A CrossTec Corporation

Instructional Setup Guide

Activeworx Security Center

Quick Install Guide

PREPARED BY GARY CONKLE

Activeworx Basic Installation and Configuration Guide

---

500 NE Spanish River Blvd. • Suite 201
Phone 800.675.0729 • Fax 561.391.5820
www.CrossTecCorp.com

Table of Contents

Table of Contents 3
Abstract and Definitions 4
Abstract: 4
Definitions: 4
Activeworx Security Center Components 5
Activeworx Security Center Desktop 5
Activeworx Security Center Manager and Modules 5
DB Manager 5
System Requirements 6
Database System Requirements 6
Hardware 6
Software 6
ASC Desktop System Requirements 6
Hardware 6
Software 6
ASC Manager System Requirements 6
Hardware 6
Software 6
Configuration Steps 7
Download and Unzip Installation Package 7
Installing the Activeworx Security Center Components 7
Installing/Configuring Activeworx Security Center 7
Desktop Overview 21
Conclusion 22
Copyrights 22

Abstract and Definitions

Abstract:

This guide provides basic steps for the installation and initial configuration of Activeworx Security Center (ASC) software. It is not intended to provide complete instructions for a production environment. As each network is unique in nature, it is beyond the scope of this guide to cover every network configuration. However, after a basic configuration is completed, defining additional elements should be based on your network security and reporting requirements. After completing this quick install guide, please see the ASC Evaluator's Guide also included with the installation file for more in depth information on the use and features of Activeworx Security Center. This guide is for the purpose of installing the ASC Desktop and Manager only; it will step through the install and the initial Configuration Wizard. Additional configuration information can be found under the Help Menu option on the Activeworx Security Center Desktop and the Evaluator's Guide mentioned above.

Activeworx Security Center supports many different devices, operating systems and security software. For reference purposes, we will use the generic term "Assets" to refer to devices, operating systems and software. This group contains, but is not limited to:

Firewalls
VPN's
Anti-virus software
Vulnerability scanners
Intrusion detection systems
UNIX based operating systems
Windows based operating systems

Activeworx Security Center was designed to allow Network Security Administrators to create an environment where events from different assets could be brought together under one application. This gives security administrators the ability to quickly correlate events from different assets and analyze those events to help determine if their network is being compromised or misused.

Definitions:

1) **Asset** – Any product that will be monitored by the Activeworx Security Center application.

2) **Collector/Module** – A collector/module is a component of ASC Manager that runs as a service on a Windows based computer that collects and stores the events of the assets or runs scheduled tasks.

3) **Rules** – Any general expression which is used to determine if a packet meets predefined criteria for capture and logging.

4) **Manager** – A general purpose program that will run/manage one or more Collectors/Modules.

5) **Event(s) or Network Event(s)** – Any IP packet(s) captured because it met the dual requirement of being directed towards a defined asset and meeting any of the rules defined for that asset.

Activeworx Security Center Components

Activeworx Security Center consists of three basic components:

- Activeworx Security Center Desktop
- Activeworx Security Center Manager and Modules
- Database Manager (DB Manager)

Activeworx Security Center Desktop

Activeworx Security Center Desktop is the main control program of the application. It is used to define assets, collectors/modules, rules and in conjunction with the DB Manager, event databases. It also serves as a security console that provides the tools needed to monitor the various event types, create reports and graphs, create and schedule tasks.

Activeworx Security Center Manager and Modules

There are eight types of Activeworx Security Center Manager collectors/modules:

- ***Network Collector*** – Collects all Syslog and SNMP (***S****imple* ***N****etwork* ***M****anagement* ***P****rotocol)* events and forwards them to the database server for logging.
- ***Winlog Collector*** – Communicates with Windows servers via DCOM\WMI (***W****indows* ***M****anagement and* ***I****nstrumentation)* services and requests Windows event log messages and then forwards them for storage in the event database.
- ***Checkpoint Collector*** - Used to communicate with Checkpoint firewalls and consoles via OPSEC and forward events to the appropriate event database.
- ***Cisco-IDS*** – Acts as a read-only agent that collects IDS events from Cisco-IDS using RDEP.
- ***File Collector*** – Allows the importation of data from flat (text) files that come from almost any ASC supported device.
- ***Database Collector*** – Collects events from MySQL and/or MS SQL databases that various third-party software uses as back-end databases (e.g. SNORT, ISS Site Protector and stores them in ASC event databases.
- ***Correlation Engine*** – Uses user defined flowcharts of network events to create an event for storage in an event database and/or send an alert.
- ***Schedule Engine*** – Module that will run scheduled tasks.

DB Manager

Used to create Activeworx Security Center primary database, event databases, create users and grant authorities. DB Manager may be run from the Desktop from the Options menu or as a standalone program.

System Requirements

Database System Requirements

Hardware

The minimum hardware requirements are:

CPU :	Pentium 4 or later
Memory :	512MB or Greater
Available Disk Space :	500MB

Software

The minimum software requirements are:

Operating System :	Any OS that runs MySQL, Windows for MS SQL
Other Software :	MySQL 4.x or Higher, MS SQL 2000 or Higher

ASC Desktop System Requirements

Hardware

The minimum hardware requirements are:

CPU :	Pentium 4 or later
Memory :	512MB or Greater
Available Disk Space :	200MB

Software

The minimum software requirements are:

Operating System :	Microsoft Windows 2000/2003/XP
Other Software :	.Net Framework version 2.x

ASC Manager System Requirements

Hardware

The minimum hardware requirements are:

CPU :	Pentium 4 or later
Memory :	512MB or Greater
Available Disk Space :	200MB

Software

The minimum software requirements are:

Operating System :	Microsoft Windows 2000/2003/XP
Other Software :	.Net Framework version 2.x

Configuration Steps

Download and Unzip Installation Package

If not already completed, from the CrossTec web site (www.crossteccorp.com), download the installation package. After the download is complete, unzip the files into any available folder.

Installing the Activeworx Security Center Components

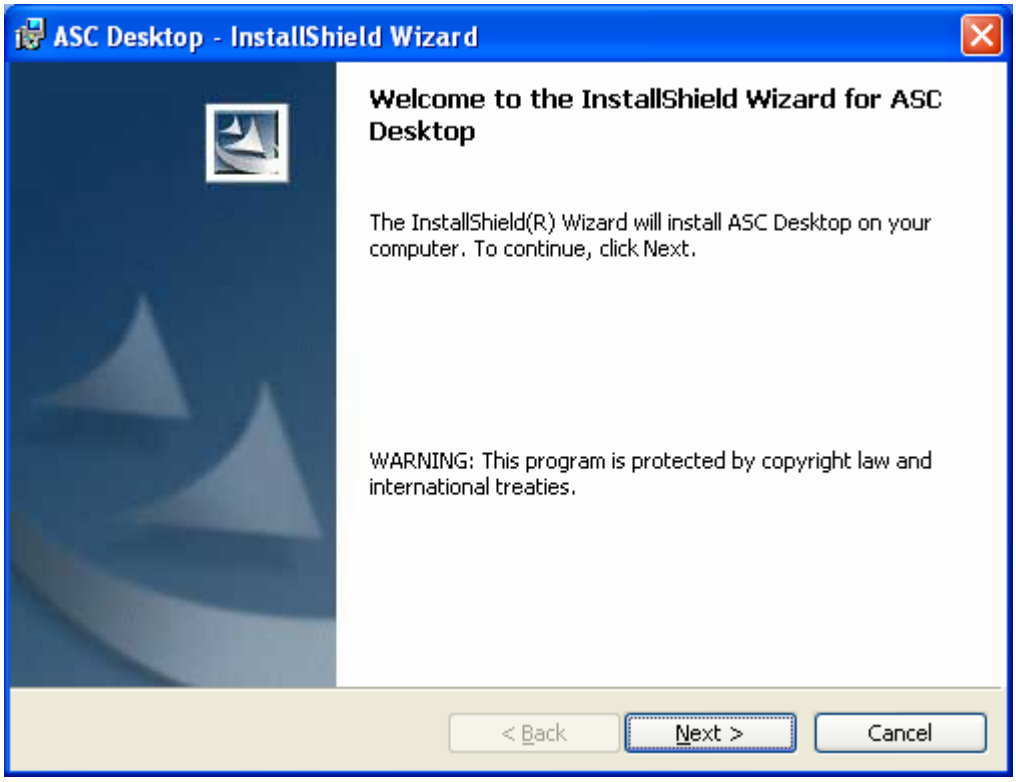
All components may be installed on any Microsoft Windows XP©, Windows 2000© Windows 2003© or Windows Vista© operating system. For evaluation purposes the Activeworx Security Center Desktop and Activeworx Security Center Manager may be installed on the same machine.

Installing/Configuring Activeworx Security Center

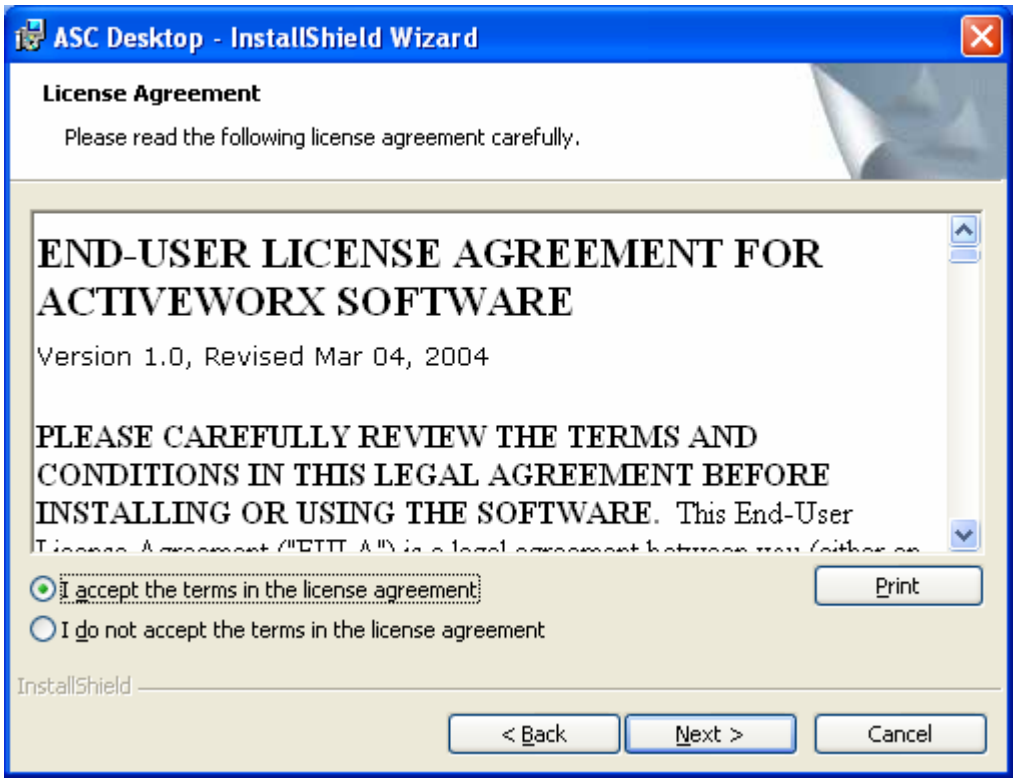
To begin the install process:

- Insure you have access to a MySQL or MS SQL server.
- Insure you have internet access as the install process will download .NET 2.x if not already installed.
- Start installation of the ASC Desktop by running the “asc.desktop.v3.6.x.x.exe” file.

When presented with the InstallShield screen, click on “Next” to continue.

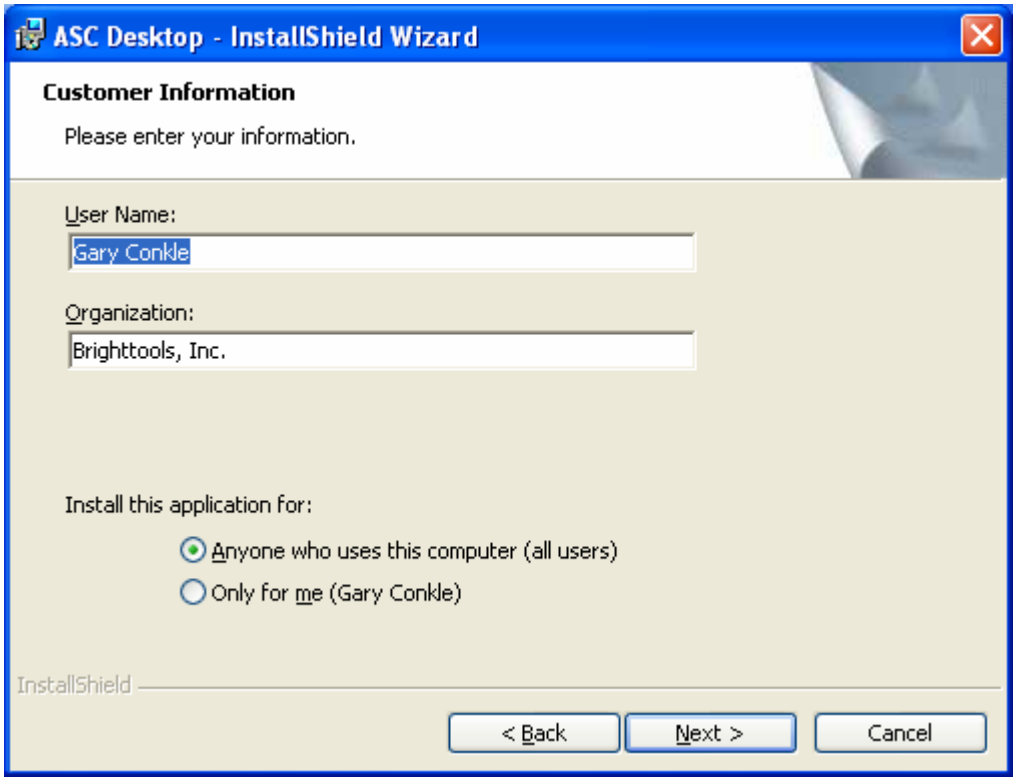


Click to accept license terms then click on “Next” to continue.



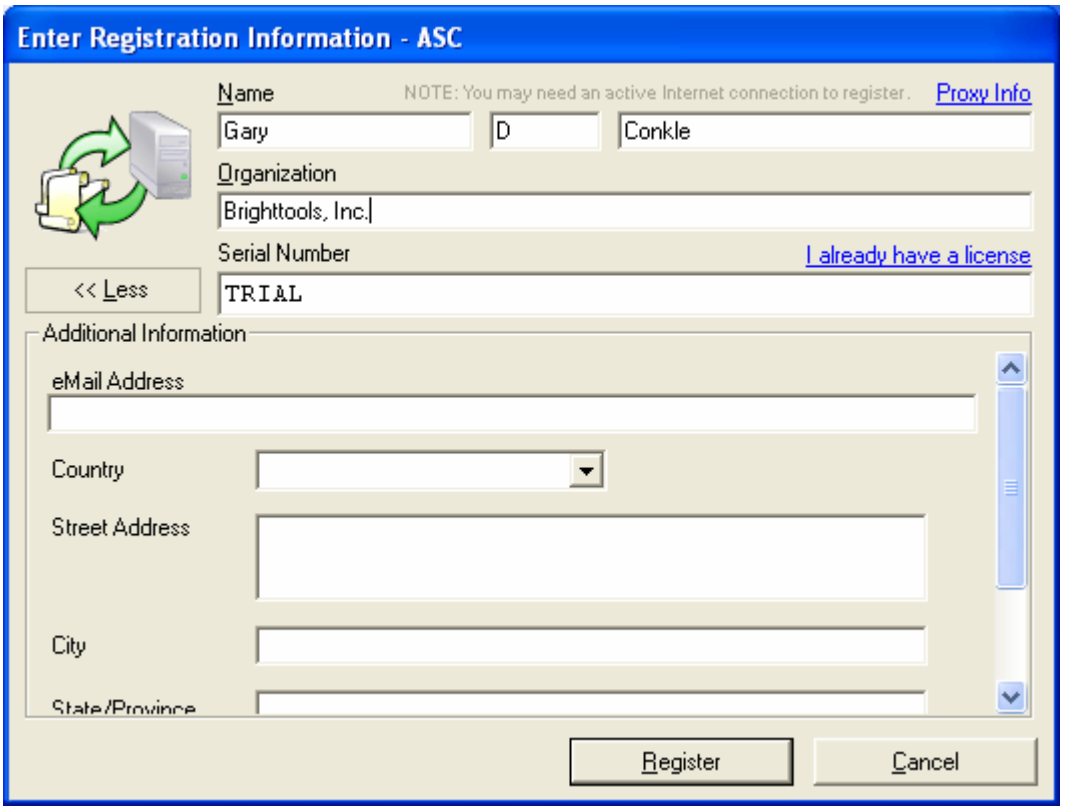
Fill in registration information and then click “Next” to continue.

When installation is complete, click on “Finish” to exit the installation procedure

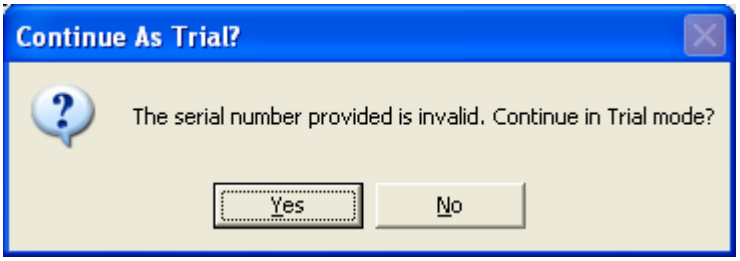


After the installation is complete, an icon for the ASC Desktop will be placed on your Windows desktop.

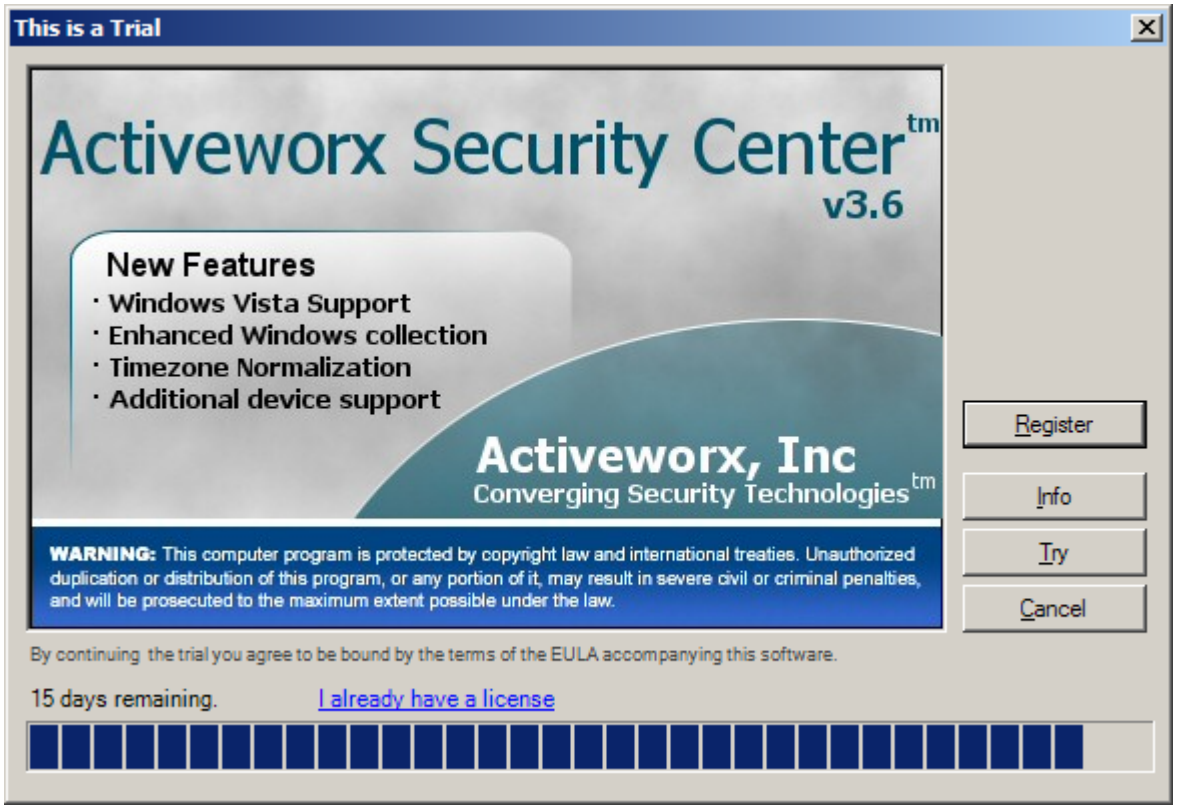
Double click the ASC Desktop icon and enter the registration information. If installing for evaluation purposes, leave the serial number as “TRIAL”. If licensed user, you may enter your serial number here.



If you are running trial mode you will receive this message. Click on “Yes” to continue.



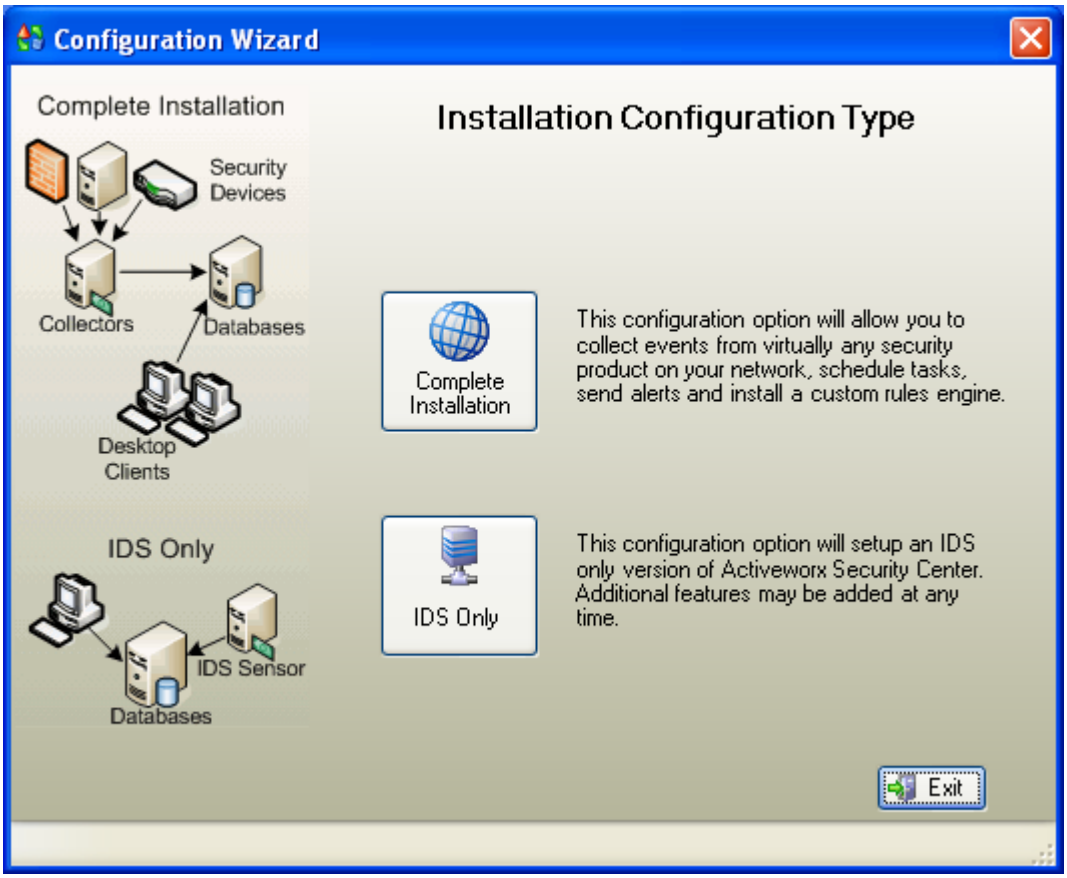
If running in trial mode, you will also be presented with this form, Click on “Try” to continue.



After the registration process is complete, the software detects it's a first time install and asks if the Configuration Wizard should be run. Click on "Yes" to continue.

The Configuration Wizard main form will be shown, click "Next" to continue.

Select type of configuration. For the purposes of this guide, select "Complete Installation".



Complete database server information as follows:

Database Server: Choose MySQL or MSSQL.

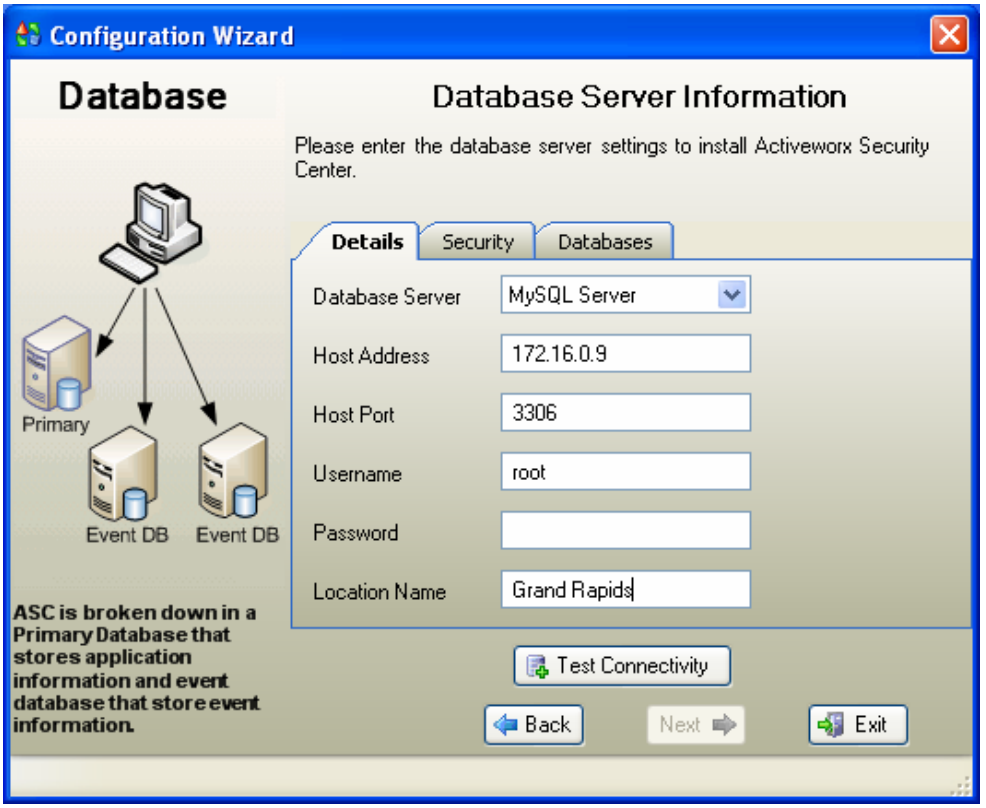
Host Address: Enter IP address of the database server.

Host Port: (MySQL only) 3306 unless changed during install of MySQL.

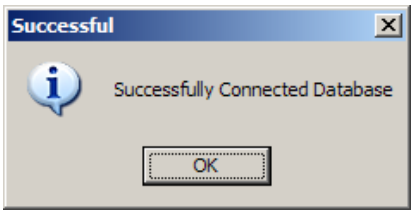
Username and Password: User with authority to create databases

Location: User Defined.

Click on “Test Connectivity” (required) to insure connection to DB Server then “Next”



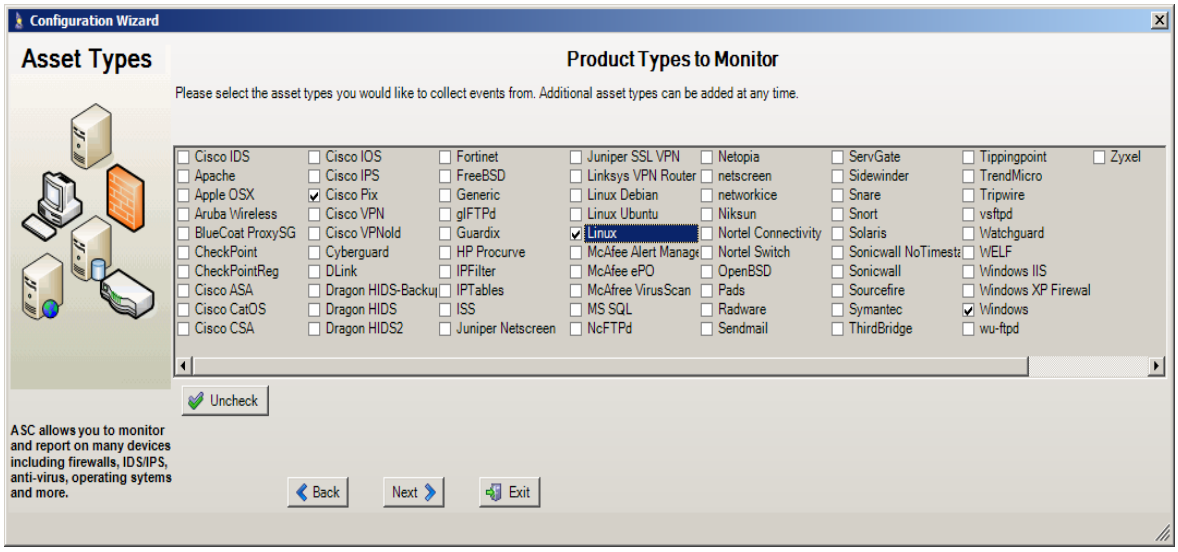
This window will be shown if successful connection:



Note: The following window has been resized to show all available options.

Select the various products that you wish to monitor.

For the purposes of this evaluation guide we will be selecting Cisco-Pix, Linux and Windows servers.

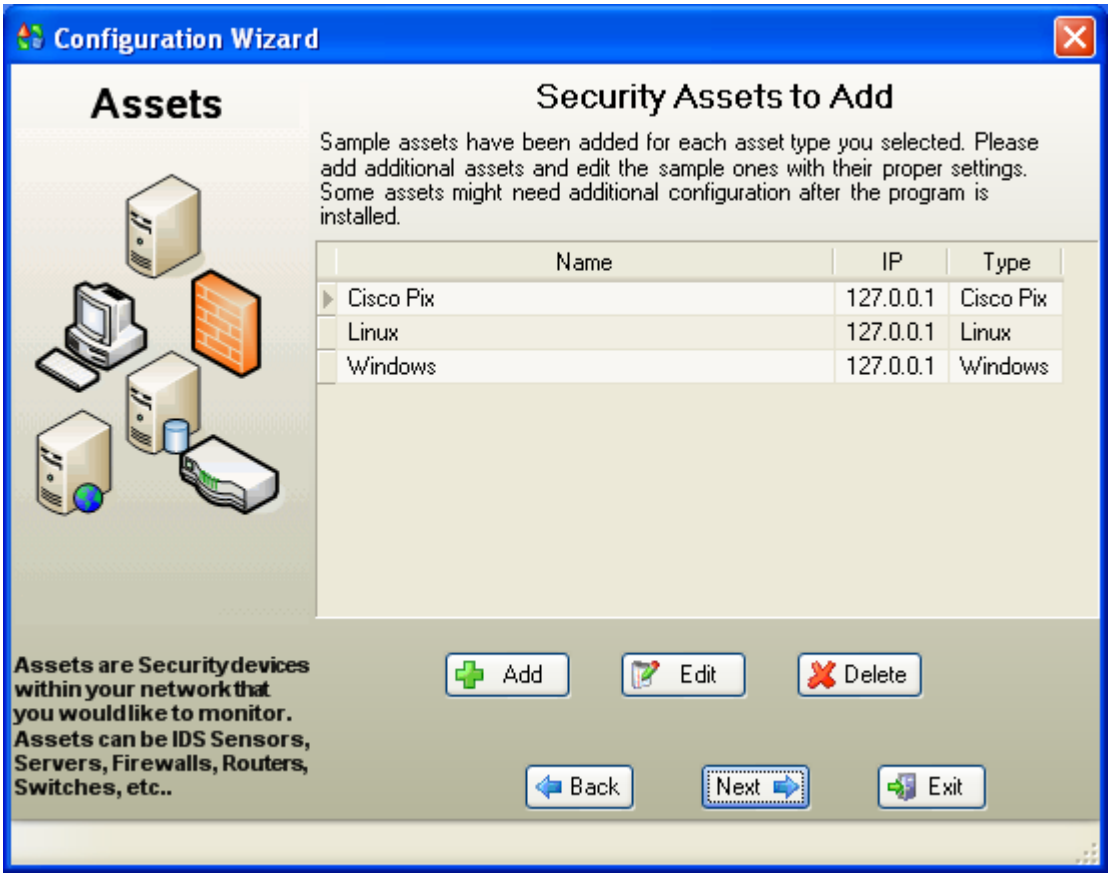


Note: If currently logging SNORT events to a SNORT database, you will not have to select SNORT. It is only used if SNORT is sending syslog messages rather than logging them to a database.

Click “Next” to continue.

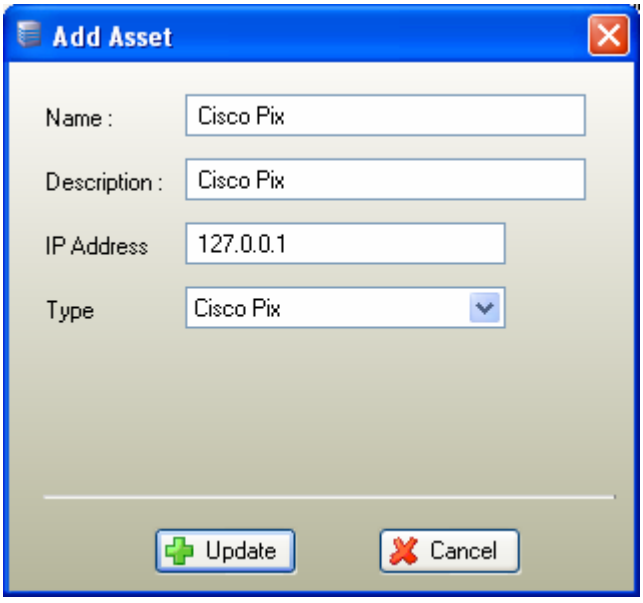
Based on the types of assets selected on the previous form, one of each type of device will be added.

Each asset should be edited to enter the actual IP address and to change the description and/or name as desired. You may also add additional devices if desired using the generated ones as a guide.

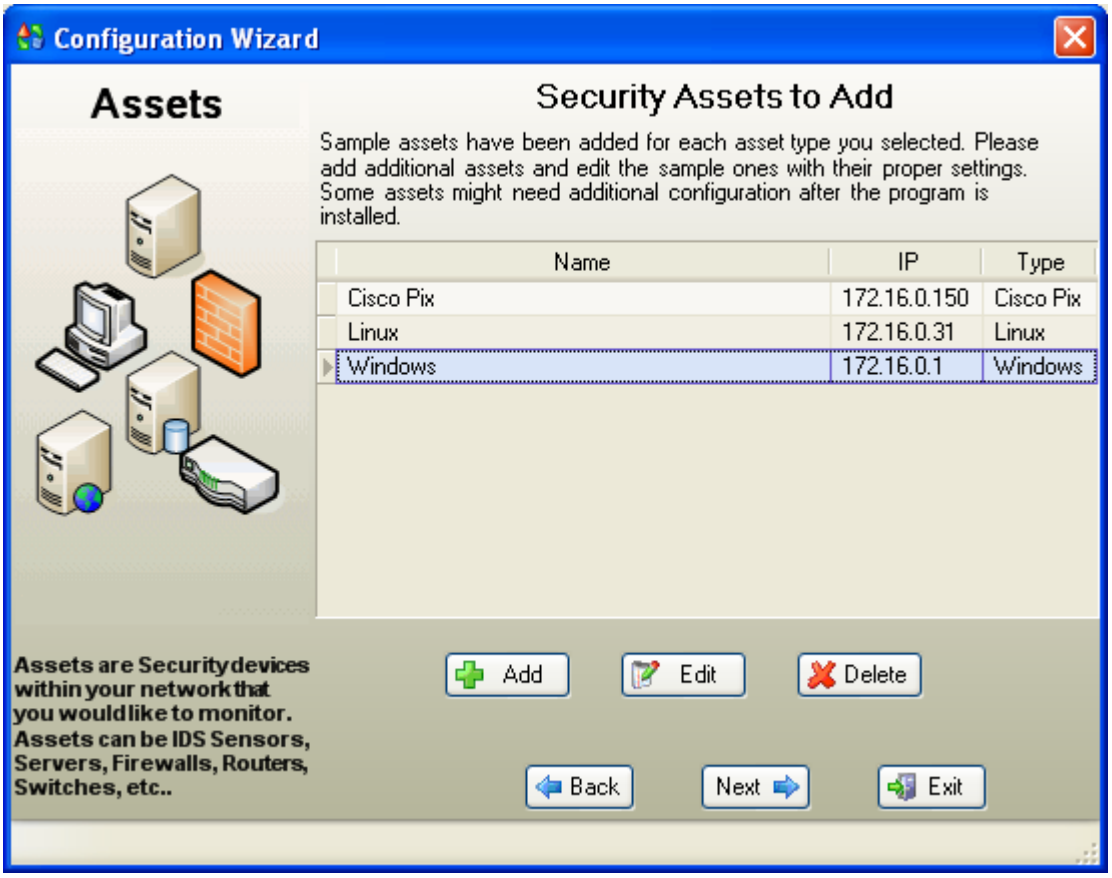


At a minimum, enter the actual IP address of the asset to be monitored. You may also update the Name and Description fields if desired.

After the appropriate changes have been made, click “Update” to save your changes.



After the assets have been updated with the actual IP addresses, click “Next” to continue.



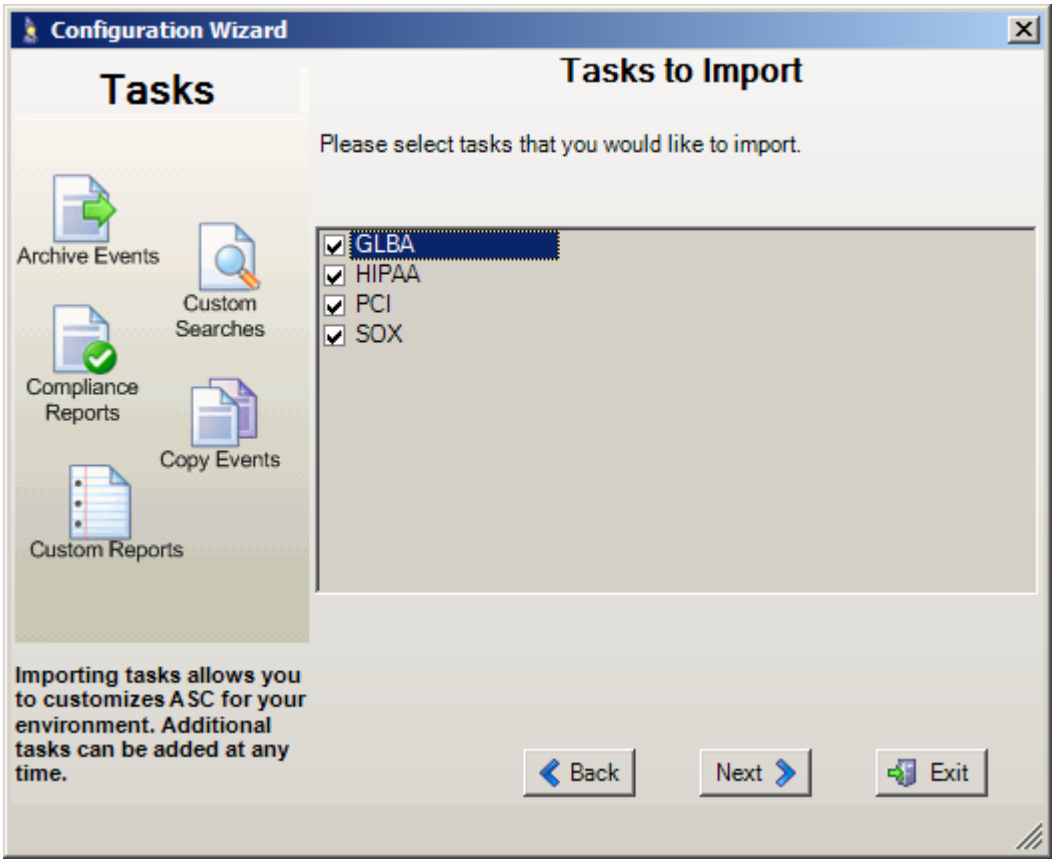
Next, enter the actual IP address of the machine that the Manager will be running on. If you plan on running the Manager on the same machine you are installing the ASC Desktop you may leave the IP addresses as local loopback address.

Click “Next” to continue.

Select any desired compliance tasks.

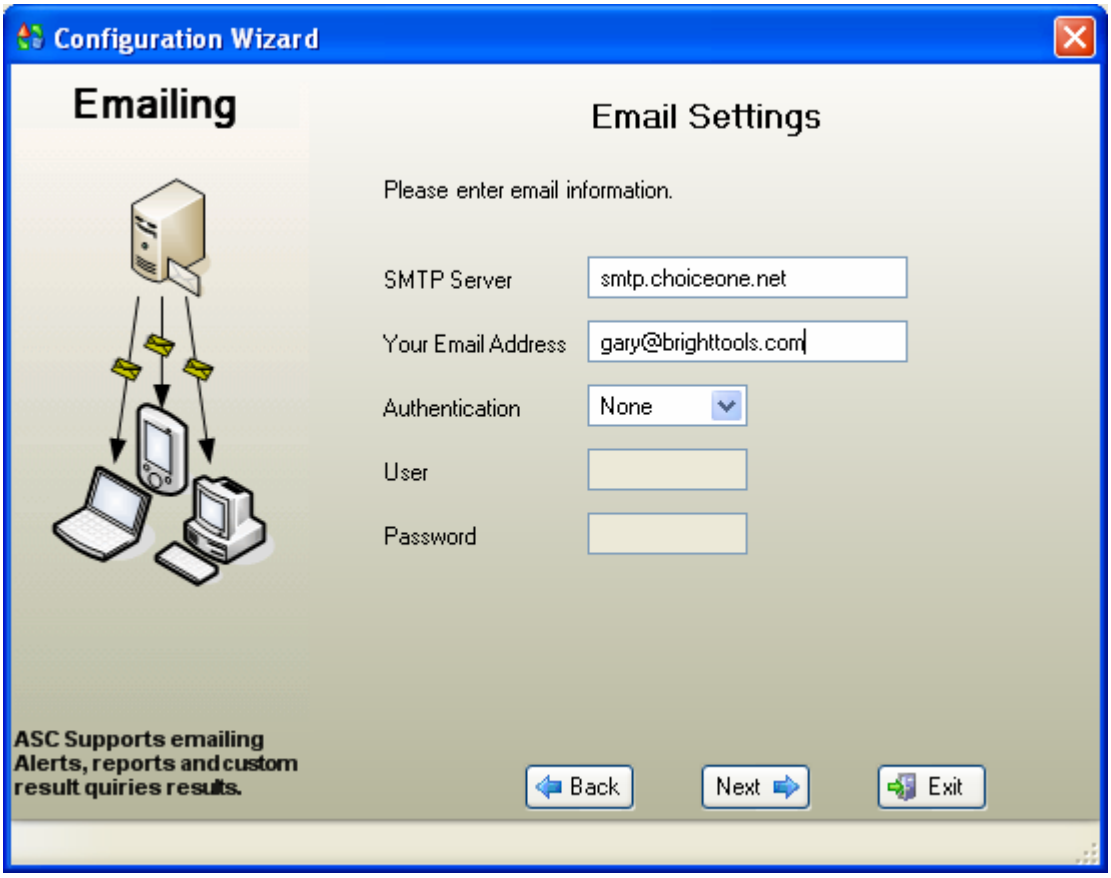
These are tasks (e.g. reports, diagrams, graphs) customized for various compliance requirements. Select all task types needed.

Click “Next” to continue.



Enter email settings. These settings are used by various functions within the ASC Desktop and Manager to send Email.

Click “Next” to continue.



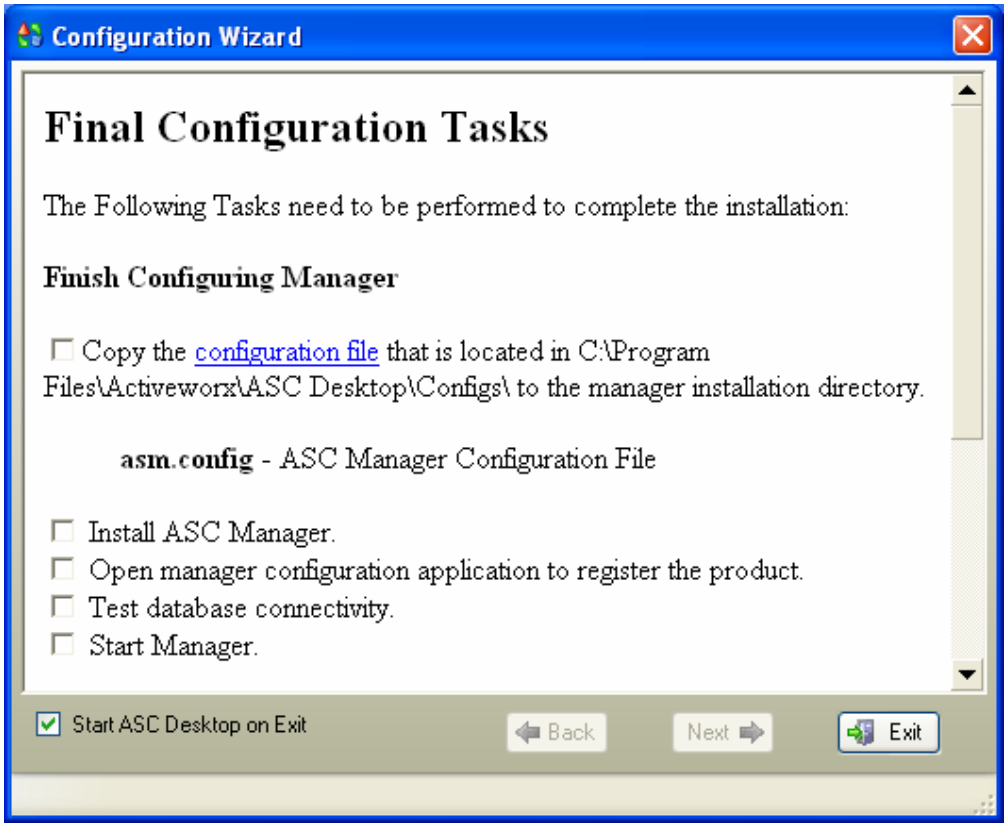
To complete the Configuration Wizard, click on “Start”. Various messages will be displayed as the items are created and configured.

If any errors occur, you may rerun the Wizard after the source of the problem is determined.

After the configuration has been completed, you will be presented with the “Final Configuration Tasks” form. This form outlines the necessary tasks to complete the installation and configuration.

You may print the form by right clicking anywhere on the form and then select the print option.

After these tasks are complete, Activeworx Security Center should be operational.
Click “Exit” to close Wizard.



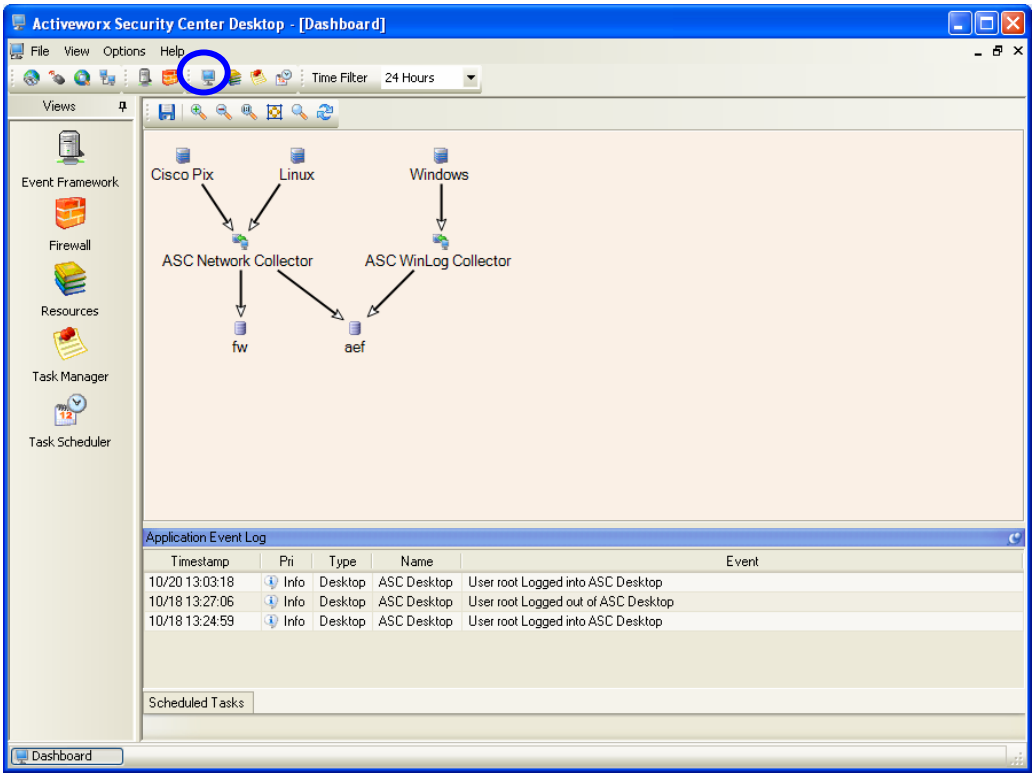
After exiting the Configuration Wizard the login form for the Activeworx Security Desktop will be displayed. Enter the Username and Password (the same ones you used for the configuration wizard) to login. All other information should be correct and left as is. Click on “Login” to complete the login process.

After a successful login, the ASC Desktop will be displayed. To verify configuration, click on the Dashboard icon (Circled) to display configuration of the product.

The diagram should match the configuration you created using the Configuration Wizard.

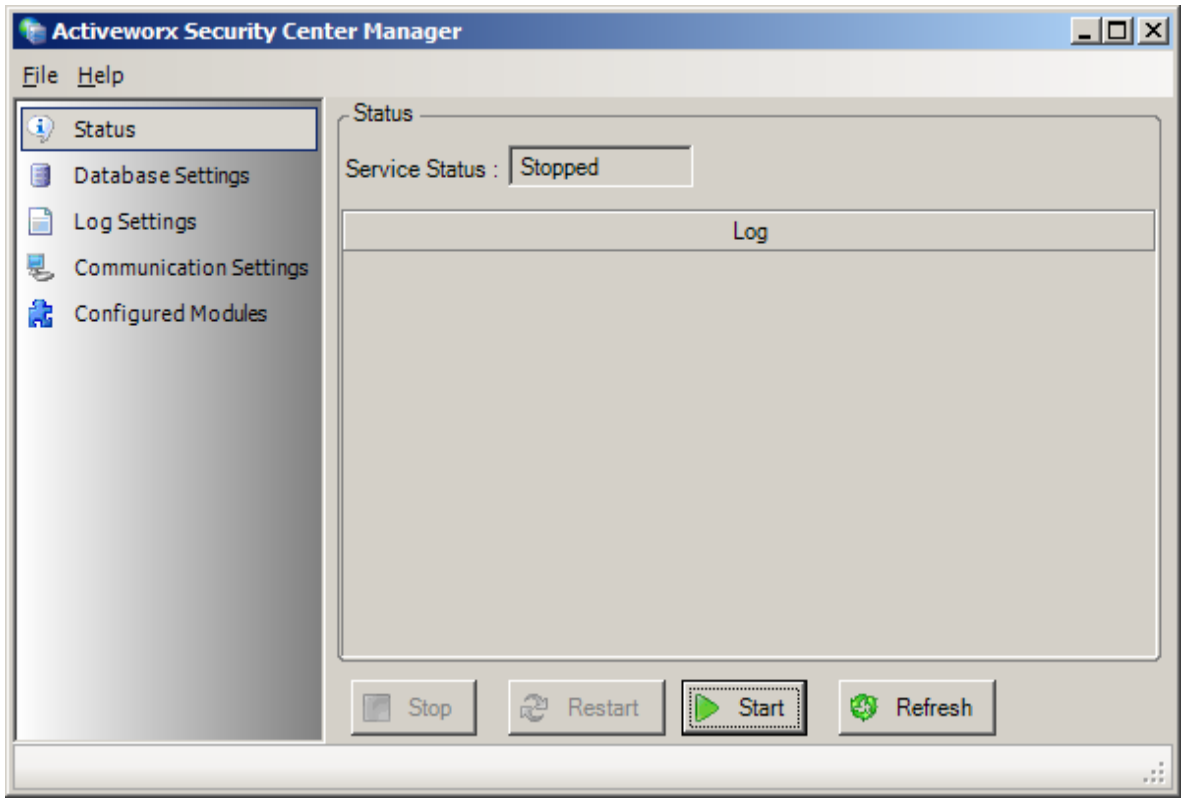
The top row of items represents the assets (firewalls, servers etc.) that will be monitored.

The next row shows the collectors that will collect network events.



The bottom row indicates the event databases that will be used to store events.

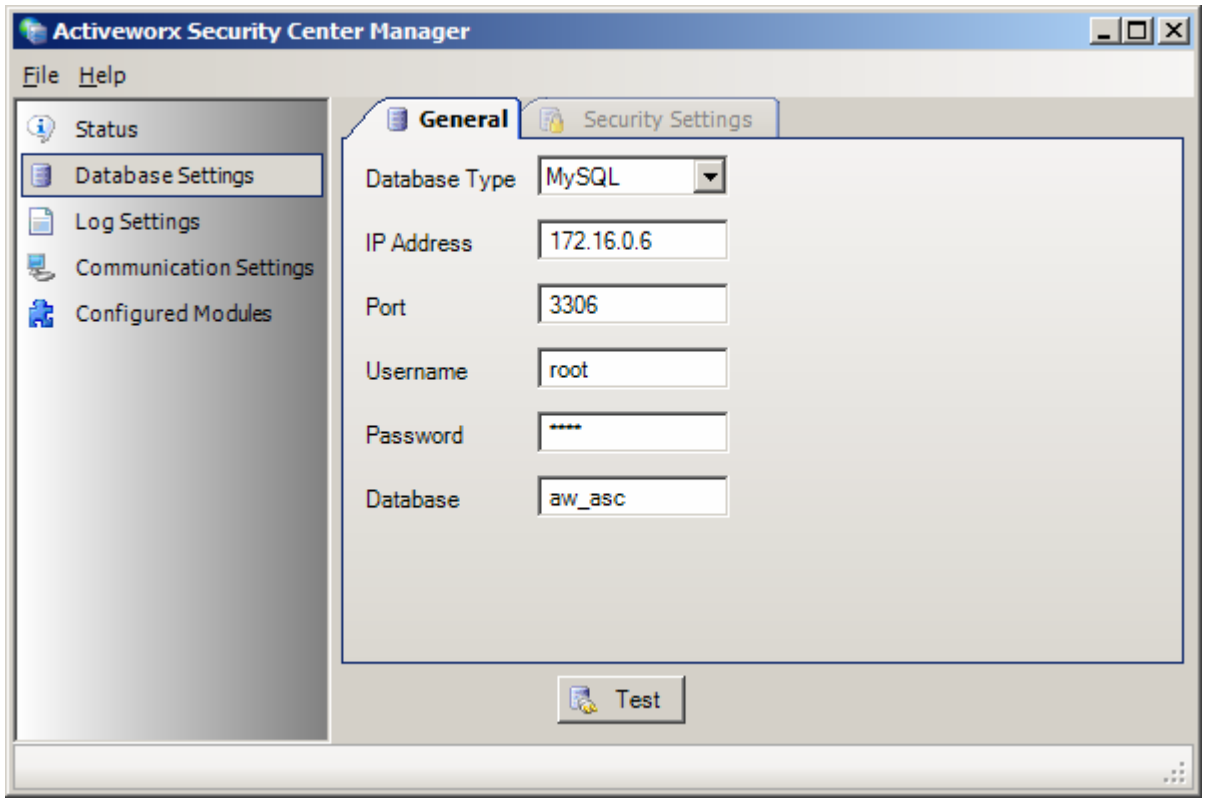
If you have not already done so install the ASC Manager on the computer with the IP address specified in the Installation Wizard using the following install file: “asc.manager.v3.6.x.x.exe”.



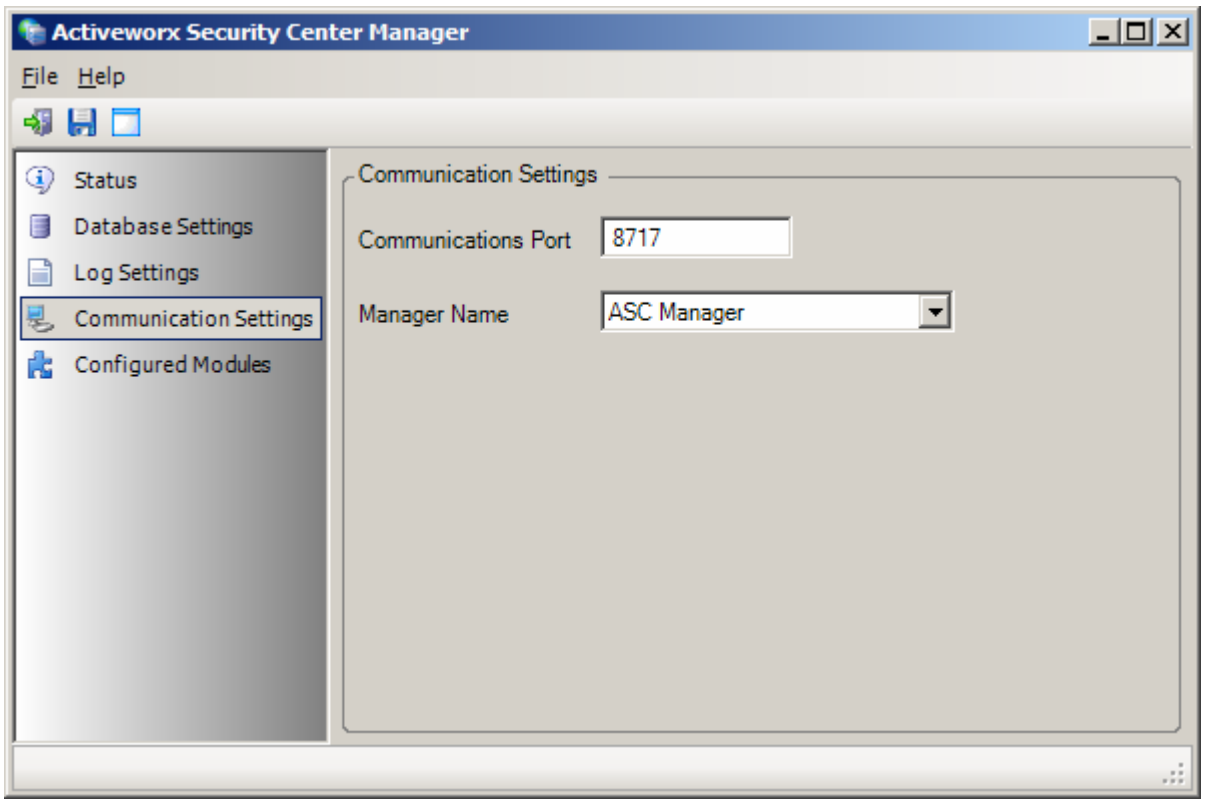
After you have completed the task of copying the configuration file to the Manager’s folder, start the collector GUI.

Icon will be on Windows desktop after install.

To test database connectivity, click on “Database Settings” then click on “Test”. You should receive a successful connect message.



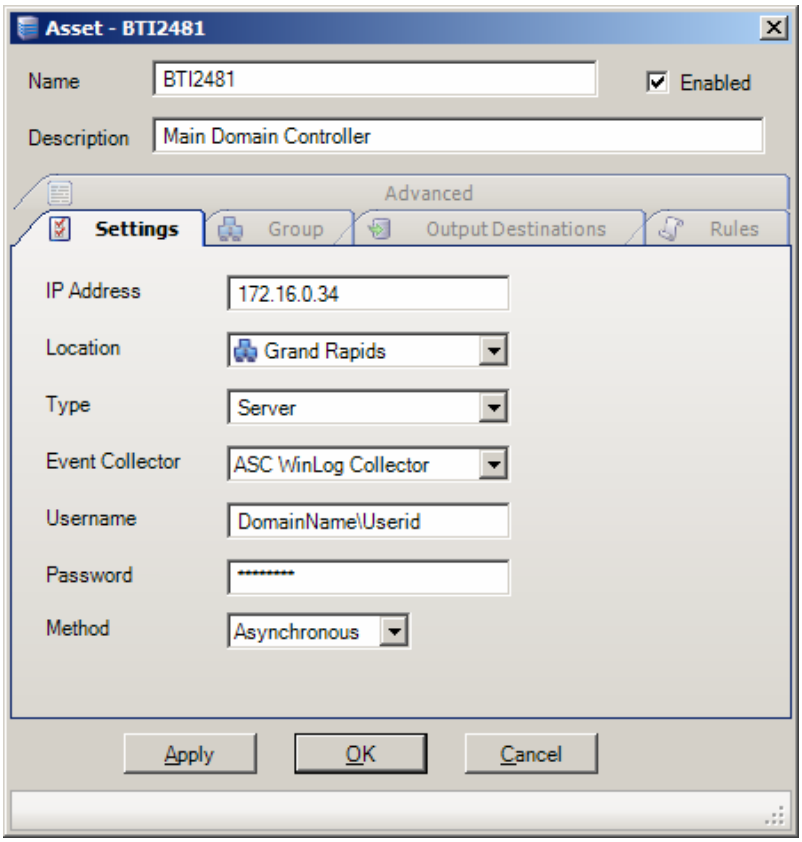
After a successful connection test, click on “Communications Settings” and verify the port and insure that the manager’s name appears. If it displays “Disabled” click the dropdown and select the manager. Click on “File” and “Save”.



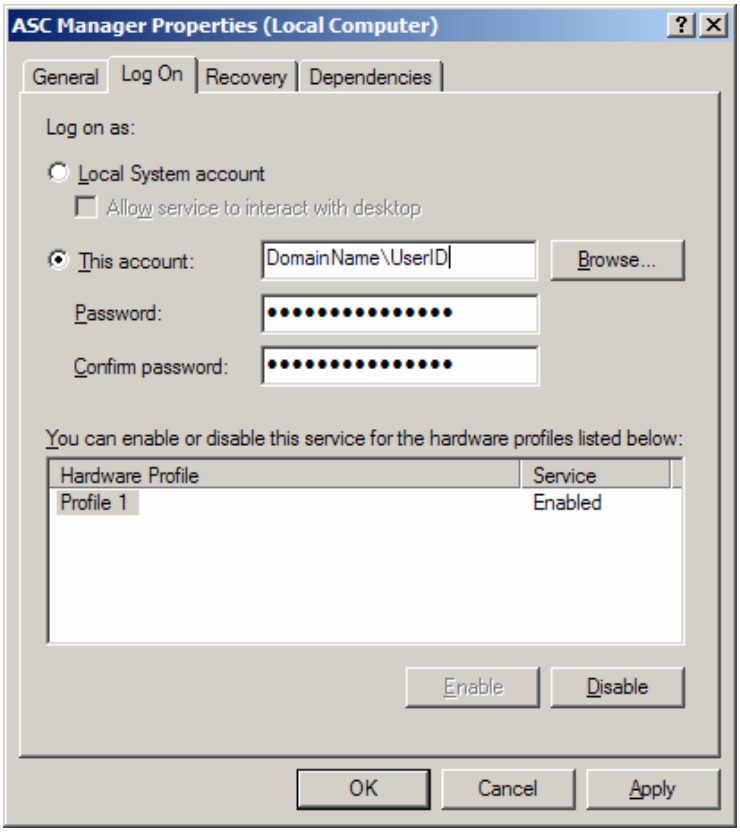
Configuring Activeworx Security Center Manager/Assets for Windows Security.
If you will be monitoring Windows you will need to provide Windows logon information that will allow the Activeworx Security Center Manager to connect to the machines it is monitoring to retrieve their event logs.

If your network is a Windows Workgroup or you are running a Domain and do not choose to use the Activeworx Security Center Manager Service method (Service method is recommended), you will need to update each defined Window's asset and add a user ID and password that has authority to access the machine.

If not already opened, start the Activeworx Security Center Desktop and go to Resources>Objects>Assets. Edit each Windows asset and add a user ID and password. For Workgroups or Domain use the following format for user ID: MachineName\UserID and enter Password. For Domain, you also have the option of using the domain user format: DomainName\UserID and enter Password.



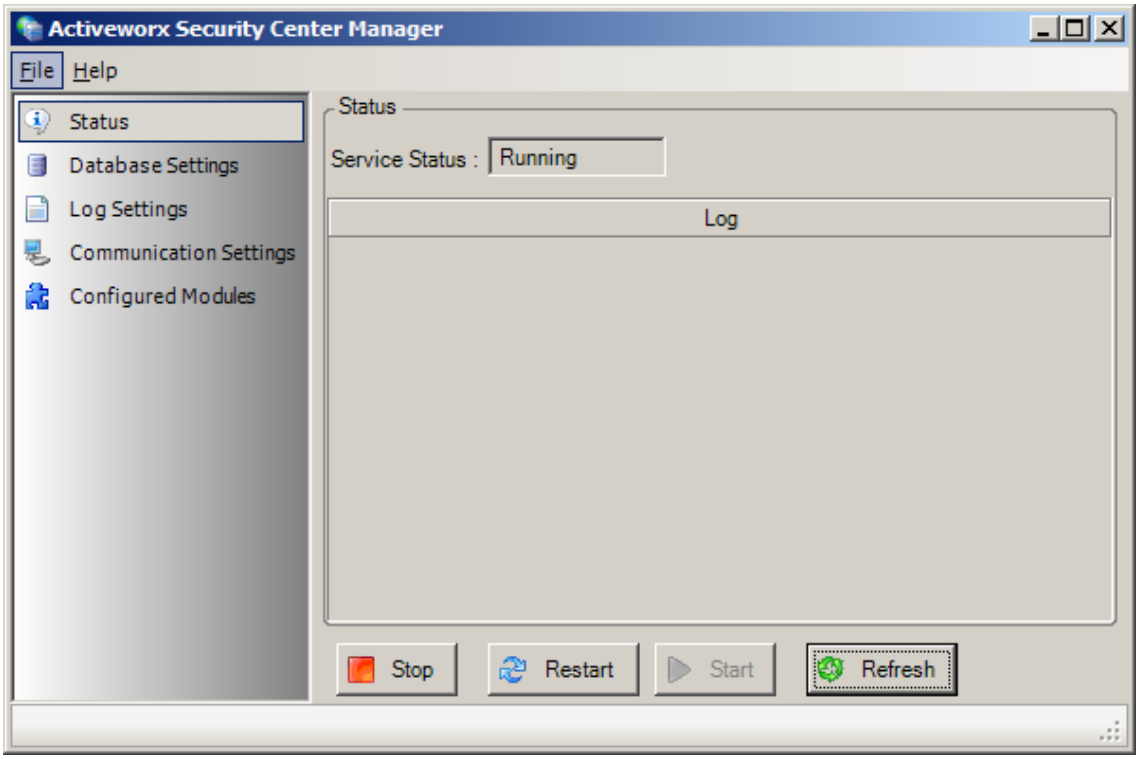
On a Domain you may avoid the necessity of updating each asset and use the Activeworx Security Center Manager Service method. Go to Control Panel>Administrative Tools>Services, right click on the ASC Manager service and left click on Properties, select the Log On tab, select "This account:" and enter the User ID using the following format: DomainName\UserID then enter the Password where indicated. Click on Apply to verify the User ID is accepted, then click on OK.



After configuring Windows security, click on “Status” then “Start”. The collector should begin to collect events and store them in the appropriate event database.

You may now close the collector GUI.

Note: Closing the Manager’s GUI does not stop the service. The Manager runs as a Windows service and will automatically start each time the computer is restarted.



Desktop Overview

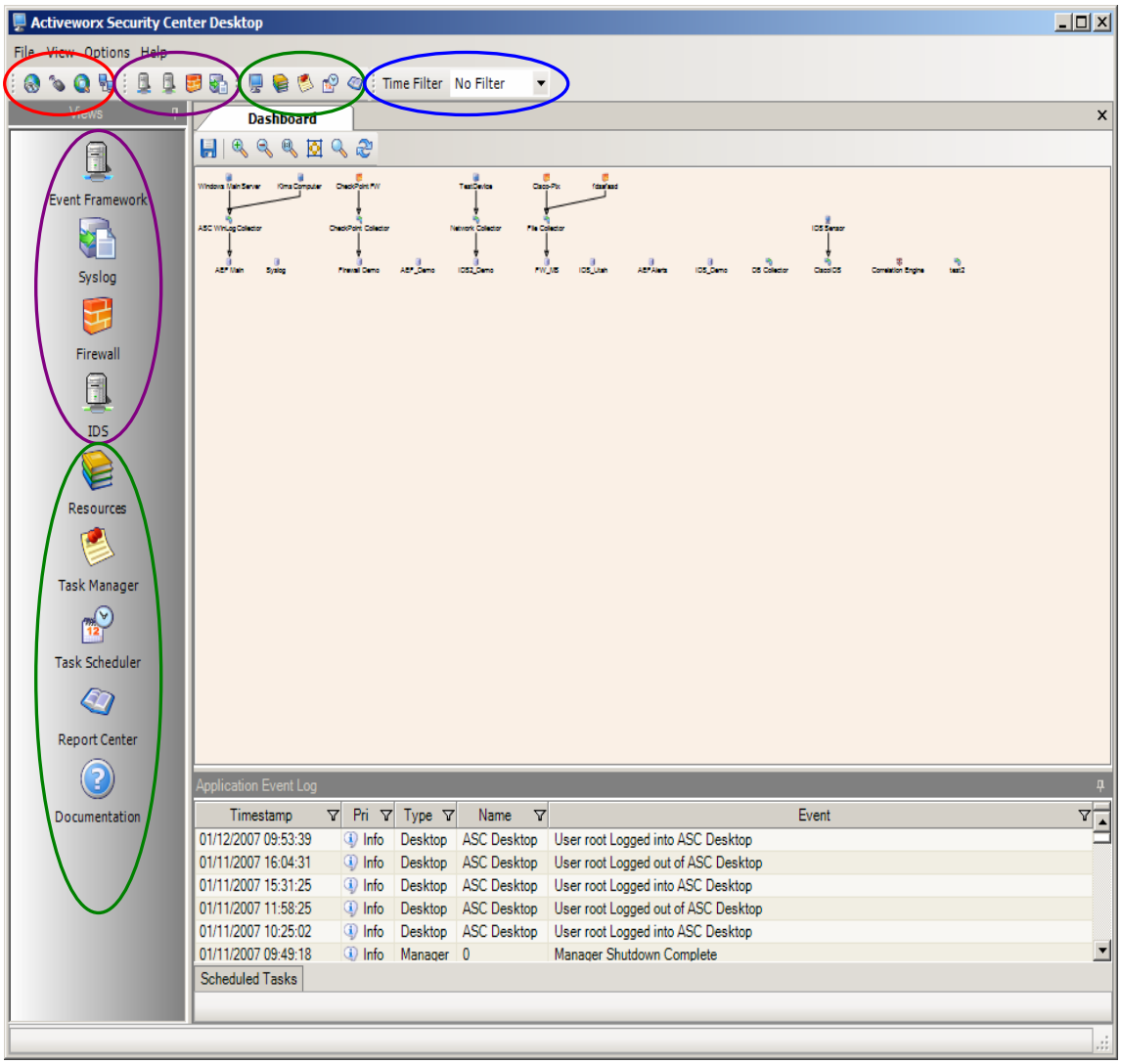
As a brief introduction to the ASC Desktop, a short explanation of each icon grouping is presented.

Red –
IP tools that may be run manually.

Purple –
Event database icons. Clicking on these icons will open the event database(s) of that type. You can then expand each database to access functions, reports, graphs etc. available to that database type.

Green –
Icons that will open various functions of the product.

Dashboard –
Displays current Activeworx configuration, application log and scheduled events for the current day.



Resources – Is used to define all assets, collectors, rules etc. and configure them.

Task Manager – Is used to create various types of tasks (i.e. reports, searches, archive functions, graphs, diagrams etc.) Tasks can be made permanent by naming them and then saving them. They can then be used later by the Task Scheduler or to be run manually.

Task Scheduler – Does exactly what the name implies. It gives the ability to schedule tasks which will be run automatically by the ASC Manager using the Scheduler module. Also gives the ability to distribute reports via email or uploading to a server.

Blue –
Time filter, when viewing events of the various event databases, determines how much data is presented on the desktop.

Conclusion

This concludes the Quick Install Guide. As stated previously, this is a starter guide for the Activeworx Security Center software. Additional set up will be necessary for a live production environment. For additional help, you may visit our website at www.crossteccorp.com for FAQ page or online help desk support.

You may also wish to consult the Evaluator's Guide that was also included in the installation Zip file for further information on the use and features of Activeworx Security Center.

You may also contact the Technical Support Group at (877) 512-4134. Technical support is provided free of charge during the evaluation period and is included in the maintenance support if you're an existing customer. In other words, it's free.

We at CrossTec, Inc. and Activeworx, Inc. would like to take this opportunity to thank you for evaluating our software.

Copyrights