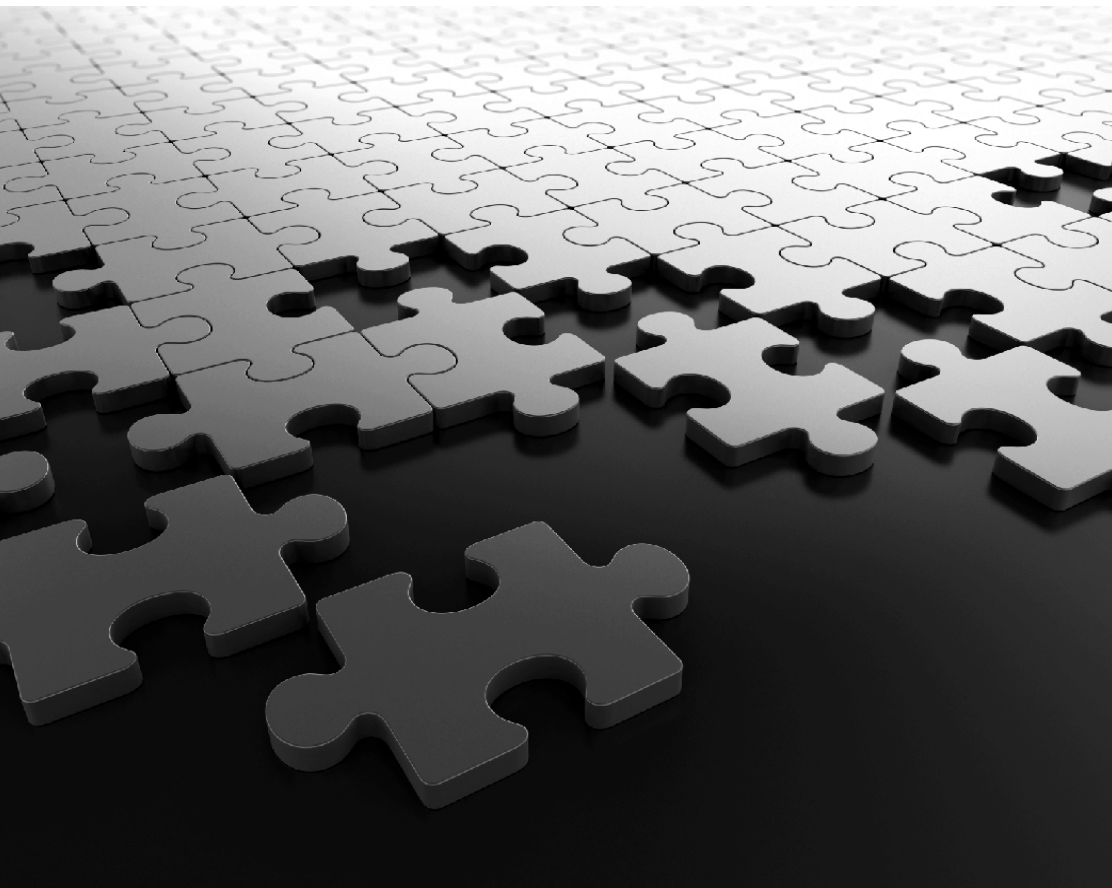


# **SATATYA SAMAS**

## **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.matrixvideosurveillance.com/product-registration-form.html>

*Version 5*

*Release date: June 2, 2023*



# Contents

---

<b>Getting Started .....</b>	<b>1</b>
<i>Introduction .....</i>	<i>1</i>
<i>System Requirements .....</i>	<i>1</i>
<b>Software Installation .....</b>	<b>5</b>
<i>System Pre-requisites .....</i>	<i>5</i>
<i>SATATYA SAMAS Installer Utility .....</i>	<i>5</i>
<i>Create/Upgrade/Backup Database .....</i>	<i>20</i>
<i>Uninstallation and Reinstallation .....</i>	<i>28</i>
<i>Installing SAMAS Components at Different Sites .....</i>	<i>30</i>
<i>Service Installation .....</i>	<i>31</i>
<i>SSL Settings .....</i>	<i>67</i>
<i>Port Forwarding .....</i>	<i>69</i>
<b>Licensing of SATATYA SAMAS .....</b>	<b>73</b>



# 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

Hardware/Software	Minimum	Recommended
Network	100 Mbps	1 Gbps
Hard disk Space	10 GB	50 GB free space
Operating System	Windows7	Microsoft® Server 2008 R2 (64 bit) or above

### **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	Windows7	Microsoft® Server 2008 R2 (64 bit) or above

### **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	Windows7	Windows7 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



Hardware/Software	Minimum	Recommended
RAM	4 GB	8 GB
Network	100 Mbps	1 Gbps
Hard disk Space	10 GB free space	10 GB free space
Operating System	Windows7	Windows7 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	Windows7	Windows7 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	Microsoft® Server 2008 R2 (64 bit) 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	Microsoft® Server 2008 R2 (64 bit) 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
- Crystal Reports Runtime 13.0
- Microsoft Visual C++ 2015-2019 Redistributable - 14.24.28127
- Access DB Engine 14.0.6119.5000



*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.*

## 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 SAMAS>.



*For credential contact Matrix Channel Partners or Matrix Support Team at [Tech.Support@MatrixComSec.com](mailto:Tech.Support@MatrixComSec.com)*

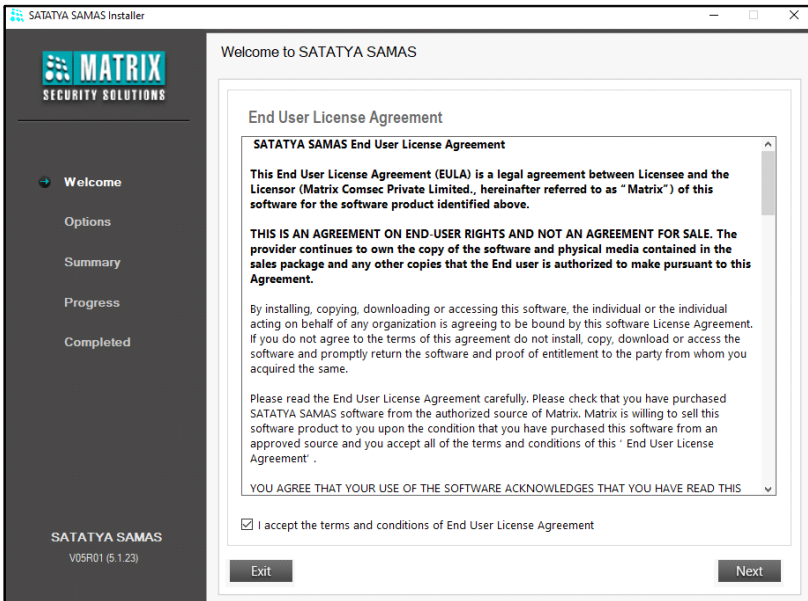
To start with the software installation, follow the steps given below:

1. Right click on **SATATYA \_SAMAS\_ Installer** and click **Run as administrator**.

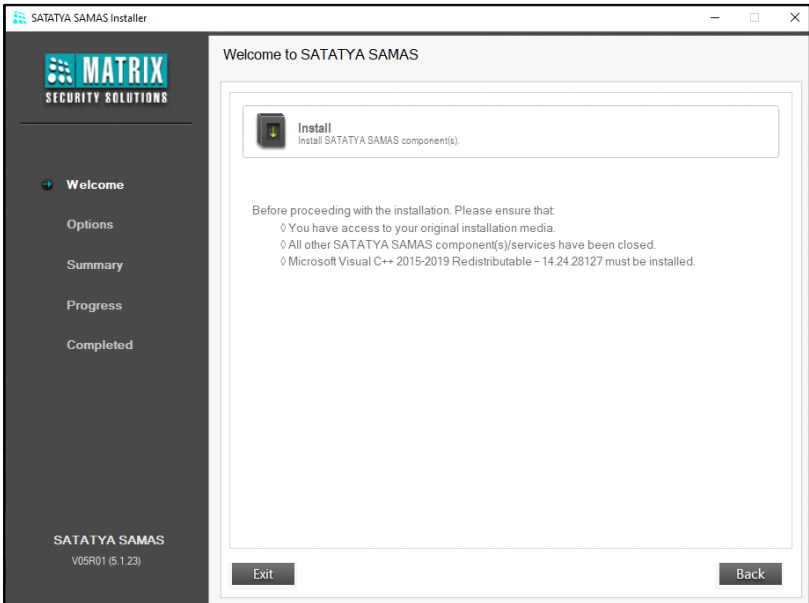
Name	Date modified	Type	Size
Help	17-Apr-18 6:29 PM	File folder	
Setup	17-Apr-18 6:29 PM	File folder	
F-R&D-SWD-09 ( Software Release to SWQA)_...	15-Dec-16 6:47 PM	Microsoft Word 9...	209 KB
SAMASInstallerNew	23-Nov-15 6:39 PM	XML Document	8 KB
SATATYA_SAMAS_Installer	29-Nov-16 11:50 A...	Application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

Administrator rights are required for installing the SATATYA setup.

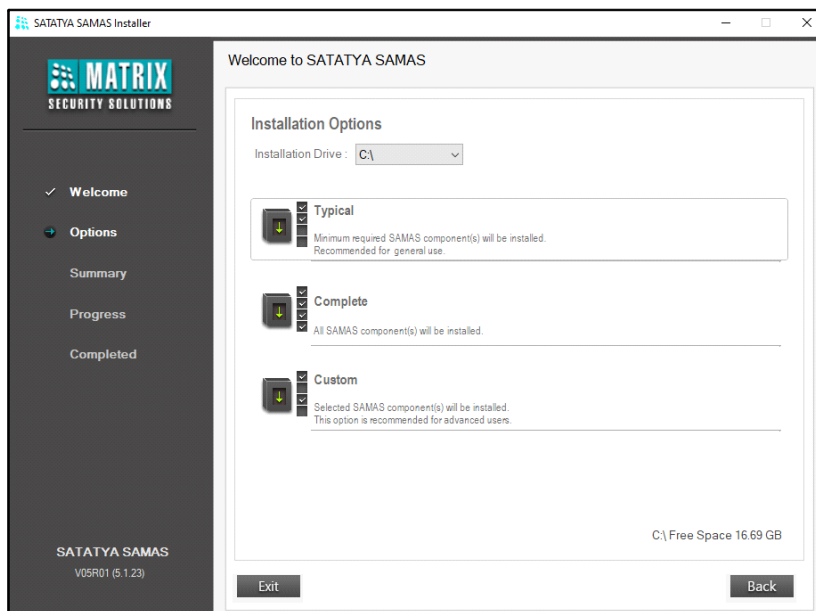
2. The **License Agreement** screen appears. Select the check box to accept the terms and conditions. Click **Next** to continue the installation process.



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



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

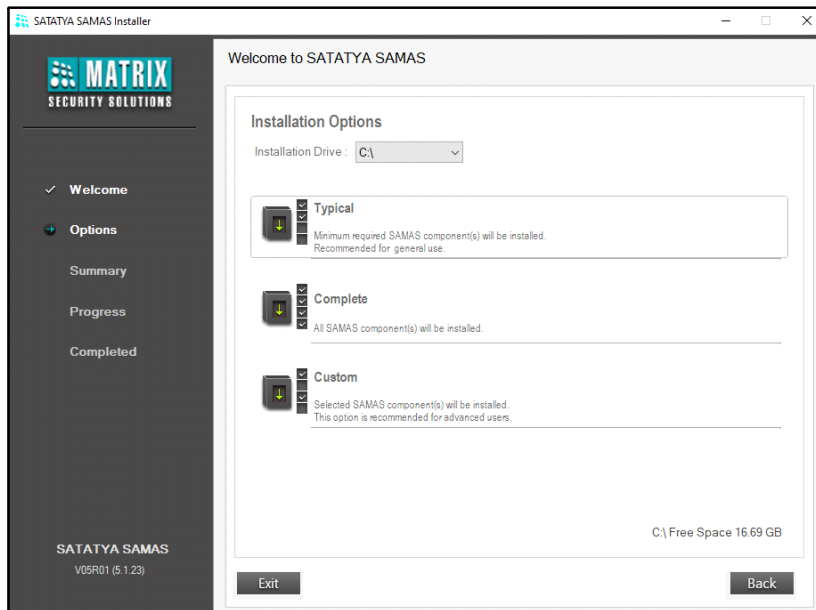


Choose the type of installation from the following options:

- **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”](#).

## Typical Installation

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



## Image Storage Drive

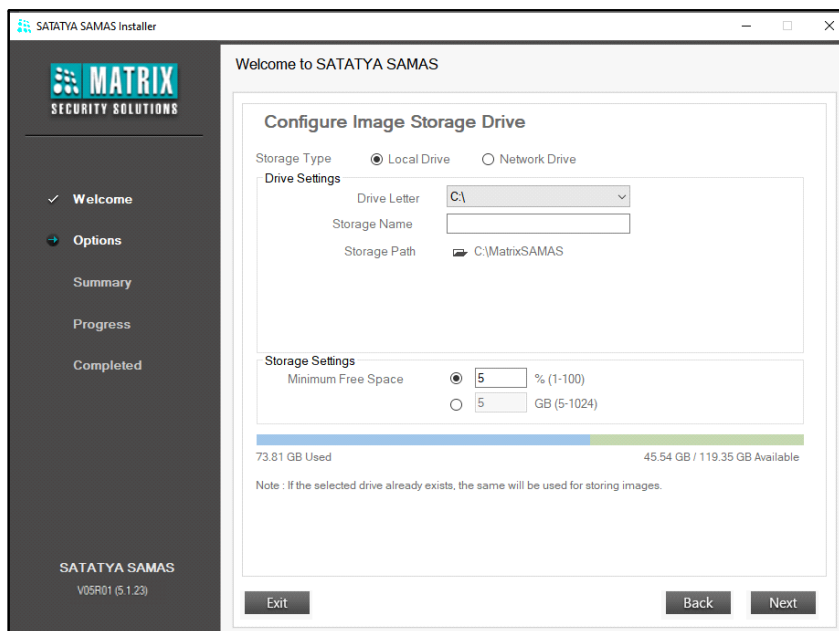
- You need to configure the Image Storage Drive as shown below.



*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. For Example: C:\
- Enter the desired **Storage Name**. For Example: Image Drive
- Browse to select the **Storage Path** (folder) in which the images will be stored.

- **Storage Settings**

- Select the desired option for **Minimum Free Space** — Percentage or GB. Enter the value which is to be maintained in the selected storage drive.

For Storage Type = Network Drive,

**SATATYA SAMAS Installer**

Welcome to SATATYA SAMAS

**Configure Image Storage Drive**

Storage Type ☐ Local Drive ☒ Network Drive

**Drive Settings**

Drive Letter

Storage Name

Storage Path

Username

Password

**Connect**

**Storage Settings**

Minimum Free Space ☒ 5 % (1-100)  
☐ 5 GB (5-1024)

Note : If the selected drive already exists, the same will be used for storing images.

**Exit** **Back** **Next**

### • **Drive Settings**

- Select the required **Drive Letter** of the Local Drive from the dropdown For Example: F:\
- Enter the desired **Storage Name**. For Example: Image Drive
- 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
- Provide the **Username** and **Password** of the computer/server to which the (network) drive belongs.

### • **Storage Settings**

- Select the desired option for **Minimum Free Space** — Percentage or GB. Enter the value which is to be maintained in the selected storage drive.

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

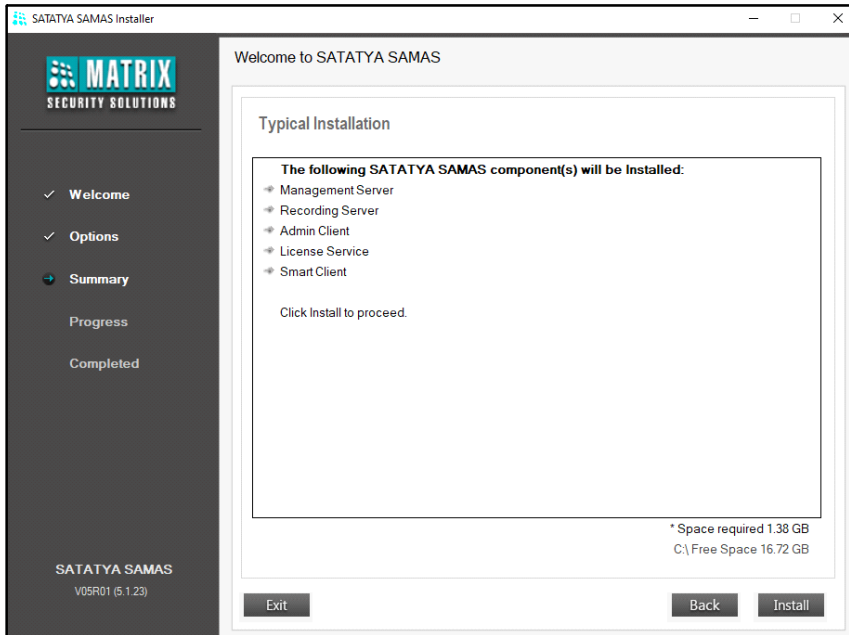
- Once the drive is connected successfully, click **Next** to proceed with the component installation.



*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.*



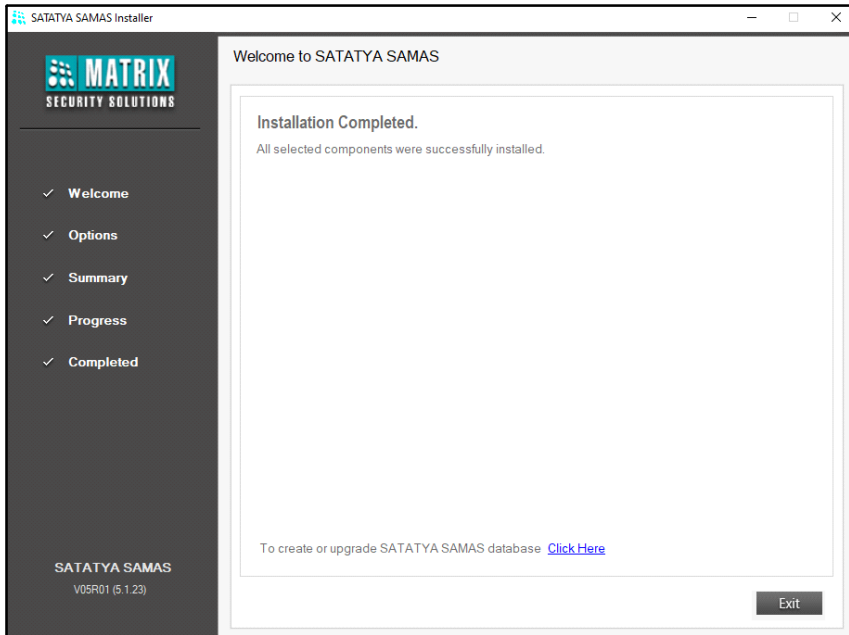
- The components to be installed will be listed as shown below. Click **Install**.



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

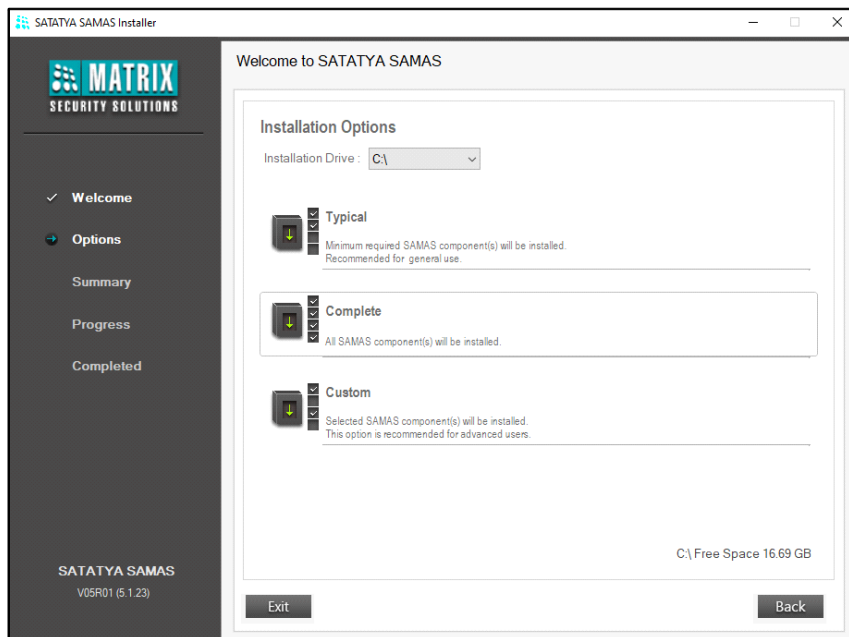
The system will start installing the SAMAS components.

- 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**.

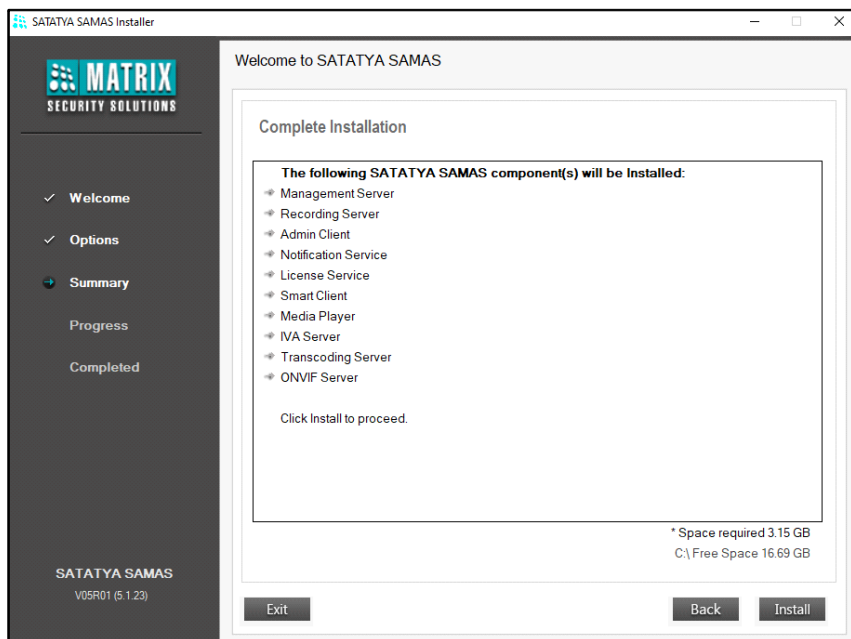


- Configure the Image Storage Drive. Refer [“Image Storage Drive”](#) for more information.
- Once the Storage Drive is configured, click **Next** to proceed further with the installation.



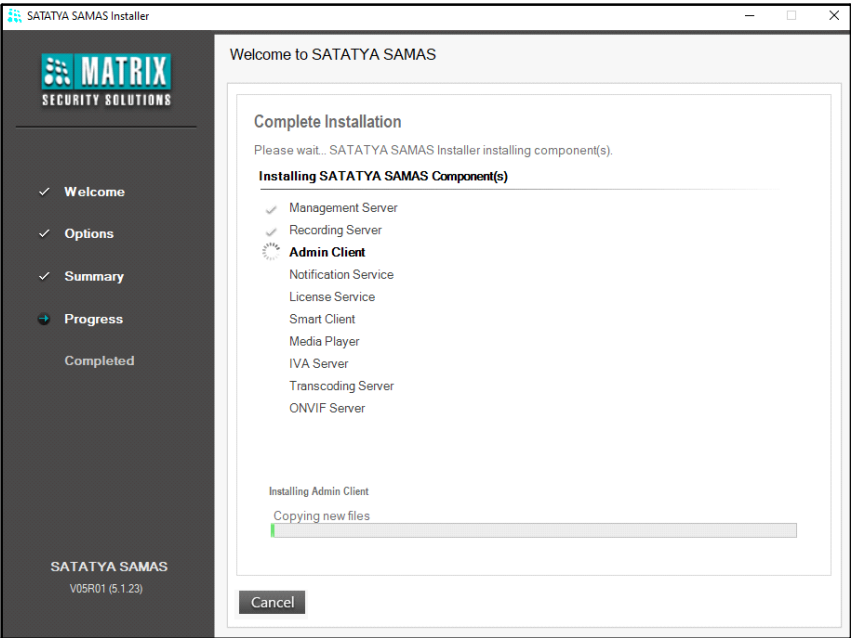
*In case you have installed any component before then, the list of the following will be displayed:*

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

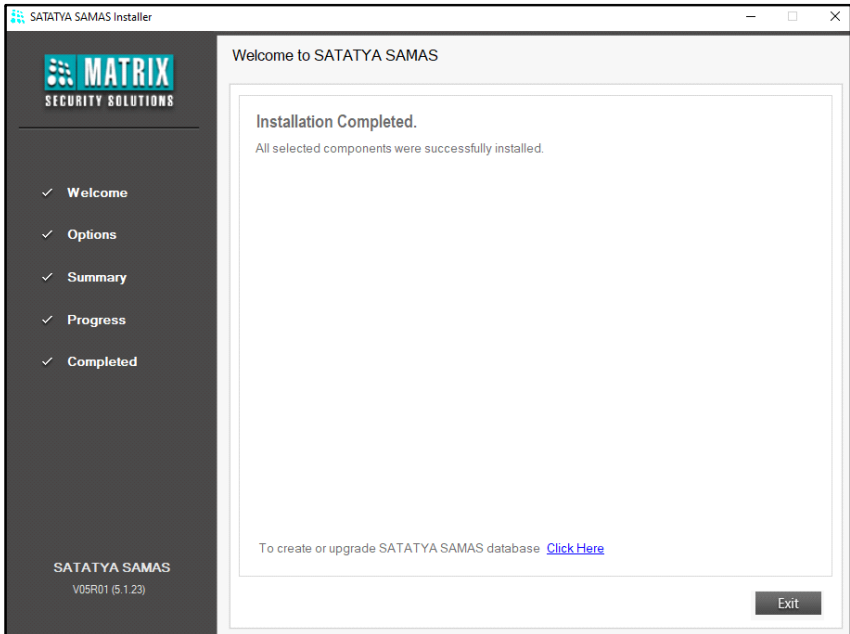


*For the Management Service and Notification Service to function, Microsoft SQL Express 2008 R2 SP2 is required.*

The system will start installing all the SAMAS components.

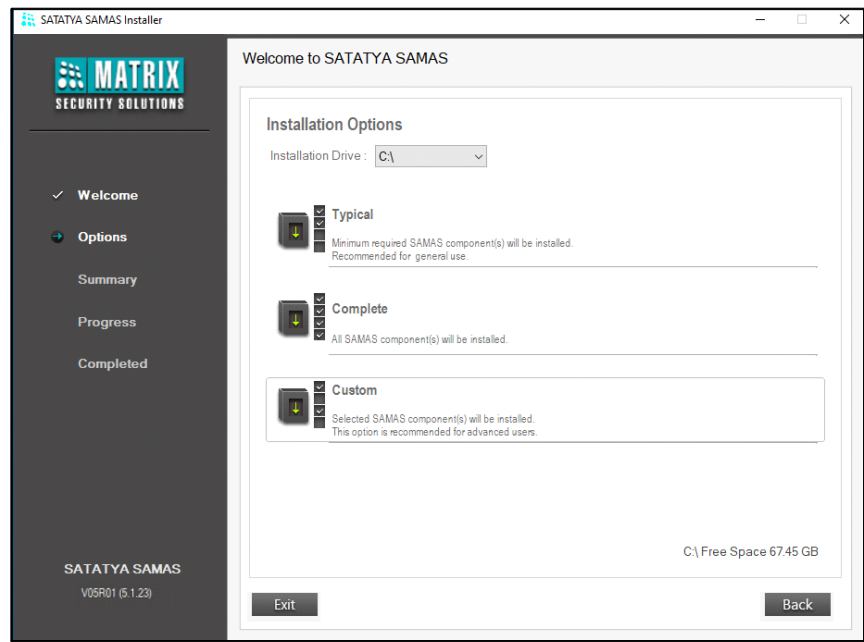


- Click **Exit** to exit from the installation window or click on the **Click Here** link to create, upgrade or take backup of the SATATYA SAMAS database. For more information, refer to “[Creating/Upgrading Database](#)”.

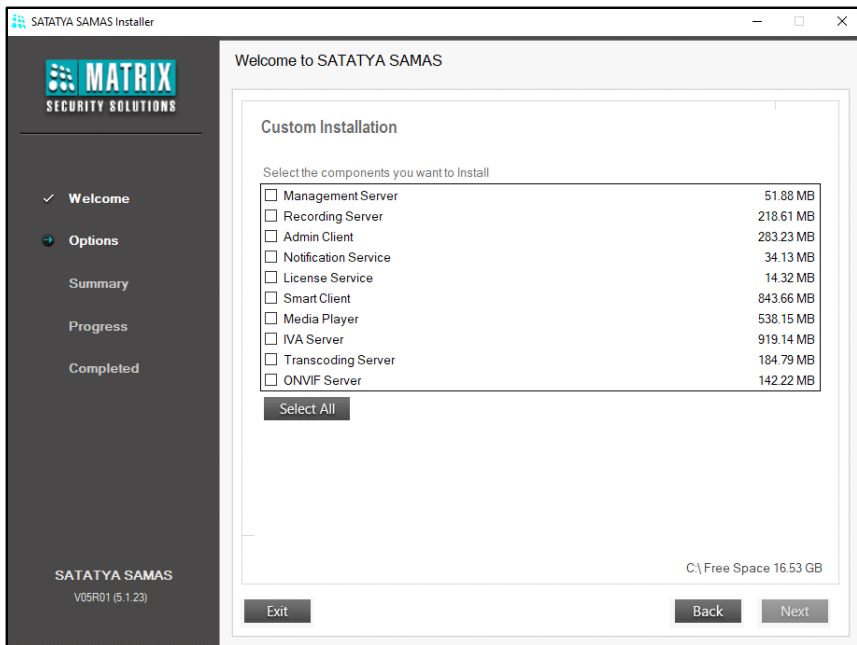


# Custom Installation

- 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.



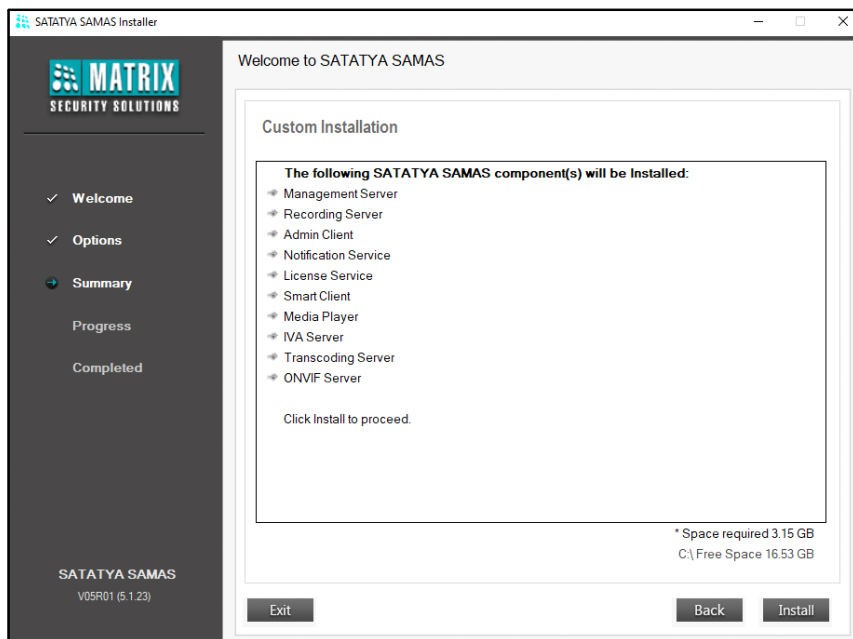
- If the 'Management Server' is selected in the list to be installed, the 'Image Storage Drive configuration' page appears. Refer "[Image Storage Drive](#)" for the detailed configuration.
- Once the Drive is configured, click **Next** to proceed further with the installation.



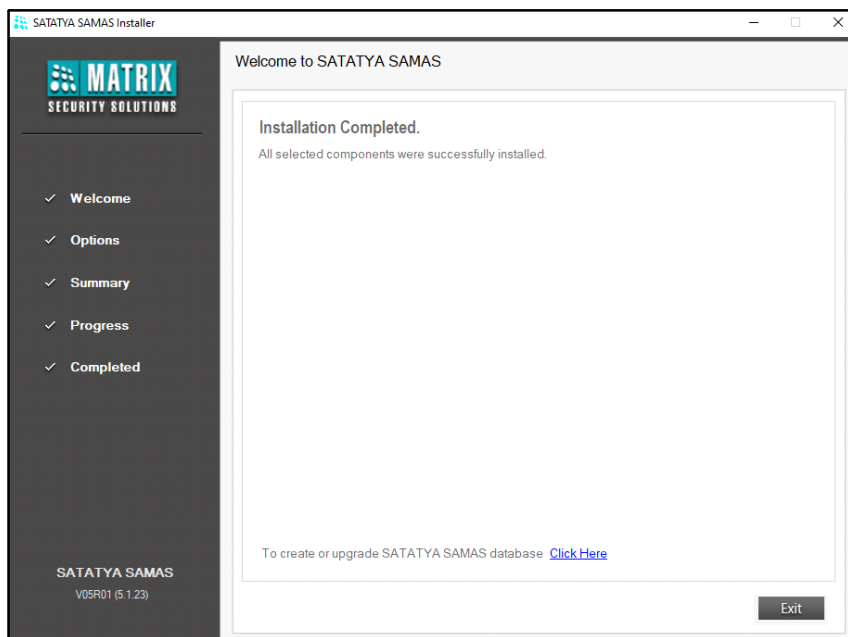
*In case you have installed any component before then, the list of the following will be displayed:*

- *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”](#).



## 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.

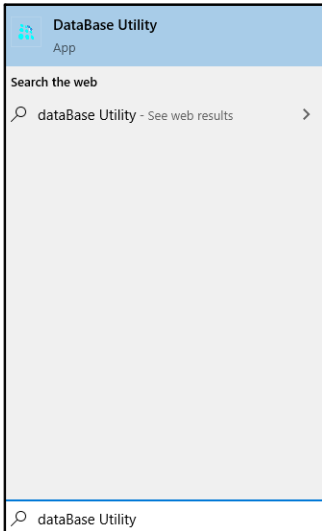
[“Creating/Upgrading Database”](#)

[“Taking Database Backup”](#)

### Creating/Upgrading Database

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

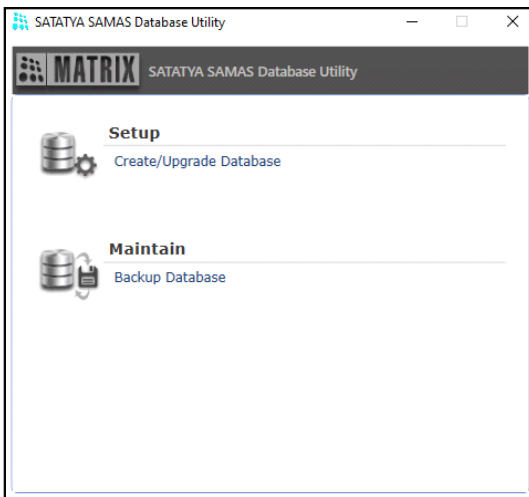
The DB Utility can be opened either by clicking on the **Click Here** link just after completion of the installation or click on your PC Search option and enter **Database Utility**. Click the same.



The SATATYA SAMAS Database Utility window appears.

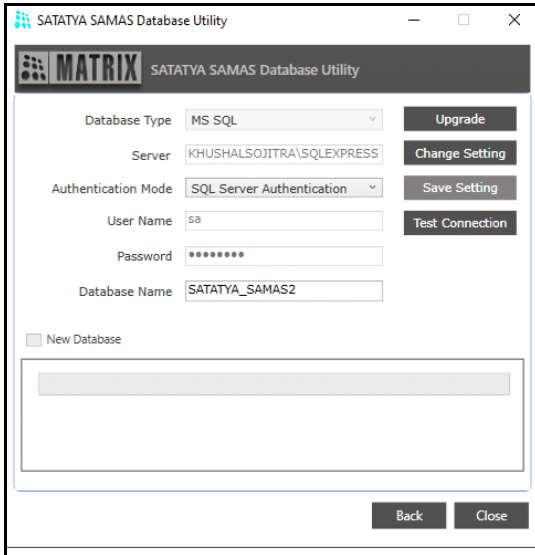


*Make sure you have MS SQL Server 2008 on which the SAMAS database can be created.*



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

The Database Utility Setup page appears. Click **Change Settings** 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.



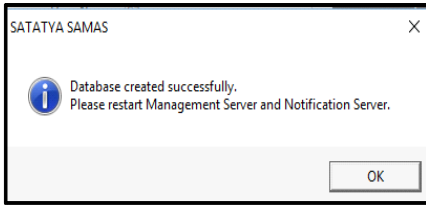
*The Server Name is the name/IP of the system where the MS SQL Server (DB Server) is installed.*

- **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.
- **Password:** Enter the Password of the SQL Server password.
- **Database Name:** Specify the Database Name of the SAMAS application. By default the application creates a database by the name of “SATATYA\_SAMAS”.

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



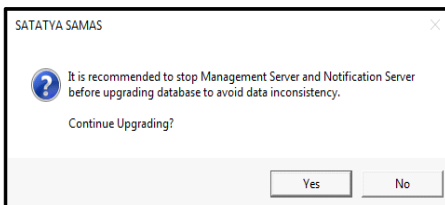
Click **Test Connection** to test the connection with the Database Server. The connection will be successful only if all the parameters have been configured correctly.

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.



## ***Taking Database Backup***

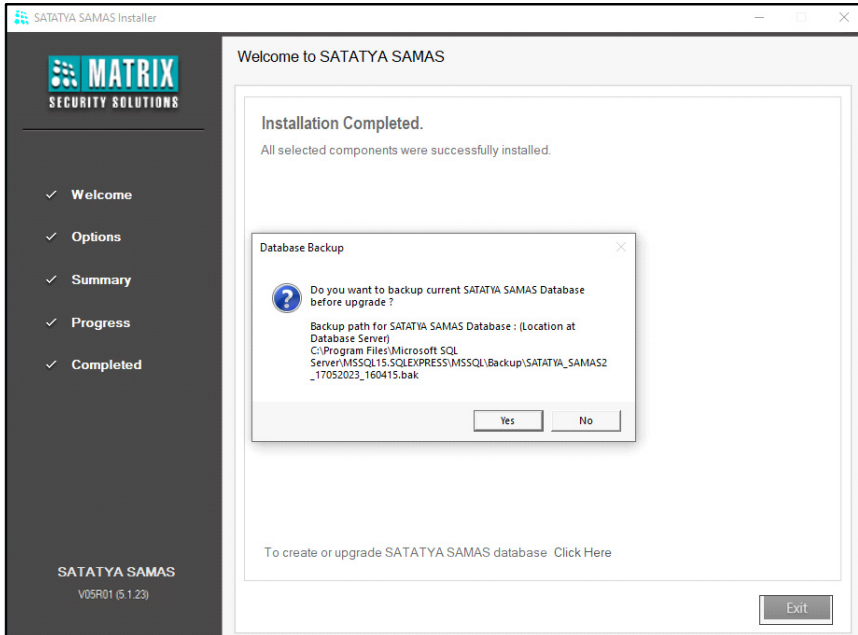
In the event of software or hardware problems, it is always a good idea to have a recent copy of your database files. The **Backup** option allows the Administrator to take the backup of the database at regular intervals.

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.

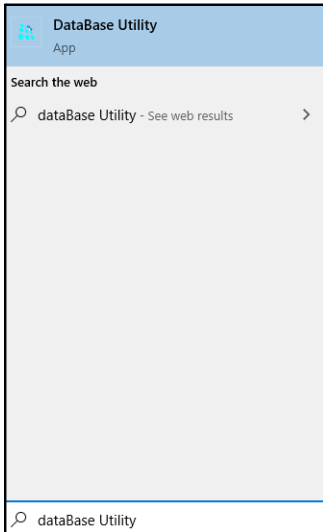


Click **Yes**, to take the Backup of the current database.

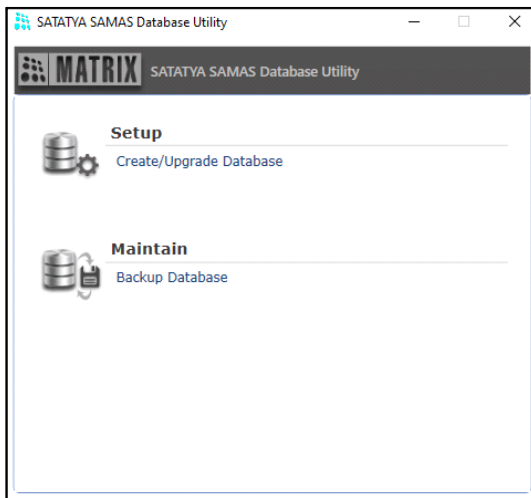
## Using Database Utility

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

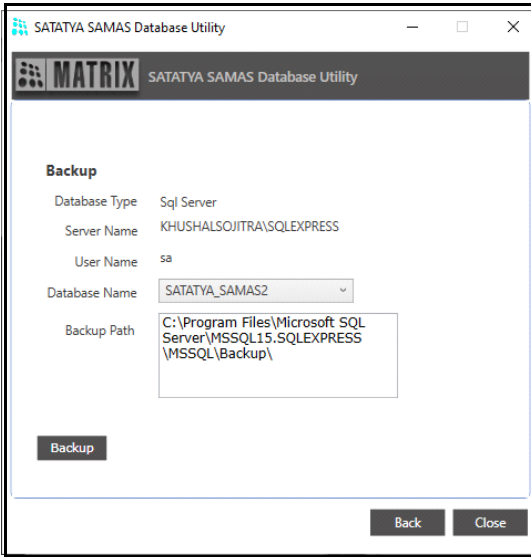
The Database Utility can be opened either by clicking on the **Click Here** link just after completion of the installation or click on your PC Search option and enter **Database Utility**. Click the same.



The SATATYA SAMAS Database Utility window appears.

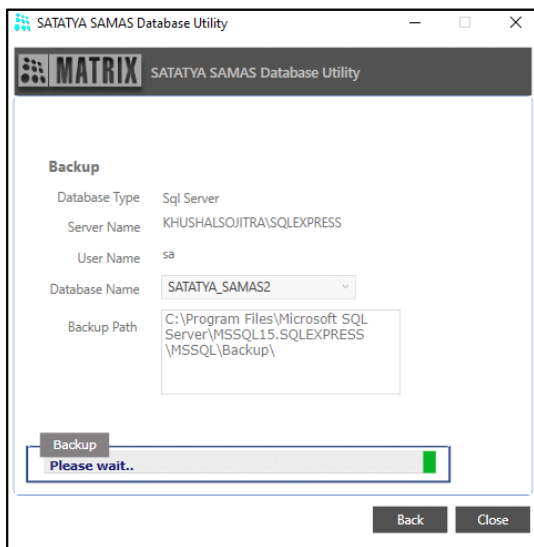


Click **Maintain** to take the backup of the database and the following window appears.

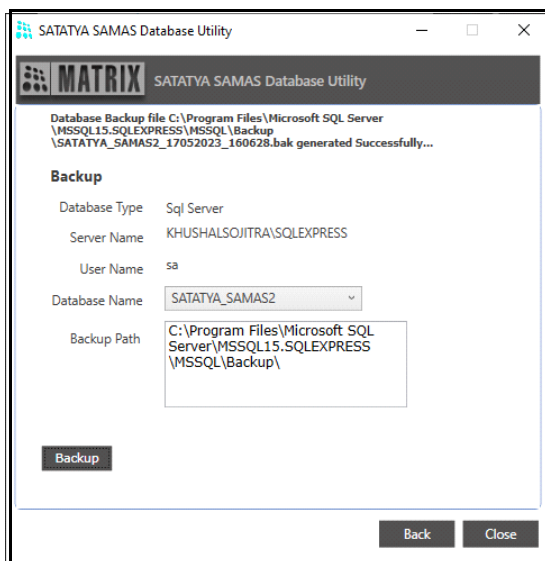


- Select the **Database Name** from the drop-down list.
- In **Backup Path**, the path of the backup file is displayed where the MS SQL has been installed. This path cannot be edited.
- Click **Backup**. The system will start the backup process.

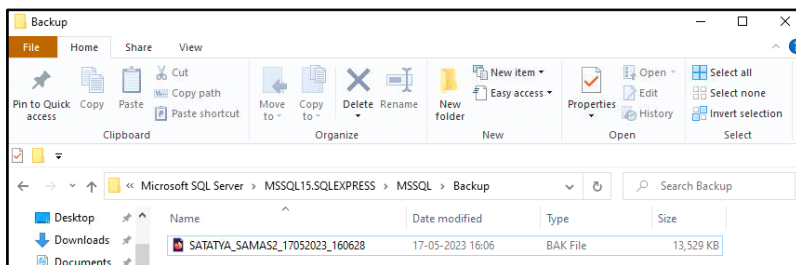




On successful completion of the process, the system displays the path as well as the name of the backup file.



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

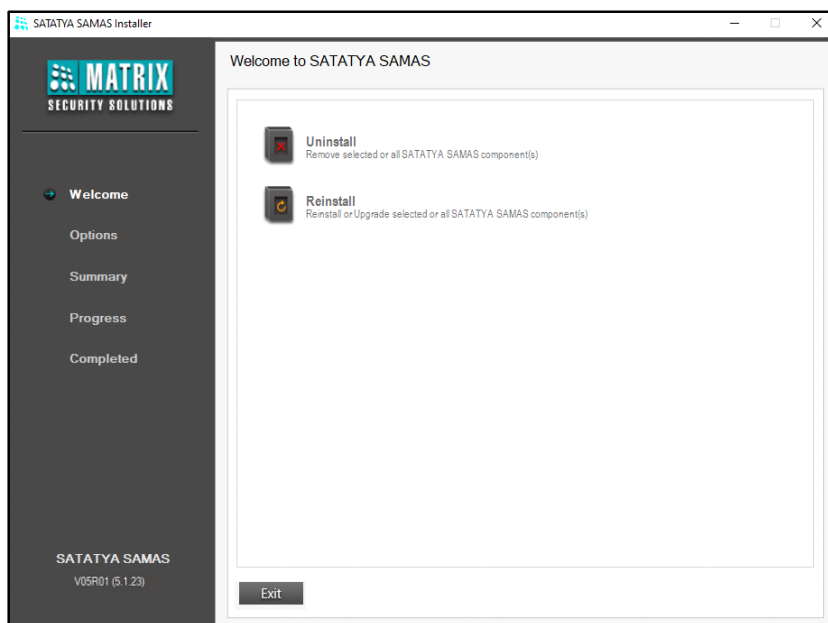


## Uninstallation and Reinstallation

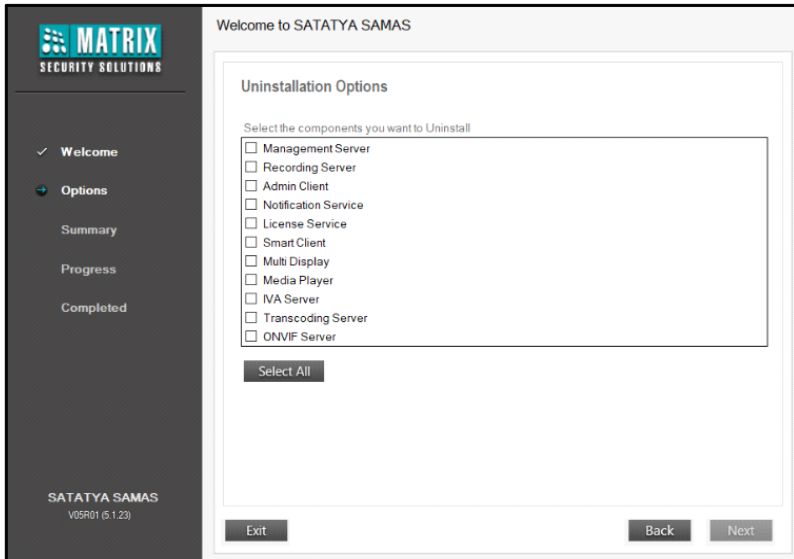
To Uninstall or Reinstall the SATATYA SAMAS components, click SATATYA\_SAMAS\_Installer. The setup window appears.



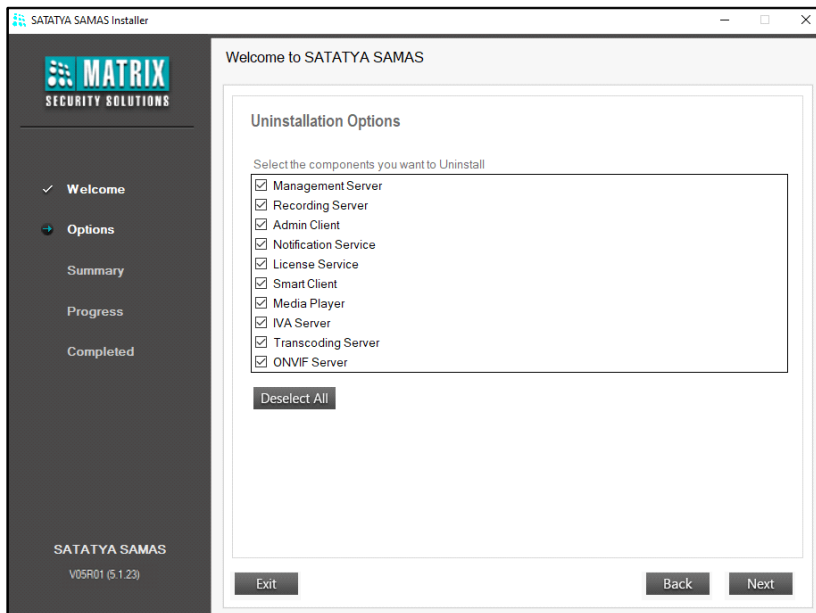
*For successful uninstallation or reinstallation of SATATYA SAMAS, it is recommended that all the services are stopped before performing these tasks.*



- 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

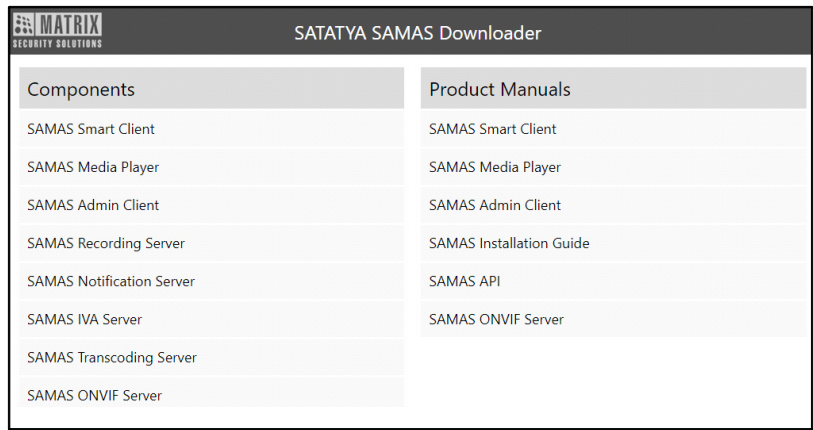
The SAMAS Downloader provides a simple solution for multi-site installations. It enables the users to download different components of SAMAS at diverse locations using a simple Web URL from any standard Web Browser.

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

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

(e.g., “`http://192.168.x.y:8711/downloader.html`”)

The SATATYA SAMAS Downloader appears.



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*.



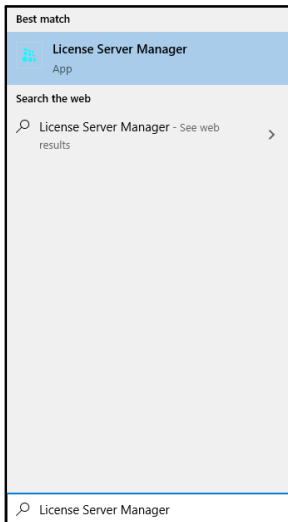
*The Management Server, License Server and Database must be in the same network.*

*Crystal Reports Runtime 13.0 which is required for report generation must be installed where Management Server is installed.*

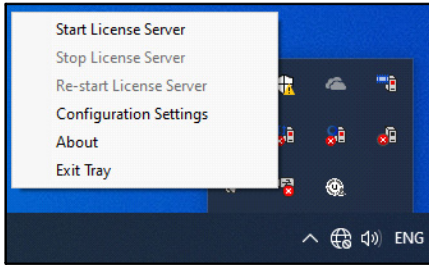
## Step-1: Configure License Server Settings using the License Server Manager Utility.

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

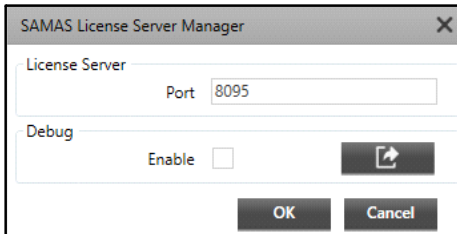
- Ensure that you have the License Dongle with you. The License Server and Dongle must be in the same PC. For Licensing details see [“Licensing of SATATYA SAMAS”](#).
- Click on your PC Search option and enter **License Server Manager**. Click the same.



- 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

- Specify the Listening **Port** on which License Server communicates with the Management Server.

## Debug

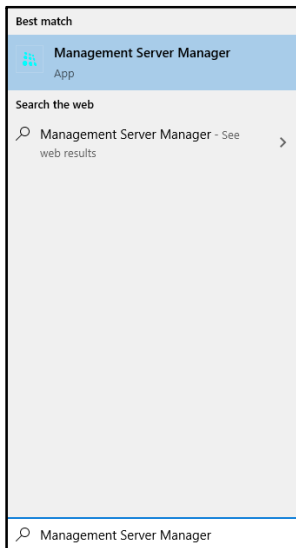
- Select the **Enable** check box to enable the debug. Click **Export Logs**  and specify the path of the local system where you wish to store the logs.
- Click **OK** to save the License Server Settings.

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

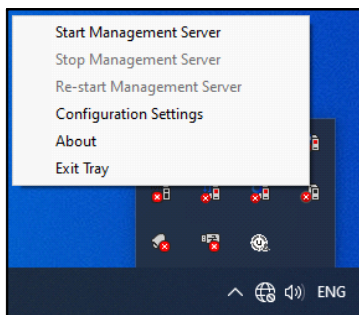
## Step-2: Configure Management Server Settings using the Management Server Manager Utility

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.

- 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.

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

Client	Server
Media Client (Smart Client)	Management Server
IVA Server	Management Server
Media Client (Smart Client)	Recording Server/ Failover Server
IVA Server	Recording Server/ Failover Server





*If Management Server is running on SSL Mode, then make sure all the other Servers and Clients are also configured to communicate on SSL Port of the Management Server for smooth functionality.*

## 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 two tabs: 'Non SSL' (selected) and 'SSL'. Under the 'Non SSL' tab, there are several port configuration fields: '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). Below these is the 'License Verification' section with a 'Select Mode' dropdown set to 'Service Based', an 'IP Address' field containing '127 . 0 . 0 . 1', and a 'Port' field containing '8095'. At the bottom is a 'Debug' section with an 'Enable' checkbox and a button with a refresh icon. 'OK' and 'Cancel' buttons are at the very bottom.

Port Name	Port Value
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

Select Mode: Service Based

IP Address: 127 . 0 . 0 . 1

Port: 8095


Debug: Enable ☐ [Refresh Icon]

OK Cancel

### License Verification

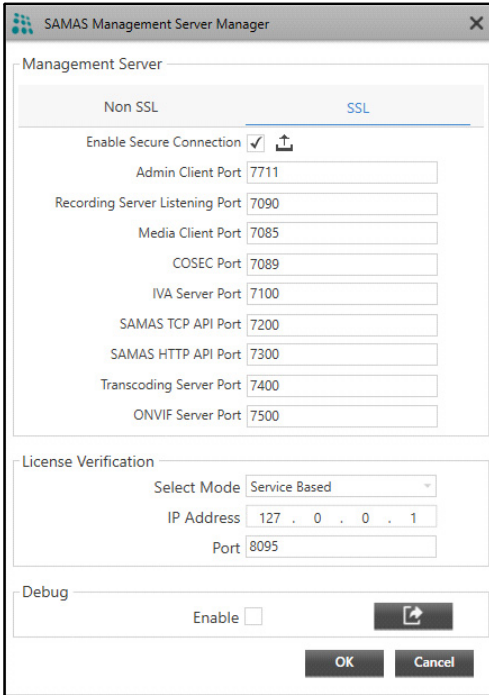
- **Select Mode:** License Verification Mode for Non SSL connection can only be **Service Based**, where the Licensed Dongle must be connected to the License Server machine.
- **IP Address:** Enter the IP Address of the License Server machine where the License Dongle is connected.
- **Port:** Specify the Listening Port on which License Server communicates with the Management Server.

## Debug


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.

## SSL Connection Configuration

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




The screenshot shows the 'SAMAS Management Server Manager' window with the 'SSL' tab selected. The 'Non SSL' tab is also visible. The 'SSL' tab contains the following settings:

- Enable Secure Connection:** ☒ 
- 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


The 'License Verification' section contains:

- Select Mode:** Service Based
- IP Address:** 127 . 0 . 0 . 1
- Port:** 8095

The 'Debug' section contains:

- Enable:** ☐ 

At the bottom are 'OK' and 'Cancel' buttons.

- Select the **Enable Secure Connection** check box and click **Upload**  to upload the SSL Certificate as well as configure the SSL Settings.

For details, refer to “[SSL Settings](#)”.

## License Verification

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

## 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 Address:** Enter the IP address of the License Server machine where the License Dongle is connected.
- **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.



*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:

License Verification

Select Mode: Device Based

Port: 15025

MAC Address: [disabled field]

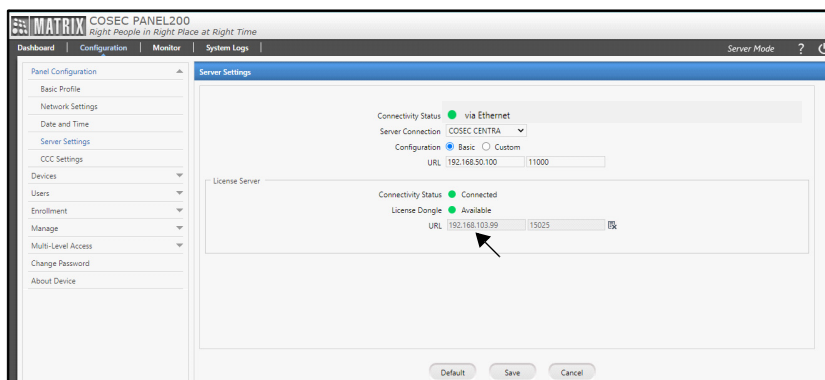
- **Port:** Enter the Port number of the COSEC Device through which the License Dongle will communicate with the Management Server.
- **MAC Address:** It is a non-editable field which displays the MAC address of the COSEC Device. It will appear once the License Dongle is linked with the IP Address of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

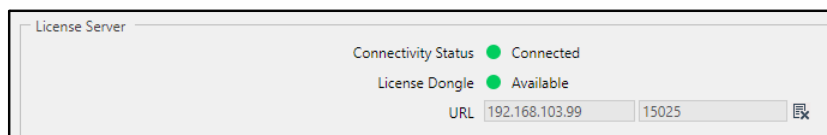
For the configuration, access your COSEC Device web page using the browser and login using the credentials.

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



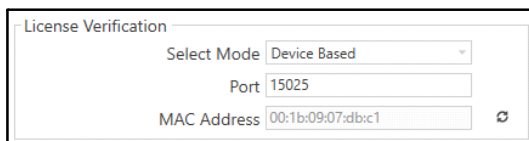
- Under the License Server section, enter the IP Address of the Management Server in the **URL** field.
- Enter the Port Number of the COSEC Device (beside the IP Address entered) through which the License Dongle will communicate with the Management Server. For example: 65535.

Valid Port Number range is 1024 to 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

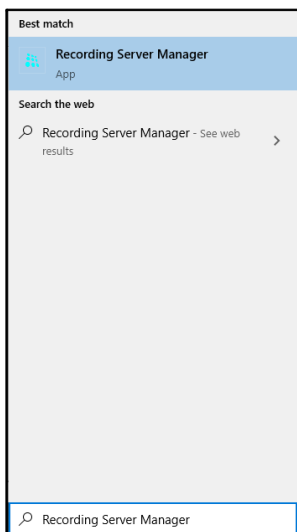
Select the **Enable** check box to enable debug. Click **Export Logs**  and specify the path of the local system where you wish to store the logs.

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

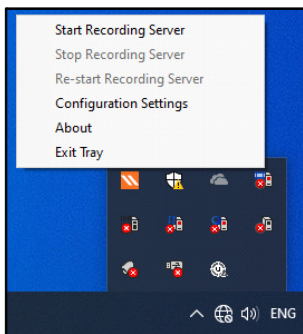
## Step-3: Configure Recording Server settings using the Recording Server Manager Utility.

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.

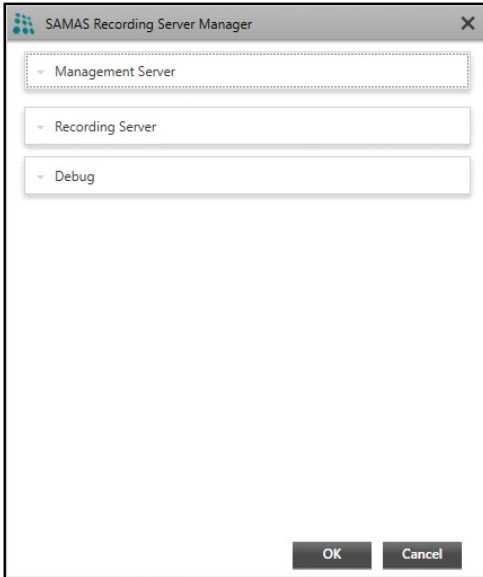
- Click on your PC Search option and enter **Recording Server Manager**. Click the same.



- 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”](#)

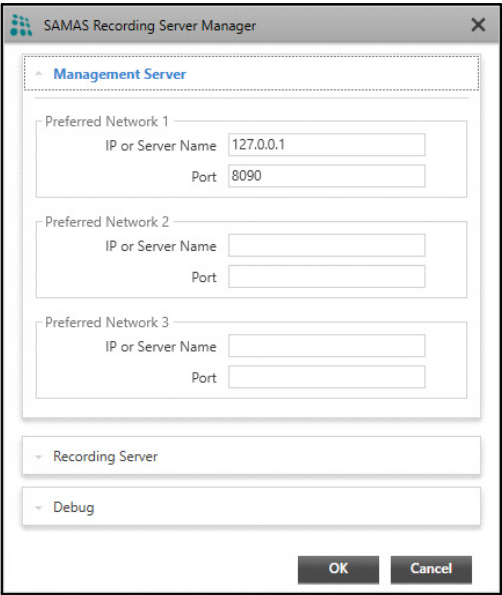
[“Recording Server”](#)

[“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:

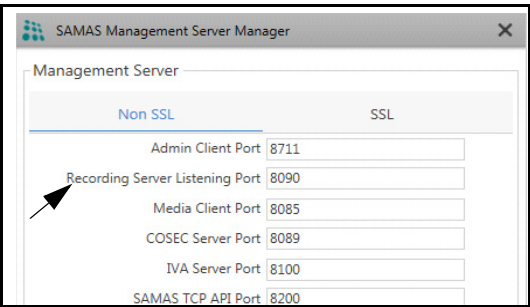


Under **Preferred Network 1 (PN1)** configure the following:

- **IP Address or Server Name:** Enter either the Private or Public IP Address of the Management Server or enter the Host Name, Domain Name or Server Name of ISP.
- **Port:** Enter either the Private or Public Port.

**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.*

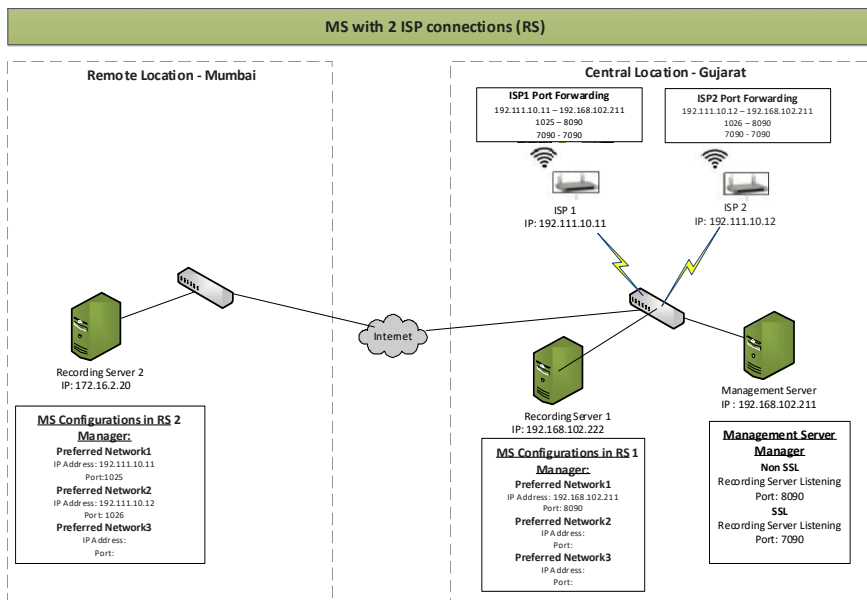
- If Public Networks, ISP1 and ISP2 are configured in PN1 and PN2 respectively.
- Now as the RS and MS are located in two different networks, the connection between them will be established via ISP1 (PN1) first. If due to some network issue, the connection is lost between RS and MS via ISP1 (PN1), then 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:**

If an organization has multiple branches. The main branch is located at the 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.
- **Auto Add Device Port:** Specify the **Auto Add Device Port** to communicate with SATATYA Devices like NVR/NVRX series and automatically add the devices to SAMAS.

Recording Server (RS)/Failover Server (FoS) will listen to Auto Addition Device request on this port.

- **Auto Detect IP Address:** If the **Auto Detect IP Address** check box is selected then IP 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 the Auto Detect IP Address check box is cleared then you need to specify the **IP Address** and **Port** of the Recording Server.

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

- **IP Address or Server Name:** Enter either Private or Public IP Address of the Recording Server. You can also enter the Host Name, Domain Name or Server Name of ISP1/2.
- **Port:** Enter either Private or Public Port on which RS/FoS will listen to client requests.

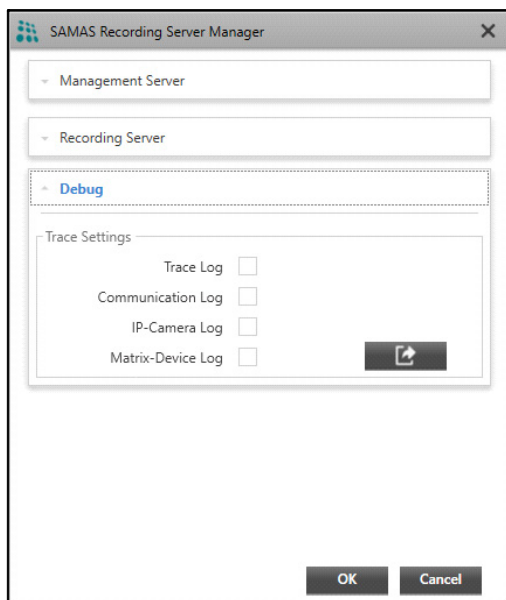
For Private Network, enter the Recording Server Port.


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



- 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.

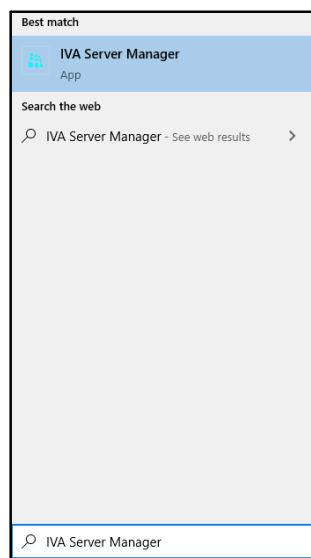
**Step-4: Configure IVA Server settings using the IVA Server Manager Utility.**

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

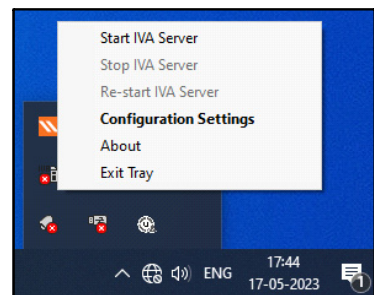
To use IVA features a connection between the Management Server (MS) and IVA Server must be established.

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.

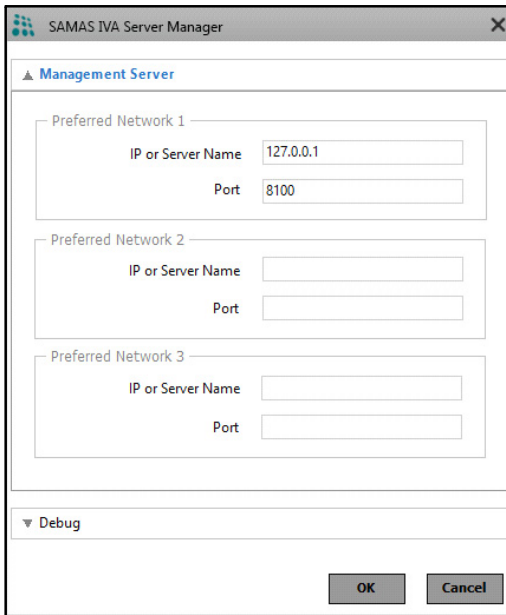
- Click on your PC Search option and enter **IVA Server Manager**. Click the same.



- 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.



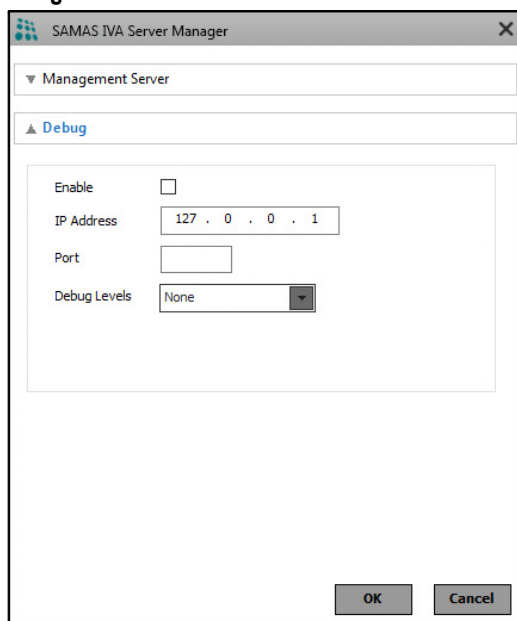
The screenshot shows the 'SAMAS IVA Server Manager' window. It has a title bar with a close button. Below the title bar is a section titled 'Management Server' with a collapse icon. This section contains three 'Preferred Network' configurations. 'Preferred Network 1' has 'IP or Server Name' set to '127.0.0.1' and 'Port' set to '8100'. 'Preferred Network 2' and 'Preferred Network 3' have empty input fields for both 'IP or Server Name' and 'Port'. Below these is a 'Debug' section with a collapse icon. At the bottom right are 'OK' and 'Cancel' buttons.

- Enter the **IP Address** and **Port** of the Management Server on which IVA Server will communicate. You can specify three Preferred Networks.

You can configure the Preferred Network 1 and 2 as public network via ISPs while Preferred Network 3 as private network.

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 tree view on the left with "Management Server" expanded and "Debug" selected. The "Debug" section contains a configuration area with the following fields:

- Enable:** A checkbox that is currently unchecked.
- IP Address:** A text box containing "127 . 0 . 0 . 1".
- Port:** An empty text box.
- Debug Levels:** A dropdown menu currently set to "None".

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

- **Enable:** Select the check box to enable the debug.
- **IP Address:** Specify the IP address of the Syslog Server.
- **Port:** Specify the port of the Syslog Server.
- **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.

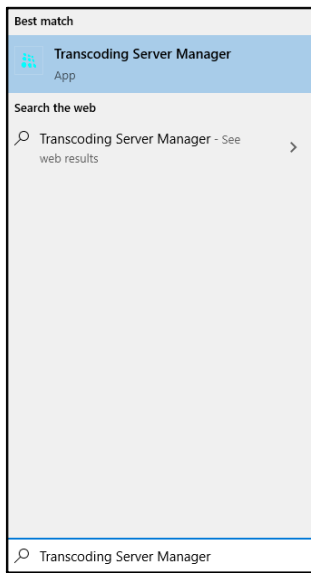
## Step-5: Configure Transcoding Server settings using the Transcoding Server Manager Utility.

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.

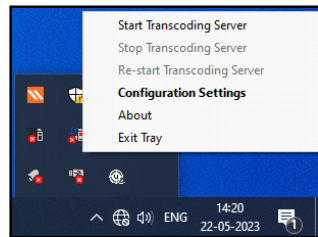
To use Transcoding features, connection between Management Server (MS), Recording Server and Transcoding Server must be established.

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.

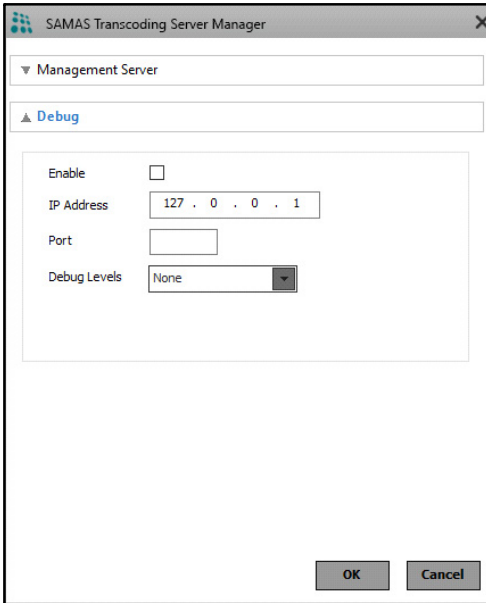
The screenshot shows the 'SAMAS Transcoding Server Manager' window. It features a 'Management Server' section with three 'Preferred Network' configurations. The first network is pre-filled with IP '127.0.0.1' and port '8400'. The other two networks are empty. A 'Debug' section is at the bottom, and 'OK' and 'Cancel' buttons are at the very bottom.

- Enter the **IP Address** of the Management Server and **Port** (this is the port configured in the Management Server for Transcoding Server) on which Transcoding Server will communicate. You can specify three Preferred Networks.

Configure the Preferred Network 1, 2 and 3 as per your installation scenario.

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 the 'SAMAS Transcoding Server Manager' window. It has a 'Management Server' tab and a 'Debug' tab. The 'Debug' tab is active, showing a configuration area with the following fields:

- Enable:** A checkbox that is currently unchecked.
- IP Address:** A text field containing '127 . 0 . 0 . 1'.
- Port:** An empty text field.
- Debug Levels:** A dropdown menu currently set to 'None'.

At the bottom right of the window are 'OK' and 'Cancel' buttons.

- **Enable:** Select the check box to enable the debug.
- **IP Address:** Specify the IP address of the Syslog Server.
- **Port:** Specify the port of the Syslog Server.
- **Debug Levels:** Select the desired level of debug — None, Information Logs or Detailed Logs.
- Click **OK** to save the configurations.

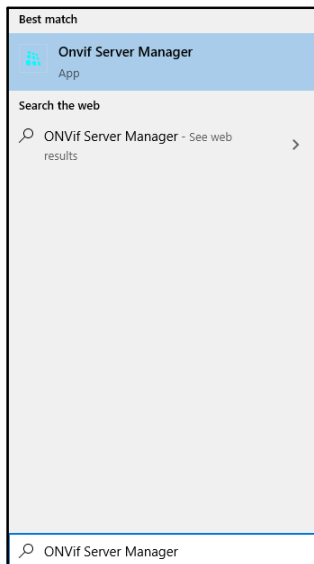
Now from the Tray, right-click on the **Transcoding Server** icon again and select **Start Transcoding Server** to start the service.

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

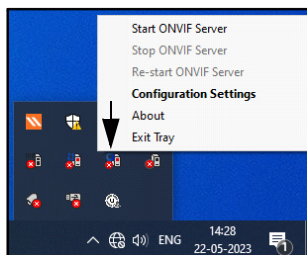
The ONVIF Server acts as a bridge between SAMAS and 3rd Party ONVIF Clients as well as RTSP Clients. This enables easy exchange of video data as well as availability of Live / Playback streams.

The ONVIF Server plays a dual role:

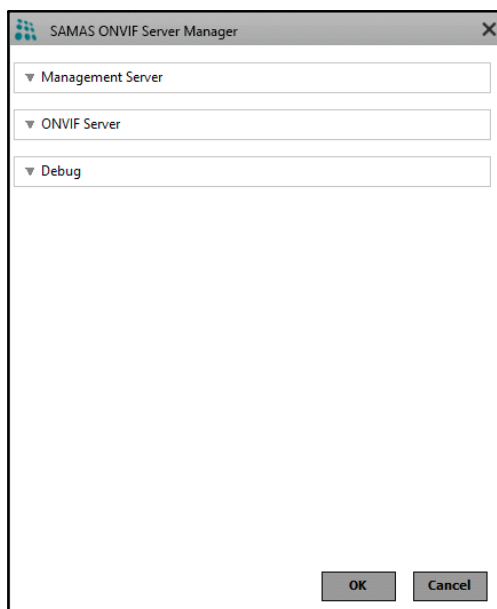
- acts as a Client for the Management Server/Recording Server
  - acts as a Server for the 3rd Party ONVIF Clients
- Click on your PC Search option and enter **ONVIF Server Manager**. Click the same.



- 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.

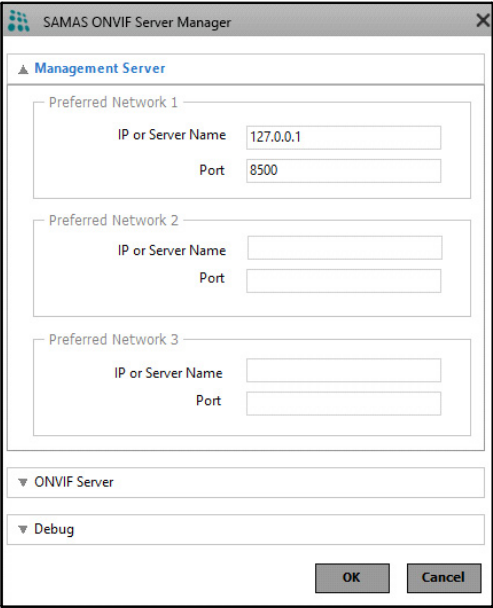
- [“Management Server”](#)
- [“ONVIF Server”](#)
- [“Debug”](#)

## 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' panel is expanded, showing three sections for Preferred Network 1, Preferred Network 2, and Preferred Network 3. Each section has input fields for 'IP or Server Name' and 'Port'. In the Preferred Network 1 section, 'IP or Server Name' is set to '127.0.0.1' and 'Port' is set to '8500'. Below these sections are two collapsed panels: 'ONVIF Server' and 'Debug'. At the bottom right are 'OK' and 'Cancel' buttons.

- **IP Address or Server Name:** Enter either Private or Public IP Address of Management Server. You can also enter Host Name, Domain Name or Server Name of ISP1 and ISP2.
- **Port:** Enter either Private or Public Port.



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

## ONVIF Server

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

The screenshot shows the SAMAS ONVIF Server Manager configuration window. The 'ONVIF Server' section is expanded, showing the following settings:

- WS-Discovery: ☐
- ONVIF Port: 580
- RTSP Port: 554
- RTP Port: 5004
- Multicast Settings:
  - Enable: ☐
  - Start IP Address: 224.0.0.1
  - End IP Address: 225.0.0.1
  - Start Port: 5000
  - End Port: 6000
  - TTL: 1

At the bottom, there is a 'Debug' section and 'OK' and 'Cancel' buttons.

- **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.
- **ONVIF Port:** Enter the ONVIF Port on which the ONVIF Client will send requests for video streams to the ONVIF Server.
- **RTSP Port:** Enter the RTSP Port. RTSP Clients will send the RTSP requests to ONVIF Server on this port.
- **RTP Port:** Enter the RTP Port to deliver audio and video over the Internet. This is the start port of RTP Port range.
- **Multicast Settings**

Multicasting helps optimize the network bandwidth consumption between the ONVIF Server and ONVIF Clients.

- **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 IP Address that is to be used for Multicasting. The Multicasting communication will be done within this range. IP 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 IP Addresses can be used.
- **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.
- **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.

## Debug

The screenshot shows the 'SAMAS ONVIF Server Manager' window. The 'Debug' section is expanded, revealing a configuration area with the following elements:

- Enable:** An unchecked checkbox.
- IP Address:** A text input field containing '127 . 0 . 0 . 1'.
- Port:** An empty text input field.
- Debug Levels:** A dropdown menu currently set to 'Information Logs'.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

- **Enable:** Select the check box to enable the debug.
- **IP Address:** Specify the IP Address of the Syslog Server.
- **Port:** Specify the port of the Syslog Server.

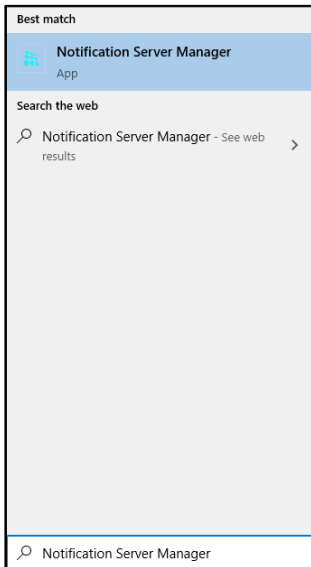
- **Debug Levels:** Select the desired level of debug — None, Information Logs or Detailed Logs.
- Click **OK** to save settings.

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

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

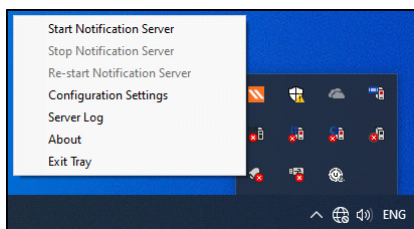
The E-mail and SMS Notification Server is responsible for configuration of Mail Server and SMS Service provider to send E-mail and SMS Notifications to the User.

- 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.
- Then click **Login**.



*Make sure the user has the configuration rights of Email and SMS Settings in System Accounts of Admin Client.*

The following window appears.

## Email Settings

For the Email Settings, configure the following parameters:

**SMTP Server:** Specify the IP Address or Name of the configured SMTP Server.

**SMTP Port Number:** Specify the TCP port for the SMTP service as set in the SMTP Server.

**Sender Email Id:** Enter the sender's Email ID.

**Sender Display Name:** Enter the User Name that will be displayed in the Emails.

**User Name:** Specify the User Name as set in the Email account.

**Password:** Specify the Password as set in the Email account.



*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.

**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.

**Active Days:** Specify the number of days the system needs to keep the unsent messages active in the event of the service being stopped.

**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.

**Email Id:** Enter the Email ID to check the connectivity and click **Send**.

Click **Apply** to save the settings.

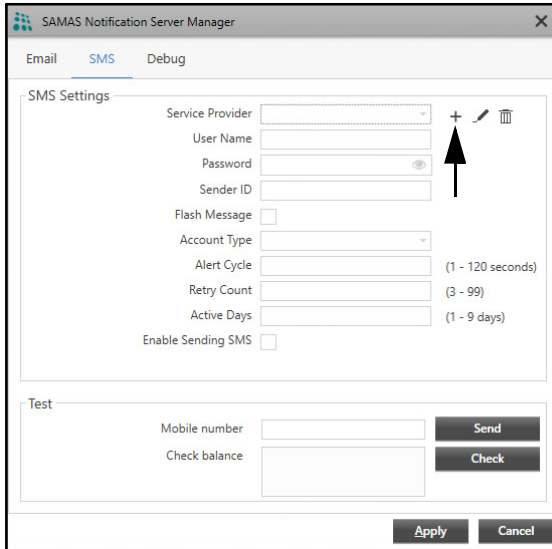
## SMS Settings

For the SMS settings, select **Custom** as the Service Provider.

## Custom Service Provider Settings

You can add a Service Provider other than the ones provided by default. To do so,

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



Specify the API configuration parameters for the new Service Provider:

### Request

**Service Provider Name:** This is the Service Provider's Name.

**Service Provider URL:** This is the Service Provider's Website used for registration etc. For example [www.smsgatewaycentre.com](http://www.smsgatewaycentre.com).

**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](http://smsgatewaycentre.com/library/send_sms_2.php)

**API Argument:** Enter the argument required to be mentioned while constructing the URL. For example "User", "Password" etc.

**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 save the new argument and value.

The screenshot shows a 'Custom Service Provider' dialog box with a close button (X) in the top right corner. It is divided into three main sections: 'Request', 'API Argument', and 'Balance'.  
The 'Request' section contains fields for 'Service Provider Name', 'Service Provider URL', 'Base URL', 'API Argument', 'Argument Value' (with a dropdown menu showing 'User Name'), and 'Custom'. Below these fields are 'Add Argument' and 'Cancel' buttons.  
The 'API Argument' section features a table with three columns: 'API Argument', 'Argument Value', and 'Delete'. The table is currently empty.  
Below the table are fields for 'Argument Separator', 'Request Method' (a dropdown menu showing 'POST'), and 'Request Preview'.  
The 'Balance' section at the bottom has a 'Balance Check' checkbox and a 'Balance URL' field. At the very bottom of the dialog are 'Apply' and 'Cancel' buttons.

**Argument Separator:** Define a character that can be used as a valid separator between arguments used to construct the API URL. For example “&”.

**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 the Balance URL to be displayed.

**Balance URL:** Displays the URL, which can be edited, if required.

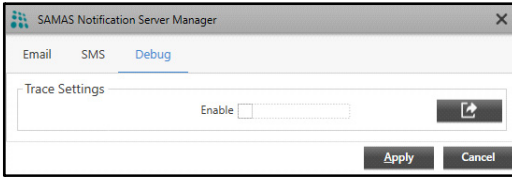
## Response


**API Response:** Define the response or error codes. Maximum 99 responses can be configured.

**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.

## Debug



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.

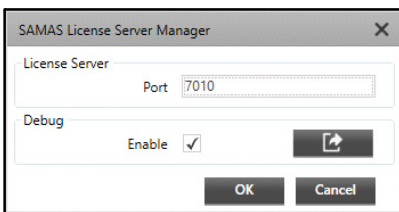
Now from the Tray, right-click on the **Notification Server** icon again and select **Start Notification Server** to start the service.

## 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

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

Select Mode

Service Based

IP Address

192 . 168 . 104 . 20


Port

7010

Debug

Enable

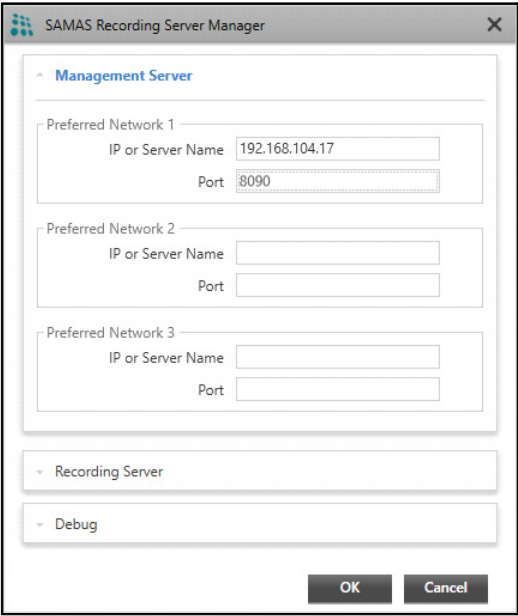
☐




OK

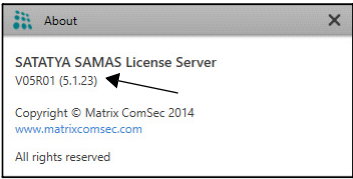
Cancel

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.



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.*



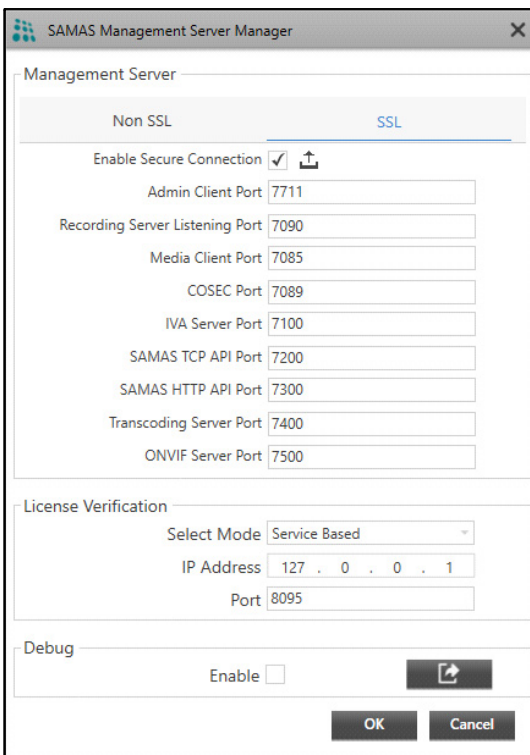


# SSL Settings

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.


Thus, 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 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 checkbox 'Enable Secure Connection' which is checked. Below it are several text input fields for ports: '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 a 'License Verification' section with a 'Select Mode' dropdown set to 'Service Based', an 'IP Address' field with '127 . 0 . 0 . 1', and a 'Port' field with '8095'. At the bottom is a 'Debug' section with an 'Enable' checkbox and a button. 'OK' and 'Cancel' buttons are at the very bottom.



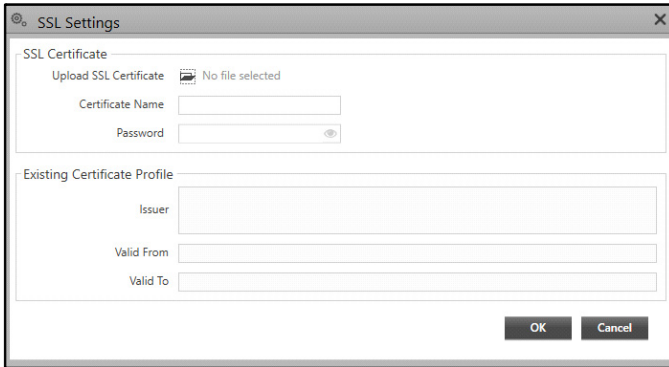
*For SSL, make sure the certificate is uploaded.*

Select the **Enable Secure Connection** check box. Click **Upload** , the **SSL Settings** window appears. Upload the SSL Certificate as well as Configure the SSL parameters for secure communications.




*After the SSL Certificate is uploaded from SSL Settings, the name of the certificate appear besides the Upload icon.*

## SSL Settings



## 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 only.



*The **Upload SSL Certificate** option will be visible only when no SSL Certificate is uploaded.*

- **Certificate Name:** Specify the Certificate Name used internally during certificate configurations. Maximum 30 characters.
- **Password:** Enter Password for accessing the certificate. Maximum 30 characters.

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.

# 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:

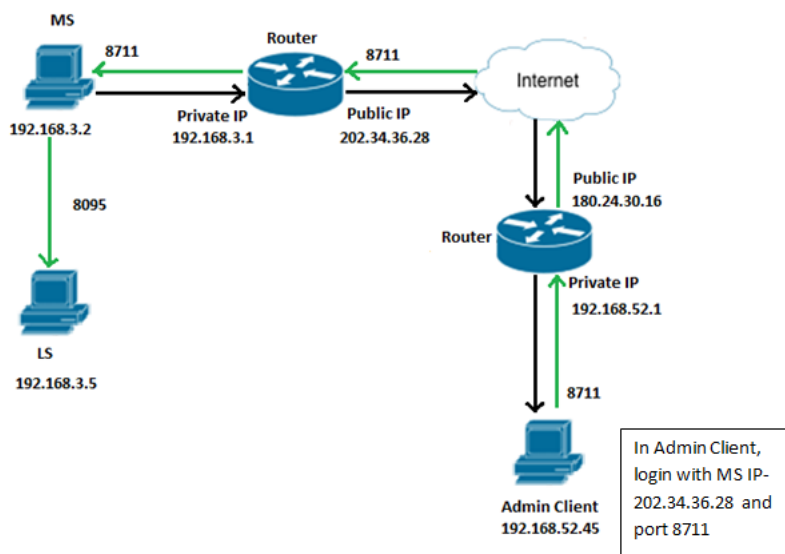
- MS + LS +NS are at Mumbai in public network.
- Recording Server is in Vadodara Matrix HO- PC1
- IVA Server is in Vadodara Matrix HO-PC2
- Failover Server is in Vadodara Matrix HO- PC3

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

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.

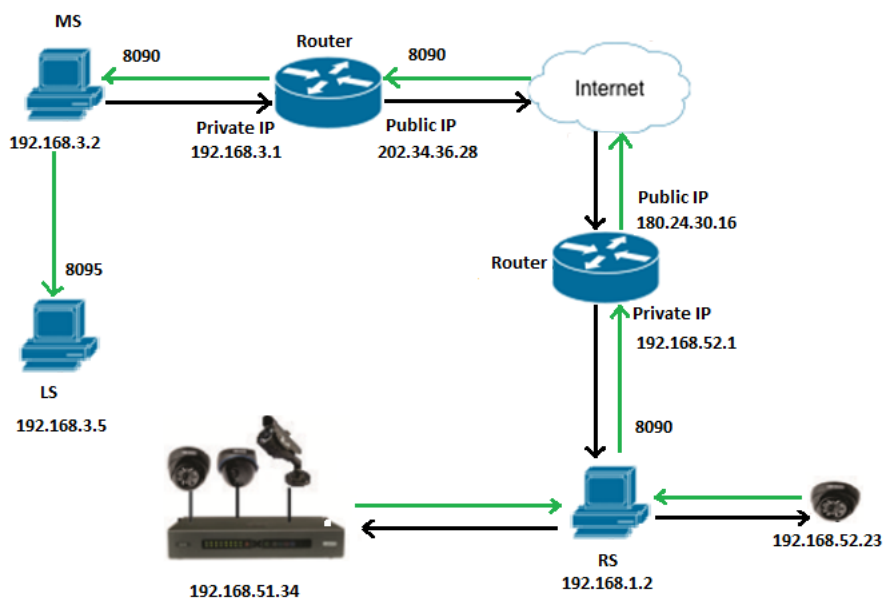
To connect Admin Client to MS:

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.

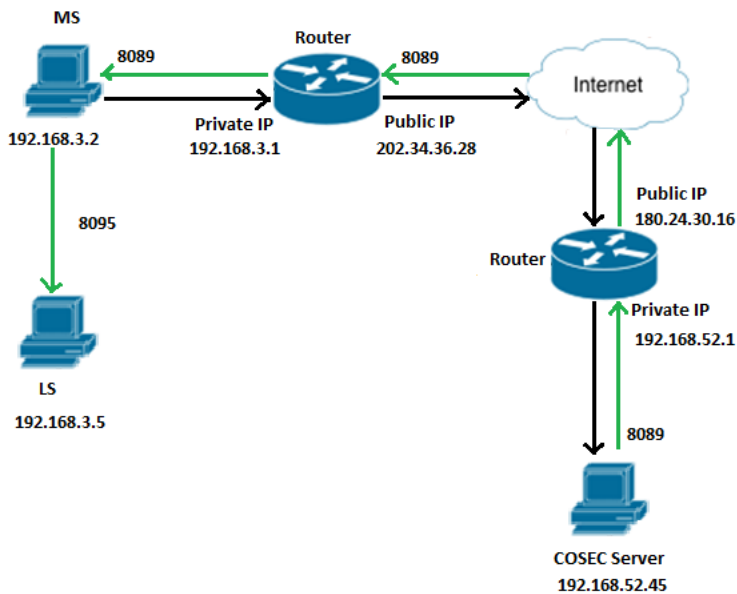


To connect API to MS:

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

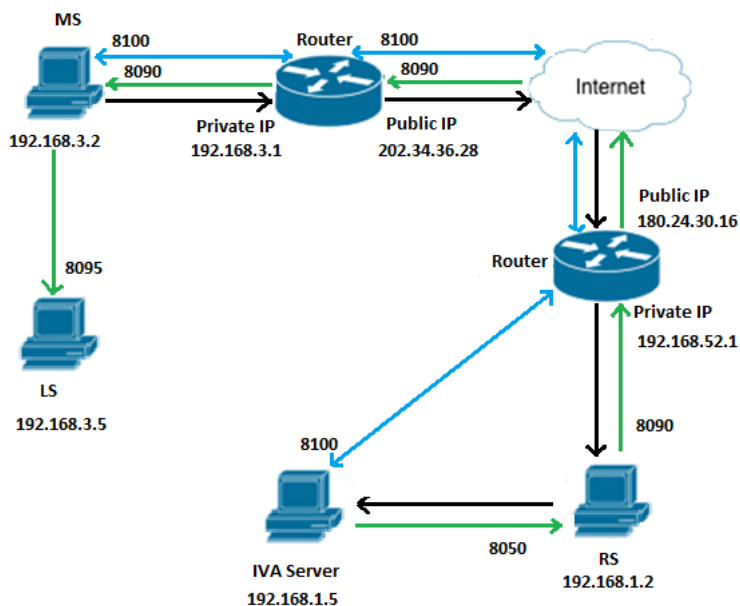
To connect COSEC Server port to MS:

- 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***

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

License Name	Abbreviation
<b>IVA License</b>	
SATATYA SAMAS Enterprise IVA Detection	EIVA Detection
SATATYA SAMAS Automatic Number Plate Recognition	ANPR
SATATYA SAMAS Face Recognition	FR
<b>Application License</b>	
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 SAMAS PLT. The **default license** of SATATYA SAMAS is as shown below:

Category	SATATYA SAMAS BASIC PLATFORM
Number of simultaneous users	1
Number of cameras	5
IVA Functions	EIVA1(1 Camera for Perimeter Events)
Application Modules	VTPM5 (5 Parking Entities), CREAM1 (1 Advance Scenario), PMTCT1(1 Camera)
Other Components	Matrix Access Control System, Media Player, Basic Scenarios

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	Top up Vouchers Available
<b>IVA License</b>		
SATATYA SAMAS Enterprise IVA Detection	To Upgrade Number of Cameras in IVA Detection (Includes Perimeter Events)	1.SAMAS EIVA1 2.SAMAS EIVA3 3.SAMAS EIVA10
SATATYA SAMAS ANPR	To Upgrade Number of Cameras in ANPR (Includes Vehicle Management Events)	1.SAMAS ANPR1 2.SAMAS ANPR3 3.SAMAS ANPR10
SATATYA SAMAS FR	To Upgrade Number of Cameras in FR (Includes Person Identification Events)	1.SAMAS FR1 2.SAMAS FR3 3.SAMAS FR10
<b>Application License</b>		
SATATYA SAMAS VTPM	To Upgrade Number of Parking Entities in VTPM (Includes Parking Management Events and Vehicle Counting event from camera)	1.SAMAS VTPM10 2.SAMAS VTPM50 3.SAMAS VTPM200
SATATYA SAMAS PMTC	To Upgrade Number of Cameras in PMTC (Includes Crowd Management Events and People Counting event from camera)	1.SAMAS PMTC1 2.SAMAS PMTC3 3.SAMAS PMTC10
SATATYA SAMAS CREAM	To Upgrade Number of Advanced Scenarios in CREAM	1.SAMAS CREAM5 2.SAMAS CREAM10 3.SAMAS CREAM50
<b>Extra License</b>		
SATATYA SAMAS Camera	To Upgrade Number of Cameras	1.SAMAS CAM5 2.SAMAS CAM20 3.SAMAS CAM100



License Name	License Category	Top up Vouchers Available
SATATYA SAMAS User	To Upgrade Number of simultaneous Users	1.SAMAS User1 2.SAMAS User3 3.SAMAS User10

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

Category	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 cameras for FR	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](mailto:Tech.Support@MatrixComSec.com)

Website: [www.matrixvideosurveillance.com](http://www.matrixvideosurveillance.com)