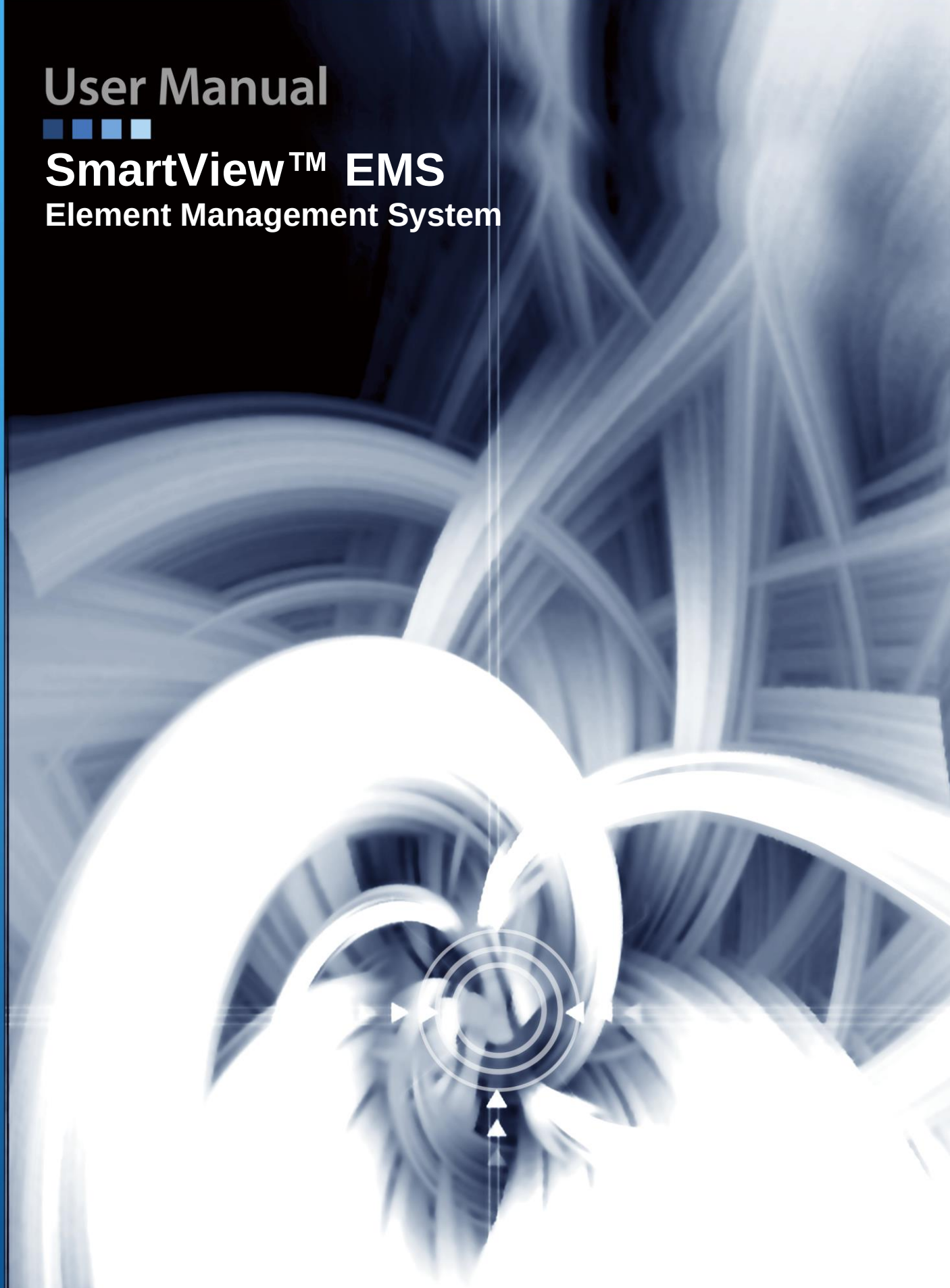
User Manual

SmartView™ EMS

Element Management System



CTC UNION TECHNOLOGIES CO., LTD.

LEGAL

The information in this publication has been carefully checked and is believed to be entirely accurate at the time of publication. CTC Union Technologies assumes no responsibility, however, for possible errors or omissions, or for any consequences resulting from the use of the information contained herein. CTC Union Technologies reserves the right to make changes in its products or product specifications with the intent to improve function or design at any time and without notice and is not required to update this documentation to reflect such changes.

CTC Union Technologies makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does CTC Union assume any liability arising out of the application or use of any product and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

CTC Union products are not designed, intended, or authorized for use in systems or applications intended to support or sustain life, or for any other application in which the failure of the product could create a situation where personal injury or death may occur. Should the Buyer purchase or use a CTC Union product for any such unintended or unauthorized application, the Buyer shall indemnify and hold CTC Union Technologies and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim of personal injury or death that may be associated with such unintended or unauthorized use, even if such claim alleges that CTC Union Technologies was negligent regarding the design or manufacture of said product.

TRADEMARKS

Windows® is a registered trademark of Microsoft® Corporation
CORBA® is a registered trademark of Object Management Group, Incorporated
Oracle and Java are registered trademarks of Oracle and/or its affiliates.
Other names may be trademarks of their respective owners.

CTC Union Technologies Co., Ltd.
Far Eastern Vienna Technology Center (Neihu Technology Park)
8F, No. 60, Zhouzi St.
Neihu District, Taipei, 114
Taiwan
Phone: +886-2-2659-1021
FAX: +886-2-2799-1355

SmartView™ EMS
(Element Management System).
Software Version 3.020 and above

User Manual
Version 3.02 January 22, 2020

This document is a continually evolving manual. Please check CTC Union's website for any updated manual or contact us by E-mail at marketing@ctcu.com. Please address any comments for improving this manual or to point out omissions or errors to marketing@ctcu.com. Thank you.

Please view the 'Product_Support.PDF' file on the installation DVD or included in any upgrade for details of supported products matrix and their required versions.

It is very important that the products that will be managed by this version of EMS have the required prerequisite firmware versions or there could be errors managing those devices or inability to connect SNMP to them.

YouTube™ video tutorials are available online that demonstrate installation and configuration steps for both Telecom and Industrial Grade products of CTC Union Technologies. For those videos, search YouTube with the key word 'ctcutech'.

Table of Contents

This page left blank intentionally.

Chapter 1 Introduction

1.1 Using This Manual

This manual contains all the information you will need to install and begin using CTC Union's SmartView™ Element Manager System (EMS), herein just called EMS. The format of the manual includes the following:

Chapter 1 Introduction
Provides an outline of this manual's structure and introduces the product.

Chapter 2 EMS Functional Specifications
An Overview of Element Manager System, provides a more in-depth look at some of the application's features and enhancements, and describes some general functions of the software platform such as configuring options, backing up data files, customizing the toolbar, and printing.

Chapter 3 Installing EMS
Step by step procedure for installing the EMS system on a single PC platform.

Chapter 4 Admin Console
Explains how to setup the EMS Service

Chapter 5 Using the Element Management Console
Configuration of the manager client for EMS.

Chapter 6 Using the Topology Feature
Provides some details for maintenance and troubleshooting problems with the EMS

Chapter 7 Using the Inventory Feature
Provides the details for inventory and accounting management of physical assets.

Chapter 8 Troubleshooting
Explains post installation issues, troubleshooting and fixes.

Appendix A, B, and C: Installing MS-SQL2008 R2 Express, MS-SQL2012 Express and MS-SQL2014 SP2 Express
Provides a step by step instruction for installing Microsoft's SQL Server for use with EMS.

1.2 The EMS system

There are two opposing points of view for management systems

Management systems designed for general enterprises
+Suitable for large networks
-Difficult to implement vendor specific functions

Vendor specific management systems
-Unsuitable for large networks
+Easy to implement vendor specific functions

This is the reason why customers need to implement both system types. The integration of these systems is not an easy task.

New requirements for NMS

To meet the customer demands for both large network management and vendor specific management, CTC Union has developed the SmartView™ Element Management System (EMS) to combine the two attributes of pure management systems producers and Telecommunication equipment vendors, specifically for CTC Union products.

Growing networks requires more Network Elements
Network Elements are becoming more complex and the collection of trap information and performance monitoring results in lots of data. Traditional vendor's NMS cannot support huge networks, nor can they capture and store the devices data for later analysis. To meet this element management challenge, we developed our own EMS.

Design considerations for modern management systems

In combining our vendor specific management features with those of large network management, we can summarize the major requirements for a management system. It must be:

- Distributed
- Database driven
- Platform independent
- Vendor optimized
- Secured
- User friendly
- Open

Other vendors planning for or already deploying new generation of management systems

- CISCO
- Alcatel-Lucent
- RAD
- Huawei

1.3 SNMP Management Systems and Network Devices

SNMP agent for Network Device

- MIB structure
- Basic functions
- Vendor specific features

SNMP based management systems integration

- SNMP agent with HP OpenView®
- SNMP agent with CA Unicenter®
- SNMP agent with SNMPc
- SNMP agent with IP Switch What's Up Gold or Orion

SNMP based performance monitoring systems

- CACTI (Open Source)
- Nagios (Open Source)
- Icigna (Open Source)
- PRTG (commercial)
- Cognos (IBM)
- SolarWinds (commercial)

Limitations

Universal management systems cannot fully present vendor specific features of Network Devices. One of EMS's benefits is that the system can run transparently next to any SNMP based management system and both types of systems can complement one another.

1.4 Element Management System

Overview

The objective of an Element Management System is to provide five major functions (FCAPS) for telecommunication operators:

- Fault Management (FM)
- Configuration Management (CM)
- Accounting Management (AM)
- Performance Management (PM)
- Security Management (SM)

Project design

The EMS design is based on the following considerations that comply with new requirements for management systems

- JAVA based

EMS is pure a JAVA project. The benefits of this technology including multi-platform support, modular design, and client-server architecture and portability.

- Event driven

Using events as primary objects for communication minimizes network loading, increases performance and allows for including a given quantity of Network Devices with predictable CPU and RAM loading, depending on this quantity.

- Data integrity

All data is in one place. User profiles are stored and loaded from one source. User created objects may be stored and loaded remotely and/or locally. There are well-defined procedures for backing up and restoring the configuration, topology, alarm, performance and user data.

- Database support

Support for any SQL server (Oracle, Informix, Microsoft etc.) Flexible SQL interface design for server. Client optimization by customer. (currently, only MS-SQL Server is supported).

- Standard SNMP and CORBA support

Design has no restrictions to any one CORBA vendor. Tested with different Object Request Brokers.

- Open architecture

Provides API and IDL files for integration with upper layer systems, i.e., North Bound Interface.

Broker Service (BS)

This is a CORBA service, responsible for registering new agents and clients and delivering events between them. CORBA is the acronym for Common Object Request Broker Architecture, a vendor-independent architecture and infrastructure that computer applications use to work together over networks. Using the standard protocol IIOP, a CORBA-based program from any vendor, on almost any computer, operating system, programming language, and network, can interoperate with a CORBA-based program from the same or another vendor, on almost any other computer, operating system, programming language, and network. One of its most important, as well most frequent, uses for CORBA is in servers that must handle a large number of clients, at high hit rates, with high reliability. Specialized versions of CORBA run real-time systems, and small embedded systems. As a part of Broker Service, CORBA supports a set of special clients. There are databases, properly installed and connected to the Broker Service. All information for each Network Device in EMS can be stored or loaded from their database.

Embedded Agent (EA)

This is the major element for EMS and is also referred to as a Network Device (ND). The Embedded Agent utilizes a standard protocol (Simple Network Management Protocol) to interact with the Broker Server. To ensure security, only the Broker Server has direct access to the Embedded Agent. It is also possible to use a direct connection from client to device at the same time as a backup solution (via HTTP or Telnet). The design of the Embedded Agents guarantees that even in the direct access case, all changes of the Embedded Agent structure and alarm messages will be delivered to the registered Broker Server. A protocol, supported by the Embedded Agents, depends on the product and can be changed in the future if necessary. Embedded Agents fully support SNMP protocol (Versions 1 and V2C) with trap notification.

EA provides all necessary functions for Fault Management (FM), Performance Management (PM), Configuration Management (CM), and Security Management (SM).

Depending on marketing demand, a set of other protocols can be implemented in EA and BS to achieve better performance, reliability and to simplify integration to the customer's network infrastructure. These are protocols such as CORBA or JMX. Implementing new protocol in all components of EMS can be easy due to modular design and open architecture.

Desktop Security (DS)

This is major administration tool for securing permissions and restrictions in the Broker Server. It allows administrators to setup different user access to the BS service. Users may have personal desktop(s) stored in database with different permissions or "Roles". For example, node administrators may have permission to change the property of any object, located in his node and lower level nodes or only manage given nodes and their devices. At the same time, another user may have permission to overview all network structure and get notification messages about structure changes.

Element Management Console (EMC)

This is the client user interface. It helps users to identify themselves to the BS, get all permissions to work with network configuration and start the management session. This session allows users to represent their network segment in a map view and/or tree view, name network objects, organize groups, regions, nodes according to actual structure of the given network and monitor status of chosen objects as well as change their properties or settings. The Element Management Console also may be used to start other EMS tools, such as Alarm view, Trap view, Topology, Performance or Inventory displays.

Transaction Service (TS)

This tool will prepare, check, execute and review the results of user transactions. This means the user can define sets of property changes for a predefined set of network objects (including node structure and permission changes). In the boundary conditions, a single set of properties can be treated as the smallest transaction. Alternately, all network structure changes can be represented as a transaction with a huge amount of commands inside. Both cases are under the control of the Transaction Manager if the user invokes a transaction and are guaranteed a detail report about each command (by user definition it may be only a failure condition for all commands or at least one command failed). The user can define the type of transaction such as "stop after first fault" or "process all commands" at will. As a transaction, ideally it is possible to rollback transactions on some conditions, mentioned above, or by user request. Transactions can be loaded from and stored to the database. This means that for some standard operations, the user can have a set of "predefined" transactions. It is possible to add parameters in these predefined transactions to allow the user to execute the same set of property changes on different instances of network objects. This can be recognized as an extension of the "copy profile" action. If necessary, this tool can start other network tools like Instantaneous Decision or Cross Connect.

Alarm Console (AC)

This is a list of current alarms that have occurred in network devices. Each alarm message is stored in the main database. At any time, the user can request all previous alarms of a specified type from a defined source for the given period, print this report, or save it in the database as personal data.

Alarms are presented as list with colors defining each alarm severity level.

Chapter 2 EMS Functional Specifications

2.1. General Description

This chapter is intended to describe the software design specification for the SmartView™ EMS Server software for CTC Union Network Devices (ND). The EMS Server is designed to provide all the configuration and maintenance functions for the network device. The method to access EMS Server functions is via CORBA protocol according OMG CORBA Specifications. When a user loads EMS Client software and sets up a link to the EMS Server it will be possible to monitor and control Network Devices via CORBA actions. The EMS Server uses SNMP Protocol to monitor and control Network Devices via SET, GET, GETNext and TRAP SNMP actions. The issues inside the mechanism described above are the scope of this chapter.

2.2. Acronyms

No.	*Acronyms*	Description	Remark
1	EMS	Element Management System	
2	EMC	Element Management Console	
3	API	Application Interface	
4	ND	Network Device	
5	CORBA	Common Object Request Broker Architecture	
6	SNMP	Simple Network Management Protocol	
7	HW	Hardware	
8	IP	Internet Protocol	
9	OS	Operating System	
10	SW	Software	
11	TCP	Transmission Control Protocol	
12	UDP	User Datagram Protocol	

2.3. Requirement

- H/W: IBM Compatible PC, 64bit Processor (minimum Intel i5, >2.2G, 8G RAM, 20G Disk Space) 1024x768 minimum display resolution, FHD (1920x1080) recommended.
- OS: Microsoft Windows 8/8.1 Professional(64), Windows 10 Professional(64), MS-Server 2012, MS-Server 2016, MS-Server 2019.
- Network: IP over LAN/WAN (Gigabit Ethernet I/F)
- JAVA JRE 1.7 (64 bit binaries included with EMS)
- MS-SQL Server 2008 R2 Express (MS-SQL Server 2014 Express for Windows 10/MS-Server 2016)

2.4. The Architecture of EMS Server

This section describes the software architecture of the EMS Server, including the functional block diagrams and the relationships between blocks.

2.4.1. Basic Client – Server Architecture

Since CORBA is used as the communication protocol, the system will be compatible with all implementations of CORBA client software. Obviously, you can use any SNMP browser to monitor and control the Network Devices. However, the advantage of using an EMS Server is that it offers continuous monitoring of all registered SNMP Agents and records in a database all system activity.

Only the version of SNMP Agent needs to be compatible with the EMS Server in terms of configuration and alarm Traps. To make an initial setup (IP address, SNMP agent Groups, polling policy etc.) the user can use the Admin Console.

EMS Broker is a persistent software agent with following functions:

- interaction of all modules with database (DBMS).
- interaction via SNMP protocol with Object (or agent, Network Device)
- interaction via CORBA with client applications (Management Console)

The communication protocol between the management EMS Server and managed network devices is SNMP, which is a standard network management protocol. For details regarding SNMP, please refer to RFC1157. Figure 2-1 presents the relationship between management server and managed devices.

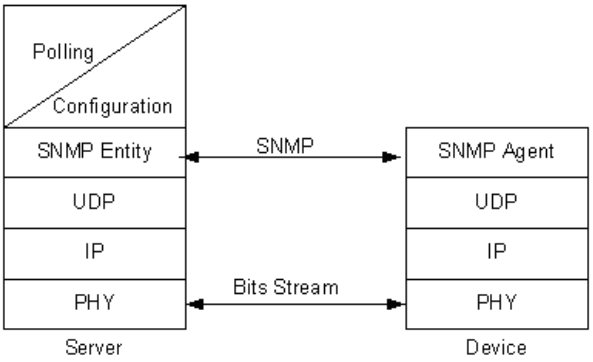


Figure 2-1 Communication between SNMP browser and device

The tasks performed by EMS Server are:

- Collect configuration information from SNMP Agents via SNMP protocol and send to the agents control commands to change their state
- Guarantee storage of all information in external database server
- Transfer control and configuration data to and from client software via CORBA
- Organize and maintain control objects in the database and client configuration constructions, which describe the system; also provide role access to above mentioned objects

2.4.2. Module definition

The EMS Server works in close connection with the following external modules:

1. Tnameserv - CORBA Name Service supplied with JRE1.7.x Standard Edition from Oracle (previously SUN Microsystems).
2. JDBC - mssql-jdbc-6.4.0 with JRE1.7
2. Database Server - MS SQL 2008/2012/2014 Server from Microsoft Corp.

These components can be distributed over a network (installed in different hosts), or they may be started in the same host (in this case it is necessary to be concerned about the host's performance when starting several powerful tasks).

The EMS Server is a multithreaded JAVA-application and interacts with the SNMP Agents via SNMP-TRAP and Get/Set SNMP protocol, which it receives asynchronously.

There are five basic modules:

- Agent Driver
- Agent Group Driver
- Database Driver
- CORBA-servant
- Database

2.5 Functional Description of EMS Server

2.5.1. Functions of Broker Agent Driver

The AD performs SNMP-interaction with the SNMP Agents, having active thread monitoring, and observes SNMP Agent's working status via polling. There are as many Agent Drivers as there are SNMP Agents.

2.5.2. Functions of Agent Group Driver

These Group Drivers control the Agent Driver threads and also at predefined intervals initiate configuration collection from all of his SNMP Agents. It is possible to have several Group Drivers. Group Driver configuration are setup by the system Administrator and stored in the database. Each GD has his own thread(s).

2.5.3. Functions of Database Driver

The Database Driver (JDBC) performs interaction with the database server; It has no active thread.

2.5.4. Functions of CORBA-servant

Realize CORBA-object to interact with clients SW. Performs client registration message sending to clients and all SW calls from client SW. There is only one active thread.

2.5.5. Functions of Database

Database itself as data schema and procedure interface.

2.5.6. Functions of SNMP stack

SNMP daemon starts in root() OS entry point with priority 90.

SNMP Architectures

Network management system contains two primary elements: a manager and an agent. The Manager is the SNMP browser through which the network administrator performs network management functions. The agent is the entity that interfaces to the actual device being managed. All managed objects include device configuration, all kinds of module parameters, cross connect information, and so on. These are arranged in what is known as a virtual information database, called a management information base or MIB. SNMP allows managers and agents to communicate for the purpose of accessing these objects.

SNMP protocol stack will provide the whole operation function for network device management. The necessary requirement will involve the followings:

- Query current running parameter
- Get response from agent
- Set variable in agent
- Acknowledge asynchronous trap event from agent

SMI and OID

In the Manager/Agent paradigm for network management, managed network objects must be logically accessible. Logical accessibility means that management information must be stored somewhere, and the information must be retrievable and modifiable. SNMP actually performs the retrieval and modification. The Structure of Management Information (SMI) is given in RFC 1155. We give a class SMI in package com.zzz.snmp to realize the SMI.

The SMI states that each managed object must have a name, syntax and an encoding. The name, an object identifier (OID), uniquely identifies the object. The syntax defines the data type, such as an integer or a string of octets. The encoding describes how the information associated with the managed objects is serialized for transmission between agent and manager. In our EMS package, OID is realized as class com.zzz.snmp.OID.

The syntax used for SNMP is the Abstract Syntax Notation One, ASN.1. The encoding used for SNMP is the Basic Encoding Rules, BER. The names used are object identifiers.

Each object represents a characteristic of one device, and must have a name by which it can be uniquely identified. That name is the object identifier. It is written as a sequence of integers, separated by periods. For example, the sequence 1.3.6.1.4.1.4756 specifies the private OID root of CTC Union. The sequence 1.3.6.1.4.1.4756.xx represents the managed OID of some SNMP Agent.

SNMP operation model

SNMP is based on a master/slave model. SNMP includes a limited set of management commands and responses. The management system issues Get, GetNext and Set messages to retrieve single or multiple object variables or to assign the value of a specified variable. The managed agent sends a Response message to complete the Get, GetNext or Set command. The managed agent sends an event notification; called a trap to the management system to notify the occurrence of conditions such as major/minor alarm occurs. In short, there are only five primitive operations:

- Get (retrieve operation)
- Get Next (traversal operation)
- Get Response (indicative operation)
- Set (alter operation)
- Trap (asynchronous trap operation)

SNMP Message structure

Each SNMP message has the format shown below. For details please refer to class SnmpMessage.
- Version Number
- Community Name
- SNMP PDU

Each SNMP PDU, realized by class SnmpPDU, has the following format:

- request id - request sequence number
- error status - zero if no error otherwise one of a small set
- error index - if non zero indicates which of the OIDs in the PDU caused the error2
- list of OIDs and values - values are null for get and get next

Trap PDU realized by class TrapPDU has the following format:

- enterprise - identifies the type of object causing the trap
- agent address - IP address of agent which sent the trap
- generic trap id - the common standard traps
- specific trap id - proprietary or enterprise trap
- time stamp - when trap occurred in time ticks
- list of OIDs and values - OIDs that may be relevant to send to the NMS

UDP communication protocol

SNMP assumes that the communication path is a connectionless communication sub network. In other words, no prearranged communication path is established prior to the transmission of data. As a result, SNMP makes no guarantees about the reliable delivery of the data. However, in practice, most messages do get through, and those that do not can be retransmitted. The primary protocols that SNMP implements are the User Datagram Protocol (UDP) and the Internet Protocol (IP). SNMP also requires Data Link Layer protocols such as Ethernet or Token Ring to implement the communication channel from the management to the managed agent.

SNMP's simplicity and connectionless communication also produce a degree of robustness. Neither the manager nor the agent relies on the other for its operation. Thus, a manager may continue to function even if a remote agent fails. When the agent resumes functioning, it can send a trap to the manager, notifying it of its change in operational status. The connectionless nature of SNMP leaves the recovery and error detection up to the NMS (Network Management Station) and even up to the agent.

Agents listen for messages from the manager on UDP port 161, and the manager listens for trap messages from the agent on UDP port 162.

ASN.1 and BER

ASN.1 is used to specify many RFCs, for example the Internet standard MIB and SNMP. ASN.1 is used widely in OSI for specification purposes. ASN.1 used for defining SMI and MIBs is a subset of the ASN language given by OSI. Please refer to the ITU-T X.208 specification.

ASN.1 modules contain module name, linkage and ASN.1 declarations. ASN.1 Macros are used to extend the standard ASN.1 notation. All comments begin with "--" and will extend to the end of this line. Their declarations specify types and permissible values. The types are listed below:

Simple types

- integer - 0 to (2**1008) - 1
- octet strings - values between 0 and 255, i.e. 8 bit fields
- object identifiers - object name
- null

Constructed types

- sequence - ordered list of elements of differing types (RECORD)
- sequence of - ordered list of elements of same type (ARRAY)
- Tagged types - for "carrying type" information in message useful for creating own types

Other types

- choice - between alternatives
- any - non specified ...

BER is the common name for the Basic Encoding Rules of ASN.1. BER is defined in ITU-T Recommendations X.209 and X.690. BER is one set of rules for encoding ASN.1 data to a stream of octets that can be transmitted over a communications link. Other methods of encoding ASN.1 data include Distinguished Encoding Rules (DER), Canonical Encoding Rules (CER), and Packing Encoding Rules (PER). Each encoding method has its application, but BER tends to be the encoding method most commonly used for SNMP.

BER defines

- Methods for encoding ASN.1 values.
- Rules for deciding when to use a given method.
- The format of specific octets in the data.

2.6. Functions of CORBA

CORBA is the acronym for Common Object Request Broker Architecture, Object Management Group's open, vendor-independent architecture and infrastructure that computer applications use to work together over networks. Using the standard protocol IIOP (Internet Inter-ORB Protocol), a CORBA-based program from any vendor, on almost any computer, operating system, programming language, and network, can interoperate with a CORBA-based program from the same or another vendor, on almost any other computer, operating system, programming language, and network.

CORBA is useful in many situations. Because of the easy way that CORBA integrates machines from so many vendors, with sizes ranging from mainframes through minis and desktops to handheld and embedded systems, it is the middleware of choice for large (and even not-so-large) enterprises. One of its most important and most frequent uses is in servers that must handle large number of clients, at high hit rates, with high reliability. CORBA works behind the scenes to allow systems using different hardware, operating systems, and programming languages to communicate. Specializations for scalability and fault-tolerance support these systems. But CORBA is not used just for large applications; specialized versions of CORBA run real-time systems, and small embedded systems.

The Common Object Request Broker Architecture (CORBA) is an emerging open distributed object computing infrastructure being standardized by OMG (Object Management Group). CORBA automates many common network programming tasks such as object registration, location, and activation; request demultiplexing; framing and error-handling; parameter marshalling and demarshalling; and operation dispatching.

The goal of CORBA is to allow the interactions between those systems to be defined in a platform-independent way, giving the system a set of well-defined interfaces to be connected to one another. This allows applications to be split into pieces (fine grained client/server applications) where components may be running on different parts of a network, on different kinds of computers, perhaps with components written in varying computer languages.

Make systems talk with each other

The key point of CORBA is that it provides a way for two programs to communicate information. The CORBA mechanism allows these two programs to be running on different machines and written in different programming languages while safely (and portably) exchanging data. They also could be running in the same program, on the same machine, in which case the process of communication is much quicker as CORBA recognizes that it does not need to open any communication channel. The CORBA mechanism is ideal for classic client/server applications, say a graphical client GUI communicating to a database server. All of these concepts have been translated into a tool that makes our lives easier. That tool is actually an architecture that is called CORBA.

Client and Servers

In CORBA, any invocation involves a caller and a callee. In CORBA terminology, they are referred to as the client and the server, respectively. Note, though, that the client and server roles may change in later calls. CORBA supports peer-to-peer communication and any node on the network may choose to be a client, server, or both. To be a client, the program makes invocations on objects elsewhere in the network. To be a server, a program must create objects and make them known to the rest of the network via the ORB (Object Request Broker).

2.7 Network Structure

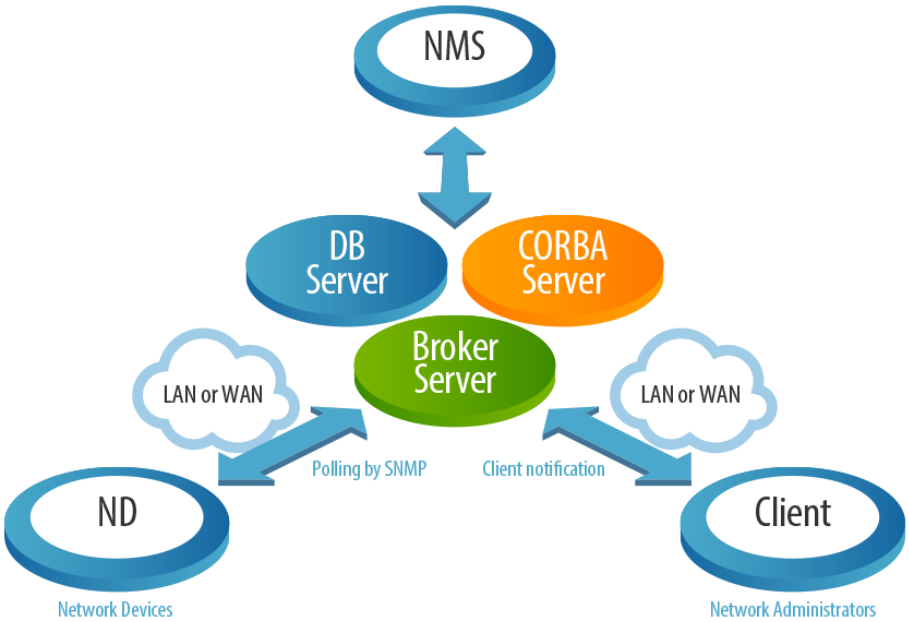


Figure 2-1 A block diagram of the EMS network

2.7.1. Agents

The very first product brought into the SmartView EMS was the FMUX01A. The FMUX01A is a 1U (1.75") high standalone or 19" rack mountable E1/T1/Data/LAN Bridge 16 channel multiplexer over fiber link, built upon a highly modular design. Other SNMP enabled products have been added to the EMS with the goal of having all of CTC Union's products managed under the umbrella of this single Element Management System.

2.7.2. CORBA Server

CORBA Name Service provides the ORB (Object Request Broker) central component of CORBA. It encompasses the entire communication infrastructure necessary to identify and locate objects, handle connection management, deliver data and is responsible for communication of requests.

2.7.3. Broker server

The Broker Server collects the information data from the specified SNMP agents and keeps updating it to the SQL server database via the JDBC (Java DataBase Connectivity) driver. Broker server is synonymous with EMS Server.

2.7.4. SQL Server

The SQL Server is the place where data is stored as the Broker collects data from SNMP agent drivers; the database will keep Alarm Traps and all performance information.

2.7.5. Workstation-Clients

The Workstations act as clients in the CORBA architecture. They utilize a JAVA applet GUI to monitor and control the Network Devices at the far end, and also receive the Alarm Traps from the corresponding SNMP agents. Multiple workstations are allowed in this server/client topology. The client may reside on the same physical machine as the server or it may be run remotely and use a network connection to the server.

This page left blank intentionally.

Chapter 3 Installing EMS

3.1 Installation Description

This chapter will describe in detail the installation procedures for the EMS (Element Management System).

3.2 Basic Requirements for EMS

This document has been arranged in such a way, that there are only two major steps, installing SQL Server and EMS Server. Manual installation of SQL Server has been separated and detailed into separate appendices for clarity at the end of this document. The installation process is performed from the EMSInstaller in just two steps (i.e., Install SQL server, then install EMS).

3.2.1. Basic knowledge and prepare to start

Before starting, please confirm that all Workstations, Servers and SNMP agents can communicate with each without problem, e.g. using ICMP ping command to diagnosis IP routes have been setup properly. EMS has been integrated into four components, the Broker Server, the SQL Database Server, the CORBA Name Service and multiple workstation Clients running EMCs (Enterprise Management Console). Each component has its own task and purpose. You can place each of these components on different hardware or all on one computer to handle all those tasks.

EMS has been developed under the JAVA environment; You could have EMS running on different OS platforms. However, in its current form, EMS relies on the MS-SQL database and therefore the database server and EMS server must be running in a MS-Windows environment. The following section will describe how to setup your EMS on MS-Windows.

Table 3-1 lists the Hardware recommendations and Software programs necessary for EMS Server/Client.

EMS Component	Hardware	Software	Operating System
EMS Server & name server	Core-2 2.8G or higher, 4096 MB RAM, HD >2GB (free).	JAVA JDK or JRE, v1.7.x.(64) EMS Kit.	Windows 64 bit
SQL database Server	Core-2 2.8G or higher, 4GB RAM, HD >10GB (free).	MS-SQL Server 2008, 2012 or 2014, including Express Edition EMS Kit.	Windows 2012/16/19 Server, (64bit) Win 8, 8.1 Pro, Win 10 Pro**
Workstation-Clients	Core-2 or higher, 2048MB RAM, HD >1GB.	JAVA JDK or JRE, v1.7.x.(64) EMS Kit.	Windows 64 bit (8, 8.1, 10)
All-In-One (EMS, name & SQL Server on one machine)	I5 or higher, 8GB or more RAM, HD >40GB (free)	JAVA JRE, EMS kit, MS-SQL Server, JDBC Driver	Windows 2012/16/19 Server, (64 bit) Win 8, 8.1, 10 Pro

Table 3-1 Hardware & Software requirements for EMS components

With any of the chosen hardware platforms, do routine maintenance to the systems. Download and apply any service packs and security updates. Perform virus and disc scans and file system checks. Do de-fragmentation on the discs to increase performance. Ensure all cooling fans are clean and operational and that any heat sinks are free of debris. Maintain the systems in a temperature and voltage stable environment. UPS for power stability is highly recommended on any computing system but even more so on a management server.

We recommend dedicating hardware or a virtual machine (VM) just for running the EMS and no other services. If you only run the EMS and no other services, a Core-2 2.0G CPU should show CPU utilization under 10%. If the server's CPU is always busy doing other jobs, then it won't have time to properly poll the network agents. You can check the CPU's utilization by opening the 'Task Manager' and view the CPU utilization graph. You can then also shut-down the EMS server to see if utilization drops to zero, or you can see what other processes are taking up CPU resource when EMS is not running, and shutdown those unneeded processes.

3.3 Setup EMS

3.3.1 Introduction

Starting with the release of EMS 2.34, the installation procedure has been streamlined with a GUI installation shell and unattended installation of MS-SQL 2008 R2 Express or MS-SQL 2014 SP2. The preferred method of installation is by using the EMS DVD. The DVD will be shipped in a full shrink-wrapped package. A ZIP file may also be downloaded, upzipped locally and run from local disk. The installation process will follow these basic steps:

1. Autorun the DVD or from the unzipped files run the "EMSInstaller.exe" program as administrator.
2. Install MS-SQL Database Server (single click un-attended installation of SQL Server Express Edition 2008 R2 SP2 on Windows 7 or SQL Server Express Edition 2014 SP2 on Windows 10 or Windows Server 2012, 2016 or 2019).
3. Exit the "EMSInstaller".
4. Restart the "EMSInstaller" and Install EMS.
5. Take ownership of the ProgramFiles\EMS folder.
6. Apply any EMS upgrade patches and re-initial database (if required).
7. Install license or manually copy your authorized SN.txt file.

3.3.2 EMSInstaller

Insert the DVD into your PC's DVD/BD drive. Open the DVD folder and right-click the "EMSInstaller" icon, choose 'Run as administrator'. Optionally, if you have downloaded and unzipped the installation set to local disk, browse to and right-click the EMSInstaller program and choose 'Run as administrator'.

1. DVD Distribution

The DVD is designed to be Autorun. It includes the 64bit 1.7.0.80 Java Runtime Environment Binaries and Microsoft's free MS-SQL Server 2008 Express and MS-SQL Server 2014 Express in English, Traditional Chinese and Simplified Chinese. If Autorun is disabled on your PC, open the DVD folder and right-click the "EMSInstaller" icon and choose 'Run as administrator'.

2. Download

The download file is a ZIP file (a folder of the original DVD but with MS-SQL Server 2008/2014 Express for English only). Use extraction software, such as 7-Zip (or WinZip™), to extract the file to the local drive. After being unzipped the EMSInstaller can be run (right-click and choose 'Run as administrator') directly from those extracted files.

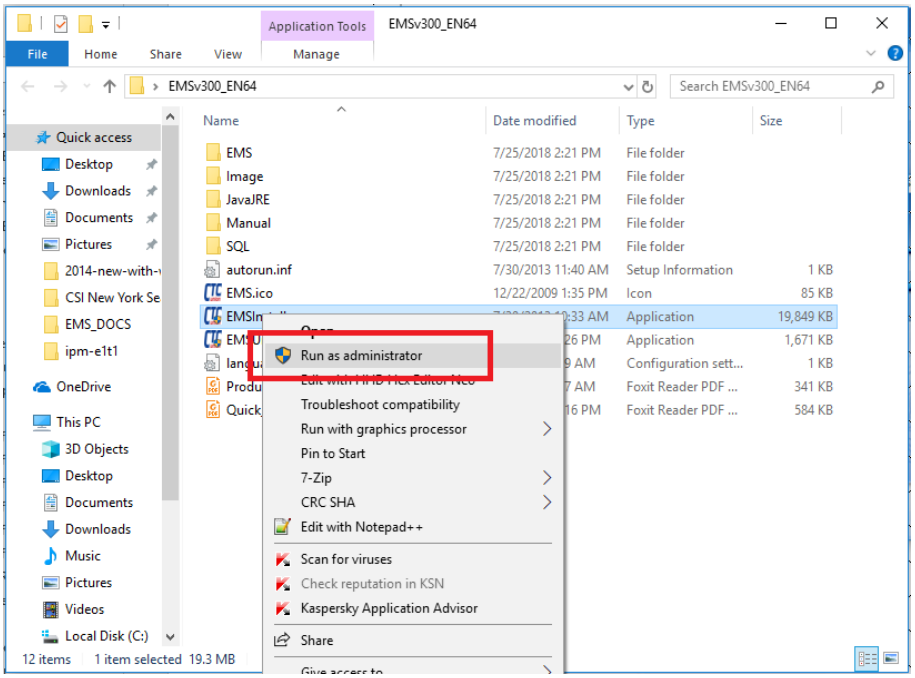


Figure 3-1 Installation folder, ready to install EMS.

3.3.3 EMSInstall Screen

Figure 3-1 The installation is available in English or Chinese language via the Language pull-down selector.

3.3.4 About Java Run Time Environment

The EMS Broker and Client are written in JAVA™ programming language. Java was an open programming language developed by Sun Microsystems and volunteer programmers. The idea was to have a programming language that would be portable across different hardware processors and operating systems and not require re-compiling of the source program on each platform. Oracle now controls this programming language, while the OpenJDK project continues the free open source JAVA released by Sun Microsystems in 2006.

SmartView v3.xx is compatible with the 64-bit Oracle Java version 1.7, but not fully compatible with 1.8. EMS version 3.xx includes the 64 bit version 1.7, Update 80 Java Runtime binaries within the EMS program folder. It doesn't matter if the host computer has Java or not or what the Java version installed is. EMS will always use its own 64bit Java 1.7.0.80 binaries for maximum stability and compatibility. There is no need to install JRE on the host computer.

Figure 3-3 Do not click the Install JAVA Runtime Environment!

3.3.5 SQL Server Install

EMS relies on ***Microsoft***® MS-SQL database to store all information. Starting with EMS version 2.34, unattended installation is now the supported default. This means only "one click" is required to install any prerequisites, install SQL server and have it configured, ready for EMS. Please refer to the detailed instructions in Appendix A, B, or C, for manual installation of SQL Express 2008, 2012, or 2014**. Refer to your Microsoft documentation when installing your own SQL Server and reference our installation procedures.

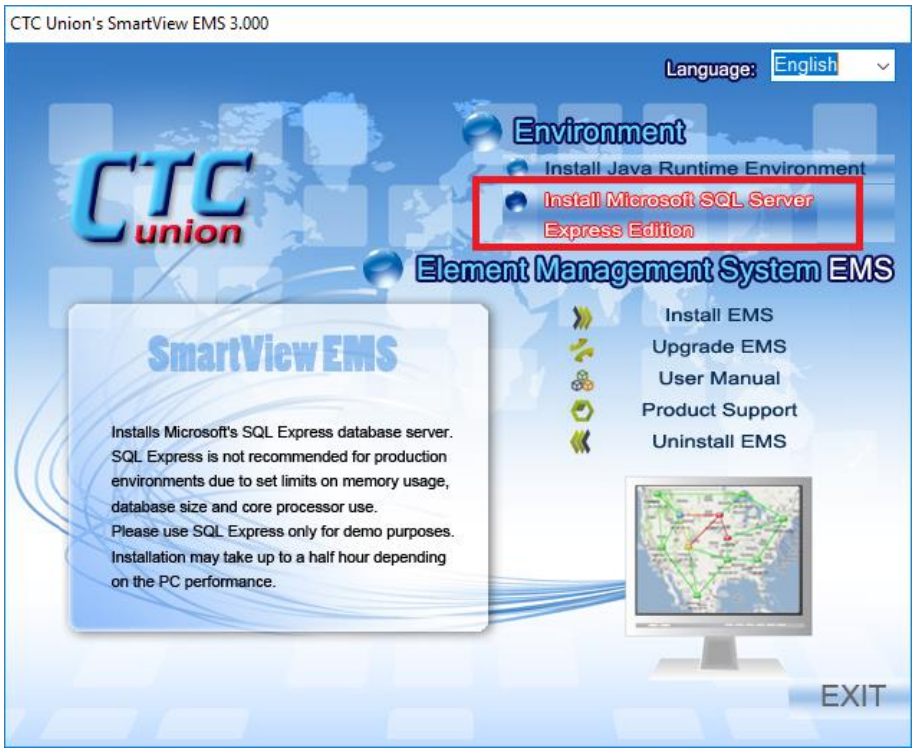


Figure 3-4 Click on "Install Microsoft SQL Server Express Edition" just one time.
** SQL2014 is the default for Windows 10/Windows Server 2016, 2019

Figure 3-5 Select the language for MS-SQL Server by clicking ONLY ONCE!

During the unattended SQL Server installation, the screen will flash several times as files are first extracted, the setup prerequisite files installed, if needed, and finally the SQL server application is installed. Just wait for the SQL Server installation to complete. This might take 5 to 10 minutes, so go grab a coffee.

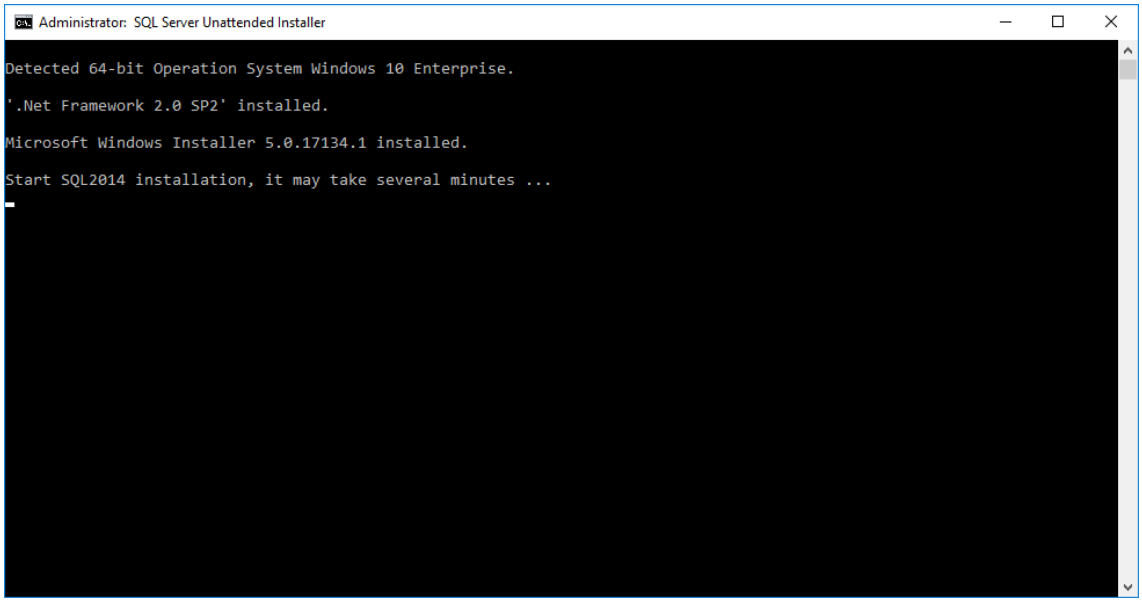


Figure 3-6 Wait for a few minutes here while Setup starts.

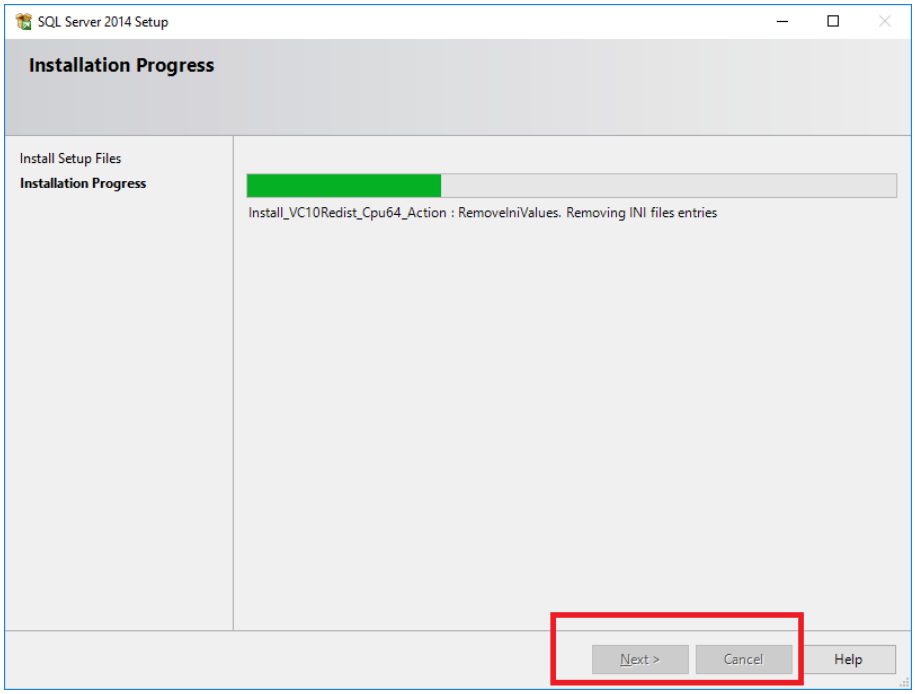


Figure 3-7 No user action is required during unattended installation of MS-SQL Server.

Following successful installation, the installer will ask if you want to keep the default SA password of '0000' (four zeros).

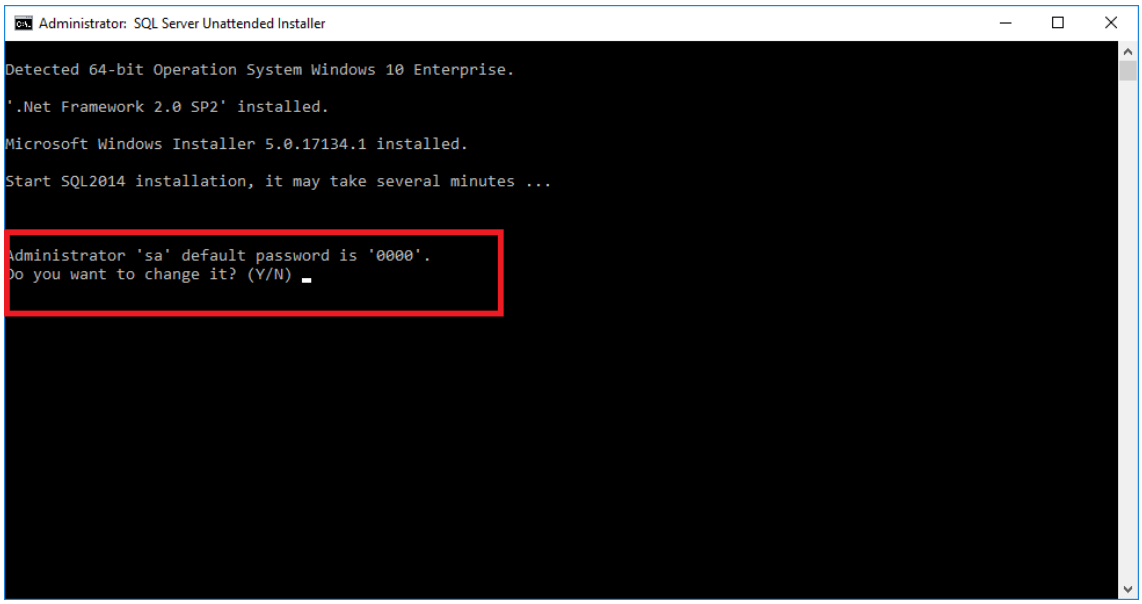


Figure 3-8 Prompt to change or leave the 'sa' password.

If you do not wish to change the password (recommended), answer "n" or "N". If you wish to change, answer "y" or "Y" and then enter the new password when prompted. But, remember, the SA password is required to successfully install SmartView.

Finally, press any key to exit the SQL installation batch program. Note: When installing MS-SQL on MS-Server, the password must meet administrator rules (at least 8 characters, an upper case and lower case letter, numbers and one special character).

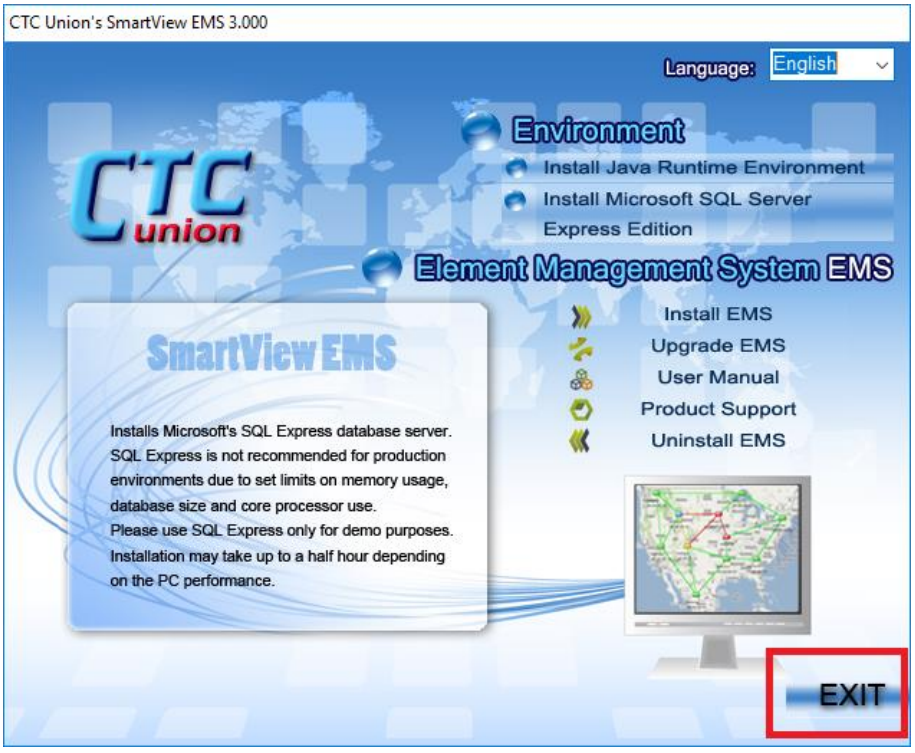


Figure 3-9 Now that MS-SQL Server is installed, exit the SmartView EMSinstaller.

You MUST exit the installer and restart the EMSInstaller so that the installer now knows the path to SQLcmd.

3.3.6 Install EMS

After exiting, browse again to the EMS installation folder and again run the EMSinstaller by right-clicking and choosing 'Run as administrator'.

Figure 3-10 Click Install EMS just once.

The EMSinstaller default installation path will place the EMS in the system root's "Program Files (x86)" folder. However, starting with SmartView 3.00, the EMS is a 64-bit program and MUST run under 64-bit OS. We recommend that EMS be installed in the 'Program Files' folder of the PC.

Click the "Browse" button and place EMS in the C:\Program Files folder and click "OK".

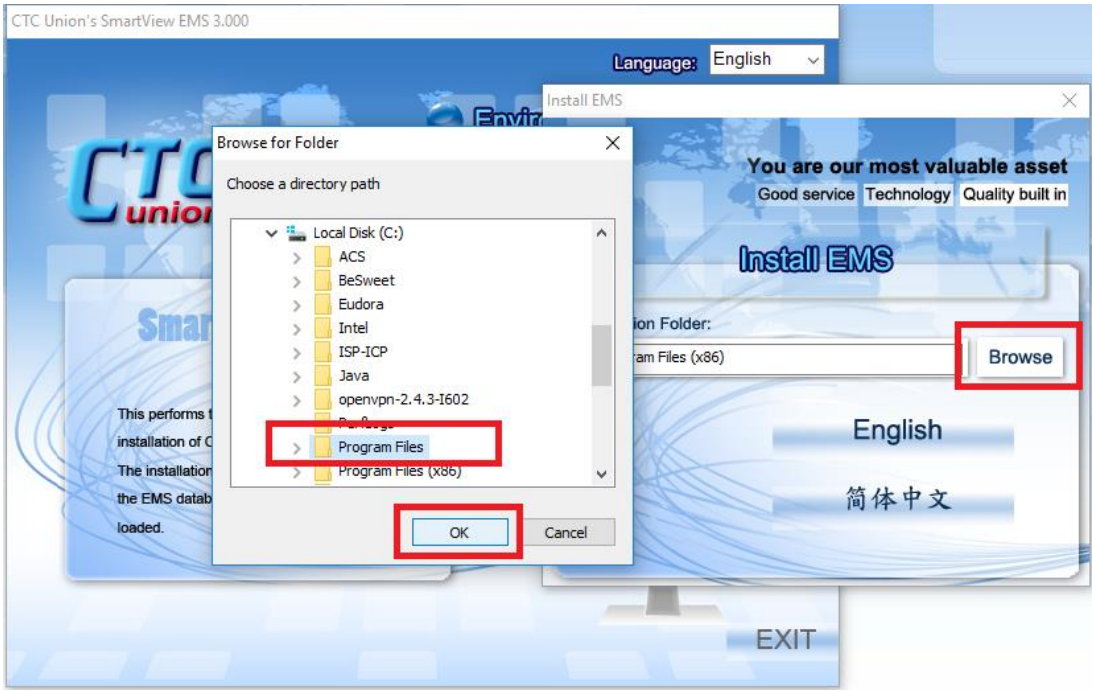


Figure 3-11 Install in the Program Files folder

This portion of the install will copy the required files to the PC, setup the desktop start icons for server and client, and start the EMS SetupTool.

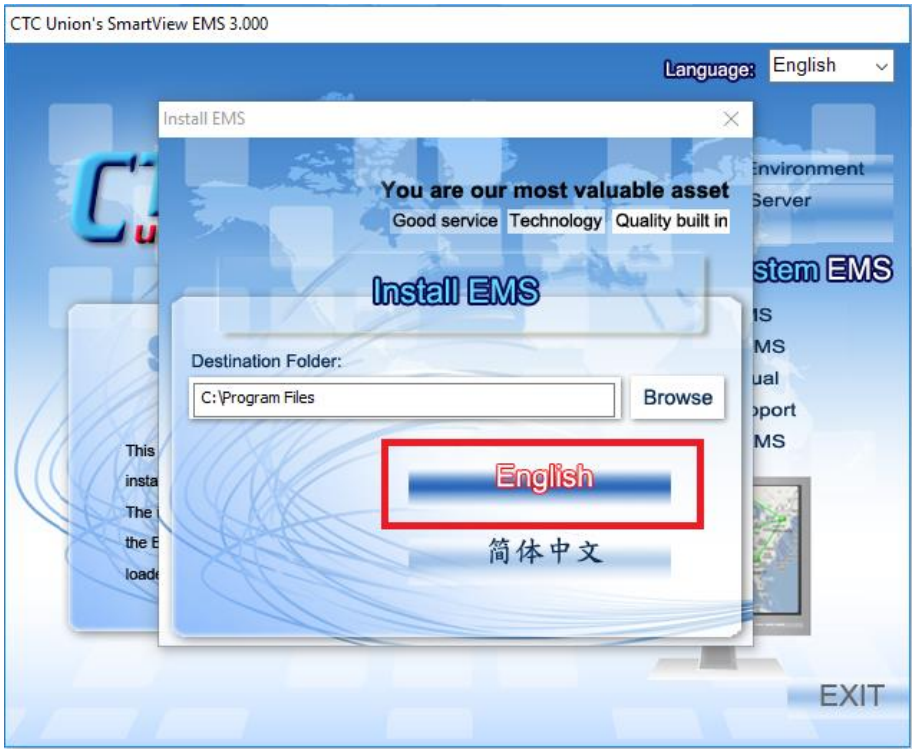


Figure 3-12 Start installation by clicking the "English" button.

3.3.7 Setup Tool

The Setup Tool is written in JAVA. If there is a problem with the JAVA environment, the tool will not be able to run. This will not be a problem in EMS versions after 2.84, which use embedded Java binaries.

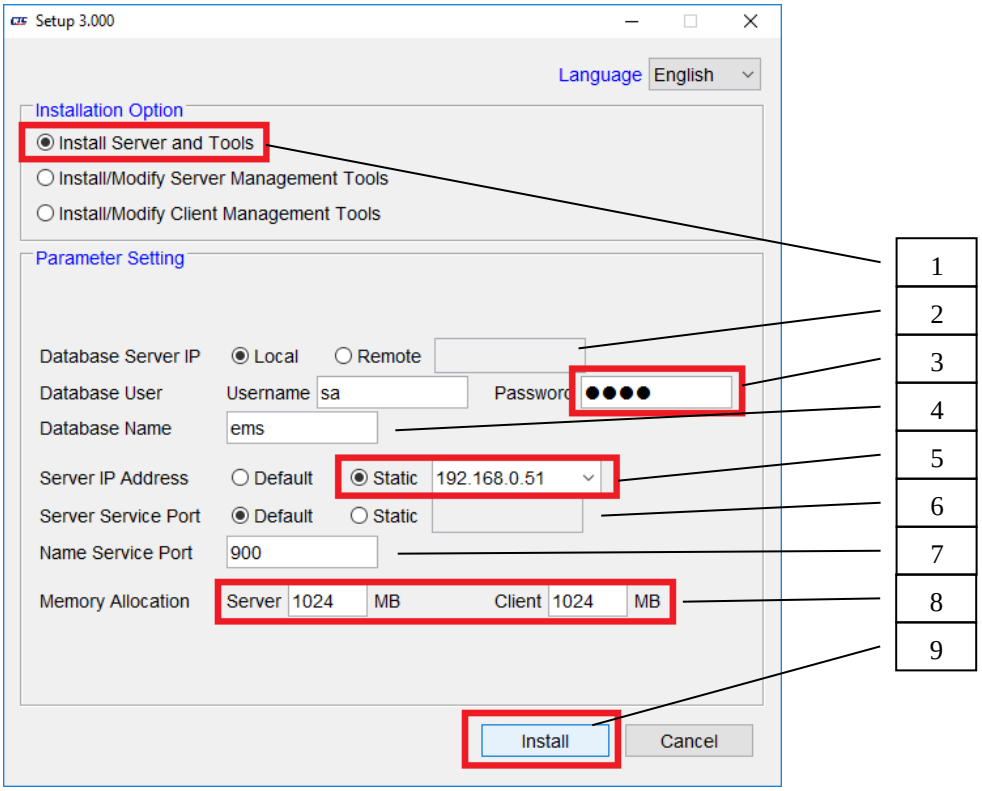


Figure 3-13 The Setup Tool

1. Since this is an initial installation, we need to "**Install Server and Tools**", therefore click the radio button for "Install Server and Tools" if not already selected. If after installation any of the configuration items need modifying (such as changing the IP address of the server, please select **"Install/Modify Server Management Tools"**. If installing only the remote "Client" software, select the **"Install/Modify Client Management Tools"**.

2. The "**Database Server IP**" is the IP address where EMS server will find the SQL server. The "Local" setting means that EMS will connect to the Database server via localhost (127.0.0.1). This is the recommended setting if the EMS server and Database server are on the same physical machine. This provides the best performance as well as allows EMS to Database connections to exist even if the physical server changes IP address or if the LAN cable is disconnected. For remote database server connection, select the 'Remote' radio button and enter the SQL server's IP address.

3. The SQL "**Database User**" is the name granted authority over creating and accessing the ems database. The default administrator user in mixed mode for MS-SQL is "sa" and EMS requires that the SQL server must be installed with mixed-mode authentication. Unless an administrator has created another user with authority to create a database, please use the "sa" user during this installation. If SQL server was installed from the EMS DVD or ZIP Download using default settings, the password for 'sa' will be four zeros (0000). For Windows Server, the default password is Pa$$w0rd.

4. The default SQL "**Database name**" for the database created by the setup tool is "ems". Change it here if you wish to use a different name. We HIGHLY recommend you leave it "ems".

5. The "**Server IP Address**" can be selected from either "Default" or "Static" settings. The EMS server's "Default" uses the first network interface in the server hardware. If the server has multiple NIC or multiple IP addresses, select the "Static" radio button and pull-down or enter the static IP address the EMS server will use. This is the setting that would be required if a laptop were being used to "demo" the EMS. Laptops typically have both a LAN interface and a WiFi interface. So, in order for EMS to know its own address, we would use the static IP address of the LAN port.

6. The "**Server Service Port**" can be selected from either "Default" or "Static" settings. When set to "Default" the port numbers used will be random. This will only be a problem if the EMS Client is separated from the EMS Server by a firewall. In this case, select the "Static" radio button and assign a fixed port number for the EMS Server's service. Then, open that port in the firewall to allow routed clients to connect to the server. Use an unregistered or reserved port that no other application will use (such as port 1030).

7. The default CORBA "**Name Service Port**" connection port is '900'. For Windows clients connecting to the EMS server, this is not a problem. But for EMS Clients running on UNIX/Linux, ports under 1024 are restricted to only root user. An acceptable alternate port for a normal user on UNIX/Linux would be '1050'. The port setting for the name server is made here.

8. The "**Memory Usage**" parameters typically do not require modification unless there are large numbers of Network Devices (ND) being polled. The default EMS Server and Client memory usages is 512MB each. This number would need to be increased, for example, if many ND were being managed. The recommended memory requirement to manage an FRM220 chassis is 2MB. If the network had 200 FRM220 chassis being managed, we would need 400MB. When increasing the memory usage, add memory in multiples of 128MB. When increasing from 512MB we could enter 640, 768, 896 or 1024. The physical memory in the server running EMS is really the most critical for performance, not the speed or number of processor cores. Processor speed and number of cores are only an advantage when polling with multiple threads. Multiple polling threads are also a new feature added starting with EMS 2.45. Since this 64 bit version 3.00, there is basically no memory setting limit (except for the server's physical memory) as there was with the older 32 bit EMS.

9. When all the settings are correct, click the "Install" button to start the installation.

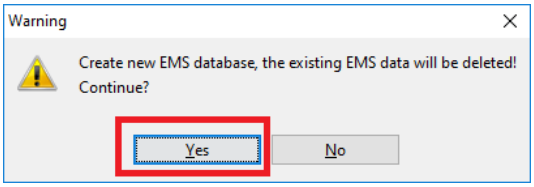


Figure 3-14 Click "Yes" to create or overwrite the EMS database for this new installation.

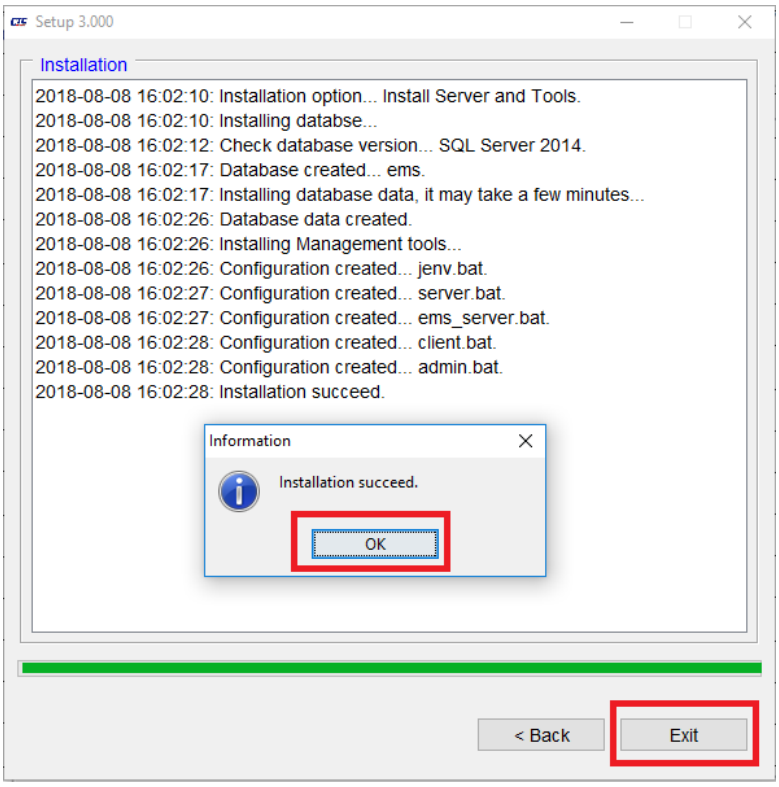


Figure 3-15 Click the "OK" button after the EMS has been installed successfully and then click "Exit".

Figure 3-16 "Exit" the EMS Installer. Be sure to perform the next steps to take ownership of EMS folder.

3.3.8 Take ownership of EMS Folder

Microsoft Windows 7 Pro, Windows 8/8.1 Pro and Windows 10 Pro all introduce permission settings on system files, such as those located in the windows and program files folders. Unless the administrator account has been enabled and the user is using administrator to log into the system (which is not particularly secure), any attempt to update the EMS will fail due to write access denied.

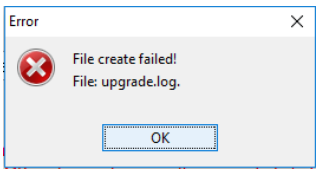


Figure 3-17 Error message

A simple fix here is to change the permissions on the EMS folder. Here is how to change the permissions for all normal logged in users.

Step 1. Browse to the **Program Files** folder and **right-click** on the **EMS** folder. Select **Properties**.

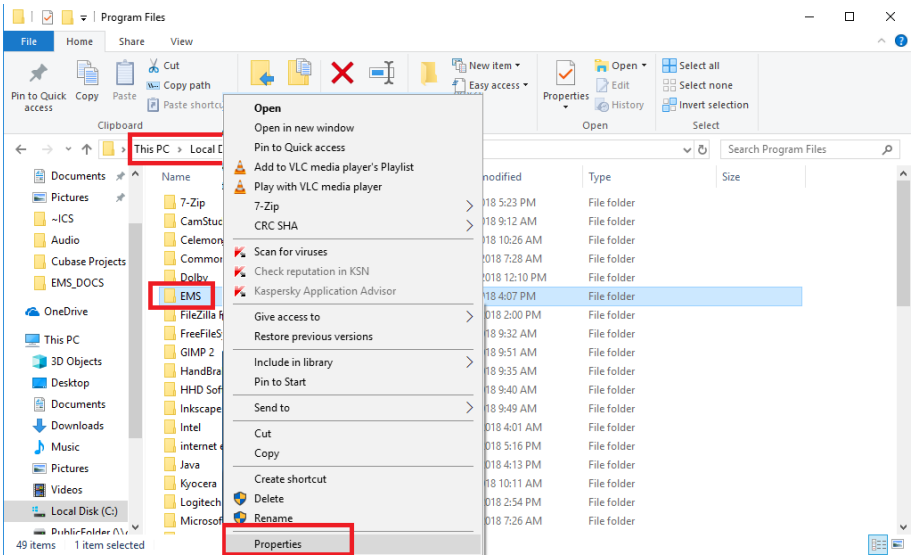


Figure 3-18 Select EMS folder properties

Step 2. Select the **Security** tab.

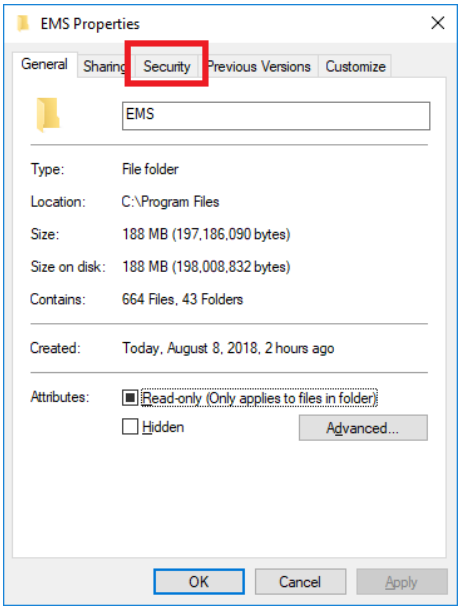


Figure 3-19 Security Tab

Step 3. Under the **Security** tab, click the **Edit** button.

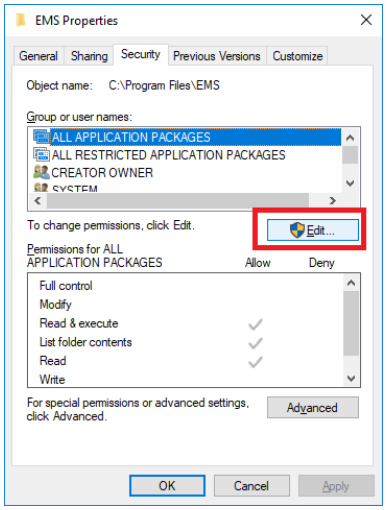


Figure 3-20 Edit Permissions

Step 4. Select the **Users** for this computer.
Step 5. Click the **Full control** and **Modify** permissions for users (both will be checked).
Step 6. Click **OK**.

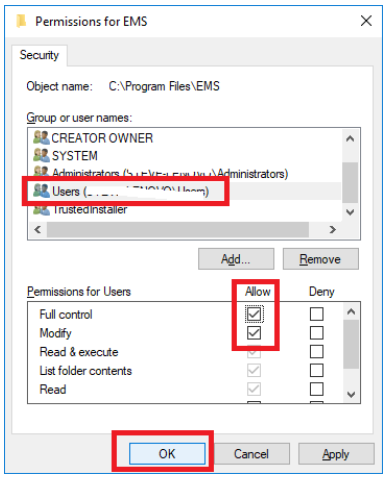


Figure 3-21 Allow users full access

Step 7. Click **OK** again.

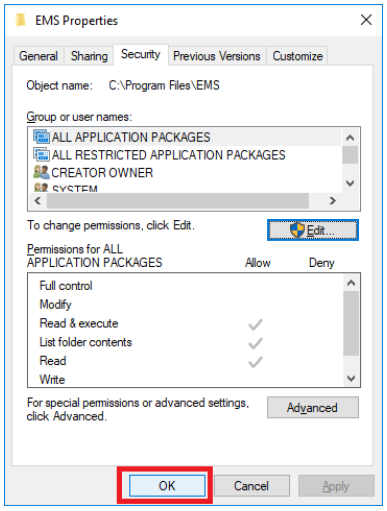


Figure 3-22 Close the Properties window

Now that all users have full permission for the EMS folder, the update patches and configuration changes can be applied without any error messages regarding file access rights.

3.3.9 Using Update Tool

CAUTION: EMS version is tightly matched to NMC or other firmware versions of CTC Union products. Prior to doing any upgrading of EMS, please ensure all ND (Network Devices) are properly upgraded and compatible with the new EMS version (refer to the included Product_Support.PDF with any SmartView version). There is no method to "down grade" the EMS except to re-install the previous version as changes are made to the database through upgrade and cannot be rolled back. Making a backup of the database and of the entire EMS folder will aid in doing a quick recovery. Please see the Appendix on the methods to perform a complete backup of the EMS system and database before performing EMS upgrade.

Find the latest Upgrade Tool from CTC Union's download area.
https://www.ctcu.com.tw/download/EMS/

IMPORTANT: Make sure clients are logged off and terminated, the Admin Console logged off and terminated and that the Server Console is 'stopped' and terminated prior to doing any Upgrade.

The Upgrade Tool will be distributed as a 'ZIP' file. Move it to the EMS server's desktop and extract in place. Click into the 'Upgrade' folder, 'right-click' on the 'upgrade.bat' file and select 'Run as Administrator'.

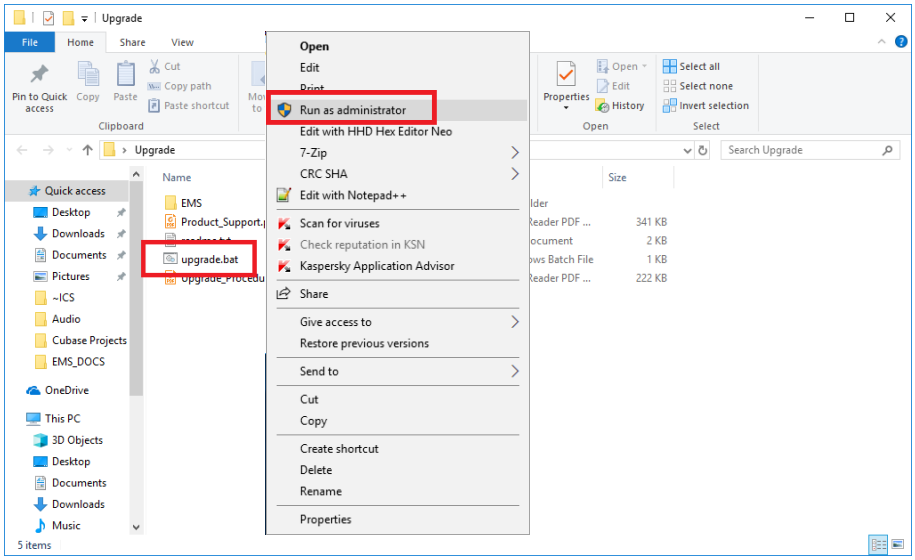


Figure 3-23 Upgrade Batch file in extracted Upgrade ZIP file.

The Setup Tool for Upgrade will start. (Hint: for 64 bit OS, EMS should be in C:\Program Files\EMS)

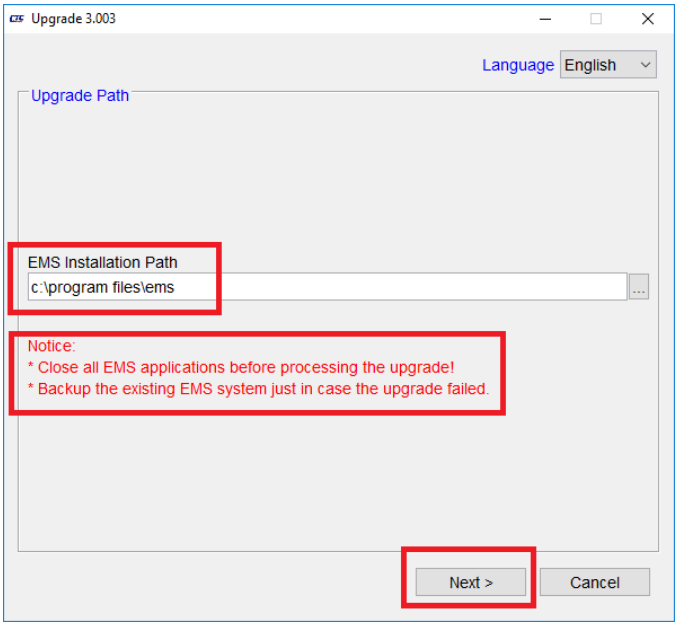


Figure 3-24 The installation folder is auto detected for EMS, so just click "Next".

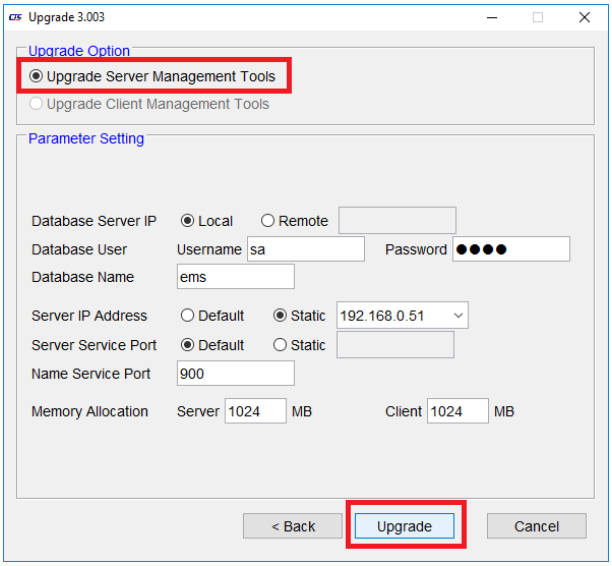


Figure 3-25 Start the upgrade from Upgrade Tool

All settings should be identical to the original installation or the previous upgrade. Make sure the Database Server IP, Database user and password and Database name are correct. Make sure the Server IP address and port are correct. Make sure the CORBA name service port is correct. Make sure any client on the local server is logged out and client has exited. Logout and close **Admin Console** if it is running. Stop and exit the EMS server. Then click "**Upgrade**".

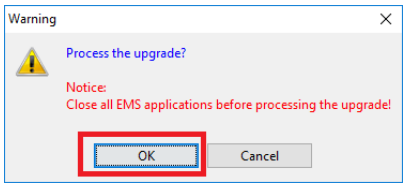


Figure 3-26 Confirmation. Heed the warning notice!

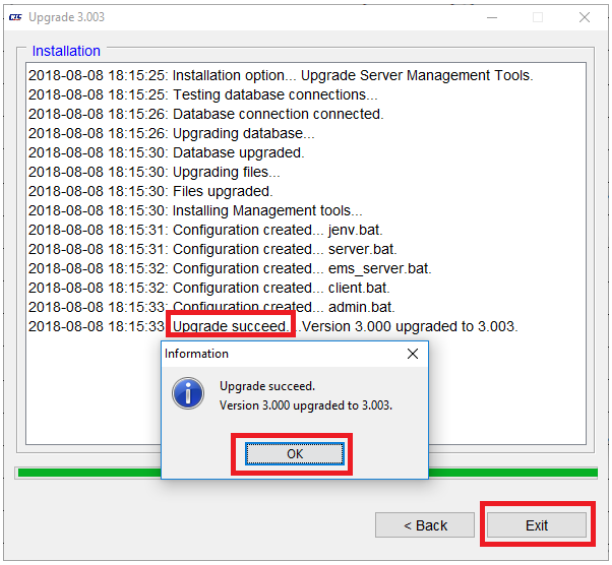


Figure 3-27 Upgrade completed successfully.

Warning: Under Windows Vista and above (Windows 7, 8, 8.1, 10), unless the logged in user is the Administrator, the Upgrade Tool will fail to write the new files into the protected EMS folder. Refer to 3.3.8 or 8.1.1 for a short guide on how to take ownership of the EMS folder.

3.3.10 Uninstalling SmartView EMS

On an occasion when EMS must be un-installed, the uninstall methods are outlined here.

1. Prior to running the uninstaller, make a backup copy of the license file (SN.txt) located in the Program Files\EMS folder. This file can be re-installed or manually copied back in a new installation on the same PC. However, it WILL be deleted during the un-install.

2. Perform Uninstall through the Window's Start Menu.

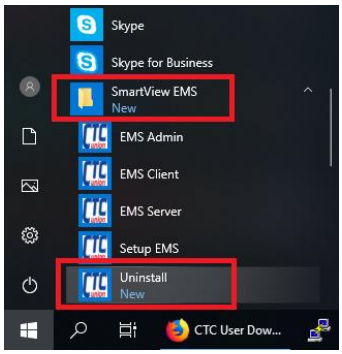


Figure 3-28 Windows Start Menu Uninstall

2. Perform a manual uninstall (run with administrator privileges)
   a. Delete the EMS installation folder, located in c:\Program Files.
   b. Delete the EMS Server and Client shortcuts from the Desktop
   c. Delete the 'SmartView EMS' folder in:
"c:\Users\{username}\AppData\Roaming\Microsoft\Windows\Start Menu\Programs"
   d. Delete the registry key \\HKLM\SOFTWARE\Wow6432Node\EMSInstaller

3.3.11 Serial Number File

The EMS system requires registration and a serial number file placed in the EMS directory or it will only run in evaluation mode. This "authentication" file is keyed to the host computer's MAC address. If you are changing hardware or upgrading, you may have to apply for a new serial key to match the new MAC address, or simply move the old NIC (Network Interface Card) to the new hardware platform and the EMS will continue to find and confirm the authentication key.

The serial number file is a simple text file that may be opened and viewed with any pure text editor, such as Windows Notepad. If you maintain many keys, the MAC address is listed at the last line of the SN.txt file. There are two methods to install the license; 1. Manually copy, or 2. Use the Server Console tool.

1. Manually installing license

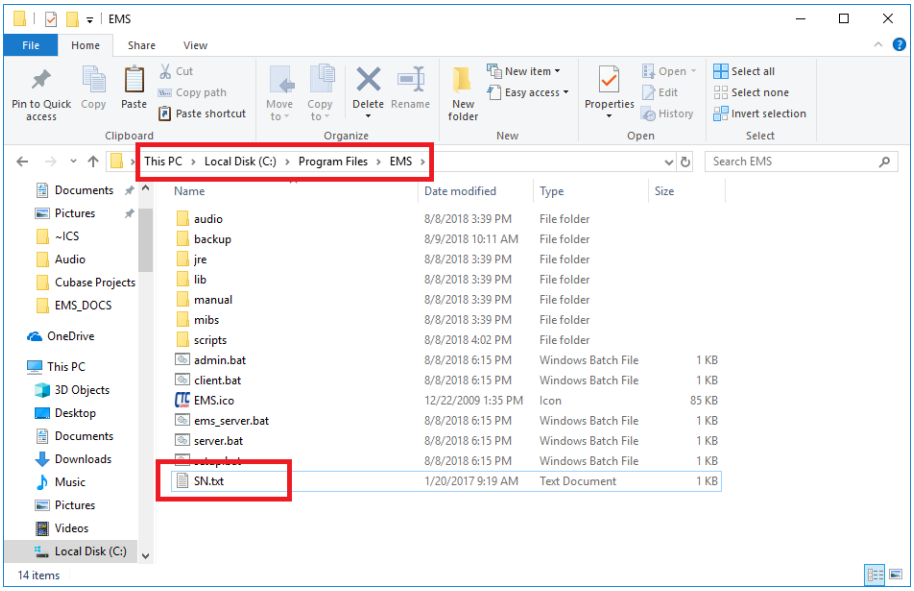


Figure 3-29 Manually copying license file to EMS folder

2. Installing license via the Server Console

Click the 'Tools' menu item of Server Console and select the "Import License" item.

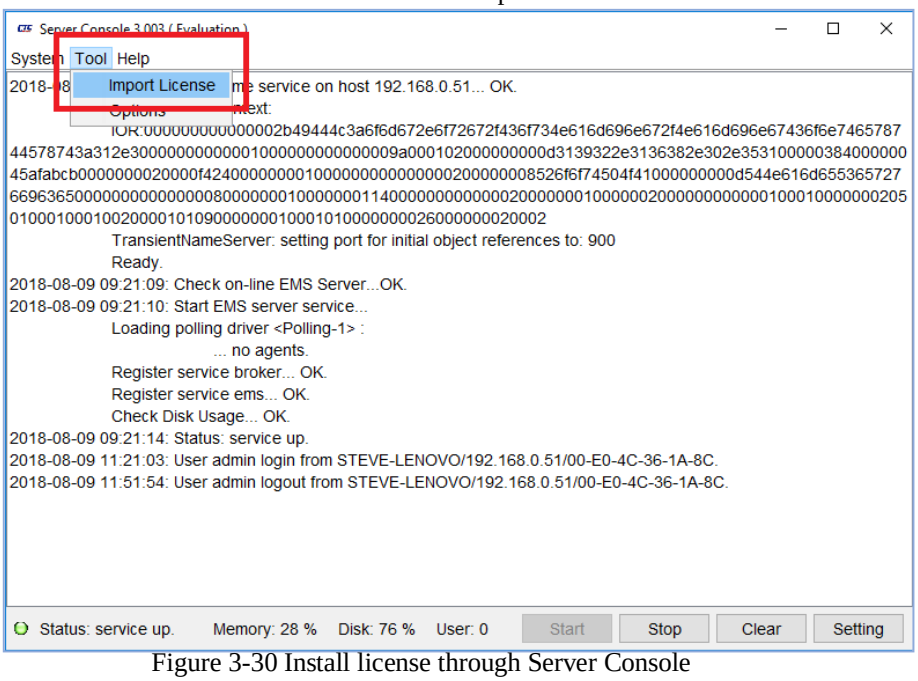


Figure 3-30 Install license through Server Console

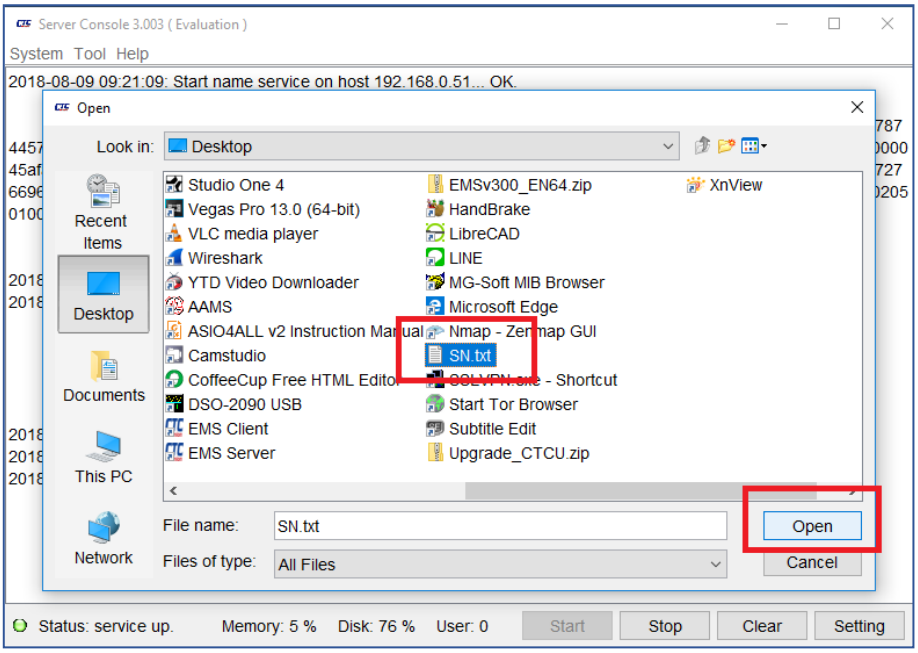


Figure 3-31 Select license file for installation

Browse to and select the SN.txt file. Click "Open" and it will be automatically copied to the EMS installed directory.

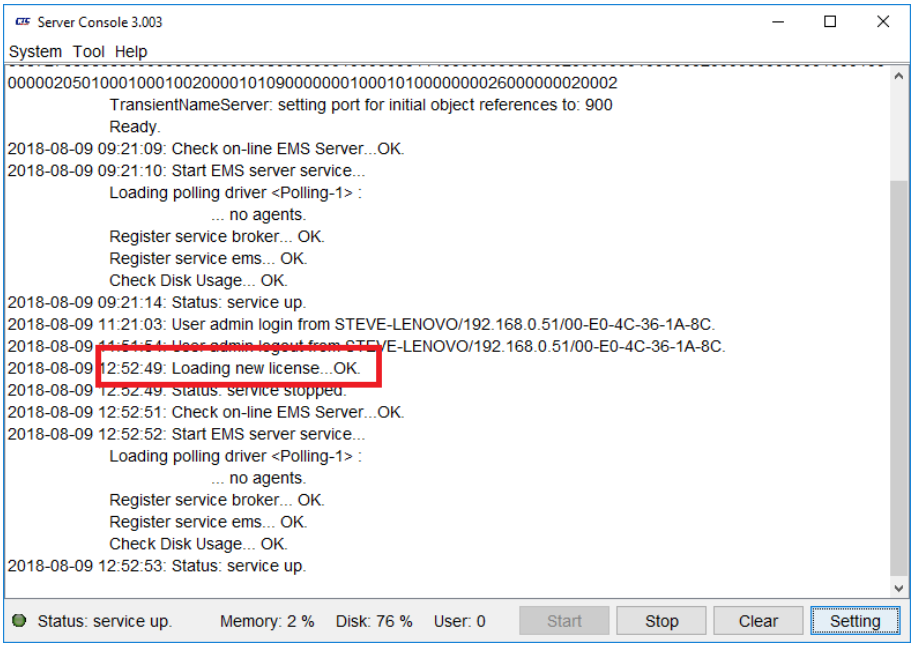


Figure 3-32 Successful license installation

After the license is installed, the server will automatically re-start.

3.3.12 Evaluation Version EMS

Version 3.xx of SmartView EMS is a FULL FEATURED evaluation version which allows the EMS to run in '**evaluation mode**' WITHOUT any serial key. The EMS is one software, but with two different actions:

If EMS detects a valid license file, it runs all functions normally within the limits of the license. Otherwise, it runs in Evaluation mode, with the following limits:

- 90 days Evaluation. (Run setup and recreate database must be done to continue)
- 15 Managed SNMP Agents.
- All Device Modules. i.e. PDH, FOM, FRM, Industrial and CWDM
- 1 only Login Client at a time. (local or remote)

3.3.13 Resources

For **MS-SQL** evaluation versions or for the free Express editions, go to the Microsoft Download Center page at:
http://www.microsoft.com/en-us/download/
In the "Search Download Center" bar, key-in "sql server express".
Valid downloads would include:
SQL Server Express 2008 R2 SP2 (Win7) 1G memory, 1 physical processor (4-cores), 10G database storage
SQL Server Express 2012 SP3 (Win 7, Server 2008 R2) 1G memory, 1 physical processor, 10G database storage
SQL Server Express 2014 SP3 (Win 8,8.1,10, Server 2012,2016,2019) 1G, 1 cpu (4-cores), 10G database
SQL Server Express 2016 SP2 (Win 8,8.1,10, Server 2012,2016,2019) 1G, 1cpu (4-cores), 10G database
(EMS version 2.89 or above is required to support SQL2012 and above)
EMS 3.xx ships with the 64 bit version of SQL Server Express 2014 SP2 and 64 bit version of SQL Server Express 2008 R2 SP2.

3.4 Console Server Tools

In addition to the license import (see 3.3.11) an **Options** menu item is available under Tools.

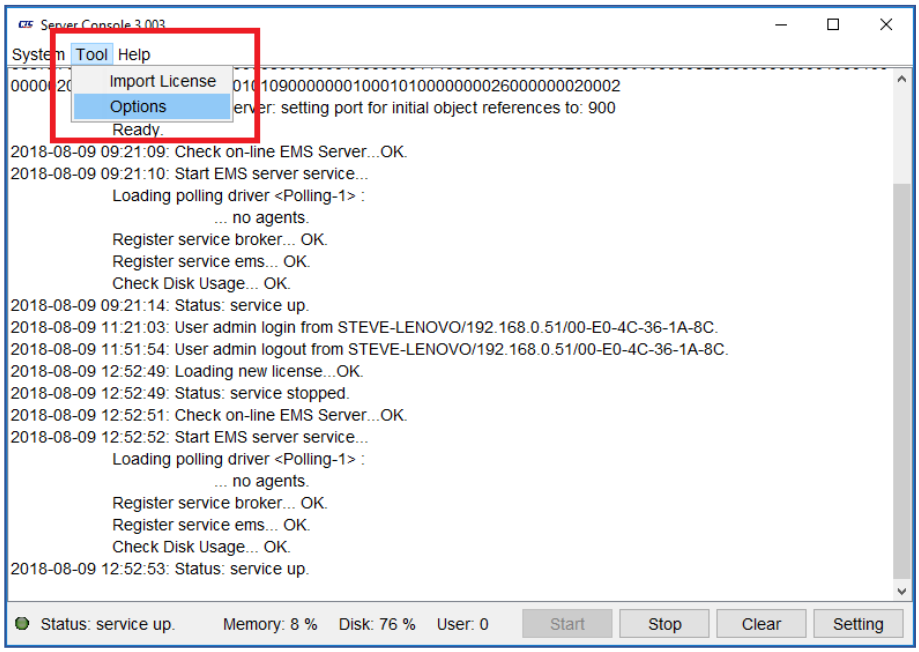


Figure 3-33 Options Menu Item

3.4.1 Memory

The Memory allocation is displayed for the EMS Server (read only).

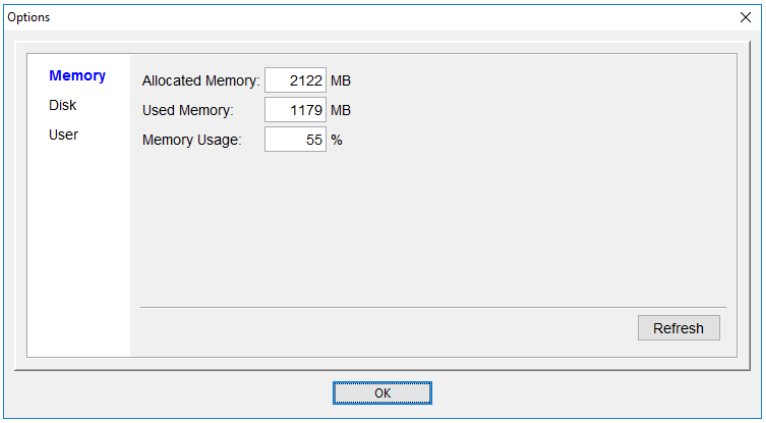


Figure 3-34 Memory Display

3.4.2 Disk Allocation

The Service Stop and Warning Usage are both writable variables. After changing, click 'Apply'.

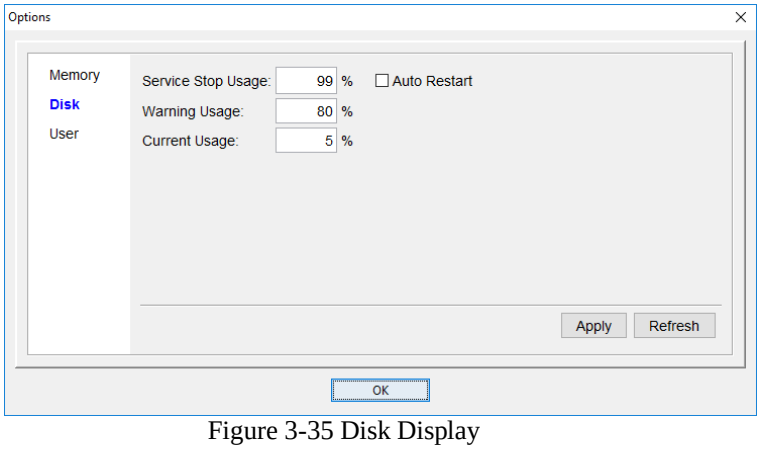


Figure 3-35 Disk Display

3.4.3 User

The **User** that are logged in along with how long they have been logged in are displayed here.

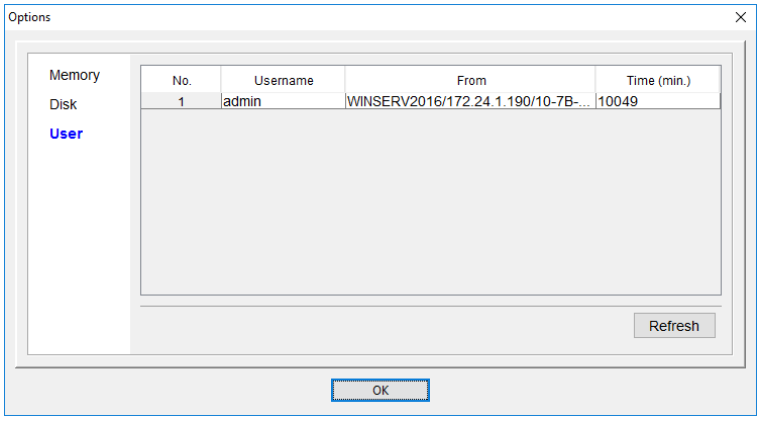


Figure 3-36 Users Logged In

3.5 Startup and shutdown EMS

Follow this procedure after the normal installation and broker configuration have been completed (see Chapter 4).

Startup:

1. Make sure the SQL Database is running.

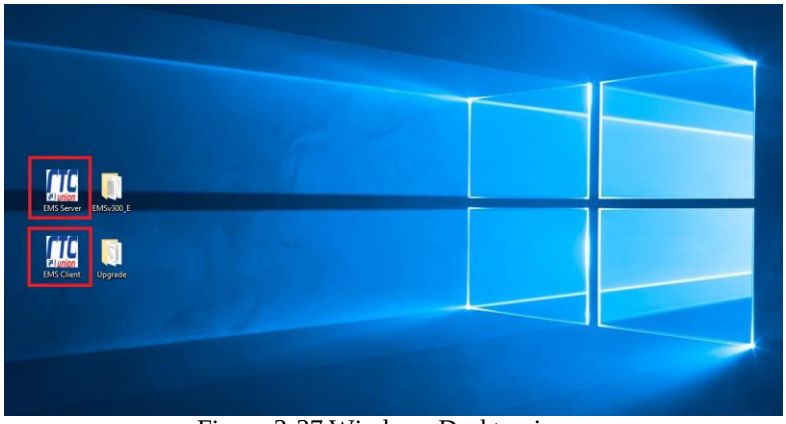


Figure 3-37 Windows Desktop icons

2. Shortcuts to the EMS Server and EMS Client will have been placed on the Desktop during installation.
3. Double-click the "EMS Server" icon to startup the EMS Server Console.
4. Double-click the "EMS Client" icon to start the Element Management Console.

Shutdown:

Logout and close any Admin or Management consoles, then:

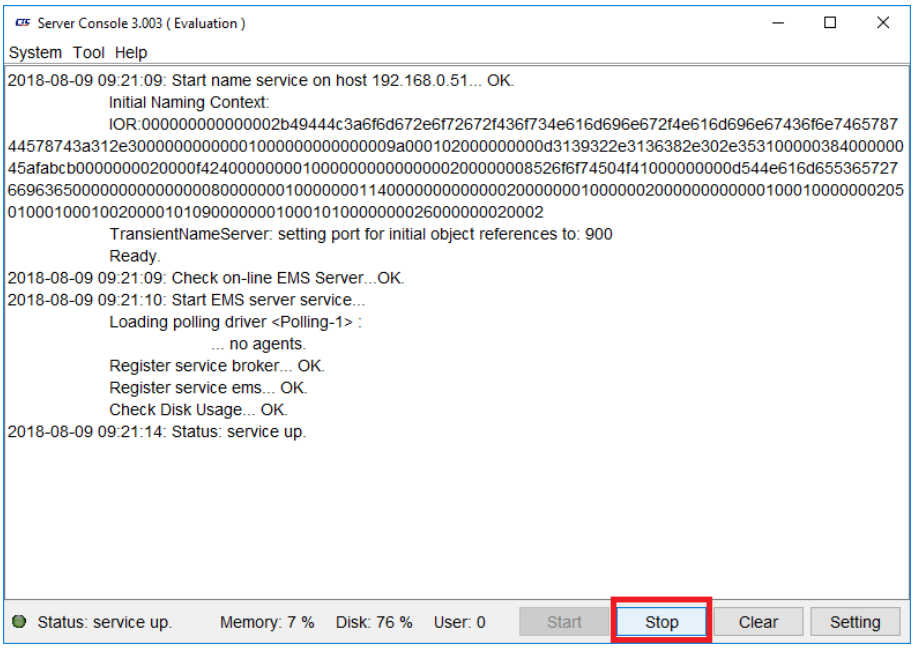


Figure 3-38 Stopping EMS Server

1. From Server Console, click the 'Stop' button.

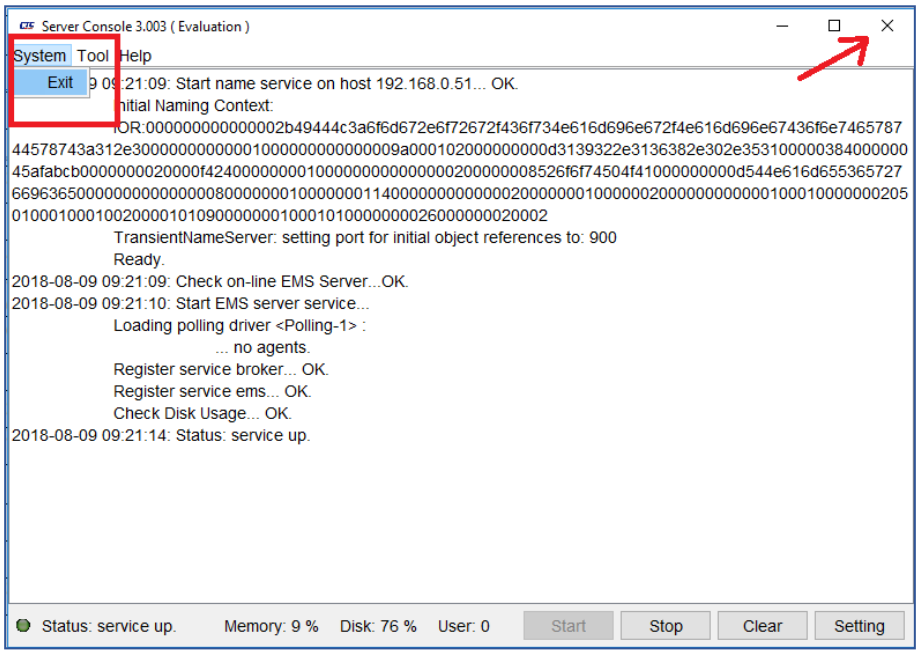


Figure 3-39 Close the window by clicking the 'X' in the upper right corner

Alternately, from the Server Console, click 'System' menu and select 'Exit'.

WARNING: Clicking the "X" will close the Console window and effectively kill the CORBA and Broker server processes. The CORBA Name Server and Broker Server both run in the "Server Console" window. During normal server operations, this window may be minimized to the Windows Task bar, but not closed. DO NOT CLOSE THIS WINDOW or the server will be terminated. The "Server Console" window must remain open or EMS Server is terminated.

Chapter 4 Admin Console Operation

4.1 Introduction

This chapter will explain in detail all the configuration parameters for the EMS Admin Server. Starting with EMS version 2.45, the Setup Tool will no longer automatically start the login for the Admin Console. **If you are coming here just to do configuration and the Admin Console is not running, you need to start it with the following procedure:**

1. Make sure the SQL Database is running.
2. On the desktop, double-click the "EMS Server" icon to startup the EMS Server Console (if not already running).
3. Click the "Setting" button to start the "Admin Console".

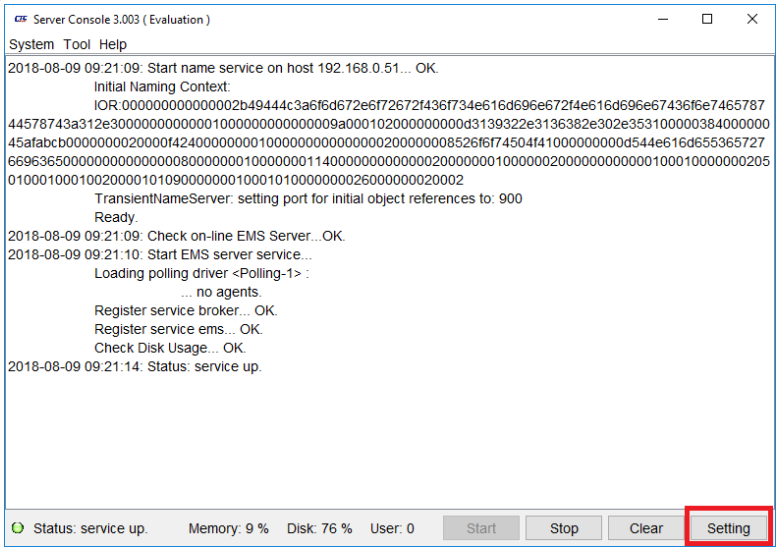
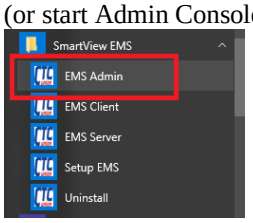


Figure 4-1 EMS Server Console

(or start Admin Console via Window's All Apps Menu)



Use the "admin" administrator username and default password "0000" to login.

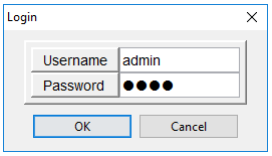


Figure 4-2 Admin Login

Admin Console Window (note: runs only on EMS Server)

Broker: Defines server broker's names, IP addresses, polling drivers, active and inactive polling agent lists.
Agent: Defines agent (device) names, IP addresses, and the SNMP parameters (community strings, MIB, etc.).
User: Defines client login username, password and role authority.
Role: Defines both client and device roles to aid in providing distributed management.
ACL: Access Control List to securely define user login from specific IP and/or MAC address.
User Log: Records client log-in and log-out data time records.
ActionLog: Records every administrative or operational action conducted by any user.
Messengers: When trap alarms occur, they can be sent to those E-mail and SMS account lists according to the filter conditions.
Event: Administrator may configure very basic 'north bound' functions for forwarding traps from SmartView EMS to other network management software and for sending log events to a network configured syslog server.
Storage: All functions related to database management are located under this tab
Discovery: This tool helps to find SNMP agents automatically on your network and quickly add to the Agent list.

4.2. Broker

The Broker setting sets the IP address for EMS to attach to the Database Server. For a default installation, the Database Server resides on the same physical hardware as the EMS Server and therefore uses the localhost address.

4.2.1 Edit Broker

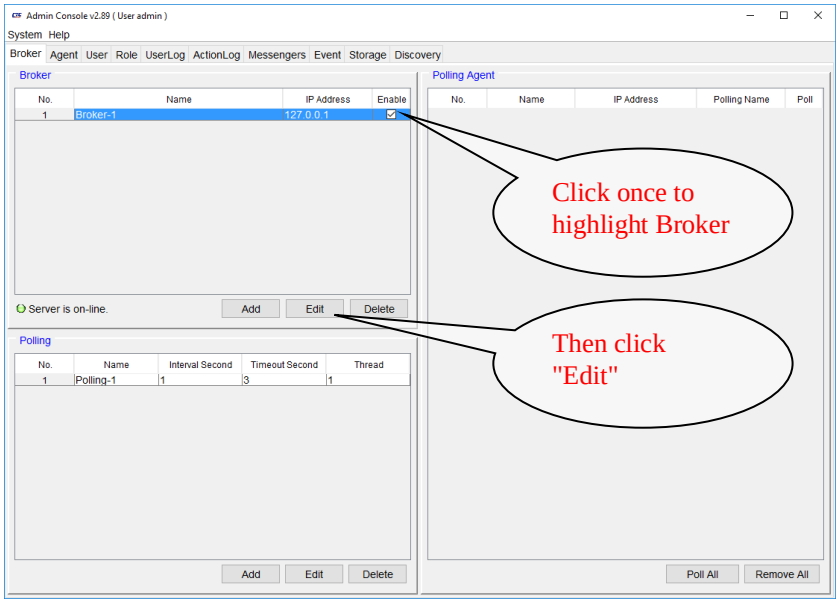


Figure 4-3 The Broker Administrator default startup screen

Select the Broker from the "Broker Pane" and then click the "Edit" button. A popup window will appear to modify the broker contents. A default broker already exists and points to the localhost IP 127.0.0.1. Additional Brokers may be created. **Note: Only one Broker may be active at any one time**.

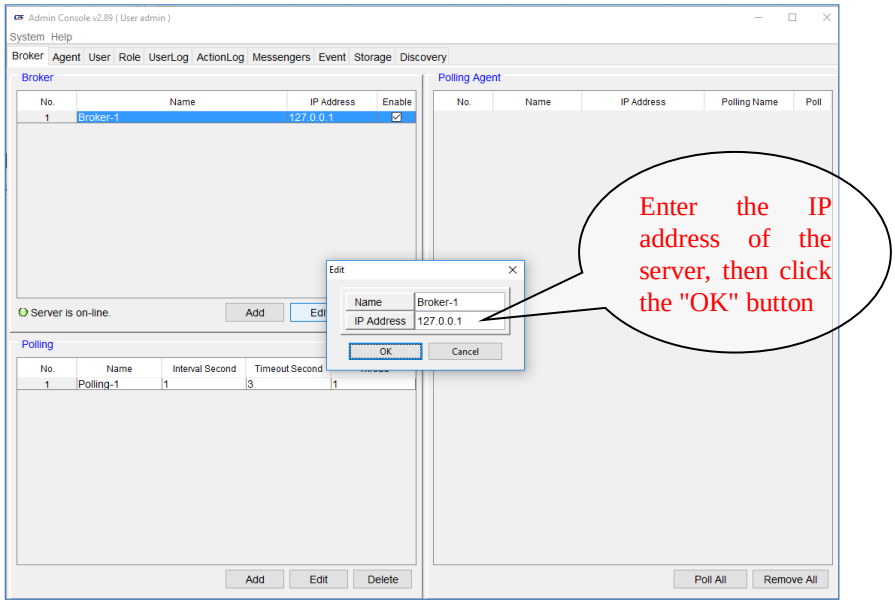


Figure 4-4 Edit Broker Popup

Normally, this item requires no modification. However, in the event the server's IP address needs to be changed, this is one of the items that must be manually configured. Starting with EMS version 2.45, when the default is selected during installation, the server's IP address will be the IPv4 local host address, 127.0.0.1. The best performance between EMS server and Database Server (if installed on the same physical hardware) is realized by using the localhost IP address.

4.2.2 Edit Polling Driver

Use this procedure to modify the Polling Driver for the specific Broker.

On the Brokers tab, choose Polling record and press the "Edit" button. Multiple Polling drivers may be created and specific agents assigned to a specific driver. They all must act under the same Broker however.

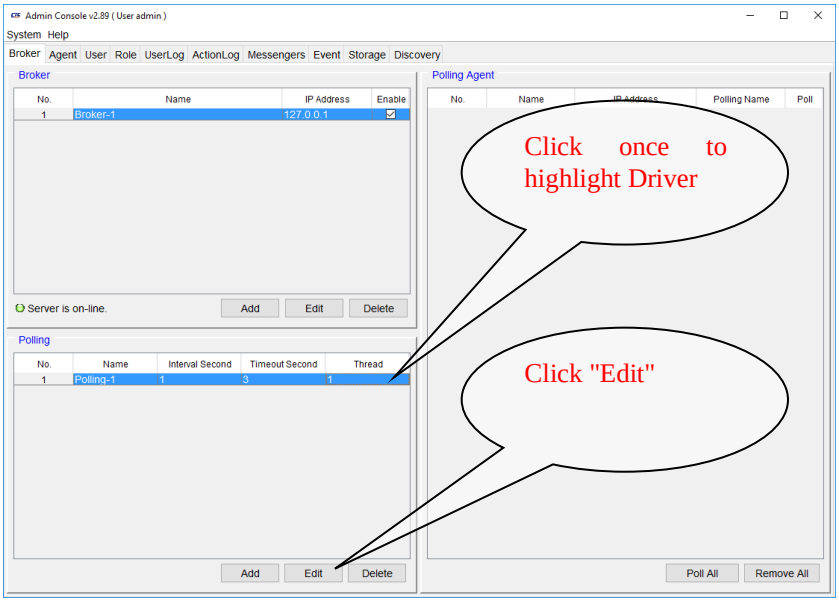


Figure 4-5 Modify Driver

Explanation of parameters:

1. The "Name" is the common name given to this polling setup. Default is "Polling-1".
2. The 'Interval Second' is the delay period between when all assigned network elements have been polled and when the polling starts again. All network elements are polled, one by one. The equivalent action would be if you accessed each network element and did an SNMP walk of the entire MIB. The EMS will complete the poll of one network element, before moving on to the next one, then on and on until all elements have been polled. Then it waits the 'Interval Second' (delay) before starting to poll all over again. The default is 1 second (1000ms). Increasing this value will increase the 'wait' after all elements have been polled. It should not be less than 1000 milliseconds, otherwise the server will always be busy polling agent status.
3. The "Timeout Second" is a heartbeat for all agents registered in this driver. If an agent does not respond within the Timeout period (default 3 seconds), it will be shown as "disconnected". If polling is done over long distance or over a WAN connection, the timeout value may need to be increased or elements may be shown as disconnected when in fact they are not.
4. Starting with EMS version 2.45, the SNMP poller has been updated to allow configuring multiple polling "threads". The idea of using multiple threads is an advantage when polling large numbers of ND (network devices). The polling cycle for all ND can be reduced significantly. Please note that multiple threads will require both more network bandwidth, more processing power and more memory from the server. This should not be a problem for servers with 1G network connections, multiple CPU cores and expanded memory (more than 8GB).

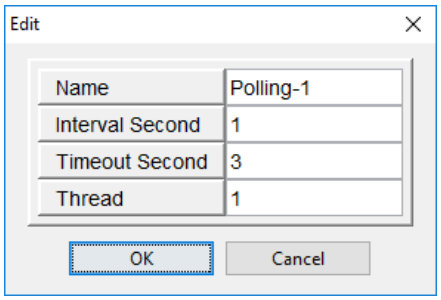


Figure 4-6 Edit Polling Pop-up

4.2.3 Add Polling Driver

Use this procedure to add a Polling Driver for the specific Broker. This may be done when different groups of equipment may be WAN connected (requiring longer timeout settings) or if more or less threads are required to poll groups of equipment. Upon installation, a default polling driver has already been installed and configured. It is not uncommon to have ten or more pollers in a large network with many devices spread over a large geographic area.

On the Brokers tab, choose the Polling record, and press the "Add" button.

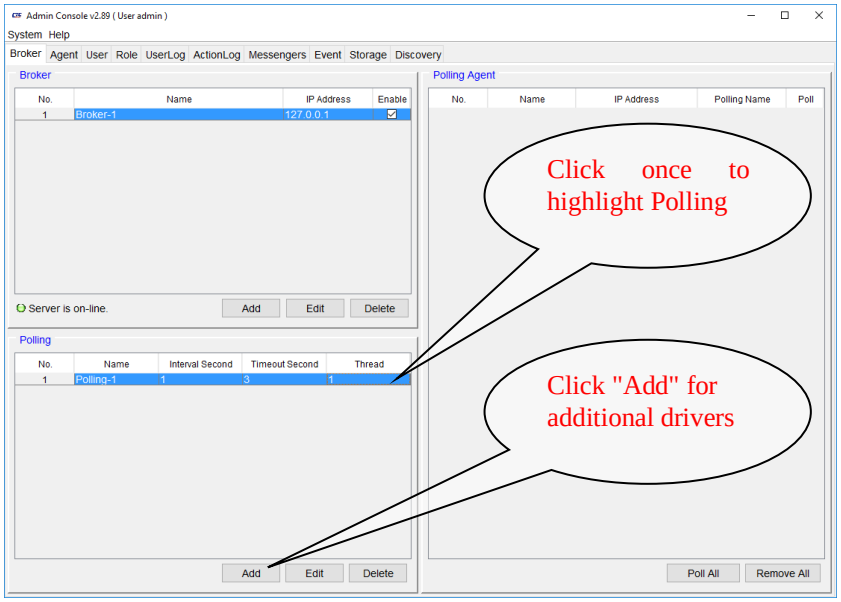


Figure 4-7 Add Polling Driver

Use the dialogue box to enter the timeout parameters for the new driver. The 'Interval Second' is the delay period between when all network elements have been polled and when the polling starts again. All network elements are polled, one by one. The equivalent action would be if you accessed each network element and did an SNMP walk of the entire MIB. The EMS will complete the poll of one network element, before moving on to the next one, then on and on until all elements have been polled. Then it waits the 'Interval Second' (delay) before starting to poll all over again. It should not be less 1000 milliseconds, otherwise the server will be very busy polling agent status and network traffic will be increased unnecessarily.

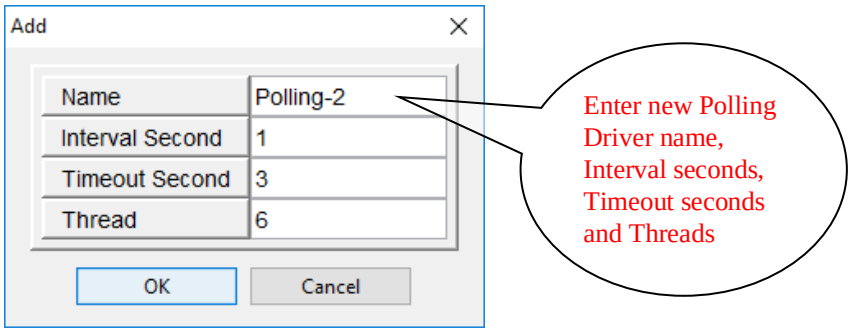


Figure 4-8 Add Polling Pop-up

In the above settings, the server will wait 1 seconds after completing a polling cycle. The server will wait 3 seconds before disconnecting a ND which times out. The poller will use 6 concurrent threads to do ND polling.

4.3 User Administrator

Users are the clients that run Element Management Consoles (EMC). The default user "admin" is the super user with full power. Additional users should be created and given different authorities based on the management needs.

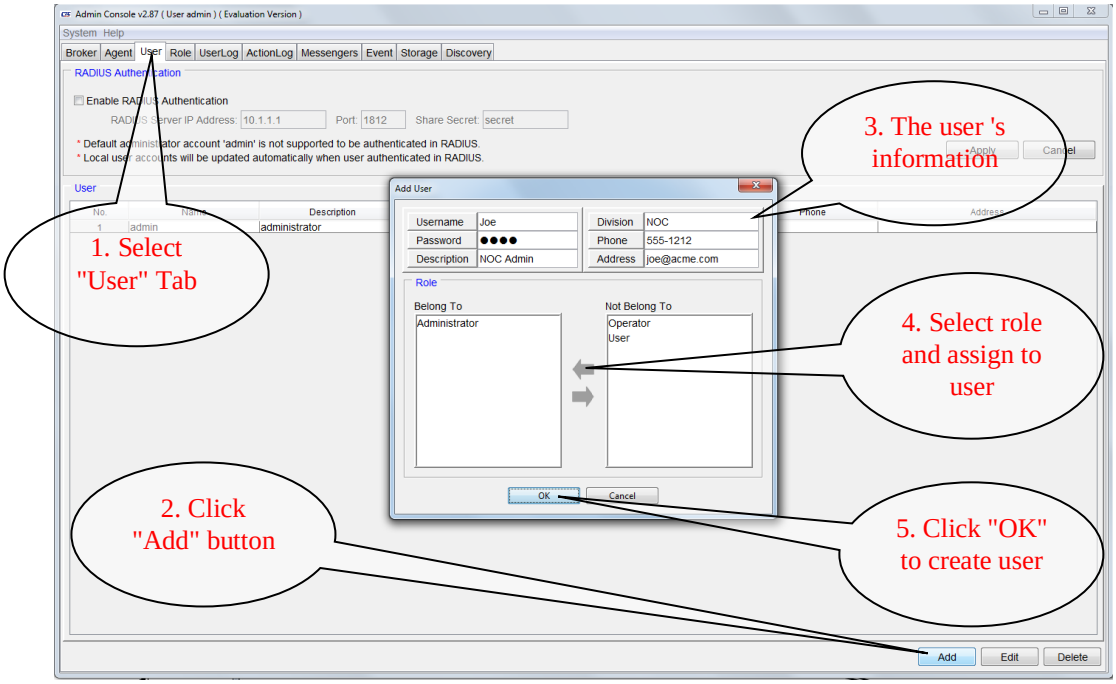


Figure 4-9 Adding client users

On the User tab, the default user "admin" and all EMC Workstation Clients are shown in the User table. Note that these users are not SQL Server clients. This EMC Workstation User registry is stored in the SQL database and provides login security for the user terminals. Alternately, RADIUS server can be configured to provide authentication login, storing user credentials in the AAA server. The Broker administrator can add necessary user logins with specific privileges, from Administrator to Operator and lastly to normal user. The user ID "admin" cannot be deleted, and it has the highest priority. An administrator being authenticated via RADIUS cannot use the "admin" username. The "admin" account is build-in for EMC Admin Console administrator login only. You may add additional users with other login names and passwords. Note: Only users with administrator Role can add users to the system.

The administrator can select "Edit" to edit existing users or "Add" to setup new user accounts. To delete a user account, select it with one mouse click, then click the "Delete" button. A confirmation dialogue box will pop up.

Once a user is deleted, it cannot be undone.

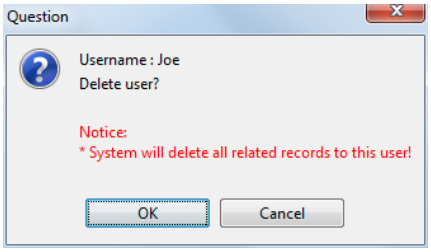


Figure 4-10 Delete User Prompt

Roles will be explained in more detail in the next section. When an admin creates a user, they may be given 'administrator' role, allowing them to create other users and to add devices into the system to manage. When a user is assigned the role of 'operator', they will have read/write access to all devices that have been assigned to them. A user that has the role 'user' will have read only access to the devices to which they have been assigned.

4.3.1 Roles

Starting with EMS version 2.81, the concept of role management was added. Different roles may be created, and those roles may be assigned to users and/or agents (devices). The roles concept, when implemented, enables detailed distributed management where groups or individual users are assigned control over different levels of management and/or over groups of network devices. This is especially important when delegating management in a large deployment of devices.

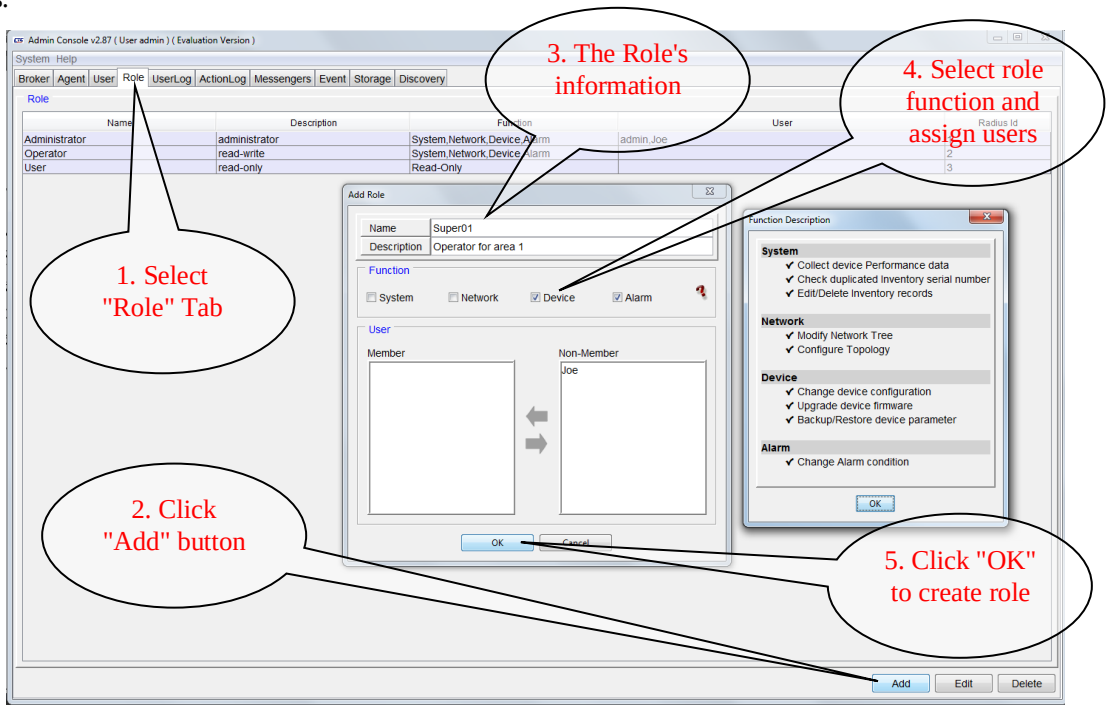


Figure 4-11 Adding roles

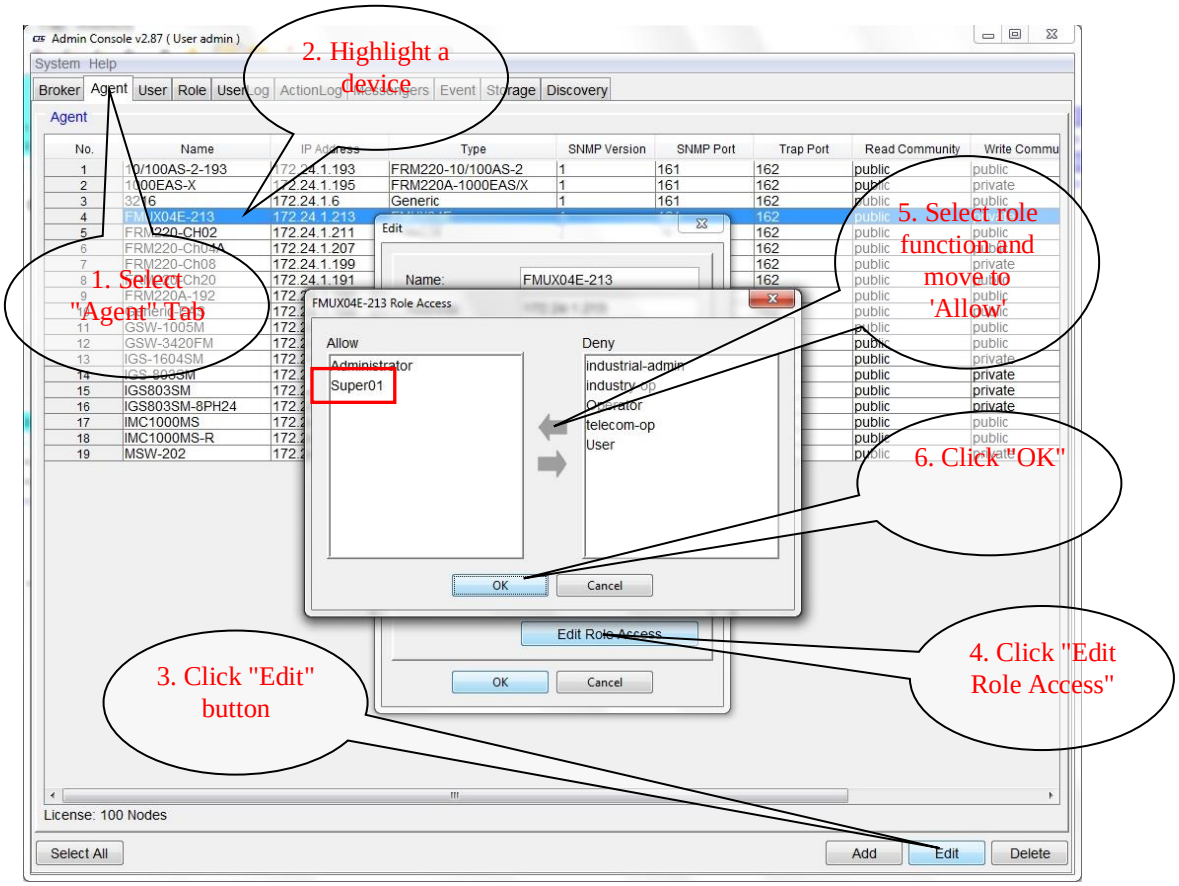


Figure 4-12 Placing devices under Roles

4.3.2 ACL Administration

An access control list (ACL), with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject and an operation. For instance, if a file object has an ACL that contains (Alice: read,write; Bob: read), this would give Alice permission to read and write the file and Bob to only read it.(Wikipedia) ACL in EMS server however controls a user's login by locking it to a specific IP address and/or MAC address. Once specified in the ACL list, this user must login in from the specific IP address and/or MAC address or they will not be authenticated. The IP address may be a specific IP or a subnet that allows only local users.

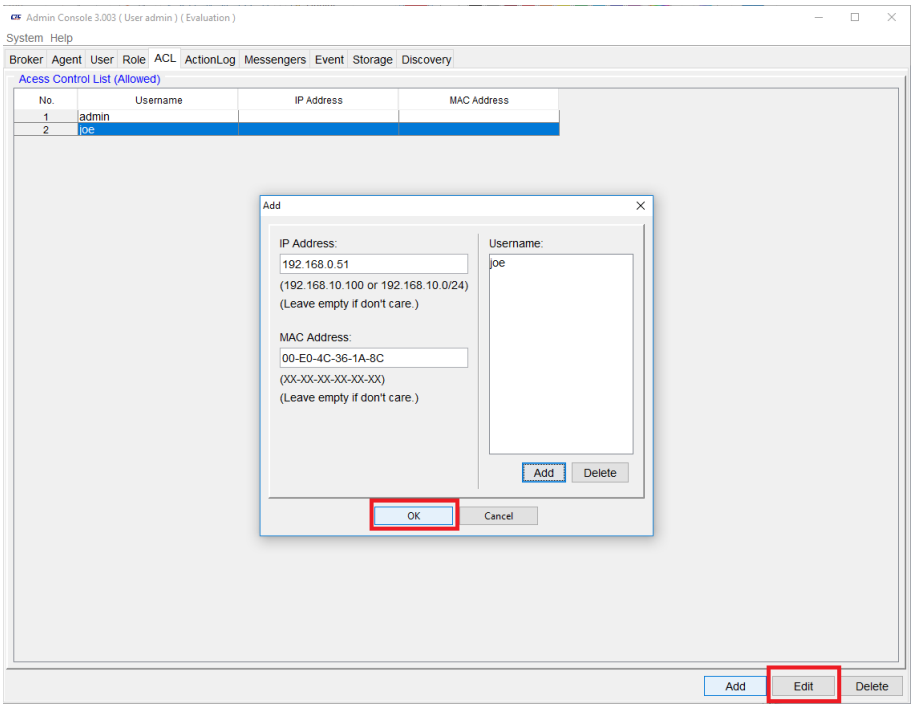


Figure 4-13 Placing users under Access Control List

In the example here, we have locked the user 'joe' to one specific PC with a fixed IP and MAC Address. Joe cannot login from any other physical machine. If someone tries to login with Joe's credentials from another PC, the login will fail.

4.4 Agent (Device) Administration

4.4.1 Using Discovery to find agents

The discovery feature is used to scan a pre-defined range of IP addresses, looking for and finding any SNMP agents that match the defined community string.

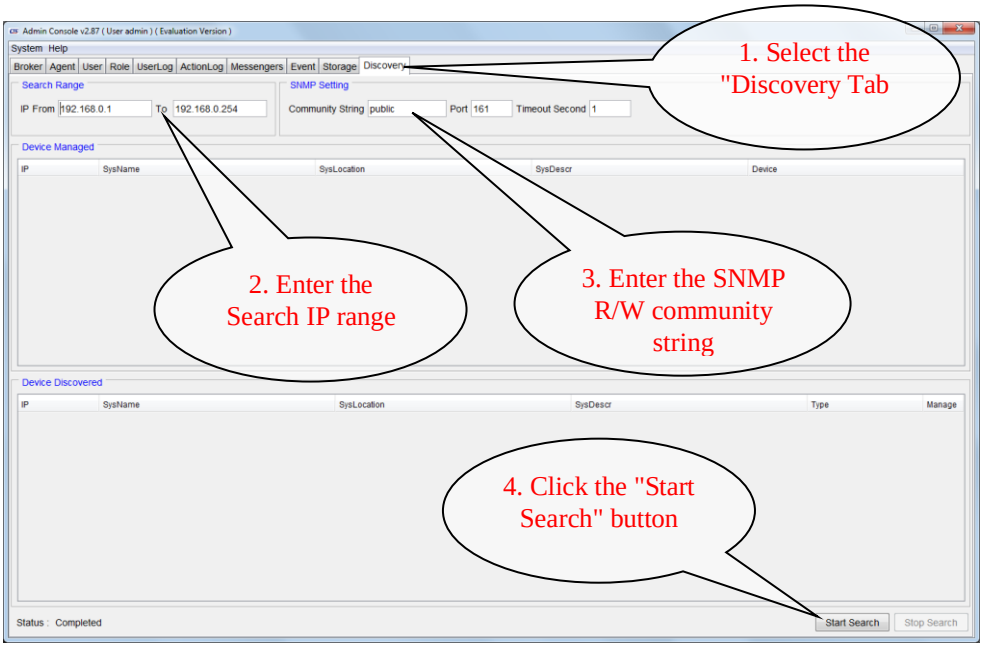


Figure 4-14 Discovery

As agents are discovered during scanning, they will be listed, one-by-one under the "Device Discovered" table. Any agents found that are already registered would display in the "Device Managed" table. The agents "SysName", "Location" and "SysDescr" are all taken from the standard MIB-2 system parameters (OID contents).

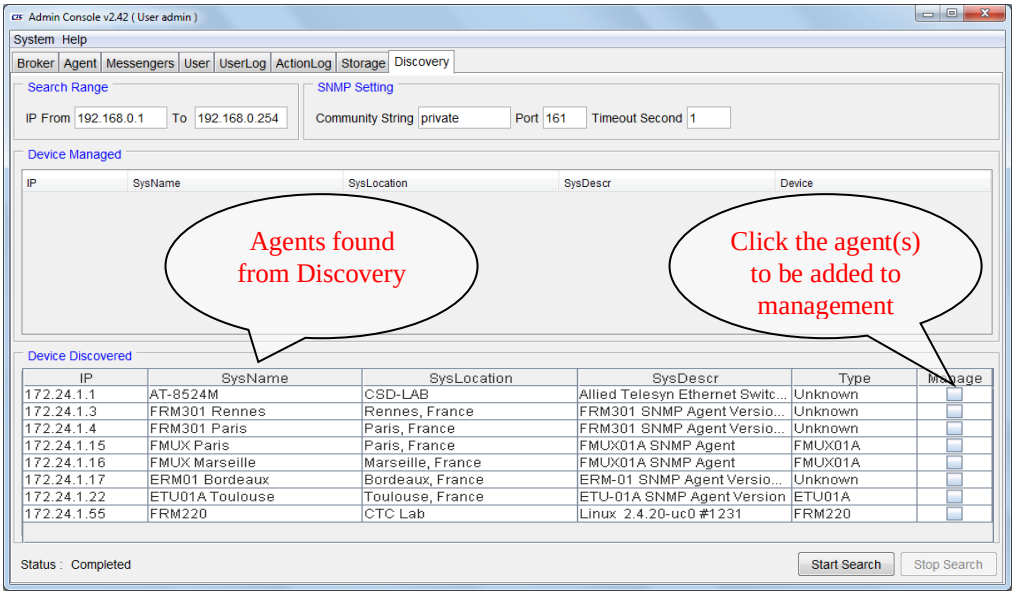


Figure 4-15 Discovery Search Results

Once discovered, click any of the "Manage" buttons, one-by-one, to add these discovered devices to the Managed Agents window.

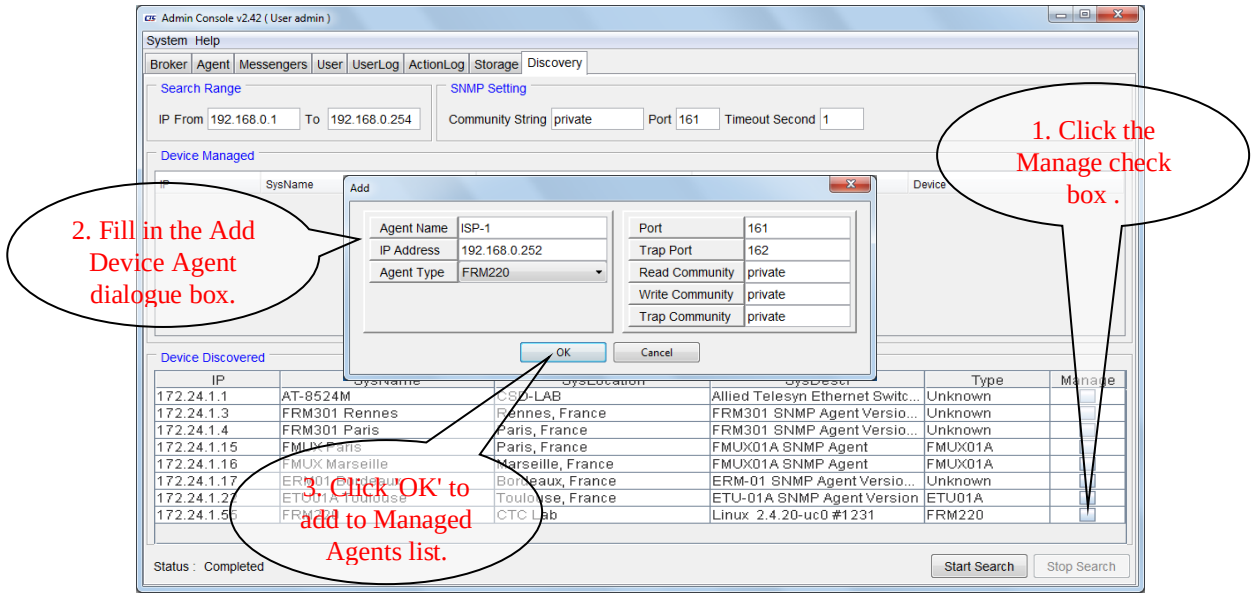


Figure 4-16 Discovery Add Agent

1. Agent name: This should be a unique name that makes the device easy to identify. Do not use Chinese or any special characters in this name. It also makes sense to have the agent name and the SysName be the same as traps and alarms are shown with the SysName.
2. IP address: This address is set from the auto discovery.
3. Agent Type: This is a pull-down list showing the agent types that the EMS supports. Select the right type for the discovered equipment. This agent type should be correctly identified from the discovery, but if it is not, correct it.
4. Ports: These are the default SNMP ports and should not need to be changed.
5. Community: These text strings act as passwords for the SNMP protocol. The Write string allows access to the agent to control the network device.

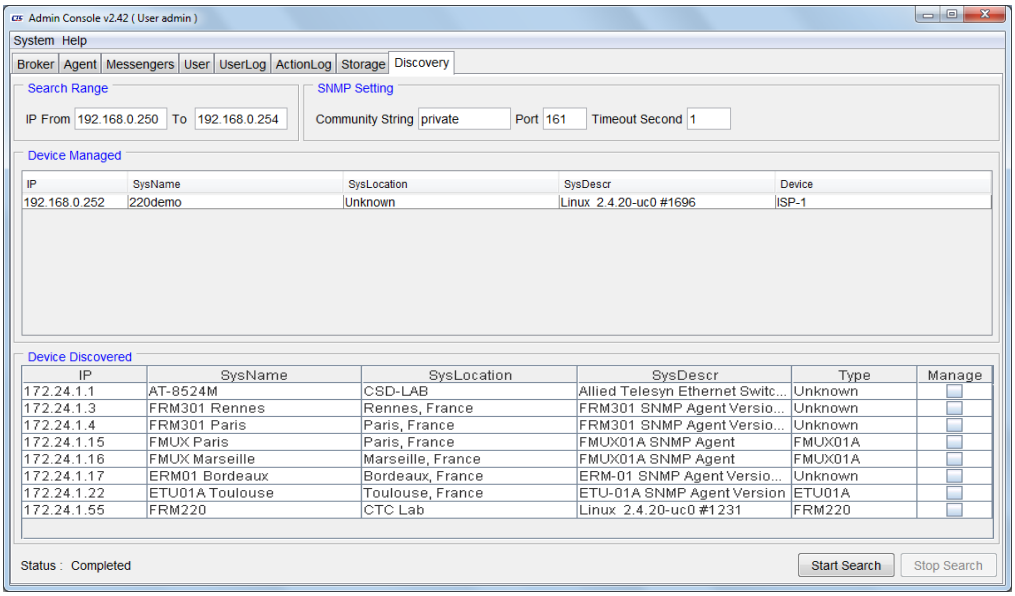


Figure 4-17 Add Agent Results

4.4.2 Manually Setup Agents

The following explains the method for adding agents manually. Click the 'Agent' tab and click the 'Add' button. Fill in the dialogue box and click "OK".

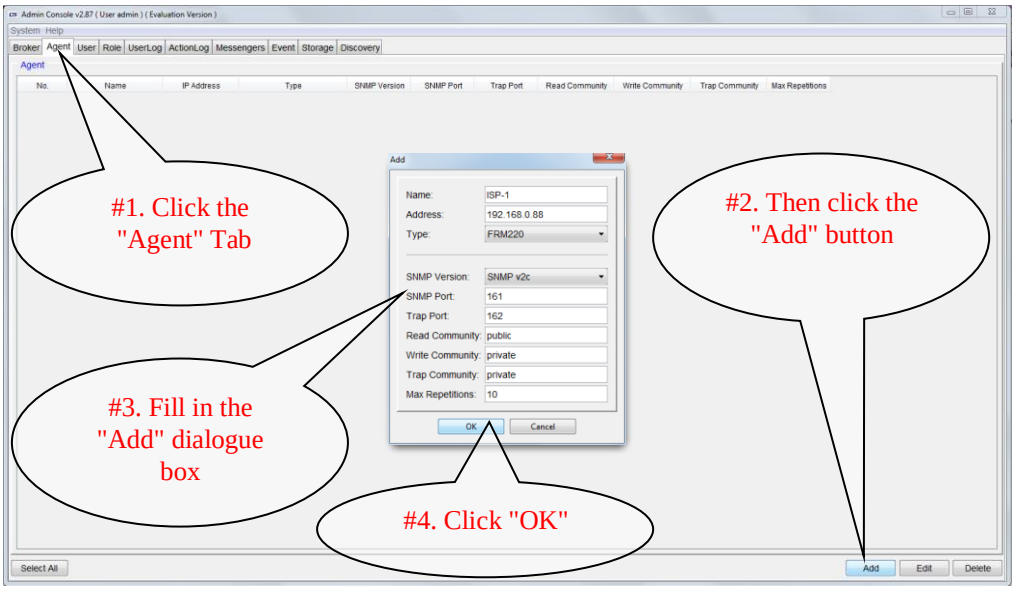


Figure 4-18 Add Agent Results

Device Agents are the network devices which will be managed by the EMS. Give the agent a unique name, enter its proper IP address, select the device type from the pull-down menu (in this example FRM220) and make sure the appropriate community strings are entered to manage the agent (depends on the configuration done in the agent itself). Then click "OK".

4.4.3 Adding Agents to Polling

This procedure is used to add agents to the polling system. After this step the broker server will automatically restart the service and start polling the device.

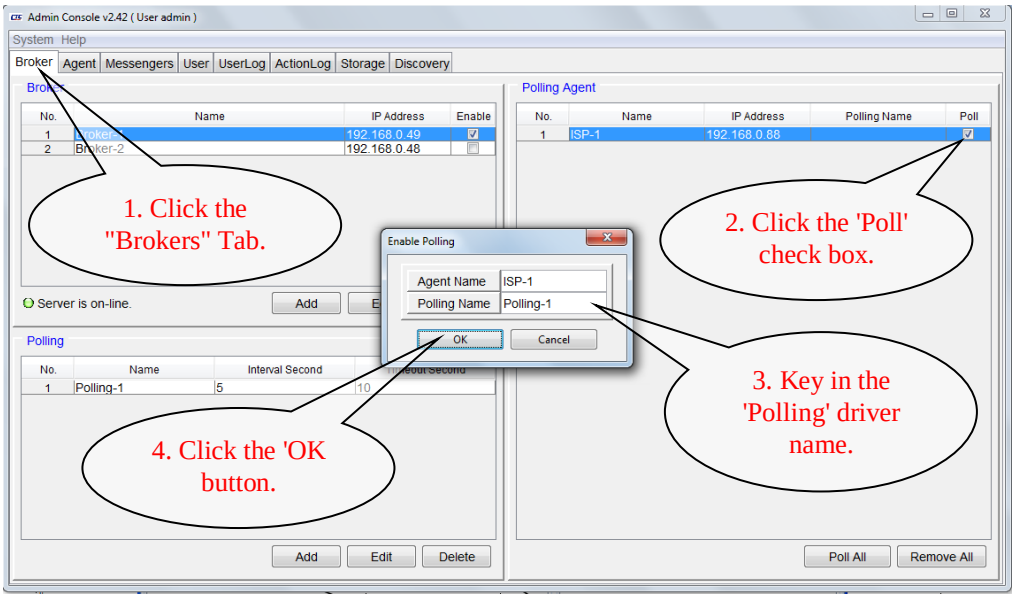


Figure 4-19 Enable agent polling

The following procedure will add all agents to the polling list.

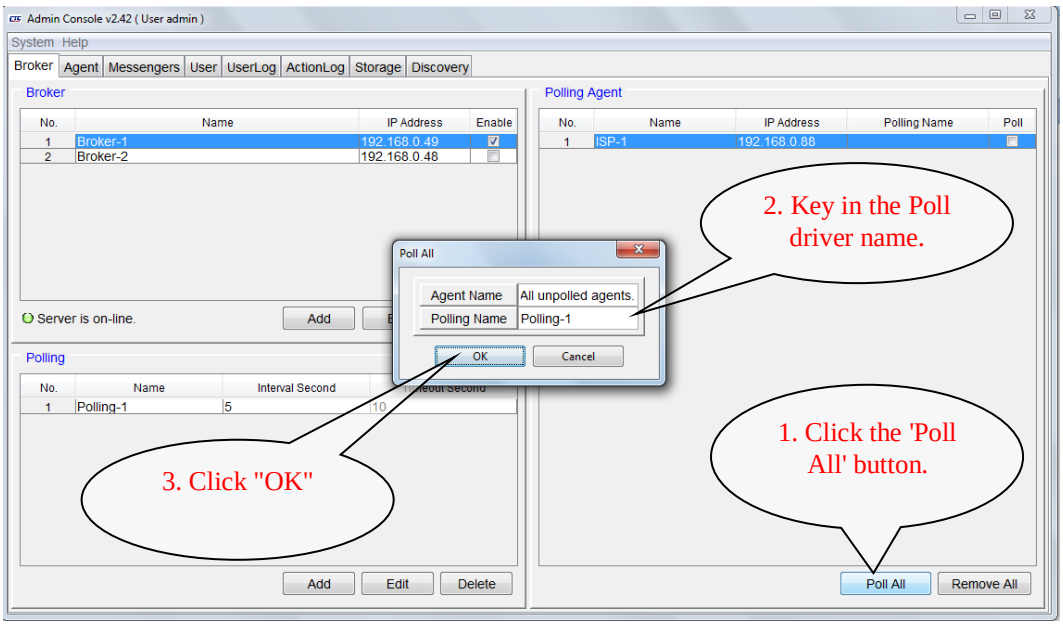


Figure 4-20 Add All Agents for Polling

Note: After adding or removing polling units, the broker server will automatically be restarted.

4.4.4 Removing Agents from Polling

To remove individual agents from polling, simply un-check the 'Poll' check box.
To remove all agents from polling, click the 'Remove All' button.

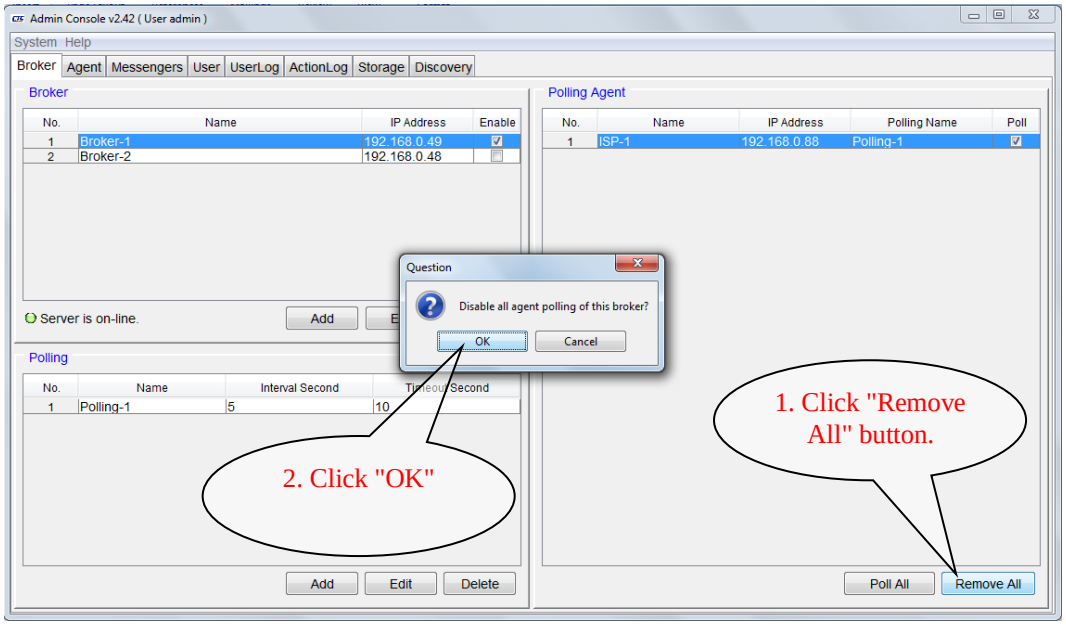


Figure 4-21 Remove All Polled Agents

Note: After adding or removing polling units, the broker server will automatically restart.
Note: When in 'Evaluation' mode, the maximum polled elements are limited to 15 devices.

4.4.5 Manually Restarting EMS Server

In the Server Console, click the 'Stop' button. The server is stopped.

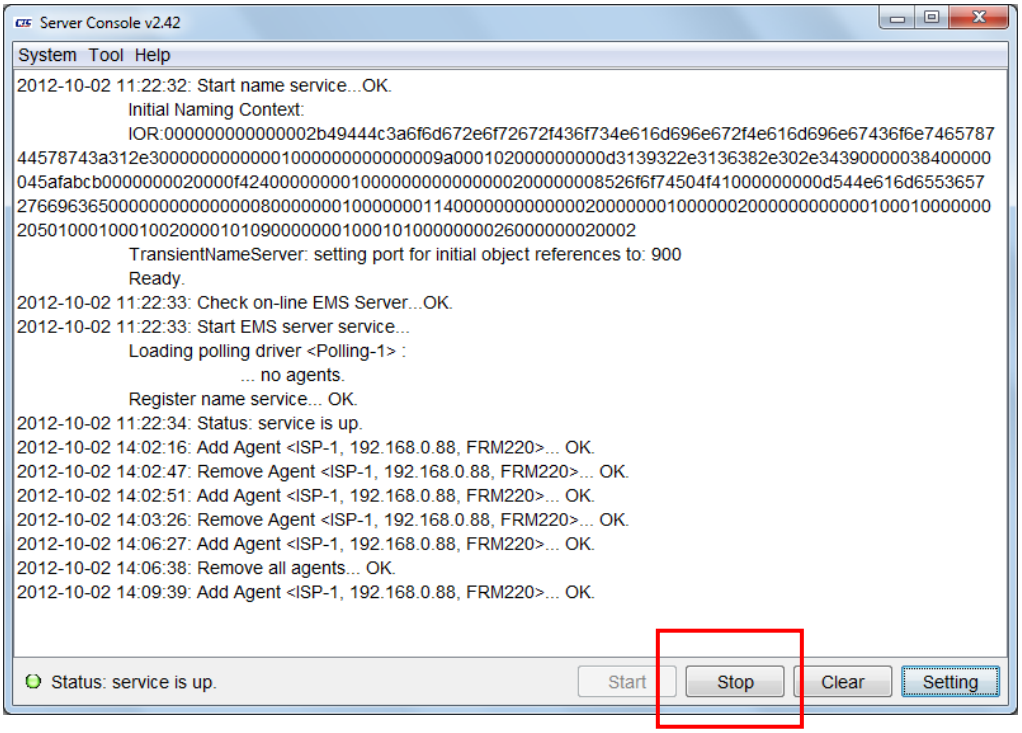


Figure 4-22 Stopping the EMS Server

In the Server Console, click the 'Start' button. The server is restarted.

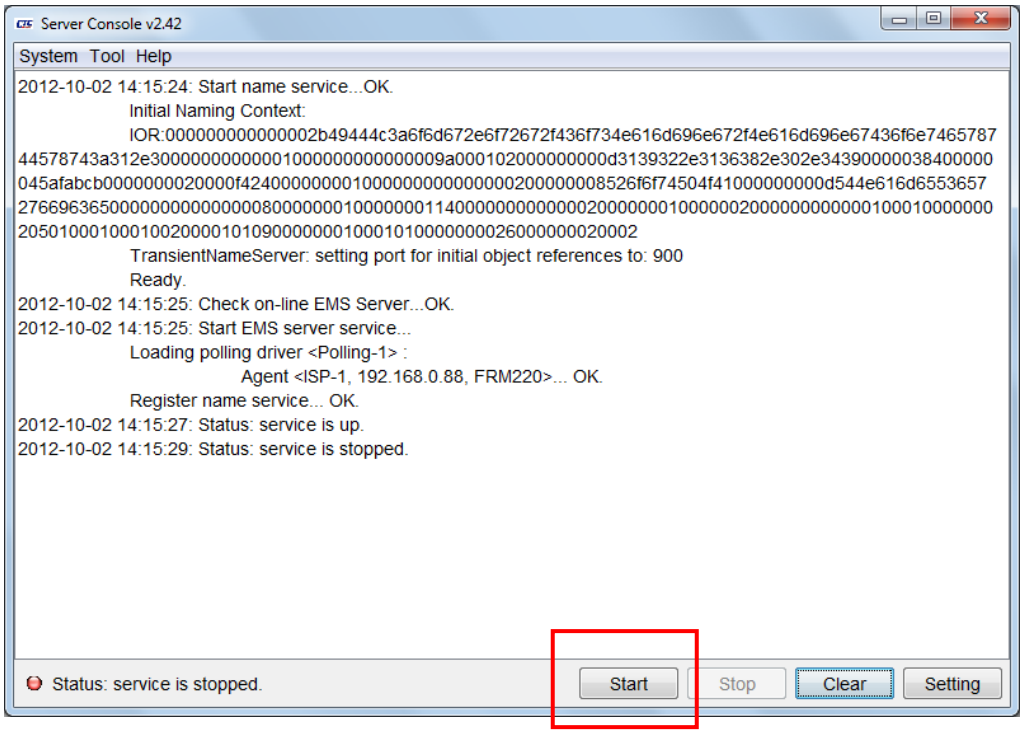


Figure 4-23 Restarting the EMS Server

4.5 E-Mail and SMS Filter Administrator

This section will describe how to setup the E-mail and SMS functions in the EMS and how to use the messengers to send specific alarms to E-mail and/or SMS messages.

4.5.1. E-Mail Setup

From the Server Administrator select the 'Messengers' tab. With the SMTP tab highlighted, click the 'Add' button

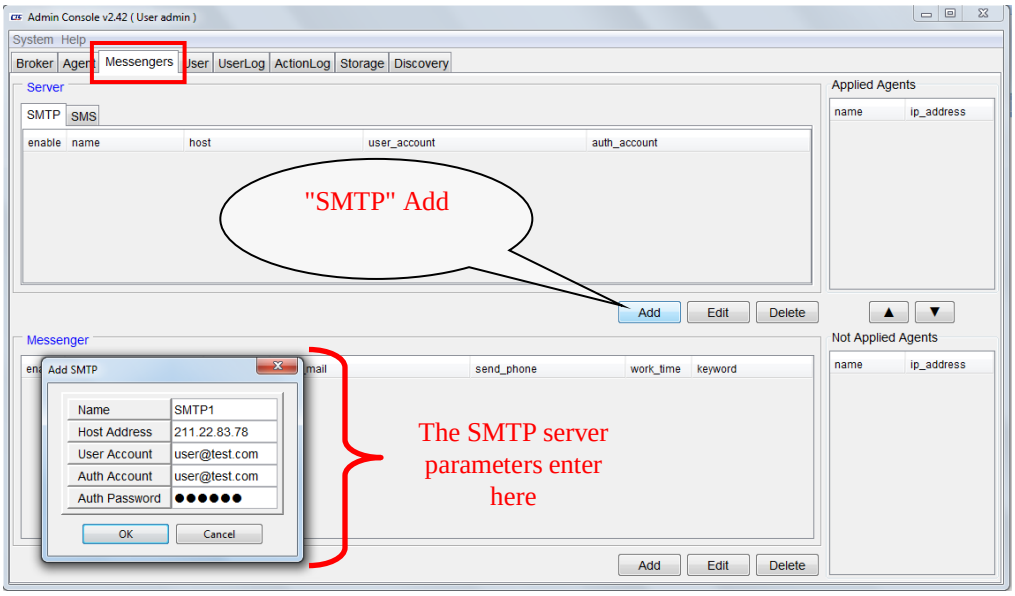


Figure 4-24 The Messengers Tab

Enter parameters in the "Add SMTP" dialogue box.

SMTP Parameters

1. Name: This is an administrator assigned name for this particular SMTP entry in the EMS system.
2. Host Address: The SMTP Server parameter is the real domain name or IP address of the mail relay server that will forward mail from the EMS system.
3. User Account: This is the user account used by the SMTP server to send mail.
4. Auth Account: The SMTP Auth account is typically the same as the Sender account. This is the account required for the SMTP server to accept mail for relay, although it may be without the domain name.
5. Auth Password: The SMTP Auth password is the authentication password that goes with the account name and is required so the SMTP server will relay the mail from the EMS system.

4.5.2. SMS Setup

With the SMS tab highlighted, click the 'Add' button. Enter the SMS account details provided by your service provider. Then click 'OK'.

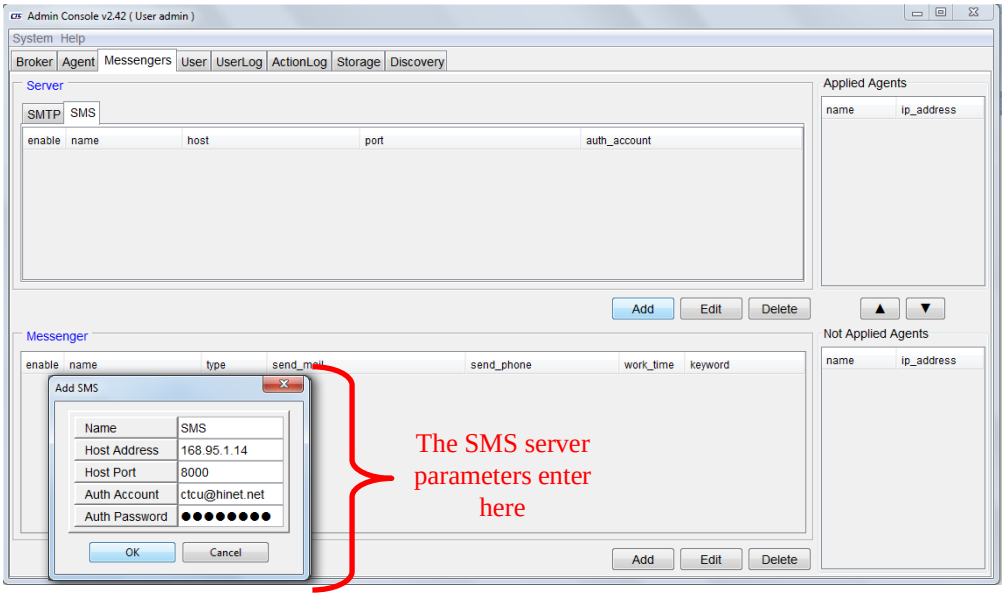


Figure 4-25 Example of SMS configuration

SMS Parameters

1. Name: This is an administrator assigned name for this particular SMS entry in the EMS system.
2. Host Address: The SMS Server parameter is the real domain name or IP address of the SMS messenger server that will forward messages to the mobile phone system for your area.
3. Host Port: The server port is defined by the ISP that provides the SMS messenger service. The default is port 8000.
4. Auth Account: The sender account is required by the SMS server for authentication and billing when sending messages.
5. Auth Password: The sender password is required for authentication of the sender account.

4.5.3. Delivering SMS and SMTP Setup

The 'Messenger' block is used to setup the user who gets messages and for what reasons. In the lower 'Messenger' window, click the 'Add' button. This example sends both an SMS message and Email to the recipient's phone number and email box, if the alarm message keyword is 'LOS' and if the event happens from 6:30PM until 8:30AM.

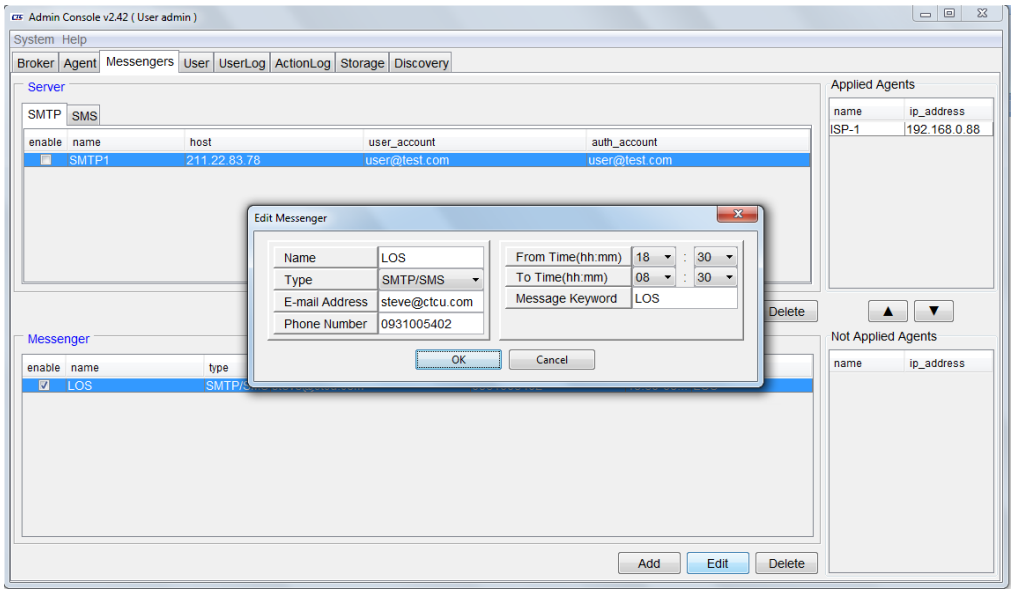


Figure 4-26 Example of SMS add Messenger (alarm filter)

Following the addition of the Messenger entry, select one of the "Not Applied Agents" and click the Up button. This Agent will then be in the "Applied Agent" space as shown below. The filter will send the SMS message if LOS is detected from the applied agent(s) and the other messenger conditions are met.

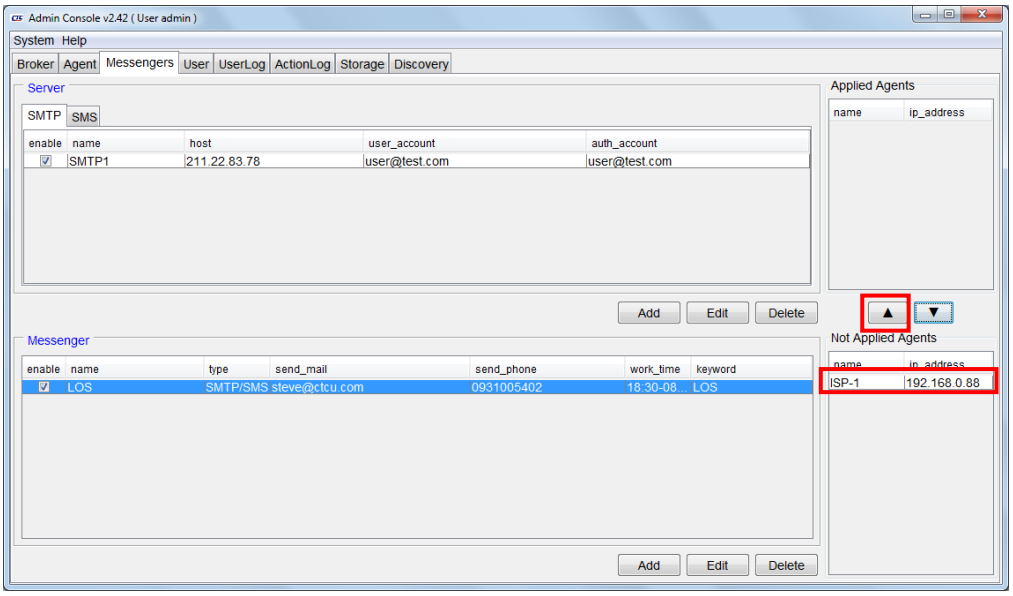


Figure 4-27 SMS Messenger applied to active Agent

4.6 Viewing and Clearing the User Log

By clicking on the "UserLog" tab in the Admin Console, a complete record of client login & logouts is displayed. The records include accurate time stamping as well as recording the client's source IP address. The UserLog is stored in the SQL database. By clicking the "Clear" button, the entries will be permanently deleted from the database. It is also possible to select specific system time frames for deleting the log entries or by specific client name. A confirmation popup prevents against accidental erasure. Only an administrator has authority to delete these records. Search function is supported per user and time.

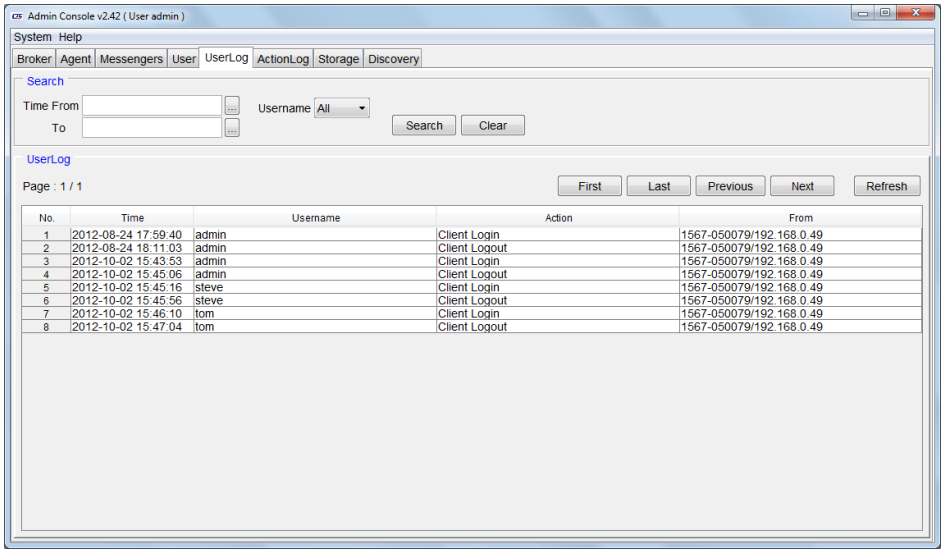


Figure 4-28 Viewing the User Log

4.7 Viewing and Clearing the Action Log

The Action Log can be viewed by clicking on the "ActionLog" tab in the Admin Console. The actions include accurate time stamping of the time any changes were made to any agents (network devices) as well as recording the client's name and action performed. The ActionLog is stored in the SQL database. By clicking the "Clear" button, the entries will be permanently deleted from the database. A confirmation popup prevents against accidental erasure. Only an administrator has authority to delete these records. Search function is supported per user and/or device and time.

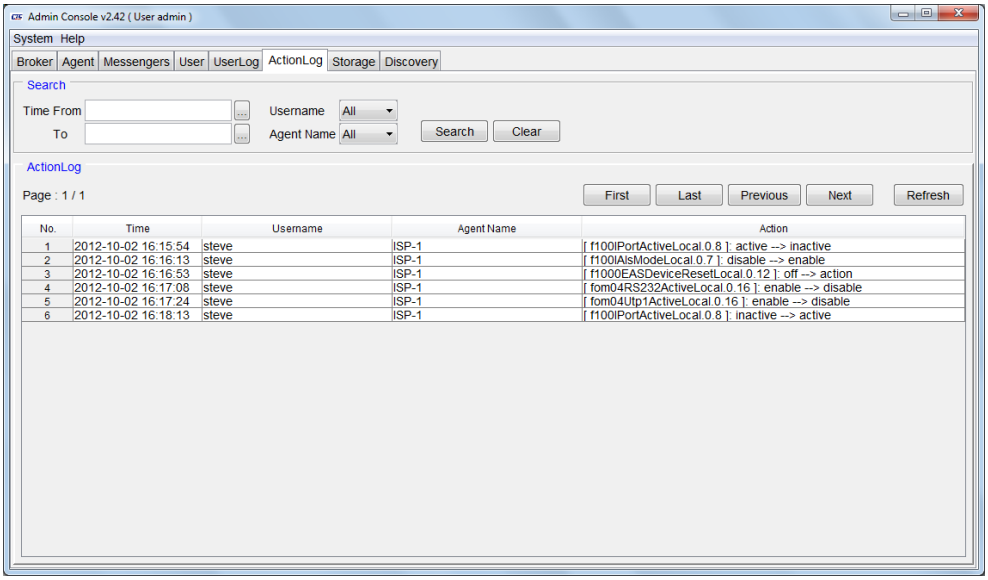


Figure 4-29 Viewing the Action Log

4.8 Event (Forwarding Traps and Syslog)

EMS Server is able to forward traps generated from Agents (devices) to one other NMS (network management system). EMS Server may also send generated SysLog events to a central SysLog Server as a backup and long-term storage archive. Click the 'Event' tab in the Admin Console.

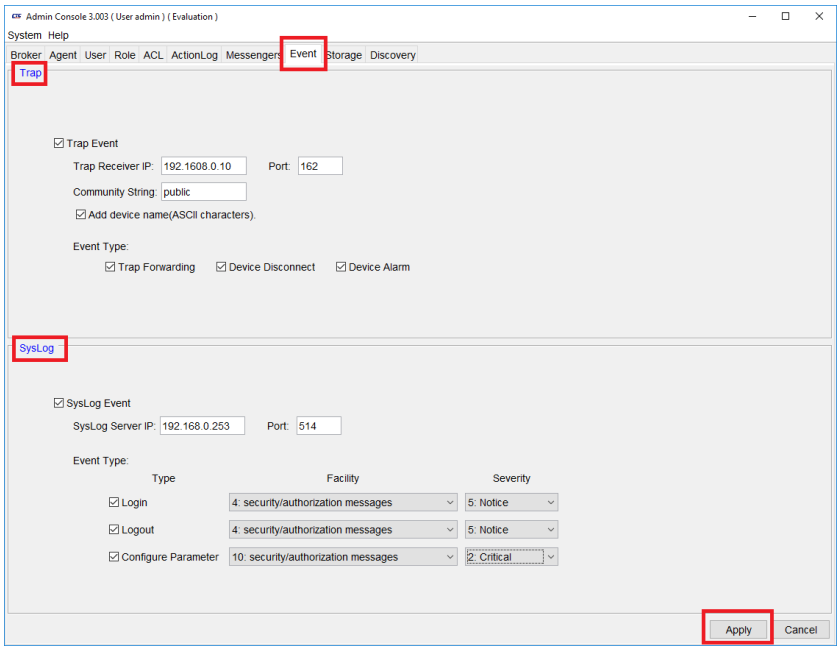


Figure 4-30 Event Forwarding

Make the appropriate changes for Traps or SysLogs and then click 'Apply'.

4.9 Storage (Log and Performance Database Management)

All the alarm and traps will be received by the server and stored into the database in real-time. The Performance data will also be collected by the server during polling and stored into database from network elements that support performance monitoring. The function of the Storage tab is to provide database management of the logs and performance records by selectively erasing records that match a system time window. Excessive traps and performance data can be cleared from the database under the 'Storage' tab of the Admin Console. All logs, traps and performance can be cleared or records from specific time frame may be cleared. A confirmation popup prevents against accidental erasure.

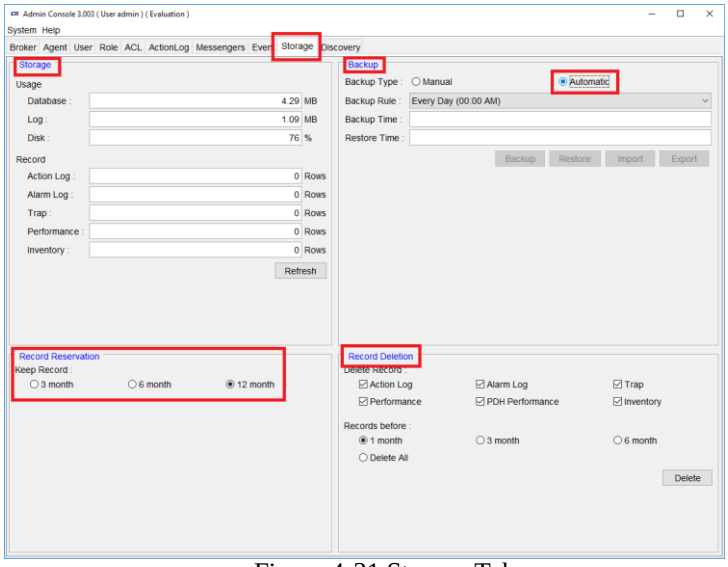


Figure 4-31 Storage Tab

In addition, a backup utility is provided for database maintenance. The database can be backed up or restored and it may also be exported as a file within the server's filesystem, to a network drive or a portable pendrive for safe keeping.

4.9.1. Manual Database Backup

From the Admin Console, on the Storage tab, and within the Backup window, click "Backup" button. A confirmation popup will appear. Confirm by clicking "Yes" and the database will be snap-shot backed up. The backup location will be in the Program Files\Microsoft SQL Server\ MSSQL12.MSSQLSERVER\MSSQL\Backup folder. (This assumes the default installation used the included SQL 2014 Express.)

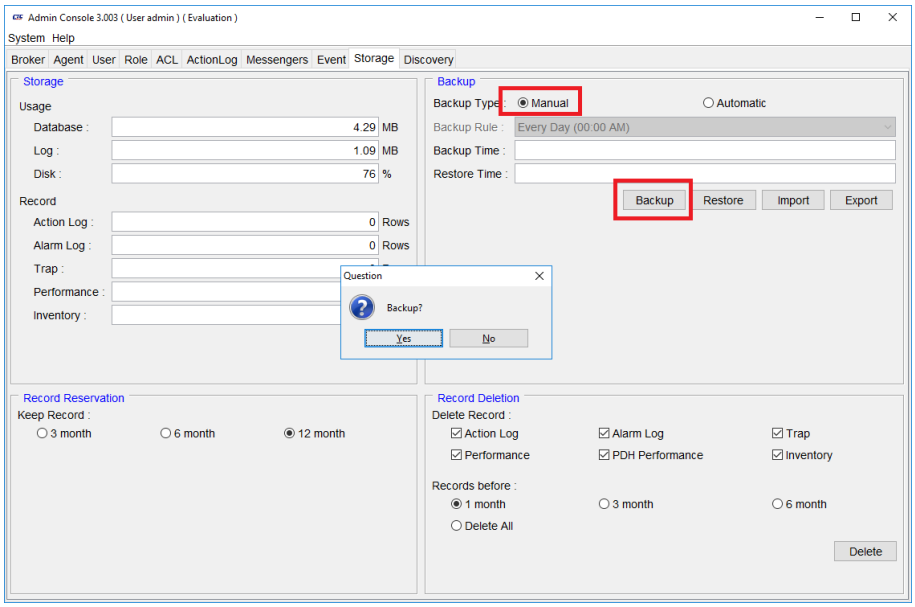


Figure 4-32 Database Backup

Notice: If these buttons appear to be 'greyed out' it is because the user running EMS is not allowed access to the Backup folder. Open the Windows File Explorer and browse to either:
C:\Program Files (x86)\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\Backup or
C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\Backup
Click on 'Continue'. The backup function will then be available via EMS.

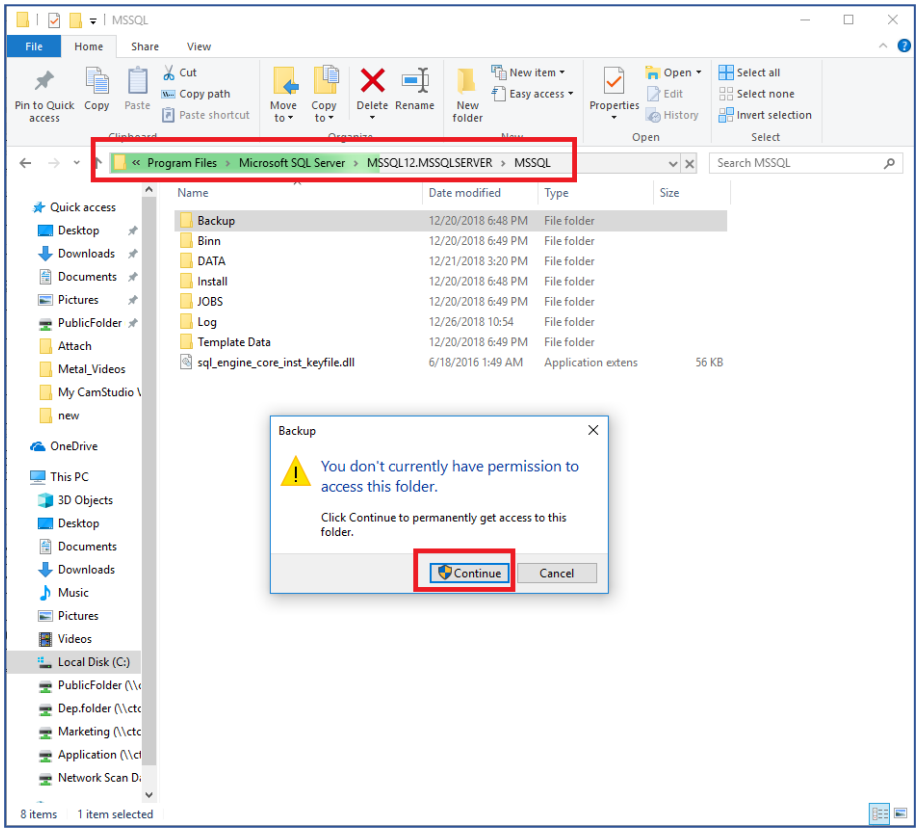


Figure 4-33 Gain access to Backup folder

Chapter 5 Using the Element Management Console

This chapter will go through the SmartView Client operation, the EMC (Element Management Console). After the EMS is configured properly, you may then run the EMC to manage all agent devices supported by CTC Union.

5.1. Run EMC as Local Client

In this example, the Client is run from the EMS server machine itself. Later we will introduce the client installation and remote login procedure for remote clients.

Step 1. Make sure the EMS environment is already configured. This assumes all steps for "Admin Console", as explained in Chapter 4, have been completed and that devices have been added under Agents.
Step 2. Double click the 'EMS Server' icon from the server's desktop to start EMS.
Step 3. Start the EMC by double clicking the 'EMS Client' icon from the Window's desktop.

The Element Management Console will open, the client applet will popup and ask you to enter the EMS server's IP, username and password for authentication. (This user account was set in "Admin Console" client record.) The default super-user is 'admin' and password is '0000'. If the client is running on the EMS Server, the localhost IP address will work.

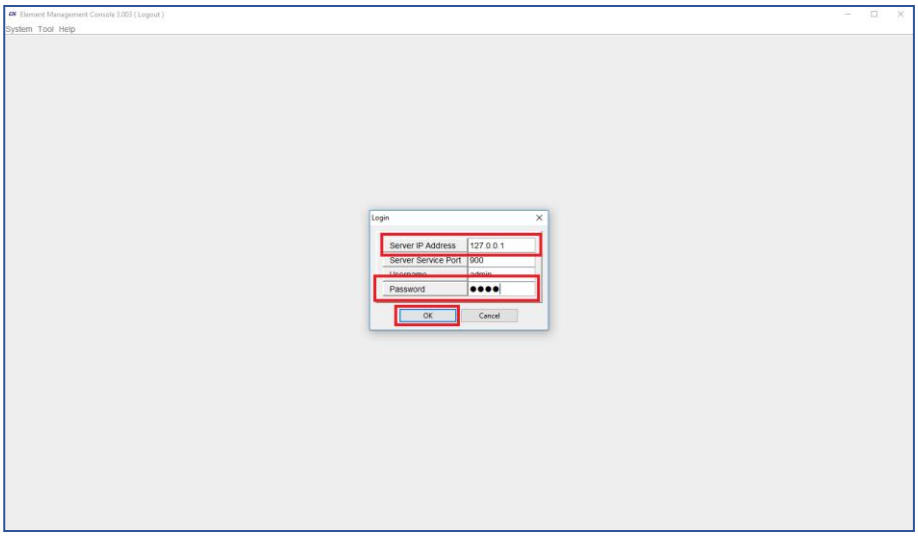


Figure 5-1 EMC Login

Server IP Address: This is the IP address of the EMS Server. If started locally, it is the local server's IP. Clients may also login remotely, in which case the IP address needs to be that of the EMS Server, not the local PC.
Server Service Port: This is the name service port. The default is 900 and should not need to be entered or changed.
Username: Users are created in the User Administrator of Admin Console. The system default super-user is 'admin'.
Password: A password is required for authentication. The default user 'admin' has a password of '0000'. It can be changed and additional users created in the Admin Console. See Chapter 4.

5.2. Setting Up a Remote Client

5.2.1 Introduction

The normal licensed SmartView EMS supports 25 simultaneous client connections. A client could be run directly on the same hardware as the server or clients could be run remotely. This section explains how to setup a remote client.

5.2.2 Copy Files

From the original setup media (DVD or extracted files), browse into the EMS folder, then into the EMS_EN folder. Copy the entire EMS folder to the destination client computer. Place the folder in any convenient location, such as on the Desktop, in My Documents or root directory, for example in C:\EMS or D:\EMS.

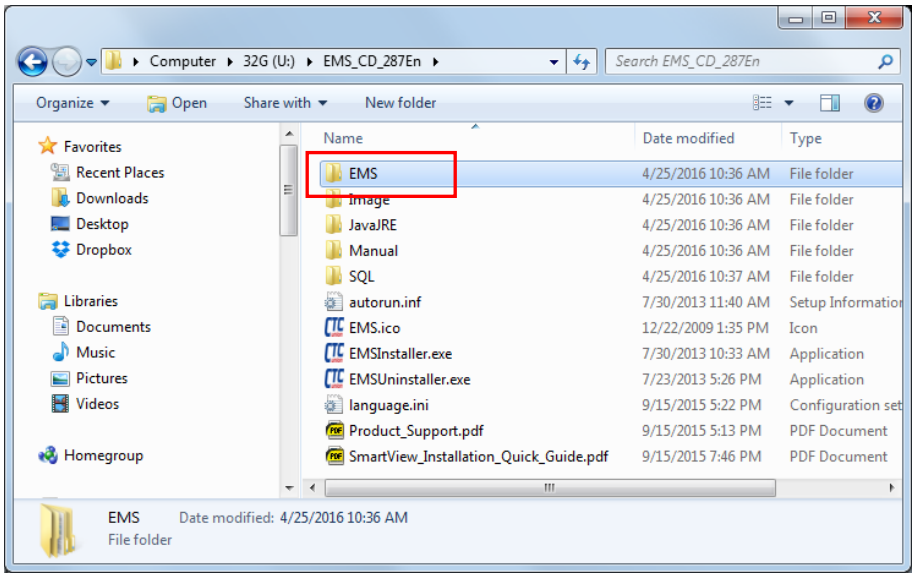


Figure 5-2 EMS Installation Folder

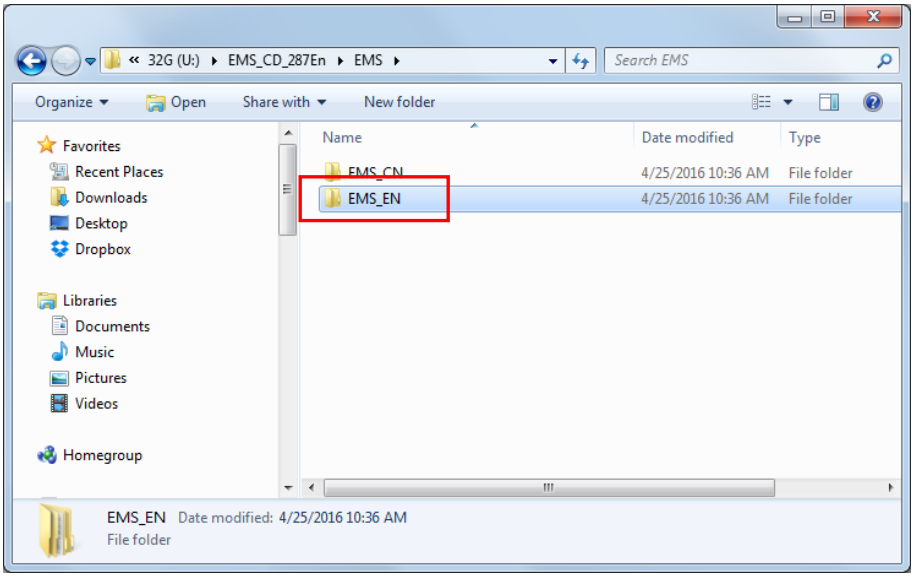


Figure 5-3 EMS_ENGLISH Folder

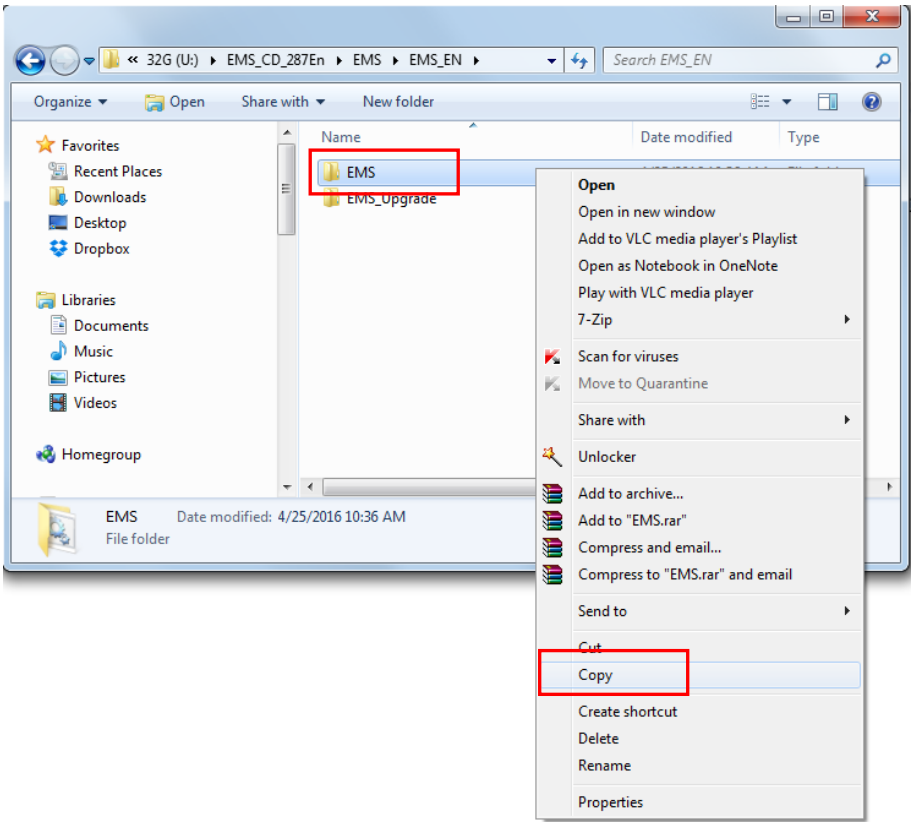


Figure 5-4 Copy EMS Folder

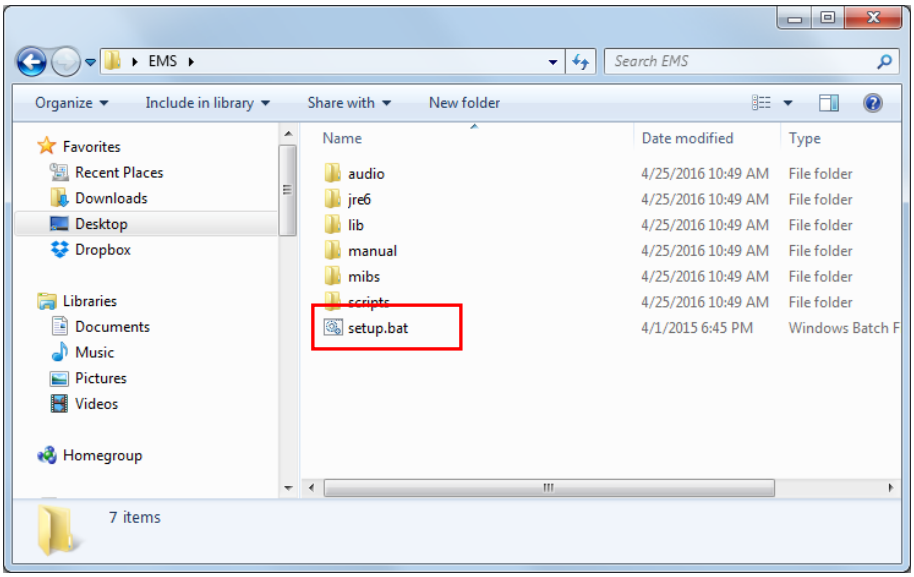


Figure 5-5 Pasted EMS Folder contents (on Desktop in this example)

Right click the "Setup" icon and select "Run as Administrator".

The "Setup Tool" will start. DO NOT select the "Install Server and Tools" radio button. We are installing a remote 'Client', not the 'Server'.

1. Select the "Install/Modify Client Management Tools".
2. Click the Server IP Address 'Remote' radio button.
3. Enter the IP address for the EMS server in the parameter space labeled "Server IP Address" (172.24.1.190 in this example).
4. If this computer has more than one Ethernet interface (such as a laptop with both LAN and WiFi interfaces), select the Client IP Address 'Static' radio button and choose the correct LAN IP address from the pull-down menu (10.8.0.4 VPN connection in the example).
5. If your laptop has 8GB or 16GB of memory, it is OK to increase the client 'Memory Usage' from the default of 512MB to 1024MB.

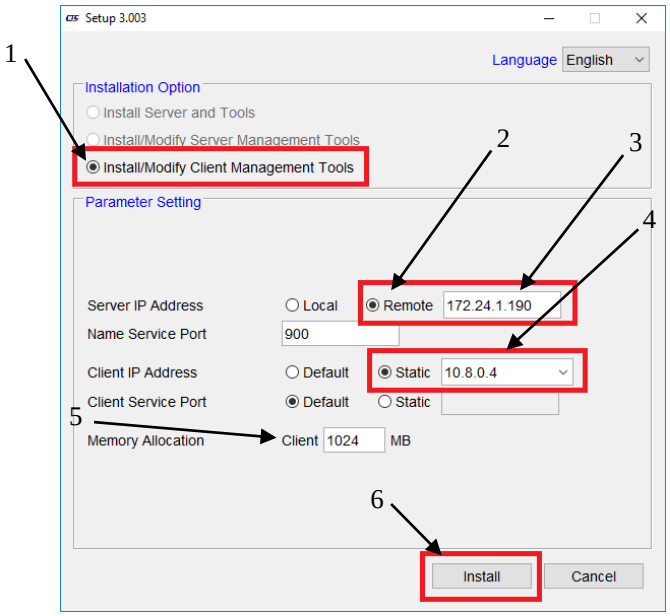


Figure 5-6 Setup Tool

6. Click 'Install' and the "client.bat" file will be created.

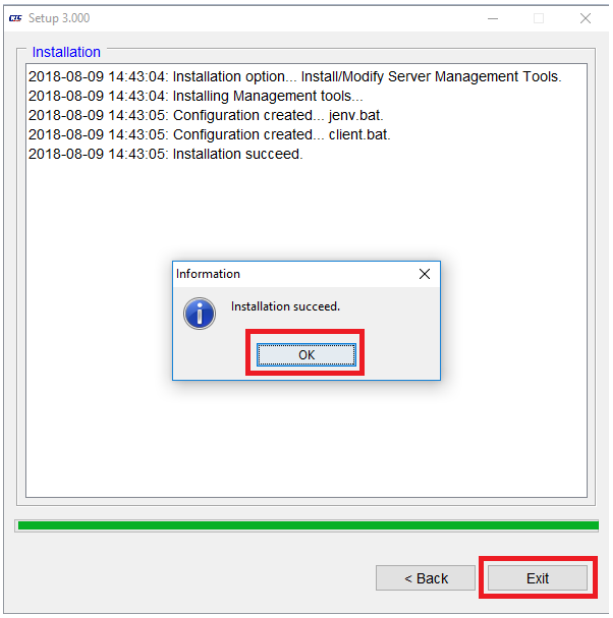


Figure 5-7 EMS Client Installation Complete

Click the 'OK' button and then 'Exit'.

If checking the client EMS folder, an extra file is created by the Setup Tool.

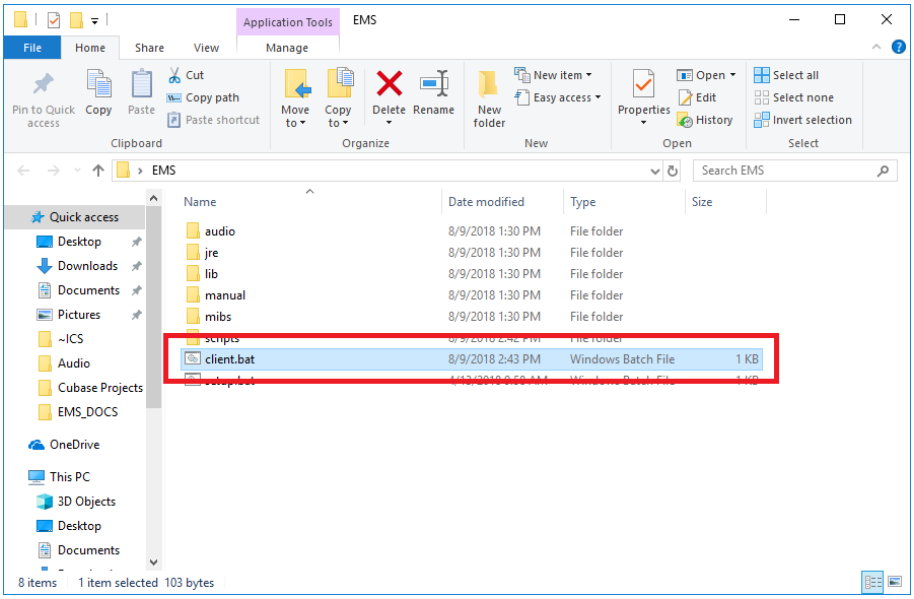


Figure 5-8 EMS Installation Folder

To start the remote client, double click the "client" icon.

Enter the username and password to login (must be valid user created within the server's Admin Console or the admin user. Continue in this chapter with the client operation.

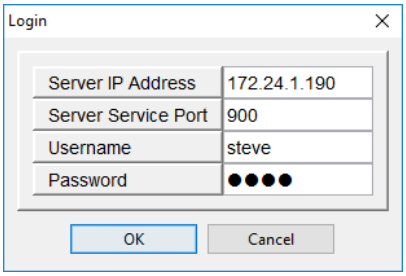


Figure 5-9 EMS Client Login

5.3. Introduction to the EMC GUI Interface

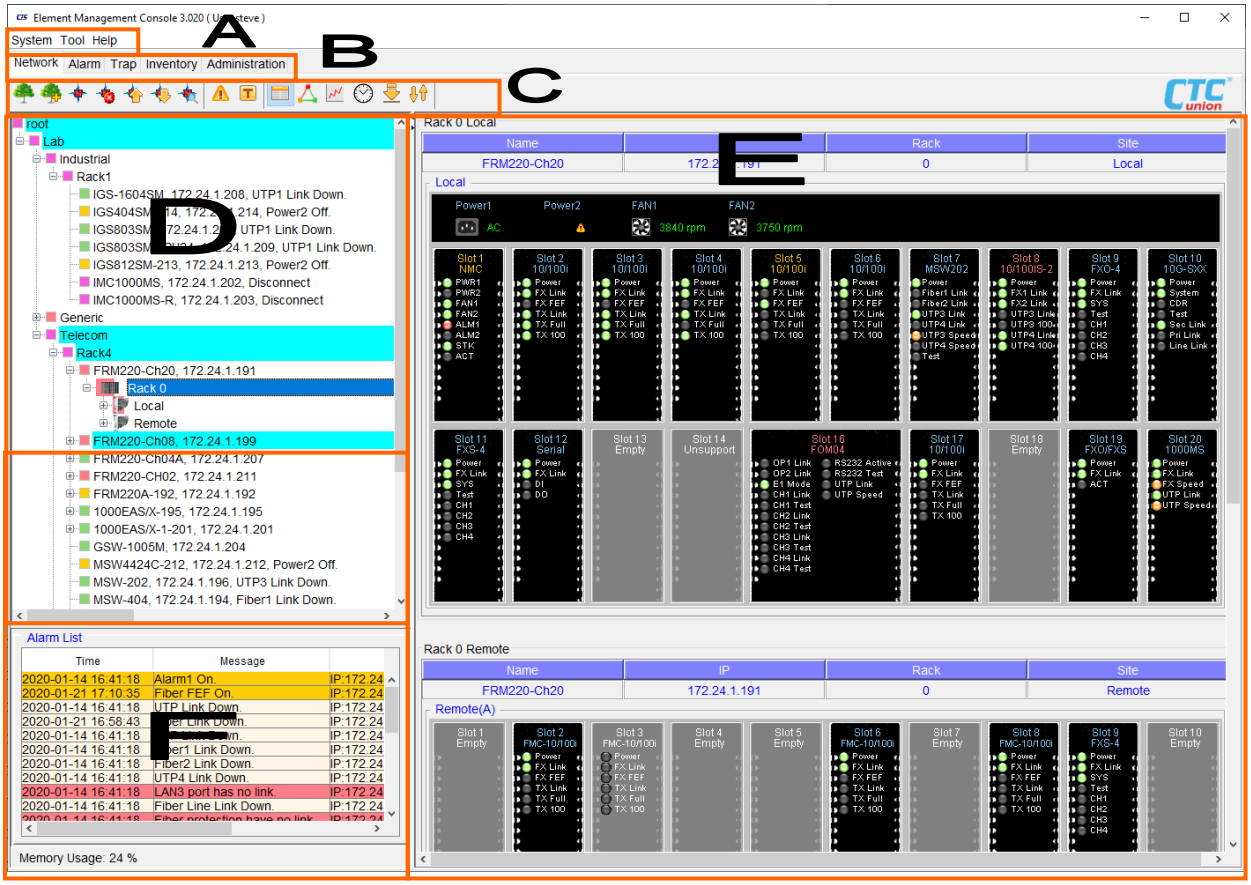


Figure 5-10 EMC Introduction

Location A – Pull-down Menus (System, Tool, Help)
Location B – Management Console Function Tabs (Network, Alarm, Trap, Inventory, Administration***)
Location C – Quick Icons and Management Buttons (Trees, Nodes, Alarms, Device, Multi-Device, Topology, Performance, Network Time Protocol, Upgrading, Parameter Management)
Location D – Root, Nodes and Devices panel
Location E – Device View Panel
Location F – Real time Alarm List

*** Administration from client is a new feature since EMS version 3.016. See section 5.9.

5.4. Organization of the Console Tree

The system administrator or users can manage their Console tree by adding different groups of objects. This Console tree is maintained in the SQL database on the EMS server and is available to the client user from any remote client machine by using their login username.

5.4.1 Adding Trees

The user can create and delete trees using the  button in management area. Figure 5-12 below shows an example of how to create a tree.

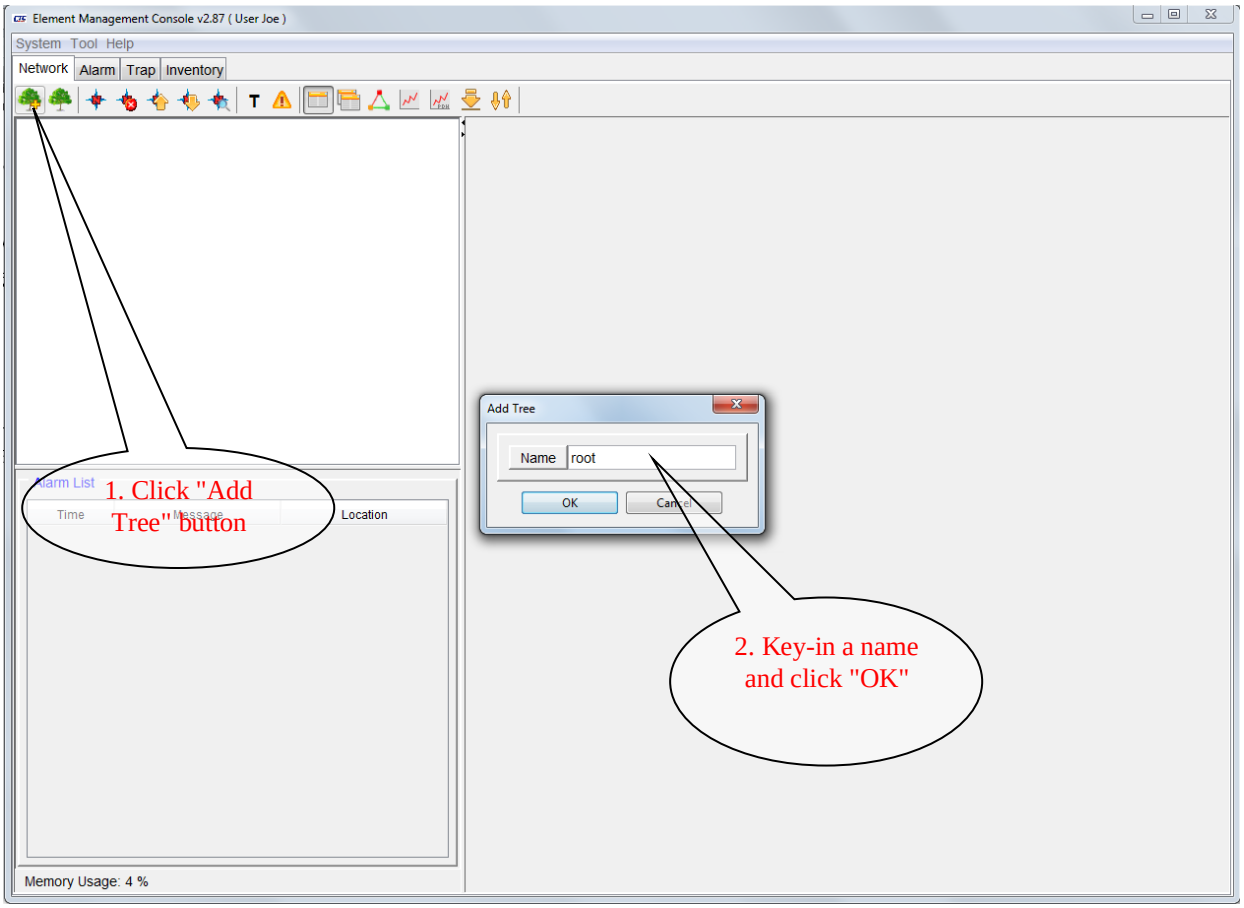


Figure 5-11 Creating a tree

Tree.

Once a tree is created, it can be accessed by this user of the EMS.

Nodes.

The User can add or delete nodes using buttons (Location C) in Node management area (Location D, see Figure 5-10).

When a node is being created, the system will ask for the node type. The EMS supports two node types; "Tree" or "Agent" type.

Tree node.

A Tree node has only a text description name. Tree nodes are useful in separating equipment by different geographical location or by equipment types. The node names could be countries, cities, building, room names, device types, etc.

Agent node.

An Agent node is selected from a list of products that the EMS supports and is currently polling. These will appear in the right panel. (If no devices have been entered for polling, no agent will be available here. Refer to Chapter 4 and the specific section 4.4 Agent (Device) Administration to add agents to EMS.)

5.4.2 Adding Nodes

The user can create and delete nodes using button  in management area. Figure 5-12 below shows an example of how to create a node.

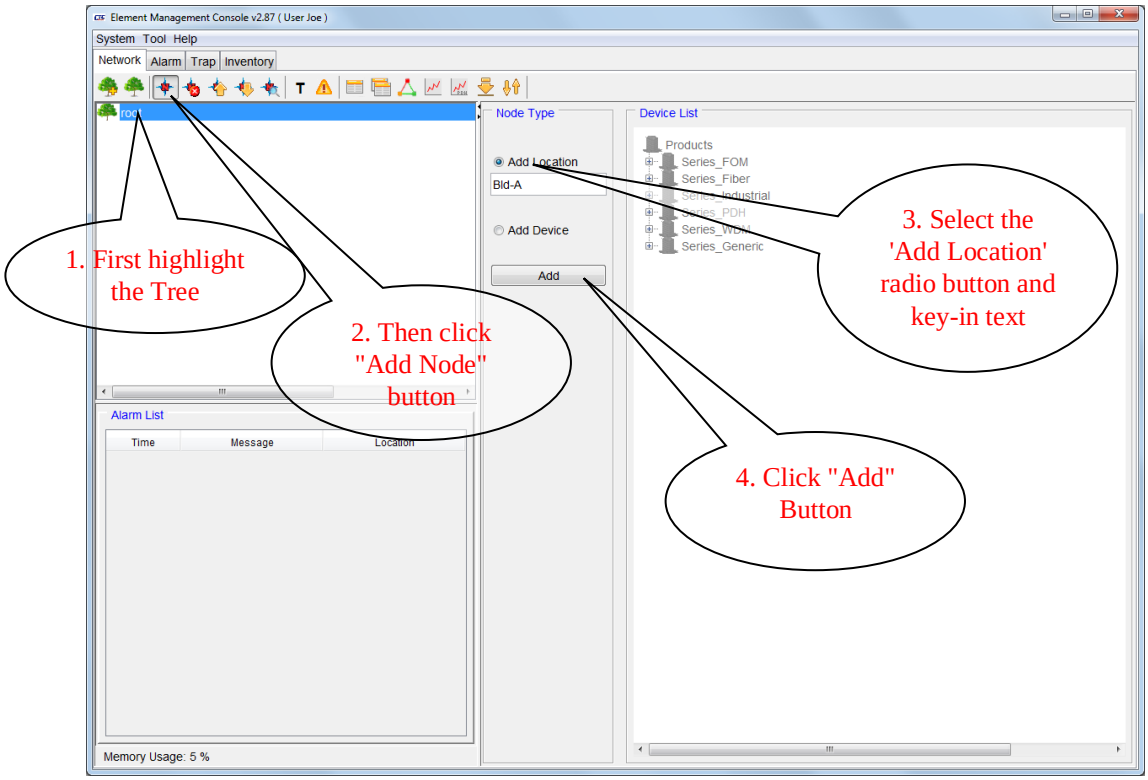


Figure 5-12 Creating a Location Node

These nodes help to make the hierarchy of a large tree more manageable and easier to navigate. They also can be name searched, for added ease in finding equipment.

5.4.3 Adding Agent Nodes

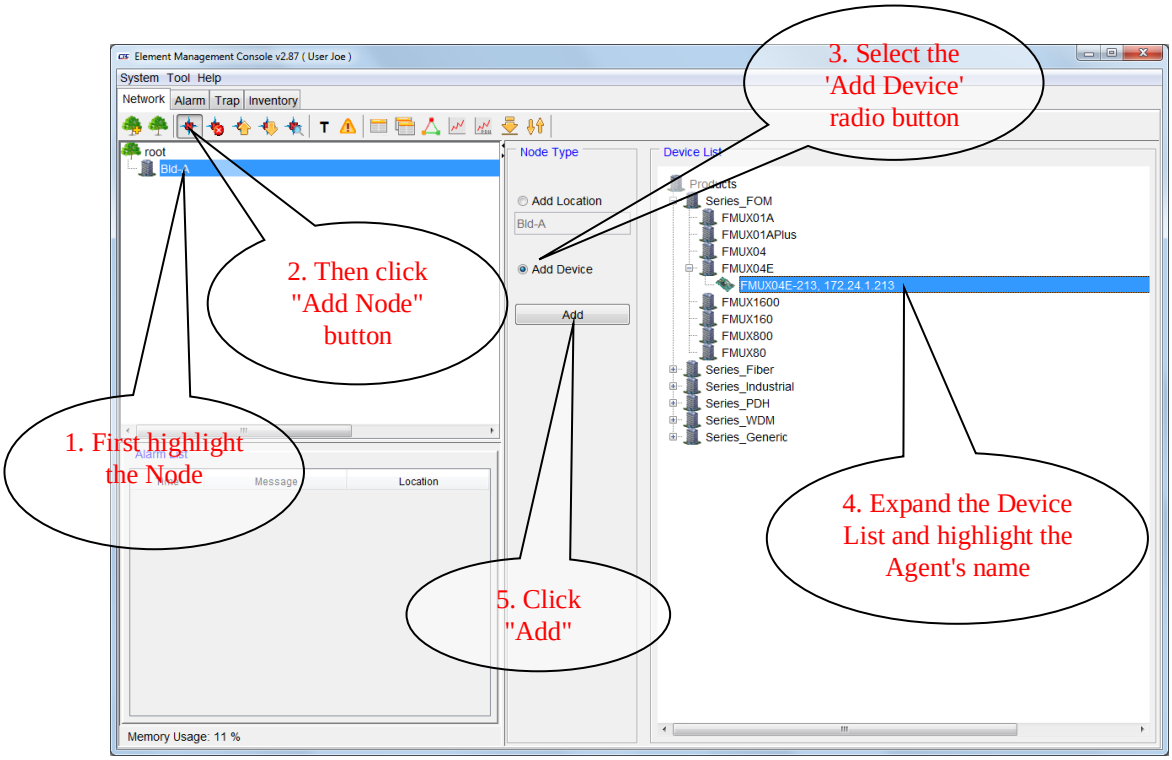


Figure 5-13 Creating an Agent Node

When adding Agent nodes, you could also choose to add any of the intermediate product groups as nodes. However, in the example above we directly added the network element, the FMUX04E.

5.4.4 Example Agent Nodes

Click the "Device View" icon to view device information in the right panel.

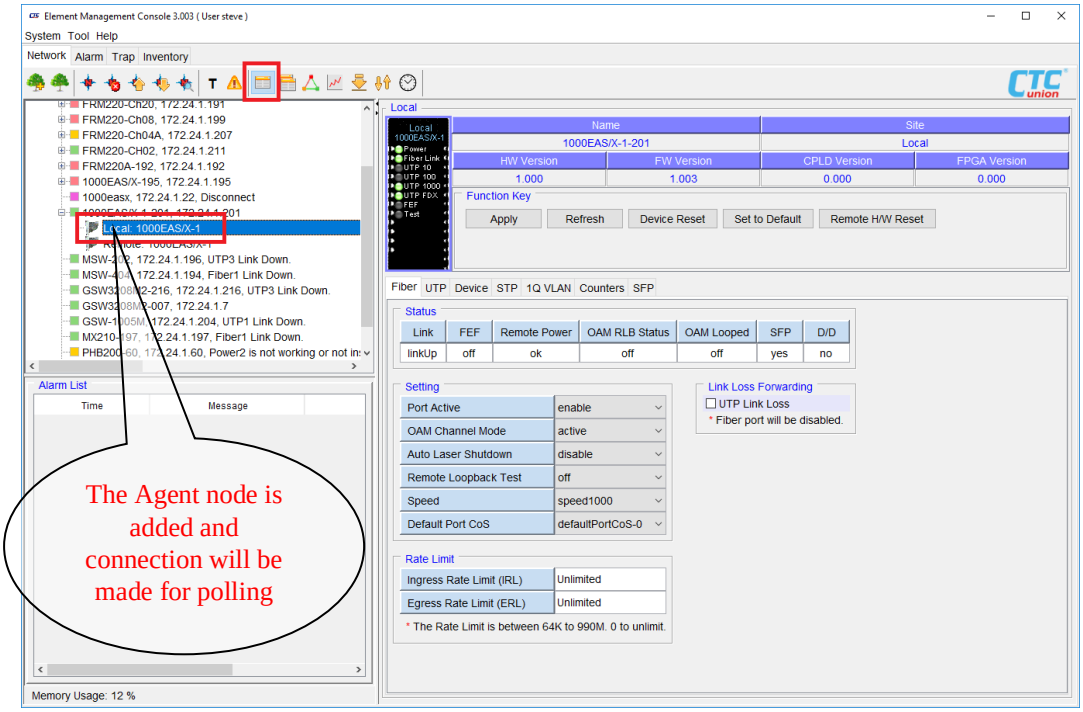


Figure 5-14 Example display of an Agent Node

The following is an example of display of a remote (in-band managed) 1000EAS/X-1 unit.

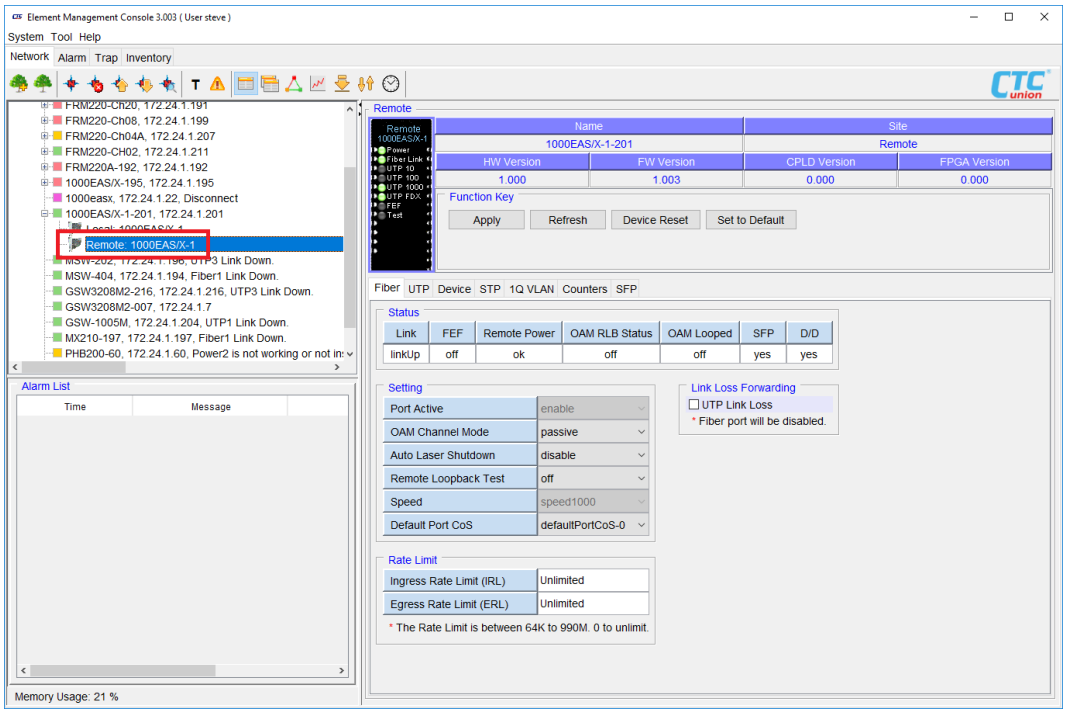


Figure 5-15 Display example of remote OAM media converter

The following is an example of display of a full FRM220 CH20 unit with all local and remote converters.

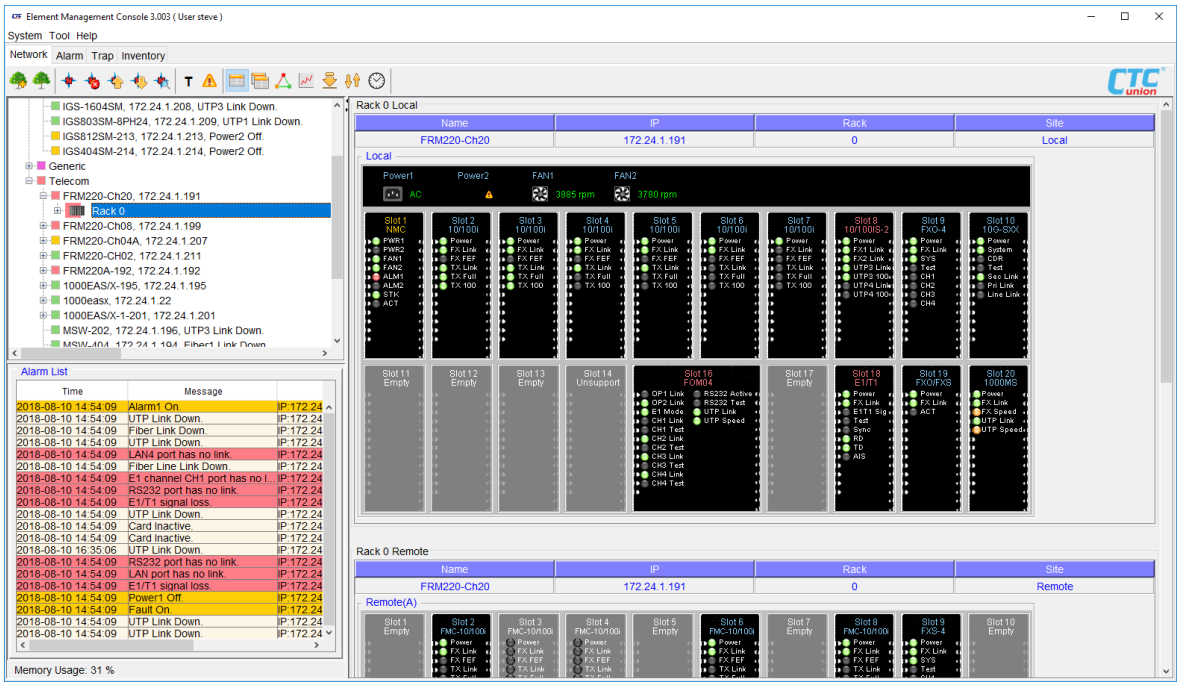


Figure 5-16 Full display example of CH20, local and remote

The following is an example of display of a full FRM220 CH08 unit with all local and remote converters.

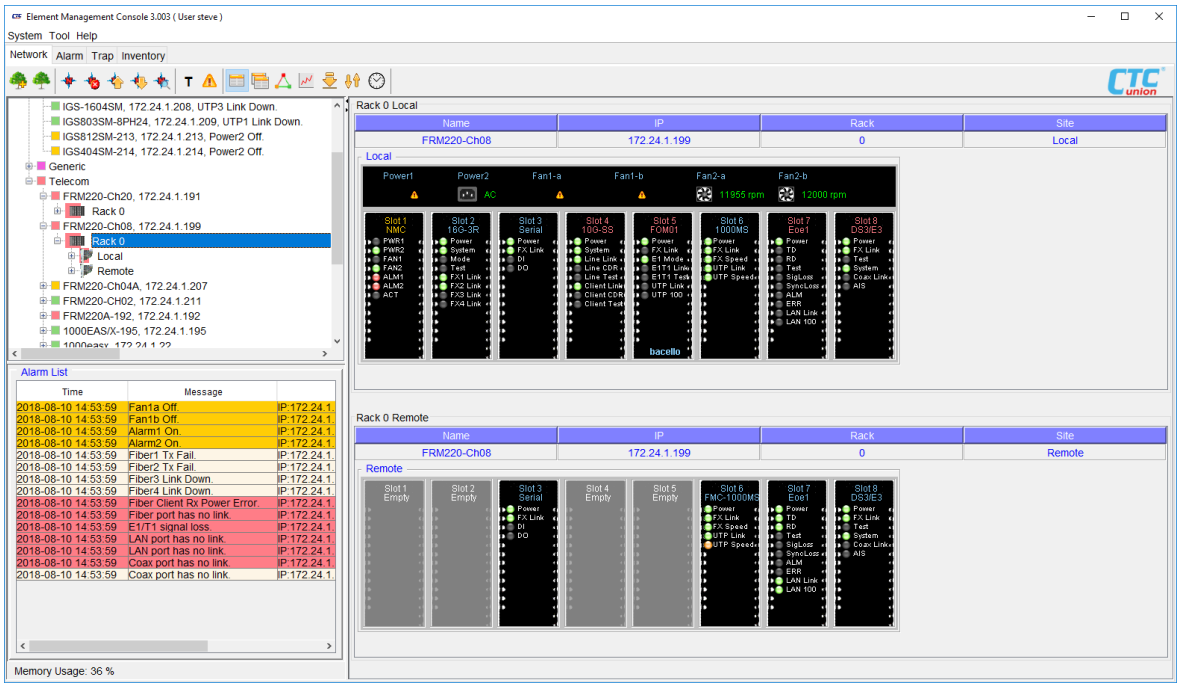


Figure 5-17 Full display example of CH08, local and remote

5.5. Monitoring and Provisioning via EMC

The following example describes how to enable bandwidth control and do control setting for 10/100i card in FRM220 chassis. Refer to the FRM220 NMC Operation Manual for details of the actual functions and settings of the FRM220-10/100i card.

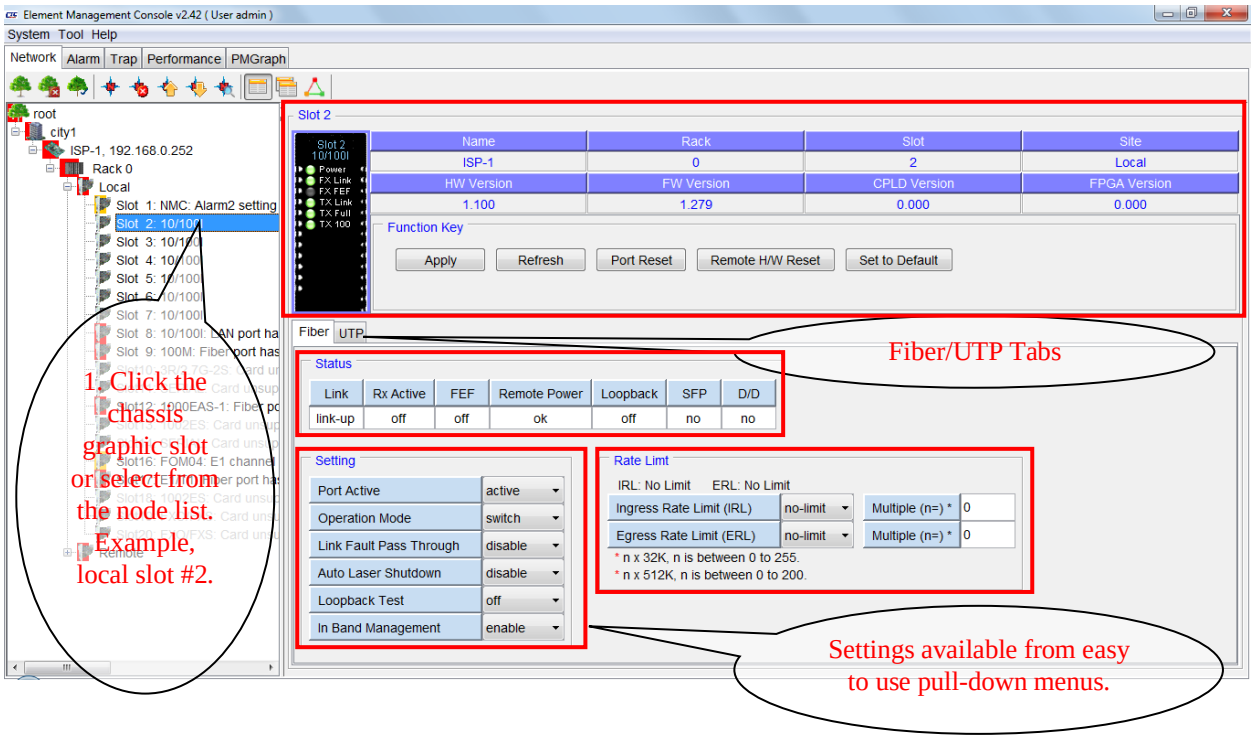


Figure 5-18 Point and Click user interface

The interface is very user friendly. Pointing, clicking to open menus, double clicking on slot graphics, "help" items (with question mark "?") along with informational windows all aid in allowing the network administrator to quickly configure, monitor and find faults for all active elements on the network supported by the SmartView EMS.

5.5.1 Provisioning example via EMC

The following four step example describes how to configure bandwidth control on a 10/100i media converter, for 10Mbps.

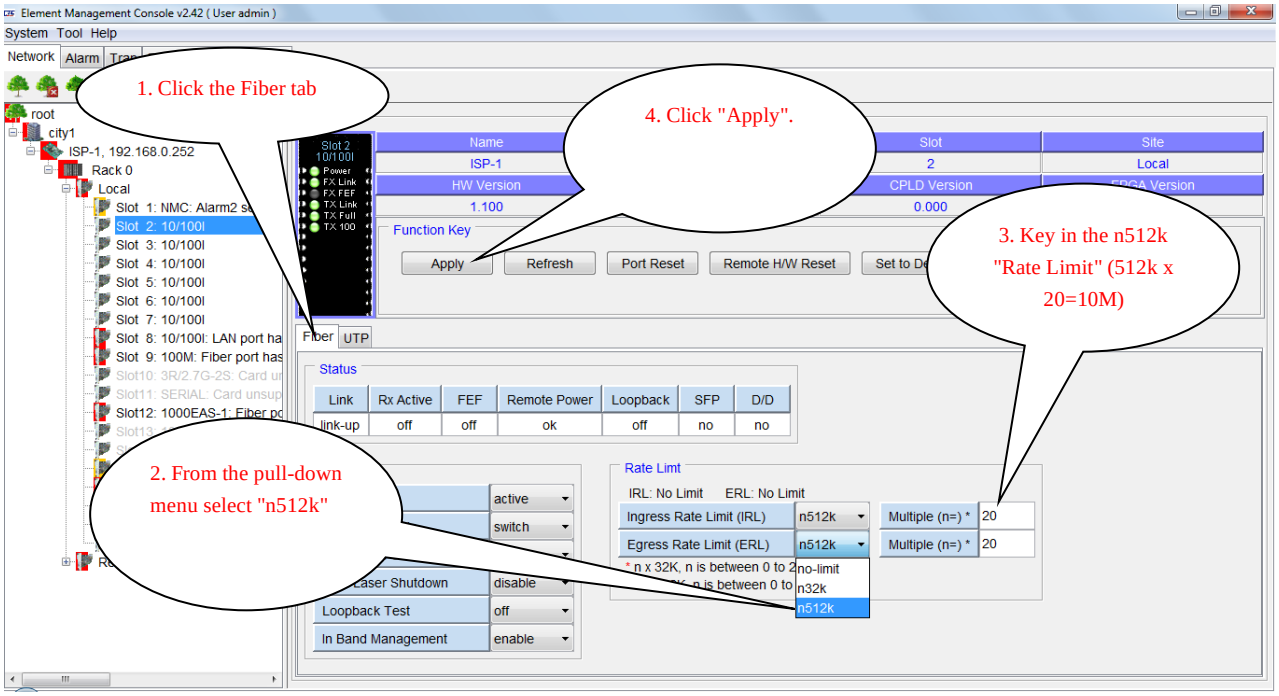


Figure 5-19 Set the Rate Limit Mode (no-limit, 32k or 512k)

5.5.2 Alarm Handling

When alarms (minor or major) are detected, the tree icons will change color. In the tree, the Green color indicates that the device has no alarm conditions. The Yellow color is used to indicate minor alarms, while the Red color is used to indicate major alarms. In the 'Alarm List' frame, all active alarms are listed for the selected equipment (the local 1000EAS/X in this example). In the Alarm list, no color is used to indicate a warning alarm, while Yellow is a minor alarm and Red is a major alarm.

Alarms are defined in the Alarm Selection by clicking the icon. Types of conditions are listed, there are enable check boxes for each type and the 'severity' may be selected from a pull-down menu. The "Global Apply" button, will set that alarm definition for all of the same device types (1000EAS/X in this example).

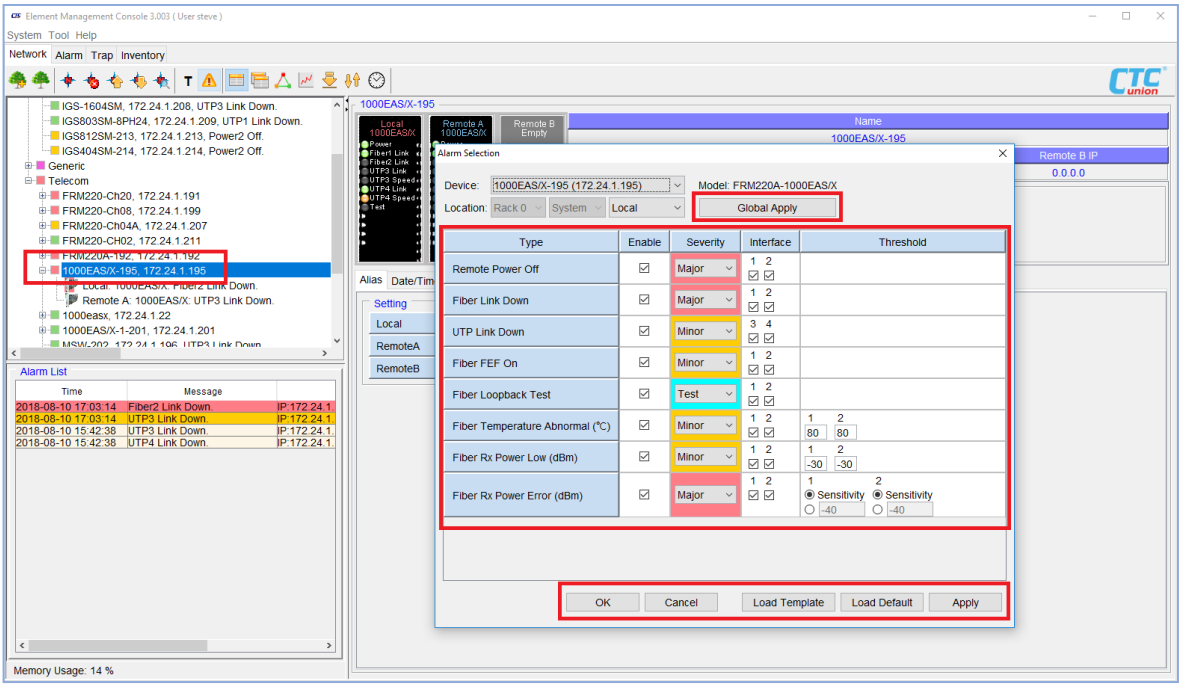


Figure 5-20 Minor alarm indication, shown in Yellow, Major in Red.

5.5.3 Alarm Templates

EMS uses Alarm Templates that are pre-defined for each device type. These templates may be customized by the client so they are tailored exactly for each application. To view and edit templates, click the icon. The template editor has a pull-down for each device type. Customize the template and click 'Apply'. Exit by clicking 'OK'. The 'Load Default' button will return the template to EMS default.

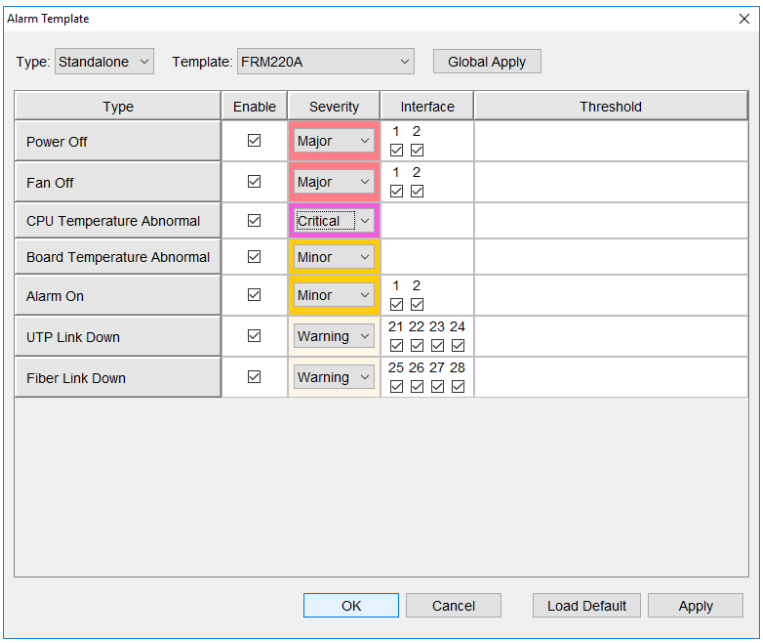


Figure 5-21 Edit Alarm Templates for Devices

5.5.4 Alarm Log

All major and minor alarms are recorded and kept in the database. To view these, just click the 'Alarm' tab. The export function allows saving the alarm log externally in CSV (comma separated values).

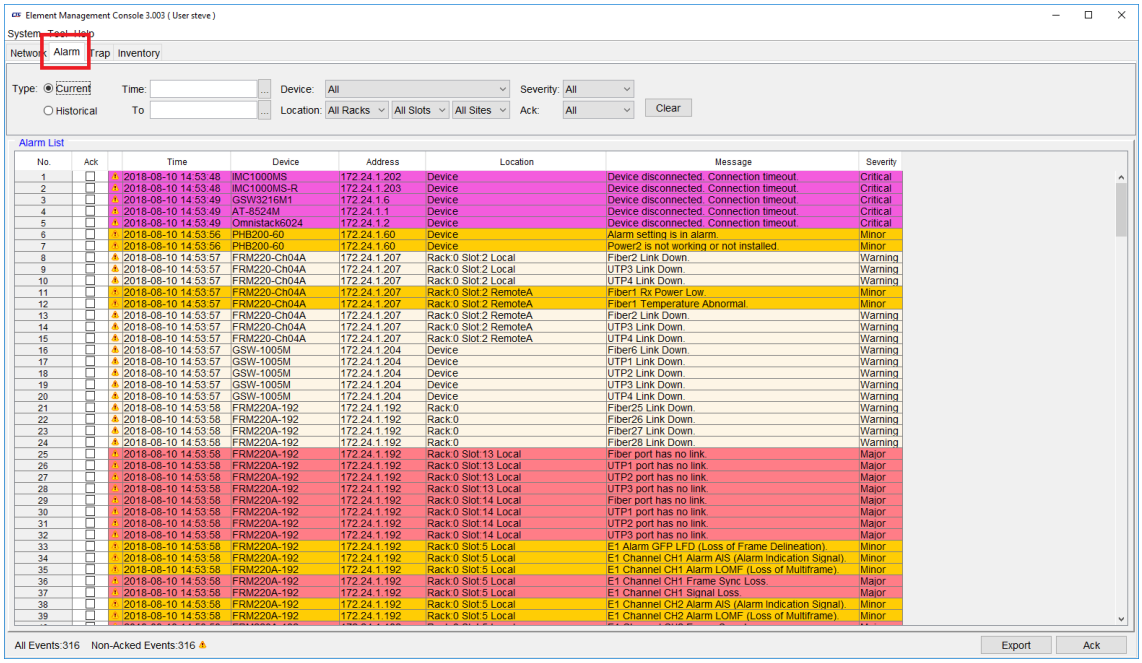


Figure 5-22 Major alarms shown in Red, Minor alarms shown in Yellow, warnings White

5.5.5 Traps

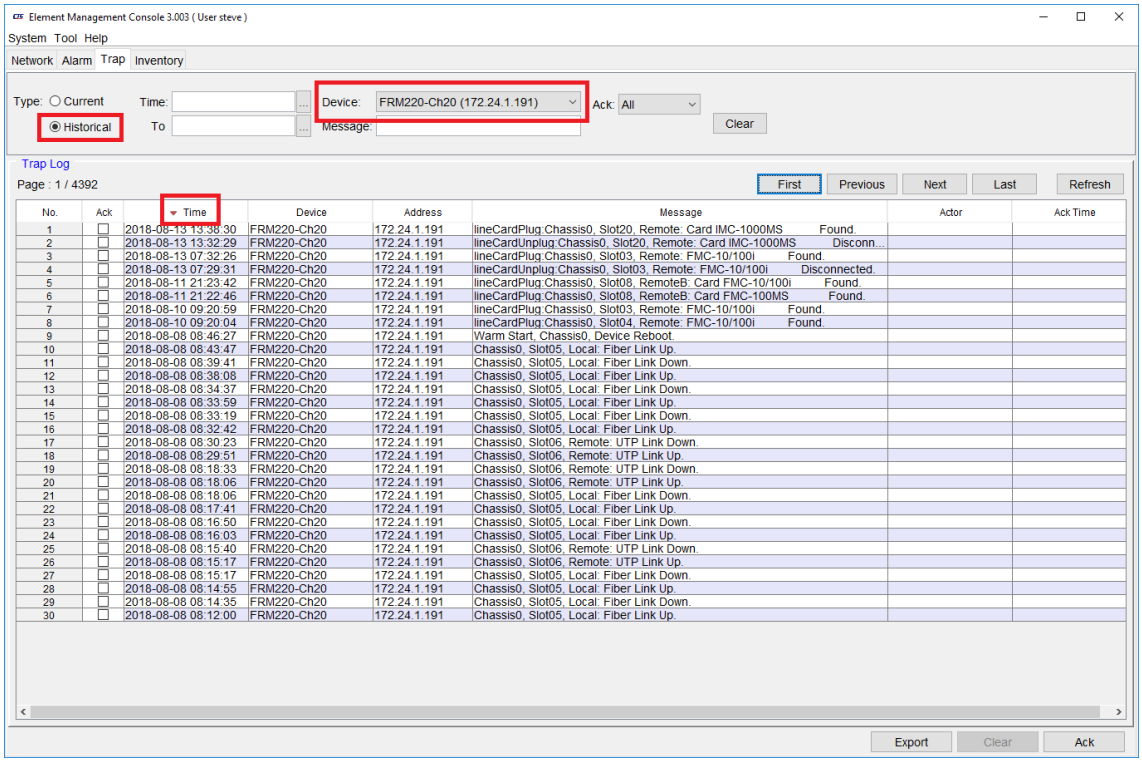


Figure 5-23 View of the Trap window and filters

The trap window has a number of filters that can be applied to view acknowledged traps, un-acknowledged traps, traps by agent, traps during specific time period or traps by specific message (mask filter).

The 'Export' button will create a CSV (comma separated values) file on the local computer. This file may then be manipulated or viewed with other software, for example, Microsoft Excel.

5.5.6 Performance

All the performance values can be monitored and displayed on control template in real-time. However, not all network elements have performance data. So, for those elements, there is nothing to show. Performance data is typically limited to transmissions such as G.703 E1 or T1 (DS1) in Access Units as well as optical aggregate performance in Fiber Optical Multiplexers and SDH Multiplexers. It is also available from RMON data from switches as well as SFP DDMI data such as temperature and Fiber Rx power.

All the performance records are read and stored in the database at user programmable intervals of 5, 10, 15, 30 minutes or 1 hour. Performance displays are user programmable for 1, 12, 24 hours or 7, 30 days. On the Performances page, press "Refresh" to get the current performance records in database. Press "Export" to get the current performance records in database and save to files on the local disk. Three format types may be exported; an HTML formatted file which can be opened in any browser, a simple Text formatted file with an indexed list of all performance records, or CSV (comma separated values) format which can be opened by spreadsheet software such as Microsoft Excel. The performance exports can be found in the 'Reports' folder in the root EMS folder.

5.5.7 Setup for Performance Monitoring

In this example, a media converter with SFP that supports DDMI will be monitored for RX power performance.

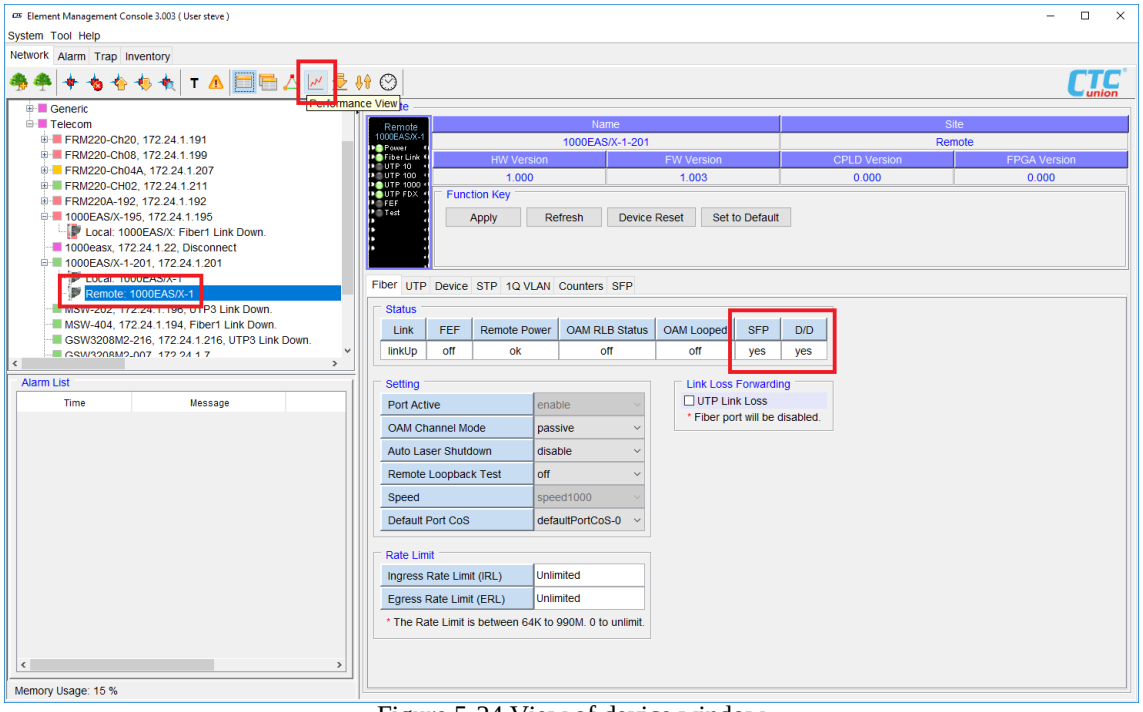


Figure 5-24 View of device window

Once highlighting the device, click on the  'performance view icon'.

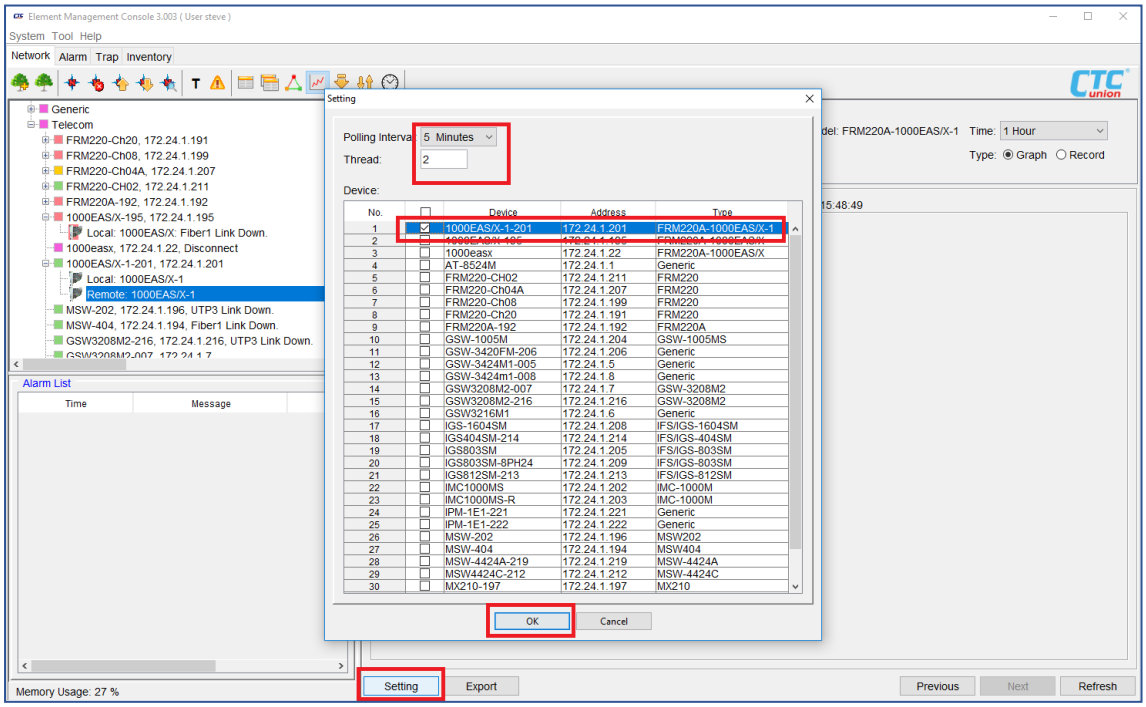


Figure 5-25 Setup device for performance monitoring

Click the 'Setting' button to get the popup. Polling interval is set to shortest, i.e., 5 minutes, the device to be polled is selected by check box and then click 'OK'.

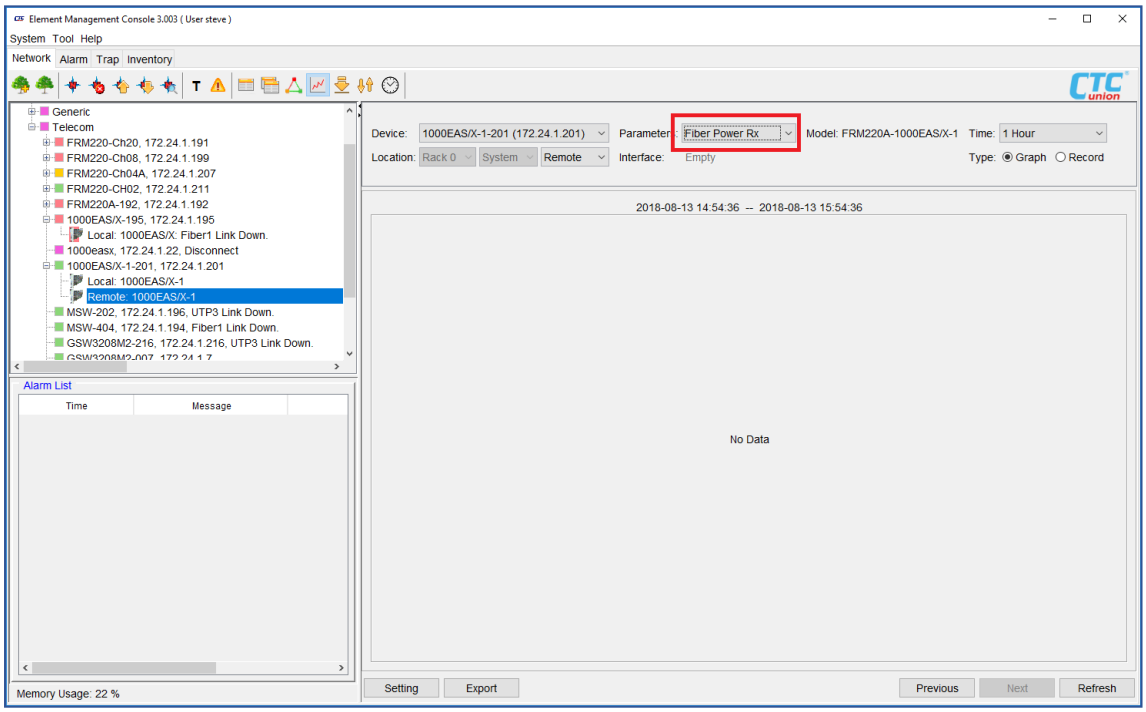


Figure 5-26 Waiting for performance data

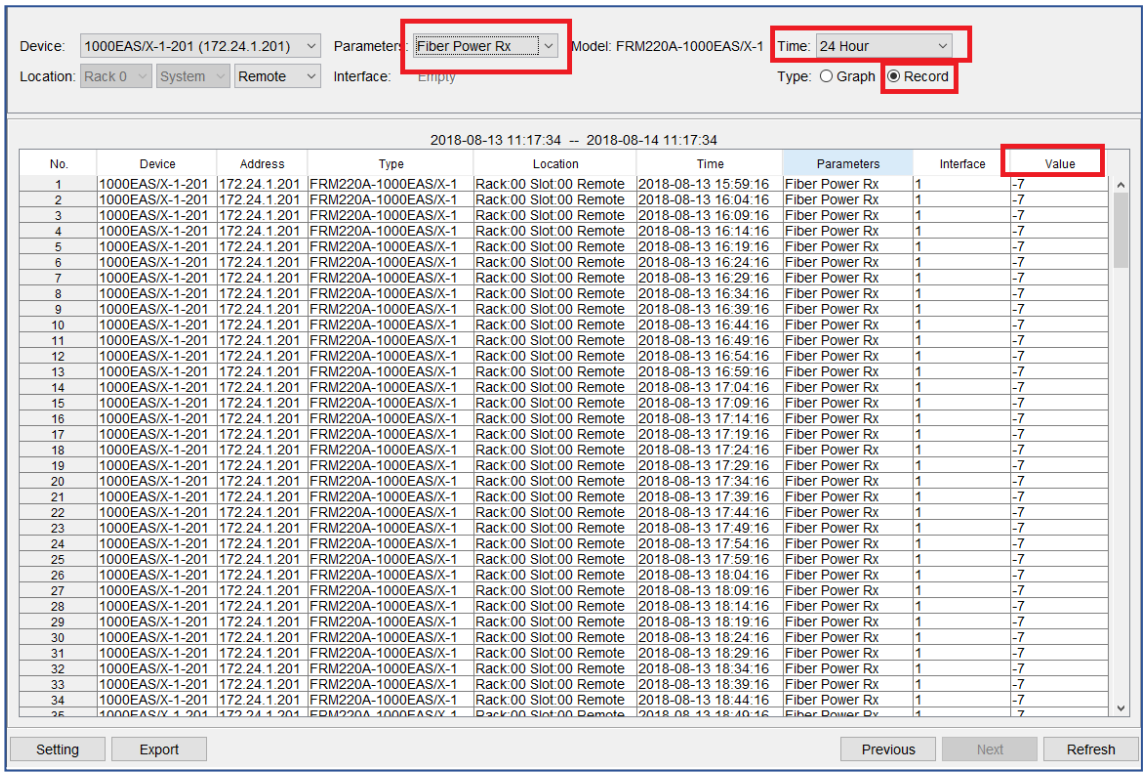
The device is now polled every 5 minutes. We'll need to wait at least 1 hour before any data is available.

Reporting and sorting of performance is accomplished by setting a time window (from and to), by selecting agent name, and by providing text filter and mask. If no sorting criteria are entered, the display will show all the records.

After 24 hours, we have some data.

5.5.8 PM Records and Graphs

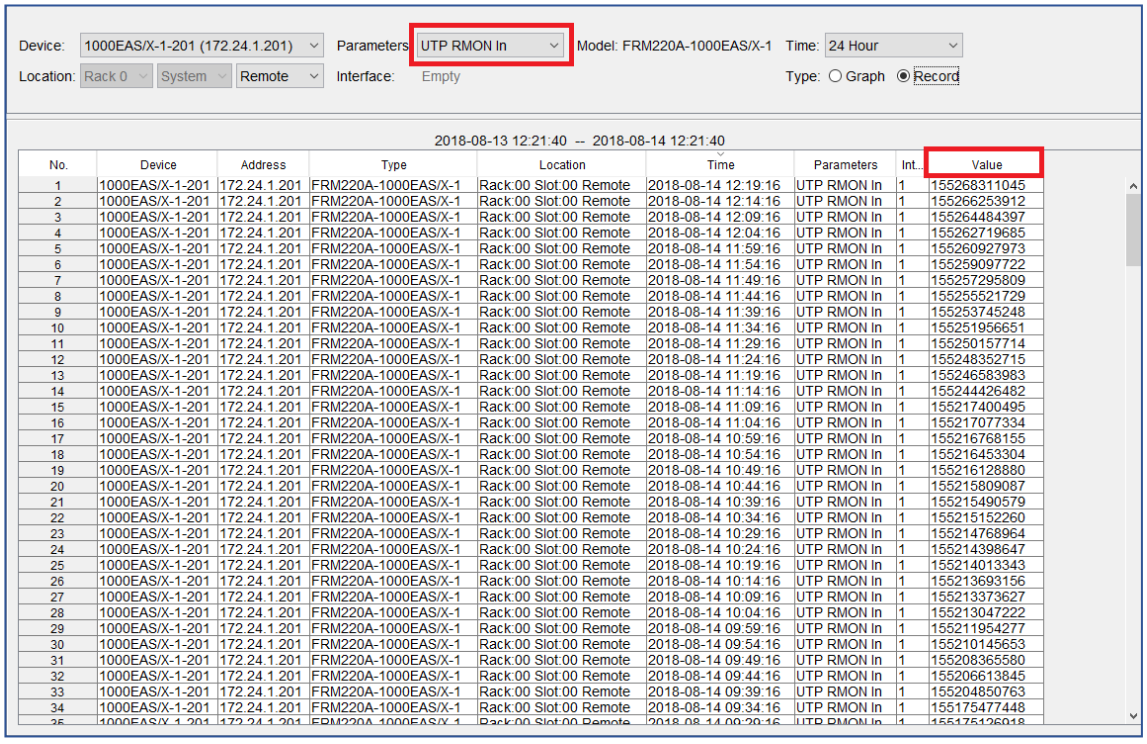
From the  'performance view icon', select the device, location, parameter and time period. To view in 'record' form, i.e., as a table, make sure to click the radio button to "Record".



No.	Device	Address	Type	Location	Time	Parameters	Interface	Value
1	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 15:59:16	Fiber Power Rx	1	-7
2	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 16:04:16	Fiber Power Rx	1	-7
3	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 16:09:16	Fiber Power Rx	1	-7
4	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 16:14:16	Fiber Power Rx	1	-7
5	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 16:19:16	Fiber Power Rx	1	-7
6	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 16:24:16	Fiber Power Rx	1	-7
7	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 16:29:16	Fiber Power Rx	1	-7
8	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 16:34:16	Fiber Power Rx	1	-7
9	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 16:39:16	Fiber Power Rx	1	-7
10	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 16:44:16	Fiber Power Rx	1	-7
11	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 16:49:16	Fiber Power Rx	1	-7
12	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 16:54:16	Fiber Power Rx	1	-7
13	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 16:59:16	Fiber Power Rx	1	-7
14	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 17:04:16	Fiber Power Rx	1	-7
15	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 17:09:16	Fiber Power Rx	1	-7
16	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 17:14:16	Fiber Power Rx	1	-7
17	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 17:19:16	Fiber Power Rx	1	-7
18	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 17:24:16	Fiber Power Rx	1	-7
19	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 17:29:16	Fiber Power Rx	1	-7
20	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 17:34:16	Fiber Power Rx	1	-7
21	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 17:39:16	Fiber Power Rx	1	-7
22	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 17:44:16	Fiber Power Rx	1	-7
23	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 17:49:16	Fiber Power Rx	1	-7
24	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 17:54:16	Fiber Power Rx	1	-7
25	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 17:59:16	Fiber Power Rx	1	-7
26	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 18:04:16	Fiber Power Rx	1	-7
27	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 18:09:16	Fiber Power Rx	1	-7
28	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 18:14:16	Fiber Power Rx	1	-7
29	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 18:19:16	Fiber Power Rx	1	-7
30	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 18:24:16	Fiber Power Rx	1	-7
31	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 18:29:16	Fiber Power Rx	1	-7
32	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 18:34:16	Fiber Power Rx	1	-7
33	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 18:39:16	Fiber Power Rx	1	-7
34	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-13 18:44:16	Fiber Power Rx	1	-7

Figure 5-27 View of Performance Record

The above is an example of RX power on an 1000EAS/X-1 SFP in Port 1 over a 24 hour period and it remains at -7dBm.



No.	Device	Address	Type	Location	Time	Parameters	Int...	Value
1	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 12:19:16	UTP RMON In	1	155268311045
2	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 12:14:16	UTP RMON In	1	155266253912
3	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 12:09:16	UTP RMON In	1	155264484397
4	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 12:04:16	UTP RMON In	1	155262719685
5	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 11:59:16	UTP RMON In	1	155260927973
6	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 11:54:16	UTP RMON In	1	155259097722
7	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 11:49:16	UTP RMON In	1	155257295809
8	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 11:44:16	UTP RMON In	1	155255521729
9	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 11:39:16	UTP RMON In	1	155253745248
10	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 11:34:16	UTP RMON In	1	155251956651
11	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 11:29:16	UTP RMON In	1	155250157714
12	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 11:24:16	UTP RMON In	1	155248352715
13	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 11:19:16	UTP RMON In	1	155246583983
14	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 11:14:16	UTP RMON In	1	155244426482
15	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 11:09:16	UTP RMON In	1	155217400495
16	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 11:04:16	UTP RMON In	1	155217077334
17	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 10:59:16	UTP RMON In	1	155216768155
18	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 10:54:16	UTP RMON In	1	155216453304
19	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 10:49:16	UTP RMON In	1	155216128880
20	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 10:44:16	UTP RMON In	1	155215809087
21	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 10:39:16	UTP RMON In	1	155215490579
22	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 10:34:16	UTP RMON In	1	155215152260
23	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 10:29:16	UTP RMON In	1	155214768964
24	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 10:24:16	UTP RMON In	1	155214398647
25	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 10:19:16	UTP RMON In	1	155214013343
26	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 10:14:16	UTP RMON In	1	155213693156
27	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 10:09:16	UTP RMON In	1	155213373627
28	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 10:04:16	UTP RMON In	1	155213047222
29	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 09:59:16	UTP RMON In	1	155211954277
30	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 09:54:16	UTP RMON In	1	155210145653
31	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 09:49:16	UTP RMON In	1	155208365580
32	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 09:44:16	UTP RMON In	1	155206613845
33	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 09:39:16	UTP RMON In	1	155204850763
34	1000EAS/X-1-201	172.24.1.201	FRM220A-1000EAS/X-1	Rack:00 Slot:00 Remote	2018-08-14 09:34:16	UTP RMON In	1	155175477448

Figure 5-28 Another view of Performance Record

This example shows the increasing ingress RMON byte counter for the UTP port.

We could also display this as a graph. Simply click the 'graph' radio button.

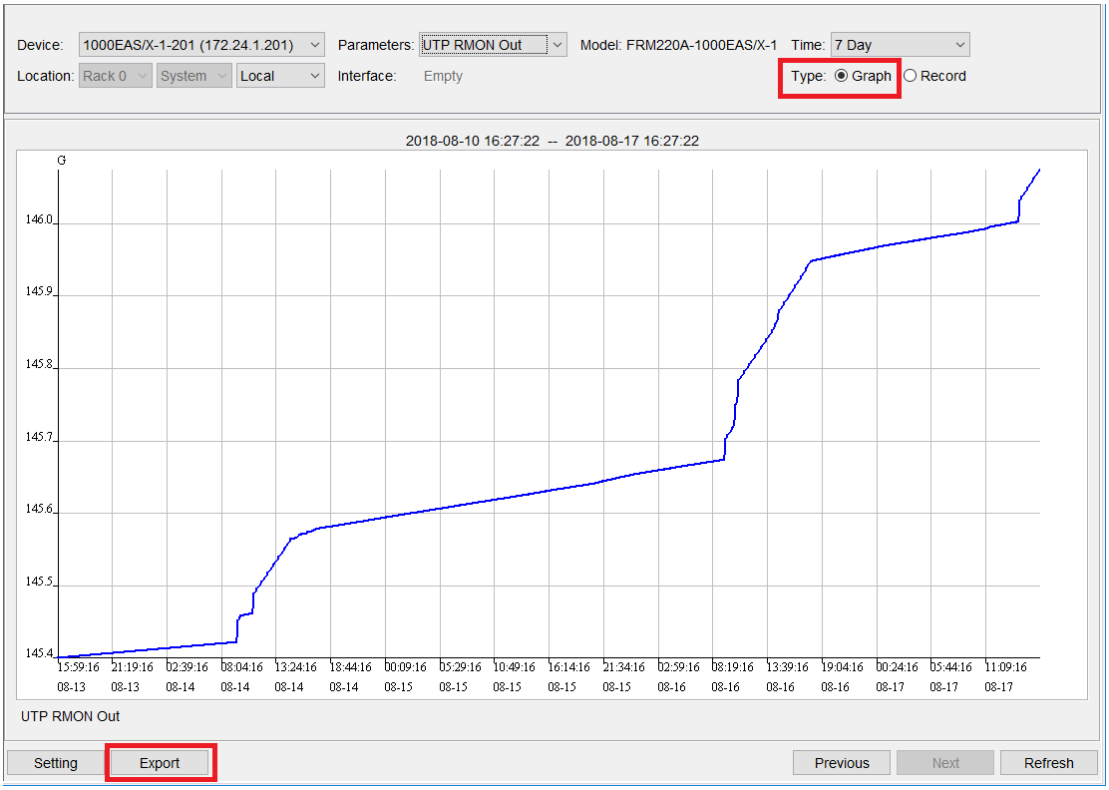


Figure 5-29 RMON counter graph

Let's say we want a graph that shows throughput over time. We can export this data, which is just an increasing counter, sampled every 5 minutes for 24 hours. We can manipulate the data in Excel to take the change of each interval, multiply each value by 8 (change bytes to bits) and divide by 300 (300 seconds equals 5 minutes) and have data to display bits per second over 24 hours.

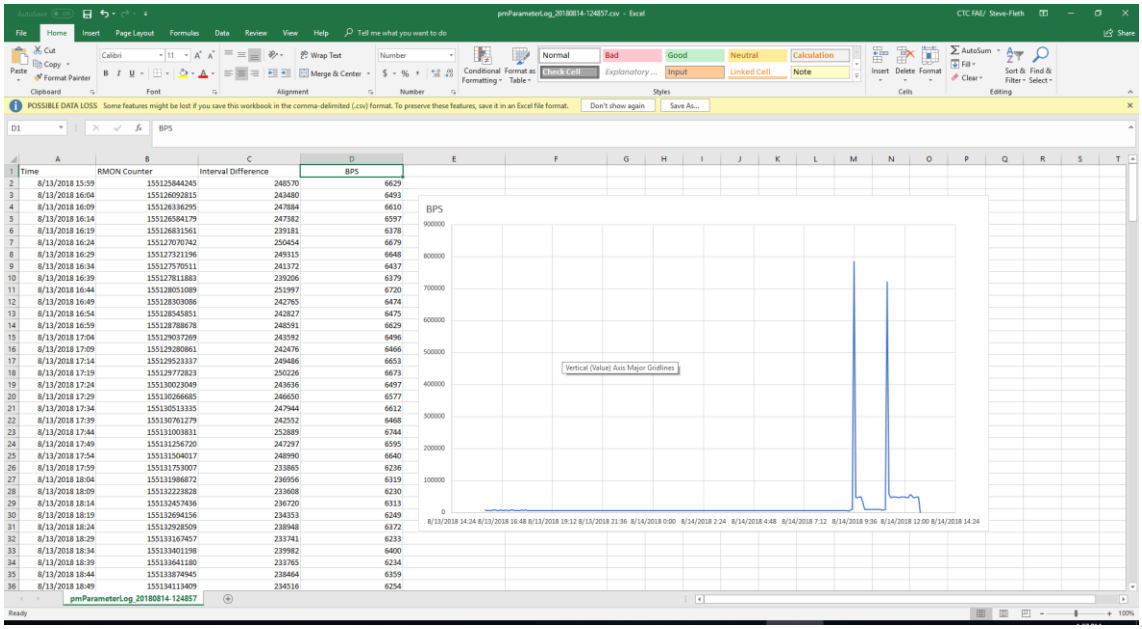


Figure 5-30 Using Excel to manipulate data and build a BPS graph

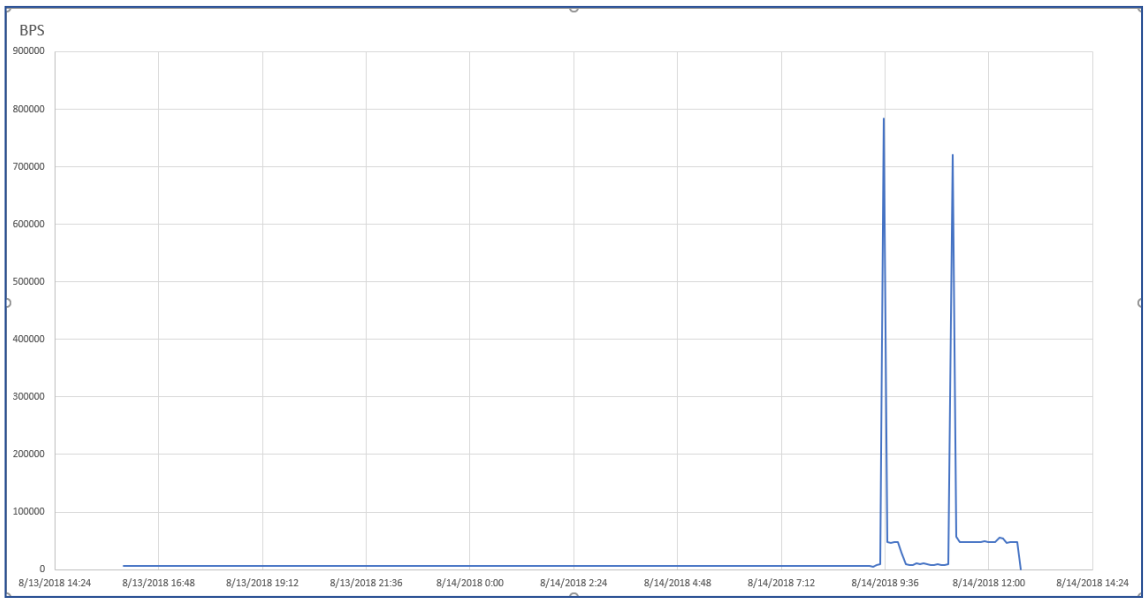


Figure 5-31 Microsoft Excel graph to show bits per second over 24 hour period

Performance monitoring is not available with all devices. However, when it is available, it can be used to monitor throughput trends, SFP temperatures and Rx Power figures and other "performance" related data. This is a very powerful tool and by exporting data, many different graphs can be realized.

5.6 Upgrade View

A few products support scheduling updates, such as FRM220 NMC cards, FRM220A-1000EAS/X, All IFS/IGS Managed Industrial Switches, MSW-4424A, MSW-202/404 and MX210.

Get to the **Upgrade View** by clicking the **Upgrade View** icon. If possible, key in now the IP address for the TFTP Server which will be used and that has the proper image files loaded on it.

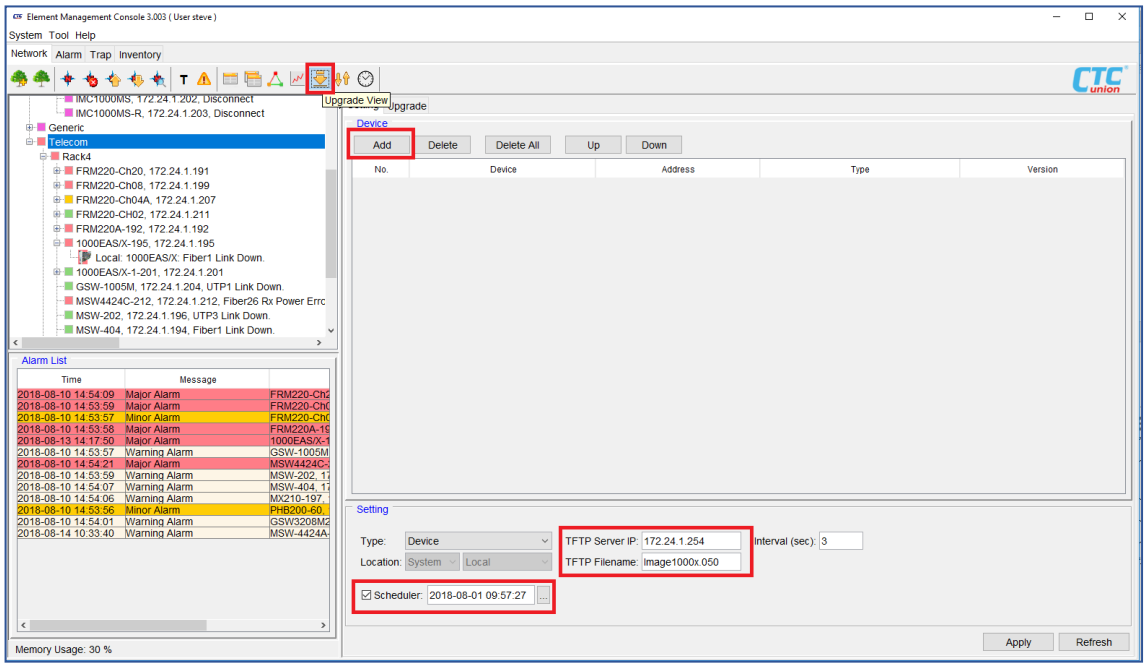


Figure 5-32 Upgrade View Panel

5.6.1 Add Devices

Step 1. In the Setting tab, click the **Add** button in the **Device** window.

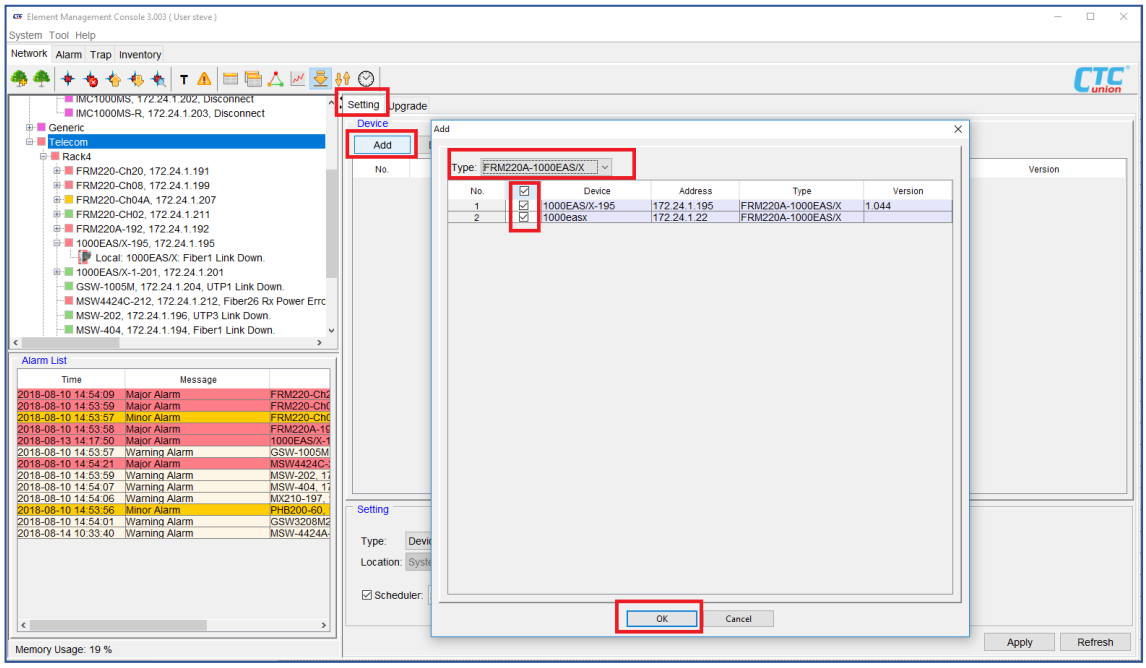


Figure 5-33 Add Device

Step 2. Select the device type from the **Type** pulldown menu.
Step 3. Check the units that will be upgraded.
Step 4. Click **OK**.

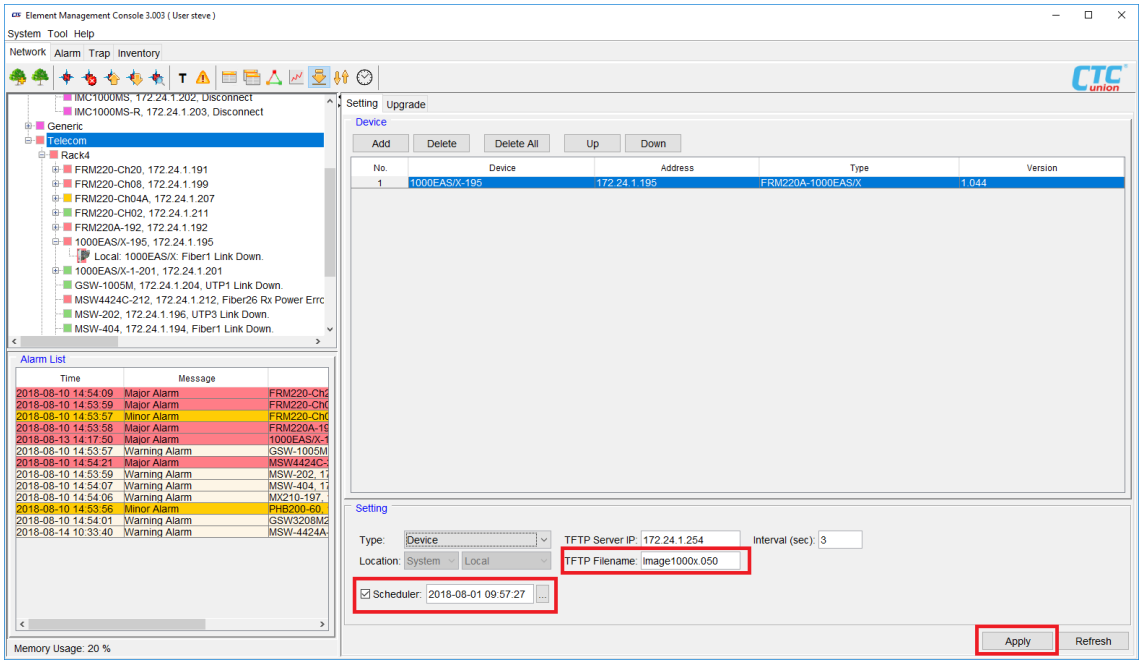


Figure 5-34 Scheduling and filename

5.6.2 Set Scheduling

Step 5. Enter the correct filename for the firmware image located on the TFTP Server.
Step 6. Setup the **Scheduler**, the button will call up a popup to aid in entering the exact date and time.

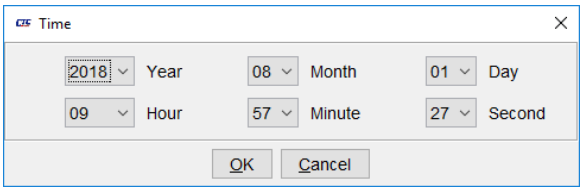


Figure 5-35 Time Entry

Step 7. Click **Apply**.

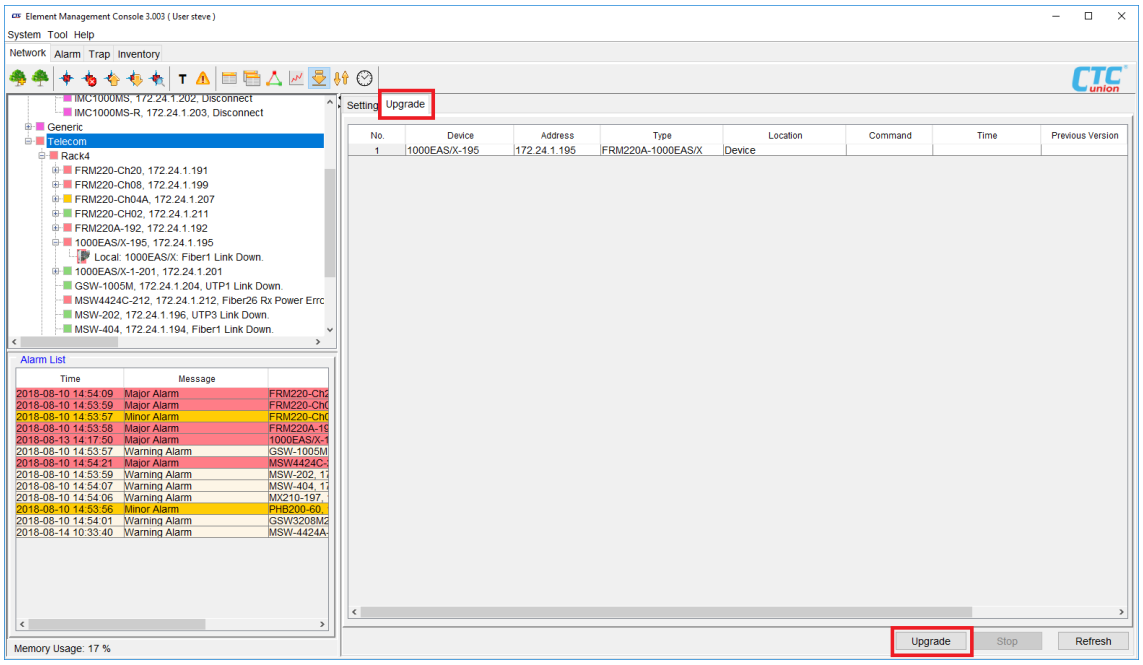


Figure 5-36 Upgrade Window

Step 8. Click the **Upgrade** tab and view the devices set for upgrade.

5.6.3 Upgrade

Step 9. Click **Upgrade**.

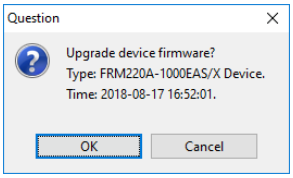


Figure 5-37 Confirmation Dialog Box

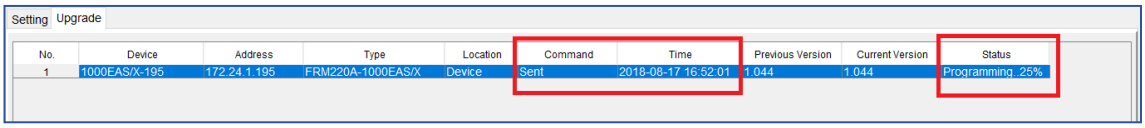


Figure 5-38 Programming

5.6.4 Upgrade Status

Following the upgrade, the status for all upgraded devices will be displayed. Normal status is a success. The previous and new versions are both reported.

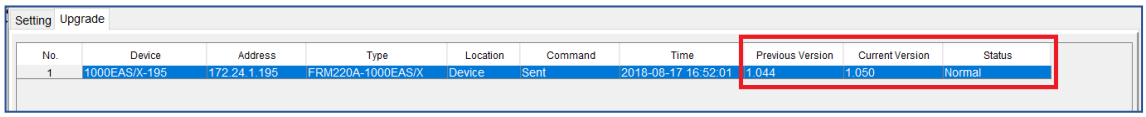


Figure 5-39 Upgrade Status

5.7 Parameter Management

Open the Parameter Management window by clicking on the icon. EMS is able to backup, restore and copy configurations for the FRM220 family.

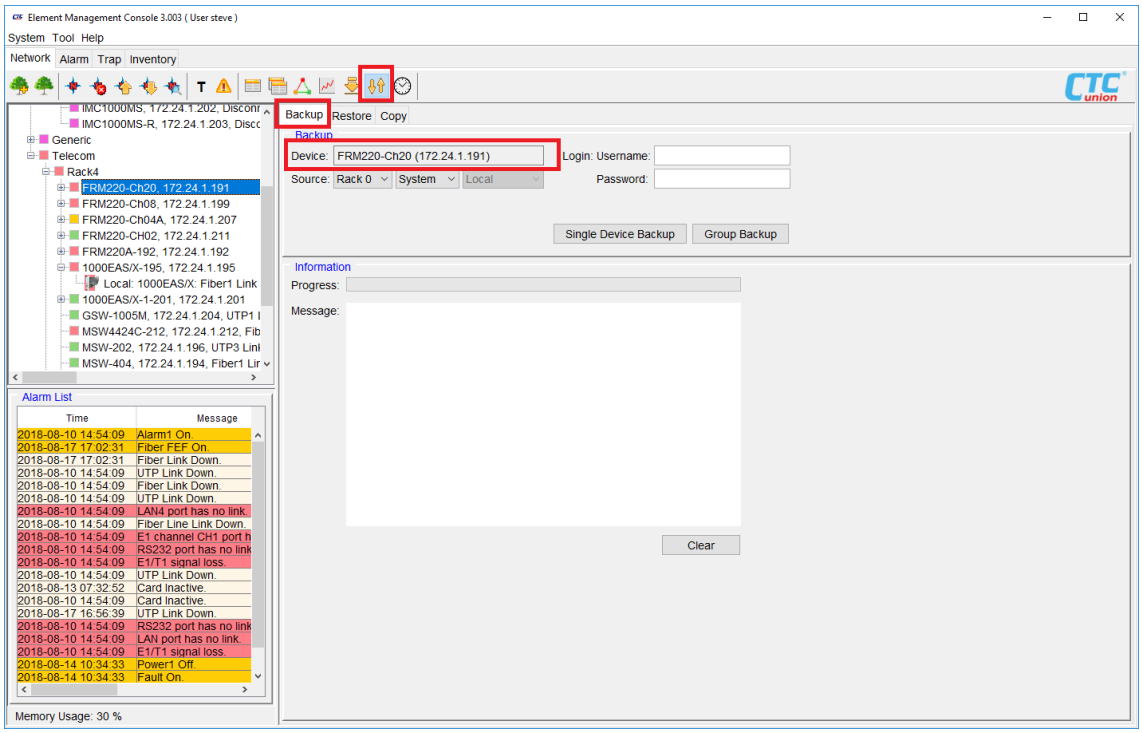


Figure 5-40 Parameter Management Backup

5.7.1 Backup FRM220 System

A system backup includes the NMC IP address, mask, gateway, and all SNMP, SNTP and system settings. Installed line cards may also be backed up as all cards or as single card backup.

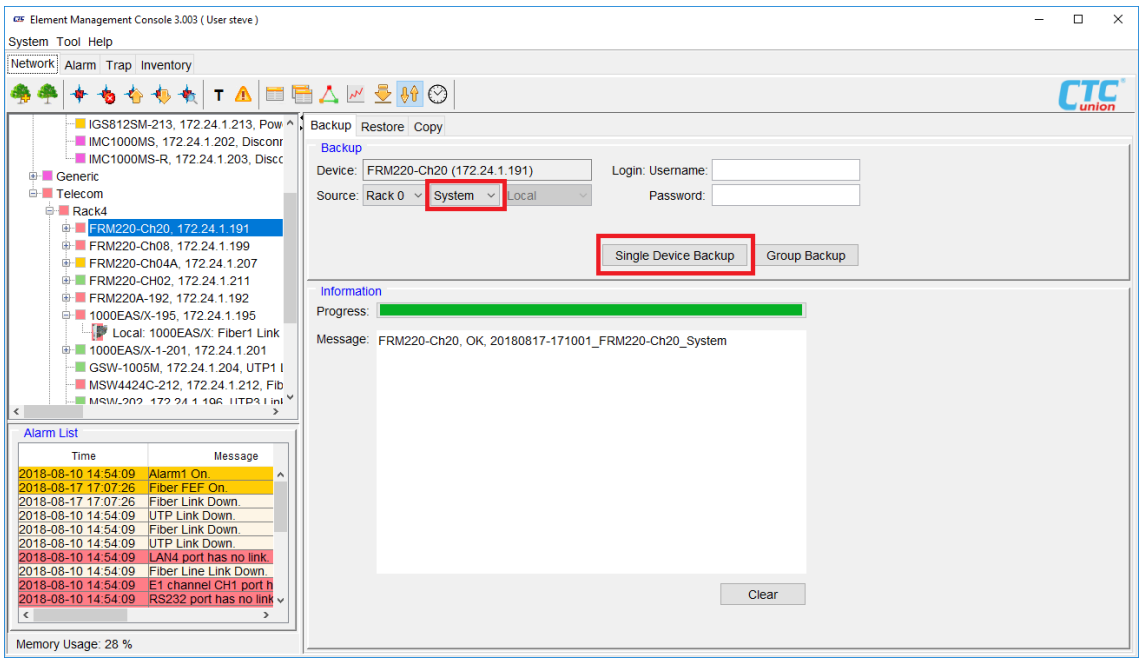


Figure 5-41 Backup FRM220 System

5.7.2 Restore FRM220 System

Click the **Restore** tab and select the Device. Click the **Single Device Restore**. Choose the correct 'system' file and click **Open**.

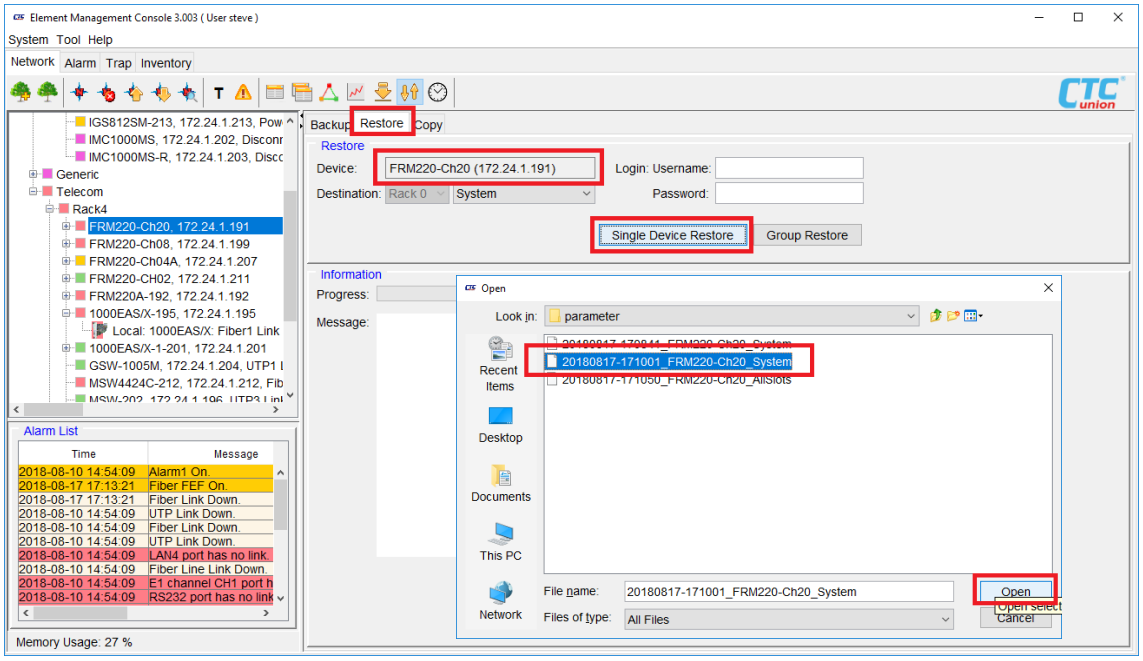


Figure 5-42 Restore FRM220 System

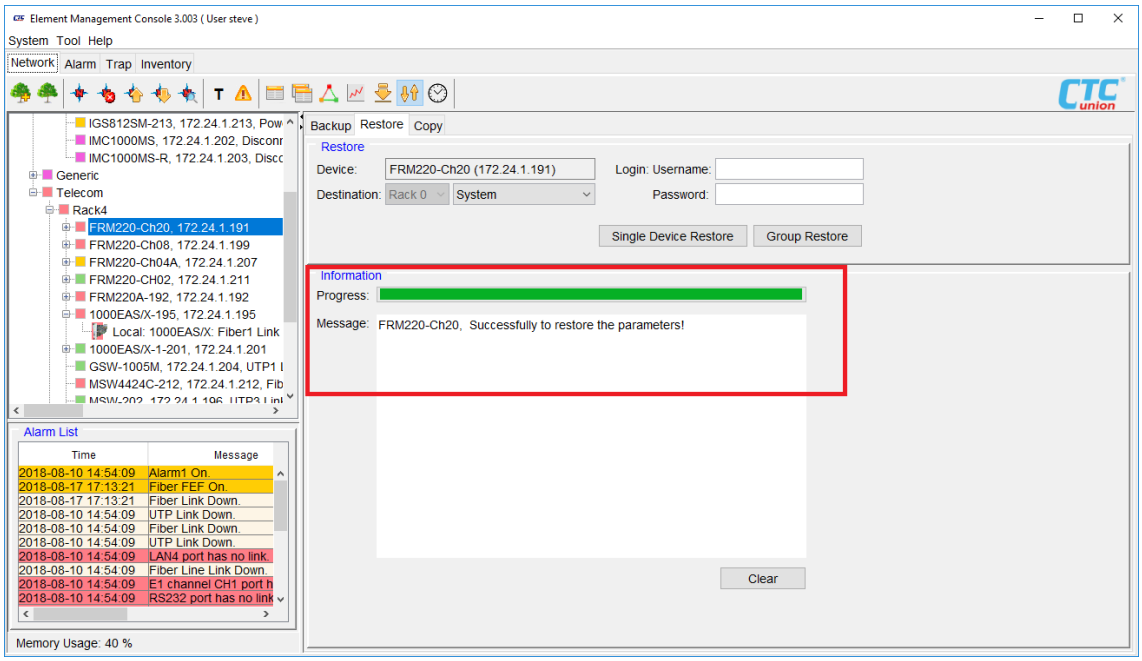


Figure 5-43 Restore Success

5.7.3 Copy Line Card Parameters (clone)

Card cloning is a very useful function when a chassis contains a large number of same type cards and the configurations for the cards are the same.

Step 1. Go to the **Copy** tab.

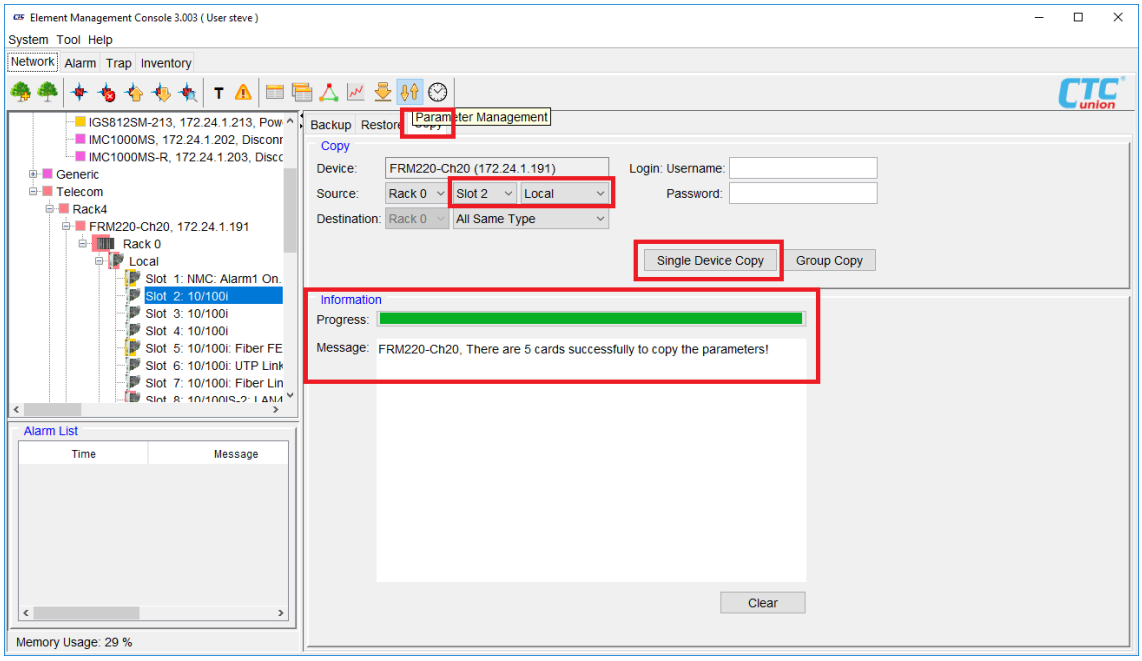


Figure 5-44 Card Copy

Step 2. Select the device, the slot (Slot 2 in example) and the local location for the **source**.
Step 3. Select the **All Same Type** to clone settings to the same type card.
Step 4. Click **Single Device Copy** button.
Results are displayed in the **Information** window.

5.8 NTP Sync

EMS is may configure a list of devices and set the NTP time server IP address for all.

5.8.1 Open NTP Sync window

Select the  icon to open the Sync Window.

5.8.2 Setup IP of NTP Server and Apply.

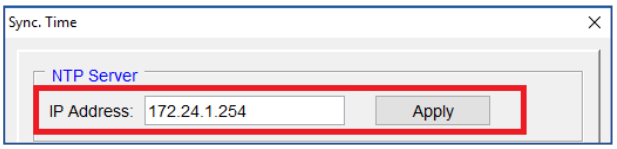


Figure 5-45 Set NTP Server IP

5.8.3 Edit Device's NTP Source

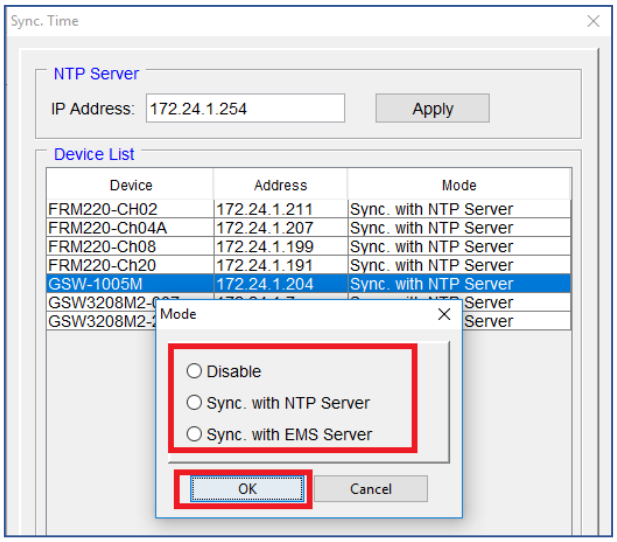


Figure 5-46 Edit and set device NTP Server source

5.8.4 Synchronize with NTP Server

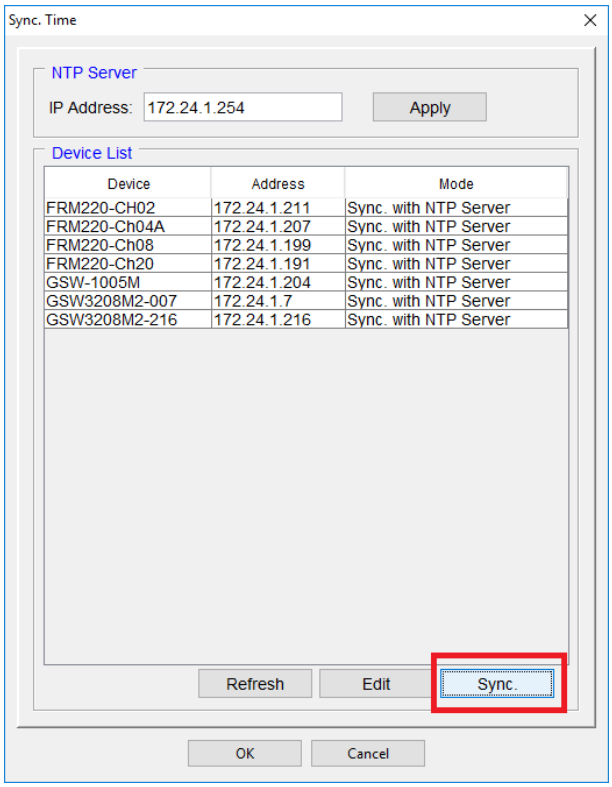


Figure 5-47 Sync devices with NTP Server

5.9 Administration from Client

Starting with EMS version 3.016, the ability to perform most administration tasks which previously could only be performed from the Admin Console on the physical EMS server, are now available to any client user that has been assigned administrator privileges.

5.9.1 Device Administration

NOTE: Only users which have been assigned the 'administrator' role will have access to these administration features in the EMC Client. Discovery, Poller and Polling work exactly as in the Admin Console, so please refer to Chapter 4.

Remote Administration

The graphic below is an example of an Element Manager Client with the administrative features.

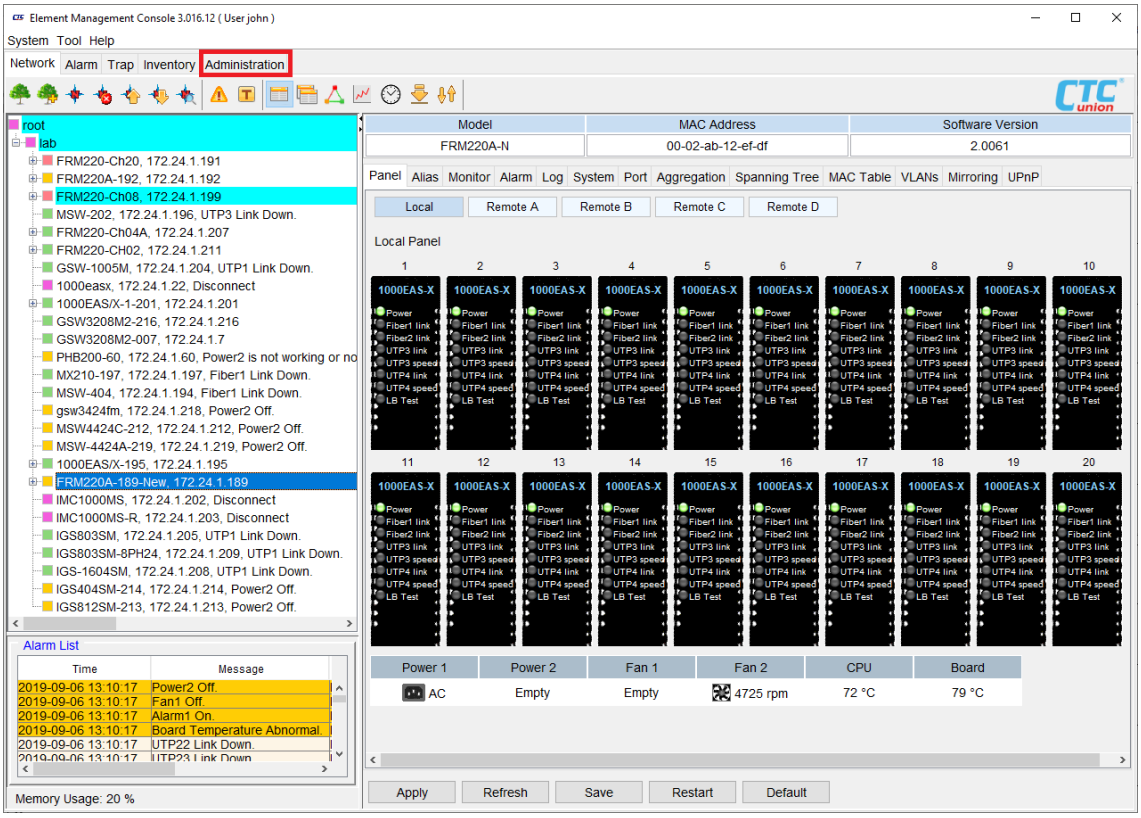


Figure 5-48. Element Manager Console Remote Client Screen

In the above graphic, the SmartView user 'john' has been assigned the administrator role and now has an extra "Administration" menu.

After clicking on the 'Administration' tab, the window will reveal 7 sub-menus, Device, Discovery, Polling, Poller, User, Role and Security.

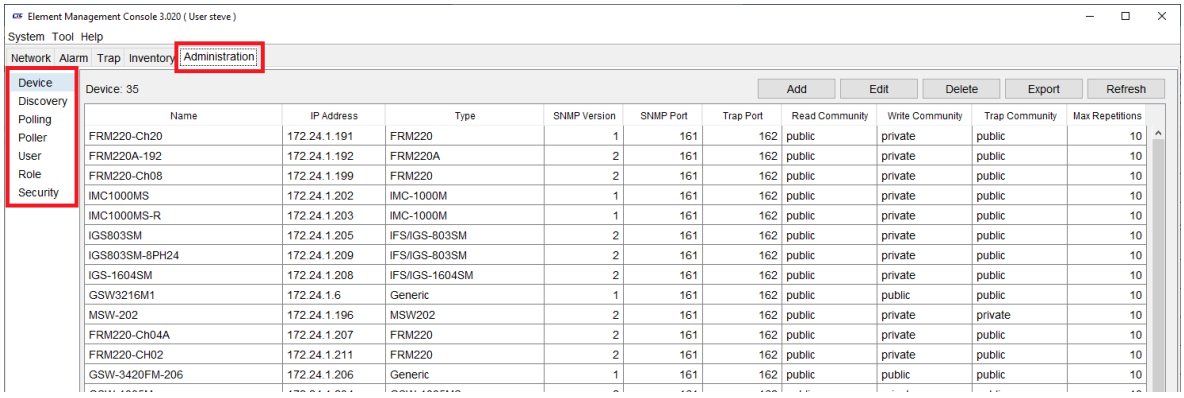


Figure 5-49. Administration Panel

The device functions will list all the current devices, device 'alias' names, IP address, model name, SNMP version, SNMP & SNMP trap ports, community string names, etc. A single device can be edited by highlighting and clicking the "Edit" button. Multiple devices may also be selected by mouse dragging so that common settings can be applied to multiple devices at the same time. Devices may be manually added, deleted and the device database can be exported to text, CSV or html.

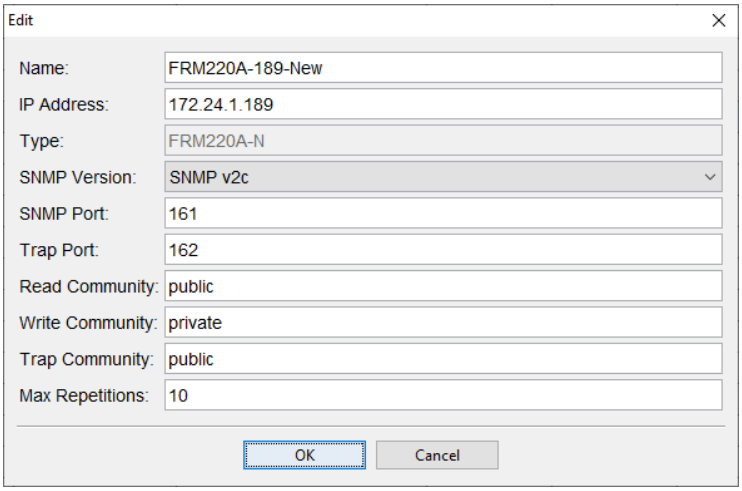


Figure 5-50. Single Device Edit

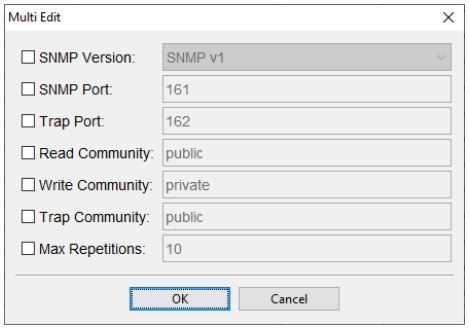
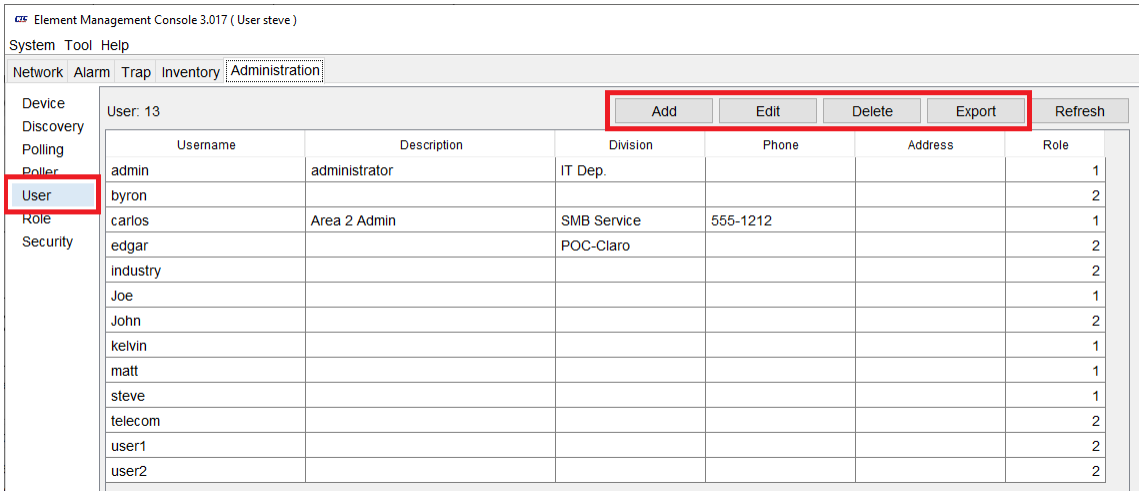


Figure 5-51. Multiple Devices

5.9.2 User

Clicking on the "User" menu item will display the User Panel.



Fiber 5-52. User Panel

Four functions are available: "Add" a new user to the system; "Edit" an existing user; "Delete" a user from the system permanently (cannot be undone); "Export" the user database to text, CSV or html.

Add User

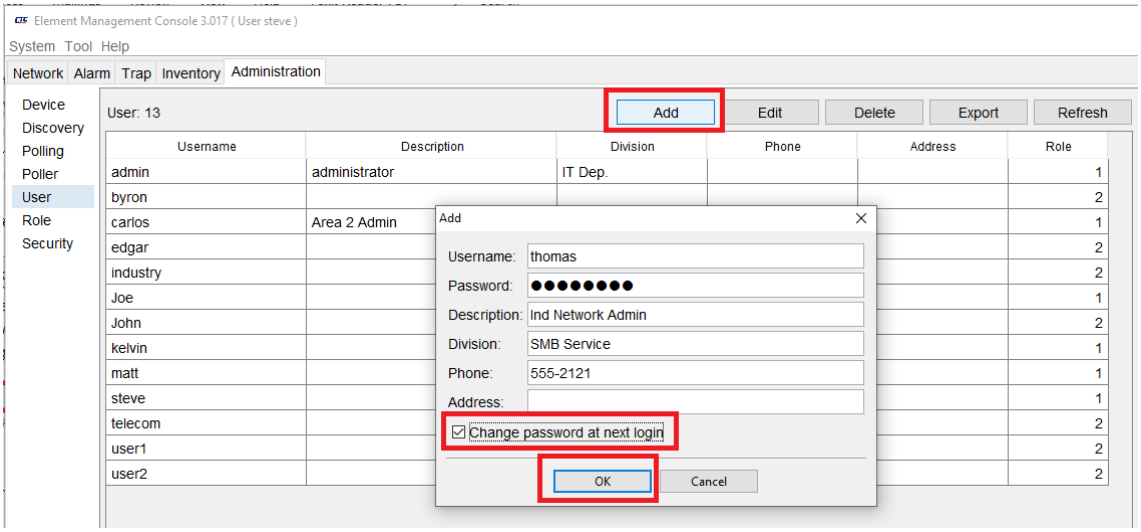


Figure 5-53 Adding Users

A new user can be added to the system by clicking the "Add" button. For this new user, the check box has been selected to force this user to change a new password when they login.

Edit User

To edit an existing user, select the user and click the "Edit" button.

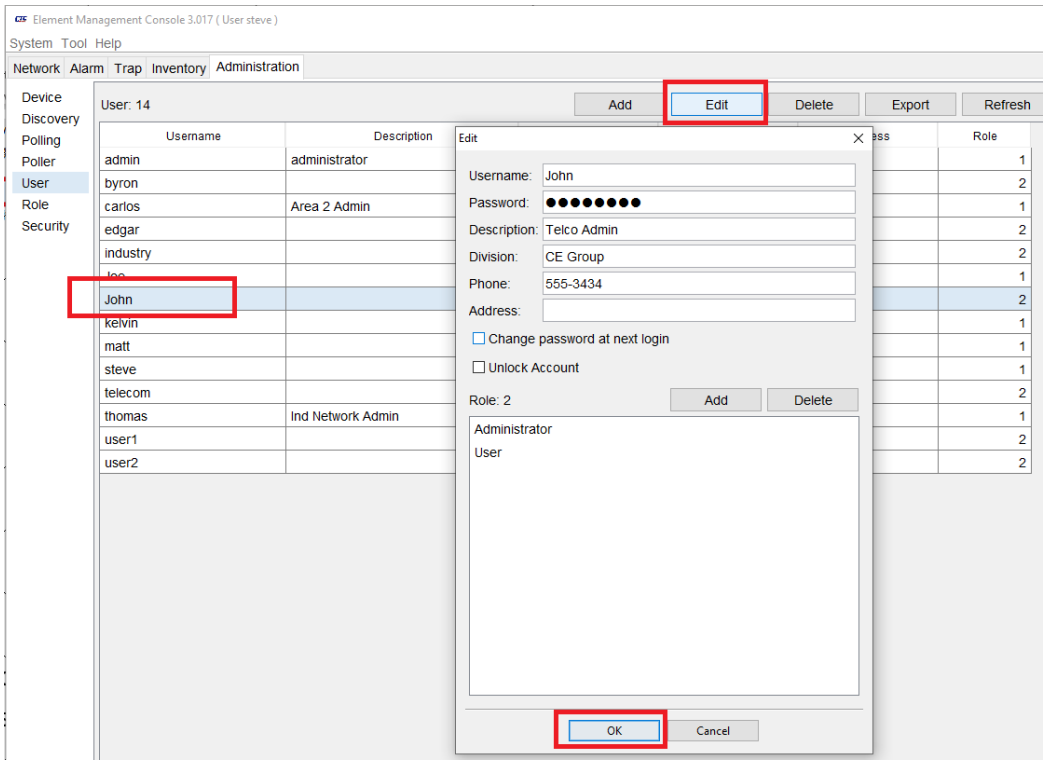


Figure 5-54. Edit User

Administrator can Edit user, change forgotten password, force password change at next login, unlock a locked account and assign additional roles to this user.

5.9.3 Roles

Probably the most important function in EMS is the concept of 'roles' and how they are created and assigned to users, devices, groups of users, groups of devices and trees/nodes. Role creation and assignment requires detailed planning of 'who' will be responsible for the different networking and administrative tasks for all or groups of devices under EMS management. Planning and creating definable roles from the start will allow devices and users to be precisely deployed with job functions that provide secure operations.

Planning

Divide devices into logical groups; These could be by region, customer or device types. Create roles for these device groups. This will make delegation of responsibility for device groups easy, once user roles are created. Create user roles, such as super admins, network admins, operators and supervisory users. Then, when creating users, apply their proper role for their level and equipment they are responsible for. A super admin is someone with all power to create new users and roles and do any other actions. A network admin will be able to add devices to the network, to configure and monitor, but cannot create new users or roles. An operator has been assigned equipment to 'operate' and monitor. The operations they can perform are those related to device configurations. A 'monitor' or 'supervisor' is someone who has been given the rights to view device status, to look at traps and see device alarms, but they cannot change configurations.

Planning up front will make device installation and delegation of management much easier during both deployment stages and operational phase.

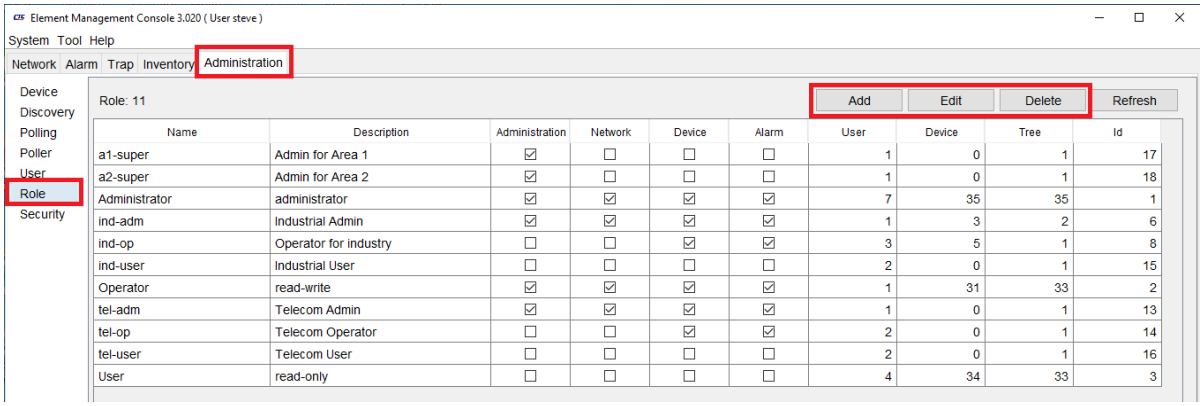


Figure 5-55. Roles

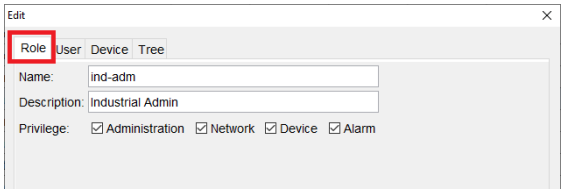


Figure 5-56 Define Role

Figure 5-57 Define User

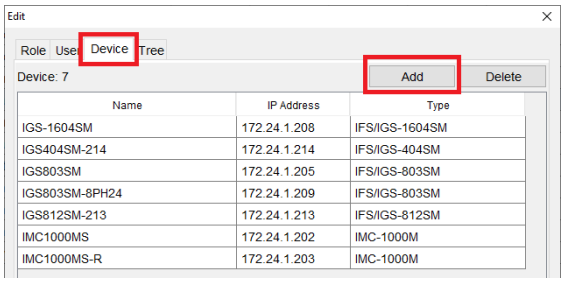


Figure 5-58 Define Devices

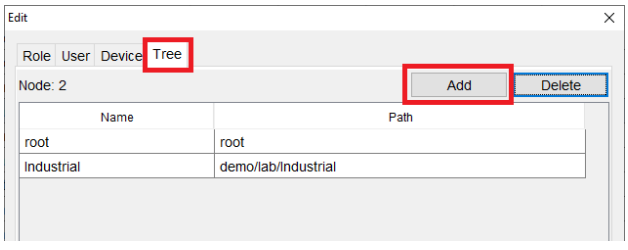


Figure 5-59 Define Tree

We've created the role of admin for Industrial Grade products, then we have added a user 'thomas' to this role, next we add all the devices that will be managed under this role. Lastly we select a tree that has been designed specifically for this role. Now the user 'thomas' can only administer the group of devices assigned to him.

5.9.4 Security

New security features have been added for user logins. They will be highlighted below.

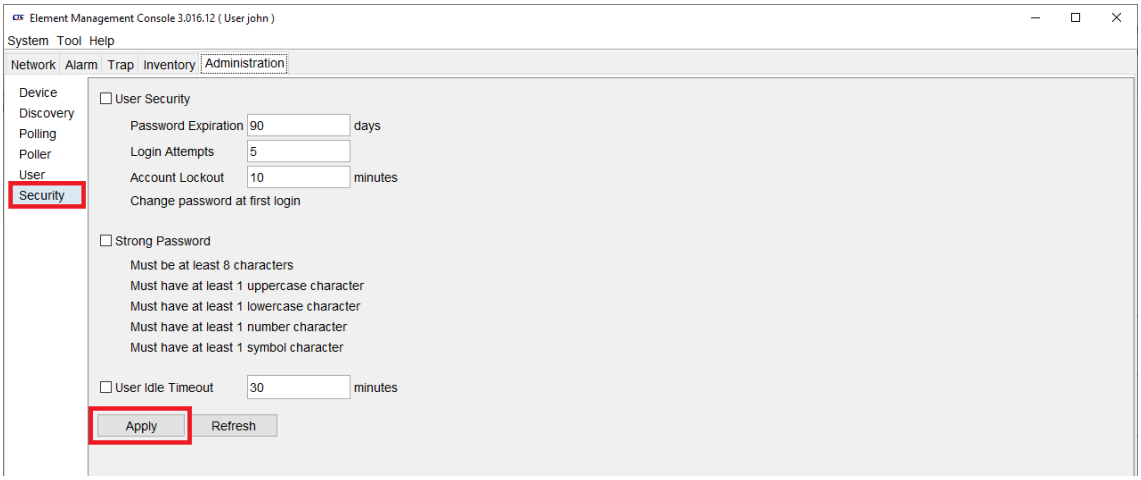


Figure 5-60. Security

User Security

To enable "User Security", click the check box. Adjust the parameters for "Password Expiration" in days. In the example above, 90 days after applying this function, all users will be forced to reset their password.

When the number of login attempts is reached, the user will be locked out. In the above example, the count is 5. On the fifth try, if the password is still not correctly entered, the account will be locked by the system.

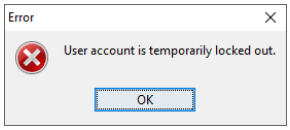


Figure 5-61. Account Locked

The "Account Lockout" setting programs the number of minutes an account will remain locked after being locked due to exceeding the number of login attempts. This will help deter brute force login attempts.

Strong Password

By checking this check box, any new users or users forced to change their password, MUST follow the new password rules. Those rules are listed and are the same as the default password rules for a user on a Microsoft Server. Failure to follow the password rules will result in the following pop-up.

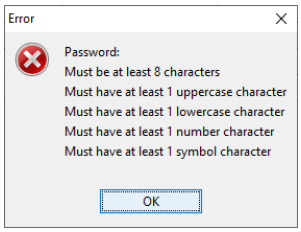


Figure 5-62. Password Rule Warning

User Idle Timeout

By enabling this check box and setting a timeout in minutes, user will automatically be logged out of the EMS client if their computer is idle (no key strokes, no mouse movement) for the entered number of minutes. The timeout depends on the user's activity on the client's computer. If the timeout is set to 5 minutes and the computer is left idle for 5 minutes, the EMS client will automatically log out. Enabling this setting will affect ALL EMS client users.

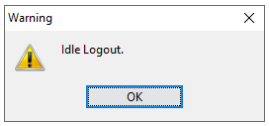


Figure 5-63. Idle logout Pop-up

Note: This function has been removed from the EMS Server's Options and is now only available under EMC.

Example Setting

The graphic below is a typical setting example that will provide for Password Renewal every 90 days, up to 5 failed login attempts before account locking, locking timeout of 10 minutes, forced secure passwords and an user idle timeout of 5 minutes. Press the "Apply" button after editing this screen.

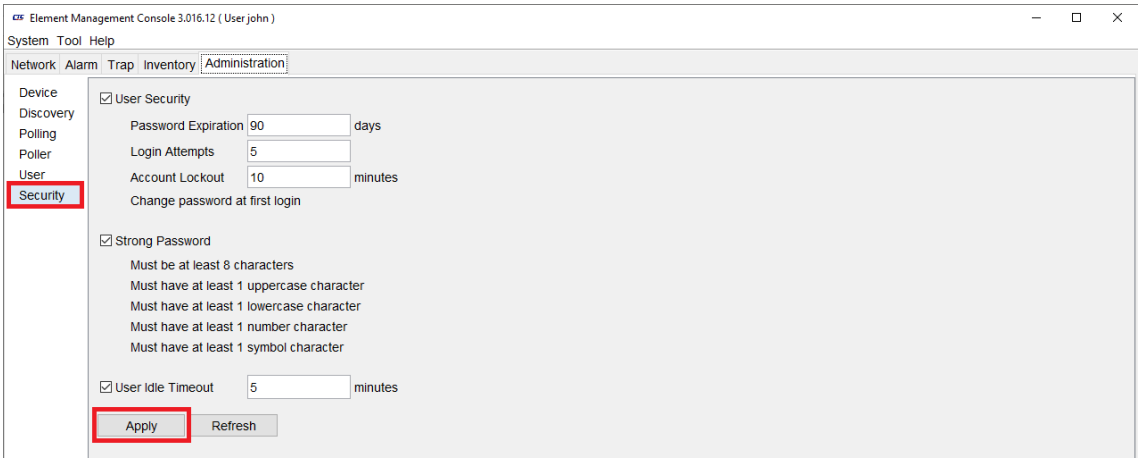


Figure 5-64. Security Example

Chapter 6 Using the Topology Feature

6.1 Introduction

The Topology feature of the EMS allows graphic maps to be loaded into the operation template. From here, network devices may be dragged and dropped onto the map, indicating the physical locations of the ND.

The topology mapping feature is hierographic in nature. When the nodes attached to the root tree are well thought out and executed, each intermediate node will be able to have a map assigned to it.

Map images are imported from Graphics Interchange Format (gif), Joint Photographic Experts Group (jpg) or Portable Network Graphics (png) files and may be actual map files created from Google Maps, architectural drawings or physical representations of floor layouts or rack space. Files imported are stored in the database and will be available to every EMS user.

6.2 Operation

6.2.1 Topology View

Highlight the root (or whatever name has been given) node, then click the **Topology View** icon.

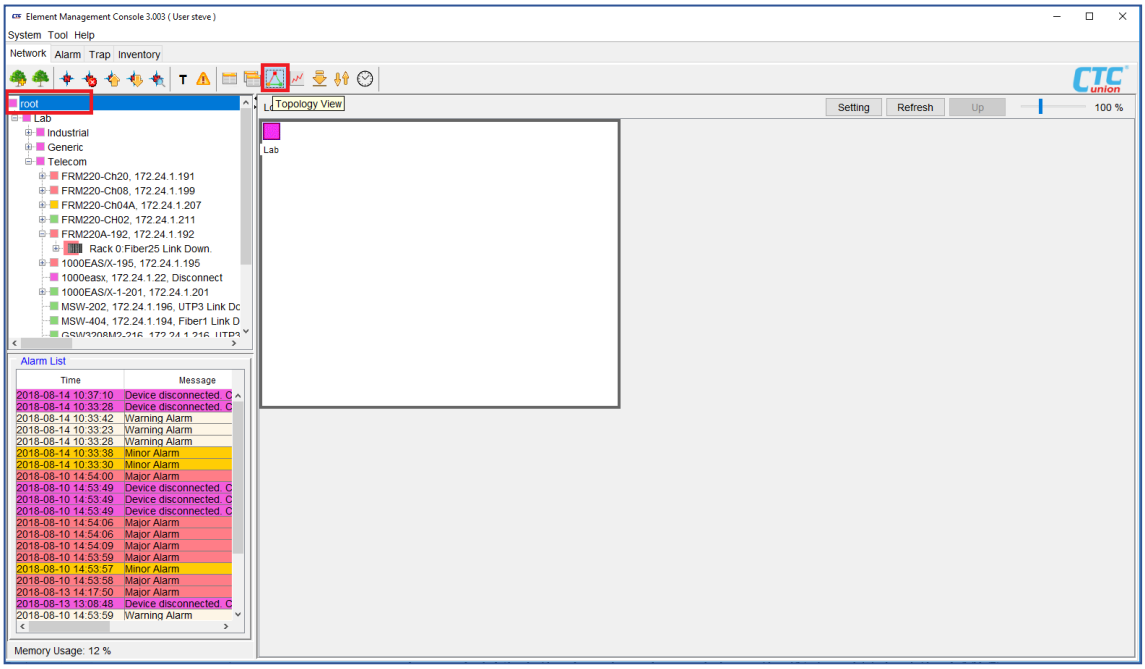


Figure 6-1 Click the **Topology** Icon while highlighting the root of the EMC

6.2.2 Maps

Place the cursor within the **map window** and **Right-Click**. From the pull-down menu, select **Map**.

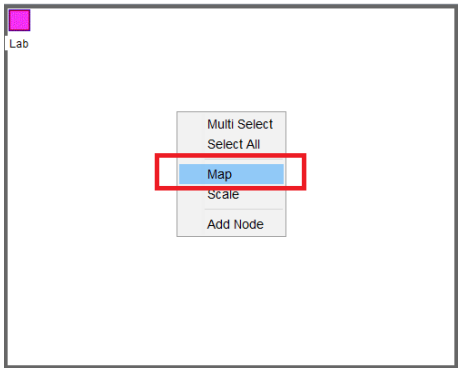


Figure 6-2 Map Window Menu

Select radio button

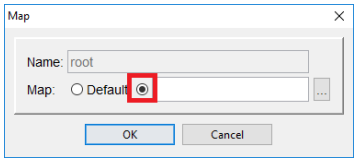


Figure 6-3 Map

6.2.3 Adding Maps to Database

On a freshly installed system, there will be no maps in the database. In the example here, there are already 18 maps that have been added in the database and are available to all users. To add additional map files, click the **Add** button.

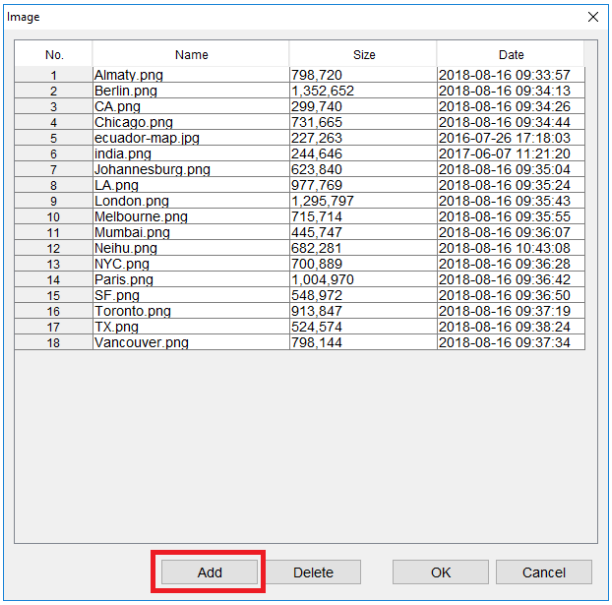


Figure 6-4 Adding Map Files

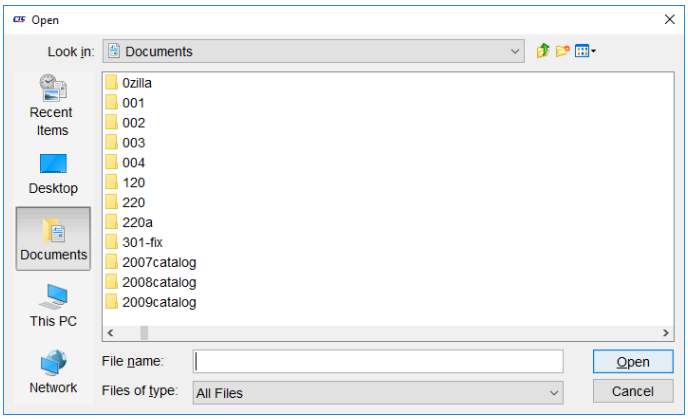


Figure 6-5 Browsing Window

Browse to find the graphic file and then click **Open**. The image will be imported into the database.

6.2.4 Adding a Map to Topology View

Right-Click in the **Topology View** window.

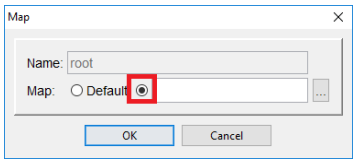


Figure 6-6 Map

Click the radio button to open the **Image** list

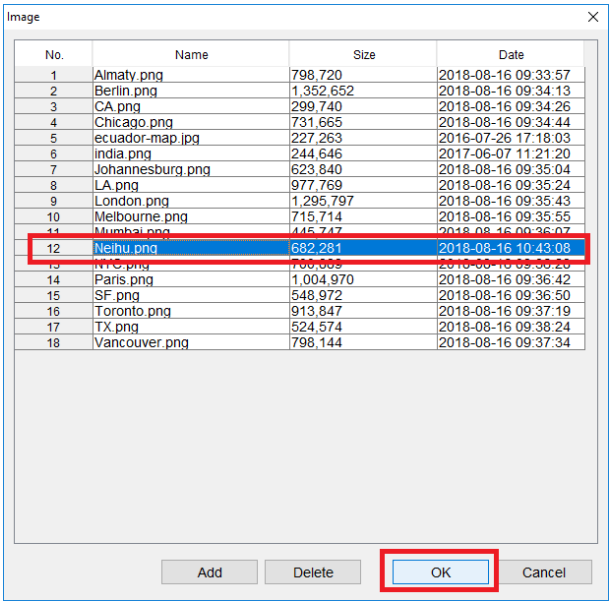


Figure 6-7 Add an image to Topology View

6.2.5 Drag and Drop Node Icons

Drag and drop the **node icon** to the desired location on the map or image.

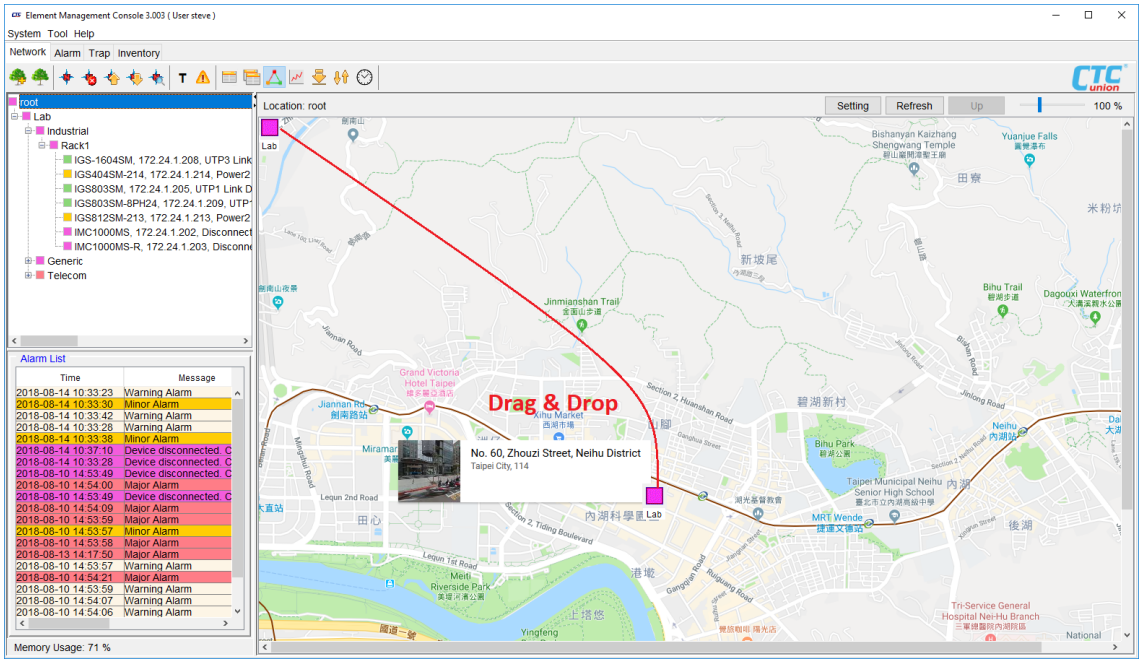


Figure 6-8 Drag & Drop Node Icon(s)

6.2.6 Drag and Drop Agents

For the Rack1 node, a Map image has already been imported and selected for this node. All the agent devices under this node will be 'stacked' in the upper-left hand corner. Drag and drop each device individually and place them in their proper location.

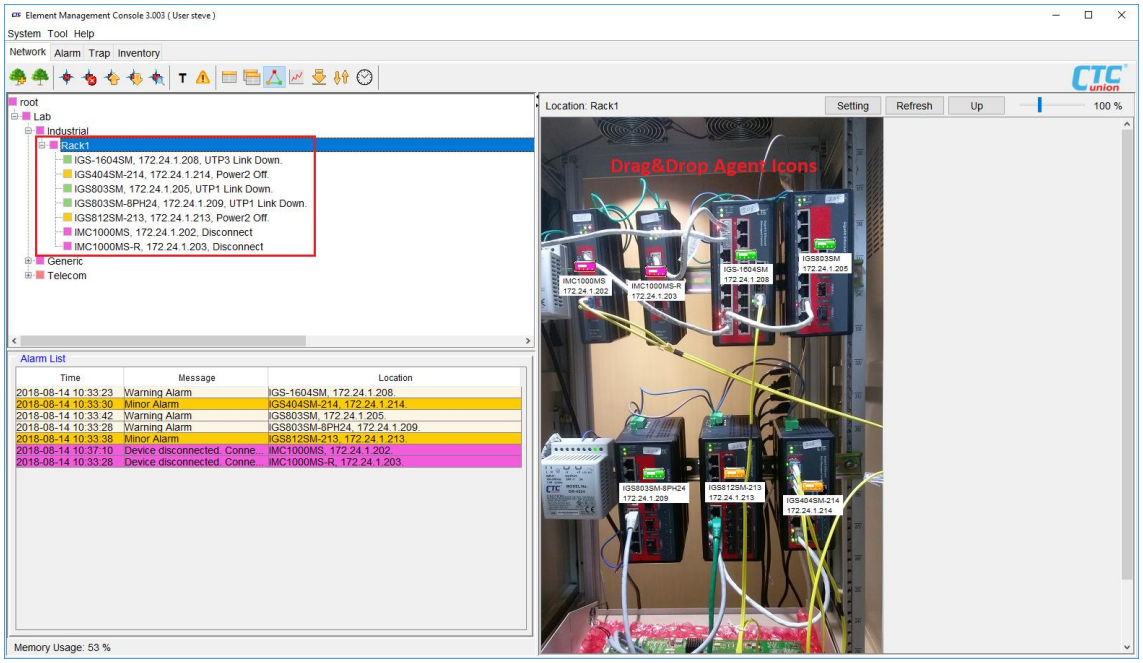


Figure 6-9 Drag & Drop Agent Icon(s)

6.2.7 Troubleshooting Alarms

If any Agent experiences an **alarm condition**, the agent's icon color will change from "Green" to "Yellow" or "Red". Yellow indicates a **minor alarm** while Red indicates a **major alarm**. Click on one of the device icons. It will then have a green background color, and the device will be highlighted in the EMC tree with the alarm condition (Device disconnected in this example) will be listed in the **Alarm List**. Use the mouse and Right-click the device node in the tree list. The pull-down menu will appear as below. Ping is one of the tools available to help troubleshoot device problems. It is also possible to directly access the device by Telnet or HTTP.

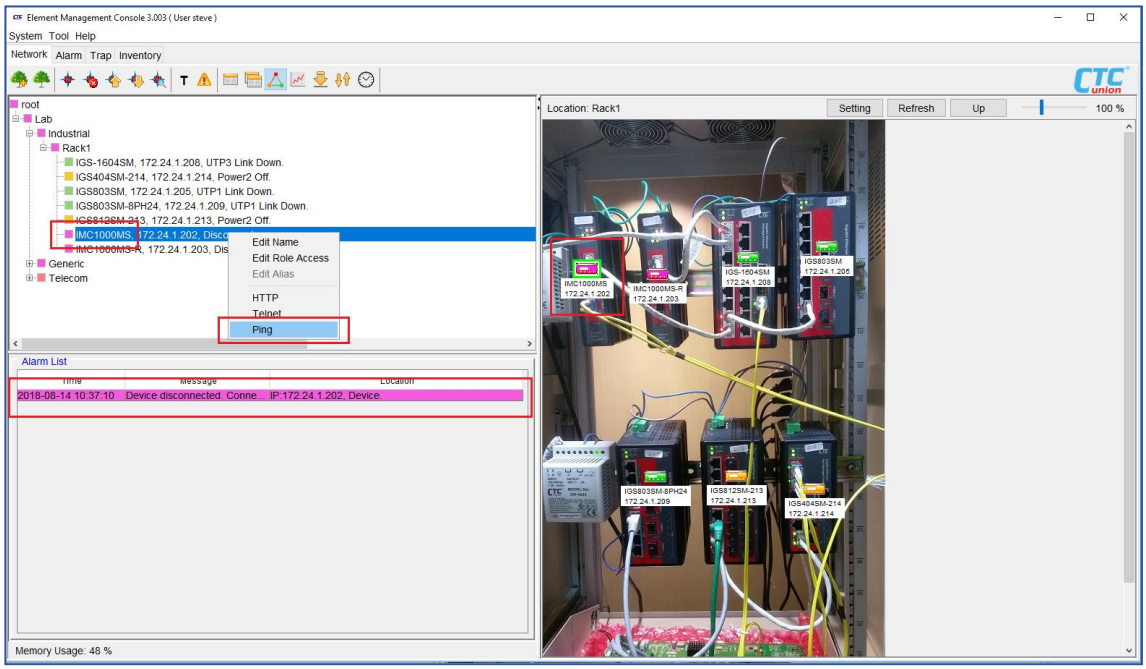


Figure 6-10 Handling Alarms

Click **Ping**

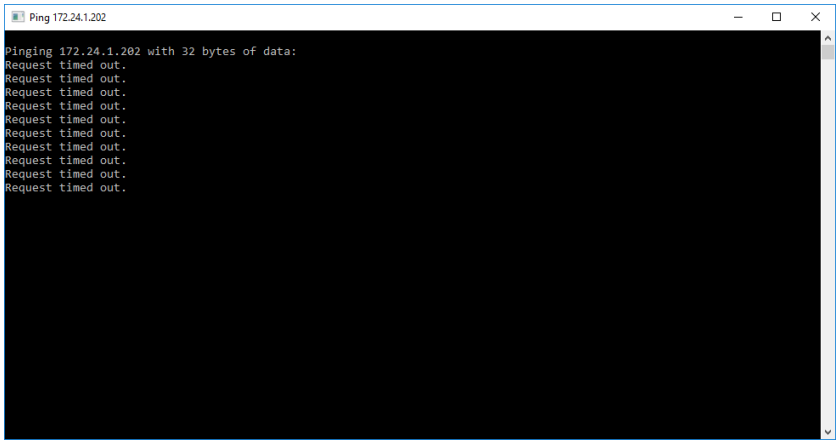


Figure 6-11 Ping indicates device cannot be reached

Troubleshoot another device with alarm.

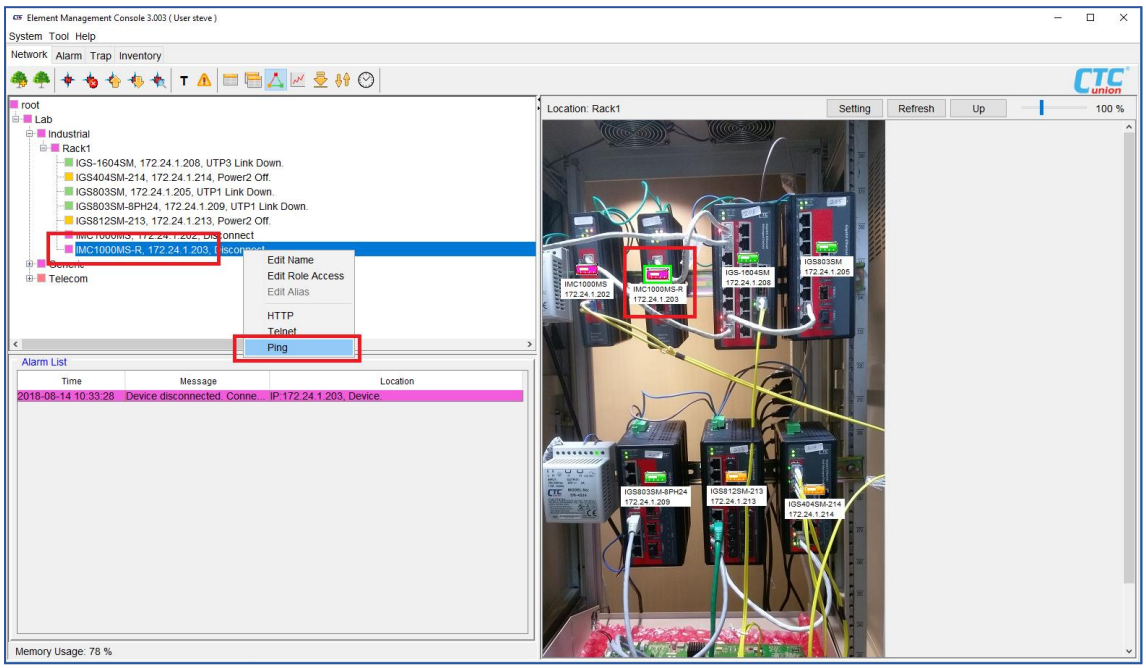


Figure 6-12 Checking another device with alarm

Click **Ping**

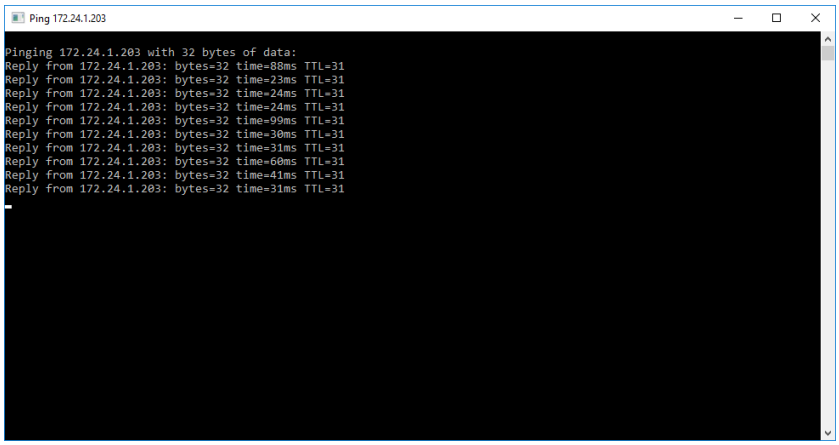


Figure 6-12 Device can ping but is disconnected from EMS (SNMP problem)

6.2.8 Connect with HTTP

Troubleshooting can be done in the main EMC console or directly in the agent by HTTP or Telnet. The following is an example of using HTTP, connecting to the Agent and observing and correcting the alarm condition.

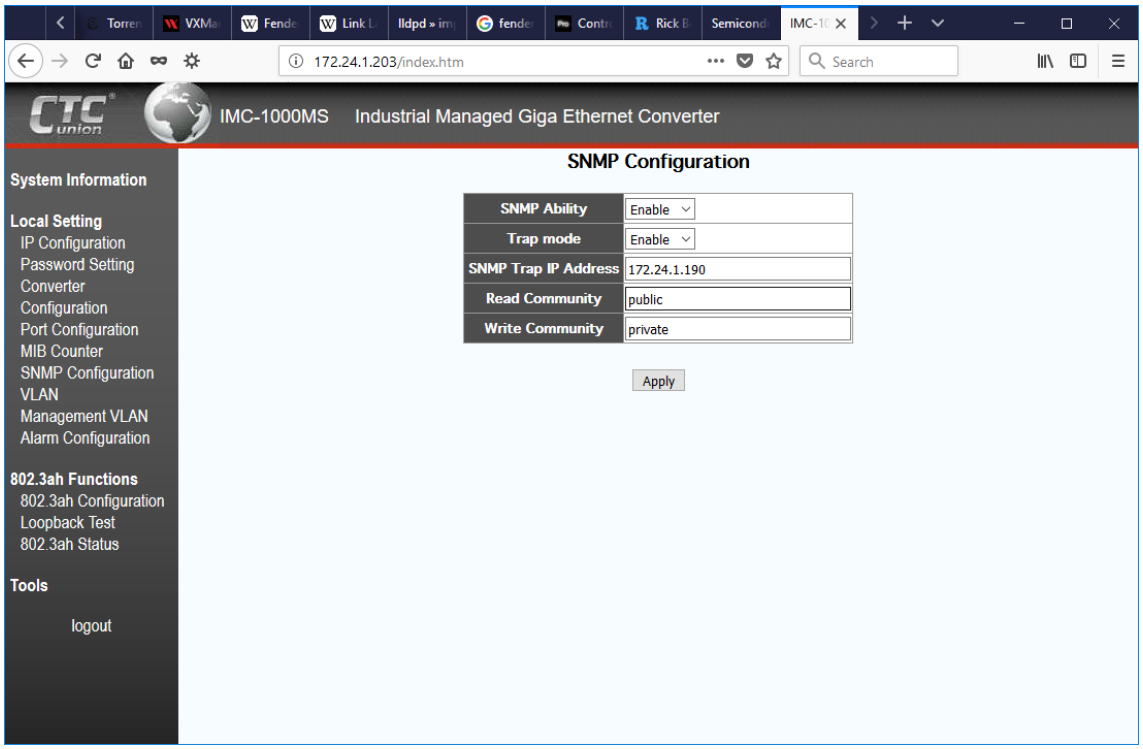


Figure 6-13 Via HTTP, setup the device's SNMP

Chapter 7 Using the Inventory Feature

7.1 Introduction

The inventory management feature integrated into SmartView EMS is a new feature being introduced in version 2.54 specifically for the FRM220/FRM220A series platform. Currently there are only a small number of newer line cards which support reading a factory programmed serial number specific for each line card. Additionally, the cards are only programmed with serial number upon request.

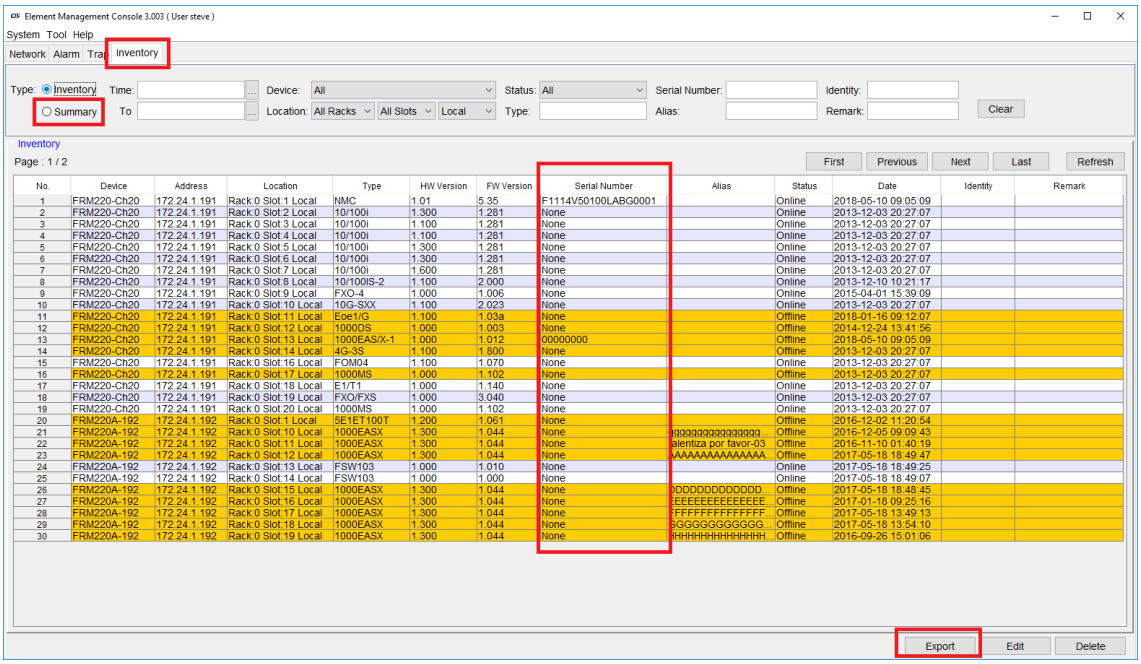


Figure 7-1 Inventory Panel

The above screen capture shows the preliminary functions of the inventory feature. This tool has search and sorting functions as well as the ability to export results in CSV for further manipulation in MS Excel.

When searching, the 'Time' parameter indicates when the type of equipment was first recognized as being in the managed system. From this point, the equipment type will be either 'On Line' or 'Disabled'. Disabled means the system is not able to find the equipment because it has been removed.

Other search criteria include selecting device types, rack numbers, slot numbers, local or remote devices as well as user keyed in Alias, Identity and remarks.

Each device can have user configured 'Identity' and 'Remark' attributes that will become locked to this type's serial number. (Serial numbers are factory set during manufacturing.) A common usage of the 'Identity' field could be to place your 'asset number' used for your own internal inventory tracking. The 'Remark' field could include purchase details such a PO, date of purchase, warrantee status, card location or connected client information. Just be aware that if the card is moved to a different slot or different chassis, these remarks will 'follow the physical card'.

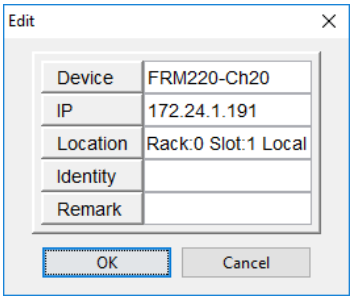


Figure 7-2 Edit

7.2 Export

The inventory collected by SmartView EMS can be exported in a number of common, usable formats. The exported files are found in the 'report' folder, inside the EMS installed folder.

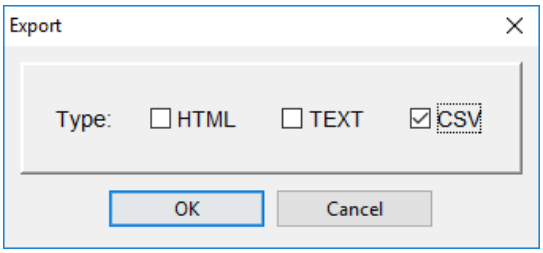
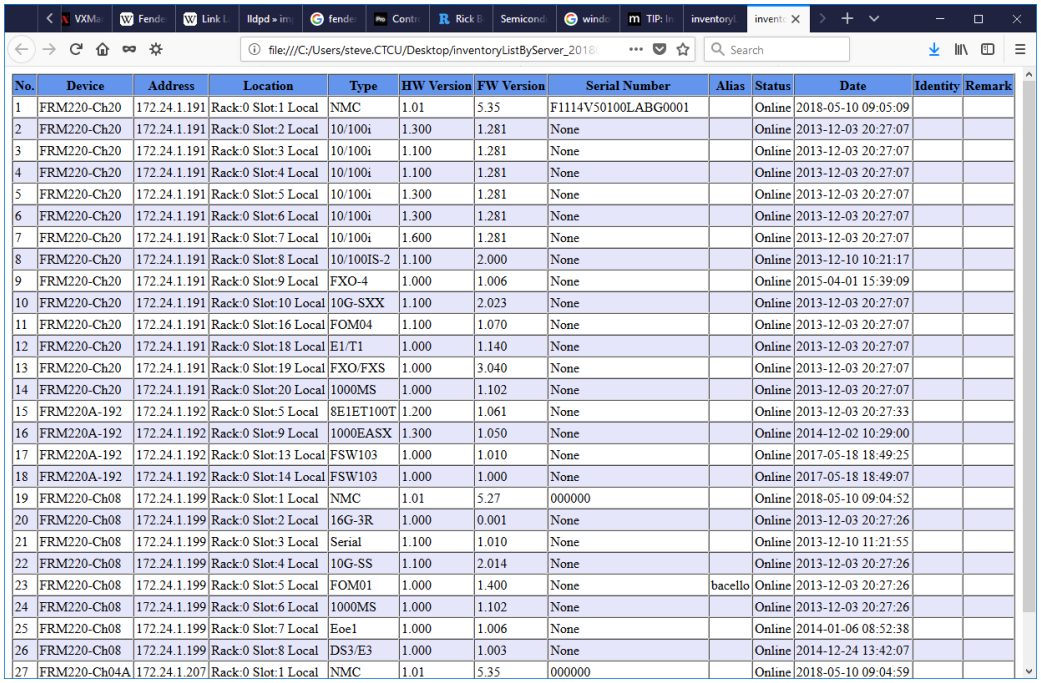


Figure 7-3 Export Inventory

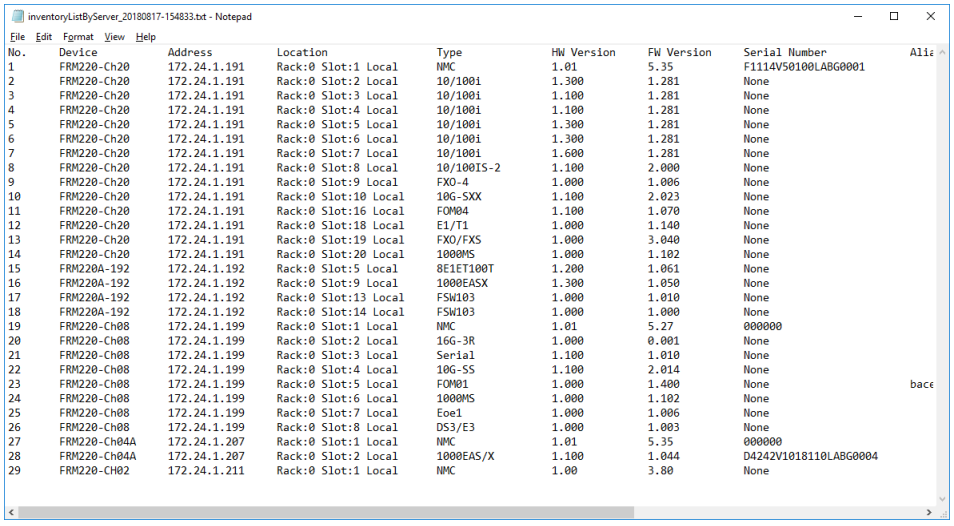
HTML (Hyper Text Markup Language) can be viewed across many different platforms (Windows, Linux, Unix, OSX, iOS, or Android) by using a web browser.



No.	Device	Address	Location	Type	HW Version	FW Version	Serial Number	Alias	Status	Date	Identity	Remark
1	FRM220-Ch20	172.24.1.191	Rack:0 Slot:1 Local	NMC	1.01	5.35	F1114V50100LABG0001		Online	2018-05-10 09:05:09		
2	FRM220-Ch20	172.24.1.191	Rack:0 Slot:2 Local	10/100i	1.300	1.281	None		Online	2013-12-03 20:27:07		
3	FRM220-Ch20	172.24.1.191	Rack:0 Slot:3 Local	10/100i	1.100	1.281	None		Online	2013-12-03 20:27:07		
4	FRM220-Ch20	172.24.1.191	Rack:0 Slot:4 Local	10/100i	1.100	1.281	None		Online	2013-12-03 20:27:07		
5	FRM220-Ch20	172.24.1.191	Rack:0 Slot:5 Local	10/100i	1.300	1.281	None		Online	2013-12-03 20:27:07		
6	FRM220-Ch20	172.24.1.191	Rack:0 Slot:6 Local	10/100i	1.300	1.281	None		Online	2013-12-03 20:27:07		
7	FRM220-Ch20	172.24.1.191	Rack:0 Slot:7 Local	10/100i	1.600	1.281	None		Online	2013-12-03 20:27:07		
8	FRM220-Ch20	172.24.1.191	Rack:0 Slot:8 Local	10/100IS-2	1.100	2.000	None		Online	2013-12-10 10:21:17		
9	FRM220-Ch20	172.24.1.191	Rack:0 Slot:9 Local	FXO-4	1.000	1.006	None		Online	2015-04-01 15:39:09		
10	FRM220-Ch20	172.24.1.191	Rack:0 Slot:10 Local	10G-SXX	1.100	2.023	None		Online	2013-12-03 20:27:07		
11	FRM220-Ch20	172.24.1.191	Rack:0 Slot:16 Local	FOM04	1.100	1.070	None		Online	2013-12-03 20:27:07		
12	FRM220-Ch20	172.24.1.191	Rack:0 Slot:18 Local	E1/T1	1.000	1.140	None		Online	2013-12-03 20:27:07		
13	FRM220-Ch20	172.24.1.191	Rack:0 Slot:19 Local	FXO/FXS	1.000	3.040	None		Online	2013-12-03 20:27:07		
14	FRM220-Ch20	172.24.1.191	Rack:0 Slot:20 Local	1000MS	1.000	1.102	None		Online	2013-12-03 20:27:07		
15	FRM220A-192	172.24.1.192	Rack:0 Slot:5 Local	8E1ET100T	1.200	1.061	None		Online	2013-12-03 20:27:33		
16	FRM220A-192	172.24.1.192	Rack:0 Slot:9 Local	1000EASX	1.300	1.050	None		Online	2014-12-02 10:29:00		
17	FRM220A-192	172.24.1.192	Rack:0 Slot:13 Local	FSW103	1.000	1.010	None		Online	2017-05-18 18:49:25		
18	FRM220A-192	172.24.1.192	Rack:0 Slot:14 Local	FSW103	1.000	1.000	None		Online	2017-05-18 18:49:07		
19	FRM220-Ch08	172.24.1.199	Rack:0 Slot:1 Local	NMC	1.01	5.27	000000		Online	2018-05-10 09:04:52		
20	FRM220-Ch08	172.24.1.199	Rack:0 Slot:2 Local	16G-3R	1.000	0.001	None		Online	2013-12-03 20:27:26		
21	FRM220-Ch08	172.24.1.199	Rack:0 Slot:3 Local	Serial	1.100	1.010	None		Online	2013-12-10 11:21:55		
22	FRM220-Ch08	172.24.1.199	Rack:0 Slot:4 Local	10G-SS	1.100	2.014	None		Online	2013-12-03 20:27:26		
23	FRM220-Ch08	172.24.1.199	Rack:0 Slot:5 Local	FOM01	1.000	1.400	None	bacello	Online	2013-12-03 20:27:26		
24	FRM220-Ch08	172.24.1.199	Rack:0 Slot:6 Local	1000MS	1.000	1.102	None		Online	2013-12-03 20:27:26		
25	FRM220-Ch08	172.24.1.199	Rack:0 Slot:7 Local	Eoe1	1.000	1.006	None		Online	2014-01-06 08:52:38		
26	FRM220-Ch08	172.24.1.199	Rack:0 Slot:8 Local	DS3/E3	1.000	1.003	None		Online	2014-12-24 13:42:07		
27	FRM220-Ch04A	172.24.1.207	Rack:0 Slot:1 Local	NMC	1.01	5.35	000000		Online	2018-05-10 09:04:59		

Figure 7-4 Exported Inventory, viewed in Firefox

Text exports can be viewed in any text viewers.



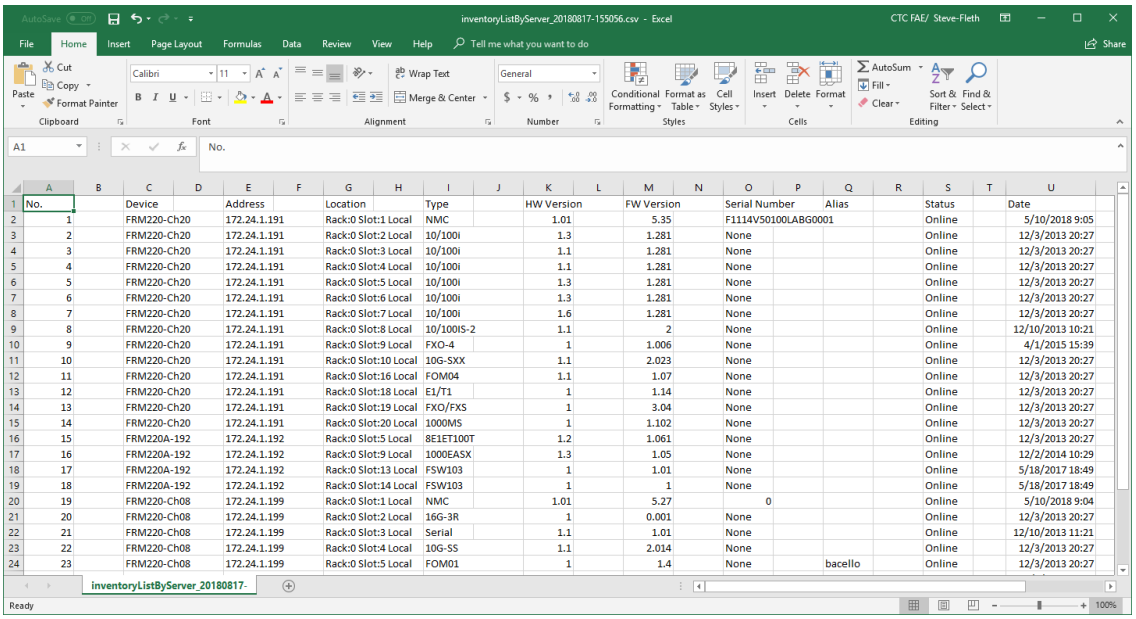
inventoryListByServer_20180817-154833.txt - Notepad

File Edit Format View Help

No.	Device	Address	Location	Type	HW Version	FW Version	Serial Number	Alia
1	FRM220-Ch20	172.24.1.191	Rack:0 Slot:1 Local	NMC	1.01	5.35	F1114V50100LABG0001	
2	FRM220-Ch20	172.24.1.191	Rack:0 Slot:2 Local	10/100i	1.300	1.281	None	
3	FRM220-Ch20	172.24.1.191	Rack:0 Slot:3 Local	10/100i	1.100	1.281	None	
4	FRM220-Ch20	172.24.1.191	Rack:0 Slot:4 Local	10/100i	1.100	1.281	None	
5	FRM220-Ch20	172.24.1.191	Rack:0 Slot:5 Local	10/100i	1.300	1.281	None	
6	FRM220-Ch20	172.24.1.191	Rack:0 Slot:6 Local	10/100i	1.300	1.281	None	
7	FRM220-Ch20	172.24.1.191	Rack:0 Slot:7 Local	10/100i	1.600	1.281	None	
8	FRM220-Ch20	172.24.1.191	Rack:0 Slot:8 Local	10/100IS-2	1.100	2.000	None	
9	FRM220-Ch20	172.24.1.191	Rack:0 Slot:9 Local	FXO-4	1.000	1.006	None	
10	FRM220-Ch20	172.24.1.191	Rack:0 Slot:10 Local	10G-SXX	1.100	2.023	None	
11	FRM220-Ch20	172.24.1.191	Rack:0 Slot:16 Local	FOM04	1.100	1.070	None	
12	FRM220-Ch20	172.24.1.191	Rack:0 Slot:18 Local	E1/T1	1.000	1.140	None	
13	FRM220-Ch20	172.24.1.191	Rack:0 Slot:19 Local	FXO/FXS	1.000	3.040	None	
14	FRM220-Ch20	172.24.1.191	Rack:0 Slot:20 Local	1000MS	1.000	1.102	None	
15	FRM220A-192	172.24.1.192	Rack:0 Slot:5 Local	8E1ET100T	1.200	1.061	None	
16	FRM220A-192	172.24.1.192	Rack:0 Slot:9 Local	1000EASX	1.300	1.050	None	
17	FRM220A-192	172.24.1.192	Rack:0 Slot:13 Local	FSW103	1.000	1.010	None	
18	FRM220A-192	172.24.1.192	Rack:0 Slot:14 Local	FSW103	1.000	1.000	None	
19	FRM220-Ch08	172.24.1.199	Rack:0 Slot:1 Local	NMC	1.01	5.27	000000	
20	FRM220-Ch08	172.24.1.199	Rack:0 Slot:2 Local	16G-3R	1.000	0.001	None	
21	FRM220-Ch08	172.24.1.199	Rack:0 Slot:3 Local	Serial	1.100	1.010	None	
22	FRM220-Ch08	172.24.1.199	Rack:0 Slot:4 Local	10G-SS	1.100	2.014	None	
23	FRM220-Ch08	172.24.1.199	Rack:0 Slot:5 Local	FOM01	1.000	1.400	None	bace
24	FRM220-Ch08	172.24.1.199	Rack:0 Slot:6 Local	1000MS	1.000	1.102	None	
25	FRM220-Ch08	172.24.1.199	Rack:0 Slot:7 Local	Eoe1	1.000	1.006	None	
26	FRM220-Ch08	172.24.1.199	Rack:0 Slot:8 Local	DS3/E3	1.000	1.003	None	
27	FRM220-Ch04A	172.24.1.207	Rack:0 Slot:1 Local	NMC	1.01	5.35	000000	
28	FRM220-Ch04A	172.24.1.207	Rack:0 Slot:2 Local	1000EAS/X	1.100	1.044	D4242V1018110LABG0004	
29	FRM220-CH02	172.24.1.211	Rack:0 Slot:1 Local	NMC	1.00	3.80	None	

Figure 7-5 Exported Inventory, viewed in Notepad

CSV stands for 'comma separated values'. This type of format can be used directly by MS-Excel and could also be used to create a table in MS-Word. CSV format can also be used as a conversion format between different database platforms. This means it is possible to export the inventory from EMS and use this data to import into Oracle, MySQL or other database platforms.



No.	Device	Address	Location	Type	HW Version	FW Version	Serial Number	Alias	Status	Date
1	FRM220-Ch20	172.24.1.191	Rack:0 Slot:1 Local	NMC	1.01	5.35	F1114V50100LABG0001		Online	5/10/2018 9:05
2	FRM220-Ch20	172.24.1.191	Rack:0 Slot:2 Local	10/100i	1.3	1.281	None		Online	12/3/2013 20:27
3	FRM220-Ch20	172.24.1.191	Rack:0 Slot:3 Local	10/100i	1.1	1.281	None		Online	12/3/2013 20:27
4	FRM220-Ch20	172.24.1.191	Rack:0 Slot:4 Local	10/100i	1.1	1.281	None		Online	12/3/2013 20:27
5	FRM220-Ch20	172.24.1.191	Rack:0 Slot:5 Local	10/100i	1.3	1.281	None		Online	12/3/2013 20:27
6	FRM220-Ch20	172.24.1.191	Rack:0 Slot:6 Local	10/100i	1.3	1.281	None		Online	12/3/2013 20:27
7	FRM220-Ch20	172.24.1.191	Rack:0 Slot:7 Local	10/100i	1.6	1.281	None		Online	12/3/2013 20:27
8	FRM220-Ch20	172.24.1.191	Rack:0 Slot:8 Local	10/100IS-2	1.1	2	None		Online	12/10/2013 10:21
9	FRM220-Ch20	172.24.1.191	Rack:0 Slot:9 Local	FXO-4	1	1.006	None		Online	4/1/2015 15:39
10	FRM220-Ch20	172.24.1.191	Rack:0 Slot:10 Local	10G-SXX	1.1	2.023	None		Online	12/3/2013 20:27
11	FRM220-Ch20	172.24.1.191	Rack:0 Slot:16 Local	FOM04	1.1	1.07	None		Online	12/3/2013 20:27
12	FRM220-Ch20	172.24.1.191	Rack:0 Slot:18 Local	E1/T1	1	1.14	None		Online	12/3/2013 20:27
13	FRM220-Ch20	172.24.1.191	Rack:0 Slot:19 Local	FXO/FXS	1	3.04	None		Online	12/3/2013 20:27
14	FRM220-Ch20	172.24.1.191	Rack:0 Slot:20 Local	1000MS	1	1.102	None		Online	12/3/2013 20:27
15	FRM220A-192	172.24.1.192	Rack:0 Slot:5 Local	8E1ET100T	1.2	1.061	None		Online	12/3/2013 20:27
16	FRM220A-192	172.24.1.192	Rack:0 Slot:9 Local	1000EASX	1.3	1.05	None		Online	12/2/2014 10:29
17	FRM220A-192	172.24.1.192	Rack:0 Slot:13 Local	FSW103	1	1.01	None		Online	5/18/2017 18:49
18	FRM220A-192	172.24.1.192	Rack:0 Slot:14 Local	FSW103	1	1	None		Online	5/18/2017 18:49
19	FRM220-Ch08	172.24.1.199	Rack:0 Slot:1 Local	NMC	1.01	5.27	0		Online	5/10/2018 9:04
20	FRM220-Ch08	172.24.1.199	Rack:0 Slot:2 Local	16G-3R	1	0.001	None		Online	12/3/2013 20:27
21	FRM220-Ch08	172.24.1.199	Rack:0 Slot:3 Local	Serial	1.1	1.01	None		Online	12/10/2013 11:21
22	FRM220-Ch08	172.24.1.199	Rack:0 Slot:4 Local	10G-SS	1.1	2.014	None		Online	12/3/2013 20:27
23	FRM220-Ch08	172.24.1.199	Rack:0 Slot:5 Local	FOM01	1	1.4	None	bacello	Online	12/3/2013 20:27

Figure 7-6 Exported Inventory, viewed in MS-Excel

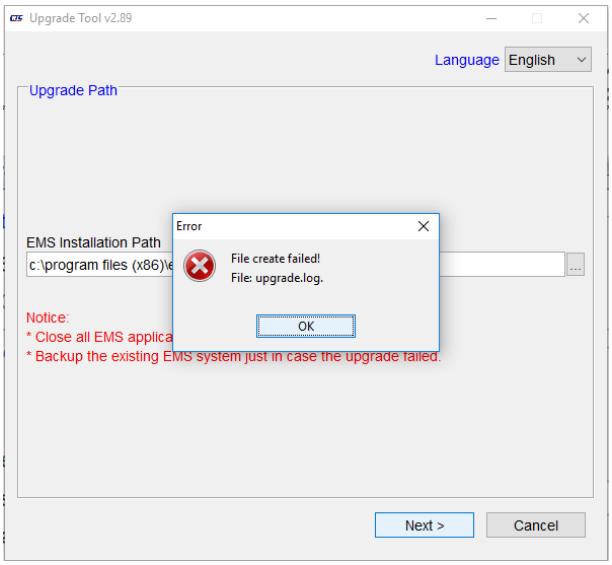
As the inventory feature is a new function in SmartView EMS, our engineers will continue to fine tune and add valuable features in later releases. In addition, the number of line cards that can support the embedded serial number will be slowly increased as time allows.

This page left blank intentionally

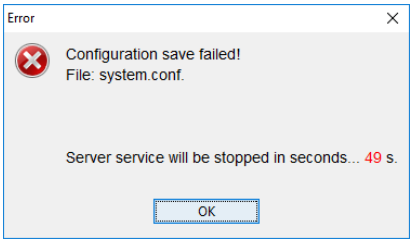
Chapter 8 Troubleshooting

8.1 Post Installation

If you see these error messages pop up, chances are the permissions are not right for the EMS folder.



OR

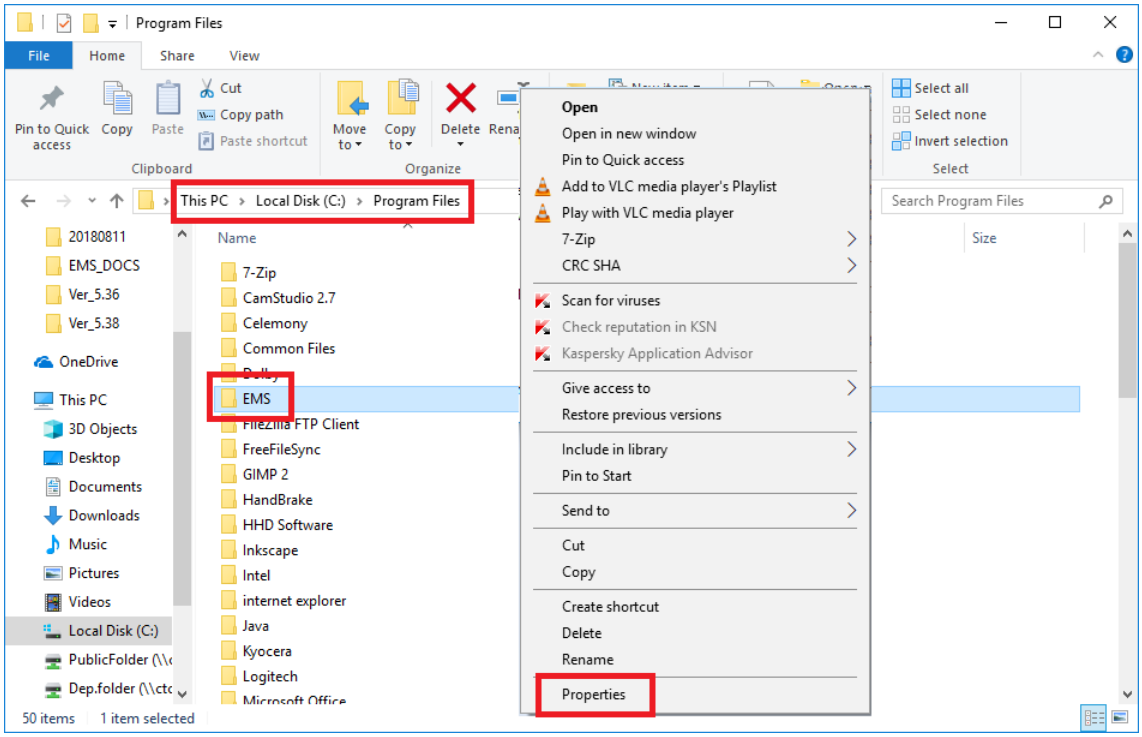


8.1.1 Take Permission of EMS Folder

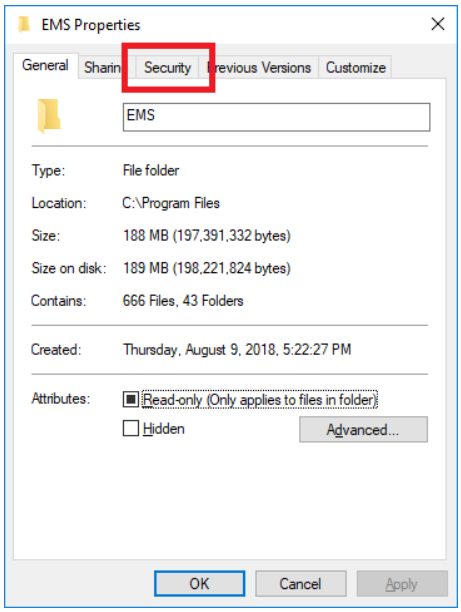
Microsoft Vista, Windows 7, Windows 8, Windows 8.1 and Windows 10 all introduce permission settings on system files, such as those located in the windows and program files folders. Unless the administrator account has been enabled and the user is using administrator to log into the system, any attempt to update the EMS will fail due to write access denied.

A simple fix here is to have the logged in user take full permission of the EMS folder. Here is how to change the permissions for all normal logged in users.

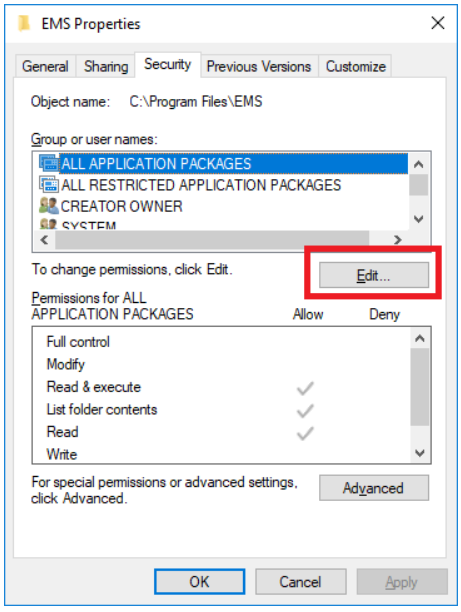
Step 1. Browse to the Program Files folder and "right-click" on the EMS folder. Select 'Properties'.



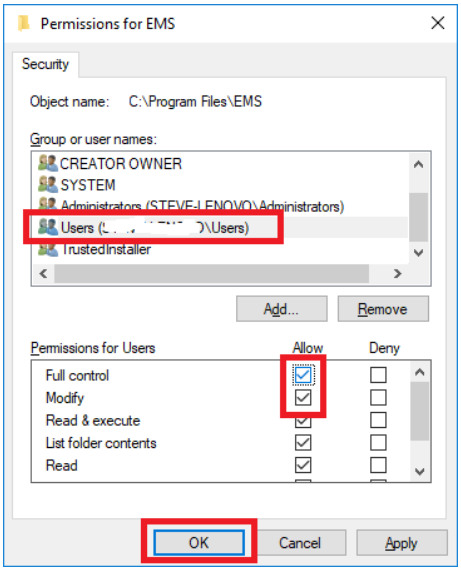
Step 2. Select the "Security" tab.



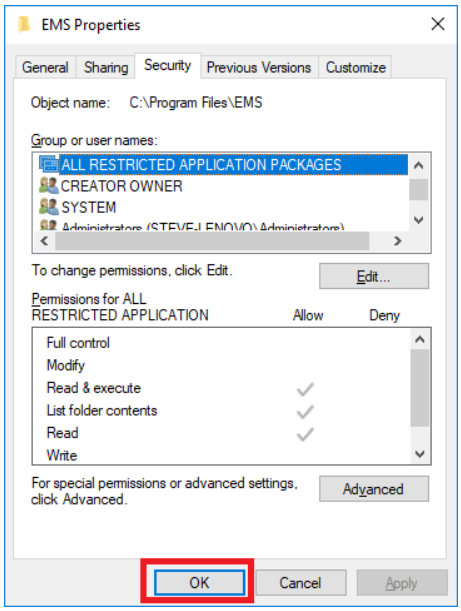
Step 3. Under the 'Security' tab, click the "Edit" button.



Step 4. Select the "Users" group for this computer.
Step 5. Click the "Full control" and "Modify" permissions for users (all will be checked).
Step 6. Click "OK".



Step 7. Click "OK".



Now that all users have full permission for the EMS folder, the update patches can be applied without any error messages regarding file access rights.

8.1.2. Enable Administrator Account

By default, the administrator account is disabled in Windows 7, 8, 8.1 and 10. For a Windows 7 machine dedicated to running EMS, the administrator account can be enabled and used as the default login to the server. The EMS can then be installed and upgraded at any time without any problem with file permissions.

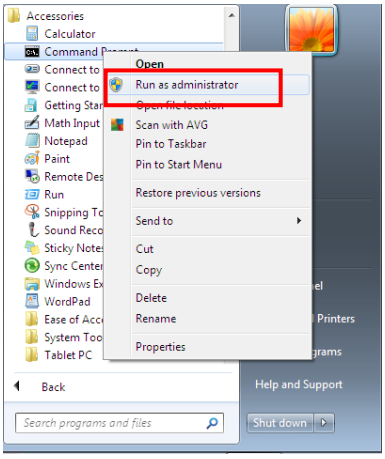
Note: Only Professional or Enterprise versions of Windows can support enabling the administrator user. In addition, this may cause a security issue if someone has physical access to the machine or if it should become compromised. For better security, it is still recommended to use a normal user account and follow the instructions in 8.1 Take Permission of EMS Folder. However, we have included the procedure to enable the administrator account.

Windows 7 Starter, Windows 7 Basic, and Windows 7~10 Home Premium do not have an administrator account. Therefore, to run EMS on these flavors of Windows, it is best to place the EMS installation folder into a writeable user location rather than in 'Program Files'.

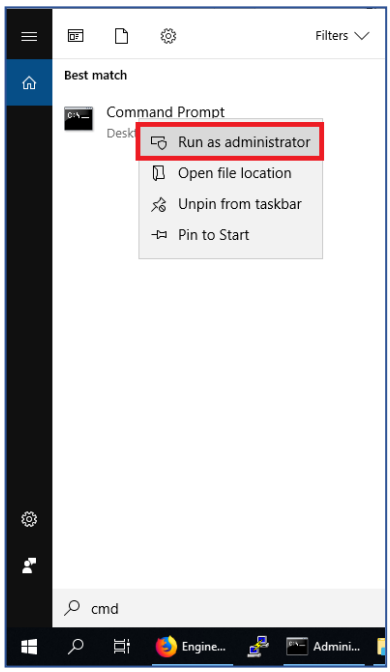
8.1.3 Enable Administrator using Command

This is the quickest way to enable the administrator account on Windows 7.

Step 1. Click the **Start** button, click **All Programs**, click **Accessories**, then Right-Click **Command Prompt** and choose **Run as administrator**. Click **Yes**.



In Windows 8, 8.1, 10, use **Windows Key +s** (search), key in **cmd** and when **Command Prompt** shows, right-click it and select **Run as administrator**. Click **Yes** on the UAC (user access control) prompt.



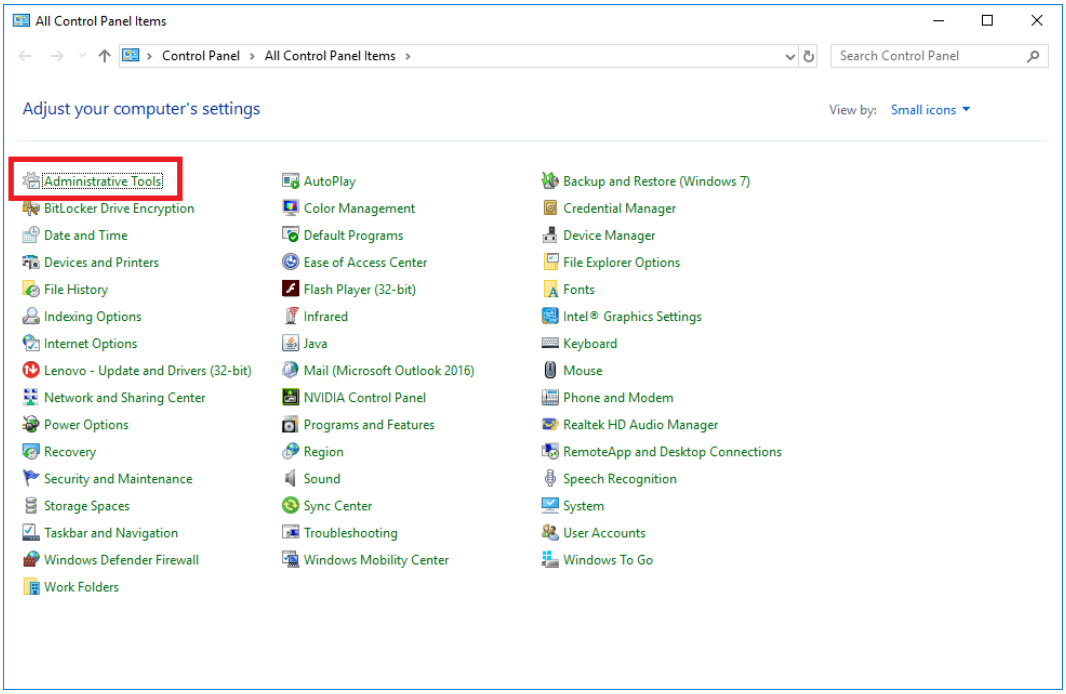
Step 2. In the command window type in the command exactly as below.

```
net user administrator /active:yes
```

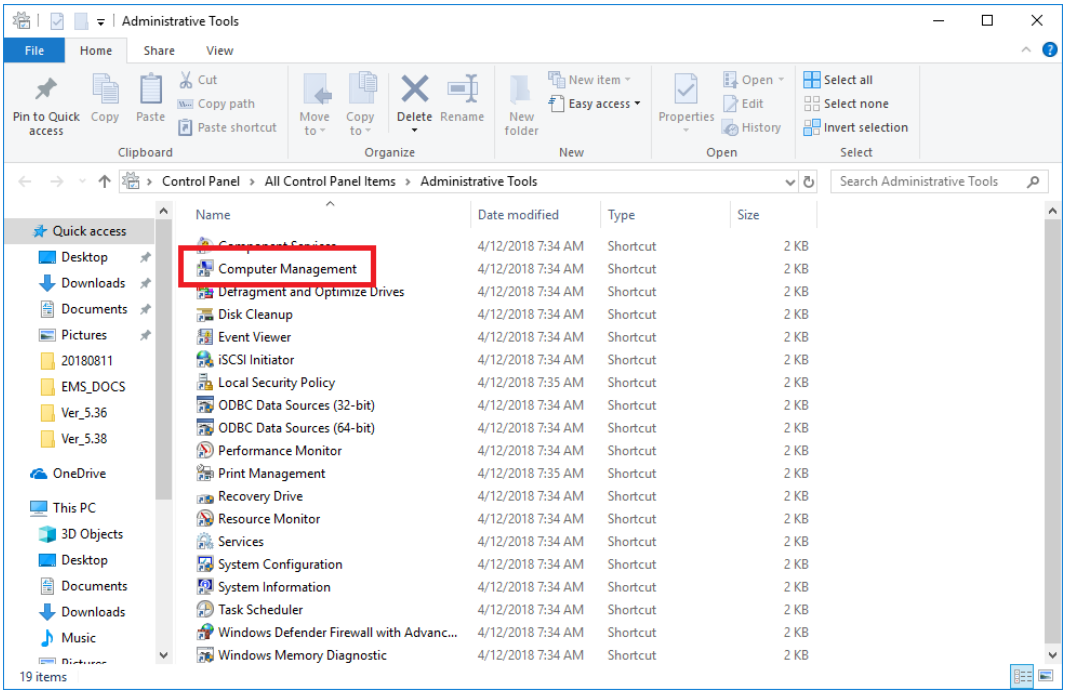
Step 3. Exit and logoff. Then login as administrator and set password.

8.1.4 Enable Administrator Account Using Control Panel

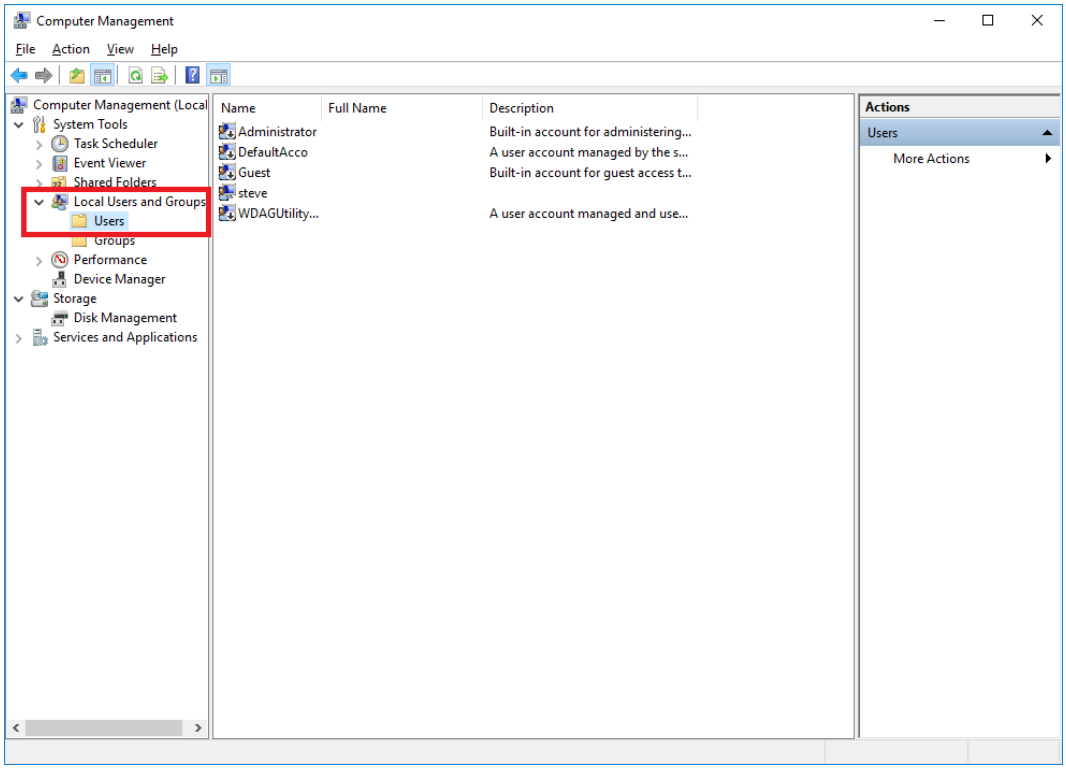
Step 1. Use **Windows Key + r** (Run) and key in **control**. Double click **Administrative Tools**.



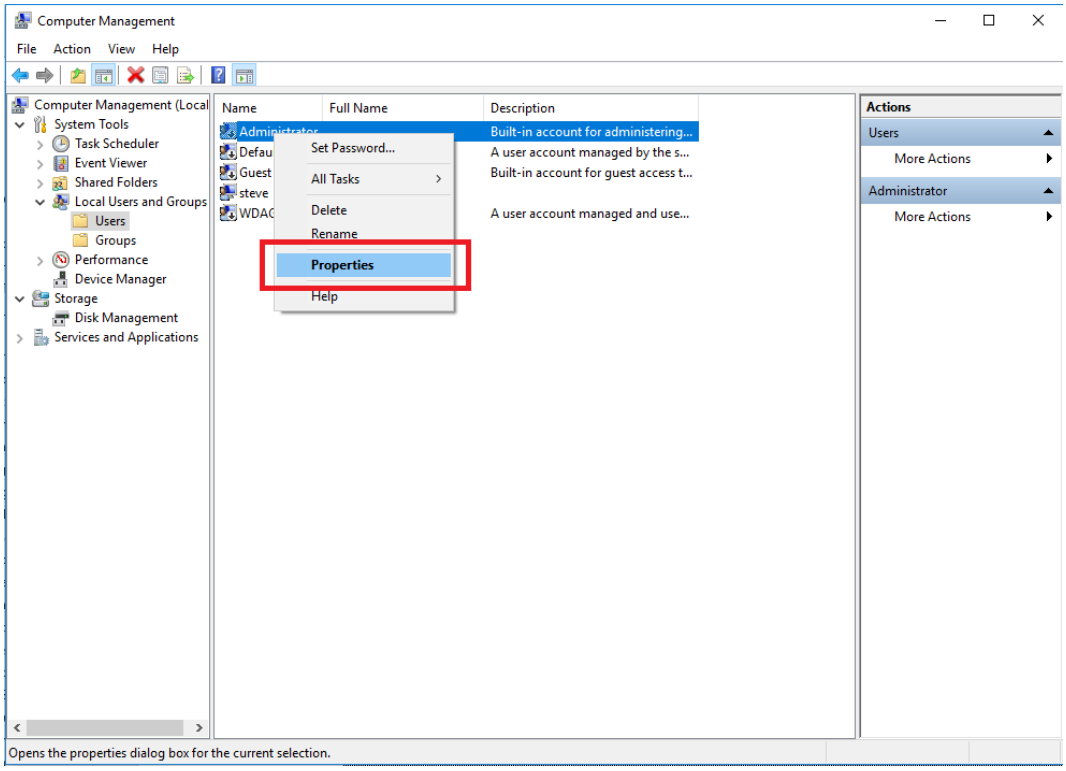
Step 2. Double click **Computer Management**.



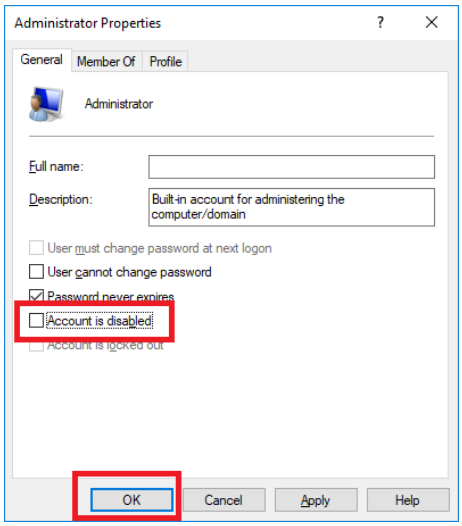
Step 3. Open up the "Local Users and Groups" and select "Users".



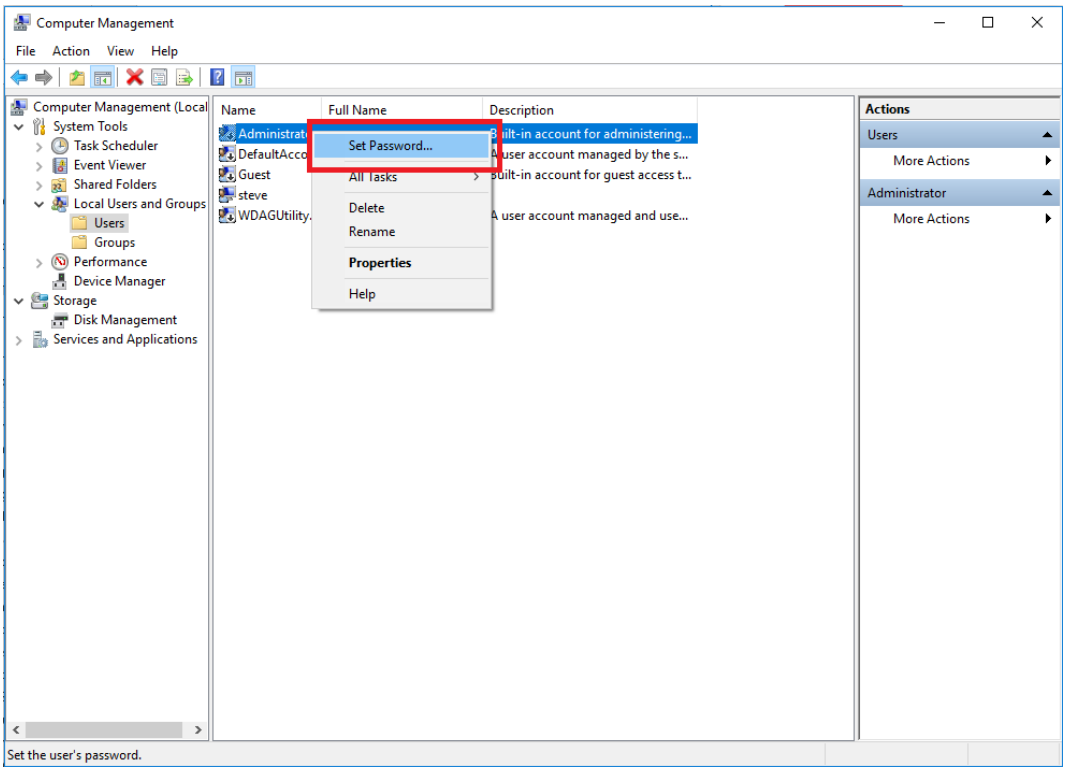
Step 4. Right-click on the user **Administrator** and click **Properties**.



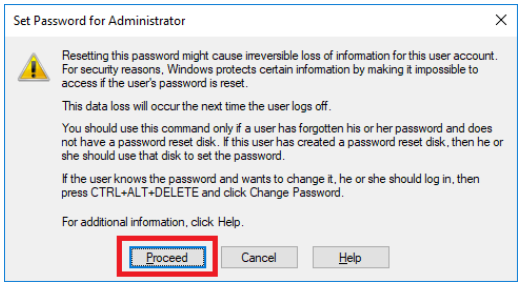
Step 5. Uncheck the "Account is disabled" check box and click OK.



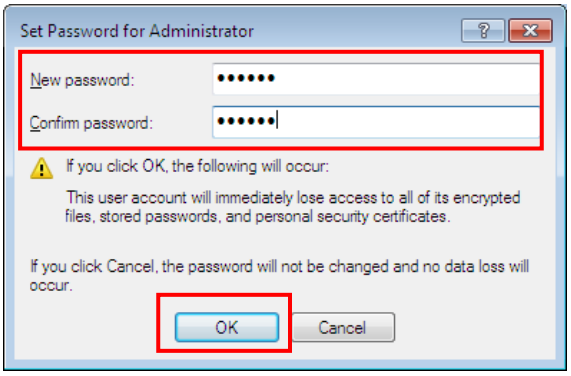
Step 6. Right-click the **Administrator** again and this time select **Set Password**.



Step 7. Ignore the warning and click **Proceed**.



Step 8. Enter a secure password twice and click OK.

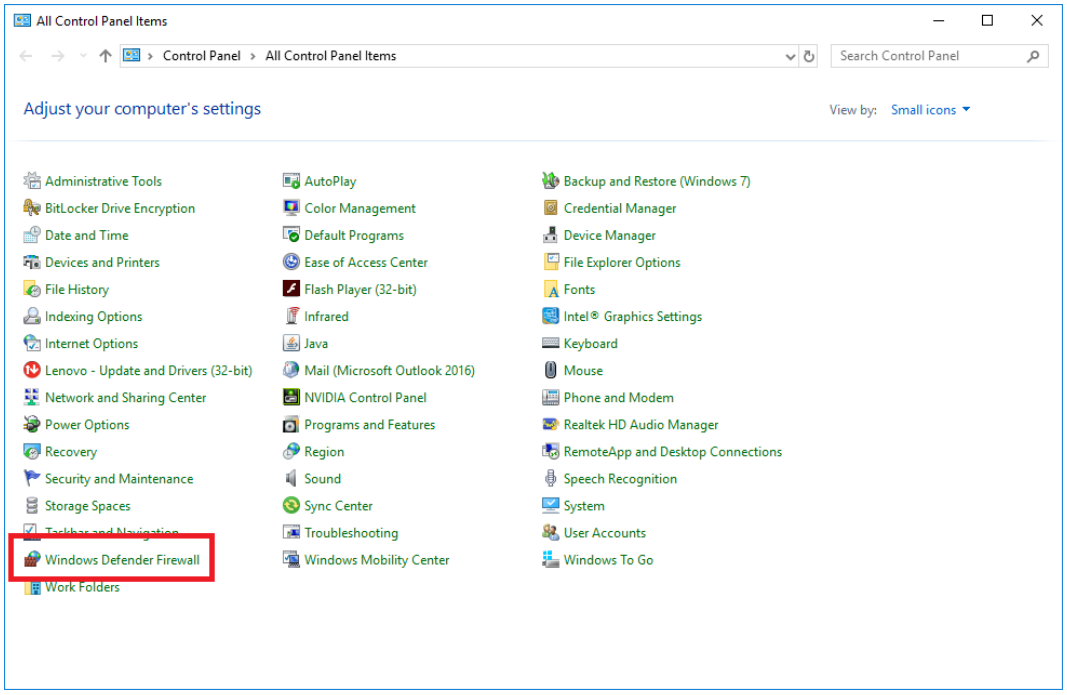


Now logout and log back in with the now activated administrator account.

8.1.5 Open Firewall for SNMP Traps

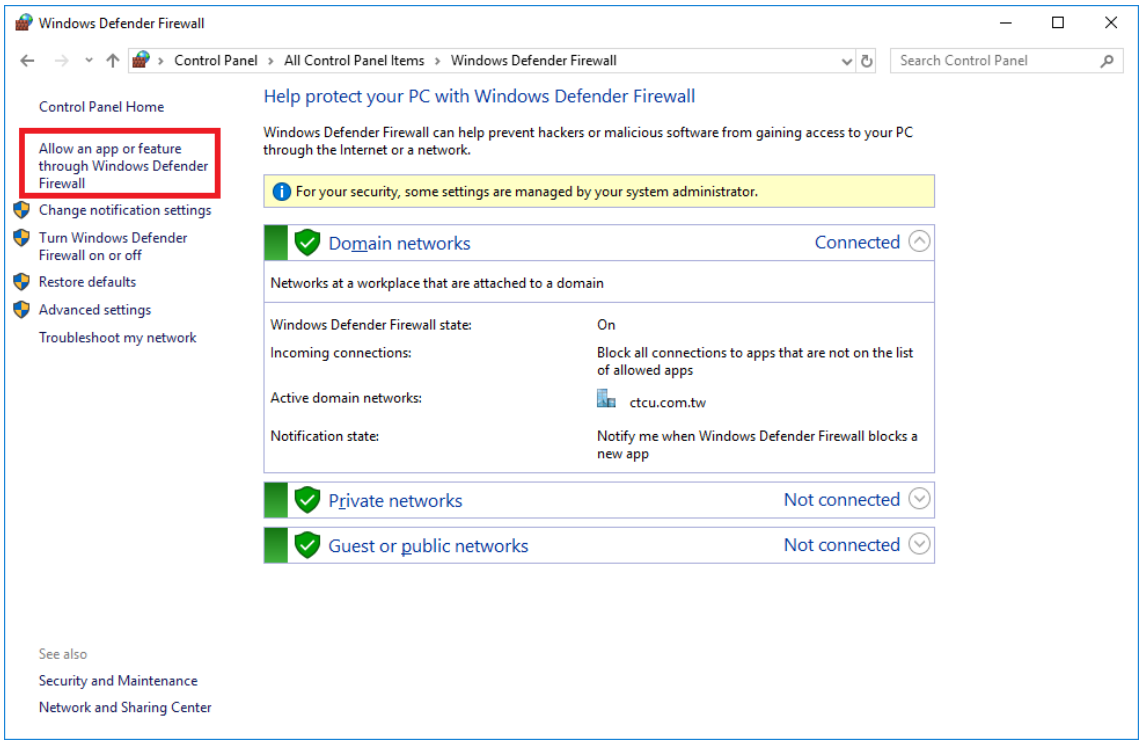
Both Windows 10 and Windows Server 2016 have SNMP Traps blocked by default. The EMS server will not show any traps until the Firewall is opened for SNMP Traps.

Step 1. Use the **Windows Key + r** (Run) and key in **control**. This will open the **Control Panel**.

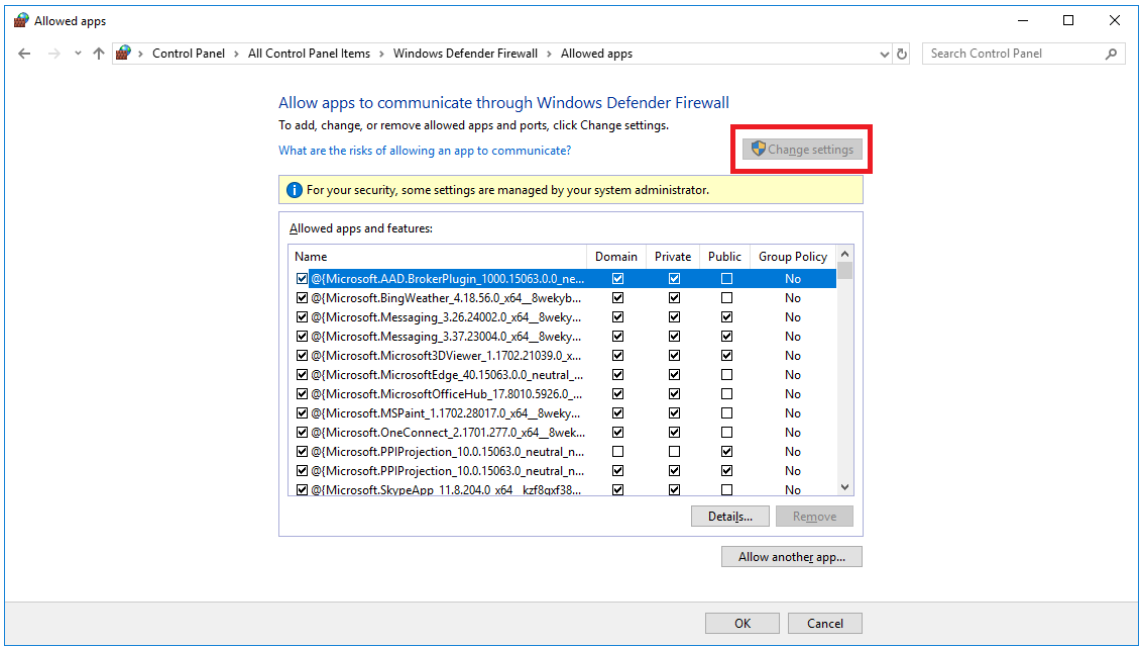


Step 2. Double click the **Windows Defender Firewall**

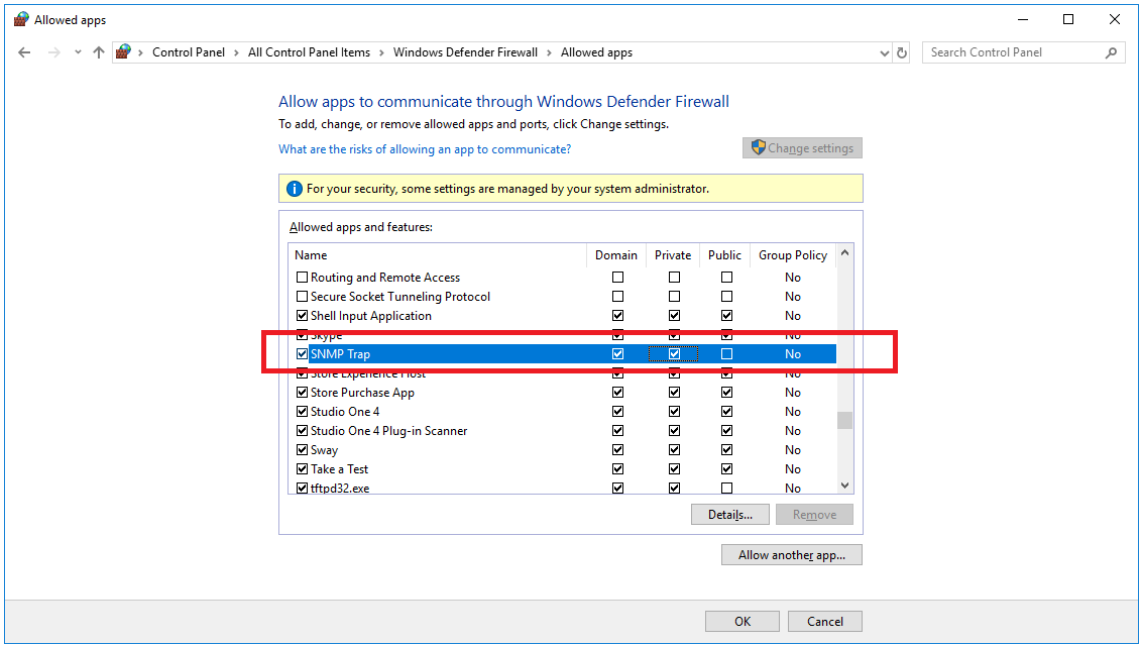
Step 3. Click the **Allow an app or feature….**



Step 4. Click **Change settings**



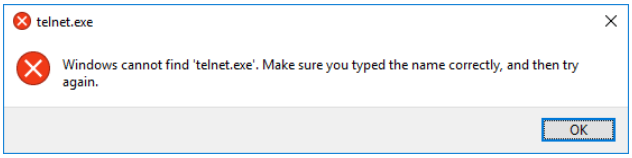
Step 5. Pull down and find **SNMP Trap**, then enable the check box. Finally, click **OK**.



SNMP traps will then be received by Smartview.

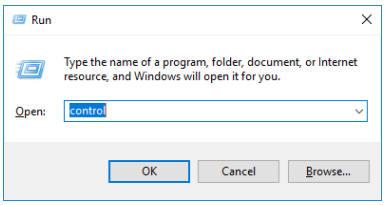
8.1.6 Telnet Won't Open when Right Clicking Device

Have you been presented with the following pop up window?

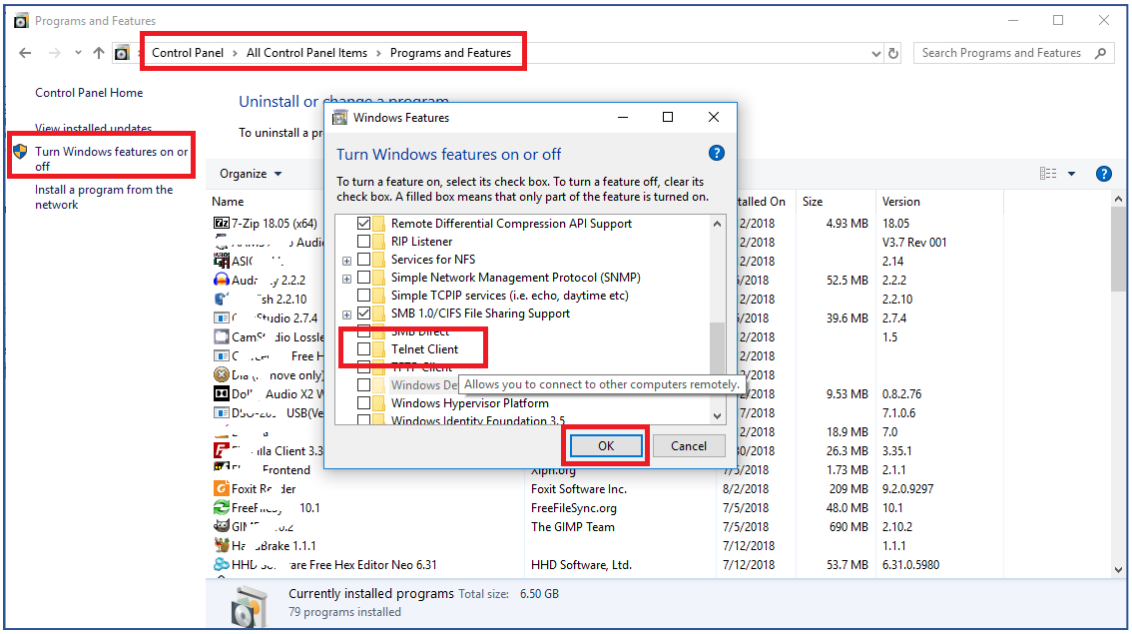


We have found that the Telnet client is NOT active by default for either Windows 10 or for Windows Server 2016.

Step 1. Open up **Control Panel** by using **Windows Key +r** and keying in **control**.

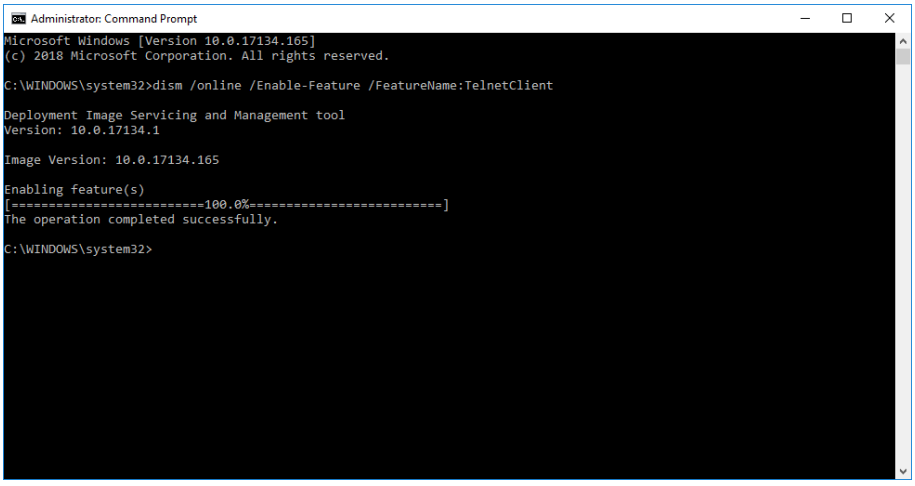


Step 2. Double click **Programs and Features**. Click **Turn Windows features on or off**.



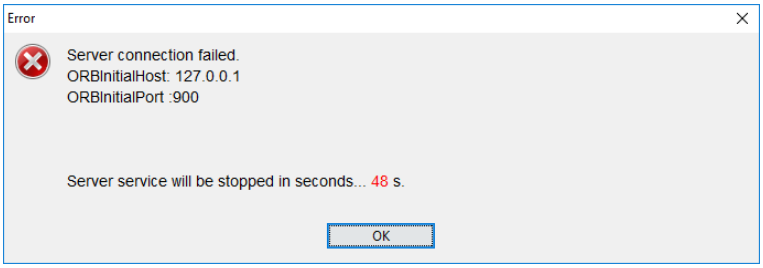
Step 3. In the pop up window, pull down until finding **Telnet Client**. Enable the check box and click **OK**.

If you feel confident using the command prompt, it is possible to enable this feature with elevated privileges: **dism /online /Enable-Feature /FeatureName:TelnetClient**



8.1.7 Server Startup Error

This is an error that normally only happens on an EMS server that is not in a fixed installation. If installing EMS on a laptop for demonstration purposes, it is possible to get the following error message when starting the EMS Server Console.



This error message occurs if the IP address has changed. Fix this issue by following the section 8.4 by either re-running the setup or by manually modifying the configuration (text) file.

8.2 Remote Client Issues

Most client login problems can be traced to one of two issues:
A) Incorrect client version that doesn't match the server.
B) Firewall not opening for JAVA processes

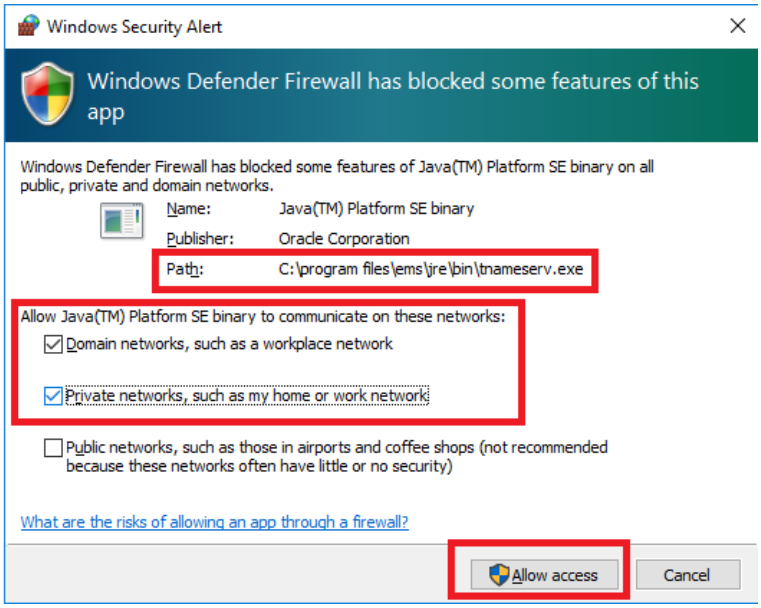
8.2.1 Version Incompatibility

To correct A, use the EMS folder of either the DVD used to install Smartview, or from the last used Upgrade Tool and re-run the setup for client. Placing the EMS folder on the desktop is a good way to always quickly find the client folder to start the EMC (Element Management Console) and to quickly overwrite with new versions.

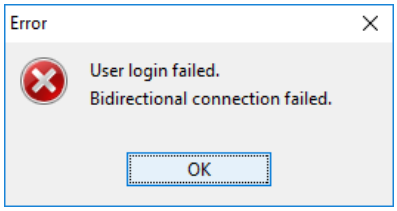
8.2.2 Firewall Issues

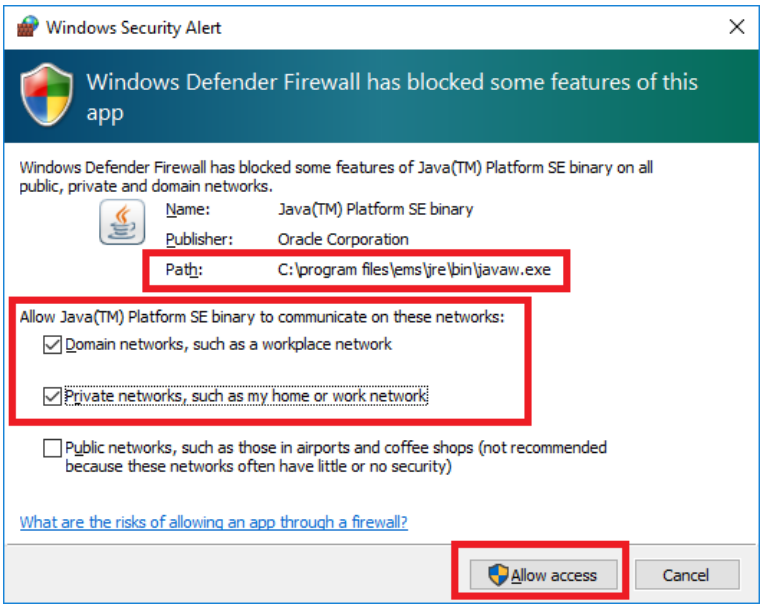
To correct B, firewall issues, JAVA SE and Tnameservice need to be allowed through the firewall.

When first starting the SmartView client, there should be two pop-up windows from the Firewall asking if the Java SE and the Java Tnameservice should be allowed.



The above pop up window from **Windows Defender Firewall** (Windows 10 or Windows Server 2016) is with regards to the 'name service' required by the **CORBA** connection between **EMS Server** and **EMS Client**. By default, we recommend that the two check boxes for **Domain networks** and **Private networks** both be checked. If the client will connect remotely, and for remote connection we highly recommend using **VPN**, then the **Public networks** should also be checked. Failure to do so will result in the following message pop up.



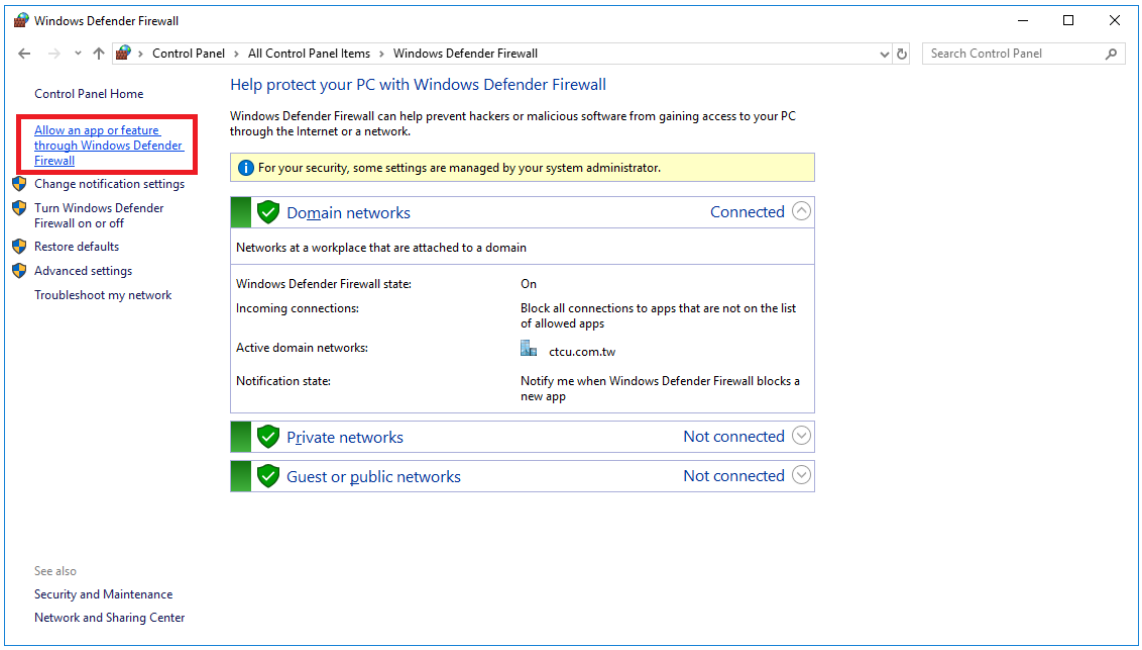


The above pop-up window from **Windows Defender Firewall** (Windows 10 or Windows Server 2016) is with regards to the Java SE (javaw.exe) required by the **EMS Client**. By default, we recommend that the two check boxes for **Domain networks** and **Private networks** both be checked. If the client will connect remotely, and for remote connection we highly recommend using **VPN**, then the **Public networks** should also be checked.

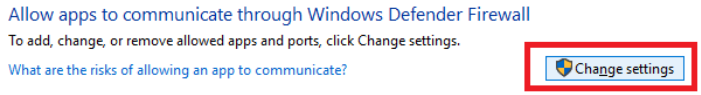
8.2.3 Modifying Firewall

If the Firewall permissions were never granted or if they need to be modified, here is the procedure for **Windows Defender Firewall** (in Windows 10 and Windows Server 2016).

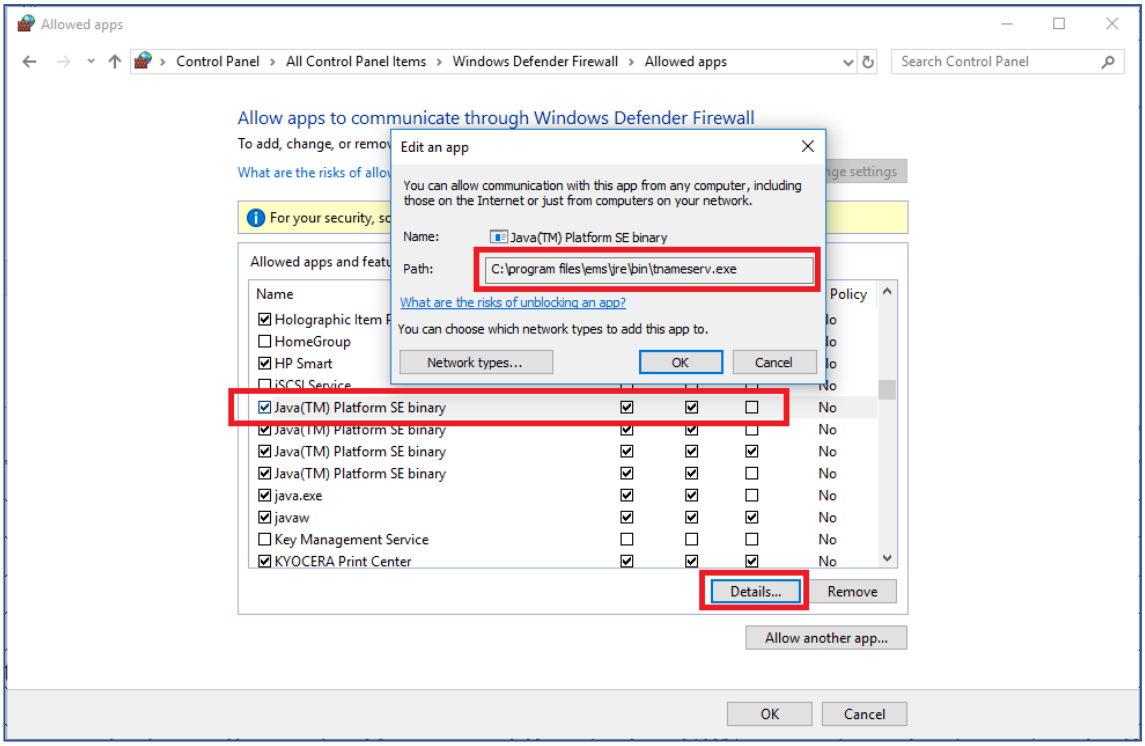
From **Windows Defender Firewall**, under **Control Panel**;
Step 1. Click 'Allow an app or feature…'



Step 2. Click the **Change settings** button.



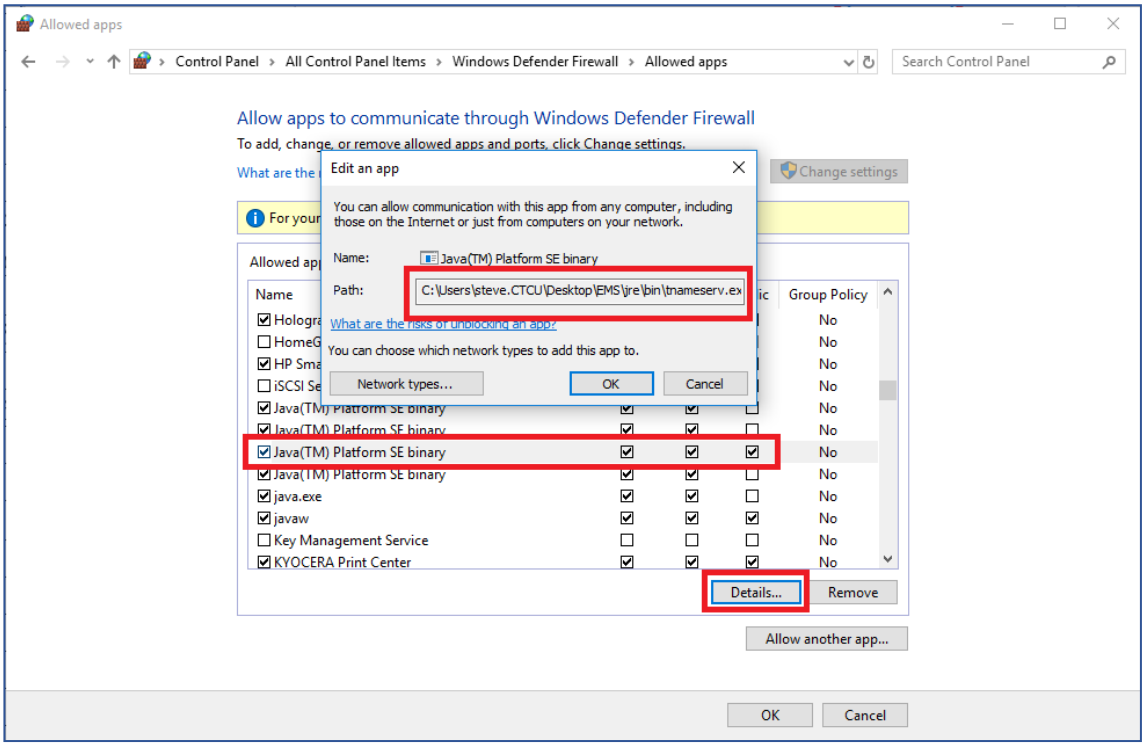
Step 3. Scroll down and find and highlight the app labeled **Java™ Platform SE binary**. Click the **Details** button.



Step 4. The pop up has identified the name server app used by both EMS Server and EMS Clients. Click OK and adjust the communications (Domain, Private, Public) accordingly.

Step 5. Do this for both the ems\jre\bin\tnameserv.exe and for ems\jre\bin\javaw.exe applications.

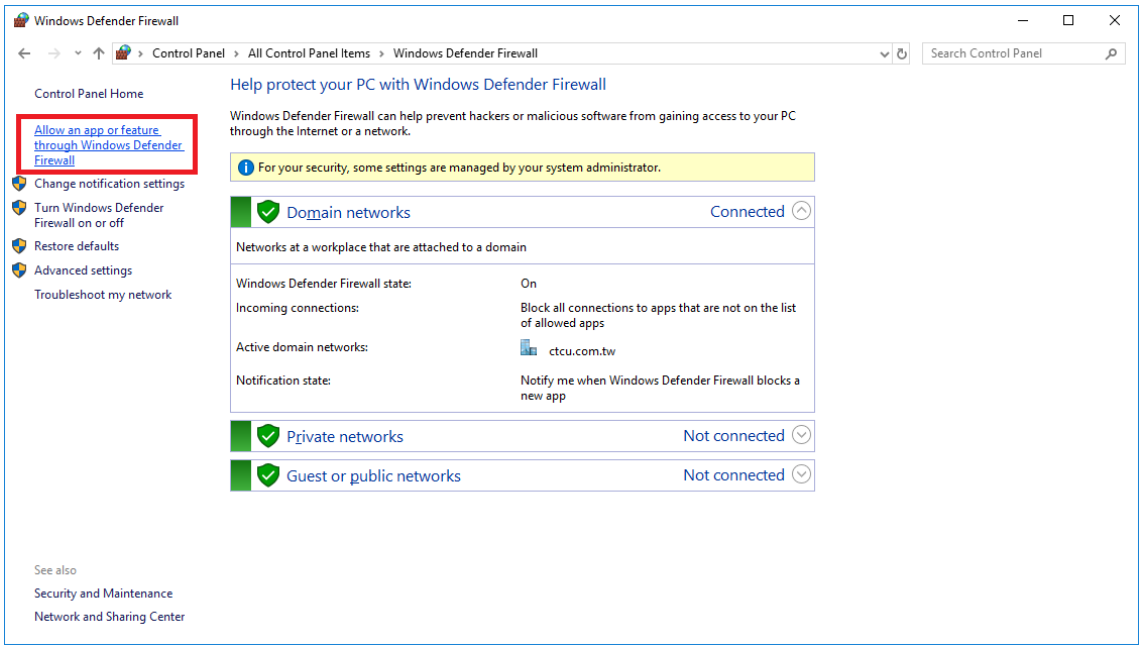
Step 6. For **client access**, find those binaries located in your client installation folder (example here is on the **Desktop**).



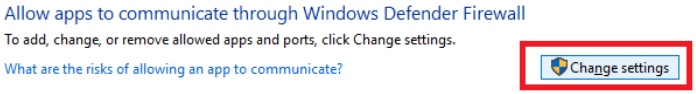
8.2.4 Adding App to Firewall

If a normal installation has been performed, it should not be necessary to add the applications to the list. However, if it is found that the Java binaries are NOT in the list, they can be manually added using this procedure.

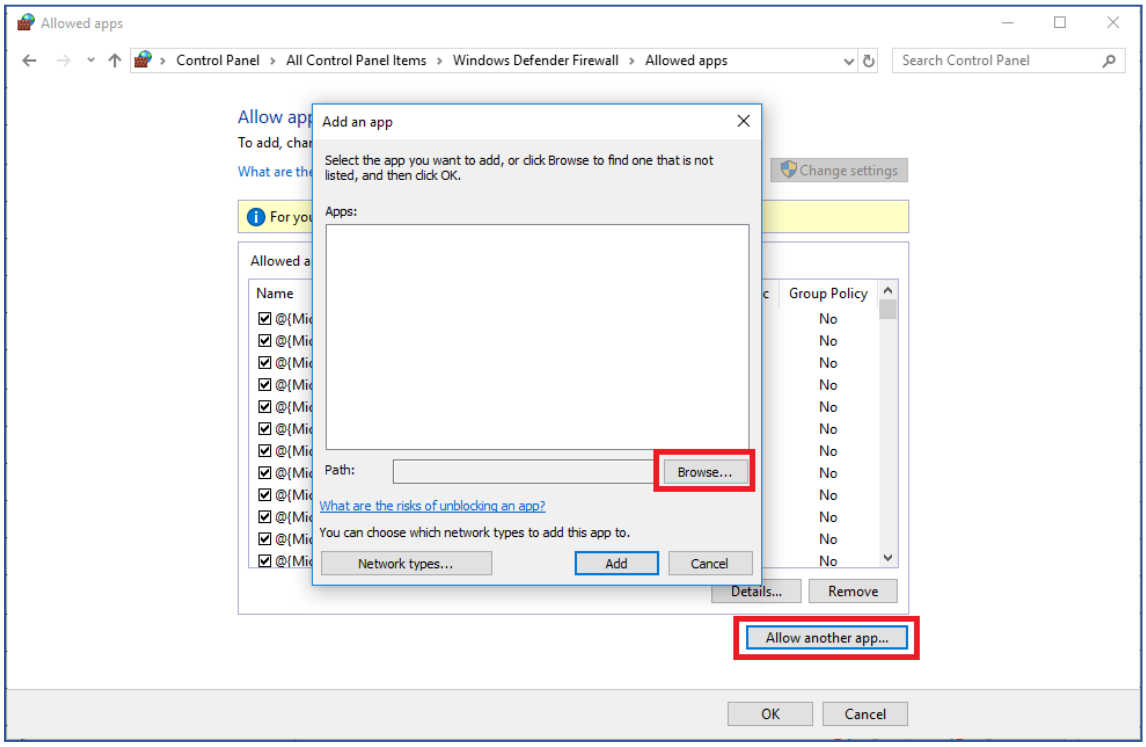
Step 1. Click 'Allow an app or feature…'



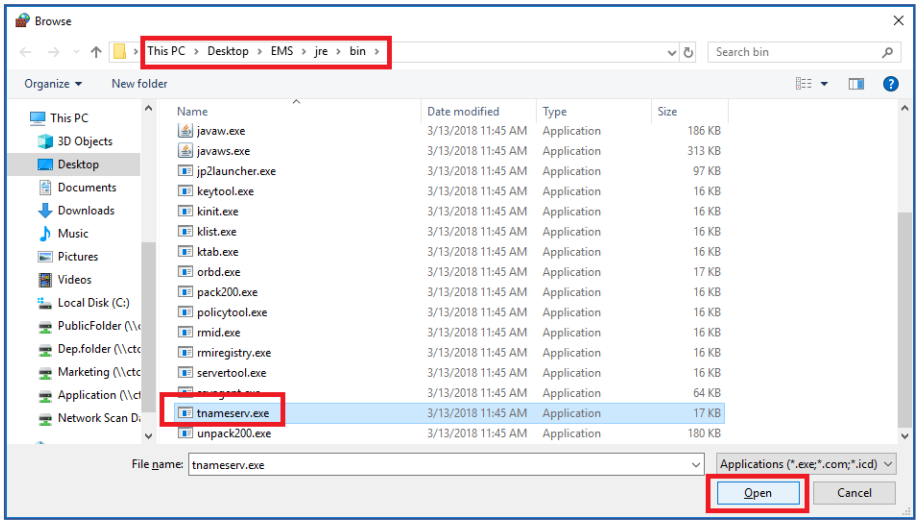
Step 2. Click the **Change settings** button.



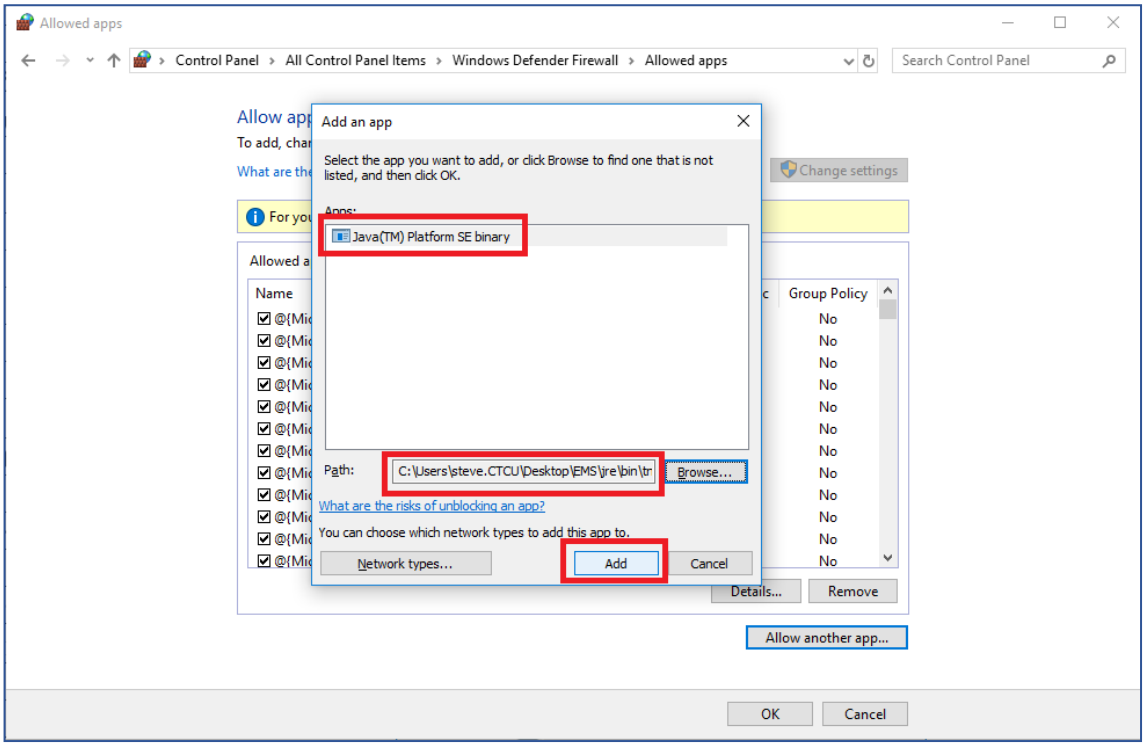
Step 3. Click the **Allow another app** button.



Step 4. Click the **Browse** button.



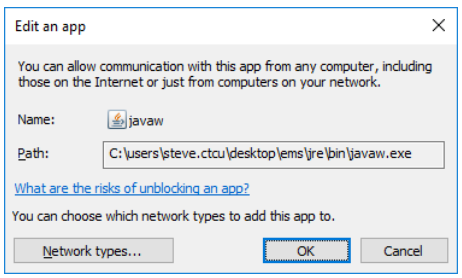
Step 5. Locate your client folder (example here is Desktop\EMS) and find the binary file to open. Do this for both the **javaw.exe** file and the **tnameserv.exe** files.



Step 6. Confirm the java binary was found, the path relates to your client location and click **Add**.

Step 7. Follow the previous example to edit the firewall settings for this app.

EMS Java Client
(client on Desktop)



8.3 Database and Connection Issues

Most problems that arise with EMS installations are related to the MS-SQL database installation and configuration (or lack of).

CTC Union support engineers are resolving SQL connectivity issues all the time, but usually the problems are caused by not following the SQL server installation instructions. Here is some help on how to resolve connectivity issues.

8.3.1 Connection Failure List

Basically, when Smartview fails to connect to your SQL Server, the issue could be:

1) Network issue. (Assuming the SQL Server is not on the same machine as Smartview server)

2). SQL not installed with "Default Instance" and/or "Mixed Mode" Authentication.

3) SQL Server configuration issue.

4) Firewall issue.

5) Client driver issue.

6) Application configuration issue.

7) Authentication and logon issue.

8.3.2 Network Issue

If SQL Server is running on the same machine as the EMS Server, the network is NOT an issue. EMS Server should always be able to make local connection without a working network, if *localhost* was chosen during Smartview EMS installation. In our EMS installation, we rely on a *localhost* connection (127.0.0.1), as it provides the best performance when the SQL Server and EMS Server are located on the same machine. For remote connections, a stable network is required. The first thing to troubleshoot SQL connectivity issues is to make sure the network we rely on is workable and stable. Please run the following commands:
Hint: **Windows Key + r cmd** and **OK**

ping -a <your_target_machine>

ping -a <Your_remote_IPAddress>

nslookup (type your local and remote machine name and IP address multiple times)

Be careful to see any mismatch on the returned results. If you are not able to ping your target machine, there is a high chance that either the network is broken or the target machine is not running. It's possible the target machine is behind a firewall and the firewall blocks the packets sent by ping. (See Step 4) The correctness of DNS configuration on the network is vital to SQL connection if connecting by name. Wrong DNS entry could cause of all sorts of connectivity issue later.

8.3.3 No "Default Instance" or no "Mixed Mode" Setup During Install

SmartView EMS uses a Java DBC connection to the default instance of SQL Server. If during a manual installation of SQL Server, all the default settings were clicked with the user just clicking 'Next' repeatedly, then EMS will NOT be able to connect to the database server. During installation, we must select the "Default Instance" option and for authentication, "Mixed Mode" must be selected and the SA account password defined.

The best way to install MS-SQL is to use the **EMSinstaller** and select the **MS-SQL Express installation**. This will choose the best SQL version for installation (Windows 7 will install **SQL-Server Express 2008 R2** while Windows 10 or Windows Server 2016 will install **SQL-Server Express 2014 SP2**). In addition, the installation will be performed in **unattended mode** so that the correct **Default Instance** and **Mixed Mode** settings are established.

There is NO WAY to correct an installation which did not create a Default Instance. The only way we have found to correct this mistake is to completely uninstall SQL Server from the machine, reboot, manually delete the installed folder, edit the windows registry to remove the keys for MS SQL, reboot again, then do a fresh install following the procedure outlined in the appropriate Appendix. (This is confirmed from Microsoft.) Again, we still recommend letting our **EMSinstaller** do the **MS-SQL Express** installation to avoid these pitfalls.

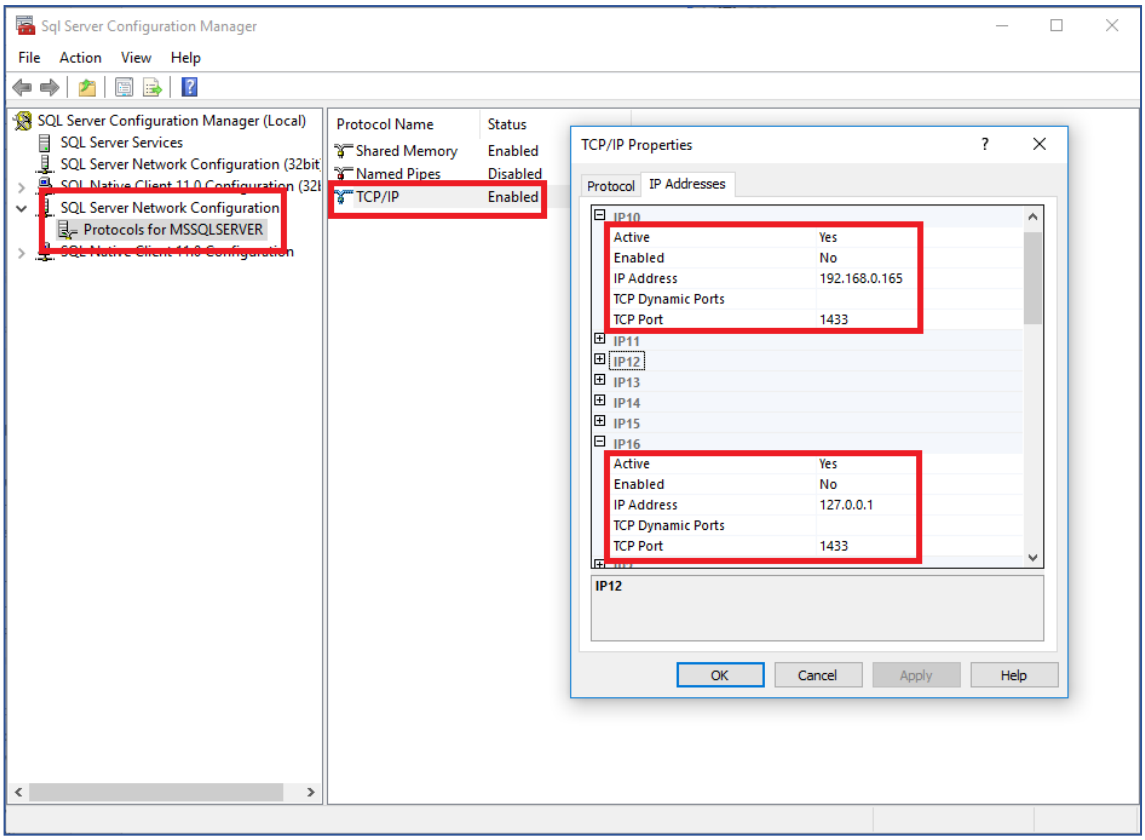
8.3.4 Must Restart EMSinstaller

When installing SQL Server through our **EMSinstaller** the installer must exit and be restarted before installing EMS. The reason is that when MS-SQL is installed, the 'sqlcmd' command is added to the environment path. While **EMSinstaller** is running, its path information is not updated. Exit **EMSinstaller**, then run **EMSinstaller** again and Smartview will be installed successfully every time.

8.3.5 SQL Server Configuration Issues

It is important to make sure the target SQL Server is running and is listening on appropriate protocols. You can use SQL Server Configuration Manager (SCM) to enable protocols on the server machine. SQL Server supports Shared Memory, Named Pipes, and TCP protocols (and VIA which needs special hardware and is rarely used). But for CTC Union's EMS, we only require that TCP/IP protocol be enabled. For both local and remote connections, TCP protocols must be enabled. Once you enabled protocols in SCM, please make sure restart the SQL Server. Details for Network Configuration of MS-SQL is given in the appendices of the EMS User Manual for SQL 2008, 2012 and 2014.

Here is an example screen for the SQL Server Configuration Manager for Server 2014.



Find the **Protocols for MSSQLSERVER** under **SQL Server Network Configuration**. This will display the three protocols in the right window. **TCP/IP** must be enabled. Select it and right-click to then select **Properties**. The **TCP/IP Properties** pop up will appear. Go to the **IP Addresses** tab and make sure there are both localhost (127.0.0.1) and your server's IP (this example is 192.168.0.165) configured. Make sure they are 'Active' and using Port 1433.

You must restart the **SQL Server** after making any changes here.

8.3.6 SQL and Firewalls

A firewall on the SQL Server machine (or anywhere between client and server) could block SQL connection request. An easy way to isolate if this is a firewall issue is to turn off firewall for a short time if you can. Long term solution is to put exception for SQL Server and SQL Browser.

For TCP protocol, you need put the TCP port on which the SQL Server listens on into exception.

For SQL server, the listening port is 1433.
For SQL Browser, please put UDP port 1434 into exception. (Not required for EMS.)

Meanwhile, you can put sqlservr.exe and sqlbrowser.exe into exception as well, but this is not recommended. IPSec between machines that we are not trusted could also block some packets.

8.3.7 Connection Tests

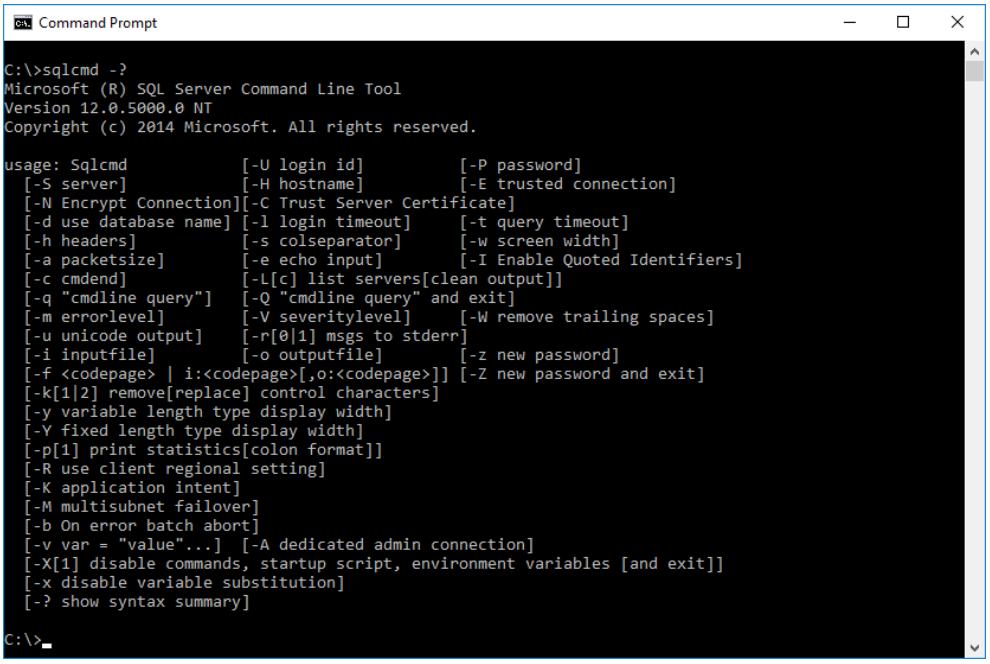
At this stage, you can test your connection using some tools. The tests need to be done on a client machine.

First try:

telnet <your_target_machine> <TCP_Port>

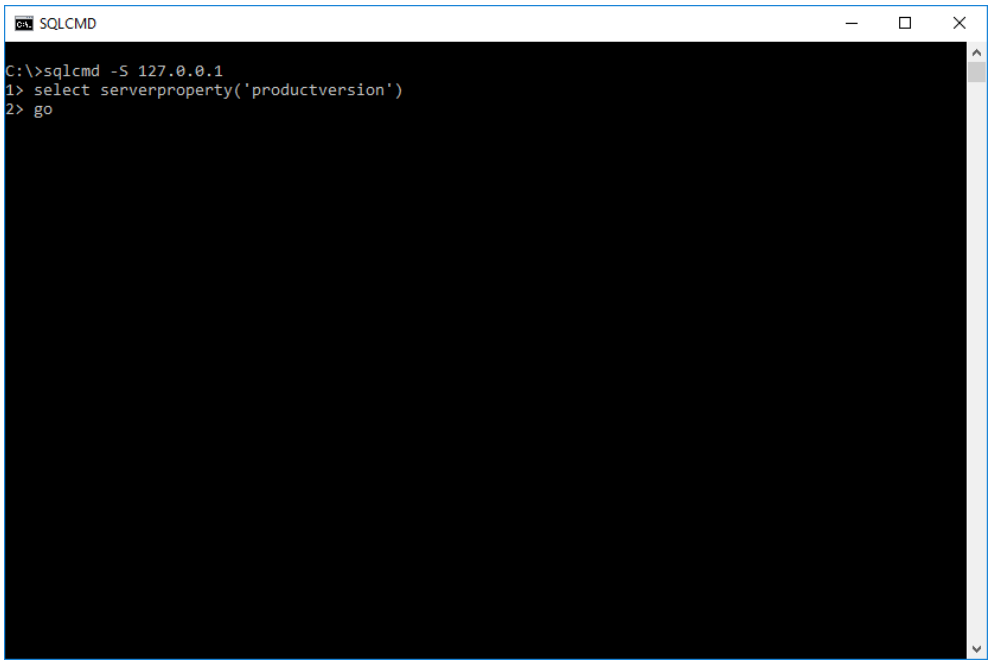
You should be able to telnet to the SQL server TCP port (1433) if TCP is enabled. Then, use SQLCMD and/or **SQL Management Studio** to test SQL connections. If you don't have those tools, please download SQL Express from Microsoft and you can get those tools for free. Another way to quickly troubleshoot is by using CLI. If you did a Telnet to your target's TCP port, the command window will wait for commands.

sqlcmd -?



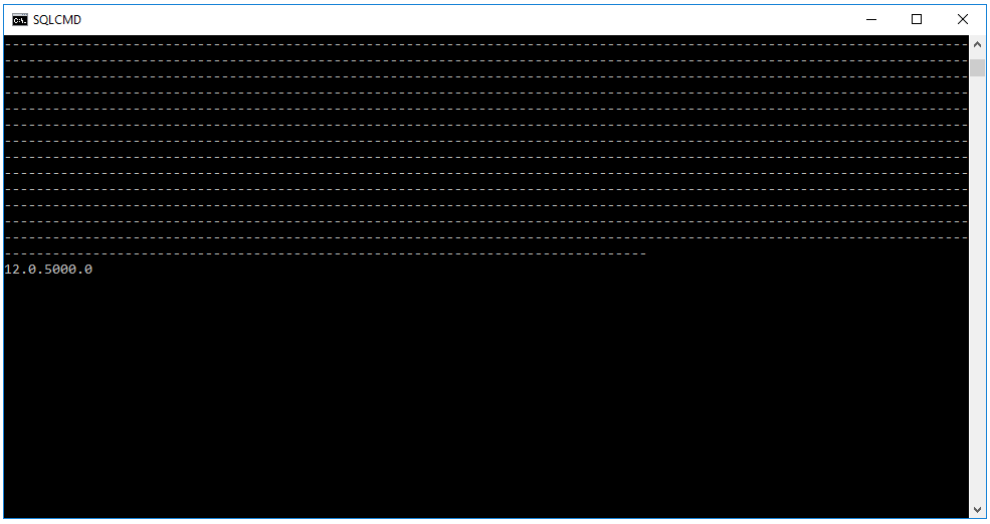
sqlcmd -S <your_target_machine>

In the example here, the **SQL Server** is running on the same machine as the **EMS Server**. So, we can connect by using the *localhost* IP address, 127.0.0.1.



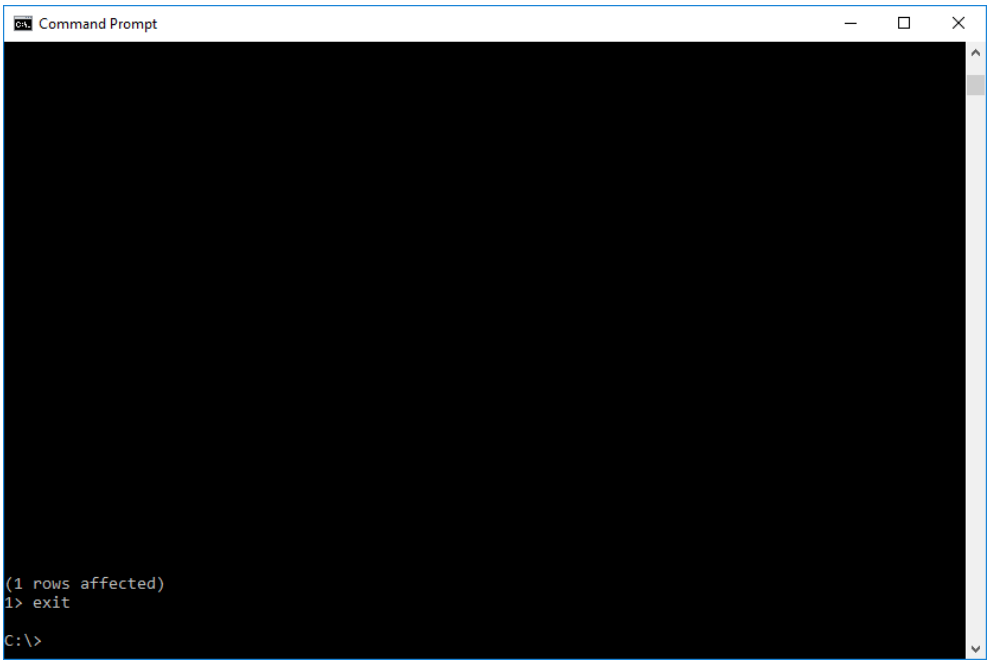
Example for finding your SQL Server version.

There will be many lines of 'dashed' output but the version will be displayed. (9.xx for MS-SQL Server 2005, 10.xx for MS-SQL Server 2008, 11.xx for MS-SQL Server 2012 and 12.xx for MS-SQL Server 2014)



Hint: Scroll back some to reveal this info.

Quit the command by entering 'exit'



SQLCMD (shipped with SQL Server 2005 & 2008) uses SNAC OLEDB.

SQL Management Studio (shipped with SQL Server 2005 & 2008) uses SQLClient.

8.3.8 Application Issue

If you succeed with steps 8.3.1~8.3.7 but still see failure in your EMSapplication, it's likely a configuration issue in your application. Think about couple of possible issues here.

a) Is your application running under the same account with the account you did tests in step 4? If not, you might want to try testing under that account or change to a workable service account for your application if possible.

8.3.9 Authentication and logon issue

This is probably the most difficult part for SQL connectivity issues. It's often related to the configuration on your network, your OS and your SQL Server database. There is no simple solution for this, and we have to solve it case by case. There are already several blogs in SQL protocols talking about some special cases and you can check them to see if any of them apply to your case. Apart from that, things to keep in mind:

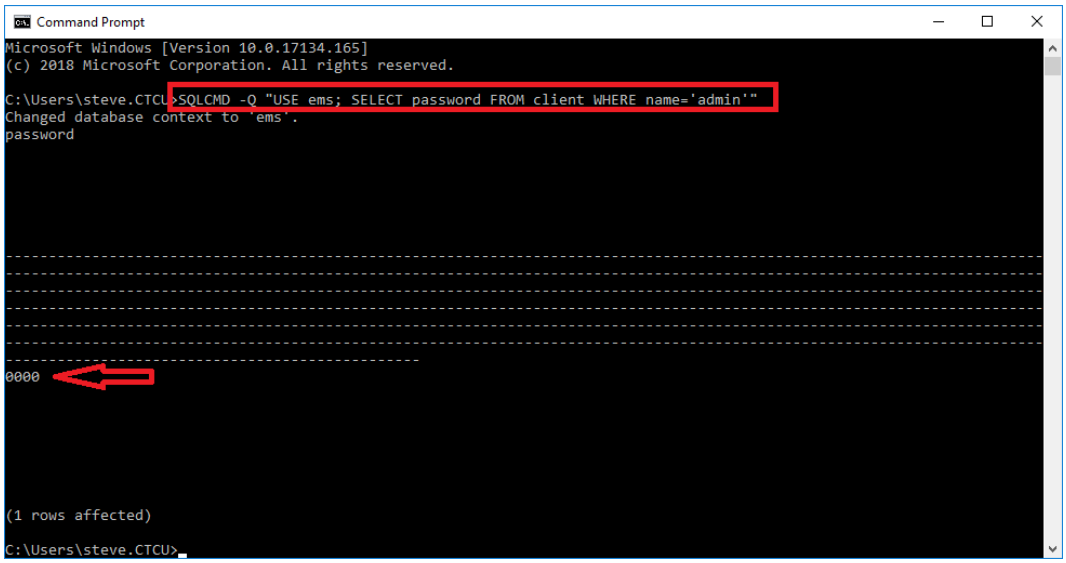
SmartView EMS uses **SQL Auth**, therefore mixed authentication must be enabled. Check this page for reference http://msdn.microsoft.com/en-us/library/ms188670.aspx.

In our EMS User Manual, the appendix for installing MS-SQL specifically shows how we deviate from normal install and choose "Mixed Mode" for authentication.

If you didn't choose this mode, it is probably best to uninstall and re-install MS-SQL and follow the procedure outlined in the appendices of the EMS User Manual. Better yet, use the **EMSinstaller** to install MS-SQL Server.

8.3.10 Forgot EMS Admin Password

The default admin password for EMS Server Console and Admin Console is 0000 (four zeros). If the password for admin is ever changed and forgotten, it can be shown in plain text by doing a database query.



Copy and Paste this entire command into the **Command Prompt** window.

```
SQLCMD -Q "USE ems; SELECT password FROM client WHERE name='admin'"
```

By substituting any EMS username for admin in this example, the password may be recovered for any EMS user.

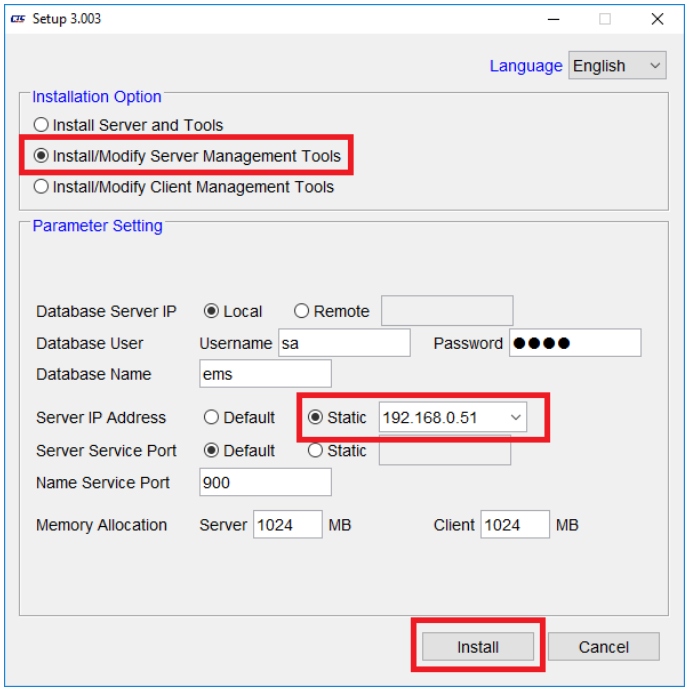
8.4 Changing Server IP Address

There may come a time when the EMS Server must have an IP address change. This is especially true if EMS is being demoed and the IP address needs changing.

8.4.1 Changing IP Through Setup

The quickest way to setup EMS for a new IP is to re-run the setup.

Step 1. Make sure EMC, Admin Console, and Server Console are closed.
Step 2. Browse to the EMS installation folder (default is c:\Program Files\EMS).
Step 3. Right click on the Setup(.bat) file and choose **Run as administrator**.

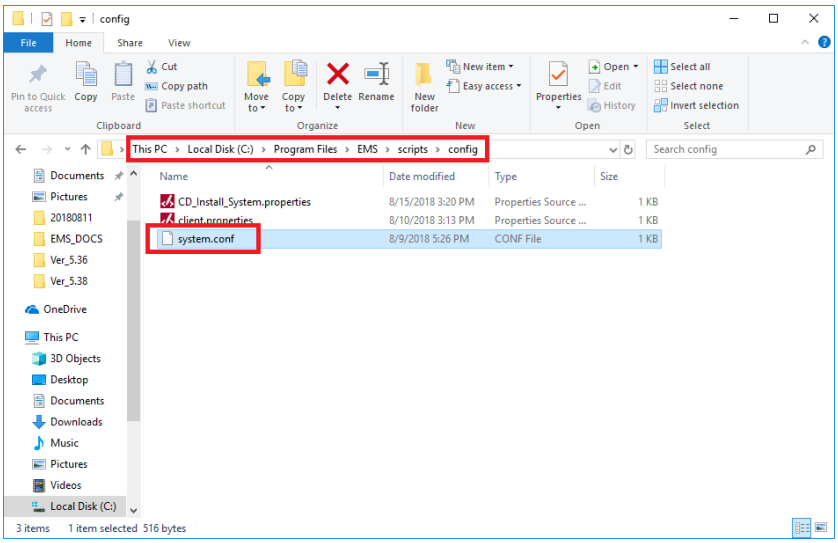


Step 4. Only select the **Install/Modify Server Management Tools**.
Step 5. Change the **Static** IP address and click **Install**.
The configuration will be modified.

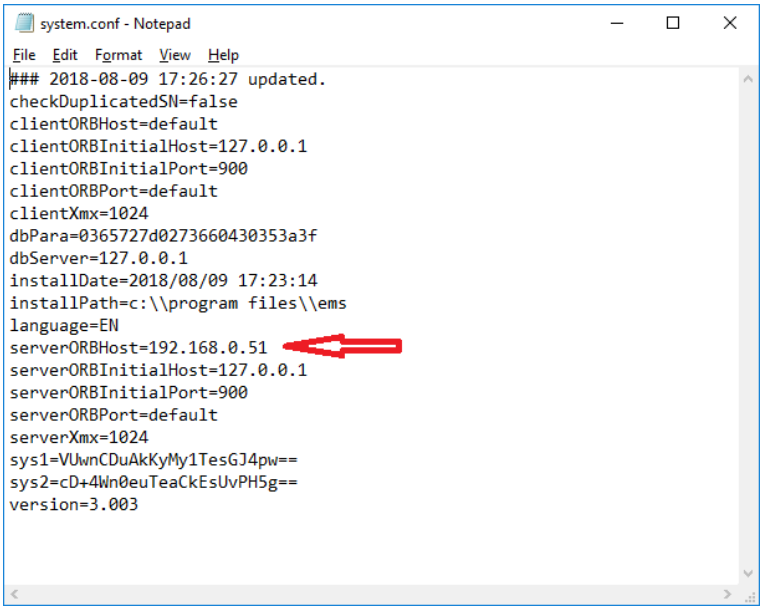
8.4.2 Manually Changing IP address

We are placing this here as it may also help in troubleshooting issues. Do this only if you feel comfortable editing configuration files. The best and quickest way to change IP is still by re-running Setup.

Find and edit the **system.conf** file located in the EMS\scripts\config folder.



Edit the line **serverORBHost** with the new IP address and save.



Be sure to use the new IP address from EMS Client when logging in. It is also convenient to use the localhost IP (127.0.0.1) when the client is running on the EMS server. The local client will always be able to connect via localhost.

8.6 Complete EMS System and Database Backup

It may be prudent to do occasional EMS System backup from time to time and move the backup off server. If is also recommended that a complete backup be made before doing EMS upgrade so that in case of trouble, the previously working system may be restored.

Backup:

Step 1. Logout and close any EMS client, Admin Console and Server Console.

Step 2. Browse to and copy the entire EMS folder (located at c:\Program Files\), save the copy.

Step 3. Browse to and copy the two **ems** database files (ems.mdf and ems_log.ldf) and save the copies. (c:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA\ems.mdf and ems_log.ldf)

Now that the EMS folder and the Database files have been backed up, they may be used to 'recover' back to this version in the event of some problem with a newer upgrade version EMS.

These files may also be used to clone the EMS server on to a new server, after doing a normal installation of course.

Recovery:

Copy over the database files, with administrator rights. Delete the contents of Program Files\EMS and copy the old contents into the EMS folder. Have all users take permission of the new EMS folder.

A new SN.txt license is required to run on new hardware, unless the MAC was from a NIC (network interface card) that can be moved to the new hardware.

Appendix A Installing MS-SQL 2008 R2 Express

A.1 Introduction

This chapter will detail the installation and configuration steps for the Free Edition of MS-SQL, Microsoft SQL Server 2008 R2 Express Edition. Server Express is a powerful and reliable data management product that delivers rich features, data protection, and performance for embedded application clients, light Web applications, and local data stores. SQL 2008 R2 Express can be installed on Windows Server 2008, Windows Server 2008 R2, Windows XP, Windows Vista, or Windows 7. (SQL 2008 R2 is not compatible with Windows 8.1 or Windows 10.)

Note:

SQL Server 2008 R2 SP2 Express Edition is differentiated from the rest of the SQL Server 2008 editions only by the following:

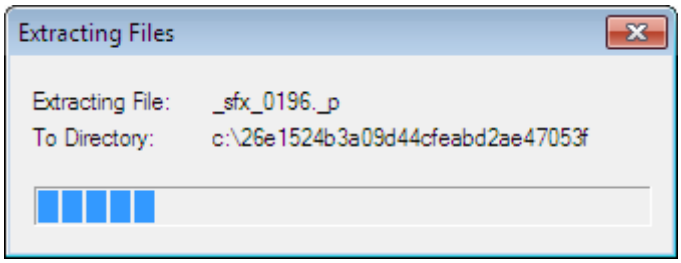
Lack of enterprise features support
Limited to one CPU socket or 4 CPU cores
One GB memory limit for the SQL Server Engine
Databases have a 10 GB maximum size

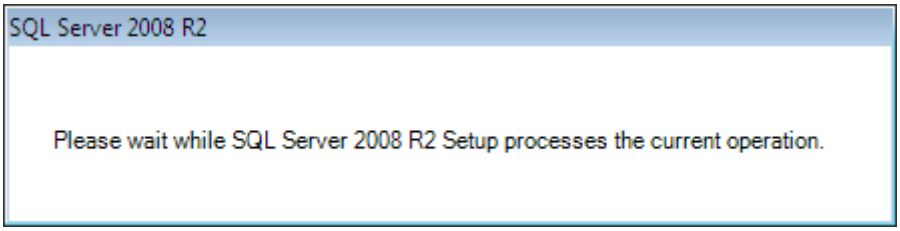
A.2 SQL Express Software Installation

In the following example, the step-by-step procedure is given for the free version of Microsoft® SQL Server 2008 R2 SP2. The free version may be downloaded from Microsoft's Download Center website and is a good choice for demonstrating or for evaluating the EMS in a non-production environment. For production use, please have your purchased version of MS-SQL Server 2008 and CD-Key from your Certificate of Authenticity (COA) and follow through the Microsoft documentation for installation.

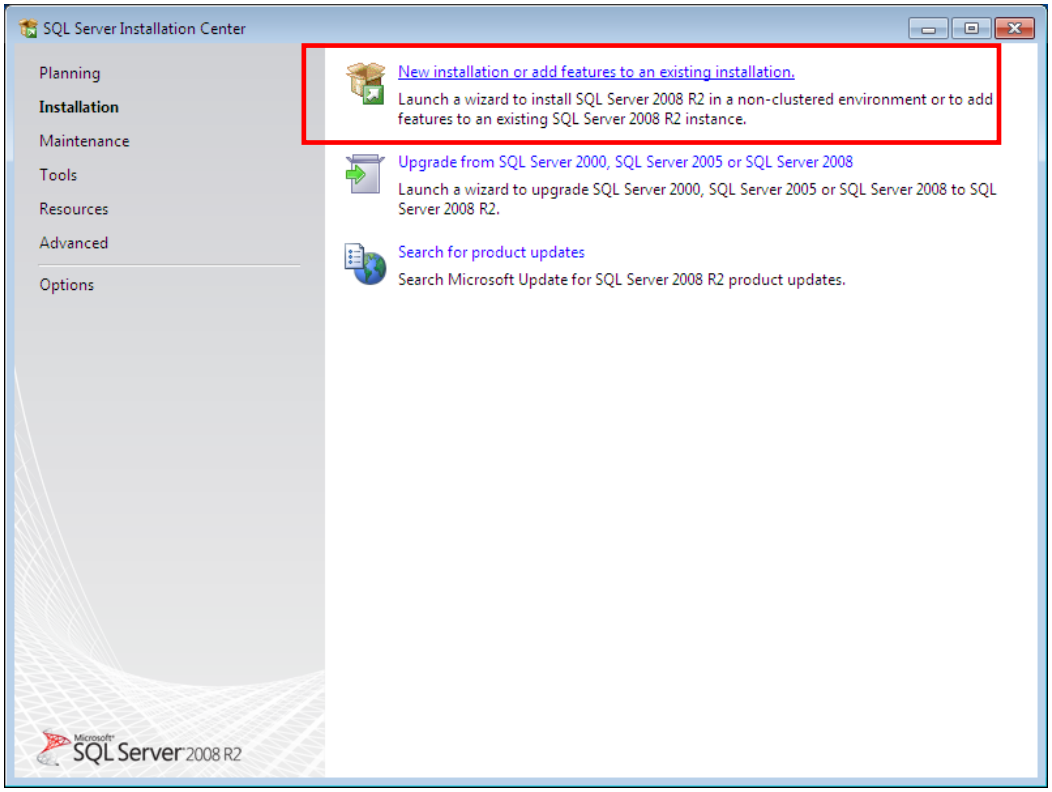
Find the location of your download files on the local disk and double-click into the ' SQLEXPR_x86_ENU.EXE' icon.

The downloaded file is a self-executable compressed file. First the files will be extracted to your system.

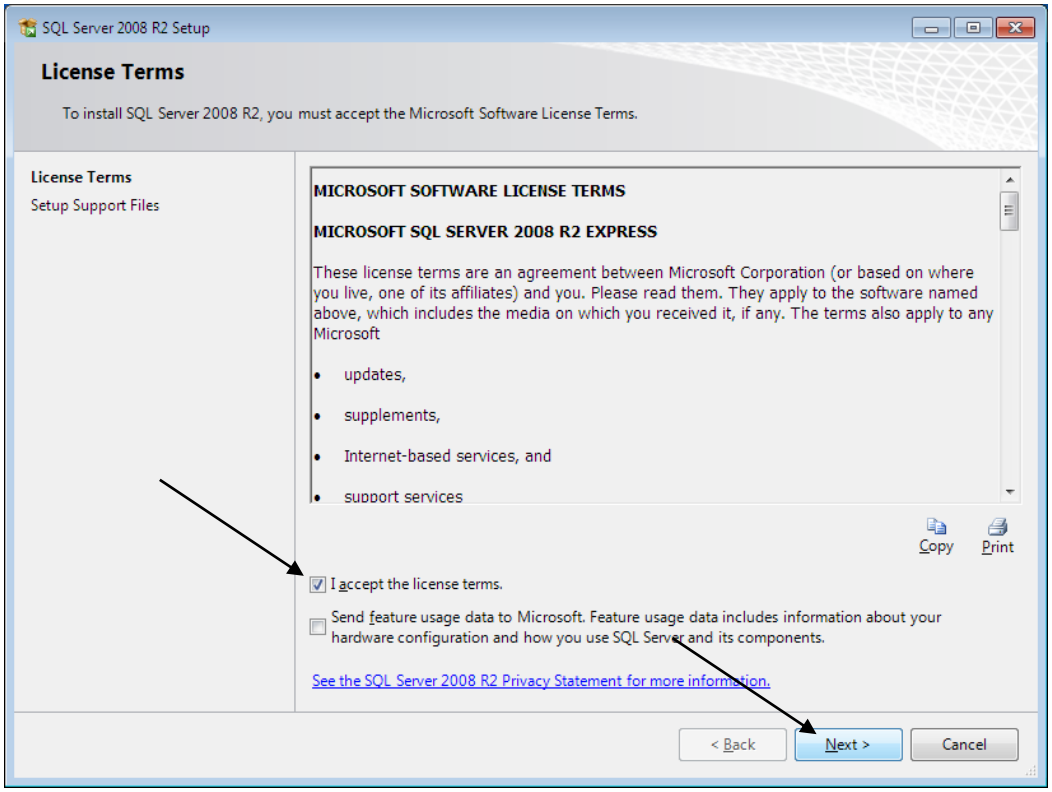




The 'SQL Server Installation Center' will be the starting point for either a fresh SQL Server installation or for upgrading from a previous SQL Server version.

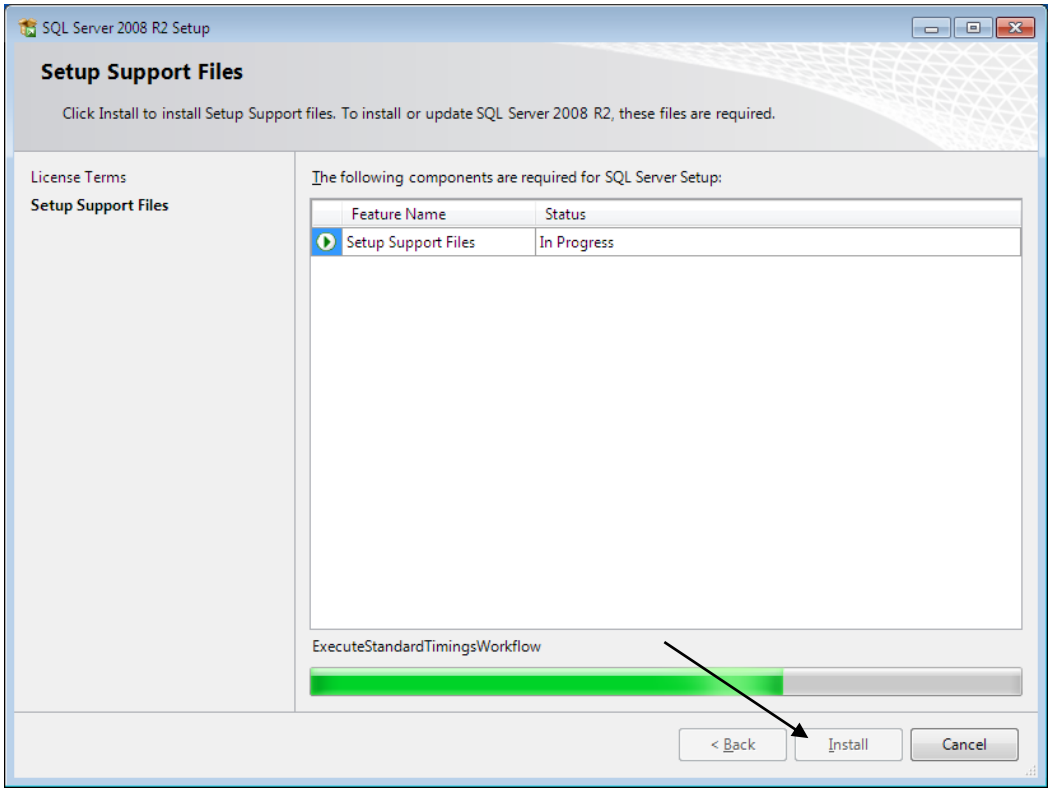


Double click the 'New SQL Server' to launch the installation wizard.

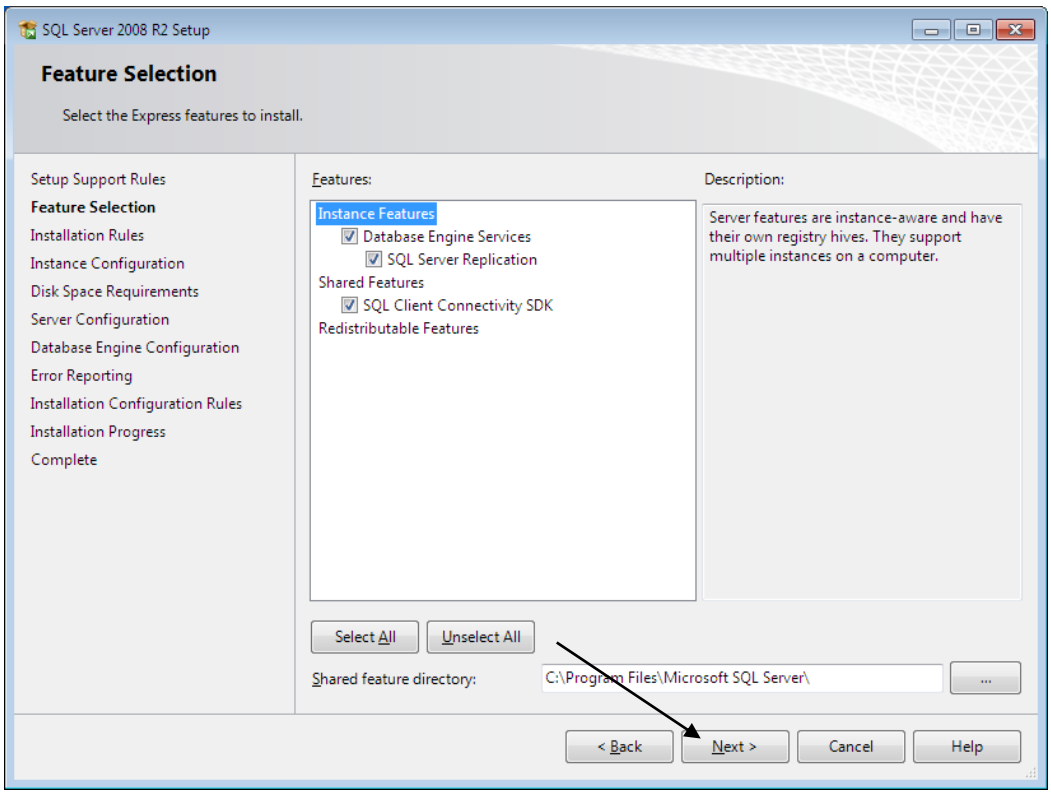


Check the "I accept the license terms." check-box and click the "Next" button.

The following screen indicates the setup files installation status. Click "Install" when finished.

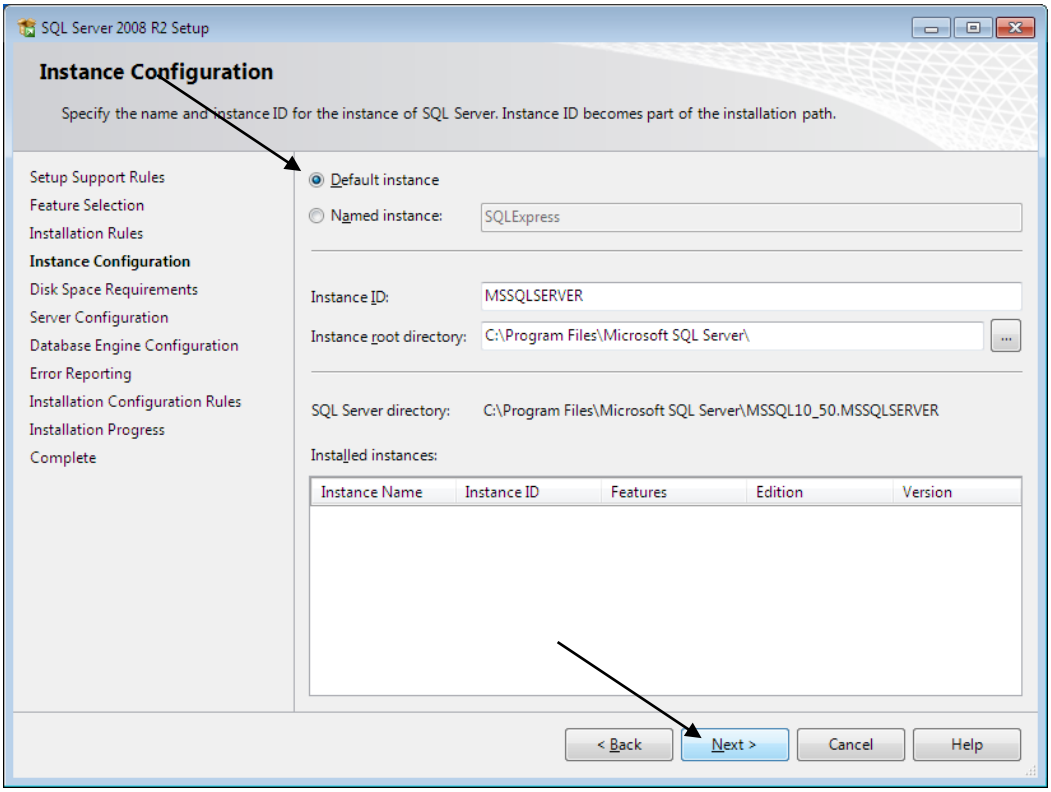


The following screen is for feature selection. Make sure all features are checked, then click "Next".

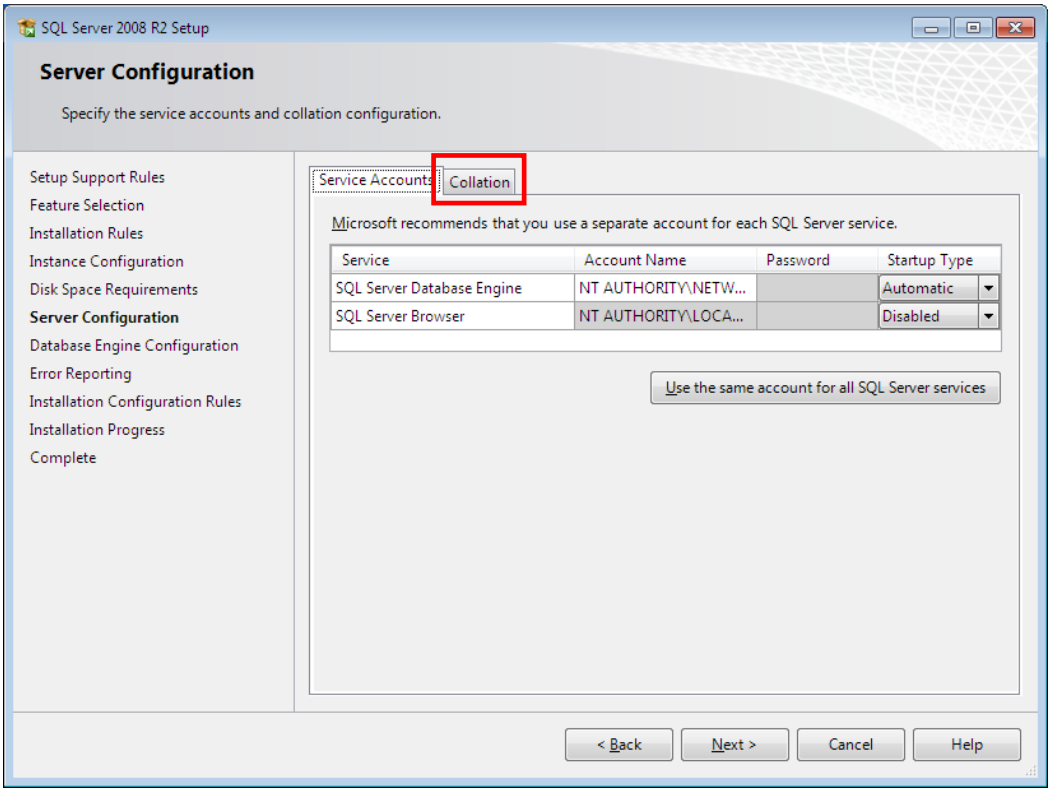


SQL Server 2008 requires MS Visual C++ 2008 Shell and if not on your system it will be installed from the installation files. SQL Server also requires .NET Framework 4.0 (on Windows 7). Make sure you have Internet access and this will also be installed automatically.

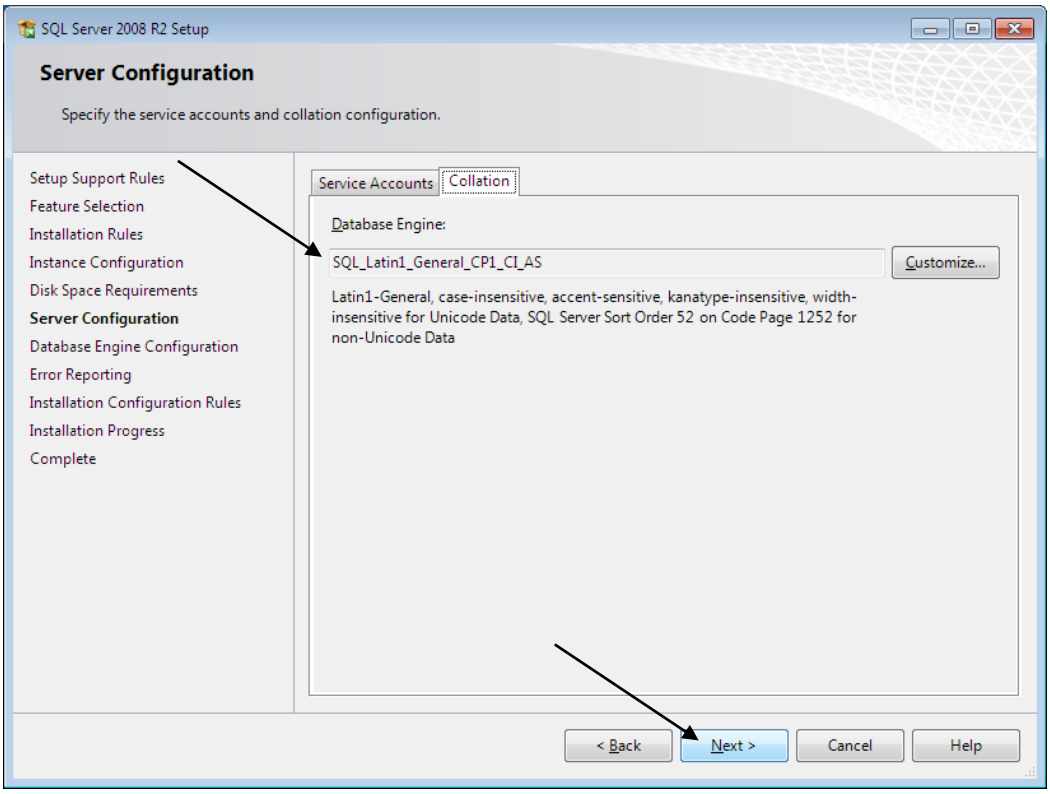
This screen shows the Instance Configuration. IMPORTANT!! Change the selection to "Default instance" then click "Next".



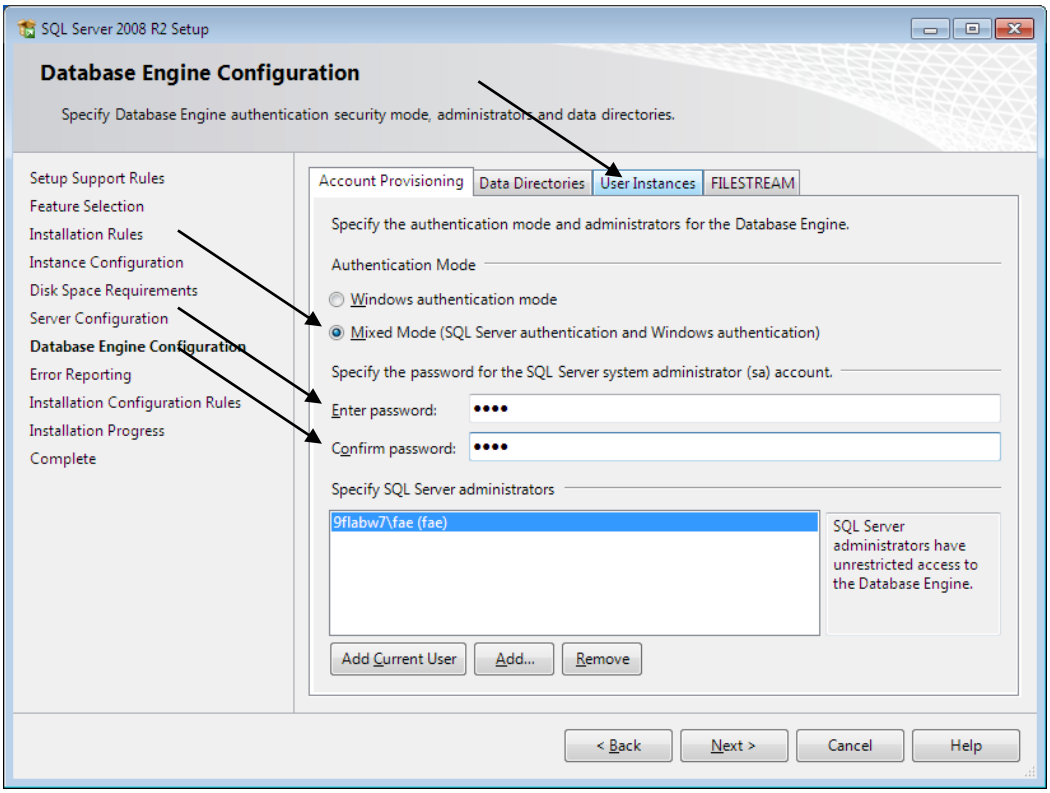
Here is the Server Configuration page. Check the "Collation" tab.



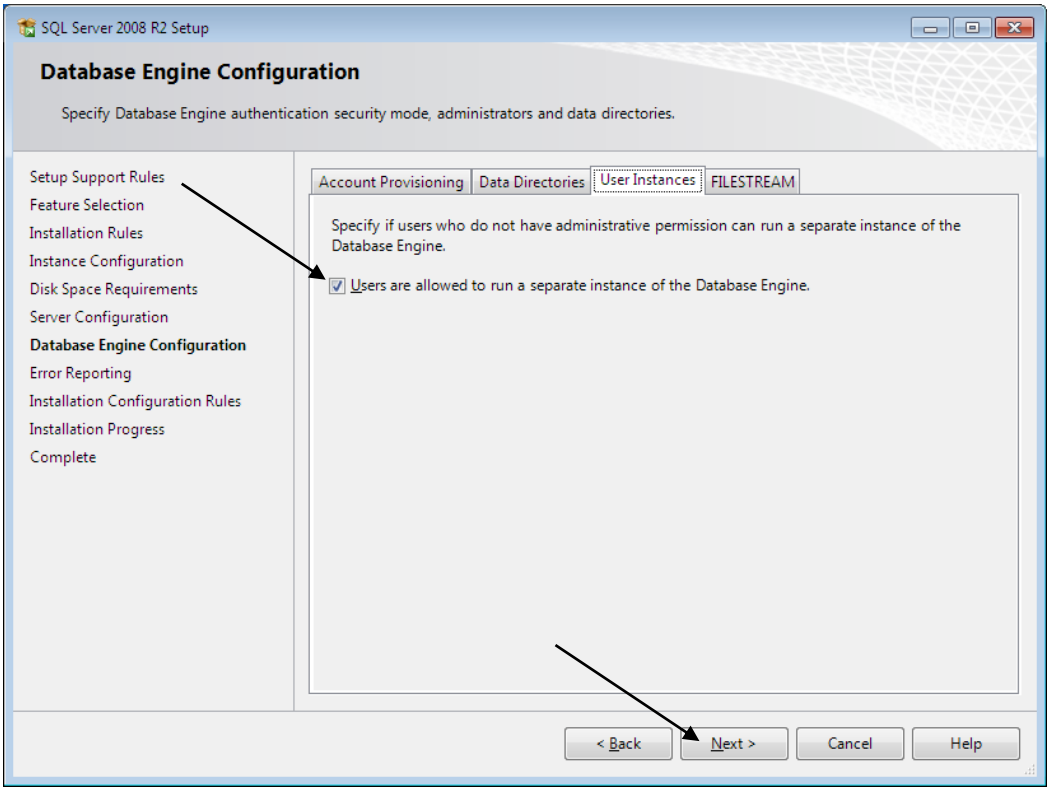
By default use the Latin1-General collation. Leave it for you OS detected language.



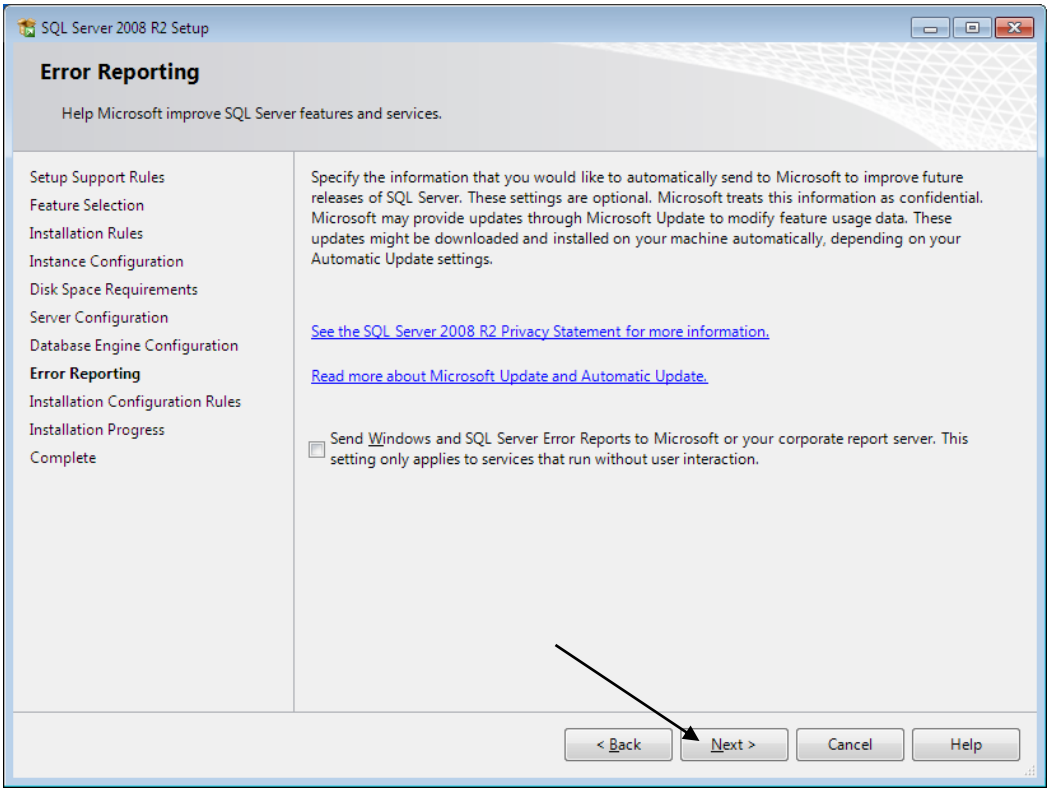
The following is the Database Engine Configuration. IMPORTANT!! Switch to "Mixed Mode" and enter the sa password twice. (throughout our examples we use a password of '0000' (four zeros). Check the "User Instances" tab.



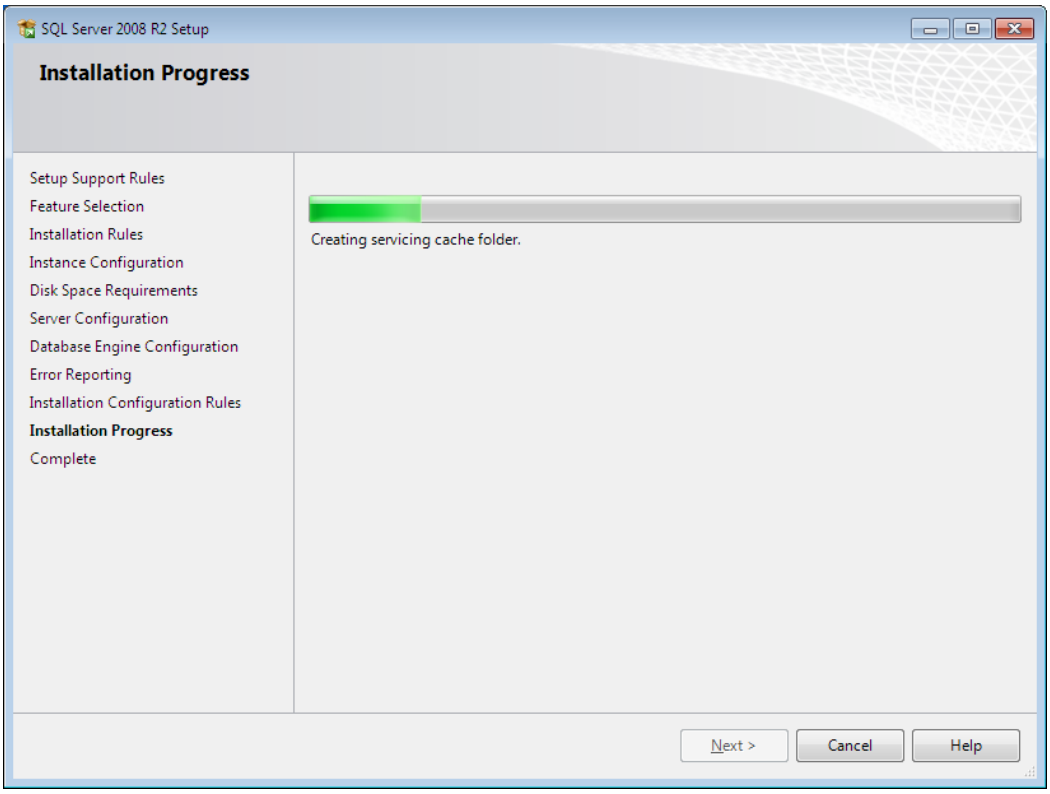
Make sure the check box is checked under "User Instances", then click "Next".



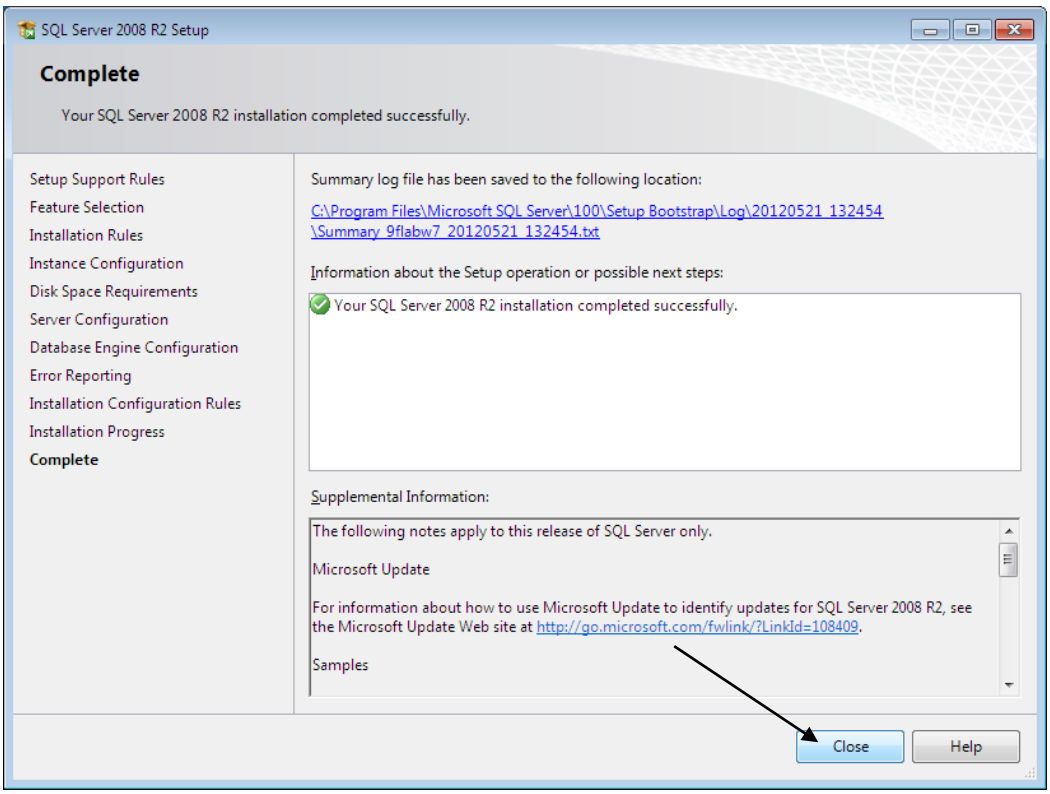
No need to check Error Reporting. Just click "Next".



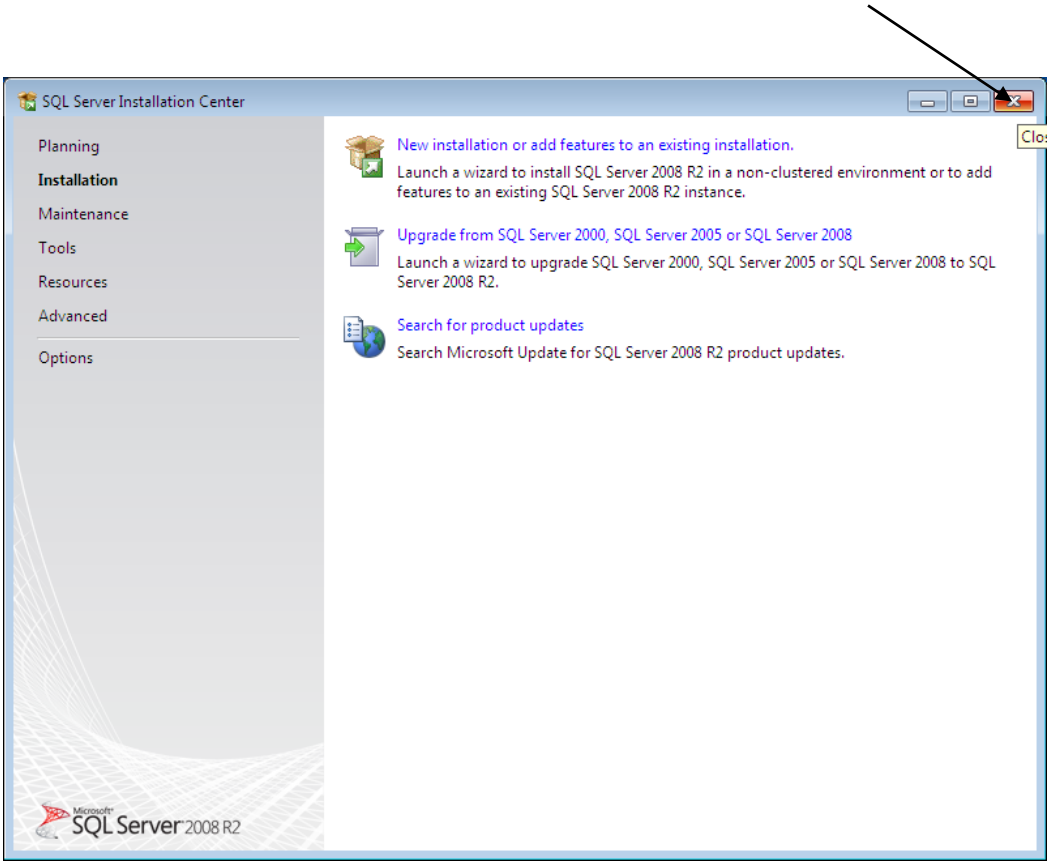
Now observe the Installation Progress. If any errors occur, click "OK" and "Retry"



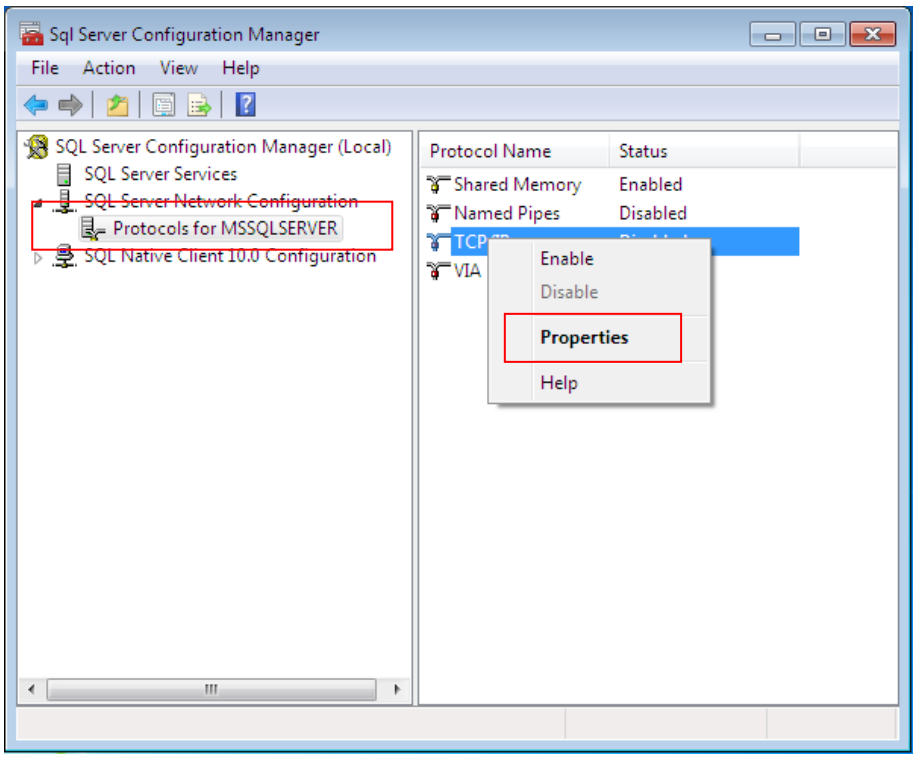
The application has now been installed. Click "Close".



Close the Installation Center window. **IMPORTANT: Don't forget your password for the 'sa' master account.**

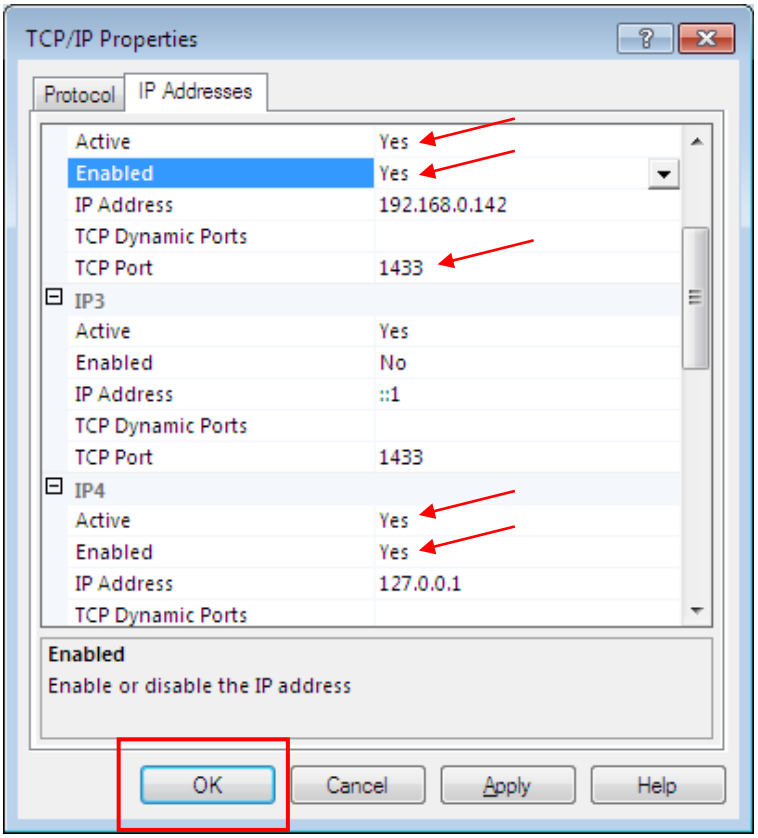


Now we recommend rebooting the machine. After rebooting, open the "SQL Configuration Manager" by clicking "Start > All Programs > Microsoft SQL Server 2008 R2 > Configuration Tools > **SQL Server Configuration Manager**". Find the "Protocols for MSSQLSERVER", under "SQL Server Network Configuration. Right-click on TCP/IP and select 'Properties'.



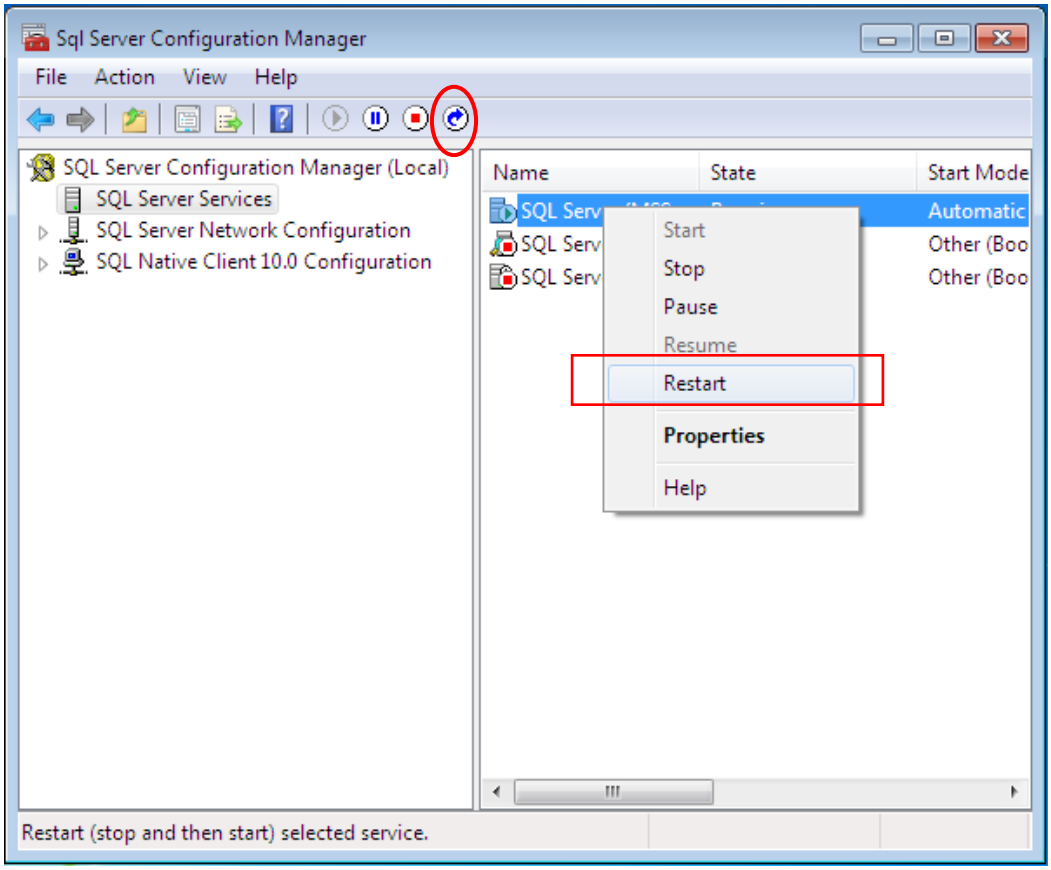
First, under the "Protocol" tab, make sure TCP/IP is enabled.

Next, under the "IP Address" tab, make sure the LAN port and Local Host connections are 'Active' and 'Enabled' and that the TCP Port is 1433.



Click "OK"

Restart the server after any configuration change. Highlight the SQL Server, Right-click and select "Restart" or just click the "Restart" icon.



This finishes the installation of MS-SQL 2008 R2 Express.

Appendix B Installing MS-SQL 2012 Express

B.1 Introduction

This chapter will detail the installation and configuration steps for the Free Edition of MS-SQL, Microsoft SQL Server 2012 Express Edition. Server Express is a powerful and reliable data management product that delivers rich features, data protection, and performance for embedded application clients, light Web applications, and local data stores. SQL Server 2012 is designed to run on Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2008 Service Pack 2, or Windows Vista Service Pack 2. SQL Server 2012 Express cannot be installed on Windows XP.

Note:

SQL Server 2012 Express Edition is differentiated from the rest of the SQL Server 2012 editions only by the following:

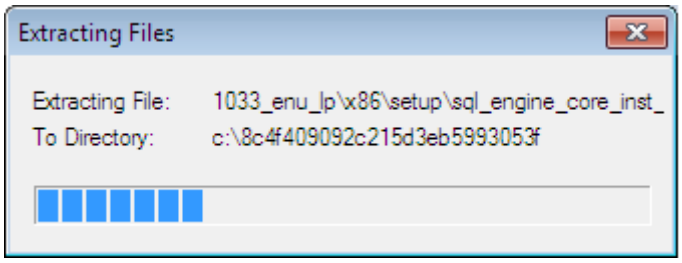
Lack of enterprise features support
Limited to one socket or 4 CPU cores
One GB memory limit for the SQL Server Engine
Databases have a 10 GB maximum size

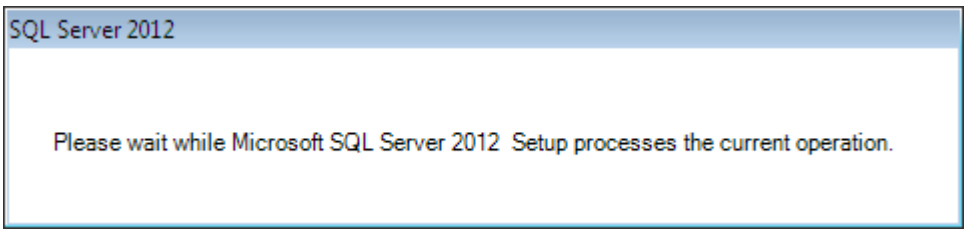
B.2 SQL Express Software Installation

In the following example, the step-by-step procedure is given for the free version of Microsoft® SQL Server 2012. The free version may be downloaded from Microsoft's Download Center website and is a good choice for demonstrating or for evaluating the EMS in a non-production environment. For production use, please have your purchased version of MS-SQL Server 2012 and CD-Key from your Certificate of Authenticity (COA) and follow through the Microsoft documentation for installation.

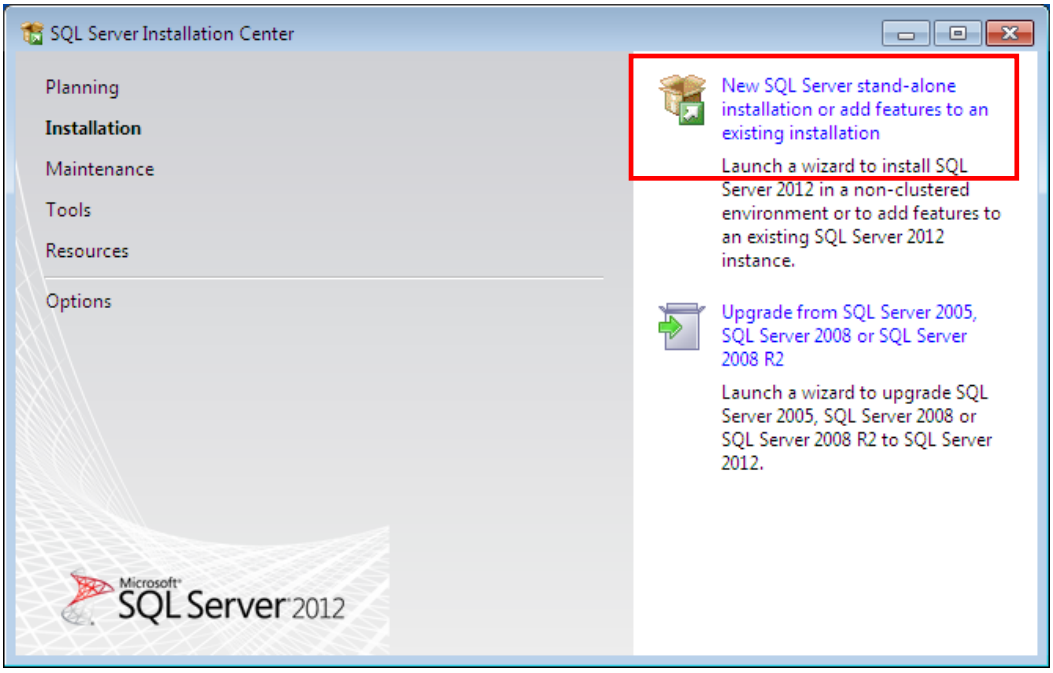
Find the location of your download files on the local disk and double-click into the ' SQLEXPR_x86_ENU.EXE' icon.

The downloaded file is a self-executable compressed file. First the files will be extracted to your system.

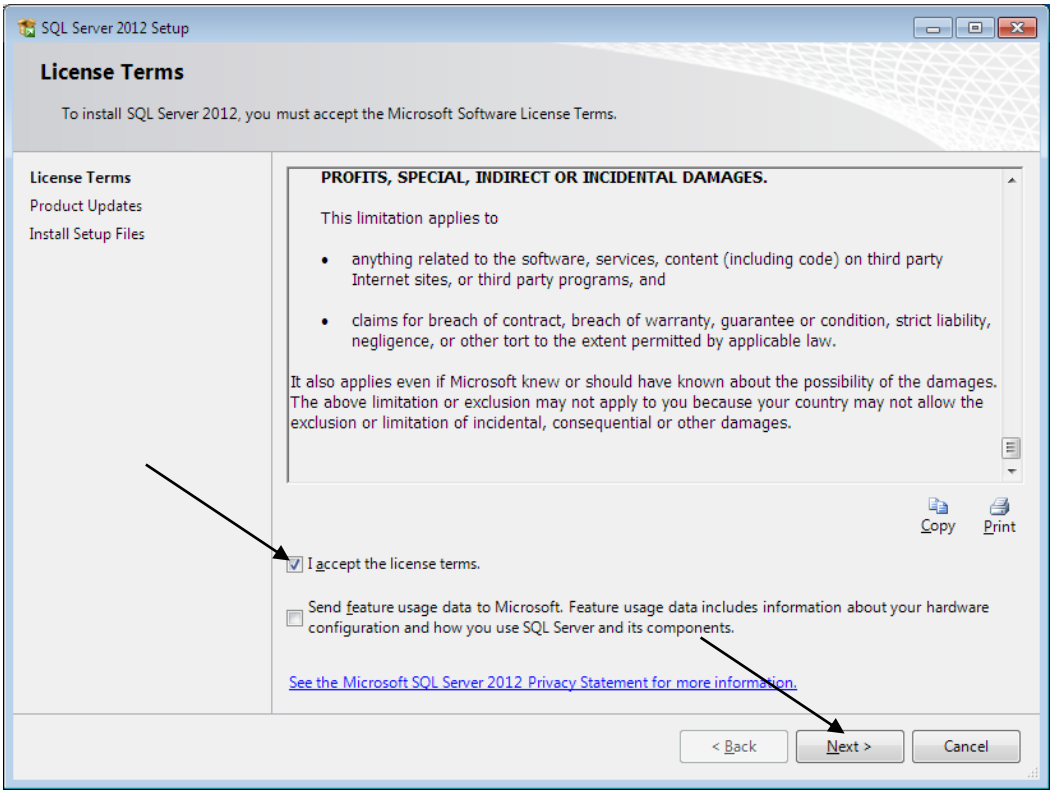




The 'SQL Server Installation Center' will be the starting point for either a fresh SQL Server installation or for upgrading from a previous SQL Server version.

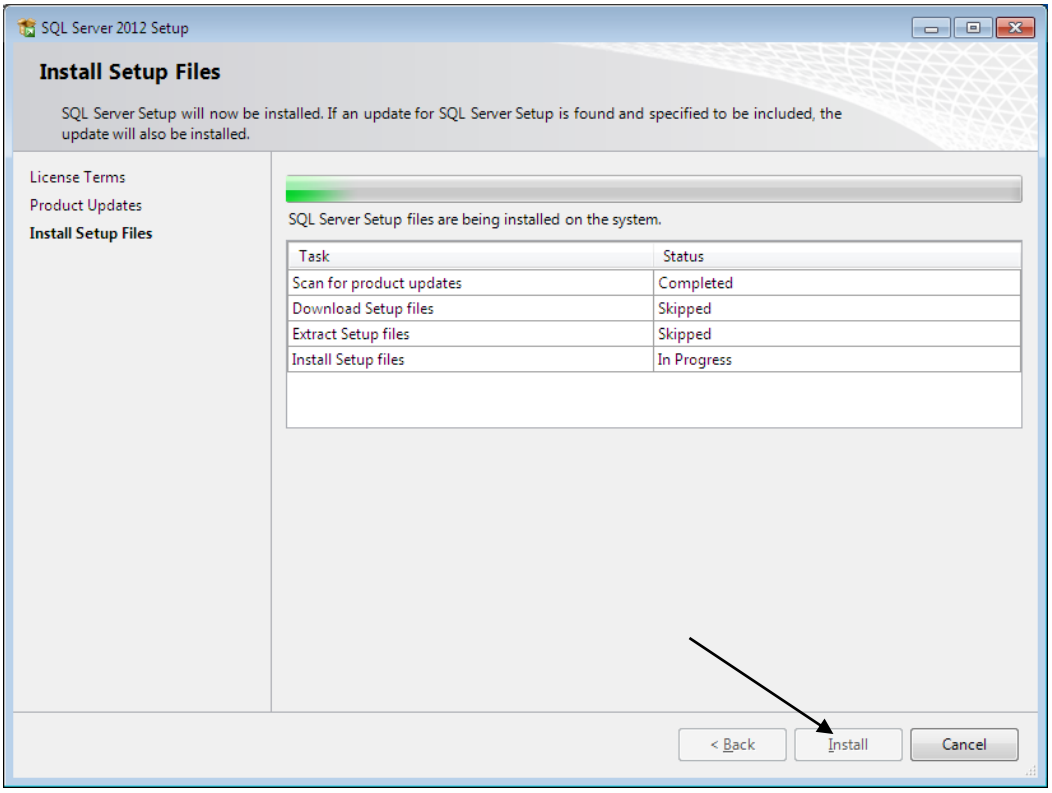


Double click the 'New SQL Server' to launch the installation wizard.

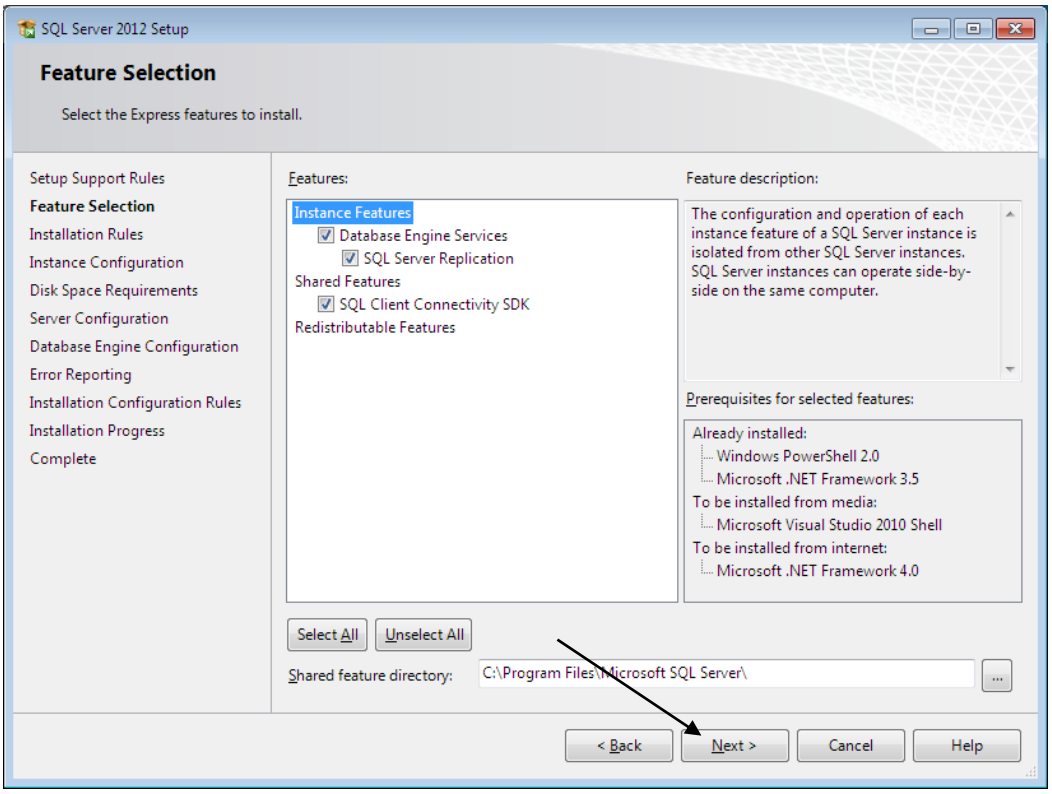


Check the "I accept the license terms." check-box and click the "Next" button.

The following screen indicates the setup files installation status. Click "Install" when finished.

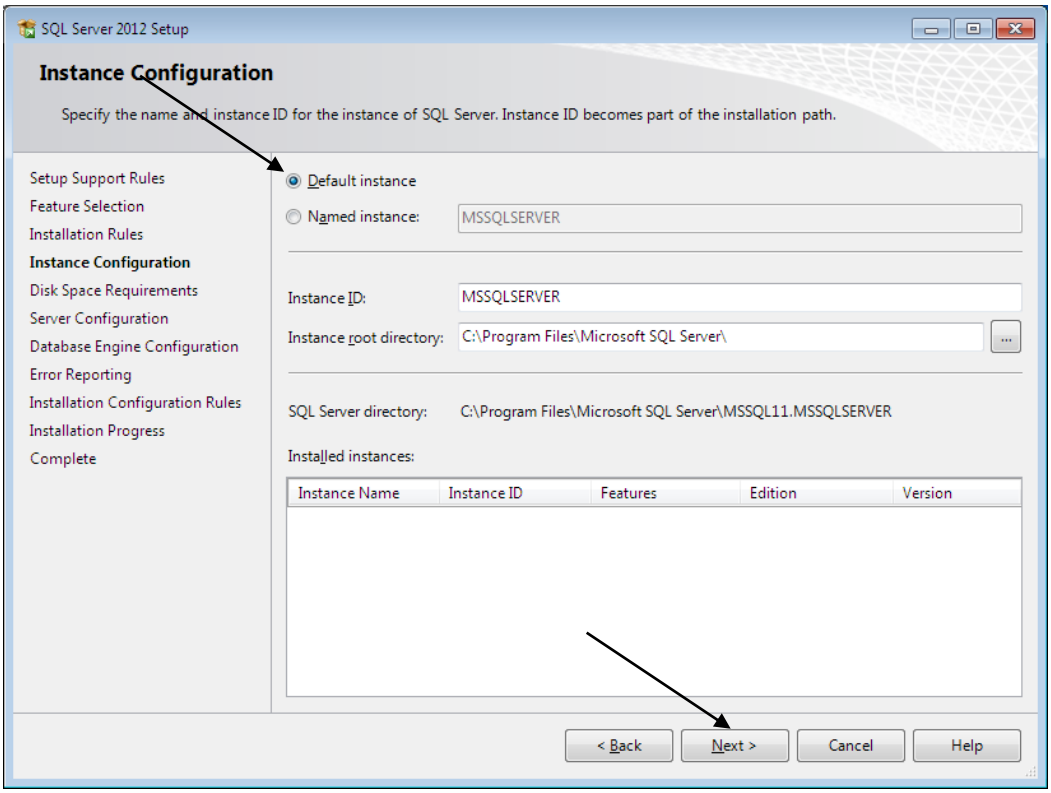


The following screen is for feature selection. Make sure all features are checked, then click "Next".

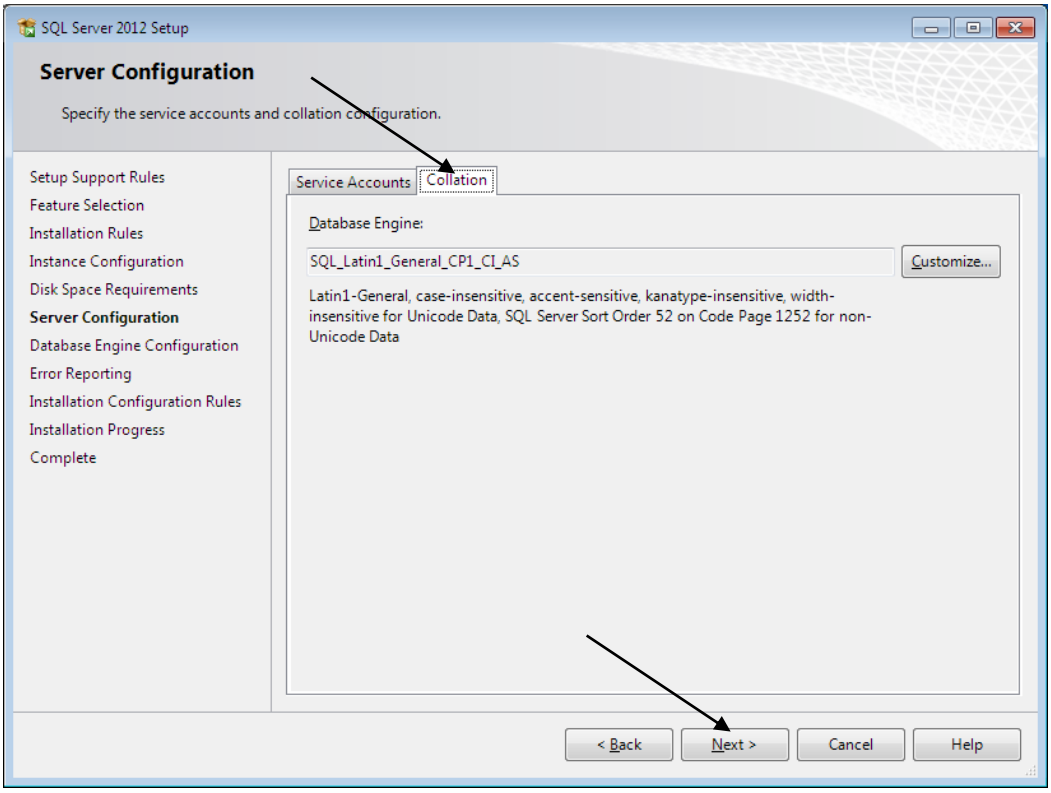


SQL Server 2012 requires MS Visual Studio 2010 Shell and if not on your system it will be installed from the installation files. SQL Server also requires .NET Framework 4.0. Make sure you have Internet access and this will also be installed automatically.

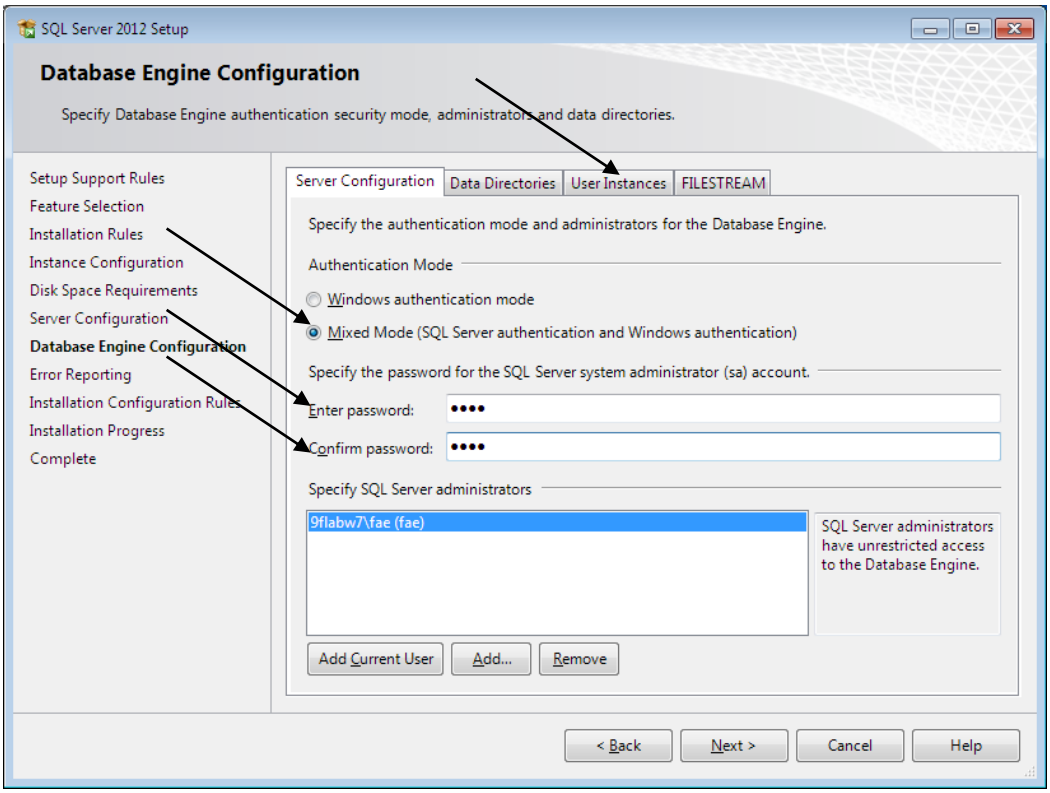
This screen shows the Instance Configuration. IMPORTANT!! Change the selection to "Default instance" then click "Next".



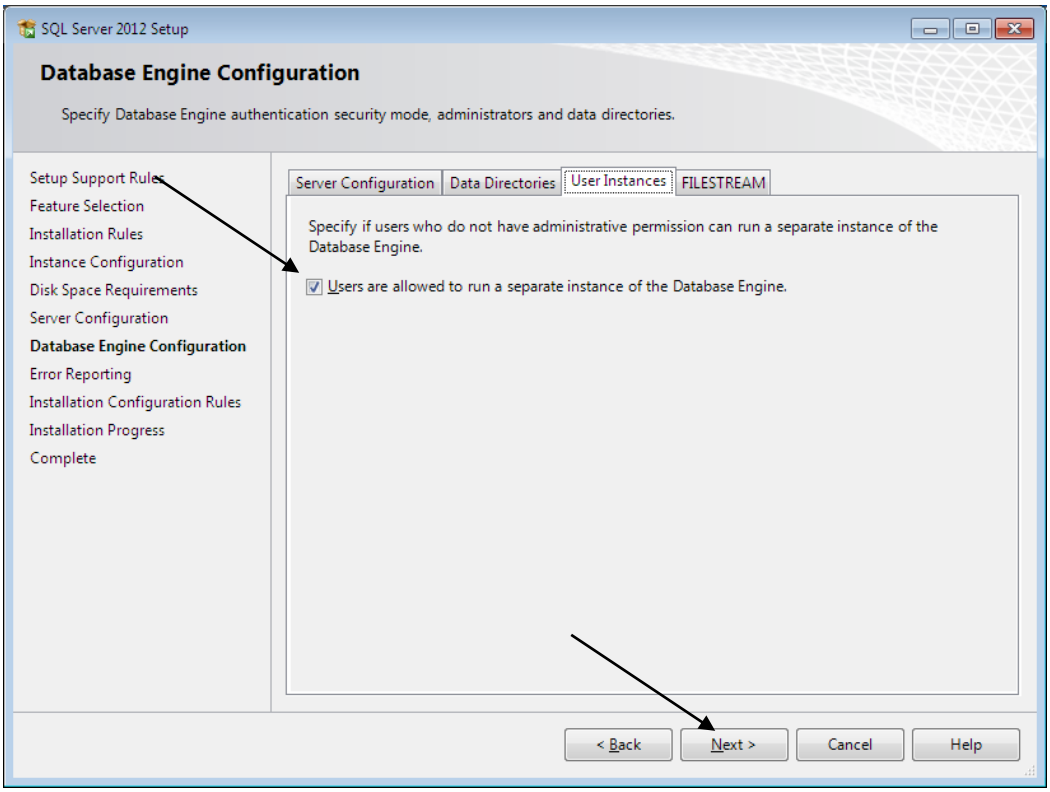
Here is the Server Configuration page. Check the "Collation" tab and use the default automatically found for you OS language.



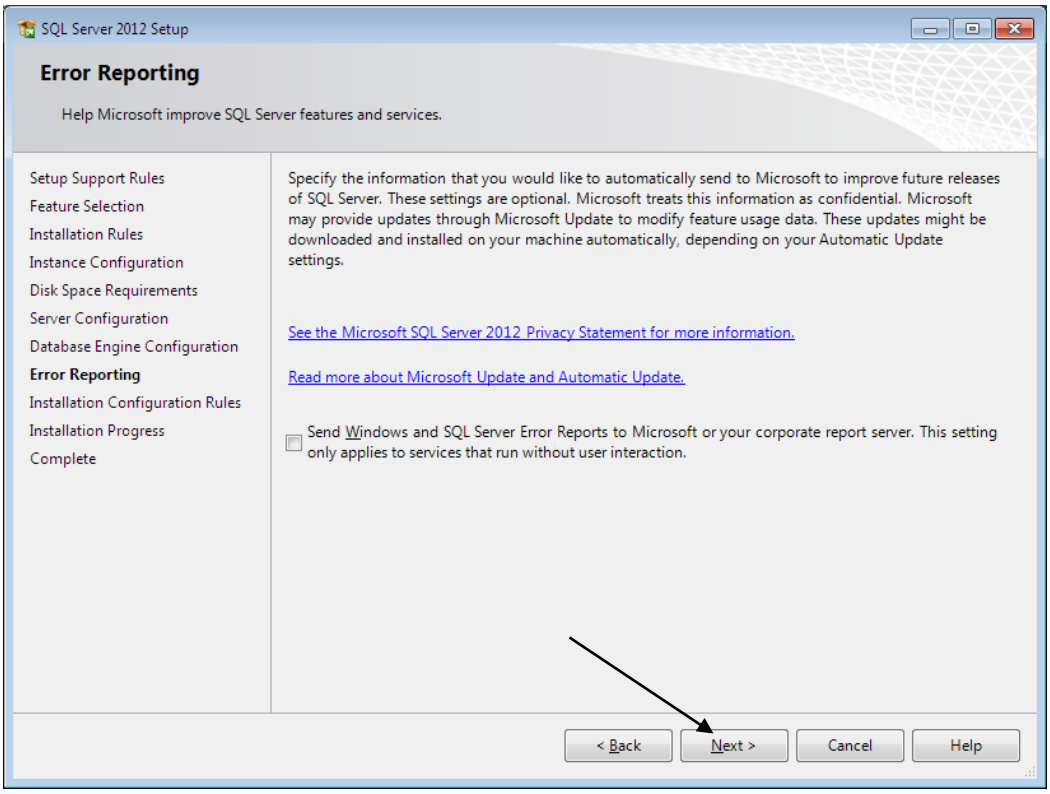
The following is the Database Engine Configuration. IMPORTANT!! Switch to "Mixed Mode" and enter the sa password twice. (throughout our examples we use a password of '0000' (four zeros). Check the "User Instances" tab.



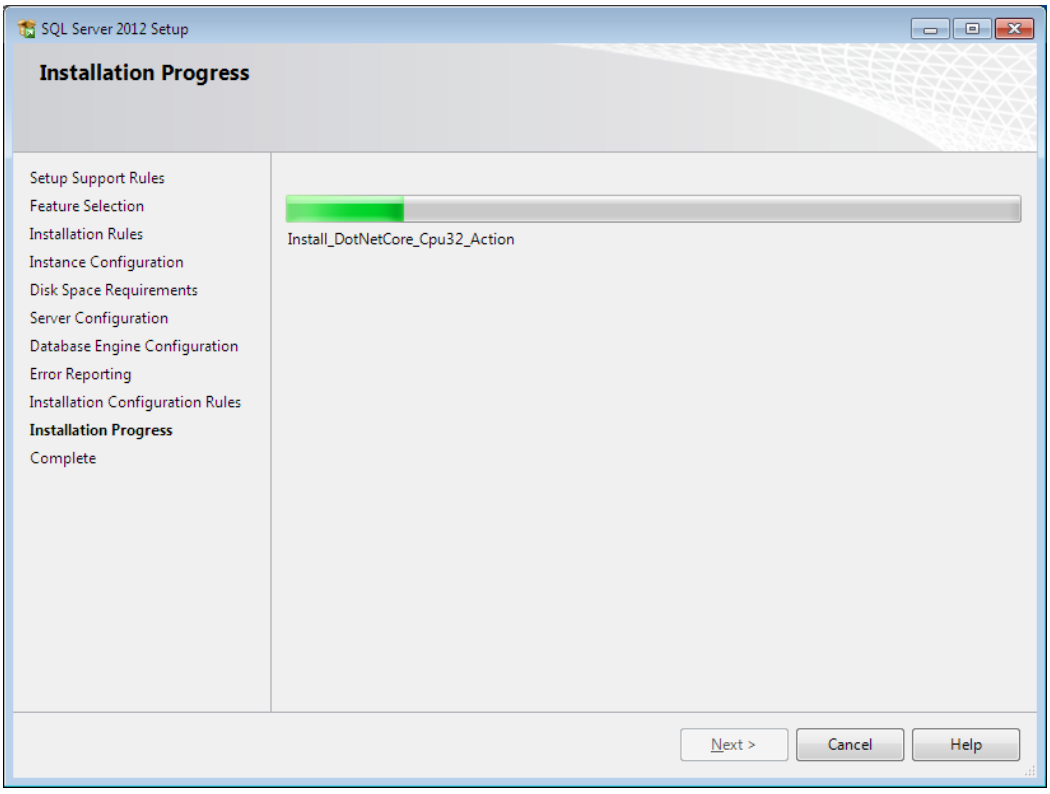
Make sure the check box is checked under "User Instances", then click "Next".



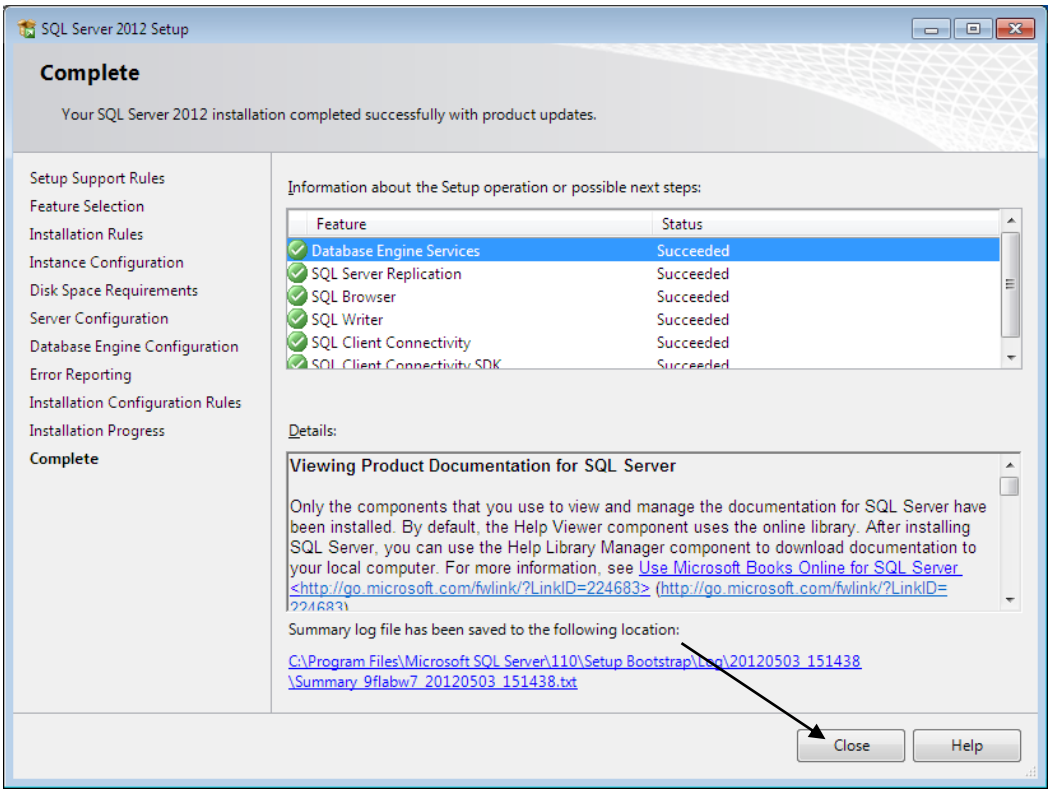
No need to check Error Reporting. Just click "Next".



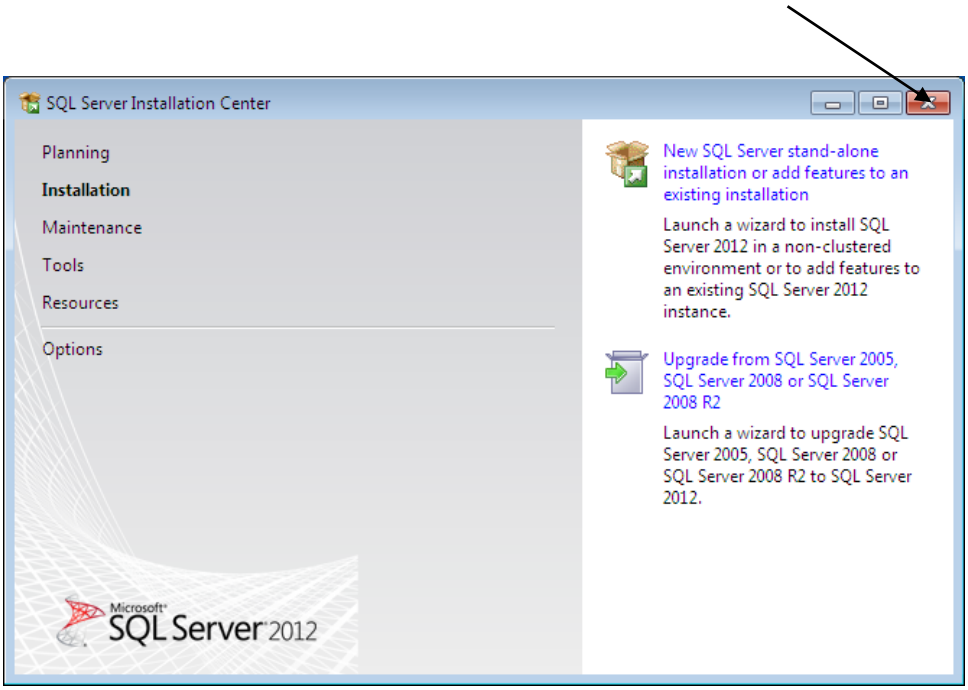
Now observe the Installation Progress. If any errors occur, click "OK" and "Retry"



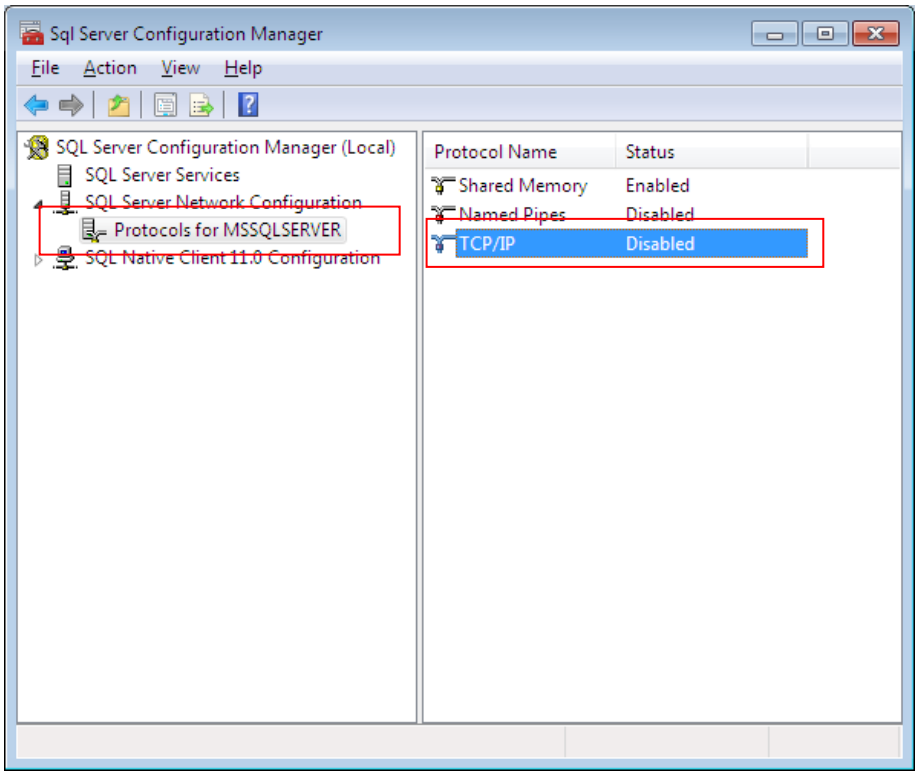
The application has now been installed. Click "Close".



Close the Installation Center window. **IMPORTANT: Don't forget your password for the 'sa' master account.**

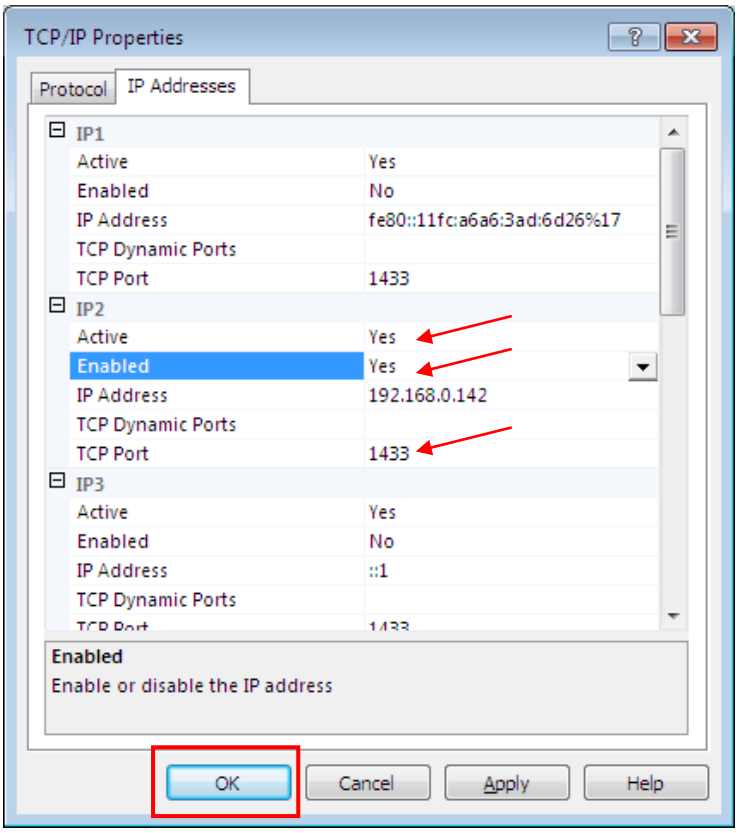


Now we recommend rebooting the machine. After rebooting, open the "SQL Configuration Manager" by clicking "Start > All Programs > Microsoft SQL Server 2012 > Configuration Tools > **SQL Server Configuration Manager**". Find the "Protocols for SQLEXPRESS". Right-click on TCP/IP and select 'Properties'.



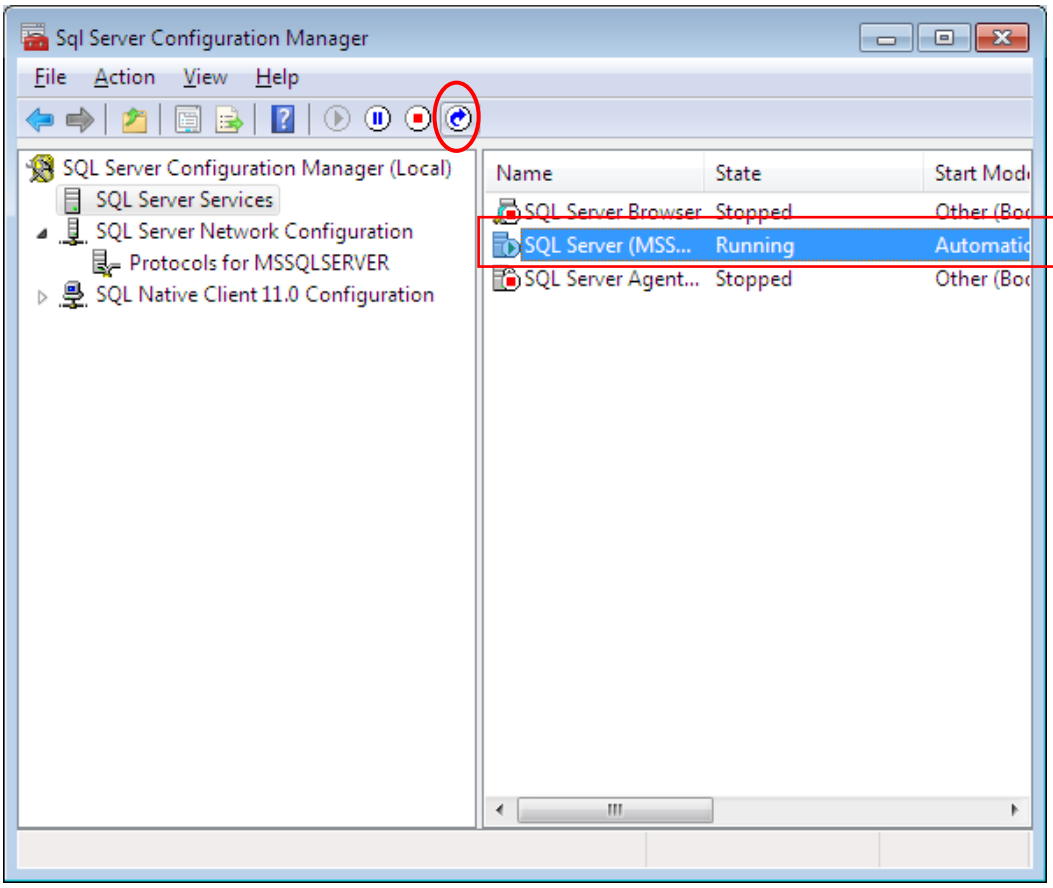
First, under the "Protocol" tab, make sure TCP/IP is enabled.

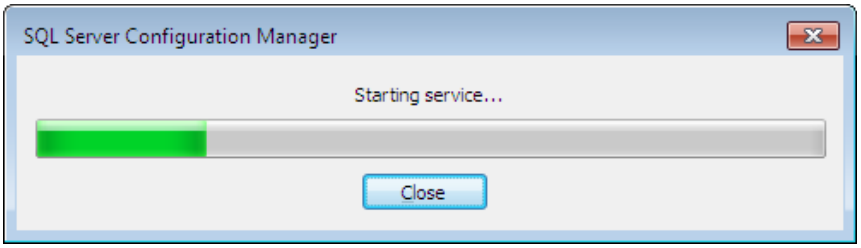
Next, under the "IP Address" tab, make sure the LAN port and Local Host connections are 'Active' and 'Enabled' and that the TCP Port is 1433.



Click "OK"

Restart the server after any configuration change. Highlight the SQL server, right-click and select Restart or just click the "Restart" icon.





The SQL Server will restart and run with the new configuration.

This completes the installation of SQL2012 Express.

Appendix C Installing MS-SQL 2014 Express

C.1 Introduction

This chapter will detail the installation and configuration steps for the Free Edition of MS-SQL, Microsoft SQL Server 2014 Express Edition. Server Express is a powerful and reliable data management product that delivers rich features, data protection, and performance for embedded application clients, light Web applications, and local data stores. SQL Server 2014 is designed to run on Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2008 R2 Service Pack 1, Windows Server 2012, or Windows Server 2012 R2. SQL Server 2014 Express cannot be installed on Windows XP, Vista Windows 7 or Windows 8.

Note:

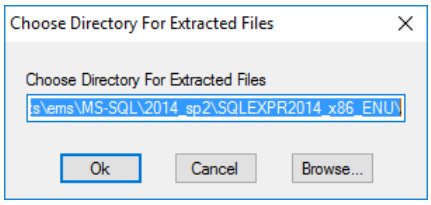
SQL Server 2014 Express Edition is differentiated from the rest of the SQL Server 2014 editions only by the following:

Lack of enterprise features support
Limited to one socket or 4 CPU cores
One GB memory limit for the SQL Server Engine
Databases have a 10 GB maximum size

C.2 SQL Express Software Installation

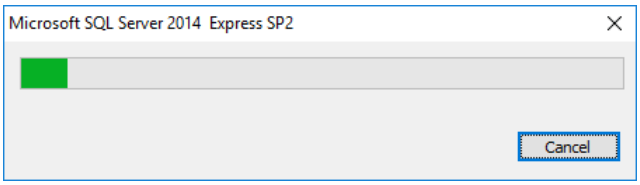
In the following example, the step-by-step procedure is given for the free version of Microsoft® SQL Server 2014. The free version may be downloaded from Microsoft's Download Center website and is a good choice for demonstrating or for evaluating the EMS in a non-production environment. For production use, please have your purchased version of MS-SQL Server 2014 and CD-Key from your Certificate of Authenticity (COA) and follow through the Microsoft documentation for installation.

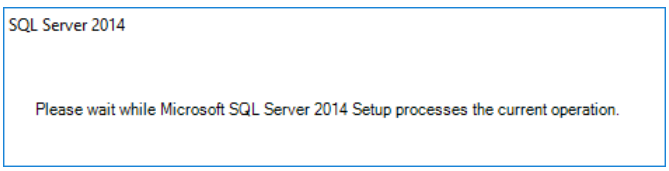
Find the location of your download files on the local disk and double-click into the ' SQLEXPR_x86_ENU.EXE' icon.



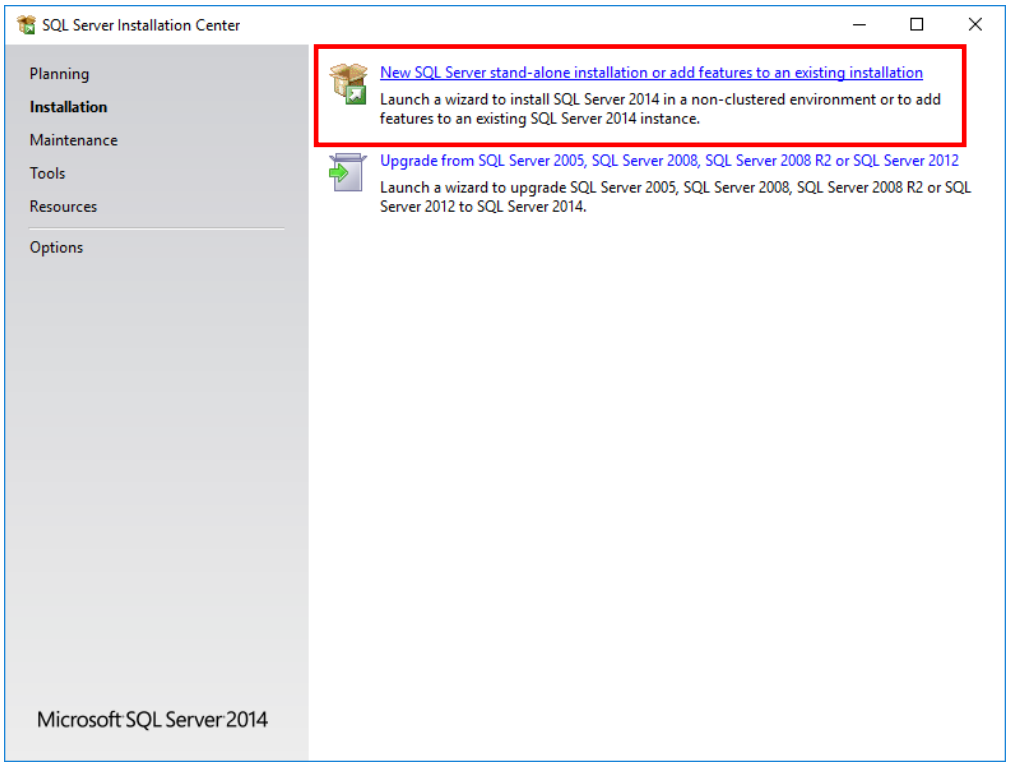
Starting with SQL Server 2014 an extraction directory can be manually selected. If the downloaded file is on a writable media with enough space, just click "OK".

The downloaded file is a self-executable compressed file. First the files will be extracted to your system.

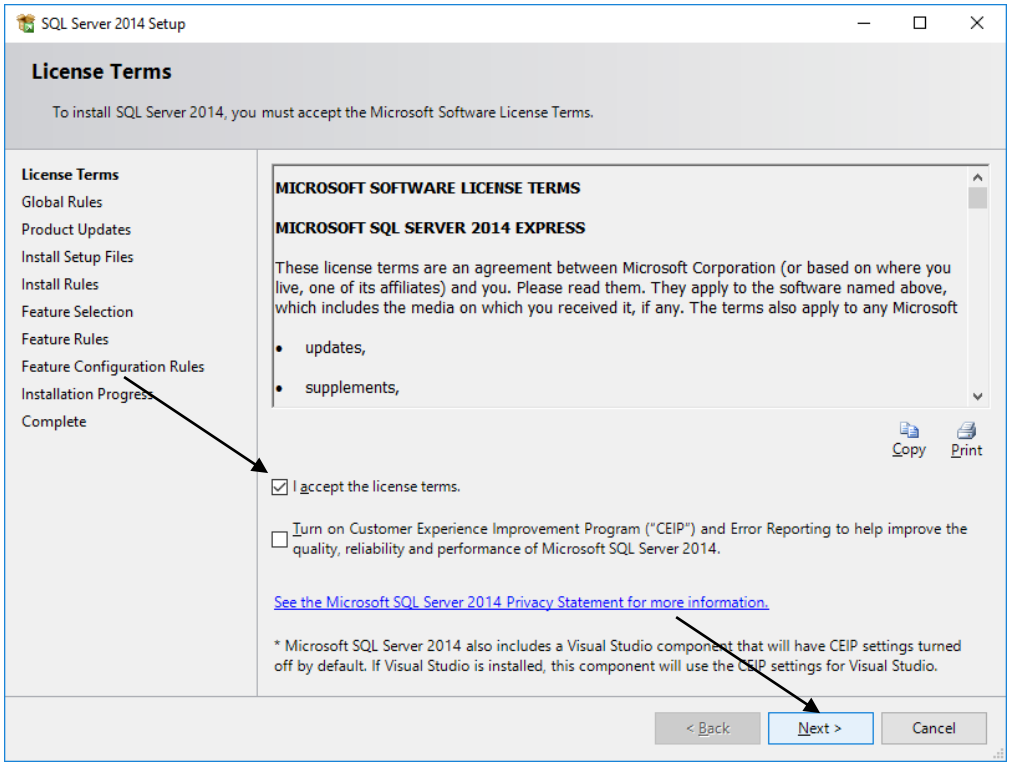




The 'SQL Server Installation Center' will be the starting point for either a fresh SQL Server installation or for upgrading from a previous SQL Server version.

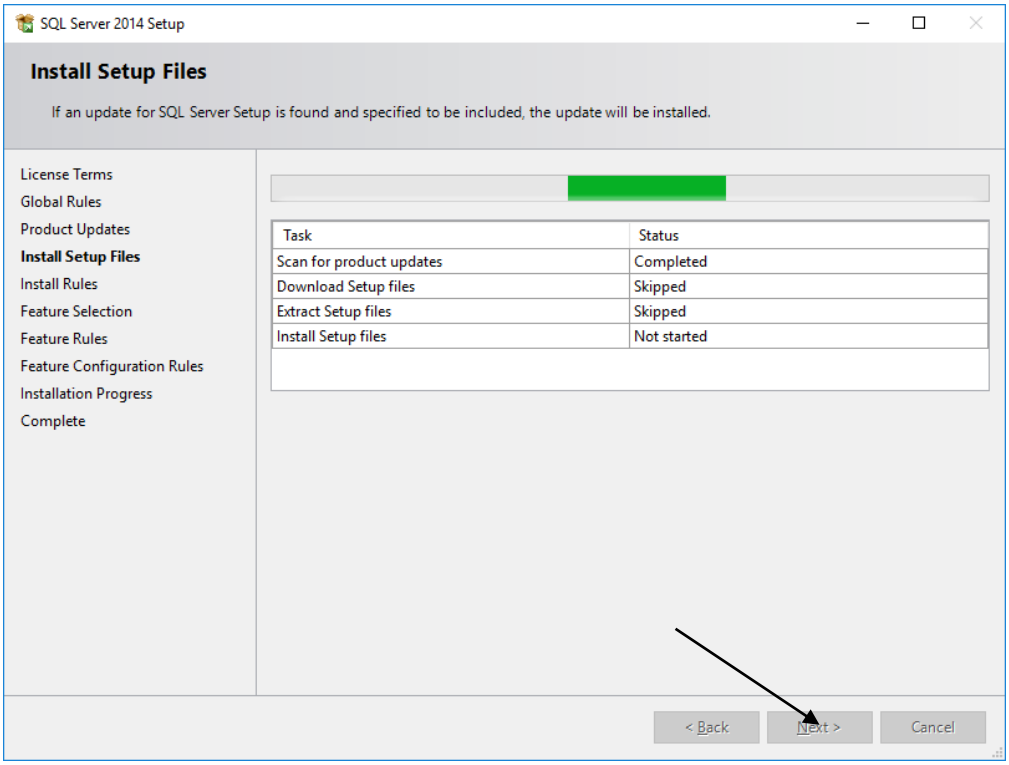


Double click the 'New SQL Server' to launch the installation wizard.

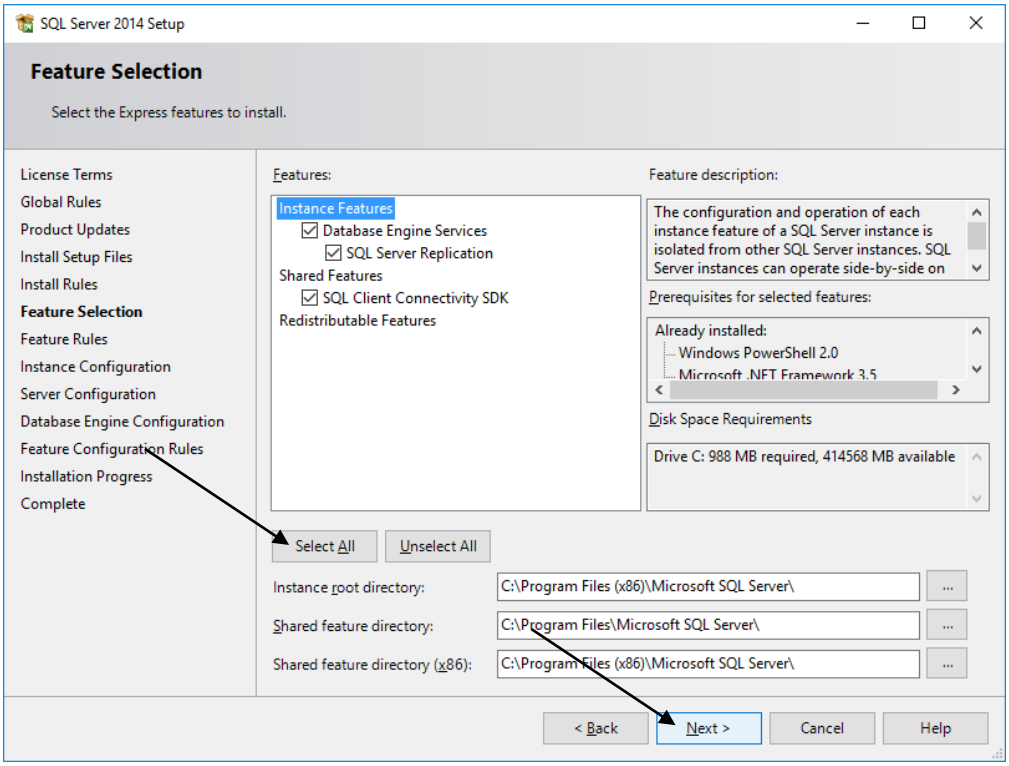


Check the "I accept the license terms." check-box and click the "Next" button.

The following screen indicates the setup files installation status. Click "Install" when finished.

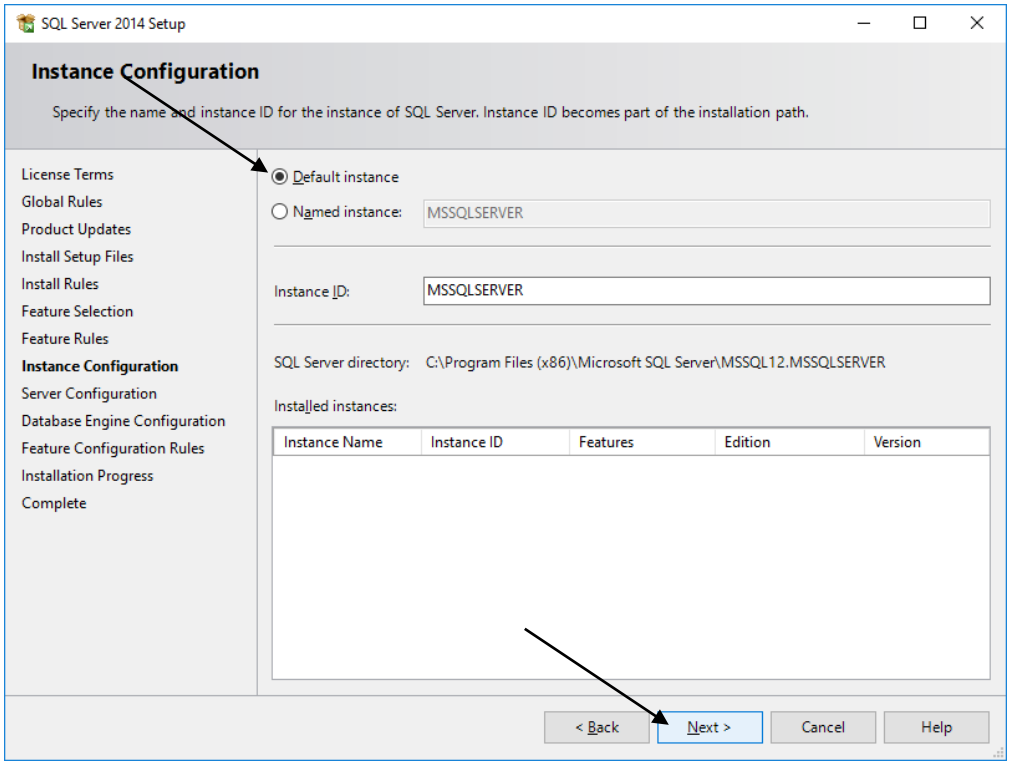


The following screen is for feature selection. Make sure all features are checked, then click "Next".

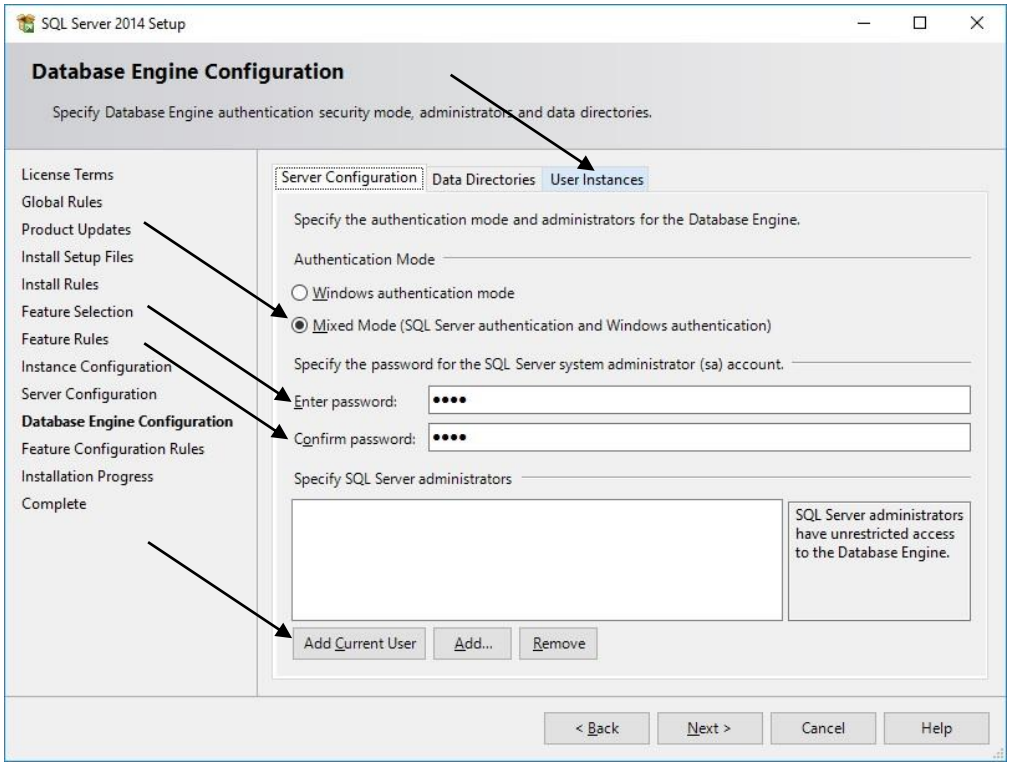


SQL Server 2014 requires MS Visual Studio 2010 Shell and if not on your system it will be installed from the installation files. SQL Server also requires .NET Framework 4.0. Make sure you have Internet access and this will also be installed automatically.

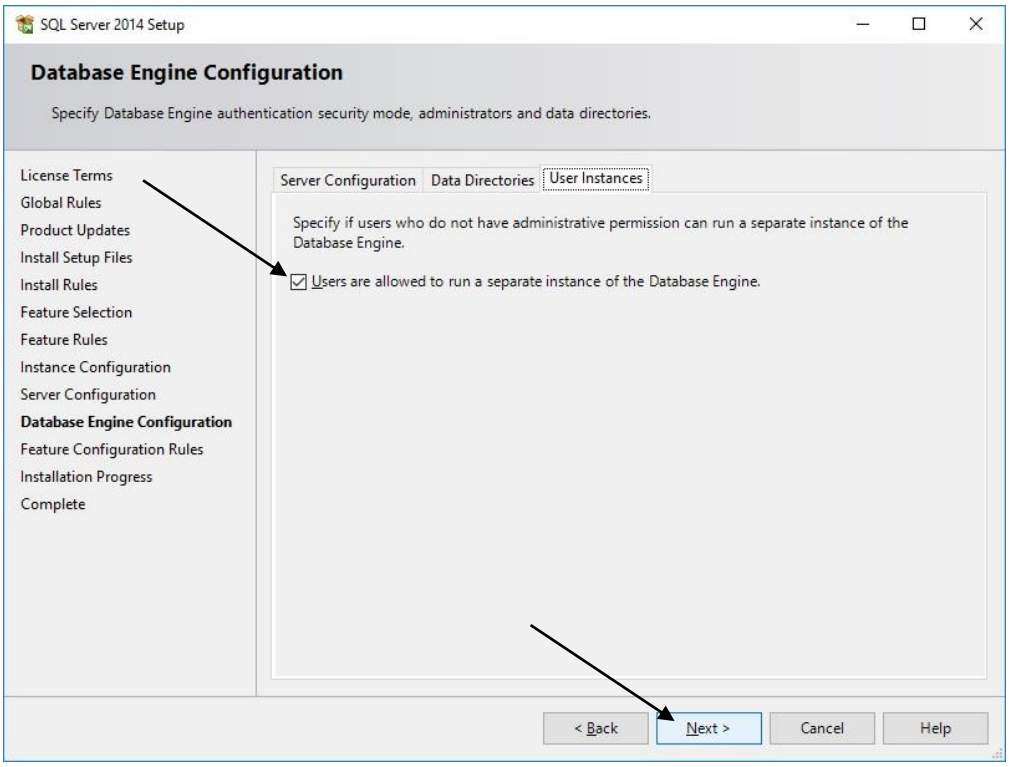
This screen shows the Instance Configuration. IMPORTANT!! Change the selection to "Default instance" then click "Next".



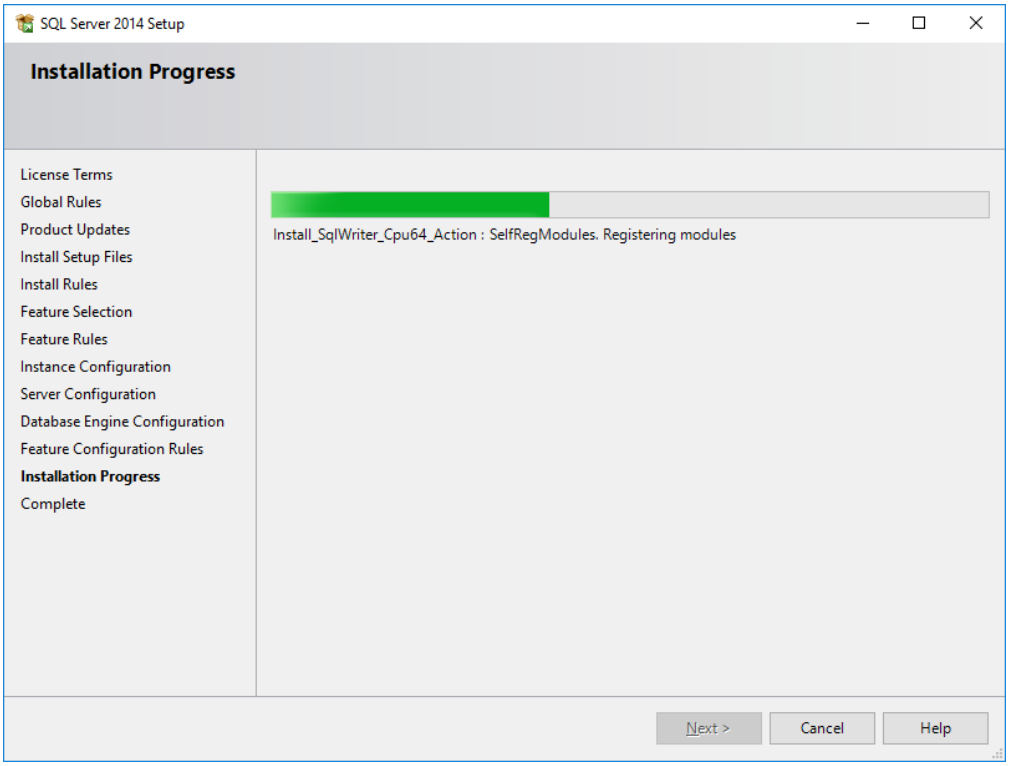
The following is the Database Engine Configuration. IMPORTANT!! Switch to "Mixed Mode" and enter the sa password twice. (throughout our examples we use a password of '0000' (four zeros). Be sure to "Add Current User" as a specific SQL Server administrator. Check the "User Instances" tab.



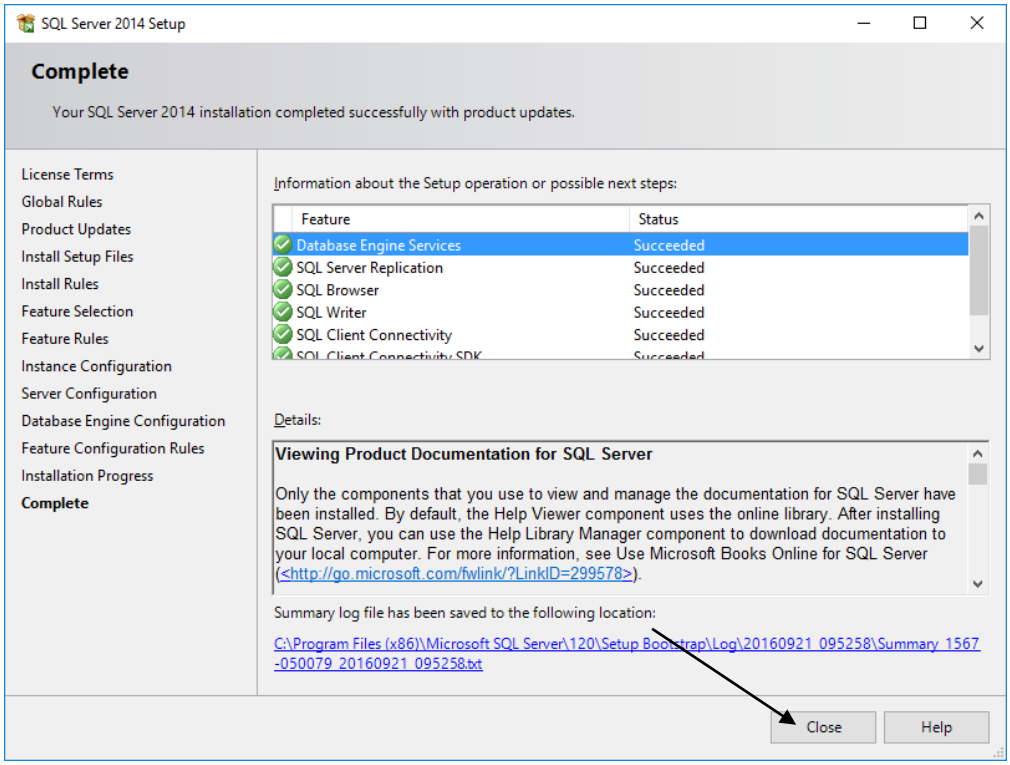
Make sure the check box is checked under "User Instances", then click "Next".



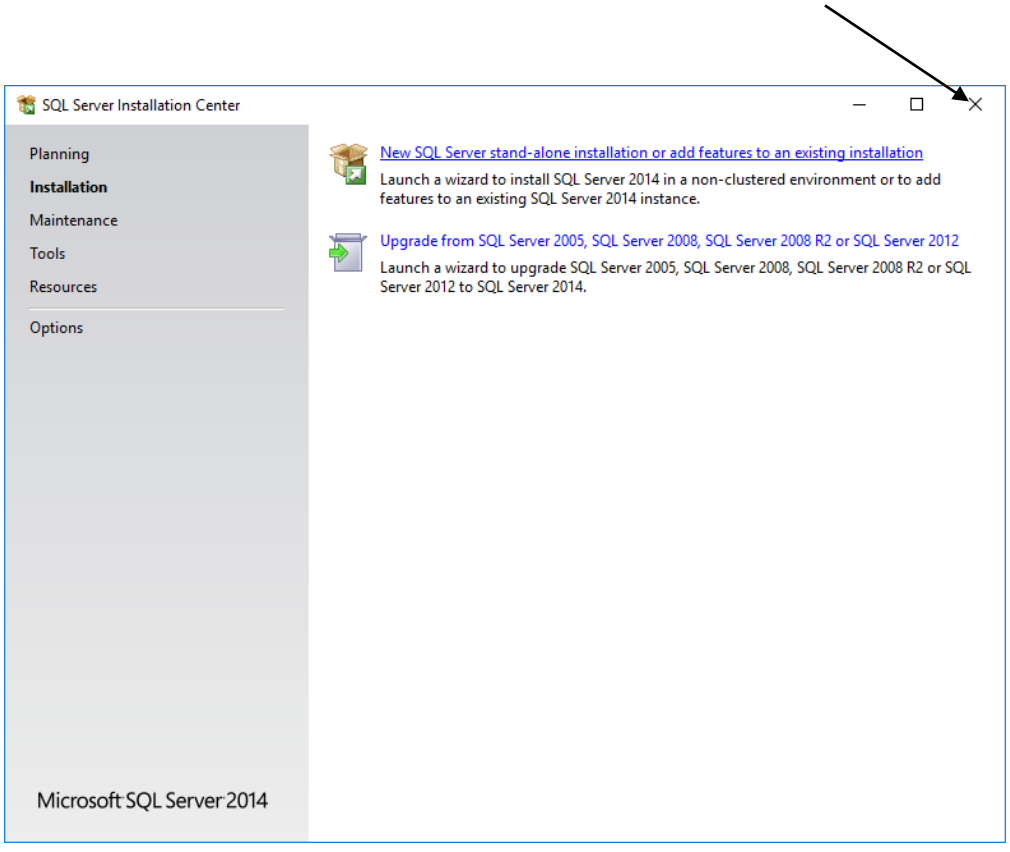
Now observe the Installation Progress. If any errors occur, click "OK" and "Retry"



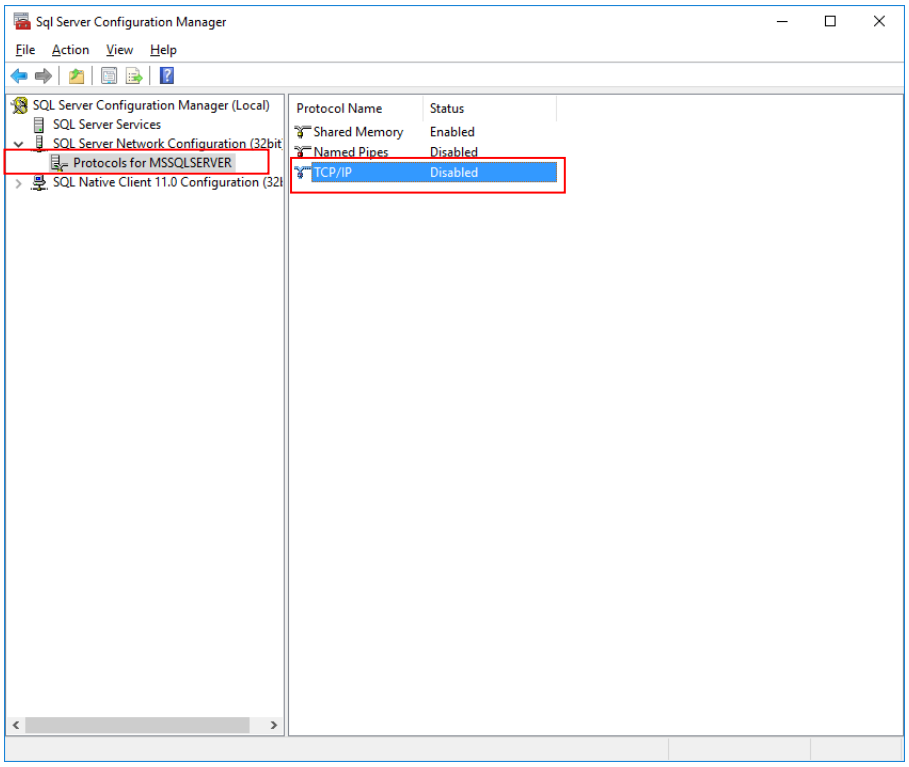
The application has now been installed. Click "Close".



Close the Installation Center window. **IMPORTANT: Don't forget your password for the 'sa' master account.**

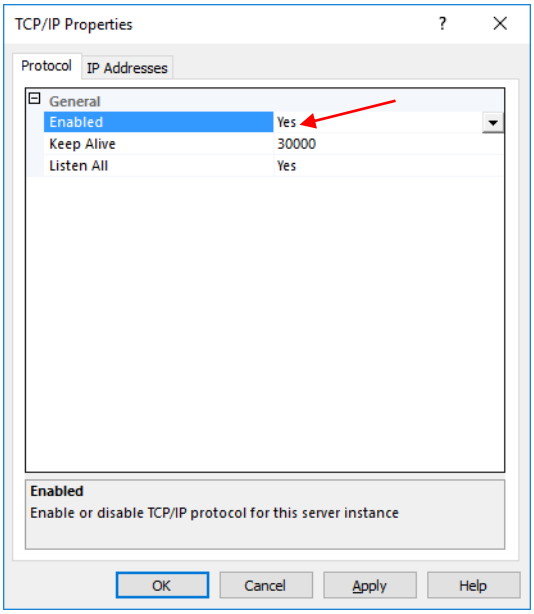


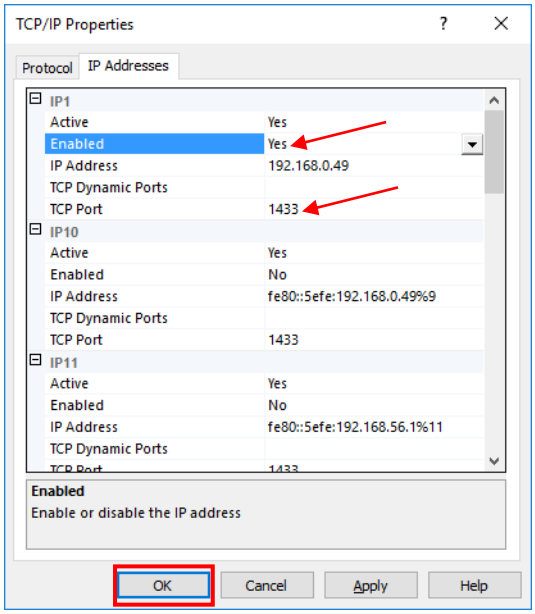
Now reboot the machine. After rebooting, open the "SQL Configuration Manager" by clicking "Start > All Apps > Microsoft SQL Server 2012 > **SQL Server Configuration Manager**". Find the "Protocols for SQLEXPRESS". Right-click on TCP/IP and select 'Properties'.



First, under the "Protocol" tab, make sure TCP/IP is enabled.

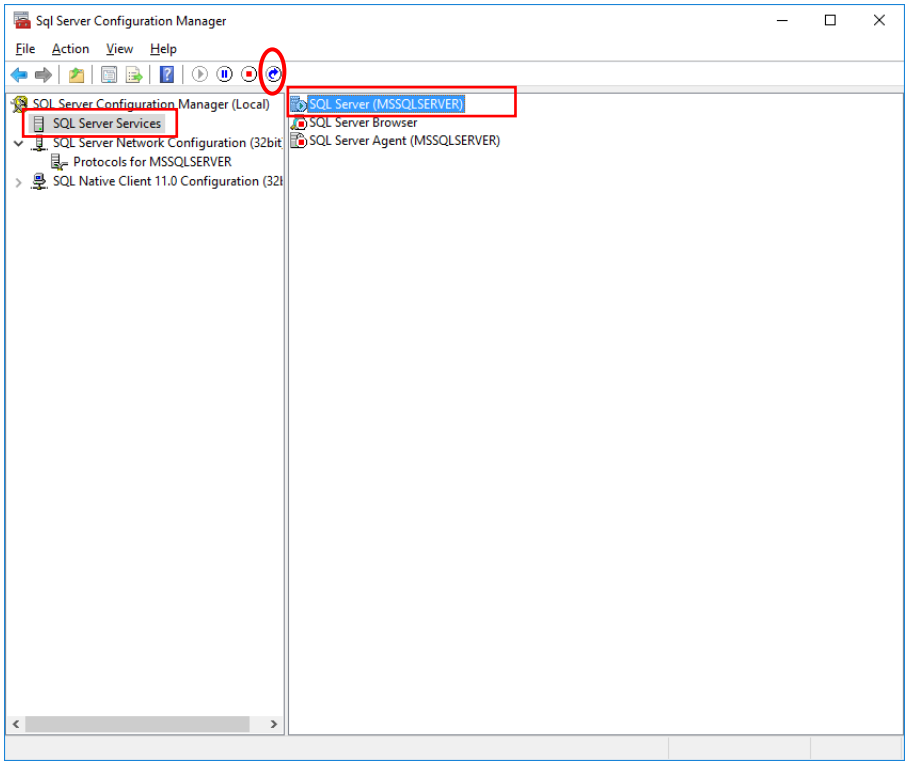
Next, under the "IP Address" tab, make sure the LAN port and Local Host connections are 'Active' and 'Enabled' and that the TCP Port is 1433.

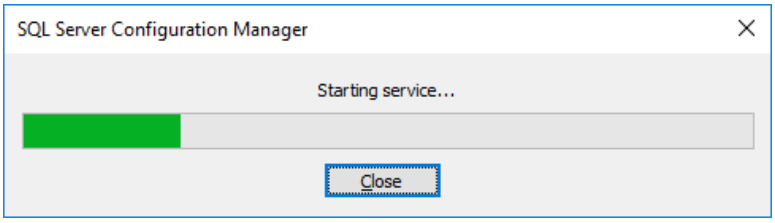




Click "OK"

Restart the server after any configuration change. Highlight the SQL server, right-click and select Restart or just click the "Restart" icon.





The SQL Server will restart and run with the new configuration.

This completes the installation of SQL2014 Express.

CTC union®

www.ctcu.com

T +886-2 2659-1021 F +886-2 2659-0237 E sales@ctcu.com