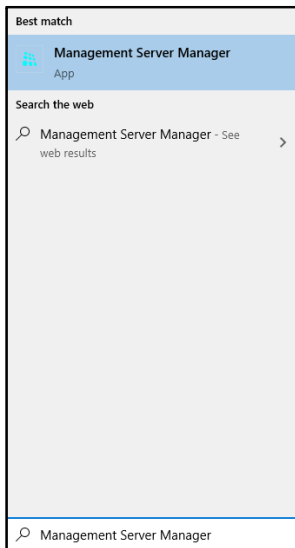
- **Enable:** Select the check box to enable the debug. Click **Export Logs**  and specify the path of the local system where you wish to store the logs.
- Click **OK** to save the License Server Settings.

Now from the Tray, right-click on the **License Server** icon again and select **Start License Server** to start the server.

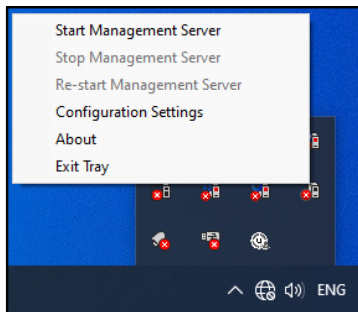
Step-2: Configure Management Server Settings using the Management Server Manager Utility

The Management Server is responsible for centralized authentication, logging (events, actions, user activities, etc.) and configuration of the security system consisting of video surveillance devices.

- Click on your PC Search option and enter **Management Server Manager**. Click the same.



- The Management Server icon appears in the Tray. Right-click on the **Management Server** icon.



- Select **Configuration Settings**. The **SAMAS Management Server Manager** window appears.



SAMAS TCP API and SAMAS HTTP API Port are supported till Software Release V5R6 as well as from Software Release V6R2 and onwards.

The screenshot shows the 'SAMAS Management Server Manager' window. It has three main sections: 'Management Server', 'License Verification', and 'Debug'. The 'Management Server' section has two tabs: 'Non SSL' (selected) and 'SSL'. Under 'Non SSL', there are input fields for various ports: Admin Client Port (8711), Recording Server Listening Port (8090), Media Client Port (8085), COSEC Port (8089), IVA Server Port (8100), SAMAS TCP API Port (8200), SAMAS HTTP API Port (8300), Transcoding Server Port (8400), and ONVIF Server Port (8500). The 'License Verification' section has a checkbox for 'Enable Secure Connection', a 'Select Mode' dropdown (set to 'Service Based'), an 'IP or Server Name' field (127.0.0.1), and a 'Port' field (8095). The 'Debug' section has an 'Enable' checkbox and a button with a refresh icon. At the bottom are 'OK' and 'Cancel' buttons.

- You can configure the following — Port configurations for establishing communication with Admin Client, Recording Server, Media Client, COSEC Server, IVA Server, Transcoding Server, ONVIF Server, HTTP and TCP Port and License Server with SSL or Non SSL connection as required. Valid Range: 1024-65535.

If you have enabled SSL, then the following communication between Client and Server will be made secure.

Client	Server
Admin Client/ Smart Client/ Media Client	Management Server
IVA Server, Transcoding Server and ONVIF Server	Management Server
Recording Server	Management Server
Admin Client/ Smart Client/ Media Client	Recording Server/ Failover Server
IVA Server, Transcoding Server and ONVIF Server	Recording Server/ Failover Server
Management Server	License Server



If Management Server is running on SSL Mode, then it is mandatory that all the other Servers and Clients are also configured to communicate on SSL Port of the Management Server.


SSL Connection Configuration

The **SSL** connection port settings are as displayed below:

The screenshot shows the 'SAMAS Management Server Manager' window. It has a tabbed interface with 'Non SSL' and 'SSL' tabs. The 'SSL' tab is selected. Under the 'Management Server' section, there is a list of settings: 'Enable Secure Connection' (checked), 'Certificate' (set to 'SAMAS DEFAULT CERTIFICATE'), 'Admin Client Port' (7711), 'Recording Server Listening Port' (7090), 'Media Client Port' (7085), 'COSEC Port' (7089), 'IVA Server Port' (7100), 'SAMAS TCP API Port' (7200), 'SAMAS HTTP API Port' (7300), 'Transcoding Server Port' (7400), and 'ONVIF Server Port' (7500). Below this is the 'License Verification' section with 'Enable Secure Connection' (checked), 'Select Mode' (Service Based), 'IP or Server Name' (127.0.0.1), and 'Port' (8095). At the bottom is a 'Debug' section with 'Enable' (unchecked) and a button with a refresh icon. 'OK' and 'Cancel' buttons are at the bottom right.

- **Enable Secure Connection:** For secure communication between the Management Server and License Server, select the **Enable Secure Connection** check box.
- **Certificate:** By default, the SAMAS Default Certificate is selected. The **Certificate** drop-down list displays the certificates fetched from the Windows Certificate Store (In PC Search option, enter Manage User Certificates to view all the certificates). From the list, select the desired certificate and click **OK**. To place the certificates in the folder manually, refer to [“Uploading SSL Certificate”](#).

OR

If you wish to upload a new certificate automatically, select the **select** option from the list and click **Upload** . The **SSL Settings** window appears to upload the SSL Certificate as well as configure the SSL Settings. For details, refer to “[SSL Settings](#)”. This uploaded certificate will now appear in the Certificate drop-down list. Select the same.



*Make sure you have logged in as administrator to view the list of certificates in the **Certificate** drop-down list.*

Make sure the desired SSL Certificates are placed in the Window Certificate Store to enable the system to fetch the same.

In case the custom SSL Certificate uploaded is not available, then the system will continue functioning with the SAMAS Default Certificate.

License Verification

The screenshot shows the 'SAMAS Management Server Manager' window. The 'License Verification' section is expanded, showing the 'Enable Secure Connection' checkbox checked. Below it, the 'Select Mode' dropdown menu is open, displaying three options: 'Service Based' (highlighted), 'Device Based', and 'Virtual License'. The 'IP or Server Name' and 'Port' fields are visible but empty. The 'Debug' section at the bottom has the 'Enable' checkbox unchecked. At the bottom right are 'OK' and 'Cancel' buttons.

- **Enable Secure Connection:** For secure communication between the Management Server and License Verifying Server/Device, select the **Enable Secure Connection** check box.

- **Select Mode:** License Verification Mode for SSL Connection can be **Service Based** or **Device Based** or **Virtual License**.



SATATYA SAMAS supports IPv6 addressing for Service Based License Verification Mode only.

Virtual License

With the introduction of Virtual License, the need of a Dongle is eliminated. You can opt for Virtual License in the following scenarios:

- Fresh installation of SATATYA SAMAS.
- You already have a Dongle License but you wish to migrate to Virtual License. In this case:
 - The existing activations in the Dongle License will not be transferred to the Virtual License and you need to purchase all the required licenses again.
 - You can switch from a Dongle License to Virtual License.

For Virtual License (Fresh Installation), make sure you have:

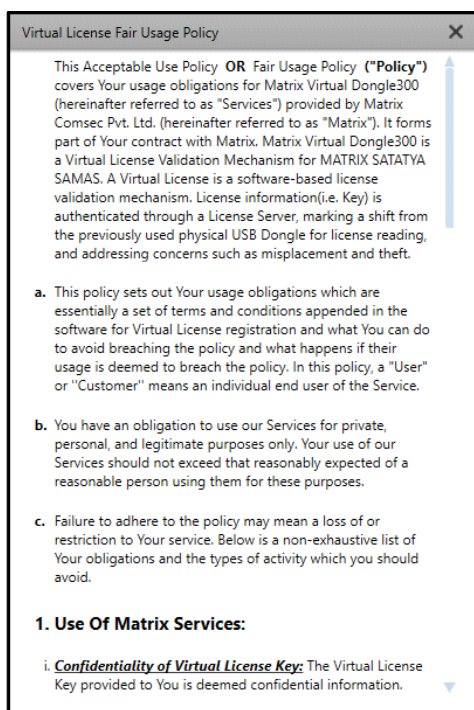
- Persistent Internet connection with good speed.
- Received the MATRIX VIRTUAL DONGLE300 Key in PDF form.
- Received the SATATYA SAMAS PLT Key in PDF form.
- Received the desired module activation License Keys as per your requirement.



Incase you are migrating (existing user) from a Service/Device Based License to Virtual License, make sure:

- *You have persistent Internet connection with good speed.*
- *You have received the Virtual License key PDF by contacting the Matrix Support Team.*
- *Right-click on the Management Server icon from the Tray and select **Stop Management Server**.*
- *Select **Configuration Settings**, the SAMAS Management Server Manager window appears.*
- *Select the desired tab — Non SSL, SSL.*
- *In **Select Mode**, select Virtual License.*

As soon as you select Virtual License from the **Select Mode** drop-down list, the Virtual License Fair Usage Policy pop-up appears.



Virtual License Fair Usage Policy

3. Rights and Remedies:

- i. If Matrix determines (in its sole and absolute discretion) that a Customer has materially failed to comply with this Policy, including by engaging in a Prohibited Activity, Matrix may at any time:
- ii. Suspend or terminate the Service;
- iii. Impose additional charges on the Customer in proportion to the impact of the Prohibited Activity;
- iv. Nothing in this Policy Matrix's rights and remedies (available at law or in equity) in any way concerning any Prohibited Activity.

4. Modification of Fair Usage Policy:

The software provider reserves the right to modify or update this Fair Usage Policy as necessary. Any changes to the policy will be communicated to the organization in a timely manner.

By proceeding with the registration of the Virtual License Key, the organization acknowledges and agrees to abide by the terms and conditions outlined in this Policy. Failure to comply with these terms may result in the suspension or termination of the license agreement.

☒ **I have read and agree to the Fair Usage Policy**

Continue

Scroll to the bottom and select the **I have read and agree to the Fair Usage Policy** check box.

Click **Continue**. The pop-up closes.

The licenses need to be purchased as per your requirement. For details, refer to [“Licensing of SATATYA SAMAS”](#)

Once the keys are received you need to Register/Update the same. For details, refer to License Management Settings in the SATATYA SAMAS Admin Client Manual.

The registration request is sent to the Virtual License Manager. The Virtual License Manager checks for the authenticity of the key as well as it communicates with the Matrix License Manager. Thereafter, the request is served.

Service Based

If you select Service Based mode from the **Select Mode** drop-down list and the License Dongle is connected with the License Server machine, configure the following:

- **IP or Server Name:** Enter the IPv4/IPv6 Address or Server Name of the License Server machine where the License Dongle is connected. In IP or Server Name, you can enter upto 255 characters. Default: 127.0.0.1



If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.

- **Port:** Specify the Listening port on which License Server communicates with the Management Server. Make sure the same Port number is entered in the License Server. Valid Range: 1024-65535. Default: 8095.



By default, Management Server runs on the IP Address of the system where it is installed.

Device Based

Device Based is a more secure mode of License Verification as the License Dongle is connected within the COSEC Device, which reduces the risk of Dongle loss or theft. In this case the user does not need a separate machine for the License Verification.

If you select Device Based mode from the **Select Mode** drop-down list, configure the following:

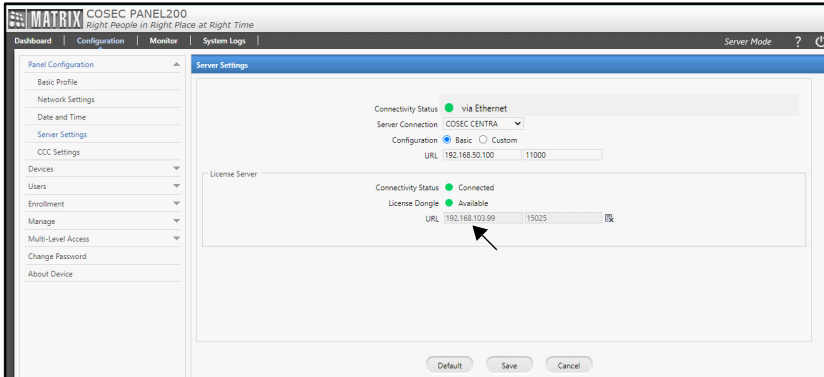
- **Port:** Enter the Port number of the COSEC Device through which the License Dongle will communicate with the Management Server. Valid Range: 1024-65535. Default: 15025.
- **MAC Address:** It is a non-editable field which displays the MAC address of the COSEC Device. It will appear once the License Dongle is linked with the IP Address of the Management Server.

Make sure the configuration of License Dongle has been done in the COSEC Device before configuring the License Verification as Device Based mode.

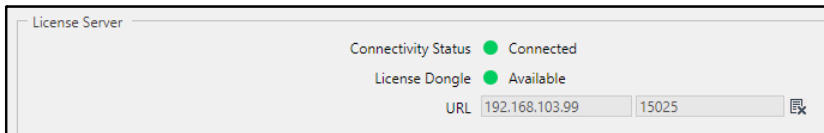
COSEC Device - License Configurations

For the configuration, access your COSEC Device web page using the browser and login using the credentials.

- Click **Configuration > Panel Configuration > Server Settings** and the following page appears.

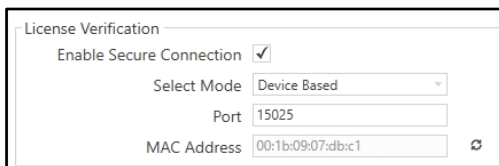


- Under the License Server section, enter the IP Address of the Management Server in the **URL** field.
- Enter the Port Number of the COSEC Device (beside the IP Address entered) through which the License Dongle will communicate with the Management Server. For example: 65535.



In the Management Server Manager window, make sure the same Port number is entered under License Verification as entered for COSEC Device License Server.

- Right-click on the Management Server icon from the Tray. Select **Configuration Settings**, the SAMAS Management Server Manager window appears. The MAC Address of COSEC Device will be displayed for the entered Port Number as shown below.




- To reset the MAC Address, click **Reset** . A pop up appears.



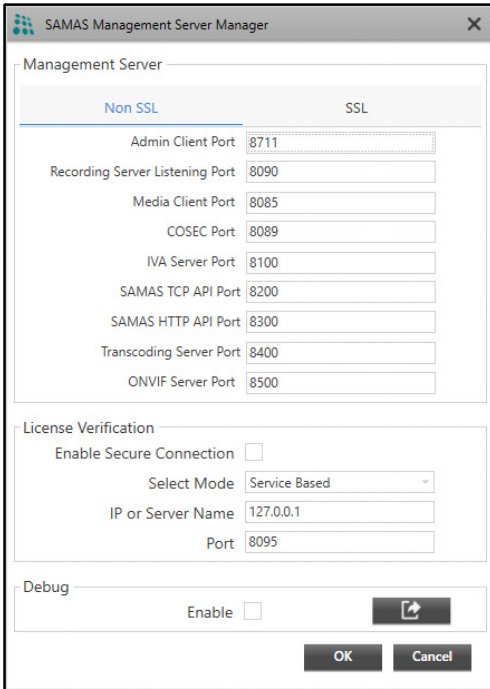
- Click **Yes** to de-register the configured device and register a new device or click **No** to cancel the reset.
- Click **OK** to save the settings.

Debug

- **Enable:** Select the check box to enable debug. Click **Export Logs**  and specify the path of the local system where you wish to store the logs.

Non SSL Connection Configurations

The **Non SSL** connection port settings are as displayed below:



The screenshot shows the 'SAMAS Management Server Manager' window. It has a tabbed interface with 'Non SSL' and 'SSL' tabs. The 'Non SSL' tab is active, displaying a list of ports for various services. Below this is a 'License Verification' section with checkboxes and input fields. At the bottom is a 'Debug' section with an 'Enable' checkbox and an 'Export Logs' button. 'OK' and 'Cancel' buttons are at the very bottom.

	Non SSL	SSL
Admin Client Port	8711	
Recording Server Listening Port	8090	
Media Client Port	8085	
COSEC Port	8089	
IVA Server Port	8100	
SAMAS TCP API Port	8200	
SAMAS HTTP API Port	8300	
Transcoding Server Port	8400	
ONVIF Server Port	8500	

License Verification


Enable Secure Connection ☐

Select Mode: Service Based

IP or Server Name: 127.0.0.1

Port: 8095

Debug


Enable ☐ 

OK Cancel

License Verification

- **Enable Secure Connection:** For secure communication between the Management Server and License Verifying Server/Device, select the **Enable Secure Connection** check box.
- **Select Mode:** License Verification Mode for Non SSL Connection can be **Service Based** or **Device Based** or **Virtual License**. For details, refer to "[License Verification](#)".

Debug

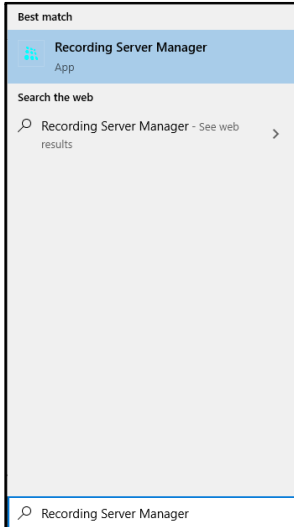
- **Enable:** Select the check box to enable debug. Click **Export Logs**  and specify the path of the local system where you wish to store the logs.

Now from the Tray, right-click on the **Management Server** icon again and select **Start Management Server** to start the service.

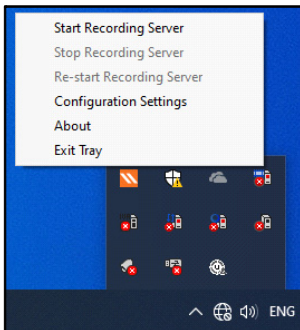
Step-3: Configure Recording Server settings using the Recording Server Manager Utility.

The Recording Server is responsible for communicating with the video surveillance devices, recording the video streams into its storage drive and streaming live/recorded videos to the clients.

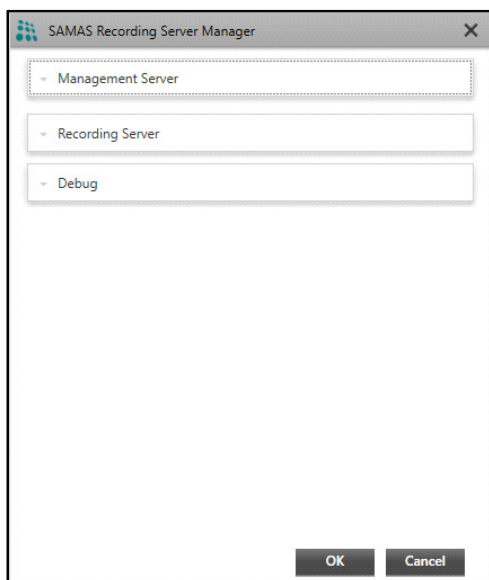
- Click on your PC Search option and enter **Recording Server Manager**. Click the same.



- The Recording Server icon appears in the Tray. Right-click on the **Recording Server** icon.



- Select **Configuration Settings** and the **SAMAS Recording Server Manager** window appears.



It includes the configuration of Management Server, Recording Server as well as the Debug. For details, click on the respective link.

[“Management Server”](#)

[“Recording Server”](#)

[“Debug”](#)

Management Server

For the Recording Server (RS) to communicate with the Management Server (MS), a connection between them needs to be established by configuring the MS IP Address and Port in the RS Manager. But it is not necessary that both the components are located in same network (private), they may be located in two different networks (public). Hence, SAMAS allows you to configure 3 Preferred Networks where you can add private networks as well as public networks of MS.

Click the **Management Server** collapsible panel and configure the following parameters:

The screenshot shows the 'SAMAS Recording Server Manager' window. The 'Management Server' section is expanded, revealing a checkbox for 'Enable Secure Connection' which is currently unchecked. Below this, there are three network configuration sections: 'Preferred Network 1', 'Preferred Network 2', and 'Preferred Network 3'. 'Preferred Network 1' is populated with 'IP or Server Name' as '127.0.0.1' and 'Port' as '8090'. The other two sections are empty. At the bottom of the window, there are two collapsed sections: 'Recording Server' and 'Debug'. The 'OK' and 'Cancel' buttons are located at the bottom right of the dialog.

- **Enable Secure Connection:** Select the check box for Recording Server to communicate with the Management Server securely.

Under **Preferred Network 1 (PN1)** configure the following:

- **IP or Server Name:** Enter either the Private or Public IPv4/IPv6 Address of the Management Server or enter the Host Name, Domain Name or Server Name of ISP. In IP or Server Name, you can enter upto 255 characters. Default: 127.0.0.1

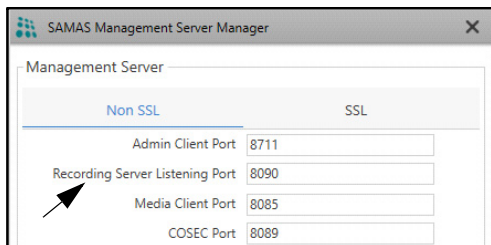


If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.

- **Port:** Enter either the Private or Public Port. Valid Range: 1-65535. Default: 8090.

Scenario1: If the RS and MS are located in the same network.

- To establish the connection between them, Private Network configuration is required.
- Hence, enter Private IP Address and Port of MS. Make sure the port configured here is same as the Recording Server's Listening Port configured in the MS Manager.



- Now the RS and MS will be connected via PN1.

Scenario2: If the RS and MS are located in two different networks.

- To establish the connection between them, Public Network configuration is required. You can specify three Public Network IP Addresses and Ports. The port that is to be configured is ISP's port that has been mapped with the Recording Server's Listening Port in MS Manager.



Contact the Administrator regarding Port Forwarding configurations.

- Similarly, configure the parameters of **Preferred Network 2 (PN2)/ Preferred Network 3 (PN3)** as per your requirement.



Configure the network with the highest priority in Preferred Network 1.

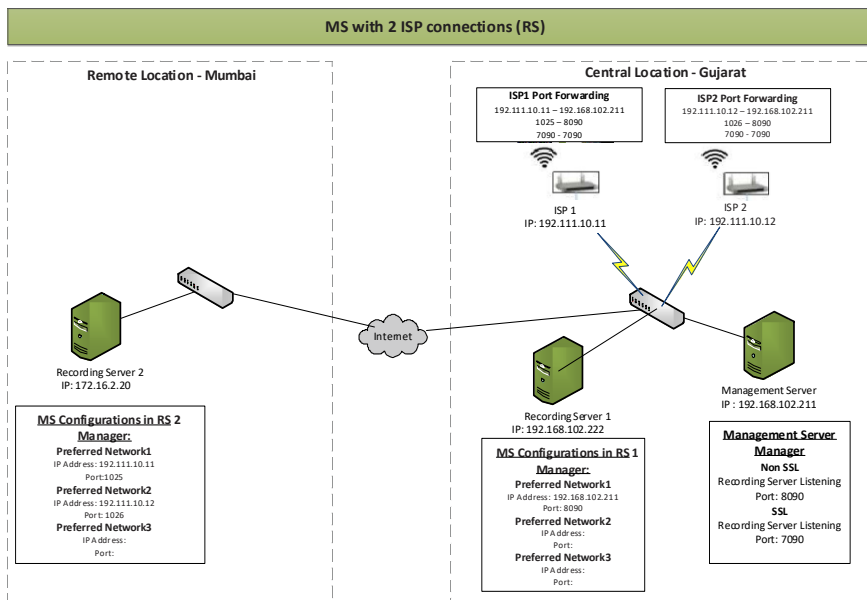
- If Public Networks, ISP1 and ISP2 are configured in PN1 and PN2 respectively.
- Now as the RS and MS are located in two different networks, the connection between them will be established via ISP1 (PN1) first. If due to some network issue, the connection is lost between RS and MS via ISP1 (PN1), then ISP will fall-back on ISP2, allowing the RS to re-establish the connection via ISP2 (PN2). When PN1 connectivity is resumed, then the connection will be switched over from the PN2 to PN1.

Example:

An organization has multiple branches. The main branch is located at a Central location, Gujarat while the other branch is located in Mumbai.

Also, the MS and RS1 have been installed in the same network at the Central location (Gujarat), while RS2 is installed at remote location (Mumbai).

Now refer to the following architecture for the network configuration setup. It also explains that how the connection is established between RS1 & MS and RS2 & MS.

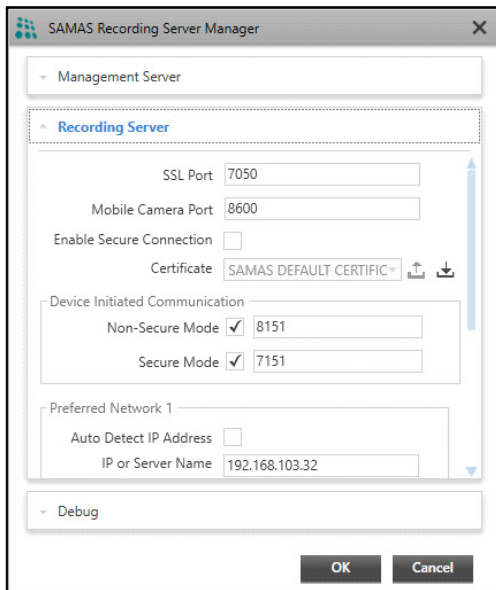


Recording Server

Live Stream of the cameras can be accessed using clients such as Admin Client, Smart Client and IVA Server. For this, clients have to communicate with the Recording Server (RS)/Failover Server (FoS).


Also, it is not necessary that both the client and RS/FoS are located in the same network, they may be located in two different networks. So, to serve both the scenarios, SAMAS allows you to configure Preferred Networks, where you can add private as well as public networks of RS.

Click the **Recording Server** collapsible panel and configure the following parameters:



- **SSL Port:** Specify the **SSL Port** where secure connection with RS will be established. Valid Range: 1-65535. Default: 7050.
- **Mobile Camera Port:** Specify the Mobile Camera Port on which the Mobile Camera will communicate with the Recording Server to push data. Valid Range: 1-65535. Default: 8600.
- **Enable Secure Connection:** Select the check box for Recording Server to communicate with the other servers —IVA, Transcoding, ONVIF — securely.
- **Certificate:** By default, the SAMAS Default Certificate is selected. The **Certificate** drop-down list displays the certificates fetched from the Windows Certificate Store (In PC Search option, enter Manage User Certificates to view all the certificates). From the list, select the desired certificate and click **OK**. To place the certificates in the folder manually, refer to [“Uploading SSL Certificate”](#).

OR

If you wish to upload a new certificate automatically, select the **select** option from the list and click **Upload** . The **SSL Settings** window appears to upload the SSL Certificate as well as configure the SSL Settings. For details, refer to [“SSL Settings”](#). This uploaded certificate will now appear in the Certificate drop-down list. Select the same.



*Make sure you have logged in as administrator to view the list of certificates in the **Certificate** drop-down list.*

Make sure the desired SSL Certificates are placed in the Window Certificate Store to enable the system to fetch the same.

In case the custom SSL Certificate uploaded is not available, then the system will continue functioning with the SAMAS Default Certificate.

You can also download the certificate and save it on your local PC in **.CER** format. Click Download



and select the desired folder where you wish to save the certificate. This certificate can be uploaded in the device to make the communication between device and Recording Server secure.

Device Initiated Communication

- **Non-Secure Mode:** Select the check box for the devices (Matrix IP Camera/SATAYA Devices like NVR) to communicate in non-secure mode with the Recording Server and automatically add the devices to SAMAS. Specify the Non-Secure Mode Port for communication between devices and Recording Server. Recording Server (RS)/Failover Server (FoS) will listen to Auto Addition Device request on this port. Valid Range: 1-65535. Default: 8151.
- **Secure Mode:** Select the check box for the Matrix IP Camera to communicate in secure mode with the Recording Server and automatically add the cameras to SAMAS. Specify the Secure Mode Port for communication between camera and Recording Server. Recording Server (RS)/Failover Server (FoS) will listen to Auto Addition Device request on this port. The SSL Certificate uploaded in Recording Server will be used for secure communication. Valid Range: 1-65535. Default: 7151.

For secure communication, make sure the Secure Communication with Server check box is enabled in IP Cameras.

If same Port is configured in Non-Secure and Secure Mode, then by default only Non-Secure Mode Port will be considered for communication.



For the Device Initiated Communication feature to work, you must ensure that SATATYA SAMAS Integration is enabled for Matrix Devices and IP Cameras in the Device Client and camera web-page respectively. Make sure the Recording Server IPv4/IPv6 Address and the Non-Secure Mode/Secure Mode port is configured in Device Client or camera web-page.

To ensure smooth functioning of this feature, make sure the Recording Server and Management Server are upgraded to the latest and same version.

Preferred Network 1

- **Auto Detect IP Address:** If the **Auto Detect IP Address** check box is selected then IPv4/IPv6 Address of your PC where Recording Server is installed is considered as IP Address of Recording Server. Whenever the IP Address of the PC is changed then the same is updated as the Recording Server's IP Address.



If both IPv4 and IPv6 is enabled on the system where Recording Server is installed, then IPv4 IP Address will be given priority.

If the Auto Detect IP Address check box is cleared then you need to specify the **IP Address** and **Port** of the Recording Server in Preferred Network 1/2/3.

Configure the following parameters of the Recording Server in **Preferred Network 1,2 and 3**.

- **IP or Server Name:** Enter either Private or Public IPv4/IPv6 Address of the Recording Server. You can also enter the Host Name, Domain Name or Server Name of ISP1/2. In IP or Server Name, you can enter upto 255 characters. Default: Blank.



If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.

Make sure the IP Addressing Protocol (IPv4/IPv6) in Recording Server and the clients is same to establish communication.

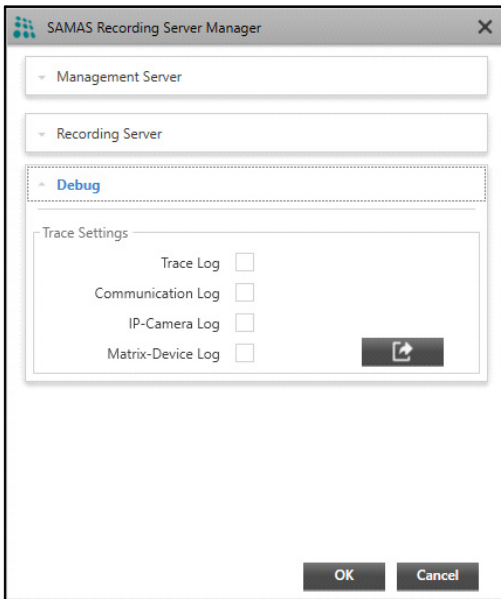
- **Port:** Enter either Private or Public Port on which RS/FoS will listen to client requests. For Private Network, enter the Recording Server Port. Valid Range: 1-65535. Default: 8050.


For Public network, enter the Forwarded Port (ISP1/ISP2 Port) that has been mapped with the internal Recording Server Port.

The functionality of preferred network is same as explained while configuring preferred networks of the Management Server. For details refer to [“Management Server”](#).

- Click **OK** to save the settings.

Debug



- **Trace Settings:** Select the check boxes of the desired options for which you wish to enable debug. Click **Export Logs**  and specify the path of the local system where you wish to store the logs.
- Now from the Tray, right-click on the **Recording Server** icon again and select **Start Recording Server** to start the service.
- The Recording Server will display Activation Pending till the Server is not activated. The Servers are activated from the Admin Client.
- After activating, the Recording Server will start.

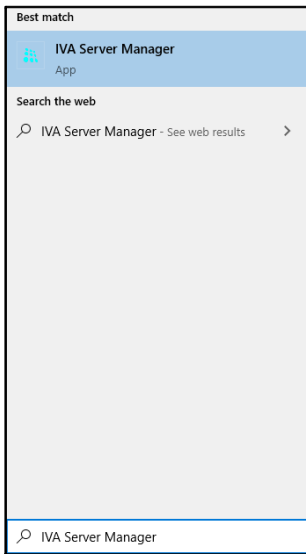
Step-4: Configure IVA Server settings using the IVA Server Manager Utility.

IVA Server provides an option to the User to detect events such as Motion for those Cameras which do not support motion detection. Also, the IVA Server provides many other features. Refer to the Admin Client and Smart Client Manuals for details.

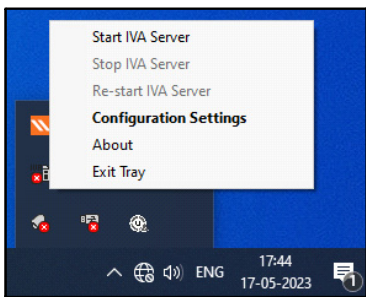
To use IVA features a connection between the Management Server (MS) and IVA Server must be established.

The IVA Server may be located in the same network or in a different network. Hence, SAMAS allows you to configure multiple preferred networks, where user can add private network as well as public network via ISPs.

- Click on your PC Search option and enter **IVA Server Manager**. Click the same.



- The IVA Server icon appears in the Tray. Right-click on the **IVA Server** icon.



- Select **Configuration Settings** and the **SAMAS IVA Server Manager** window appears.

- **Enable Secure Connection:** Select the check box for IVA Server to communicate with the Management Server securely.

Preferred Network 1/2/3

- **IP or Server Name:** Enter either Private or Public IPv4/IPv6 Address of the Management Server on which IVA Server will communicate. You can also enter the Host Name, Domain Name or Server Name of ISP1/2. In IP or Server Name, you can enter upto 255 characters. Default: 127.0.0.1



If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.

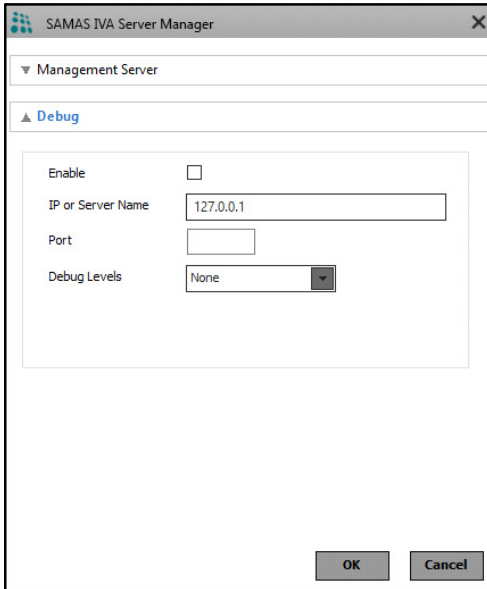
- **Port:** Enter either Private or Public Port on which IVA Server will communicate. Valid Range: 1024-65535. Default: 8100.

For Private Network, enter the IVA Server Port.

For Public network, enter the Forwarded Port (ISP1/ISP2 Port) that has been mapped with the internal IVA Server Port.

The functionality of preferred network is same as explained while configuring preferred networks of Management Server. For details, refer to [“Management Server”](#).

Debug



The screenshot shows a window titled "SAMAS IVA Server Manager" with a close button (X) in the top right corner. Inside the window, there is a "Management Server" section with a dropdown arrow. Below it is a "Debug" section with a plus icon and the word "Debug". The "Debug" section contains a form with the following fields:

- Enable:** A checkbox that is currently unchecked.
- IP or Server Name:** A text input field containing the value "127.0.0.1".
- Port:** An empty text input field.
- Debug Levels:** A dropdown menu with "None" selected.

At the bottom right of the window are two buttons: "OK" and "Cancel".

- **Enable:** Select the check box to enable the debug.
- **IP or Server Name:** Specify the IPv4/IPv6 Address or Server Name of the Syslog Server. In IP or Server Name, you can enter upto 255 characters. Default: 127.0.0.1



If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.

- **Port:** Specify the Port of the Syslog Server. Valid Range: 1024-65535. Default: Blank.
- **Debug Levels:** Select the desired level of debug — None, Information Logs or Detailed Logs.
- Click **OK** to save the configurations.

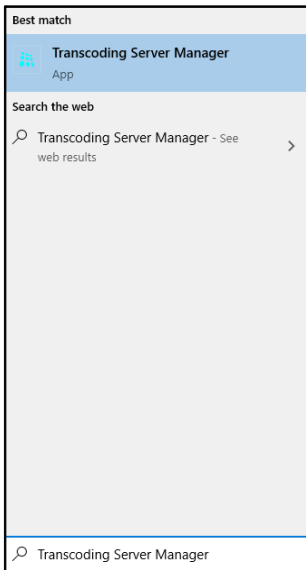
Now from the Tray, right-click on the **IVA Server** icon again and select **Start IVA Server** to start the service.

Step-5: Configure Transcoding Server settings using the Transcoding Server Manager Utility.

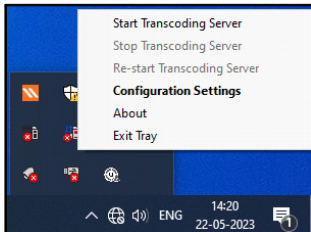
The Transcoding Server optimizes the bandwidth for the stream usage. When there is congestion, the frames are sent to the Transcoding Server which eliminates interrupted Live View/Playback. To use Transcoding features, connection between Management Server (MS), Recording Server and Transcoding Server must be established.

Transcoding Server may be located in the same network or in different network. Hence, SAMAS allows to configure multiple preferred networks, where you can add private network as well as public network via ISPs.

- Click on your PC Search option and enter **Transcoding Server Manager**. Click the same.



- The Transcoding Server icon appears in the Tray. Right-click on the **Transcoding Server** icon.



- Select **Configuration Settings** and the **SAMAS Transcoding Server Manager** window appears.

- **Enable Secure Connection:** Select the check box for Transcoding Server to communicate with the Management Server securely.

Preferred Network 1/2/3

- **IP or Server Name:** Enter either Private or Public IPv4/IPv6 Address of the Management Server on which Transcoding Server will communicate. You can also enter the Host Name, Domain Name or Server Name of ISP1/2. In IP or Server Name, you can enter upto 255 characters. Default: 127.0.0.1



If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.

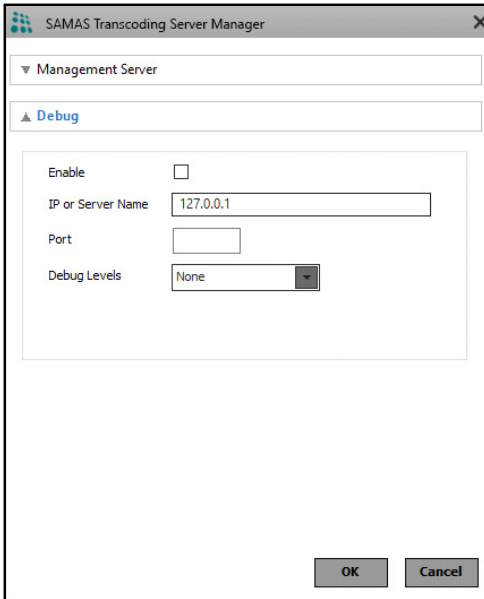
- **Port:** Enter either Private or Public Port on which Transcoding Server will communicate. Valid Range: 1024-65535. Default: 8400.

For Private Network, enter the Transcoding Server Port.

For Public network, enter the Forwarded Port (ISP1/ISP2 Port) that has been mapped with the internal Transcoding Server Port.

The functionality of preferred network is same as explained while configuring preferred networks of Management Server. For details, refer to [“Management Server”](#).

Debug



The screenshot shows a window titled "SAMAS Transcoding Server Manager" with a close button (X) in the top right corner. Inside the window, there is a "Management Server" section with a dropdown arrow and a "Debug" section with an expand/collapse arrow. The "Debug" section contains the following fields:

- Enable:** A checkbox that is currently unchecked.
- IP or Server Name:** A text input field containing "127.0.0.1".
- Port:** An empty text input field.
- Debug Levels:** A dropdown menu with "None" selected.

At the bottom right of the dialog box are two buttons: "OK" and "Cancel".

- **Enable:** Select the check box to enable the debug.
- **IP or Server Name:** Specify the IPv4/IPv6 Address or Server Name of the Syslog Server. In IP or Server Name, you can enter upto 255 characters. Default: 127.0.0.1



If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.

- **Port:** Specify the Port of the Syslog Server. Valid Range: 1024-65535. Default: Blank.
- **Debug Levels:** Select the desired level of debug — None, Information Logs or Detailed Logs.
- Click **OK** to save the configurations.

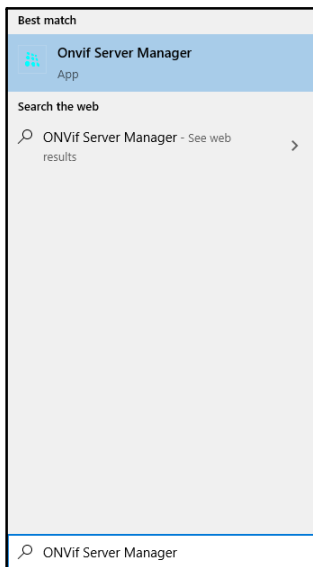
Now from the Tray, right-click on the **Transcoding Server** icon again and select **Start Transcoding Server** to start the service.

Step-6: Configure ONVIF Server settings using the ONVIF Server Manager Utility.

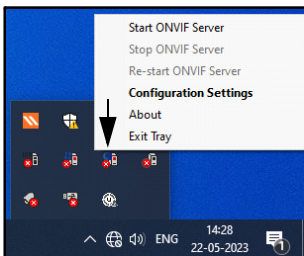
The ONVIF Server acts as a bridge between SAMAS and 3rd Party ONVIF Clients as well as RTSP Clients. This enables easy exchange of video data as well as availability of Live / Playback streams.

The ONVIF Server plays a dual role:

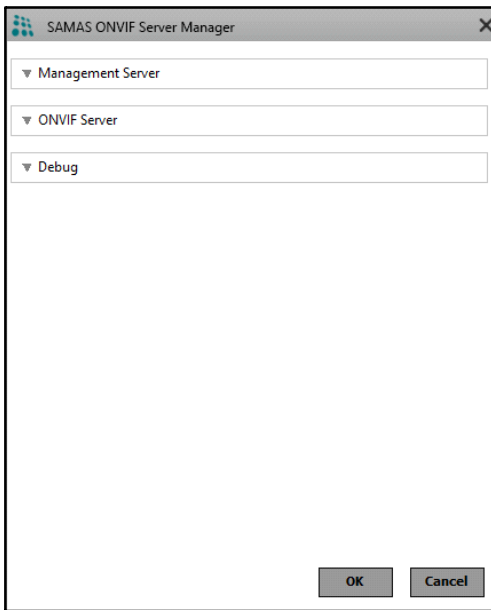
- acts as a Client for the Management Server/Recording Server
- acts as a Server for the 3rd Party ONVIF Clients
- Click on your PC Search option and enter **ONVIF Server Manager**. Click the same.



- The ONVIF Server icon appears in the Tray. Right-click on the **ONVIF Server** icon.



- Select **Configuration Settings** and the **SAMAS ONVIF Server Manager** window appears.



It includes the configuration of Management Server, ONVIF Server and Debug. Click on the links below for the detailed explanation.

- [“Management Server”](#)
- [“ONVIF Server”](#)
- [“Debug”](#)

Management Server

For the ONVIF Server to communicate with the Management Server (MS), a connection between them needs to be established by configuring the MS IP Address and Port in the ONVIF Manager. But it is not necessary that both the components are located in the same network (private), they may be located in two different networks (public).

Hence, SAMAS allows you to configure 3 Preferred Networks where you can add private network as well as public network of MS.

Click **Management Server** collapsible panel and configure the following parameters for Preferred Network 1(PN1), Preferred Network 2(PN2) and Preferred Network 3 (PN3):

The screenshot shows the SAMAS ONVIF Server Manager window. The 'Management Server' section is expanded, revealing three network configuration options. 'Preferred Network 1' is pre-filled with IP 127.0.0.1 and port 8500. The other two networks are empty. There are also sections for 'ONVIF Server' and 'Debug' which are currently collapsed. The 'Enable Secure Connection' checkbox is unchecked. At the bottom right, there are 'OK' and 'Cancel' buttons.

- **Enable Secure Connection:** Select the check box for ONVIF Server to communicate with the Management Server securely.

Preferred Network 1/2/3

- **IP or Server Name:** Enter either Private or Public IPv4/IPv6 Address of the Management Server on which ONVIF Server will communicate. You can also enter the Host Name, Domain Name or Server Name of ISP1/2. In IP or Server Name, you can enter upto 255 characters. Default: 127.0.0.1



If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.

- **Port:** Enter either Private or Public Port on which ONVIF Server will communicate. Valid Range: 1024-65535. Default: 8500.

For Private Network, enter the ONVIF Server Port.

For Public network, enter the Forwarded Port (ISP1/ISP2 Port) that has been mapped with the internal ONVIF Server Port.

The functionality of preferred network is same as explained while configuring preferred networks of Management Server. For details, refer to “[Management Server](#)”.



Configure the network with the highest priority in Preferred Network 1.


ONVIF Server

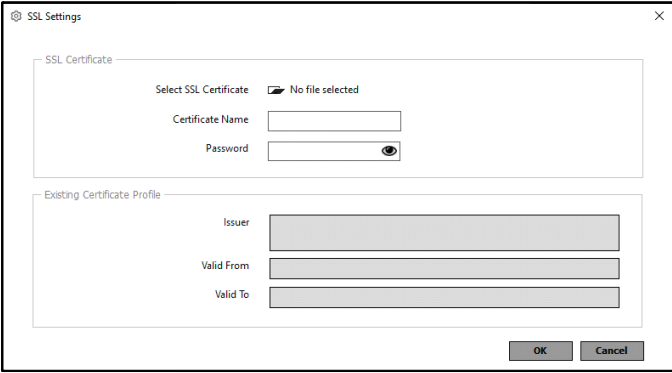
Click on **ONVIF Server** collapsible panel and configure the following parameters:

- **WS-Discovery:** WS-Discovery (Web Services Dynamic Discovery) is a technical specification that defines a multi-cast discovery protocol to locate services on a local network. Select the check box to enable discovering of web-based services within the network automatically.
- **Communicate Over:** Select the desired option — All Interface, Specific Interface — over which you wish the ONVIF Server and ONVIF Client should communicate.




*If you have selected **Communicate Over as All Interface**, then ONVIF Server will communicate on IPv4/IPv6 address through which the ONVIF Client has sent the request.*

- **ONVIF IP:** If you have selected **Communicate Over** as **Specific Interface**, configure the IPv4/IPv6 address of the ONVIF Server on which the ONVIF Client should communicate. In ONVIF IP, you can enter upto 39 characters. Default: Blank.
- **ONVIF Port:** Enter the ONVIF Port on which the ONVIF Client will send requests for video streams to the ONVIF Server. Valid Range: 1024-65535. Default: 580.
- **RTSP Port:** Enter the RTSP Port. RTSP Clients will send the RTSP requests to ONVIF Server on this port. Valid Range: 1024-65535. Default: 554.
- **RTP Port:** Enter the RTP Port to deliver audio and video over the Internet. This is the start port of RTP Port range. Valid Range: 1024-65535. Default: 5004.
- **Enable Secure Connection:** Select the check box for ONVIF Server to communicate with ONVIF Clients securely. Click **Upload Certificate** . The **SSL Settings** window appears.



SSL Settings

SSL Certificate

Select SSL Certificate  No file selected

Certificate Name

Password


Existing Certificate Profile

Issuer

Valid From

Valid To


OK Cancel

- **Select SSL Certificate:** Click **Browse**  and browse the path from where you wish to upload the SSL certificate. Make sure the certificate is in **.pfx** format.
- **Certificate Name:** Enter a name for the certificate. In Certificate, you can enter upto 30 characters. Default: Blank.
- **Password:** Enter Password for accessing the certificate. In Password, you can enter upto 30 characters. Default: Blank.

Click **OK** to save the SSL certificate or click **Cancel** to discard. If you click **OK**, the details of this certificate appear under Existing Certificate Profile.

Existing Certificate Profile

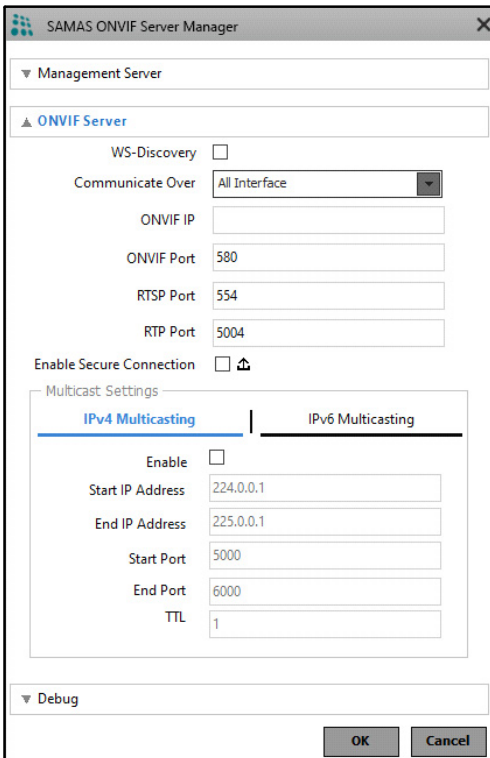
- **Issuer:** It displays the details of the certificate issuer.
- **Valid From:** It displays the validity **From** date and time of the certificate.
- **Valid To:** It displays the validity **To** date and time of the certificate.

If you wish to upload another certificate, click **Delete**  to delete the existing certificate and then click **Upload Certificate**  to upload a new certificate.


Multicast Settings

Multicasting helps optimize the network bandwidth consumption between the ONVIF Server and ONVIF Clients. Click the respective tabs — “[IPv4 Multicasting](#)”, “[IPv6 Multicasting](#)” — to configure the multicast settings.

IPv4 Multicasting



The screenshot shows the SAMAS ONVIF Server Manager window. The 'ONVIF Server' section is expanded, showing various configuration options. The 'Multicast Settings' section is also expanded, with the 'IPv4 Multicasting' tab selected. The 'Enable' checkbox for IPv4 Multicasting is unchecked. The 'Start IP Address' is 224.0.0.1, 'End IP Address' is 225.0.0.1, 'Start Port' is 5000, 'End Port' is 6000, and 'TTL' is 1. The 'IPv6 Multicasting' tab is also visible but not selected. The 'Debug' section is collapsed at the bottom.

Management Server	
ONVIF Server	
WS-Discovery	<input type="checkbox"/>
Communicate Over	All Interface
ONVIF IP	
ONVIF Port	580
RTSP Port	554
RTP Port	5004
Enable Secure Connection	<input type="checkbox"/> 
Multicast Settings	
IPv4 Multicasting IPv6 Multicasting	
Enable	<input type="checkbox"/>
Start IP Address	224.0.0.1
End IP Address	225.0.0.1
Start Port	5000
End Port	6000
TTL	1
Debug	

- **Enable:** Select the check box to enable Multicasting. If disabled, ONVIF will provide the stream to the RTSP Clients in Unicasting.
- **Start IP Address and End IP Address:** Enter the Start and End IPv4 Address that is to be used for Multicasting. The Multicasting communication will be done within this range. Make sure IPv4 address is configured in the system where ONVIF Server Manager is installed.

IPv4 Address Range 224.0.1.1 to 224.255.255.255 can be used for Multicasting within same subnet. For Cross Network Multicasting all other IPv4 Addresses can be used. In Start IP Address and End IP Address, you can enter upto 15 characters.

Default Range: 224.0.0.1 to 225.0.0.1

- **Start Port and End Port:** Enter the Start and End Port that is to be used for Multicasting. The Multicasting communication will be done within this range. Valid Range: 1-65535. Default Range: 5000-6000.
- **TTL:** Set the Time-to-Live (TTL) value. This defines the number of sub-networks a packet will be allowed to cross and after this the packet will be dropped. For example, if it is set as 4, a packet will be allowed to cross 4 sub-networks and then the packet will be dropped. Valid Range: 1-255.Default: 10.

IPv6 Multicasting

The screenshot shows the SAMAS ONVIF Server Manager configuration window. The 'ONVIF Server' section is expanded, showing various settings. The 'Multicast Settings' section is active, with the 'IPv6 Multicasting' tab selected. The 'Enable' checkbox is unchecked. The 'Start IP Address' is set to 'FF00::', and the 'End IP Address' is set to 'FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:F'. The 'Start Port' is set to '5000', and the 'End Port' is set to '6000'. The 'TTL' is set to '1'. The 'WS-Discovery' checkbox is unchecked. The 'Communicate Over' dropdown is set to 'All Interface'. The 'ONVIF IP' field is empty. The 'ONVIF Port' is set to '580'. The 'RTSP Port' is set to '554'. The 'RTP Port' is set to '5004'. The 'Enable Secure Connection' checkbox is unchecked. The 'Debug' section is collapsed. The 'OK' and 'Cancel' buttons are at the bottom right.

SAMAS ONVIF Server Manager

Management Server

ONVIF Server

WS-Discovery ☐

Communicate Over All Interface

ONVIF IP

ONVIF Port 580

RTSP Port 554

RTP Port 5004

Enable Secure Connection ☐

Multicast Settings

IPv4 Multicasting IPv6 Multicasting

Enable ☐

Start IP Address FF00::

End IP Address FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:F

Start Port 5000

End Port 6000

TTL 1

Debug

OK Cancel

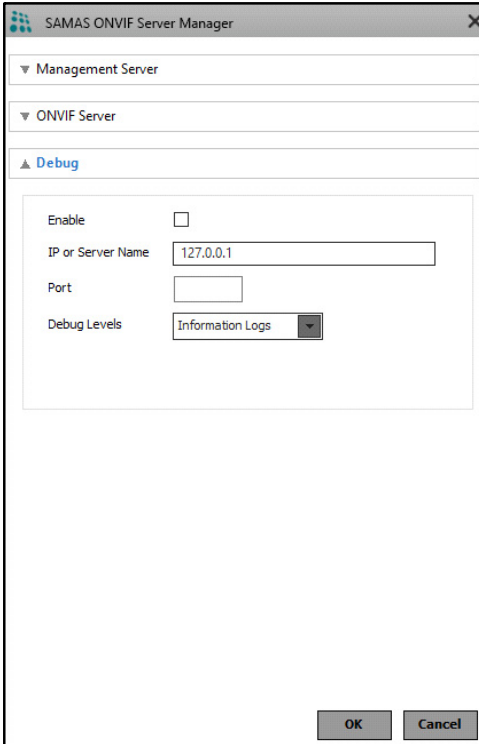
- **Enable:** Select the check box to enable Multicasting. If disabled, ONVIF will provide the stream to the RTSP Clients in Unicasting.
- **Start IP Address and End IP Address:** Enter the Start and End IPv6 Address that is to be used for Multicasting. The Multicasting communication will be done within this range. Make sure IPv6 address is configured in the system where ONVIF Server Manager is installed.

IPv6 Address Range FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF can be used for Multicasting within same subnet. For Cross Network Multicasting all other IPv6 Addresses can be used. In Start IP Address and End IP Address, you can enter upto 39 characters. Default Range: FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

- **Start Port and End Port:** Enter the Start and End Port that is to be used for Multicasting. The Multicasting communication will be done within this range. Valid Range: 1-65535. Default Range: 5000-6000.

- **TTL:** Set the Time-to-Live (TTL) value. This defines the number of sub-networks a packet will be allowed to cross and after this the packet will be dropped. For example, if it is set as 4, a packet will be allowed to cross 4 sub-networks and then the packet will be dropped. Valid Range: 1-255. Default: 10.

Debug



The screenshot shows the 'SAMAS ONVIF Server Manager' window with the 'Debug' tab selected. The 'Enable' checkbox is unchecked. The 'IP or Server Name' field contains '127.0.0.1'. The 'Port' field is empty. The 'Debug Levels' dropdown menu is set to 'Information Logs'. At the bottom are 'OK' and 'Cancel' buttons.

- **Enable:** Select the check box to enable the debug.
- **IP or Server Name:** Specify the IPv4/IPv6 Address or Server Name of the Syslog Server. In IP or Server Name, you can enter upto 255 characters. Default: 127.0.0.1



If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.

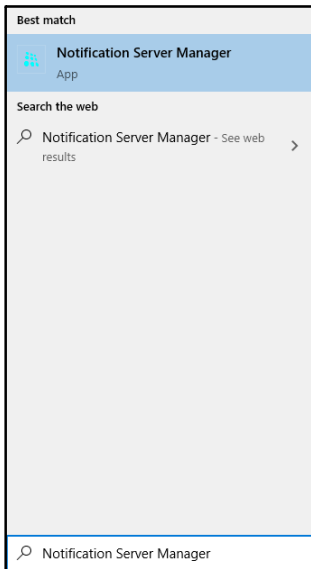
- **Port:** Specify the Port of the Syslog Server. Valid Range: 1024-65535. Default: Blank.
- **Debug Levels:** Select the desired level of debug — Information Logs or Detailed Logs.
- Click **OK** to save settings.

Now from the Tray, right-click on the **ONVIF Server** icon again and select **Start ONVIF Server** to start the service.

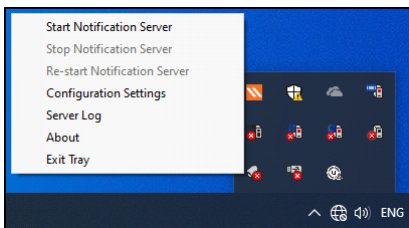
Step-7: Configure Notification Server settings using the Notification Server Manager Utility.

The Notification Server is responsible for configuration of Mail Server, SMS Service Provider and WhatsApp to send E-mail, SMS and WhatsApp Notifications to the User.

- Click on your PC Search option and enter **Notification Server Manager**. Click the same.



- The Notification Server icon appears in the Tray. Right-click on the **Notification Server** icon.



- Select **Configuration Settings**. The **SAMAS Notification Server Manager** window appears.

- Enter the **User Name** and **Password** as configured in Admin Client. In User Name and Password, you can enter upto 50 characters. Default: Blank.
- Then click **Login**.



Make sure the user has the configuration rights of Message Templates in System Accounts of Admin Client.

The following window appears.

It includes the configuration of Email, SMS, WhatsApp and Debug. Click on the links below for the detailed explanation.

- [“Email”](#)
- [“SMS”](#)
- [“WhatsApp”](#)

- “Debug”

Email

Click the **Email** tab and configure the following parameters:

Email Settings

- **SMTP Server:** Specify the IPv4/IPv6 Address or Name of the configured SMTP Server. In SMTP Server, you can enter upto 150 characters. Default: Blank.
- **SMTP Port Number:** Specify the TCP port for the SMTP service as set in the SMTP Server. Valid Range: 1-65535. Default: 25.
- **Sender Email Id:** Enter the sender's Email ID. In Sender Email Id, you can enter upto 100 characters. Default: Blank.
- **Sender Display Name:** Enter the User Name that will be displayed in the Emails. In Sender Display Name, you can enter upto 50 characters. Default: Blank.
- **User Name:** Specify the User Name as set in the Email account. In User Name, you can enter upto 50 characters. Default: Blank.
- **Password:** Specify the Password as set in the Email account. In Password, you can enter upto 16 characters. Default: Blank.



If your SMTP requires additional security authentication, such as Multi level, Third party client usage password, then use your account generated password and not your Email password.

- **Alert Cycle:** Specify the time in seconds between successive send attempts when the system tries to send the pending messages. Valid Range: 1-120. Default: 10.
- **Retry Count:** Specify the number of times the system needs to retry to send the same Email message in the event of an unsuccessful attempt. Valid Range: 3-99. Default: 3.
- **Active Days:** Specify the number of days the system needs to keep the unsent messages active in the event of the service being stopped. Valid Range: 1-99. Default: 1.
- **Enable SSL:** In the event of using an external SMTP Server like Gmail, then make sure this is enabled.
- **Enable Sending Email:** Select this check box to enable the mail sending functionality.

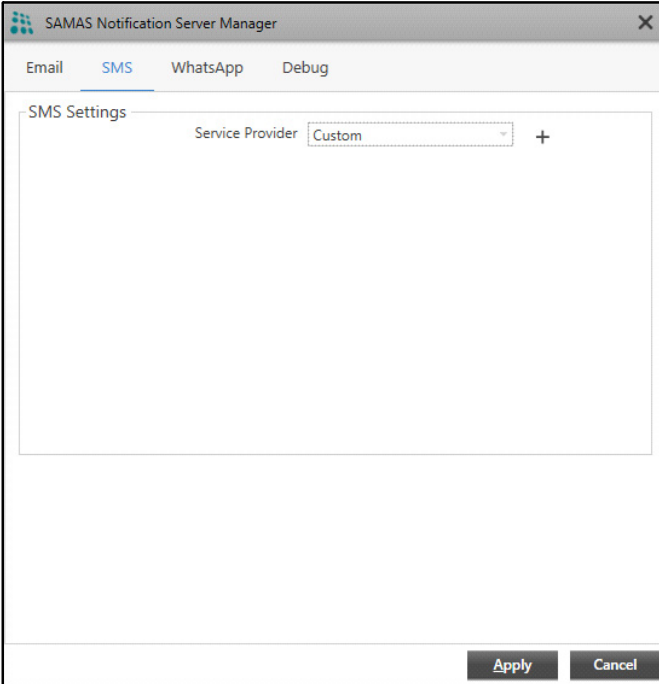
Test

- **Email Id:** Enter the Email ID to check the connectivity and click **Send**. In Email Id, you can enter upto 100 characters. Default: Blank.

Click **Apply** to save the settings.

SMS

Click the **SMS** tab, select **Custom** as the Service Provider. Once the Custom Service Provider settings are configured, they appear in the **Service Provider** drop-down list.

The screenshot shows the 'SAMAS Notification Server Manager' application window. It has four tabs: 'Email', 'SMS' (which is selected and highlighted with a blue underline), 'WhatsApp', and 'Debug'. The 'SMS Settings' section is visible, containing a 'Service Provider' dropdown menu with 'Custom' selected. To the right of the dropdown is a plus sign icon. At the bottom right of the window are two buttons: 'Apply' and 'Cancel'.

If you have already configured Default Service Providers in the software version you have installed and you are upgrading the same to V6R2, then after the re-installation process completes, you will have to manually configure the required Service Providers under Custom Service Providers.

Custom Service Provider Settings

You need to configure the desired Service Provider. To do so,

- Select **Custom** as the Service Provider option. Maximum 99 Service Providers can be added.
- Click **Add** + .

The **Custom Service Provider** pop-up appears.

Custom Service Provider

Request

Service Provider Name

Service Provider URL

Base URL

API Argument

Argument Value

Custom

Add Argument Cancel

API Argument	Argument Value	Delete

Argument Separator

Request Method

Request Preview

Balance

Balance Check ☐

Balance URL


Apply Cancel

Configure the following parameters:

Request

- **Service Provider Name:** This is the Service Provider's Name. In Service Provider Name, you can enter upto 30 characters. Default: Blank.
- **Service Provider URL:** This is the Service Provider's Website used for registration etc. For example: www.smsgatewaycentre.com. In Service Provider URL, you can enter upto 100 characters. Default: Blank.
- **Base URL:** This is the URL to which arguments such as user name, password etc. are to be appended. For example http://smsgatewaycentre.com/library/send_sms_2.php? In Base URL, you can enter upto 100 characters. Default: Blank.

- **API Argument:** Enter the argument required to be mentioned while constructing the URL. For example User, Password etc. In API Argument, you can enter upto 30 characters. Default: Blank.
- **Argument Value:** Select a value to be mapped against the defined API Argument. Select Custom to define a custom static value.

Click **Add Argument** to add the new argument and value. The new argument and value appears in the grid below. Click **Delete**  to delete the argument.

- **Argument Separator:** Define a character that can be used as a valid separator between arguments used to construct the API URL. For example &. In Argument Separator, you can enter upto 1 characters. Default: Blank.
- **Request Method:** Select a method by which the request is to be sent.
- **Request Preview:** Displays the preview of the updated API request.

Custom Service Provider

Argument Separator

Request Method POST

Request Preview

Balance

Balance Check ☐

Balance URL

Response

API Response

SAMAS Response Success

Add Response

Cancel

API Response	Samas Response	Delete

Apply

Cancel

Balance

- **Balance Check:** Select the check box if you want SAMAS to fetch the balance from the specified URL.
- **Balance URL:** Configure the URL of the Service Provider to fetch the balance. In Balance URL, you can enter upto 100 characters. Default: Blank.

Response

- **API Response:** Define the response or error codes. Maximum 99 responses can be configured. In API Response, you can enter upto 100 characters. Default: Blank.
- **SAMAS Response:** For the configured API response, select the corresponding SAMAS Response such as Success or Failure. For example: Error 404 should be considered as Failure.

Click **Add Response** to save the response configuration. The API Response and SAMAS

Response appear in the grid below. Click **Delete**  to delete the response.

The configured Service Provider appears in the **Service Provider** drop-down list under **SMS Settings**.



SMS Settings

Select the configured Service Provider from the **Service Provider** drop-down list.


SAMAS Notification Server Manager

Email **SMS** WhatsApp Debug

SMS Settings

Service Provider: Bulk SMS  

User Name:

Password: 

Sender ID:

Alert Cycle: 10 (1 - 120 seconds)

Retry Count: 3 (3 - 99)

Active Days: 1 (1 - 9 days)

Enable Sending SMS: ☐

www.bulksms.com

Test

Mobile number: **Send**

SMS Template ID:

Check balance: **Check**

Apply **Cancel**

Click **Edit**  , if you wish to edit the parameters of the created Custom Service Provider.

Click **Delete**  , if you wish to delete the created Custom Service Provider.

Configure the following parameters:

- **User Name:** Specify the User Name for the SMS Service Provider. In User Name, you can enter upto 50 characters. Default: Blank.
- **Password:** Specify the Password for the SMS Service Provider. In Password, you can enter upto 16 characters. Default: Blank.
- **Sender ID:** Enter the registered Sender ID. In Sender ID, you can enter upto 50 characters. Default: Blank.
- **Alert Cycle:** Specify the time in seconds between successive send attempts when the system tries to send the pending messages. Valid Range: 1-120. Default: 10.
- **Retry Count:** Specify the number of times the system needs to retry to send the same SMS in the event of an unsuccessful attempt. Valid Range: 3-99. Default: 3.

- **Active Days:** Specify the number of days the system needs to keep the unsent messages active in the event of the service being stopped. Valid Range: 1-9. Default: 1.
- **Enable Sending SMS:** Select this check box to enable the SMS sending functionality.

The URL displayed is a link to the website of the selected Service Provider. Click on the link and login with your User Name and Password to connect with the Service Provider.

Test

- **Mobile Number:** Enter the Mobile Number to which you wish to send the Test Message. In Mobile Number, you can enter upto 15 characters. Default: Blank.
- **SMS Template ID:** As per TRAI Regulation, an enterprise which sends messages to customers like OTP, communication message, promotional messages via SMS, have to register their entity and the content template to avoid Spam, fake and fraudulent communication through SMS.

It is mandatory for an Admin to register the SMS content template prior with your Service Provider which will be verified before it is delivered to the users.

Once registered, the Service Provider will provide a Template ID against the registered SMS content.

To send a test message, make sure a pre-defined Test Message content is registered with the desired Service Providers. For example, **Hello this is a test message.**

The Service Provider will provide a Template ID against this test message. Enter the Template ID provided by the Service Provider here. In SMS Template ID, you can enter upto 30 characters. Default: Blank.



All the SMS Templates - Default as well as Custom must be registered with the desired Service Providers to enable sending the SMS. If any modifications are done in the template after registration, then the same needs to be registered again. For details, refer to the SATATYA SAMAS Admin Client Manual, General Settings > Message Templates.

If you have multiple Service Providers, then make sure the required templates are registered with all the desired Service Providers. Hence for each template you will have multiple Templates IDs. Also make sure you maintain a record of all the registered Message Templates with their respective Template IDs for reference.

Click **Send** to send the Test Message.

Click **Check** if you wish the system to fetch the balance from the configured URL of the Service Provider.

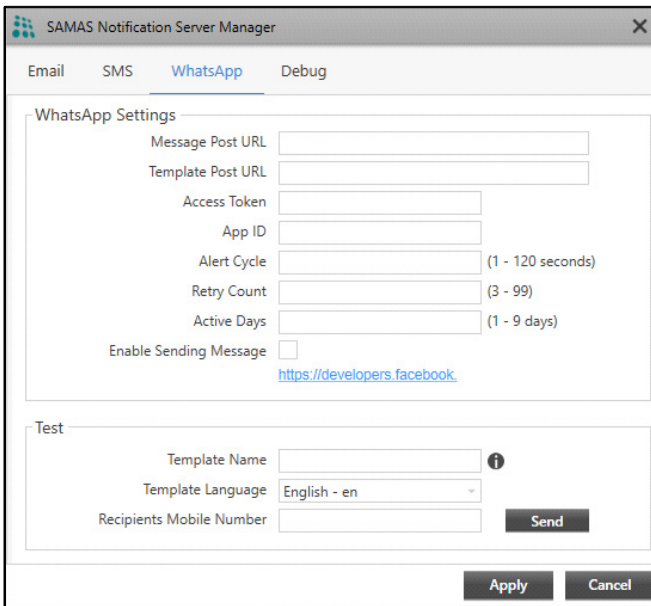
Click **Apply** to save the settings.

WhatsApp

Before configuring the WhatsApp Settings, make sure you go through the Pre-Requisites and configure the necessary parameters in the Admin Client. For details, refer to the SATATYA SAMAS Admin Client Manual, General Settings > WhatsApp Integration.

Click the **WhatsApp** tab and configure the following parameters:

WhatsApp Settings



The screenshot shows the 'SAMAS Notification Server Manager' application window with the 'WhatsApp' tab selected. The window contains two main sections: 'WhatsApp Settings' and 'Test'. The 'WhatsApp Settings' section includes input fields for 'Message Post URL', 'Template Post URL', 'Access Token', and 'App ID'. It also has dropdown menus for 'Alert Cycle' (with a range of 1 - 120 seconds), 'Retry Count' (with a range of 3 - 99), and 'Active Days' (with a range of 1 - 9 days). There is a checkbox for 'Enable Sending Message' and a link to 'https://developers.facebook.'. The 'Test' section includes input fields for 'Template Name', 'Template Language' (set to 'English - en'), and 'Recipients Mobile Number'. A 'Send' button is located next to the 'Recipients Mobile Number' field. At the bottom of the window are 'Apply' and 'Cancel' buttons.

- **Message Post URL:** This is the URL that will be used for sending WhatsApp Messages. In Message Post URL, you can enter upto 150 characters.

Default: `https://graph.facebook.com/v17.0/{Phone_Number_ID}/messages`

You only need to change the {Phone_Number_ID} in the URL, with your actual Phone Number ID. The Phone Number ID can be taken from the WhatsApp Business Account you created.

You also need to check if the version mentioned in the URI, that is v17.0, is the same as your WhatsApp Business Account Version. If not, change it as per your account version.

For example, if your Phone Number ID is 123115956238956 and version is 18, then the URL will be: <https://graph.facebook.com/v18.0/123115956238956/messages>.



The system will only consider the configured URL for sending messages. Make sure it is configured correctly.

- **Template Post URL:** In Template Post URL, you can enter upto 150 characters.
Default: https://graph.facebook.com/v17.0/{WhatsApp_Business_Account_ID}/message_templates.

You need to replace the {WhatsApp_Business_Account_ID} with your WhatsApp Business Account ID. While replacing the text make sure you remove the brackets and do not change the format. For example: https://graph.facebook.com/v17.0/111000111100/message_templates.



To check your WhatsApp Business Account ID, navigate to Business Manager > Business Settings > Accounts > WhatsApp Business Accounts. Click on your account. A panel opens with the information of your account as well as ID.

- **Access Token:** Enter the token number received after you have successfully created the WhatsApp Business Account. In Access Token, you can enter upto 500 characters.
Default: Blank.
- **App ID:** Enter the App ID of your WhatsApp Business Account. In App ID, you can enter upto 20 characters. Default: Blank.



To check your App ID, navigate to Business Manager > Business Settings > Accounts > WhatsApp Business Accounts. Click on your account. A panel opens with the information of your account as well as ID.

- **Alert Cycle:** Specify the time in seconds between successive send attempts when the system tries to send the pending messages. Valid Range: 1-120. Default: 10.
- **Retry Count:** Specify the number of times the system needs to retry to send the same WhatsApp Message in the event of an unsuccessful attempt. Valid Range: 3-99. Default: 3.
- **Active Days:** Specify the number of days the system needs to keep the unsent messages active in the event of the service being stopped. Valid Range: 1-9. Default: 1.

- **Enable Sending Message:** Select this check box to enable the WhatsApp Message sending functionality.

Test

- **Template Name:** Enter the name of the template you created as the Test Template in your WhatsApp Business Account. For details, refer to the SATATYA SAMAS Admin Client Manual, General Settings > WhatsApp Integration > Test Message Template Creation. In Template Name, you can enter upto 512 characters. Default: test_message.
- **Template Language:** Select the desired language from the drop-down list.



Make sure the Template is registered and approved by WhatsApp.

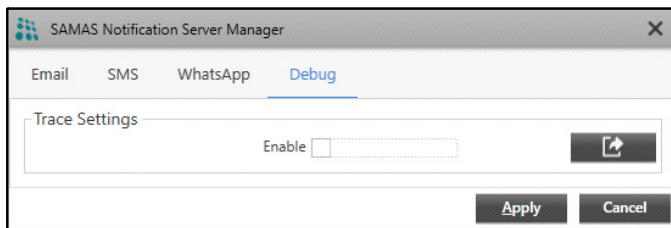
Make sure you select the same language in which the template has been registered. Selecting a different language will result in failure of sending the Test Message.


- **Recipients Mobile Number:** Enter the mobile number to which you wish to send the test WhatsApp Message. In Recipients Mobile Number, you can enter upto 15 characters. Default: Blank.
- Click **Send** to send the test WhatsApp Message.

Click **Apply** to save the settings.

To view the details of the WhatsApp Messages sent from the Notification Server, right-click on the **Notification Server Manager** icon from the Tray and select **Server Log** from the menu options. For details, refer to the SATATYA SAMAS Admin Client Manual, General Settings > Message Template > Notification Server Logs.

Debug



- **Enable:** Select the **Enable** check box to enable debug. Click **Export Logs**  and specify the path of the local system where you wish to store the logs.

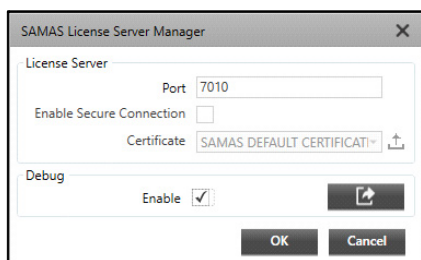
- Click **Apply** to save the changes.

Now from the Tray, right-click on the **Notification Server** icon again and select **Start Notification Server** to start the service.


Communication between Management Server (MS), Recording Server (RS) and License Server (LS)

Let us understand the communication between the three servers with the help of an example. If the License Server is located at the Head Office - 192.168.104.20, Management Server is at the Branch Office - 192.168.104.17 and Recording Server with cameras is located at the Server Room - 192.168.104.23

To view cameras in the Server Room from Branch Office, specify the License Server Port (where SAMAS Dongle is connected) in the License Server Manager of Branch Office PC.




In the Management Server Manager enter the License Server IP 192.168.104.20 and Port 7010.


SAMAS Management Server Manager
✕

Management Server

Non SSL
SSL

Enable Secure Connection
☐

Certificate
SAMAS DEFAULT CERTIFICATE


Admin Client Port
7711

Recording Server Listening Port
7090

Media Client Port
7085

COSEC Port
7089

IVA Server Port
7100

SAMAS TCP API Port
7200

SAMAS HTTP API Port
7300

Transcoding Server Port
7400

ONVIF Server Port
7500

License Verification


Enable Secure Connection
☐

Select Mode
Service Based

IP or Server Name
192.168.104.20

Port
7010

Debug

Enable
☐


OK
Cancel

Now the Recording Server is installed at 192.168.104.23. So open the Recording Server Manager and enter the IP Address as 192.168.104.17 and Port as 8090 of MS.

SAMAS Recording Server Manager

Management Server

Enable Secure Connection ☐

Preferred Network 1

IP or Server Name: 192.168.104.17

Port: 8090

Preferred Network 2

IP or Server Name:

Port:

Preferred Network 3

IP or Server Name:

Port:

Recording Server

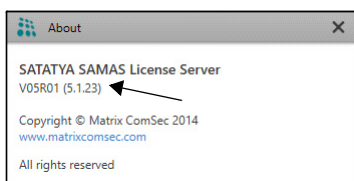
Debug

OK Cancel

The RS will send request to MS to activate. From the Admin Client the RS must be activated and then cameras of the RS can be viewed in the Smart Client.



*For the Version details about each Server, right-click on the particular Server icon in the Tray and click **About** as shown below.*



SSL Configurations

SSL (Secure Socket Layer) is a standard used for transmitting sensitive data securely in an encrypted format. It uses asymmetric keys defined in pairs of public/private key to secure the communication between client and server. Public key is available to all the clients while Private key is available only with the server holding a SSL certificate. The keys have following properties:

- Data encrypted by client using public key can be decrypted only by the server using the private key.
- Data encrypted by server's private key can be decrypted only by using the public key.

For secure communication between the components of SAMAS, SSL is required. You need to enable the Secure connection from:

- the Management Server Manager page while configuring the Management Server settings.
- the License Server Manager page while configuring the License Server settings.
- the Recording Server Manager page while configuring the Recording Server settings.

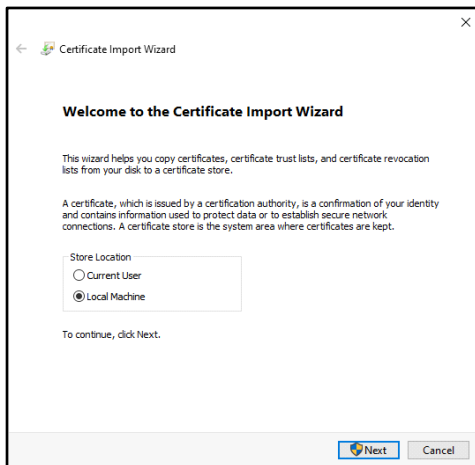
The SSL Configurations can be done as follows:

- To place the certificates in the Windows Certificate Store manually, refer to ["Uploading SSL Certificate"](#).
- OR**
- If you wish to upload a new certificate in the Windows Certificate Store automatically, refer to ["SSL Settings"](#).

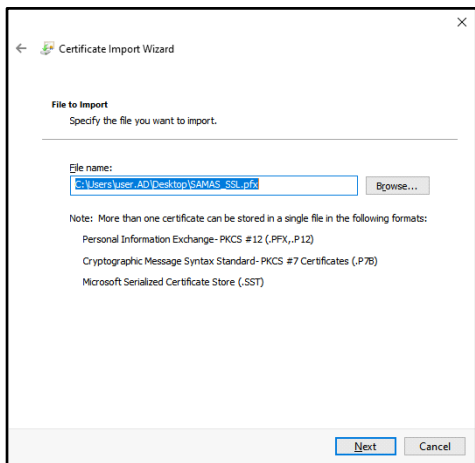
Uploading SSL Certificate

Make sure you have logged in to your PC as an administrator. Follow the steps given below to upload the certificate.

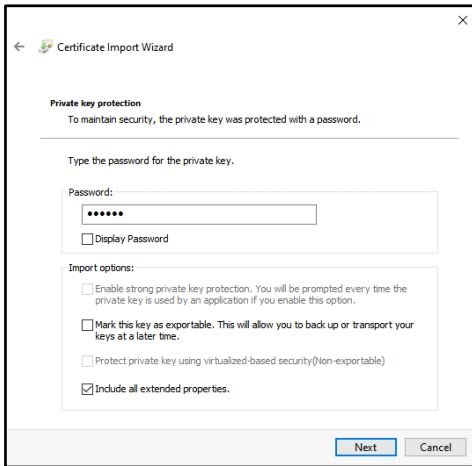
- Double-click on the SSL Certificate. The **Certificate Import Wizard** pop-up appears.



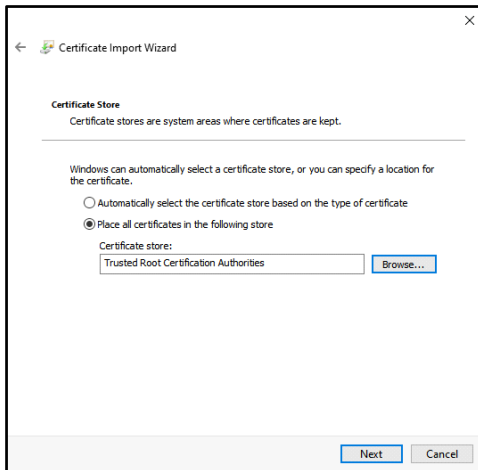
- Select **Local Machine**. Click **Next**.



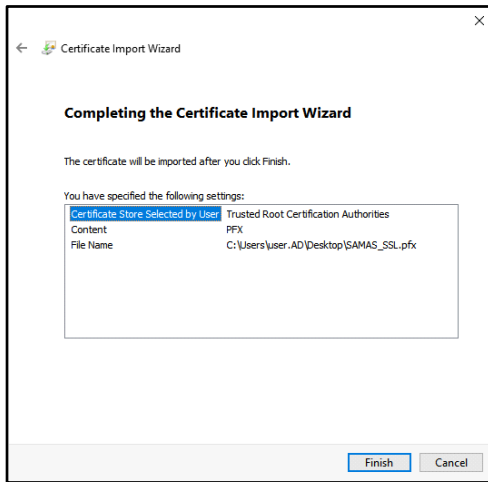
- Browse and select the path where you have saved the SSL Certificate. Click **Next**.



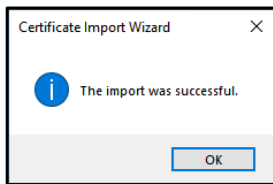
- Enter the Password of the Certificate. Click **Next**.



- Select the option **Place all certificates in the following store**. Click **Browse** and select the **Trusted Root Certification Authorities** folder. Click **Next**.



- The Certificate details are displayed. Click **Finish**.



- A pop-up for successful import appears.

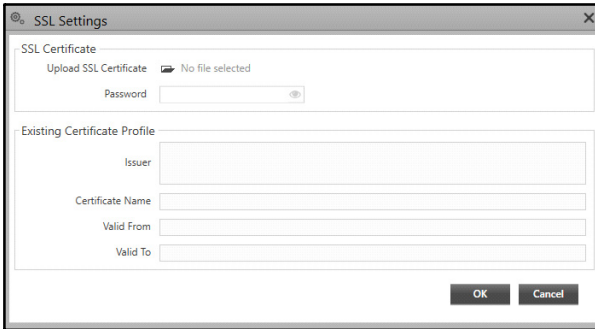
To view the certificate,

- Click on your PC Search option and enter **Manage User Certificates**. Click the same.
- Double-click the **Trusted Root Certification Authorities** folder.
- Double-click the **Certificates** folder.
- The certificate you uploaded appears here.




*You can also upload the certificate from **Certificates** folder using the Right-click > All Tasks > Import option.*

SSL Settings



SSL Settings

SSL Certificate

Upload SSL Certificate  No file selected

Password

Existing Certificate Profile

Issuer


Certificate Name

Valid From

Valid To

OK Cancel

SSL Certificate

- **Upload SSL Certificate:** Click **Browse**  and browse the path from where you wish to upload the SSL certificate. Make sure the certificate is in **.pfx** format.
- **Password:** Enter Password for accessing the certificate. In Password, you can enter upto 30 characters. Valid Values: Alphabets, numbers, space, '(', ')', '-', '_', '[' and ']'

Click **OK** to save the SSL certificate or click **Cancel** to discard. If you click **OK**, the details of this certificate appear under Existing Certificate Profile.

Existing Certificate Profile

- **Issuer:** It displays the details of the certificate issuer.
- **Certificate Name:** It displays the Certificate Name.
- **Valid From:** It displays the validity **From** date and time of the certificate.
- **Valid To:** It displays the validity **To** date and time of the certificate.

This certificate will be saved in the Windows Certificate Store (In PC Search option, enter Manage User Certificates to view this certificate).

Port Forwarding

When Management Server, Recording Server, Failover Server, Transcoding Server, ONVIF Server and IVA Server are in different networks and inter-connectivity needs to be established, then Port Forwarding is required.

Make sure the Management Server (MS), License Server (LS), Database and Notification Server (NS) are in the same network and at the same location. Also, the Recording Server and the Failover Server both should be in the same network or at the same location.

Let us understand the same with the help of an example:

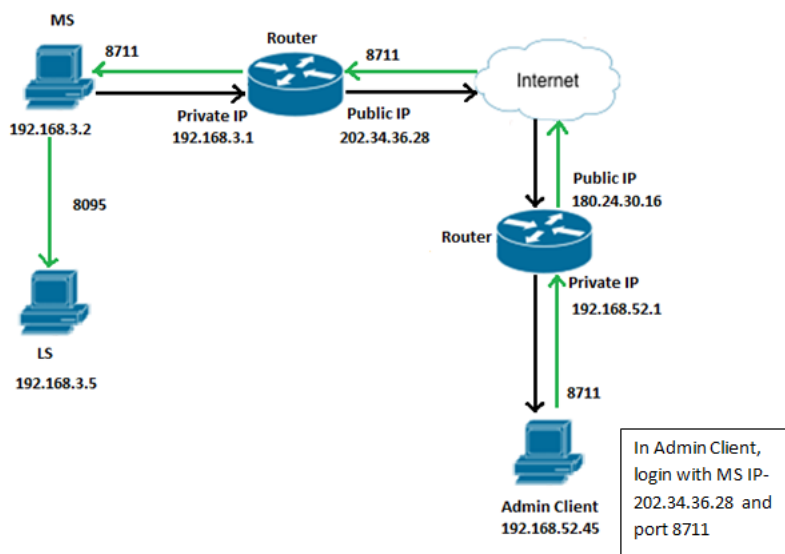
- MS + LS +NS are at Mumbai in public network.
- Recording Server is in Vadodara Matrix HO- PC1
- IVA Server is in Vadodara Matrix HO-PC2
- Failover Server is in Vadodara Matrix HO- PC3

PC IP (Private IP)	Router IP (Public IP)
RS – 192.168.1.2	173.16.20.4HO
IVA – 192.168.1.5	
FOS – 192.168.1.7	
MS, LS, NS – 192.168.3.2	202.34.36.28Mumbai

The Admin Client using IP 182.24.10.1 sends request to the router to which the port 8711 is forwarded. The router gets connected to the IP 202.34.36.28 via the Internet. Now, the 8711 port is forwarded to the router connected to MS, gets connected to MS at 192.168.3.2. The MS verifies the availability of License at port 8095 and sends the response to Admin Client.

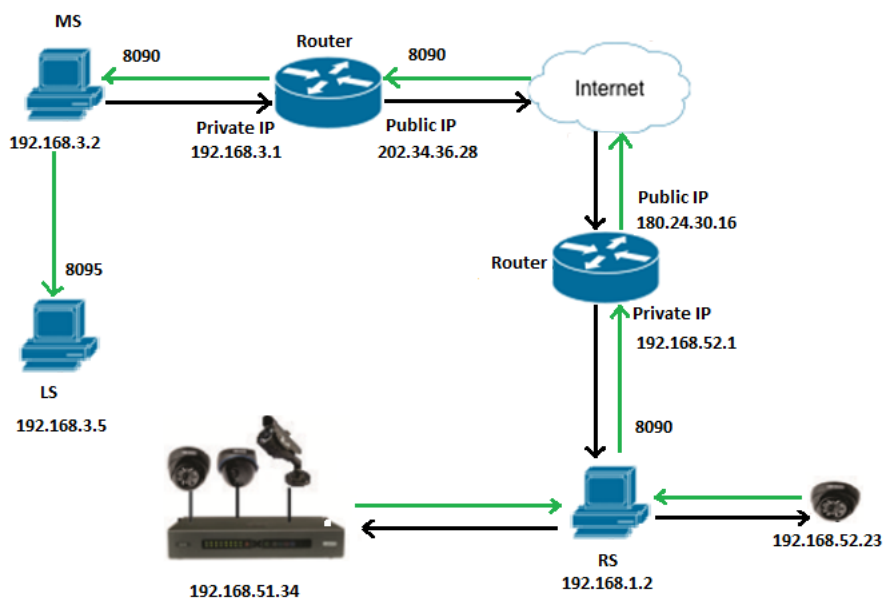
To connect Admin Client to MS:

The Admin Client Port **8711** is to be forwarded to the router connected to MS. Similarly, Media Clients (Smart Client, Mobile viewer) Port **8085** can be forwarded to the router connected to MS.



To connect Recording Server to MS:

- The Recording Server port **8090** is to be forwarded to the router connected to MS.

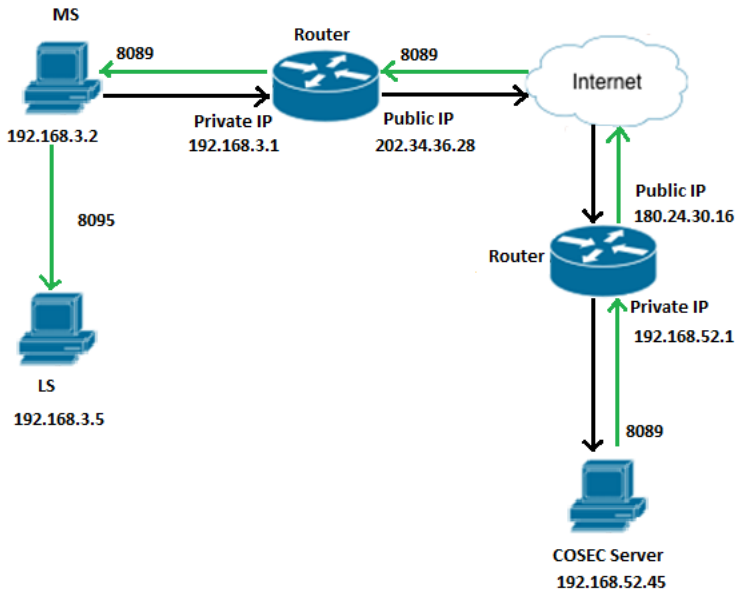


To connect API to MS:

- Port **8200** is to be forwarded to the router connected to MS.

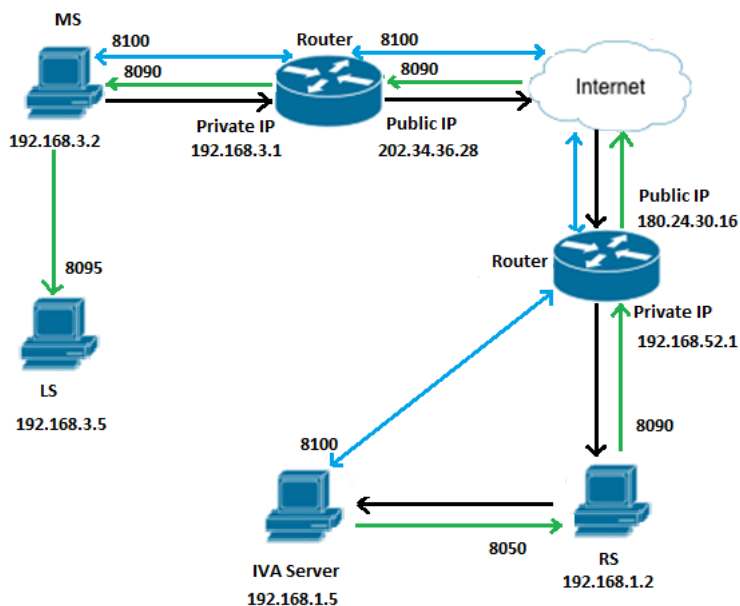
To connect COSEC Server port to MS:

- The COSEC Server port **8089** is to be forwarded to the router connected to MS.



To connect IVA Server port to MS:

- The IVA Server port **8100** is to be forwarded to the router connected to MS.



To get live streaming from cameras:

- Port **8050** is to be forwarded to the router connected to RS.

To add matrix devices to the SAMAS automatically:

- Port **8151** is to be forwarded to the router connected to RS.

Licensing of SATATYA SAMAS

License Dongles

License Name	Description
Matrix License Dongle 200	Supports all Licenses of SAMAS Application. USB Dongle needs to be inserted on a Server, COSEC VEGA, COSEC Panel200 to run the SAMAS Application. Needs to be activated.For details, refer to License Management Settings in the SATATYA SAMAS Admin Client Manual.
Matrix Virtual Dongle 300	Virtual (Dongle-less) License Management for all SAMAS Licenses. Needs to be registered. For details, refer to License Management Settings in the SATATYA SAMAS Admin Client Manual.

The SATATYA SAMAS provides IVA and Application based license. Each has been classified in the table below.

License Name	Abbreviation
IVA License	
SATATYA SAMAS Enterprise IVA Detection	EIVA Detection
SATATYA SAMAS Automatic Number Plate Recognition	ANPR
Application License	
SATATYA SAMAS Vehicle Tracking and Parking Management	VTPM
SATATYA SAMAS People Movement and Tracking	PMTCT
SATATYA SAMAS Cognitive Response Engine with Automated Monitoring	CREAM

The SATATYA SAMAS License is available as SATATYA SAMAS PLT.

If the user wish to upgrade the existing license or buy the new one, refer the table below. The table lists all the top up vouchers available for each license category.

License Name	License Category/Description	Top up Vouchers Available
SATATYA SAMAS PLT		
SATATYA SAMAS PLT	<p>Enterprise VMS: Software for up to 65,535 Cameras</p> <ul style="list-style-type: none">• Direct Connection of Matrix Video Recorders as well as Cameras to the Recording Server• 1 User, 5 Built-in Cameras and Maximum 65,535 Cameras• Unlimited Recording Servers, No License Cost for Additional Recording Servers• Remote and Centralized Viewing and Management by Admin, Smart and Mobile Clients• Automatic License Plate Recognition (ANPR) for 1 Camera• EIVA License for 1 Camera, 1 License for CREAM, Parking Managementfor5VTPMSlots• Multi-Display Supported to Connect to 2/4/8 Monitoring Screens• Real-time Notifications like Video Popup, SMS, Email, Alarms and E-Map• Software Upgradation will be FOC Validated up to one Year from the Date of Activation	-

License Name	License Category/Description	Top up Vouchers Available
MATRIX LICENSE DONGLE 200	Enterprise VMS: USB Dongle to Run SAMAS Application (Generic Key) <ul style="list-style-type: none"> • Support All Licenses of SAMAS • Dongle can be inserted on SERVER /COSEC VEGA/ COSEC PANEL LITE • Activate SAMAS License MATRIXLICENSEDONGLE200 	-
MATRIX VIRTUAL DONGLE 300	Virtual License Management for all SAMAS Licenses. <ul style="list-style-type: none"> • Dongle-less Solution for SAMAS Software • Seamlessly Managed by Software • License Data Securely stored in encrypted form • Efficient License Management, that is, reading, activation and validation through software 	-
IVA License		
SATATYA SAMAS Enterprise IVA Detection	To Upgrade Number of Cameras in IVA Detection (Includes Perimeter Events)	1.SATATYA SAMAS EIVA1 2.SATATYA SAMAS EIVA3 3.SATATYA SAMAS EIVA10
SATATYA SAMAS ANPR	To Upgrade Number of Cameras in ANPR (Includes Vehicle Management Events)	1.SATATYA SAMAS ANPR1 2.SATATYA SAMAS ANPR3 3.SATATYA SAMAS ANPR10

License Name	License Category/Description	Top up Vouchers Available
Application License		
SATATYA SAMAS VTPM	To Upgrade Number of Parking Entities in VTPM (Includes Parking Management Events and Vehicle Counting event from camera)	1.SATATYA SAMAS VTPM10 2.SATATYA SAMAS VTPM50 3.SATATYA SAMAS VTPM200
SATATYA PMTC	To Upgrade Number of Cameras in PMTC (Includes Crowd Management Events and People Counting event from camera)	1.SATATYA PMTC1 2.SATATYA PMTC3 3.SATATYA PMTC10
SATATYA SAMAS CREAM	To Upgrade Number of Advanced Scenarios in CREAM	1.SATATYA SAMAS CREAM5 2.SATATYA SAMAS CREAM10 3.SATATYA SAMAS CREAM50
Extra License		
SATATYA SAMAS Camera	To Upgrade Number of Cameras	1.SATATYASAMASCAM5 2.SATATYA SAMAS CAM20 3.SATATYA SAMAS CAM100
SATATYA SAMAS PLT AUP CAM	For Annual Upgradation of Cameras (Annual Upgradation of all the new features)	1. SATATYA SAMAS PLT AUP CAM5 2. SATATYA SAMAS PLT AUP CAM20 3. SATATYA SAMAS PLT AUP CAM100
SATATYA SAMAS User	To Upgrade Number of simultaneous Users	1.SATATYASAMASUser1 2.SATAYA SAMAS User3 3.SATATYA SAMAS User10

The **maximum upgradeable** limit of SATATYA SAMAS license is as shown below:

Category	SATATYA SAMAS PLT
Maximum number of simultaneous users	65535
Maximum number of cameras	65535
Maximum number of cameras for EIVA Detection	1023
Maximum number of cameras for ANPR	1023
Maximum number of slots for VTPM	65535
Maximum number of cameras for PMTC	1023
Maximum number of scenarios for CREAM	1023



MATRIX COMSEC

Head Office

394-GIDC, Makarpura, Vadodara - 390010, India.

Ph: (+91)1800 258 7747

E-mail: Tech.Support@MatrixComSec.com

Website: www.matrixcomsec.com