

# SECURSYS



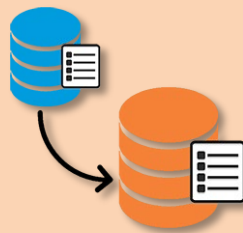
**milestone**

TECHNOLOGY  
PARTNER



**milestone**

**VERIFIED**



## **LogSync**

MIP Plugin for queuing Audit  
Log messages on SysLog  
Server

Rev. 2.0.0.0

**User Guide**

Revision Table

Rev.	Date	Changes
1.0.0.0	09/12/2019	Plugin revision first public issue
2.0.0.0	11/06/2020	Transformation of SysLog Server queuing application to a Windows Service

---

## Summary

---

<b>1</b>	<b>Copyright and Disclaimer .....</b>	<b>4</b>
<b>2</b>	<b>Intro.....</b>	<b>4</b>
	2.1 Language Used by the Plugin .....	5
<b>3</b>	<b>Installation.....</b>	<b>6</b>
<b>4</b>	<b>Specifications on Log Data Transformation.....</b>	<b>8</b>
<b>5</b>	<b>Application Operation .....</b>	<b>10</b>
	5.1 Plugin.....	10
	5.1.1 Synchronization Parameters.....	11
	5.1.2 SysLog Server Parameters .....	11
	5.1.3 Service Milestone Login Credentials .....	11
	5.2 Servizio di Windows.....	13
<b>6</b>	<b>Application License .....</b>	<b>16</b>

## 1 Copyright and Disclaimer

© Copyright SecurSys 2019-2020. All rights are reserved.

### Disclaimer

This document is intended for general information purposes only of the Plugin and its application to the Milestone XProtect Platform, of which at least basic knowledge is required.

Any risk deriving from the use of this information and/or the Plugin itself is the responsibility of the recipient who cannot in any case claim the Manufacturer.

All references to systems, people and organizations used in the document are dummy and any resemblance to real situations is purely random and unintended.

SecurSys reserves the right to make changes to the Plugin without notice.

## 2 Intro

This Application has been developed in order to periodically send all messages queued in the User Activity Log (Audit Log) to a configured SysLog Server. The transformation of the log messages from XProtect Platform and their sending complies with the current standard, described in RFC 5424 of March 2009.

The reading, transformation and sending of messages to the SysLog Server is performed by a specific Windows Service, called **MipLogSyncQueueService**. This is activated periodically (the frequency is configurable), reads the messages added after the last scheduling from the XProtect log register, transforms them as required by the reference standard and sends them to the SysLog Server, recording information on the last message carried out, in order to resume, at the next scheduling, from the next message.

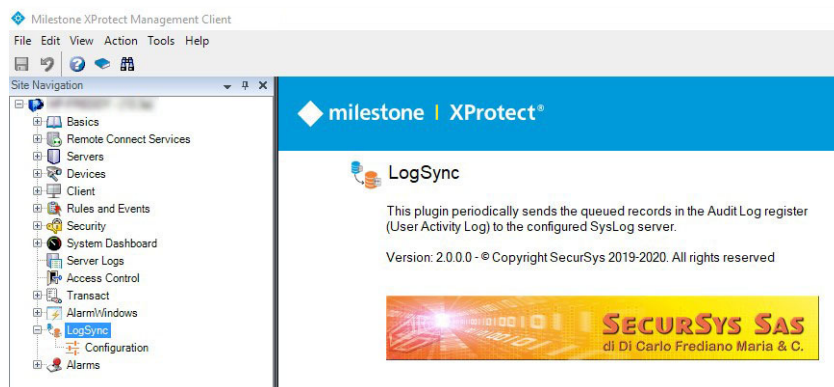
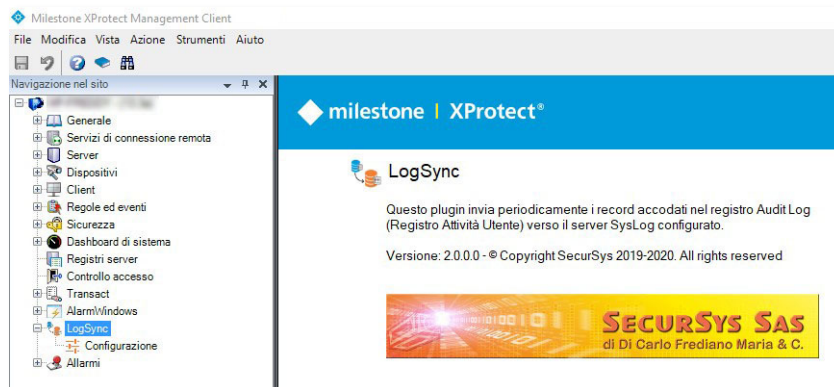
In order to function properly, the Service needs specific information (credentials for accessing the XProtect platform, SysLog Server parameters, etc.) that Users must configure through the LogSync Plugin, which operates exclusively in the Management Client environment.

The Plugin, since the Service does not interact with the User, can also be used to verify the correct functioning and progress of the transfers.

## 2.1 Language Used by the Plugin

The current version implements the Italian and English languages, the choice of which is automatic, linked to the language used by Client.

The English language is the default, therefore on any system where is not set the Italian language the plugin uses English.



### 3 Installation

The Plugin has two separate installation procedures, one for the Plugin itself and the other for the Service, which provide for the creation of folders containing what is necessary for proper operation.

The Plugin installation procedure proposes as destination folder **C:\Program Files\Milestone\MIPPlugins\LogSync**; the folder name can also be changed, but not the location ..\ MIPPlugins\ which is the one where the Plugins on 64-bit platforms must reside; however, it is advisable to leave the default unchanged.

It is also advisable to leave all the parameters of the service installation procedure unchanged, to ensure that it is correctly installed and loaded into memory when Windows starts.

In case of update, the procedures will uninstall the previous version before installing the new one.

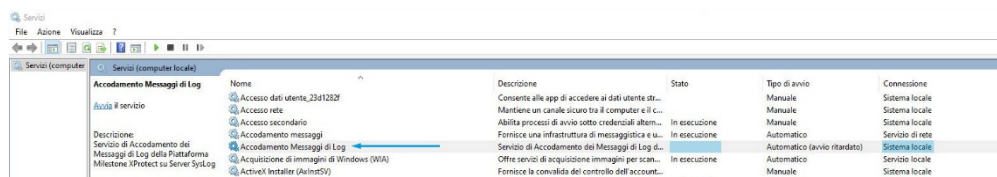
It is not necessary to stop any Milestone services to perform the installation, the Plugin operates only in the Management Client environment and as long as this application is not active the plugin will not be resident in memory.



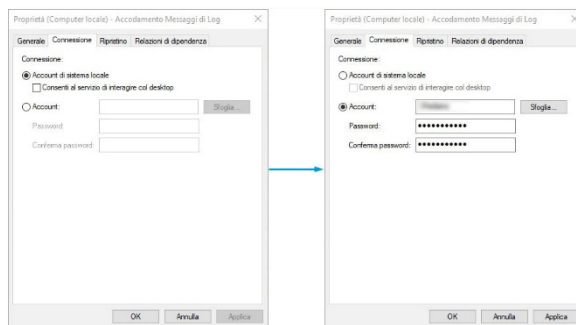
**WARNING** – due to the continuous updates of Windows aimed at increasing the security of the OS, after installing the service, it is necessary to make sure that it is started with administrative privileges, otherwise it will not work correctly.

Follow the instructions below.

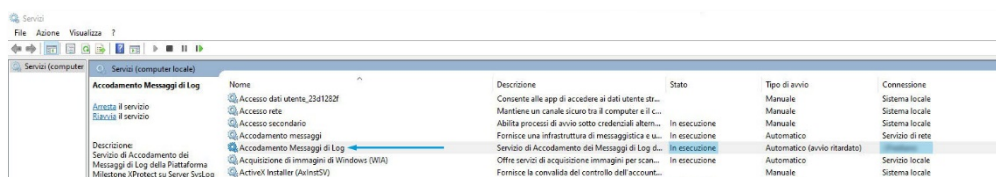
1. Start Windows Services
2. Double click on Service row



### 3. Select tab Connection, then Account, fill in Credential and OK



### 4. Start the Service



## 4 Specifications on Log Data Transformation

Each log message of the XProtect Platform has its own format, hereinafter referred to as a record, with its own fields, as shown in the following image

Local time	Message text	Permission	Category	Source type	Source name	User	User location
25/06/2020 15:00:42	User successfully logged in	Granted	Security	Server	Management Client		
25/06/2020 15:00:34	Logout	Granted	Security	Server	Management Client		
25/06/2020 14:59:07	User has accessed logs. Log type: Audit Time: 2020-06-24 12:59:03 to 2020-06-25 12:59:03 (UTC time)	Granted	Log read	Audit			fe80:150c:e14d:e615:1c96%1

Similarly, there is a specific record layout for SysLog, illustrated in the following image.

Date	Time	Facility	Severity	Hostname	Application	PID	M.ID	Message
12/06/2020	06:11:41 +02...	log audit	Info		Audit	XProtect	User	Audit has accessed logs. Log type: Audit Time: 2000-06-12 06:11:41 to 2040-06-12 06:11:41 (UTC time) [User: ...] (fe80:b0df:aed0:6d...
12/06/2020	06:11:31 +02...	log audit	Warning		Server	XProtect	Logout	Element: Management Client, Permission: Granted Server
12/06/2020	06:10:23 +02...	log audit	Info		Audit	XProtect	User	Audit has accessed logs. Log type: Audit Time: 2000-06-12 06:10:23 to 2040-06-12 06:10:23 (UTC time) [User: ...] (fe80:b0df:aed0:6d...
12/06/2020	06:08:51 +02...	log audit	Info		Audit	XProtect	User	Audit has accessed logs. Log type: Audit Time: 2000-06-12 06:08:51 to 2040-06-12 06:08:51 (UTC time) [User: ...] (fe80:b0df:aed0:6d...

Since part of the fields of each record differ from each other, it was necessary to make assumptions (conventions) in transcoding from one to the other. In particular:

- Milestone shows the Date/Time as Local Time, although internally it uses Universal Time, the Date/Time sent to the SysLog is in UTC format that SysLog clients allow you to view in various configurable formats, the image is Universal Time plus the time shift that takes into account both the Time Zone and the Solar/Summer Time (in the example the time of the first line is 08:11:41)
- The SysLog field named Equipment, represents for the reference standard the Facility parameter which can assume values from 0 to 23, each with its own meaning; for this application, the value 13 was considered more appropriate, which corresponds to the "Log Audit" type
- The Severity field (of the message) is also coded and can take 8 different values (from 0 to 7), the following rules were used to determine this field:
  - If the XProtect Log Category is Security, the Severity takes the following value:
    - Alert, if the operation was not allowed
    - Warning, if the operation has been performed
  - For all other XProtect Categories, the Severity takes the following value:
    - Warning, if the operation was not allowed
    - Info, if the operation has been performed
- The Host Name field is filled with the Name of the machine that sends the records, but it CANNOT contain any Domain name
- The Applications field corresponds to the "Source Type" field of the XProtect platform
- The P.ID (Process ID) is always filled in with "XProtect"



- The M.ID (Message ID) field provides additional information on the type of message and is normally used for search purposes only; for example, if the messages came from a switch or a firewall this field could assume the values "TCPIN" and "TCPOU" to differentiate the incoming traffic to the device from the outgoing one. When it is not explicitly set, as in the case of this application, the first word of the information content of the message is used
- Finally, the Message field is constructed starting from the XProtect log message (for example "The user is successfully logged in"), to which the other XProtect fields, otherwise not used, are added, in practice the User Name, the Source (Origin) and Permission (granted/denied), so that all information fields made available by XProtect are transferred to the SysLog Server.

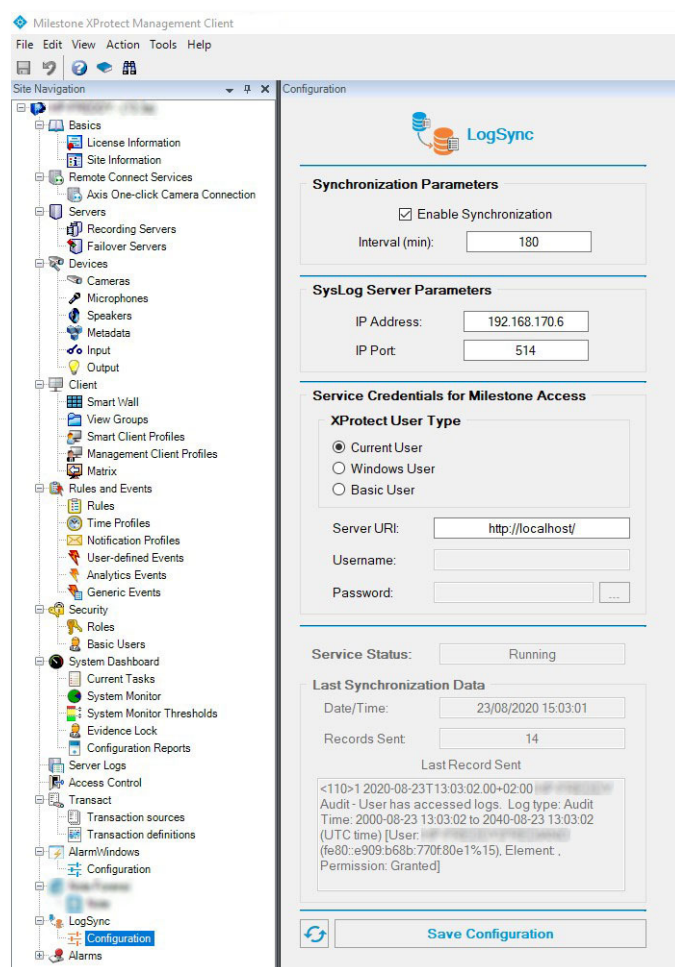
## 5 Application Operation

As indicated above, the transfer activity is entirely managed by the Windows Service, which however needs the configuration data, set through the plugin.

### 5.1 Plugin

The plugin operates exclusively in the Management Client environment, therefore to use it it's necessary to start this client; it will appear in the tree of objects managed by XProtect (on the left), as already illustrated in the figures on page **Errore. Il segnalibro non è definito.** relating to available languages.

The Plugin has a single page for configuring the operating parameters and displaying the progress status, as illustrated below.



### 5.1.1 Synchronization Parameters

The synchronization of Audit Log messages to SysLog can be suspended/enabled by un/checking the relevant box, it is then essential to specify how many minutes the synchronization procedure must be activated. The minimum value is 1', but it is definitely advisable to choose an interval of the order of one or more hours, for the following 2 reasons:

- Small time intervals tend to transfer a small number of messages and, since the procedure "remembers" the last message transferred, there is no chance that someone will be lost<sup>(1)</sup>
- The periodic scheduling induces a side effect due to the fact that the Service, at each scheduling, accesses (reads) the Log Register, which action is recorded by the XProtect Platform, therefore the closer the transfers are, the greater the possibility that only the message corresponding to the previous Service access will be transferred (and the greater the number of such messages present on both log platforms)

### 5.1.2 SysLog Server Parameters

Here are the parameters for accessing the SysLog Server; for the reasons indicated in the note it is not possible to choose between UDP and TCP, TCP is always used, the port is the standard one assigned to this service, but it can also be changed

### 5.1.3 Service Milestone Login Credentials

In this section it is necessary to specify the Access Credentials, and the URI of the Platform, which must use the Windows Service in order to read the log messages.

First of all, it is necessary to specify for what type of User the access must be granted; the rules are the following

- If the Type is Current User, ie the one logged in on Windows, there is no need for the Account parameters (User Name and Password); the Platform asks the Windows Active Directory who it is, given that this service has identified he; for this reason, the User Name box is filled with the account returned by Windows

---

<sup>(1)</sup> The statement is not fully correct since the transport protocol does not have recovery mechanisms against any packet loss. This is truer if is used the UDP protocol, allowed in the standard. The Windows service uses the TCP protocol which guarantees greater reliability in the transfer

- If the Type is a Windows User, the Password (saved encrypted and never visible) and the Account must be indicated in the form WinHost\User, where WinHost represents the name of the Windows host responsible for the authentication of the User
- If the Type is Basic User must indicate both the Password and the User Name which must NOT be preceded by any Host name, given that it is the Platform itself that authenticates this type of User.

Finally, there is the Address (URI) of the XProtect Server to which you want to connect; if the application runs on the same machine as the XProtect server, simply leave the default parameter, otherwise you must indicate the IP address or the machine name, always preceded by the suffix http://.

After making the changes to the parameters, the choices made must be saved using the appropriate button below.



**CAUTION** – when saving the Parameters, the Plugin communicates the event to the Windows Service which activates a new schedule; this first involves access to the Configuration parameters to verify that they have not changed from the previous values.

If saving takes place during a scheduling cycle, it will be necessary to wait for it to be completed before starting a new one.

The lower part of the configuration page shows both Service Status and data relating to the last scheduling, in particular:

- Date/Time of the last sending of messages to the SysLog Server
- The number of messages sent
- Il contenuto informativo dell'ultimo messaggio TCP inviato
- The payload of the last TCP message sent

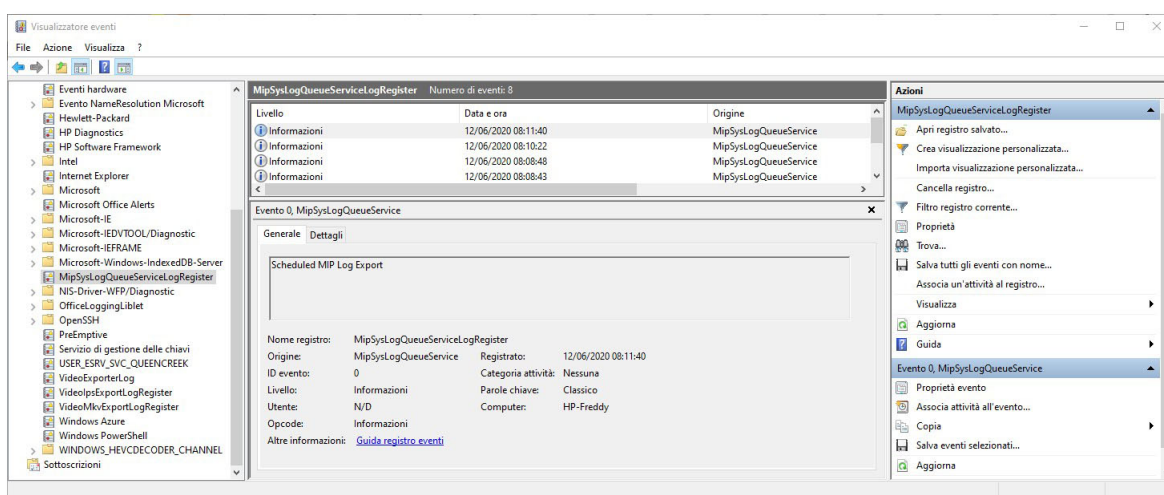
This is information for diagnostic purposes only, to make sure the Service is doing when expected. The bottom left button with the "Reload" symbol allows you to update this information.

To control the activities of the Service, it is also possible to consult, alternatively, a specific Windows log register dedicated to the application, it is called

### MipSysLogQueueServiceLogRegister

I messaggi di questo registro, oltre ad indicare se si verificano anomalie (Warning e/o Errori) consentono di verificare immediatamente se le schedulazioni avvengono con la cadenza prevista. Di seguito un esempio di tale Registro.

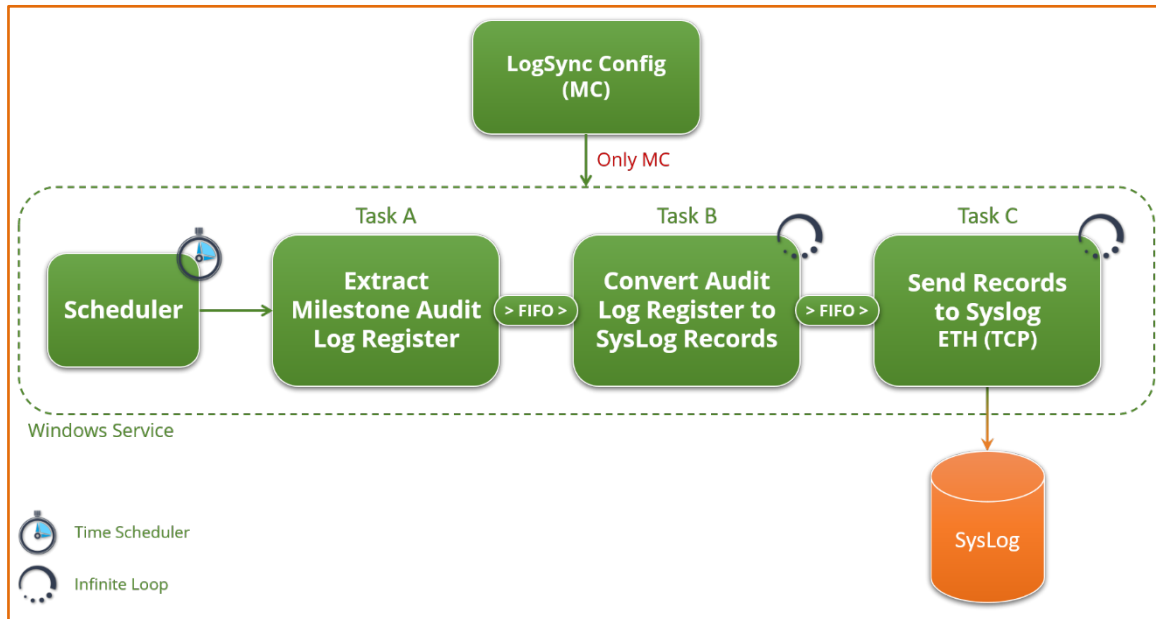
The messages in this register, in addition to indicating if anomalies occur (Warnings and/or Errors), allow you to immediately check if the schedules occur with the expected frequency. Below is an example of this register.



## 5.2 Windows Service

The Windows Service does not offer any interaction with Users, it is always resident in memory and is basically composed of 3 distinct tasks, each with a specific task.

The schematic diagram is shown in the following figure.



It should be noted that the 3 tasks, completely asynchronous with each other, exchange information using FIFO queues to ensure that a possible interruption of the chain does not create problems and, above all, the loss of messages to be sent to the SysLog Server.

For example, if the SysLog Server is not reachable, Task C will stop sending messages and its inbound queue from Task B will tend to fill up, when this happens Task B will stop queuing and will be its inbound queue that will begin to fill up, when this happens, Task A will no longer be able to queue the messages, having however kept the information of the last queued message, so when the operation is restored the first message that will be queued will be the one that is not it was possible to queue the previous schedule; the same criterion is valid for the other 2 tasks

The job of each Task is as follows:

- **Task A:** it is normally stopped waiting to be activated at pre-established intervals by the Scheduler. The specific job is to read the log messages in the XProtect register, starting from the last read, of which it retains the information, and to queue them in the FIFO towards Task B
- **Task B:** it is always active by constantly checking the presence of messages in its entry queue, which it processes immediately. The specific job is to create the SysLog record starting from the XProtect one, and then queue it in the FIFO towards Task C
- **Task C:** like the previous one, it is always active and checks the presence of messages in its entry queue. The specific job is to send, using the TCP protocol, the records to the Syslog Server

The jobs of the FIFO queues, in addition to what has been described previously, is also to make the 3 tasks completely asynchronous with each other so that no task is forced to wait for the completion of the operations of the one downstream. An example to clarify: suppose that at a given schedule there are a thousand new log messages on the XProtect Platform, after a given delay due to reading, Task A will start to queue the messages, without any type of further processing, towards the Task B which, realizing the presence of messages in the queue, will begin to process them and then queue them towards Task C. Since it has to carry out processing for each message, Task B will take longer than A, which after reading must only queue them, therefore the first FIFO will start growing. In the absence of connection interruptions, therefore, Task A will complete its task, returning to quiet state, when Task B still has messages in the queue to process. Operation between Tasks B and C is completely similar but even more marked since sending a packet over the network takes longer than it needs to be processed by Task B.

In practice, in nominal operating conditions below what happens:

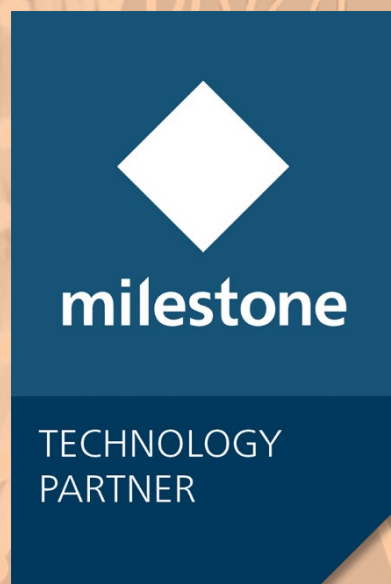
- All in quiet state with empty queues
- Start scheduling: Task A starts queuing messages which causes the start of the activities of Task B, which in turn causes the start of the Activity of Task C
- The first FIFO grows, since queuing takes less time than dequeuing by Task B, the FIFO of Task C also begins to grow, requiring even more time for dequeuing
- Task A ends its queues and returns to quiet state
- Task B continues for another time until its entry queue is empty and returns to the waiting state
- The same goes for Task C which, taking longer than the previous one, will be active for another period of time until its entry queue is emptied
- The Service is placed in the quiet state waiting for the next scheduling

## 6 Application License

License management complies with the requirements of the Milestone Licensing Framework; therefore, the specific license represents an extension of the basic license of the Platform, defined SLC (Software License Code).

The licensing scheme is based on single Server (Site License).





---

© Copyright SecurSys Sas 2019-2020. All Rights Reserved.

Documento di proprietà della SecurSys Sas. Nessuna parte del presente documento può essere riprodotta o utilizzata, anche in formato elettronico, senza l'esplicito consenso scritto da parte della SecurSys Sas, se non per i fini specifici del documento stesso.

---

**SECURSYS**