smar - System302

INSTALLATION GUIDE

System302

OCT / 09

System302

Version 7.2.2

FOUNDATION

SYS302GE

smar

www.smar.com

Specifications and information are subject to change without notice.
Up-to-date address information is available on our website.

web: www.smar.com/contactus.asp

INTRODUCTION

This guide describes what's new and updated in this release and helps you install and start the latest version of ***System302***. You can also install ***ProcessView 9.1*** and the ***System302 Documentation Pack***.

ProcessView Version 9 allows automation and IT professionals to integrate real-time manufacturing and business information into a common, Web-enabled visualization dashboard.

The ***System302 Documentation Pack*** provides the complete information about devices and software from Smar.

This guide also provides information about system requirements, product activation, network installation tips, and how to contact **Smar**.

TABLE OF CONTENTS

Section 1

SYSTEM302 VERSION 7.2.2

What's New in this Release

***System302* version 7.2.2** includes powerful new features and it is completely interoperable with all FOUNDATION™ Fieldbus, HART®, PROFIBUS®, DeviceNet, AS-i and Modbus, besides devices from other manufacturers.

System302 provides several *High Speed Ethernet* Controllers such as the DF62 and DF63 HSE/FF Controllers; DF73 HSE/Profibus-DP Controller, DF75 HSE Controller and the DF79 HSE/DeviceNet Controller.

DFI302

The **DFI302** series has three new controllers:

- **DF81:** HSE/AS-i controller with two AS-i channels, two 10/100 Mbits Ethernet ports, supporting up to 124 AS-i instruments.
- **DF95:** HSE/Profibus controller with one Profibus DP channel and two Profibus PA ports. This controller is used in applications where most instruments operate with Profibus DP but Profibus PA instruments are also installed.
- **DF97:** HSE/Profibus controller with one Profibus DP channel and four Profibus PA ports. Different from the **DF95**, this controller is used in applications where a large amount of Profibus PA instruments are installed but only few Profibus DP instruments are installed.

Another significant improvement for the **DFI302** series was restricting the controller's startup with the battery. This way, if the engineer or technician does not enable battery to turn it on, the controller will not execute its configuration. This restriction avoids loss of configuration in case of a power failure caused by environmental reasons or power supply failure.

Studio302

Studio302 integrates all applications included in the **Smar**'s Enterprise Automation System and allows you to manage your plant's device information system. For plant management, you can define a work area named *Database*, where all data processed by the plant will be stored.

It is easy to monitor links in the HSE and H1 networks using the **Live Links** tool available in ***Studio302***. From ***System302 Version 7.2.2*** on, you can also monitor input and output points from Profibus, DeviceNet and AS-i networks. Status of all links created in the ***Syscon*** configurations can be easily monitored and diagnosed during configuration, plant startup and maintenance phases.

Another functionality available in ***Studio302*** is monitoring license points according to license keys validated for ***System302*** applications. Using **License Monitor**, view the number of field devices and number of blocks used in project configurations, and the number of points still available for configuration.

The **Process Equipment Database** included in the ***Studio302*** organizes any piece of information or aspects of any of your plant components such as tanks, boilers, columns, heat exchangers and so on. You can manage installation and dimensional drawings, user's documentation, Web sources and much more.

Syscon

Syscon 6.3 supports cff version 1.7, assuring the ***System302*** interoperability with other manufacturers. Additionally, ***Syscon*** also supports *CFH* (*Capabilities Files HSE*), integrating third-party HSE instruments to ***System302***.

The new ***Area Link Tool*** lets the user create links between areas. You can define areas according to your plant process and exchange data between those areas using the ***Area Link Tool***. Different users can work simultaneously in different areas, speeding up the configuration process.

LogicView

LogicView incorporates the *Flexible Function Block* (FFB) technology, which is responsible for the data transference between the Fieldbus Subsystem and the I/O Subsystem. In addition, it allows you to customize the amount of I/O according to your necessities.

In this version, I/O points for discrete control in Profibus, DeviceNet and AS-i buses are mapped directly using ***LogicView***. Therefore, a point can be mapped only for analog control through function blocks, or for discrete control using ladder logic, or even for both cases, being suitable for any plant application.

From ***System302 Version 7.2.2*** on, ***LogicView*** provides features designed to simplify configuration and maintenance, increasing productivity:

- *Tag Matching*: change all tags in a specific network with just a few clicks.
- *Find Links*: find input and output links from FFB points, Net I/O points and functions, easily altering and identifying links in all networks.
- *Acknowledging CPU Switch*: ***LogicView*** indicates the primary CPU in a redundant system and it is no longer necessary to execute ***Syscon*** in online mode.

AssetView

AssetView Version 4.2 in ***System302*** has a new interface for ***AssetServer*** that makes it simple for the user to register and track instruments.

Along with over 100 instruments already integrated in ***AssetView***, it is easy to integrate new instruments using the ***Device Wizard***. The new **FY400** is also integrated with valve signature, diagnostics, auto-setup, etc. ***AssetView*** was extended to support asset management for Profibus instruments.

Based on the AJAX technology, web pages for equipments are more interactive, as well as the steps to add notes to the ***Device Library***. Performance is optimized by the OPC A&E support, which provides robustness for systems with a large number of instruments.

AssetView FDT tool is a FDT application that manages DTMs, drivers for specific functions from each field device used in the plant configuration, from any manufacturer. This tool provides a complete view of the plant, allows creating and managing logic connections among the DTMs and communication channels, and helps the user to access all DTM functionalities, such as online and offline parameter configuration windows, charts, calibration methods, etc.

The DTM Catalog, usually consisting of one list with all DTMs installed in the machine and another list with active DTMs in the plant projects, is also provided for **Smar** field devices.

ProfibusView

ProfibusView associated with the DF73 HSE/Profibus-DP Controller enables you to configure and monitor the main characteristics of the Profibus field devices.

Multi-user support

System302 Version 7.2.2 makes it easy for professionals to contribute to the same project. Professionals in remote offices can seamlessly contribute to the project, regardless of their location.

Access control based on the *Windows Users and Groups* allows the System Administrator to create specific groups and/or users, defining their rights to access configuration files and to execute the ***System302*** applications.

IMPORTANT
This characteristic is only available for NTFS file systems. If you are using Windows on a FAT file system, only the Administrator or the user with Administrator rights can log on to ***Studio302*** and execute the ***System302*** applications.

System Requirements

Your plant control system can be implemented by distributing the ***System302*** applications in multi-functional stations or in dedicated stations.

The table below shows the minimum requirements necessary for both stations:

Minimum System Requirements	
Computer/Processor	Pentium IV 2.0 GHz
Operational System	Windows XP Service Pack 3 or previous or Windows Server 2003 Service Pack 1 or Windows Server 2003 Service Pack 2
Ports	1 parallel port and/or 1 USB port (if SYSTEM302 uses *Hard Keys*)
Display	SVGA Monitor (256 colors)
Drives	DVD-ROM

See below the specific requirements for each type of multi-functional and dedicated stations.

IMPORTANT
If you are using Windows 2000 or Windows XP with service pack previous to **SP3**, it will be necessary to run **Windows Installer 3.1**. This file, named *WindowsInstaller-KB893803-v2-x86.exe*, is available for download at: http://www.microsoft.com/downloads/details.aspx?FamilyID=889482fc-5f56-4a38-b838-de776fd4138c&displaylang=en

Multi-Functional Stations

The typical installation of a multi-functional station can be classified as:

Typical Local Station

This station contains the following applications:

- *AssetView Client*
- *AssetView Web Server*
- *AssetServer*
- *AssetView Data Server*
- *AssetView FDT*
- *Database Client*
- *FBView*
- *FFB Manager*
- *LogicView*
- *Network Configurator*
- *OPC Servers*
- *ProfibusView*
- *Studio302*
- *Syscon*
- *Tag View*

Number of blocks:
Syscon = up to 4,096 blocks
Studio302 = up to 10,000 blocks
Number of OPC tags: up to 12,000 tags

Specific System Requirements	
Memory	2 GB RAM
Free Hard Disk Space	3 GB
Browser	Microsoft Internet Explorer 6.0.

Typical Client/Server Station

This station contains the following applications:

- *AssetView Client*
- *AssetView Web Server*
- *AssetServer*
- *AssetView Data Server*
- *AssetView FDT*
- *Database Client*
- *Database Manager*
- *FBView*
- *FFB Manager*
- *LogicView*
- *Network Configurator*
- *OPC Servers*
- *ProfibusView*
- *Studio302*
- *Syscon*
- *Tag View*

The requirements are the same as described for the **Typical Local Station**.

Typical Client Station

This station contains the following applications:

- *AssetView Client*
- *AssetView Web Server*
- *AssetServer*
- *AssetView Data Server*
- *AssetView FDT*
- *Database Client*
- *FBView*
- *FFB Manager*
- *LogicView*
- *Network Configurator*
- *OPC Servers*
- *ProfibusView*
- *Studio302*
- *Syscon*
- *Tag View*

The requirements are the same as described for the **Typical Local Station**.

Dedicated Stations

Engineering Database Station

The complete database configuration of a control system is stored is this station. There can be only one *Engineering Database Station* in a control system. In small systems, this station can also handle all the other necessary functionalities, such as operation, maintenance, OPC server, data logging, etc.

The following applications are installed:

- *AssetView Client*
- *AssetView Web Server*
- *AssetServer*
- *AssetView Data Server*
- *AssetView FDT*
- *Database Client*
- *Database Manager*
- *FBView*
- *FFB Manager*
- *LogicView*
- *Network Configurator*
- *OPC Servers*
- *ProcessView*
- *ProfibusView*
- *Studio302*
- *Syscon*
- *Tag View*

In this station, the directories *Block Support*, *Device Support* and *FFB Support* are also installed.

Number of blocks:
Syscon = up to 4,096 blocks
Studio302 = up to 10,000 blocks
Number of OPC tags: up to 12,000 tags

Specific System Requirements	
Memory	2 GB RAM
Free Hard Disk Space	3 GB

Engineering Station

This station also configures the control system. It modifies the configuration database available in the previously mentioned *Engineering Database Station*. This station can also handle other functionalities related to the plant operation.

The following applications are installed:

- *AssetView Client*
- *AssetView Web Server*
- *AssetServer*
- *AssetView Data Server*
- *AssetView FDT*
- *Database Client*
- *FBView*
- *FFB Manager*
- *LogicView*
- *Network Configurator*
- *OPC Servers*
- *ProcessView*
- *ProfibusView*
- *Studio302*
- *Syscon*
- *Tag View*

In this station, the directories *Block Support*, *Device Support* and *FFB Support* are also installed.

Number of blocks:
Syscon = up to 4,096 blocks
Studio302 = up to 10,000 blocks
Number of OPC tags: up to 12,000 tags

Specific System Requirements	
Memory	2 GB RAM
Free Hard Disk Space	3 GB
Browser	Microsoft Internet Explorer 6.0.

Operation Station

The main responsibility of this type of station is to serve as a human machine interface to the plant operation personnel.

The following applications are installed:

- *AssetView Client*
- *Database Client*
- *FBView*
- *FFB Manager*
- *OPC Servers*
- *ProcessView*
- *Studio302*
- *Tag View*

In this station, the directories *Block Support*, *Device Support* and *FFB Support* are also installed.

Number of blocks:
Studio302 = up to 10,000 blocks

Specific System Requirements	
Memory	1 GB RAM
Free Hard Disk Space	1 GB

Maintenance Station

The main purpose of the *Maintenance Station* is asset management and system diagnostics. The following applications are installed:

- *AssetView Client*
- *AssetView Web Server*
- *AssetServer*
- *AssetView Data Server*
- *AssetView FDT*
- *Database Client*
- *FBView*
- *FFB Manager*
- *Network Configurator*
- *OPC Servers*
- *ProcessView*
- *ProfibusView*
- *Studio302*
- *Syscon*
- *Tag View*

In this station, the directories *Block Support*, *Device Support* and *FFB Support* are also installed.

Number of blocks:
Syscon = up to 4,096 blocks
Studio302 = up to 10,000 blocks
AssetView Client

Specific System Requirements	
Memory	2 GB RAM
Free Hard Disk Space	3 GB
Browser	Microsoft Internet Explorer 6.0.

OPC Configuration & Supervision Server

This station is only necessary for large scale control systems. This station has two purposes: to enable the flow of configuration commands from the engineering stations to the control modules and to deliver process data to other workstations efficiently. There can be only one *OPC Configuration & Supervision Server* on each subnet. The directories from the *Block Support* and *Device Support* are also installed in this station. The following applications are installed:

- *AssetView Client*
- *AssetView Web Server*
- *AssetServer*
- *AssetView Data Server*
- *AssetView FDT*
- *Database Client*
- *FBView*
- *FFB Manager*
- *OPC Servers*
- *Studio302*
- *Tag View*

In this station, the directories *Block Support*, *Device Support* and *FFB Support* are also installed.

Number of OPC tags: up to 12,000 tags

Specific System Requirements	
Memory	2 GB RAM
Free Hard Disk Space	3 GB

OPC Supervision Server

This station is only necessary for large scale control systems. The purpose of *OPC Server Station* is delivering process data to other workstations efficiently. The following applications are installed:

- *AssetView Web Server*
- *AssetServer*
- *AssetView Data Server*
- *AssetView FDT*
- *Database Client*
- *FBView*
- *FFB Manager*
- *OPC Servers*
- *Studio302*
- *Tag View*

In this station, the directories *Block Support*, *Device Support* and *FFB Support* are also installed.

Number of OPC tags: up to 12,000 tags

Specific System Requirements	
Memory	2 GB RAM
Free Hard Disk Space	3 GB

Data Logger/Server Station

The purpose of this station is to store alarm, events and trend history data using MSDE, SQL or Oracle databases. It can also be used to store asset management history data. The following applications are installed:

- *Database Manager*
- *FBView*
- *FFB Manager*
- *OPC Servers*
- *SQL Server/MSDE*
- *Studio302*
- *Tag View*

In this station, the directories *Block Support*, *Device Support* and *FFB Support* are also installed.

Specific System Requirements	
Memory	2 GB RAM
Free Hard Disk Space	1.2 GB

Application Station

The main purpose of this workstation is to integrate third-party applications, such as advanced control and batch control, to the control system. The following applications are installed:

- *Database Client*
- *FBView*
- *FFB Manager*
- *OPC Servers*
- *Studio302*
- *Tag View*

In this station, the directories *Block Support*, *Device Support* and *FFB Support* are also installed.

Specific System Requirements	
Memory	1 GB RAM
Free Hard Disk Space	1 GB
Browser	Microsoft Internet Explorer 6.0.

Note: ***System302*** is supported on Windows XP Service Pack 2, Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 only if the execution prevention mechanism (also known as *DEP-data execution prevention* and *NX-no execution*) is not activated. Refer to the section ***Installing System302*** for further details on how to configure the DEP settings.

Uninstalling System302

Before installing your new ***System302*** version, it is recommended that you uninstall any older versions. Running multiple versions of ***System302*** applications on the same computer is not recommended or supported by Smar.

Follow these recommendations to protect existing project configurations and system information you may have on your system.

Creating a Backup from Existing Configuration Projects

Uninstall procedures do not remove project configuration files from your system. We do recommend, however, that you copy configuration files from the **Smar** folder to another location on your hard drive before uninstalling ***System302***.

Use the *Pack & Go* feature to pack your project configurations file in a single compacted file and then, after installing ***System302*** version 7.2.2, unpack and import those files to ***Studio302***.

The *Pack & Go* procedure is available from ***Syscon*** Version 6.0.0 on, which is part of ***System302*** version 6.1.9 and later versions.

Refer to **Appendix A** on this guide for details on how to pack project configurations files using ***System302*** version 6.1.9 or later versions and unpack those files using ***System302*** version 7.2.2.

IMPORTANT
Project configurations created in ***System302*** **version 7.1.0.x** are **not compatible** with the new version 7.2.2. If you are using the version 7.1.0.x, contact the Smar tech support to be compatible with the version 7.2.2.

Saving Existing Project Templates

If you edited ***Syscon*** templates files, save a copy of the template in another location on your hard drive before uninstalling ***System302***. Refer to the **Syscon User's Manual** for details about *Template Files*.

Existing ***Syscon*** templates will be overwritten during the installation if they were not renamed.

Removing System302 Installation

Use these steps to remove a previous version of ***System302*** from your system.

1. From the **Start** menu, select **Settings > Control Panel**.
2. Double-click on **Add/Remove Programs**.
3. If the ***Network Configurator*** tool is installed, select its icon from the list of programs and click **Change/Remove**. Follow the steps to uninstall the ***Network Configurator***.
4. From the list of programs that you can remove, select **SYSTEM302** and click **Change/Remove**.
5. At the ***System302*** Installation window, select the option **Remove** to remove all installed features and click **Next**.
6. At the prompt, click **Ok** to confirm that you want to remove ***System302***. The *Uninstall* procedure will take a few minutes to remove ***System302***.
7. When the *Uninstall* procedure is complete, click **Ok** to conclude.

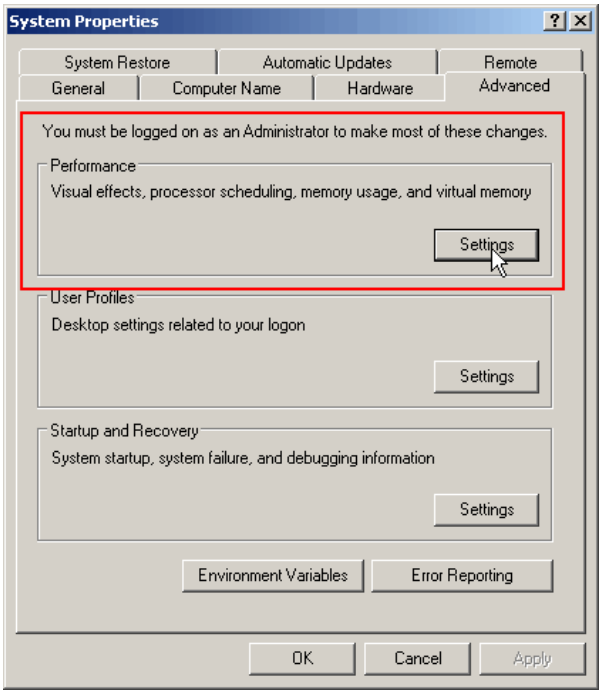
Installing System302

Before you install ***System302*** on your machine, some important settings must be configured on the Windows Operational System to guarantee the correct operation of your system.

Refer to the appendix **Security Practices for Network Administrators** on this guide and follow the procedure to configure the communication network.

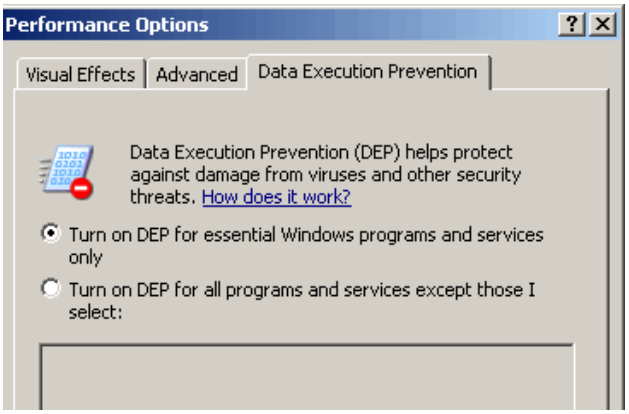
Verify the Data Execution Prevention Settings

Open the Windows **Control Panel** and double-click on **System**. The **System Properties** dialog box will open. Select the **Advanced** tab and click the button **Performance Settings**.



System Properties

The **Performance Options** dialog box will open. Select the **Data Execution Prevention** tab and mark the option **Turn on DEP for essential Windows programs and services only**.



Performance Options

Click **Ok** and close the **System Properties** dialog box. If the settings were altered, it will be necessary to restart the computer.

IMPORTANT
In case there is a need to turn on DEP for all programs and services to keep the computer safe, proceed with the ***System302*** installation and after the installation is complete, open the **Performance Options** dialog box and add **Syscon.exe** to the list of exceptions. The **Syscon.exe** file is located on the ***System302*** installation folder. The default file path is "*C:\Program Files\Smar\Syscon\Syscon.exe*".

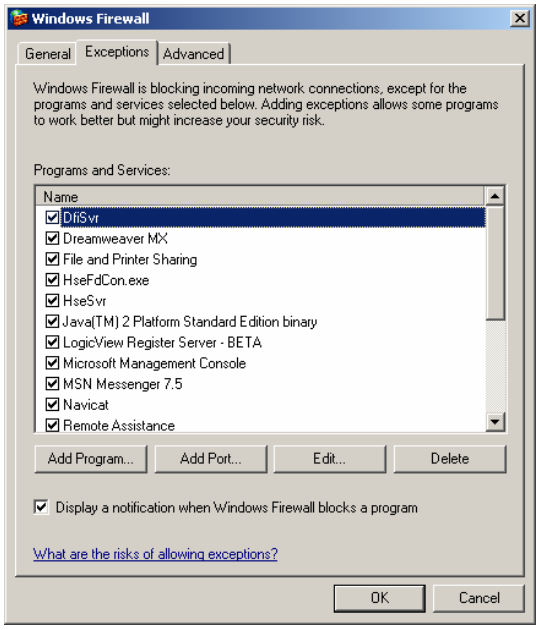
Configure the Windows Firewall Settings

If Windows Server 2003 Service Pack 1 or Windows XP Service Pack 2 will be acting as your SNTP Server, execute the following steps:

1. Using Windows Server 2003 Service Pack 1, click **Start** on the Windows taskbar, select **Settings** and click the option **Network Connections**. On the **Network Connections** window, select **Change Windows Firewall Settings** on the left pane.

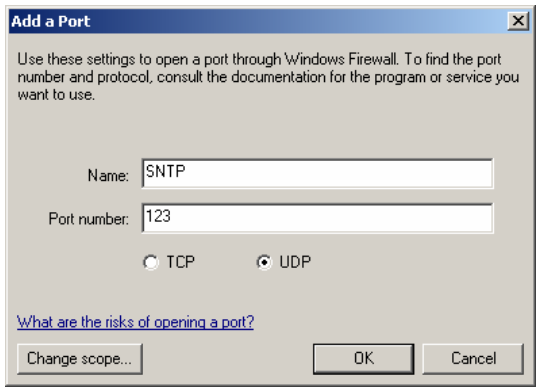
   OR

   Using Windows XP Service Pack 2, click **Start** on the Windows taskbar, select **Control Panel** and double-click the icon **Windows Firewall**.
2. The **Windows Firewall** dialog box will open. Click the **Exceptions** tab:
3. Click the button **Add Port**.



Configuring the Windows Firewall

4. On the **Add a Port** dialog box, use **SNTP** as the port name and type **123** for the port number (this is the SNTP reserved port). Select the **UDP** protocol and click **Ok** to conclude.



Configuring the SNTP Port

To access an instance of the Microsoft SQL Server Database Engine through a firewall, you must configure the firewall on the computer running SQL Server to allow access.

By default, Microsoft Windows XP Service Pack 2 enables the Windows Firewall, which closes port 1433 to prevent Internet computers from connecting to a default instance of SQL Server on your computer. To open a port in the Windows firewall for TCP access, repeat steps 3 and 4 to add the **TCP/IP** port **1433**.

To use SQL Server Browser, repeat steps 3 and 4 to add the UDP port 1434.

Executing the System302 Installation

Make sure that you are logged into your machine as the *Local Administrator* or as a user in the *Local Administrator*'s group. It is recommended to close all programs.

Insert the DVD labeled **SYSTEM302 Installation (Configuration Tools)** into your DVD-ROM drive. If the option *Autorun* is enabled on your system, the ***System302*** *Welcome Window* starts automatically. Otherwise, if the option *Autorun* is not enabled, from the **Start** menu, select **Run** and type **D:\Default.hta** (substitute the appropriate letter of your DVD-ROM drive for **D**).

On the ***System302*** welcome window, click **Launch System302 Installation** and follow the instructions on the screen to complete the installation.

By default, ***System302*** applications are installed in the directory *C:\Program Files*\. During the installation, you can change the installation directory.

During the installation, the user will be asked to select the *Setup Type*:

- TYPICAL: This is the setup type recommended for most users. ***System302*** will be installed with the most common applications. The user will select the station mode: *Local*, *Client/Server* or *Client*. These stations are described in section **Multi-Functional Stations**.

- ADVANCED: This setup type is recommended for advanced users. ***System302*** will be installed with the minimum required applications according to the station mode selected: *Engineering Database Station*; *Engineering Station*; *Operation Station*; *Maintenance Station* or *Data Logger/Server Station*. These stations are described in section **Dedicated Stations**.

- CUSTOM: This setup type is recommended for expert users. The user will select the ***System302*** applications that will be installed.

During the installation, you are asked to enable or disable the user login procedure in ***Studio302***:

- Select the option **Enable Security Management** to enable the login procedure. Users will have to type their login and password to run ***Studio302***. This option is recommended when the plant control strategy is already configured and operating.

- Select the option **Disable Security Management** to disable the login procedure. It will not be necessary to type the login and password to run ***Studio302***. This option is recommended during engineering and development phases. The system administrator is responsible for user access control.

IMPORTANT
It will be necessary to reinstall ***System302*** to change the settings for **Security Management** once the current installation procedure is complete.

The **System302 Documentation Package** is available on the same installation DVD. You can choose to install the **Documentation** on your local machine or you can skip this installation and browse the documentation files direct from the DVD.

IMPORTANT
The installation procedure will check if MSDE is already installed on your machine. If the MSDE installation is compatible to ***System302***, the user will only need to select the **Smar** database and will not lose previous information. Otherwise, it might be necessary to reinstall the MSDE. Refer to section **Known Problems and Limitations** in this guide for further details.

System302 installation procedure may take a few minutes to be complete. If you are prompted to restart your computer, click **Yes**.

After the System302 Installation

If ***System302*** is running on Windows Server 2003 Service Pack 1 or Windows XP Service Pack 2 and a Firewall is enabled, the Firewall settings must be configured to allow the ***System302*** applications to be executed.

After the ***System302*** installation, the following applications must be unblock on the Firewall settings:

- DefineParametersTool (file name: *FFBDefWizard.exe*)

  Default Path:
  `C:\Program Files\Smar\FFBDefParam` (Operational System in English)
  `C:\Arquivos de Programas\Smar\FFBDefParam` (Operational System in Portuguese)

- DfiSvr (file name: *DfiSvr.exe*)

  Default Path:
  `C:\Program Files\Smar\OleServers` (Operational System in English)
  `C:\Arquivos de programas\Smar\OleServers` (Operational System in Portuguese)

- FFB Manager (file name: *FnTypeWizard.exe*)

  Default Path:
  `C:\Program Files\Smar\FFBDefParam` (Operational System in English)
  `C:\Arquivos de programas\Smar\FFBDefParam` (Operational System in Portuguese)

- HseSvr (file name: *HseSvr.exe*)

  Default Path:
  `C:\Program Files\Smar\OleServers` (Operational System in English)
  `C:\Arquivos de programas\Smar\OleServers` (Operational System in Portuguese)

- Java(TM) 2.0 Platform Standard Edition binary (file name: *CWServer.exe*)

  Default Path:
  `C:\Program Files\Smar\ConfigurationWorkspace` (Operational System in English)
  `C:\Arquivos de programas\Smar\ConfigurationWorkspace` (OS in Portuguese)

- LogicView Register Server (file name: *LVforFFB.exe*)

  Default Path:
  `C:\Program Files\Smar\ProgTool` (Operational System in English)
  `C:\Arquivos de programas\Smar\ProgTool` (Operational System in Portuguese)

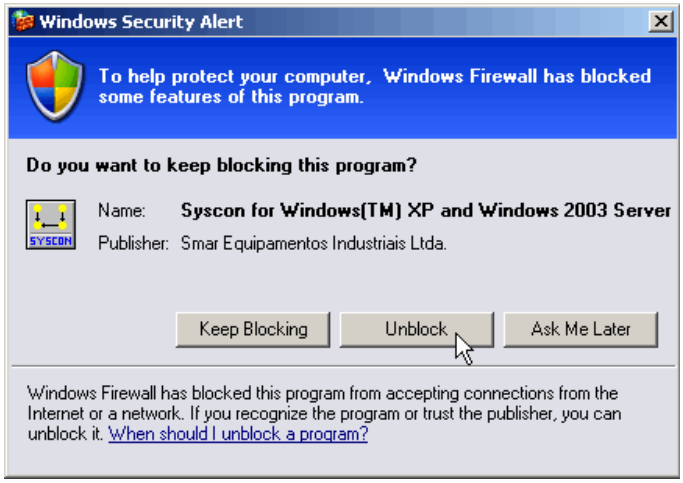
- SmarStudioBridgeProxy (file name: *SmarStudioBridgeProxy.exe*)

  Default Path:
  `C:\Program Files\Smar\Studio302\Bin` (Operational System in English)
  `C:\Arquivos de programas\Smar\Studio302\Bin` (OS in Portuguese)

- Syscon for Windows(TM) XP and Windows 2003 Server (file name: *Syscon.exe*)

  Default Path:
  `C:\Program Files\Smar\Syscon` (Operational System in English)
  `C:\Arquivos de programas\Smar\Syscon` (Operational System in Portuguese)

Using Windows OS, click **Unblock** on the **Windows Security Alert** dialog box to allow the application to be executed. See the example below:



Unblocking *System302* Applications

If another Firewall application is being used, the same settings must be applied.

If ***System302*** is being executed in the **Client/Server** mode, it will be also necessary to configure the access from the client machines to the *Database Server* station, adding the IP addresses of the client machines to the list of permitted accesses in the Firewall application installed on the server machine. Refer to the Firewall application user's manual for details on how to configure the access from remote machine editing the list of IP addresses.

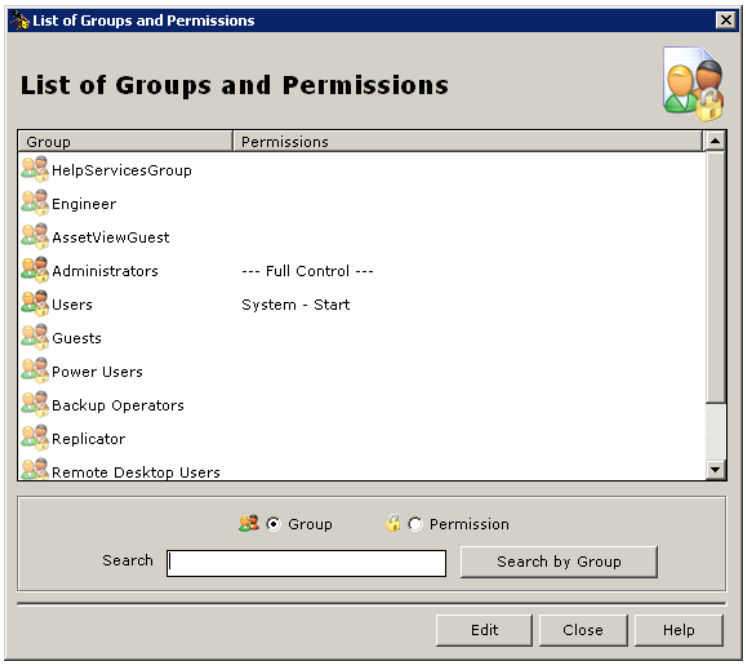
Using the Windows Firewall, the default configuration for executing applications will allow the access from client machines to the server.

Configuring DCOM Properties for *Studio302* Groups

There may be some difficulties configuring the components communication when using *Windows XP SP2* and *Windows Server 2003 SP1*, caused by advanced security properties on these operational systems. This tutorial will describe the procedure to configure some security properties in order to enable proper communication among components.

The DCOM properties must be configured only for the ***Studio302 Groups*** where the default permissions were edited. To verify which groups should be configured, open the **List of Groups and Permissions** dialog box. On the ***Studio302*** window, go to the **Settings** menu, select **Security** and click **Group Management**.

The figure below shows an example where the permissions for the groups **Users** and **Administrators** were altered and therefore only these two groups must be configured in the DCOM properties.

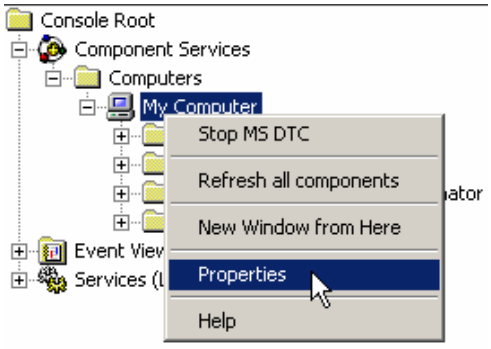


Groups and Permissions

The DCOM properties must be configured every time the List of Permissions is altered.

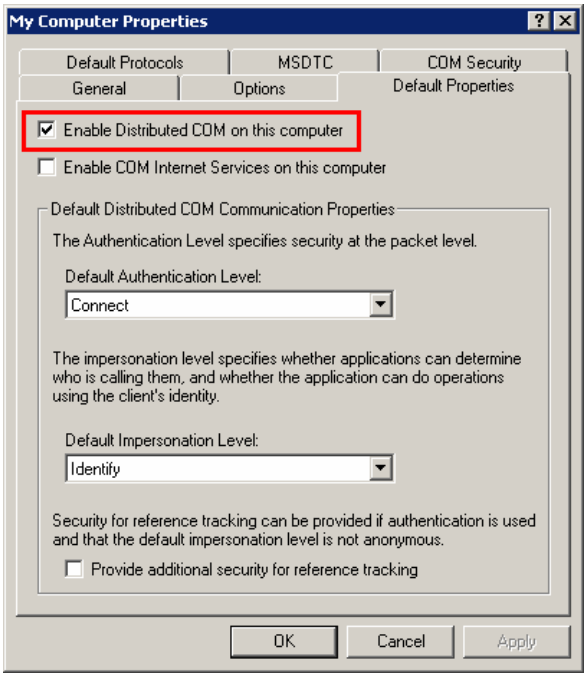
ATTENTION
By default, if the user is logged on the local machine, the groups **Users** and **Administrators** will have pre-configured permissions for ***Studio302***. If the user is logged on a domain, the groups **Domain Users** and **Domain Admins** will have pre-configured permissions for ***Studio302***. Therefore, these groups must be initially configured in the DCOM properties according to the workgroup or domain to which the computer belongs.

On the **Start** menu, click **Run**, type **dcomcnfg** and click **Ok**. The **Component Services** window will open. Expand the Root tree and locate the icon *My Computer*: **Console Root > Component Services > Computers > My Computer**.



My Computer Properties Dialog Box

Check if the DCOM is enabled: right-click the icon **My Computer** and click **Properties**. On the **My Computer Properties** dialog box, select the **Default Properties** tab and the option **Enable Distributed COM on this computer** should be marked.



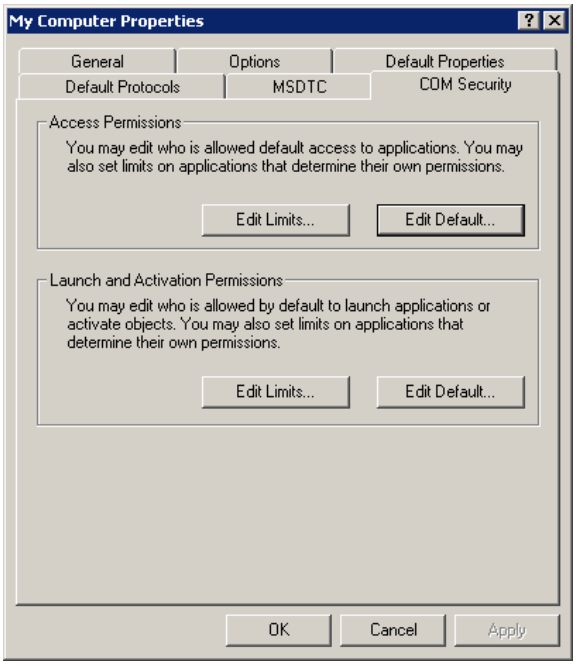
Enabling DCOM on the computer

There are two possibilities to configure the DCOM properties: configuring the default access and configuring individual component access.

Configuring Default Access

This procedure will configure the permissions for **all** of the components in the DCOM. It will not be necessary to configure the DCOM permissions for each ***Studio302*** component.

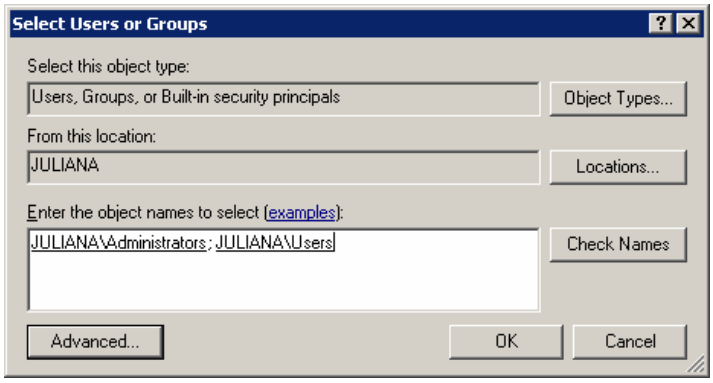
On the **Component Services** window, right-click the icon **My Computer** and click the option **Properties**. On the **My Computer Properties** dialog box, select the **COM Security** tab.



Configuring Permissions

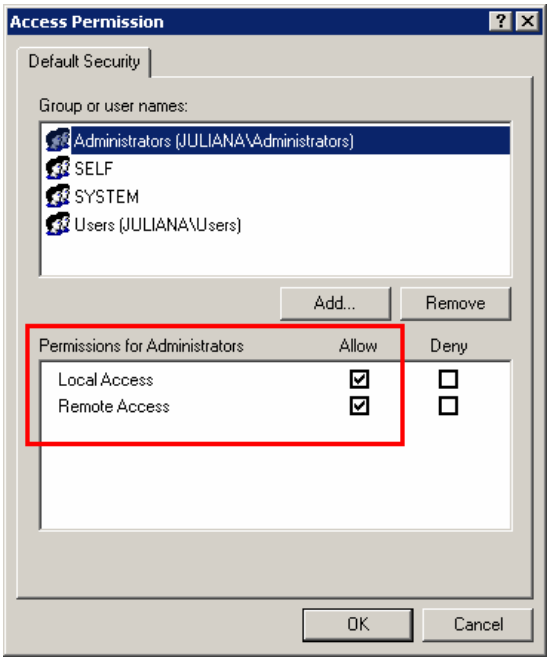
Click the button **Edit Default** on the **Access Permissions** area. On the **Access Permissions** dialog box, click **Add**. Then, on the **Select Users or Groups** dialog box, click **Advanced**. If the list of users and groups is empty, click **Locate**.

Select the icon of the user or group. To select more than one user or group, press **Ctrl** on the keyboard and click the icon of the other users/groups. Click **Ok** to conclude. See the example below:



Adding Users and Groups

Click **Ok** to return to the **Access Permissions** dialog box. Select the icon of the user/group and mark the column **Allow** for **Local Access** and **Remote Access**. See the example below:



Access Permissions

Click **Ok** to return to the **My Computer Properties** dialog box.

Click the button **Edit Default** on the **Launch and Activation Permissions** area and repeat the procedure to add users and groups related to ***Studio302***. Select **Local** and **Remote Launch**, and **Local** and **Remote Activation** permissions for each user and group added.

Configuring Individual Component Access

This procedure will configure the permissions for **each *Studio302*** and other components in the DCOM. The list below shows the components that will be configured manually:

Studio302 Components

Name	AppID
SmarProxyAE	{124BB93B-1681-41F9-A1B6-88CA170C938B}
SmarProxySE.cAE	{1061A2BF-0909-4DCC-BAC3-B2E3BCDBDED1}
SmarStudio	{0094EBDD-277C-4322-866C-C70134F5F5E7}
SmarStudioBridgeProxy	{05931DBE-7B09-4C81-B15D-DBAB7A62AC3A}
SmarWatcher.cWorkspace	{E970545E-C8C8-47A5-85E5-7BB9E04B3CF9}
SSSDetectDevice.cWatcherDB	{24A7E20D-7AFA-4F0A-8405-FFCB2421F088}
StudioTerminal	{9800A1DD-1C44-4C59-9837-5168AA5E4E68}

Other Components

Name	AppID
Device Description Server	{D131A1E2-BF1C-11D1-B72C-00A024DC2292}
OpcEnum	{13486D44-4821-11D2-A494-3CB306C10000}
Smar Alarm & Event Server	{D67847D4-EEA3-11d2-9D1E-00600802552B}
Smar OPC & Conf Server for DFI302	{D67847D1-EEA3-11d2-9D1E-00600802552B}
Smar OPC & Conf Server for HSE	{D67847D3-EEA3-11d2-9D1E-00600802552B}

IMPORTANT

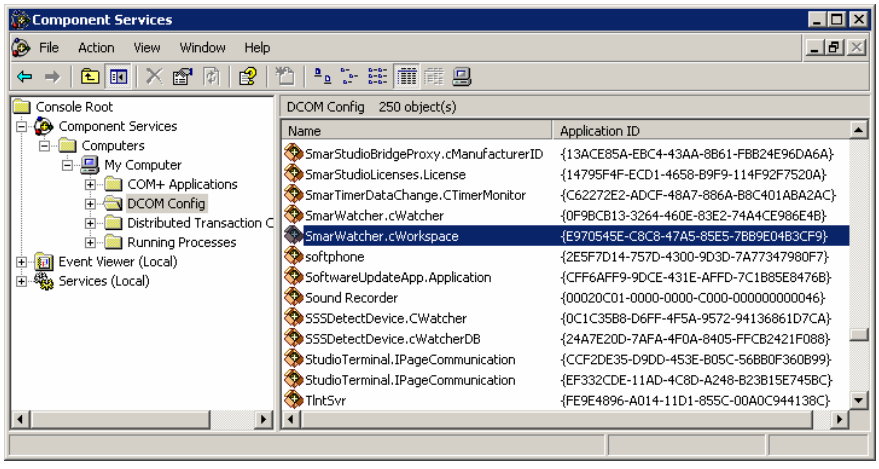
If ***AssetView*** is installed on your machine, include the ***AssetView*** users and groups to each of the components indicated above. Refer to the section **Configuring the DCOM Properties for *AssetView* Groups**.

The following example will describe the procedure to configure the component **SmarWatcher**. Refer to this example to configure all components listed above.

1) On the **Component Services** window, expand the Console Root tree and locate the *DCOM Config* folder: **Component Services > Computers > My Computer > DCOM Config**.

2) The DCOM components will be listed. The user can click the menu **View > Detail** to view a detailed list of components.

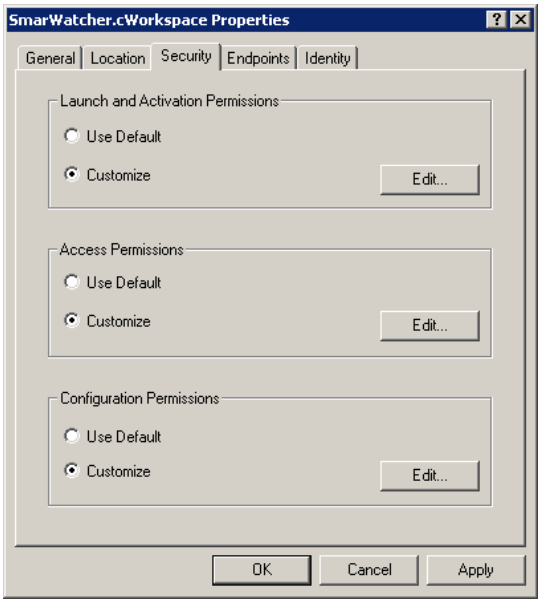
3) Locate the component **SmarWatcher** with the corresponding **AppID**.



Locating the Component

4) Right-click this component and select **Properties**.

5) On the **Component Properties** dialog box, select the **Security** tab.



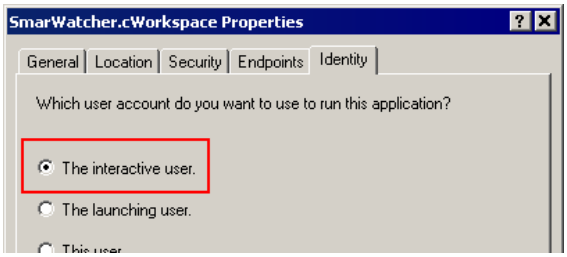
Security Tab

6) On the **Launch and Activation Permissions** area, select the option **Customize** and click **Edit**.

7) Add the ***Studio302*** Groups and select **Local** and **Remote** permissions for **Launch** and **Activation**, for all groups. Refer to the topic **Configuring the Default Access** to add users and groups.

8) Return to the **Component Properties** dialog box. On the **Access Permissions** area, select the option **Customize** and click **Edit**. Add the ***Studio302*** Groups as described on item 7.

9) Return to the **Component Properties** dialog box and select the **Identity** tab. Mark the option **The interactive user** and click **Ok** to conclude.



Identity Tab

10) Repeat these steps to configure all components listed at the beginning of this subsection.

Configuring DCOM Properties for *AssetView* Groups

If ***AssetView*** is installed on your machine, it will be necessary to configure DCOM permissions for these additional user and groups:

Name	Type
Administrators	Group
Interactive	Group
System	Group
ASP.NET	User
Engineer	Group
AssetViewGuest	Group

The procedure to configure DCOM permissions for ***AssetView*** Users and Groups is the same described for ***Studio302*** Users and Groups.

- When configuring the *Default Access*, add the ***AssetView*** user and groups indicated above to the list of users and groups on the **Access Permissions** dialog box and the **Launch and Activation Permissions** dialog box, selecting **Local** and **Remote** permissions. Refer to the topic **Configuring the Default Access** above.
- When configuring *Individual Component Access*, add the ***AssetView*** user and groups indicated above to the following ***AssetView*** component and to the list of other components indicated previously:

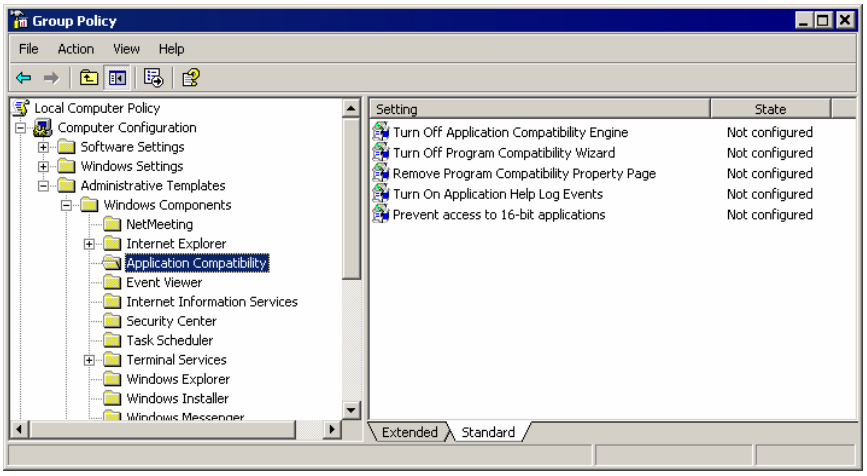
Name	AppID
AvTerminal.IPageCommunication	{E9504C4B-F9C4-4A55-8C1F-97B0C6C0B447}

Follow the procedure described in the topic **Configuring the Individual component access** above.

Configuring Access Permission to 16-Bit Applications

It is necessary to configure permissions to access 16-bit applications or applications with 16-bit components, using Windows 2003 Server or higher. This configuration is executed in the **Group Policy** window.

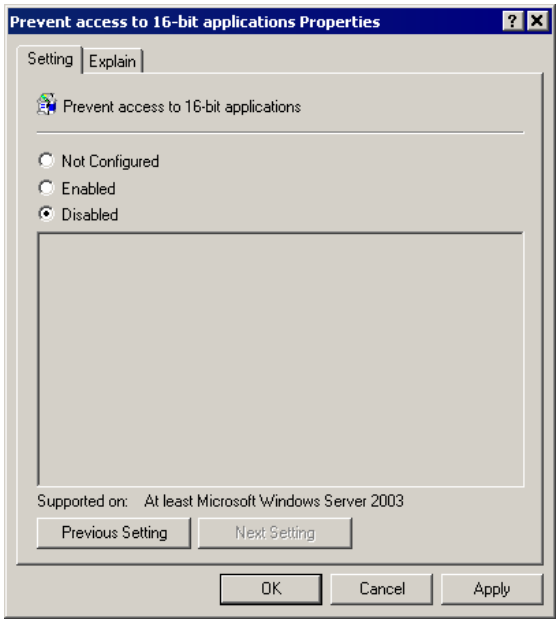
On the **Start** menu, click **Run**, type **gpedit.msc** and click **Ok** to open the window.



Group Policy Window

On the **Group Policy** window, expand the directory tree and locate the folder **Application Compatibility**. The default path is *Computer Configuration* > *Administrative Templates* > *Windows Components* > *Application Compatibility*.

Right-click the option **Prevent access to 16-bit applications** and select **Properties**. In the **Properties** dialog box, select the tab **Setting** and mark the option **Disabled**. Click **Ok** to conclude.



Properties Dialog Box

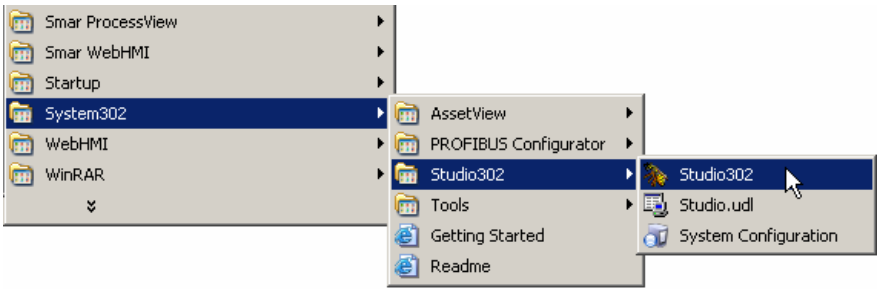
On the **Group Policy** window, click *User Configuration* > *Administrative Templates* > *Windows Components* > *Application Compatibility*. Repeat the configuration described above for the option **Prevent access to 16-bit applications**.

Configuring System302 Environment

Once you finished installed ***System302***, you should launch the ***Studio302*** application to activate the product and configure your system. If you do not activate the product, you will not be able to run any of the applications. You only need to activate ***System302*** once.

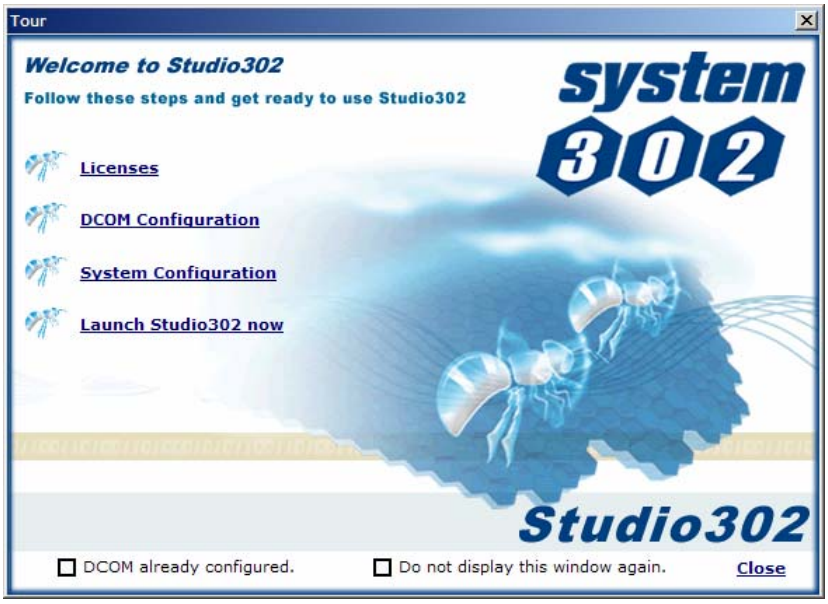
During the activation procedure, you are required to provide your company's information.

Start ***Studio302*** selecting **Start > Programs > System302 > Studio302** and clicking on **Studio302**:



Starting Studio302

The *Welcome* screen will open indicating the links to set up your system:



Welcome Screen

Activating *System302*

Click **Licenses** to run the ***Get License Info*** application.

If ***System302*** uses a *Soft Key*:

1. Click the button **Generate Fax-Back** and fill the form with the required information.
2. Select the applications that will use the *License Keys*. Click the button **Finish** to conclude and a dialog box will open indicating the *FaxBack.txt* file was generated successfully.
3. Click **Ok** to open the FAX-BACK file, print it and fax this form to Smar using the fax number indicated on the file.
4. Smar will issue the user a *License Key* to authorize the installed products.
5. On the ***Get License Info*** application, type the license key for each application and then click the button **Grant License Keys**.

If ***System302*** uses a *Hard Key*:

6. Connect the *Hard key* to the computer's USB port or parallel port.
7. On the ***Get License Info*** application, click the button **Hard Key Diagnostic** to check if the *Hard Key* is connected correctly.
8. Click **Exit** to conclude.

DCOM Configuration

The DCOM properties are configured in the *Component Services* window. Refer to the section **Configuring the DCOM properties** above for details on how to configure the DCOM properties for ***Studio302*** groups.

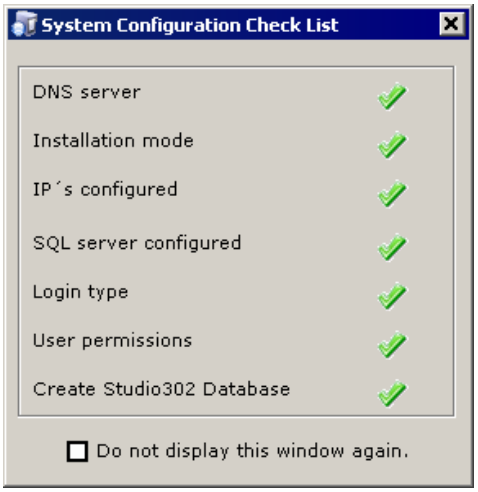
After configuring the DCOM properties, mark the option **DCOM already configured** in the *Welcome Screen*.

Configuring the System

NOTE
In case you have any doubts about the configuration, click the option **Tutorial** at the bottom of the **System Configuration** dialog box to run the configuration tutorial for ***Studio302***, which graphically shows the instructions and configuration examples.

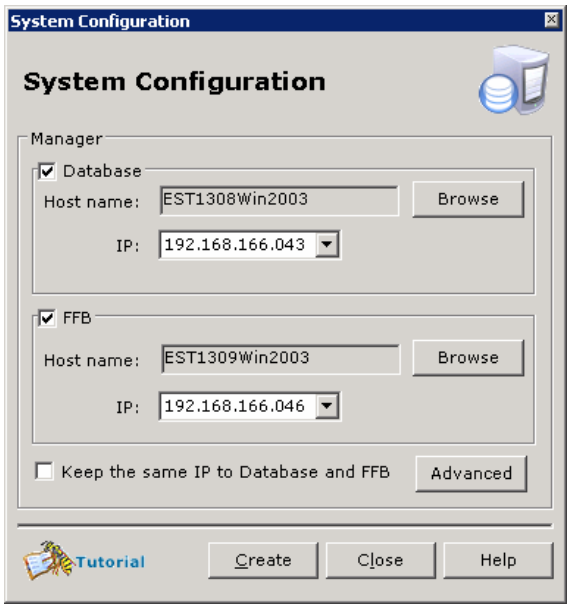
Once the ***System302*** applications are properly licensed, configure the system to execute these applications.

1. Click the link **System Configuration** to open the **System Configuration** dialog box to configure your local machine with the IP addresses of the *Managers*.
2. ***Studio302*** will verify if previous settings on the current machine are correct and indicate the steps during this verification in the **Check List** dialog box. If one step fails during the verification procedure, a red cross will appear and corrective actions must be taken. Click the link related to the step that failed on the **Check List** dialog box for details.



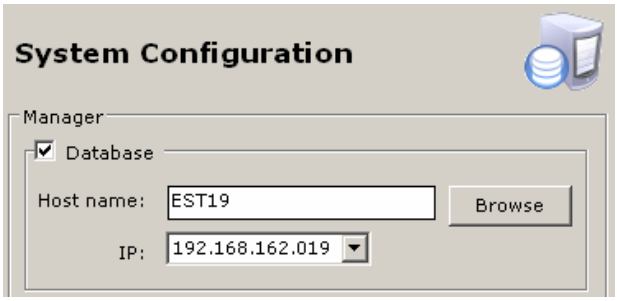
Check List

3. When all steps are executed successfully, you can start configuring the system:



Configuring the Operational System

4. Select the IP address used by the *Database Manager* in the local machine (if you have more than one NIC adapter) or click **Browse** to select the name or IP address of the remote machine where the *Database Manager* is installed.



Configuring the Database Manager

5. If the *Database Manager* and the *FFB Manager* are installed on the same machine, mark the option **Keep the same IP to Database and FFB**. Otherwise, select the IP address used by the *FFB Manager* in the local machine (if you have more than one NIC adapter) or click **Browse** to select the name or IP address of the remote machine where the *FFB Manager* is installed on the network

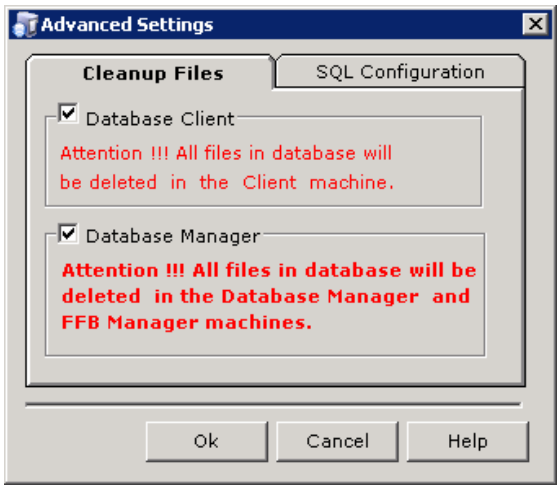
NOTE

Check the IP address configured in the *FFB Manager* application: double-click the icon on the Windows taskbar to open the *FFB Manager* application.

The IP address and server name must be the same configured in the **System Configuration** dialog box. To change the settings in the *FFB Manager* application, click the button **Configuration**, check the option **Change Host IP Address** and copy the IP address defined in the **System Configuration** dialog box. Click **Ok** to conclude and restart the *FFB Manager* to apply the changes.

6. Click the button **Advanced** in the **Manager** area to open the **Advanced Settings** dialog box.

   i. At the **Cleanup Files** tab, check the options to delete all files in the Client database and the Server database.



Deleting Database Files

   ii. At the **SQL Configuration** tab, type the communication port number for SQL data and type the SQL Server name on the network, or click the **Advanced** button to locate the remote server. At the **Process Equipment Database** tab, check the option to delete all previous information about specific instruments attributes, such as links to documentation files and instrument images.

   iii. Click **Ok** to return to the **System Configuration** dialog box.

ATTENTION
It will be necessary to configure the firewall in order to use a remote SQL Server, because the system configuration tool will establish a TCP/IP connection. Refer to the ***Server Books Online*** of the ***SQLServer*** application for further details on how to use a remote SQL Server.

7. Click **Create** at the bottom of the **System Configuration** dialog box. The procedure to create the database may take a few minutes. Wait until a message box appears informing that the database was created successfully. Click **Ok**.
8. Click **Close** on the **System Configuration** dialog box to conclude.

Opening and Closing System302 Tools

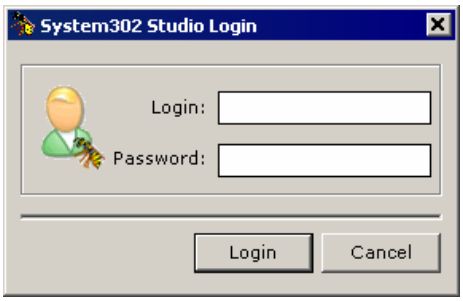
All ***System302*** tools installed according to the *Installation Mode* selected by the user are available in the **Application** toolbar, in ***Studio302***.

After validating the *License Keys*, configuring the system and creating the *Database*, click the link **Launch Studio302 now**.

If the option **Do not display this window again** is selected, the *Welcome Screen* will not be displayed when the user starts the ***Studio302*** application. The user can change this configuration in the **File** menu, selecting the option **Preferences**. Refer to the section **Defining User's Preferences** in the ***Studio302 User's Manual***.

If **Security Management** was enabled during the ***System302*** installation, users must log in every time the ***Studio302*** is initialized. ***Studio302*** incorporates Windows User Groups. Windows' users can log to ***Studio302*** using the same login name and password configured for the operational system.

The **Login** dialog box will open:



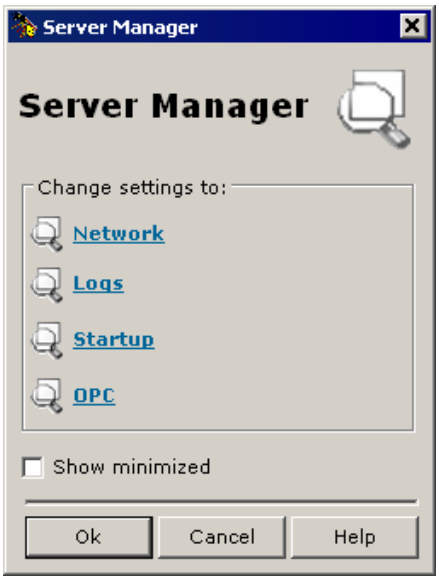
User Login

Type the user's login and password and click **Login**. Click **Cancel** to cancel the login procedure. The ***Studio302*** application will close.

Configuring the Network Settings

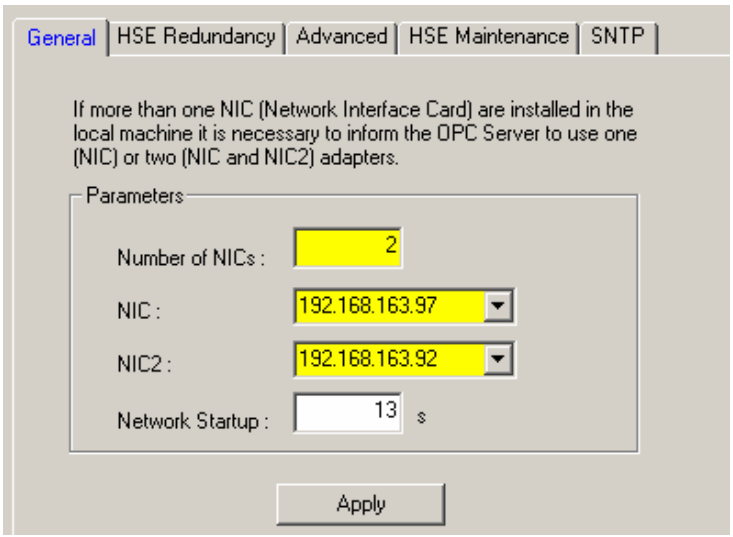
Before starting the ***System302*** online communication, it will be necessary to configure the Network parameters using the ***Server Manager*** application.

On the ***Studio302*** window, click the button  on the toolbar to execute the ***Server Manager*** application.



Server Manager Options

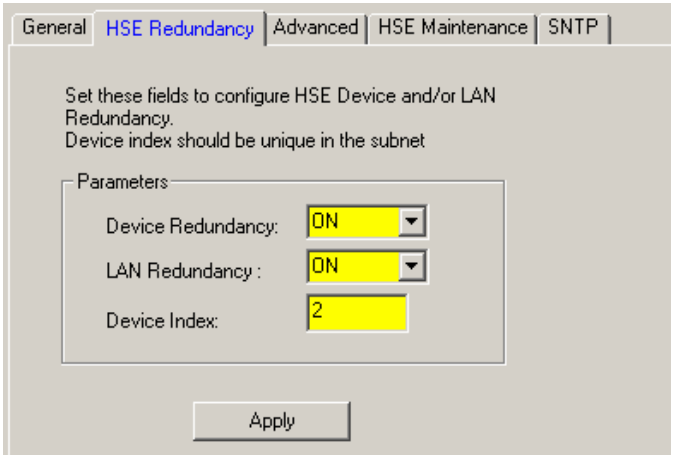
Click the link **Network** to open the ***Server Manager*** window on the **Network > General** tab.



Server Manager: General Tab

- Set the number of NICs to be used by the ***Server Manager*** in the HSE Network (type **1** if the system is not redundant or type **2** for a redundant system).
- Type the IP addresses of the NICs used by the ***Server Manager***.

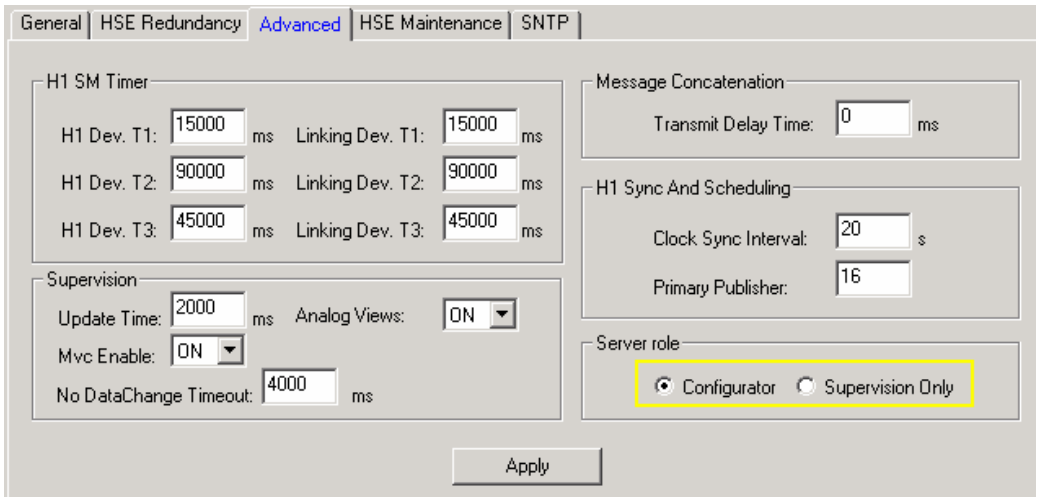
If your system is redundant, select the **HSE Redundancy** tab and configure the following parameters:



Server Manager: HSE Redundancy Tab

- Set the **Device Redundancy** and **LAN Redundancy** values to **ON**.
- At the *Device Index* text box, type a value between **1** and **9** for each machine, and every machine must have a unique number. In the HSE network, the *Device Index* represents the network address for each equipment, therefore if the values are not unique for each machine, the network redundancy will not work correctly.

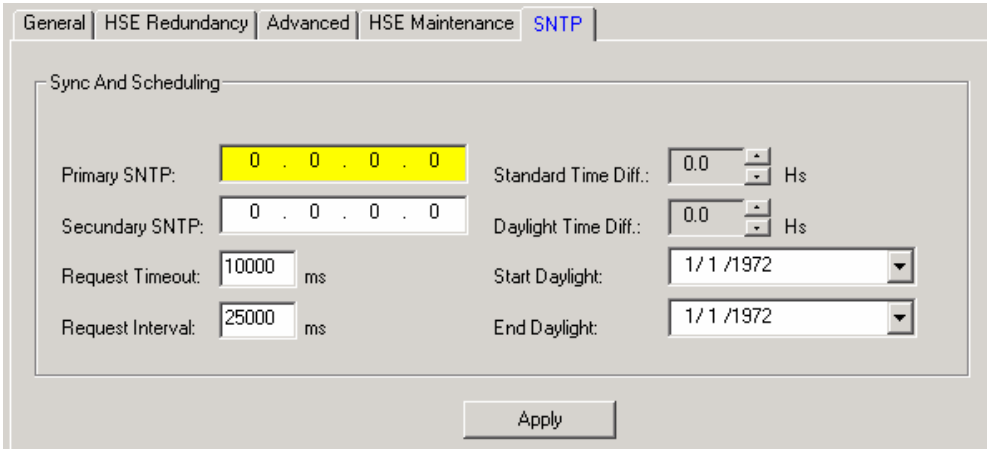
Select the **Advanced** tab and configure the following parameters:



Supervision

- Mark the option **Configurator** only for the machine where the plant configuration files are created. For the other machines where ***System302*** is also installed, mark the option **Supervision Only** to indicate that they are acting in supervision mode only.

Select the **SNTP** tab and configure the following parameter:



Synchronization

- Set the IP addresses of the SNTP Servers. If there is only one SNTP Server, type the **Primary SNTP Time Server** address and leave the **Secondary SNTP Time Server** address blank. If the machine where the SNTP Server is running has more than one NIC, you may choose an alternative IP as the **Secondary** address as long as both IPs are reachable on the network. Contact the *Information Technology Administrator* and request the SNTP time server addresses available for the system.

NOTE
The time interval that controls the message concatenation in HSE controllers is configured at **Transmit Delay Time**. This value depends on the macrocycle calculated by ***Syscon*** and therefore this option should be configured after the plant configuration project is created in ***Syscon***. Refer to the appendix about ***Server Manager*** in **Studio302 User's Manual** for more details.

Click **Apply All** to confirm the alterations and exit ***Server Manager***. The changes will take effect after re-starting the ***Server Manager***.

IMPORTANT
When closing the ***Server Manager*** application, wait a few seconds before initializing it again. This way, the list of processes executed by the operational system will be updated and the ***Server Manager*** application will be removed from this list. If the user tries to execute the ***Server Manager*** right after closing the application, the ***Server Manager*** icon will not appear on the Windows taskbar because the process will be still active on the list of processes.

Known Problems and Limitations

MB700 - Syscon configurations created with capability file (CF) version "03xxxx" may lose MB700 blocks when opened in Syscon version 6.00.00.xx or higher, or in System302 6.1.9 or higher.

Workaround:

a. Rename the CF 03xxxx located in "<System302 installation path>\Device Support\000302\0012". For example, change "030101.cff" to "030101.old".

b. Copy the CF 03xxxx used in the original project configuration to the folder mentioned in item a.

c. Open the ***Syscon*** configuration file used in ***System302*** 6.1.9 or higher.

d. Create a new bridge, MB700, using DD version 04xxxx.

e. Move the blocks from the original MB700 to the new MB700 you have just created.

f. Delete the original MB700 bridge, save the configuration file and close ***Syscon***.

g. Delete the original CF 03xxxx you have copied in item b.

h. Rename the CF "030101.old" (from item a) back to "030101.cff".

System302 operates in Multi-User mode but it is necessary to configure the server machine where the Database Manager will be executed. When a problem occurs in the network, the connection between the server and the clients can be lost. The current System302 version does not have a recover schema for these connections and when the communication is lost, the user has to restart the Database Manager and, after that, restart all Smar applications in the client machines. Only then the connections will be reestablished and the system will operate normally. For future versions, a schema for automatic re-connection will be developed to solve this problem.

Workaround:

Restart the Database Manager and, after that, restart all Smar applications in the client machines. The connections will be reestablished and the system will operate normally.

When operating in multi-user mode, the Database Manager might freeze. In this case, the client machines connected to this Database Manager freeze too. This problem occurs when the Database Manager is closed and re-opened without restarting the client machines. The correct procedure is to start the Database Manager before starting the client machines. If a client machine is already open, this machine will not establish the connection to the Database Manager when it is initialized. Use the procedure described in the previous item to solve this problem.

Workaround:

Restart the Database Manager and, after that, restart all Smar applications in the client machines. The connections will be reestablished and the system will operate normally.

If System302 and AssetView are installed in a non-English Windows version, it will be necessary to configure the DCOM properties manually.

Workaround:

a. On the **Start** menu, click **Run**, type **dcomcnfg** and click **Ok**.

b. On the **DCOM Config** dialog box, right-click the component* **AssetView** and click **Properties**.

c. At the **Identity** tab, select the option **The Interactive User**.

d. At the **Security** tab, select the options to use the default permissions.

e. Click **Ok** to conclude.

* Repeat steps b to e for each ***AssetView*** component listed below:
  - Smar OPC & Conf Server for DFI302;
  - Smar OPC & Conf Server for HSE;
  - SmarAXERefresh;
  - SmarChart;
  - SmarChartTimerOPCComm;
  - SmarChartWrite;
  - SmarDiagnostic;
  - SmarTimerDataChange;
  - AVTerminal.

MSDE was not installed during the System302 Installation.
There may be a previous MSDE installation on your machine and for that reason it was not re-installed by the System302 Installation Procedure. However, the previous installed MSDE may not be compatible and therefore the user is not able to select the Smar database.

Workaround:

The first step is to follow the procedure describe on the *Microsoft Help and Support Web Site* at http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q317328 and troubleshoot the MSDE installation.

If the information described on the *Microsoft Help and Support Web Site* did not solve the MSDE problem, analyze the log files generated by the MSDE installation located on the MSDE installation folder.

If the two steps above did not solve the problem yet, try to install the MS SQL Server instead of using MSDE.

ATTENTION
When neither the options are successful, please try to reinstall the *Service Pack* used by the Windows OS. It might even be necessary to reinstall the operational system.

When the Engineering Station executes a device or bridge download, the supervision is deactivated in every Station, including the Supervisory Station.

Workaround:

The *Engineering Station* informs the *Supervisory Stations* that a device or bridge was downloaded, and the *Supervisory Stations* should read the profile again to update the local databases, therefore the supervision is deactivate while reading the device or bridge profile.

If the current configuration station – where the configuration HSE Host is being executed – is replaced or another machine is selected as the configuration station, it will be necessary to update the profiles of all devices and bridges.

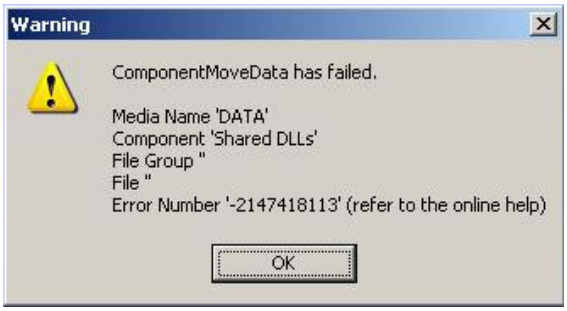
The value of the macrocycle edited by the user was modified by *Syscon*.

Workaround:

When the configuration project is edited, for example, when the user removes or adds a function block or link to a fieldbus channel, ***Syscon*** automatically calculates the macrocycle value, and if this new value is higher than the value previously defined by the user, ***Syscon*** will automatically overwrites the macrocycle value.

Refer to the **Syscon User's Manual** for further details about configuring the macrocycle.

Eventually, in some stations, the *Network Configuration* is not installed because a shared dll is being used by another software installed on the same machine. In some cases, the message in the example below appears. Or a message alerting about a failure during the installation will only appear when the *Network Configuration* is executed for the first time.



Workaround:

In the Windows **Task Manager** window, end all tasks and processes that do not affect the system operation. Only essential Windows tasks will still be executed.

Install the ***Network Configurator*** using the procedure below:

1. Insert the ***System302*** Installation DVD into your DVD-ROM drive and select the option **Browse this DVD**.
2. Locate the folder **Tools > NetConf**.
3. Run the file **Setup.exe**, double-clicking its icon.
4. Run the ***Network Configurator*** again using ***Syscon***, selecting the option **Modify Profibus Configuration**, in the *Profibus* channel.

Syscon does not automatically interpret as strings the new diagnostic values for the parameters RED_PRIMARY_BAD_CONDITIONS and RED_SECONDARY_BAD_CONDITIONS from the TRDRED function block, for firmware version V1_2_15 or higher.

Workaround:

New diagnostic values for the parameters RED_PRIMARY_BAD_CONDITIONS and RED_SECONDARY_BAD_CONDITIONS, from the TRDRED function block, were included from firmware version DF62/63/75-V1_2_15 on.

When the conditions that indicate these new values occur, they are interpreted as strings, according to the ***DFI302 User's Manual***, Section 20, Table 20.1.

If the firmware version V1_2_15 or higher is being used with a ***System302*** version previous to version 7.0.6, these new values will not be automatically interpreted as strings by ***Syscon***, but as hexadecimal values. Refer to the ***DFI302*** Manual mentioned above for further information on how to interpret these values.

Contacting Smar

Technical support for ***System302*** is provided by our award-winning Customer Support Web Site. From this Web site, customers are able to review Frequently Asked Questions, submit and check the status of support requests, and access online documentation, patches, and other downloads. Please visit the Customer Support Web Site at www.smar.com.

Appendix A

BACKING UP PROJECT CONFIGURATION FILES

System302 versions are classified in two scenarios: ***System302*** versions with integrated tools managed by ***Studio302***, and ***System302*** versions before the integration. The reference ***Integrated System302*** refers to Versions **7.0**, **7.1** and **7.2**.

Users from previous versions of ***System302***, that is, versions prior to the integration, should execute specific procedures to convert the configurations created on those versions to **Version 7.2.2**. Follow these steps **BEFORE** you uninstall ***System302*** to backup project configuration files and restore them after installing ***System302*** **version 7.2.2**.

System302 Versions Prior to Version 7.0

System302 tools are not executed from ***Studio302*** in versions prior to Version 7.0. ***Syscon*** manages all data for configuration files. You have two options to create backup files and restore project configuration files:

a) Copy and import configurations manually:

Copy the project folders created by ***Syscon*** to a temporary directory, such as *C:\temp.* Uninstall the old ***System302*** version and install **Version 7.2.2**.

Run ***Studio302***, go to the **File** menu, select **Import** and click **Syscon file**. The dialog box to import the configuration file will open. Locate the configuration file in the temporary directory, select the file icon and click **Open**.

Syscon will open while the configuration is added to ***Studio302***. A message box will open informing that the configuration was imported by ***Studio302***, indicating the corresponding *Database*. Click **Ok** to close the message box and return to ***Studio302***.

b) Execute the Pack and Unpack procedures in *Syscon*:

Open the project configuration in ***Syscon***. On the **Project File** menu, click **Pack Project**. A dialog box will open warning the user to check if the **Device Support** has all of the DDs and CFs files used in the project. If the files are correct, click **Ok** to continue.

Select the directory where the project package folder or the compacted file will be created and click **Ok**. A message box will appear informing the user if the operation was successful. Click **Ok** to conclude.

Uninstall the old ***System302*** version and install **Version 7.2.2**.

Run ***Studio302*** and click the button  on the toolbar to run ***Syscon***. Using ***Syscon***, go to the **Project File** menu and click **Unpack Project**. Select the directory where the backup package was saved and click **Ok**.

A dialog box will open to select the directory where your project configuration files will be unpacked and saved. Select the desired directory and click **Ok**. A message box will appear informing the user that the operation was successful. Click **Ok** to conclude.

Using ***Studio302***, go to the **File** menu, select **Import** and click the option **Syscon file**. The **Import Syscon file** dialog box will open. Browse the directories to locate the configuration file, select the file icon and click **Open**.

A message box will open informing the user that the configuration was imported in the ***Studio302***, indicating its corresponding *Database*. Click **Ok** to conclude.

System302 From Versions 7.0 On

From ***System302 Version 7.0*** on, run ***Studio302*** and click the button  on the main toolbar to open the **Pack & Go** dialog box. Select the mode to pack the files (**Full**, **Light** or **Customized**) and click **Create**. Refer to the **Studio302 User's Manual** for details about the **Pack** procedure.

Select the path to the destination folder, type the name for the package and click **Ok**. The procedure to pack all files selected may take a few minutes. A message box will appear informing the user if the operation was successful. Click **Ok** to conclude.

Uninstall the old ***System302*** version and install **Version 7.2.2**.

Run ***Studio302*** and click the button  on the main toolbar to open the **Unpack** dialog box. At the **Select a file to unpack**, click **Browse** to locate the compacted file. Click **Ok** to return to the **Unpack** dialog box

At the **Select the temporary path to extract the files**, click **Browse** to and select the directory where the compacted file will be extracted Click **Ok** to return to the **Unpack** dialog box.

Click **Unpack** on the **Unpack** dialog box to extract the files. A message box will appear informing the user that the operation was successful. Click **Close** to conclude.

On the ***Studio302*** window, click the **Areas** icon in the topology tree to open the **Area** dialog box. The icon of the areas corresponding to the project configurations that were unpacked indicates that the **Upgrade** procedure should be executed; otherwise the user will no be able to work with the configurations.

Right-click the area icon and select the option **Upgrade**. ***Syscon*** will automatically open to update the information related to the configuration.

RECOVERING THE SYSTEM WHEN A FAIL OCCURS

Case 1: Server (Database Manager) with no backup

If your plant does not have a backup server, Smar strongly recommends some preventive actions to assure the data integrity on your plant.

The first step is to execute the **Commit** procedure for the project files to save the alterations in the server, every time the configuration is edited or updated. This way, the latest alterations in the configuration will be certainly saved in the server.

In addition to the first step, it is strongly recommend for the server station to implement a data storage scheme to replicate data among hard drives, also known as *RAID1*. This technology is usually applied when operating with file servers. A data storage scheme copies all the information sent to the first hard drive in the second hard drive. Therefore, if one of the HDs fails, the other will promptly execute the operation and provide the information for the processes.

Contact the IT administrator for details about this functionality.

Case 2: Communication Settings blocked in *View Mode*

Although this scenario has a remote chance of occurring, follow the procedure below when all data from a workstation in *Edit Mode* is lost because of physical damages in the computer, in a multi-user system. A new station will be used with no interruption to the plant operation while the old station is being repaired.

To assure the data integrity and continue operating properly, execute these steps on the workstation that will be used to edit the configuration:

i. Run the ***Server Manager*** application, click the option **Network** and select the **HSE Maintenance** tab.

ii. Click **Delete** to delete the HSE persistency files. This option is only available for administrators or users in the Administrators group.

iii. Run ***Syscon***, go to the **Communication** menu and click the option **Settings**.

iv. A message box will open to inform the user that the alteration will not be saved or persisted in the configuration. Click **Ok** to confirm.

v. In the **Server context** box, select the option **Local**.

vi. The system will be restored and ready to continue the maintenance/configuration.

ATTENTION
If the user chooses to use an OPC Server from a remote machine instead of the machine defined above, select the option **Remote** in the **Server context** box, and select the name of the remote machine, from where the OPC Server will be accessed, in the **Node Name** box.

Appendix C

SECURITY PRACTICES FOR NETWORK ADMINISTRATORS IN SYSTEM302 V7.2 ENVIRONMENT

This document gathers a list of common practices for configuring, managing and operating control networks where ***System302*** is installed. Following these practices will assure the ***System302*** functionalities in an environment requiring access restrictions to the communication network and to files/directories.

It is important to remember that this list of common practices includes the minimum requirements when there are some restrictions to use the operational system resources properly.

Use this document as a security guide to install ***System302*** without violating the security policy defined by the IT management. The goal is to provide the necessary information to configure the operational system to allow the communication between ***System302*** and the infra-structure defined by the operational system in regard to the security policy.

The following information will be provided:

- Files and Directories: dynamic files used by ***System302*** in normal operation, that is, files and directories that should not be scanned by antivirus tools when written or altered.
- Registry and Services: type of access for application files and registers, and services that should be enabled to execute ***System302***.
- Firewall: necessary configurations to execute the applications when a firewall is enabled.
- TCP and UDP ports: specific ports used by ***System302*** and the scope, that is, the group of computers on the network that should have permission to access those ports.
- Privilege level: levels of privilege necessary for proper operation.

Files and Directories

Every user configuring, operating and executing maintenance in the ***System302*** environment must have access permissions to the Smar directory and sub-directories. The default path to the Smar directory is:

- operational system in English: `C:\Program Files\Smar`
- operational system in Portuguese: `C:\Arquivos de programas\Smar`

The table below shows ***System302*** applications and files located in the Smar installation folder, and the corresponding type of access for each file, for example, if a file is ready-only, it cannot be changed or accidentally deleted.

Application	File Name	Operation
Studio302	Studio.mdf	RW
	Studio_log.LDF	RW
	SmarStudio\bin\XmlFiles	RW
	SmarStudio.exe	R
	SmarStudioBridgeProxy.exe	R
	SmarStudioLicenses.exe	R
	SmarWatcher.exe	R
	SSSDetectDevice.exe	R
	SMARProxyAE.exe	R
	SmarMonitorRegister.exe	R
	SqlServer.exe	R
	register.bat	RW
	Frames.txt	RW
	IP.C33	RW
Syscon	Syscon.ini	RW
	Syscon.dat	RW
	Block Support	RW
	Device Support	RW
	TagInfo.ini	RW
	OFC Logger	RW
LogicView	LogicView	RW
	LVDownloaderCOM.dll	RW
	Define Parameter Tool	RW
	FFB Manager	RW
Get License	OleServer.dat	RW
	DFIOleServer.dat	RW
	Syscon.dat	RW
	LogicView.dat	RW
	Studio.dat	RW
	LicenseManager.ini	RW
Database Manager	C:\Program Files\Smar\ConfigurationWorkspace\Server	RW
	C:\Program Files\Smar\ConfigurationWorkspace\properties	W
	C:\Program Files\Smar\ConfigurationWorkspace	W
	C:\Program Files\Smar\ConfigurationWorkspace\CWTraceFiles	W
Database Client	C:\Program Files\Smar\ConfigurationWorkspace\Server	W
	C:\Program Files\Smar\ConfigurationWorkspace\properties	W
	C:\Program Files\Smar\ConfigurationWorkspace	W
	C:\Program Files\Smar\ConfigurationWorkspace\CWTraceFiles	W
	C:\Program Files\Smar\Device Support	W
	C:\Program Files\Smar\Block Support	W
	C:\Program Files\Smar\FFB Support\Instances	W
Server Manager	Smar OleServer.ini	RW
	IDShell HSE.ini	RW
OPC A&E Server	TagConv.aev	RW
OPC Servers	register.bat	RW

Application	File Name	Operation
OPC Servers (DFI, HSE, AE, PCI)	Smar OleServer.ini	RW
	TagInfo.ini	RW
IDShell HSE - HOST	IDShell HSE.ini	RW
IDShell HSE P2 - HOST	IDShell HSE.ini	RW
AssetView	C:\Program Files\Smar\AssetView\bin\CSVErrors.Log	RW
	C:\Program Files\Smar\AssetView\bin\TerminalProblem.txt	RW
	C:\Program Files\Smar\AssetView\bin\DebugFile.txt	RW
	C:\Program Files\Smar\AssetView\bin\AVDebug_PageCommunication.txt	RW
	C:\Program Files\Smar\AssetView\bin\AVDebug_Tracking.txt	RW
	C:\Program Files\Smar\AssetView\bin\AVDebug_Register.txt	RW
	C:\Program Files\Smar\AssetView\bin\AVDebug_Tracking_View.txt	RW
	C:\Program Files\Smar\AssetView\bin\AVDebug_DiagnosticView.txt	RW
	C:\Program Files\Smar\AssetView\bin\AVDebug_Scheduling.txt	RW
	C:\Program Files\Smar\AssetView\bin\AVDebug_Maintenance.txt	RW
	C:\Program Files\Smar\AssetView\bin\AVDebug_EMail_Service.txt	RW
	C:\Program Files\Smar\AssetView\bin\AVDebug_Other.txt	RW
	C:\Program Files\Smar\AssetView\bin\AVDebug_Error.txt	RW
	C:\Program Files\Smar\AssetView\bin\AVDebug.txt	RW
	C:\Program Files\Smar\AssetView\bin\LastDeviceRegistered.txt	RW
	C:\Program Files\Smar\AssetView\bin\ShutdownReport.txt	RW
	C:\Program Files\Smar\AssetView\bin\CheckRunningProcessLog.txt	RW
	C:\Program Files\Smar\AssetView\bin\AssetServerEventLog.txt	RW
	C:\Program Files\Smar\AssetView\bin\smarAVMaintenance.log	RW
	C:\Program Files\Smar\AssetView\bin\smarAVSchedule.log	RW
	C:\Program Files\Smar\AssetView\bin\smarAVScheduleSvc.log	RW
	C:\Program Files\Smar\AssetView\SQLServer Support\StuffDatabase.log	RW
	C:\Program Files\Smar\AssetView\SQLServer Support\AssetBuildSQL.sql	R
	C:\Program Files\Smar\AssetView\Web Pages\FalhaLogin.log	RW
	C:\Program Files\Smar\AssetView\Web Pages\FalhaVarSessao.log	RW
	C:\Program Files\Smar\AssetView\bin\SmarAssetView.ini	RW
	C:\Program Files\Smar\OleServers\tmp_AlarmInfo.ini	RW
	C:\Program Files\Smar\OleServers\AlarmInfo.ini	RW
	C:\Program Files\Smar\OleServers\AVAlarmInfo.ini	RW
	C:\Program Files\Smar\OleServers\AVAlarmInfo_tmp.ini	RW
	C:\Program Files\Smar\OleServers\IDShell HSE.ini	RW

Legend:
R: Read Only
W: Write Only
RW: Read and Write

Registry

The table below shows the register keys configured in the operation system during the ***System302*** installation procedure, and the corresponding access rights. For example, if the register is ready-only, it cannot be changed or accidentally deleted.

Application	Register Key Name	Operation
Syscon	HKEY_CLASSES_ROOT\Smar.Support	RW
	HKEY_CLASSES_ROOT\Syscon.Application	RW
	HKEY_CLASSES_ROOT\Syscon.Document.1	RW
ProfibusView	HKEY_LOCAL_MACHINE, "Software\Smar\System302", "Location"	R
AssetView	HKEY_LOCAL_MACHINE\SOFTWARE\Smar\AssetView\	RW
	HKEY_CLASSES_ROOT\CLSID	RW
AssetView FDT	[HKEY_LOCAL_MACHINE\SOFTWARE\Smar\AssetViewFDT]	R
DF73 Communication DTM	[HKEY_LOCAL_MACHINE\SOFTWARE\Smar\DTMs\DF73CommDTM]	R

Legend:
R: Read Only
RW: Read and Write

Services

This section provides information about which services must be enabled by the IT team to run ***System302*** applications properly.

Application	Service Name
AssetView	Smar AssetView Schedule

Environment Variables

The table below lists the system environment variables defined during the ***System302*** installation procedure, for any user logged on to the computer.

Variable Name	Value
SmarOlePath	C:\Program Files\Smar\OleServers\

Firewall

If it is necessary to enable the firewall for the operational system, refer to the ***System302 Installation Guide*** for further details on how to configure the firewall properly.

Attention

Smar strongly recommends using a control network (the network where controllers and workstations used to configure, operate and manage the plant are connected) separated from the corporative network, so that there will be no risk of losing the functionality in case the network security is not configured properly.

TCP and UDP Ports

The table below shows the ports used by ***System302*** that should be unblock for proper system operation:

Description/Type	TCP/IP	UDP
Configurable *****	80 1024:5000 1089 2421 2422 2423 12423 12422 12421 23500 29021 29022 38080	from 28000 1089 1090 1091 3622
Additional Ports	12425 12426 12427 12428 12429 12430 12432 12431 12433 12434 12435 12224	502 6972 7580
SQL Server Access Ports	1112 1433	1434
Dynamically Allocated Ports	135	• For H1 captures (used by ***FBView***) • For client/server HSE communication (used by the OPC HSE Server, as well as HSE devices)
Reserved for Smar ******	4987 4988	4987 4988
https support (when using ***AssetView***)	443	NA

(*****) Configurable ports must not be altered without previous consultation and recommendations from Smar.
(******) According to IANA (*Internet Assigned Number Authority*), available at:
http://www.iana.org/assignments/port-numbers

Privilege Levels

The necessary levels of privilege for ***System302*** are divided in two groups:

Installation

Only the *Local Administrator* or a user in the *Administrators* group can install ***System302***, even if the system is operating in a domain.

Operation

Any user can access the ***System302*** tools and functionalities, according to the respective access permissions for the Smar directory configured for each user.

Windows Updates

It is not recommended to enable Windows updates or *Hotfix*. Smar recommends updating the operational system only when a new *Service Pack* is officially release by Microsoft, previously consulting your Smar representative to confirm ***System302*** compatibility.

Antivirus

The Smar directory should not be scanned by antivirus tools. If ***System302*** performance is lost when executing an antivirus, it is recommended to disable the antivirus.

Refer to **Appendix D** on this guide for further information about installing antivirus tools with ***System302***.

Backup

System302 can provide the user with a backup copy of the configuration projects through ***Studio302***, using the **Pack & Go** procedure.

Besides the backup functionality, this procedure will pack project files related to the configuration in a single file, allowing the user to transfer this configuration to another workstation.

For further details about this procedure, refer to **Section 7** on the ***Studio302 User's Manual***. Run this procedure every time there is a significant alteration in the project configuration.

Smar recommends creating the backup copy using the **Pack & Go** procedure, so that the user will always have the latest information and status related to the plant configuration.

Details About Ports Used by System302

The table below shows detailed information related to the ports used by each ***System302*** tool.

Component	TCP/IP Ports	UDP Ports	Additional Ports
Studio302	1024:5000	1434	NA
OPC Servers	135 (Dynamically Allocated Port)	NA	NA
Database Manager	Configurable: 12423, 12422	NA	NA
Database Client	Configurable: 12421	NA	12430:12450
AssetView	80 (IIS) 443 (https support)	NA	NA
FBView	NA	7580, 502, 6972	Dynamically allocated ports for H1 capture
FBTools	4987, 4988 (reserved for Smar)	4987, 4988 (reserved for Smar)	NA
FFB manager	TCP (Configurable): 23500	TCP (Configurable): 23500	(TCP/UDP) Reserved for Smar: 4987, 4988
HSE Server	Configurable: 29021, 29022	From 28000 (Configurable), 1089, 1090 and 1091, 3622 (Configurable)	Dynamically allocated ports for client/server HSE communication
ProcessView	38080	NA	NA

Appendix D

SYSTEM302 & ANTI-VIRUS INSTALLATION

This section describes how to install and configure anti-virus software tools to be used with ***System302***. It is very important to follow all instructions described here in order to guarantee the correct operation of ***System302*** and the plant.

Anti-virus software can identify and block many viruses before they can infect your computer. Once you install anti-virus software, it is important to keep it up to date.

Although details may vary between packages, anti-virus software scans files or your computer's memory for certain patterns that may indicate an infection. The patterns it looks for are based on the signatures, or definitions, of known viruses. Virus authors are continually releasing new and updated viruses, so it is important that you have the latest definitions installed on your computer.

This guide provides information to install and configure the following anti-virus software, which have already been tested with ***System302***:

- Norton Antivirus 2008 with anti-spyware
- McAfee Total Protection with Site Advisor Plus

When using other software tools, it is **not** recommended to scan Smar directory with the antivirus.

IMPORTANT
Scanning your computer for viruses and spyware uses some of the available memory on your computer. If you have multiple programs trying to scan at the same time, you may limit the amount of resources left to perform your tasks. If ***System302*** performance seems to be running slowly when executing an antivirus, it is recommended to disable the antivirus.

The sections below describe all settings necessary for the anti-virus software mentioned above.

Before the Installation

Before installing your antivirus software, make sure the requirements related to the Operational System in the target machine are fulfilled. Refer to section **System Requirements** in the ***System302 Installation Guide*** for details.

Install ***System302*** only after completing the anti-virus software installation.

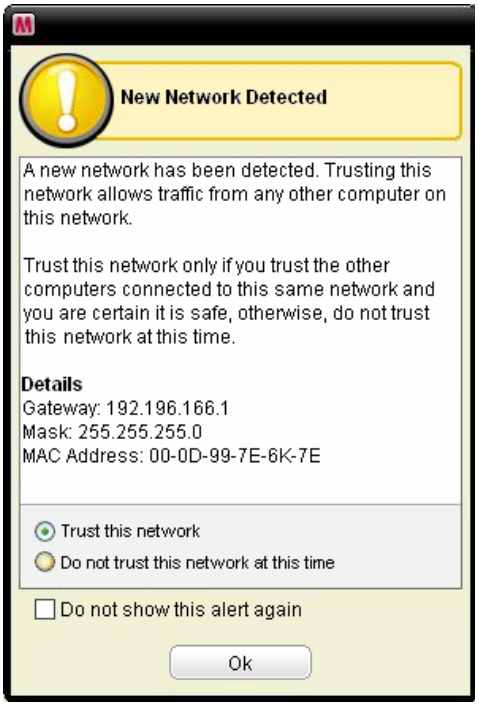
McAfee Total Protection with Site Advisor Plus

Installing McAfee

1. Insert the McAfee installation CD into your CD-ROM drive. Once the installation starts, select the **Complete** installation type.

Selecting the Installation Type

2. Select the option to install the version from CD.
3. Select the **EasyNetwork** installation mode.
4. When a new network is detected, enable communication selecting the option **Trust this network**.



Configuring a New Network

5. After the installation is finished, double-click the icon **McAfee** to run the application.
6. Click the option **Fix** to enable all security options for the anti-virus software.

Security Options

Installing SYSTEM302

1. it is necessary to disable the option **SystemGuards** to prevent McAfee from blocking the register of **Crystal Report** installation, during ***System302*** installation. Open the **McAfee SecurityCenter**, select the option **Computers and Files** and click **Configure**:

Enabling System302 Installation

2. Disable **SystemGuards** selecting the option **Off**. This option may be enabled again after ***System302*** installation is complete.
3. Install ***System302*** according to the steps described on the **System302 Installation Guide**.
4. When the installation is complete, enable the option **SystemGuards** again, and all McAfee security options will be active.

System302 is totally compatible with McAfee, but some initial configurations should be done in operation mode.

McAfee generates alarms to the user when any software starts using TCP/IP communication or tries to change a Windows register.

It is recommended to allow events related to register alterations or TCP/IP communication according to the table below, which lists ***System302*** applications that are blocked by McAfee when executed for the first time:

Occurrence	Application	McAfee Warning
After installing ***System302*** and restarting the operational system	FnTypeWizard.exe	Internet Access
After installing ***System302*** and restarting the operational system	javaw.exe	Internet Access
Creating the database	SqlServer.exe	Internet Access
Initializing ***Studio302***	SmarStudioBridge.exe	Internet Access
Initializing ***Studio302***	SmarStudio.exe	Internet Access
Initializing ***Syscon***	Syscon.exe	Internet Access
Initializing communication	HseSvr.exe	Internet Access
Initializing communication	DfSvr.exe	Internet Access
Defining Parameters	FFBDefWizard.exe	Internet Access
Executing ***LogicView***	LVfoFFB.exe	Register Exchange *
Executing ***LogicView***	LVfoFFB.exe	Internet Access
Executing ***TagView***	TagView.exe	Register Exchange**
Executing ***FBView***	FBView.exe	Register Exchange***

(*) HKEY_LOCAL_MACHINE\SOFTWARE\Classes\LogicView.Document\shell\open\command\
(**) HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TagView.Document\shell\open\command\
(***) HKEY_LOCAL_MACHINE\SOFTWARE\Classes\FBView.Document\shell\open\command\

Norton Antivirus 2008 with anti-spyware

Execute Norton Antivirus 2008 with anti-spyware standard installation and after the installation is complete, enable all anti-virus functionalities, as indicated in the following figure:

Configuring the Anti-Virus Tool

Then, run ***System302*** installation and follow the steps described in the **System302 Installation Guide**. Your system will be ready to use.

System302 is totally compatible with Norton Antivirus 2008 with anti-spyware.

Scan and update recommendations

Scanning your system

Once the anti-virus is installed, it is recommended to scan the entire computer periodically.

- *Automatic scans*: depending on what software is installed on the local machine, it is possible to configure automatic scanning for specific files or directories, and also set intervals for complete scans. It is recommended to scan the computer every day, or periodically as defined by your IT manager.

- *Manual scans*: it is also recommended to manually scan files received from external machines before opening the files. This includes:

    - Saving and scanning e-mail attachments or files downloaded from websites rather than opening files directly from the source.

    - Scanning media, including CDs and DVDs, for viruses before opening any file.

Updating anti-virus software

It is recommended to configure anti-virus software to check for updates automatically. Instructions on how to configure automatically updates are available in the **Online Help** or **User's Manual** from the anti-virus software.