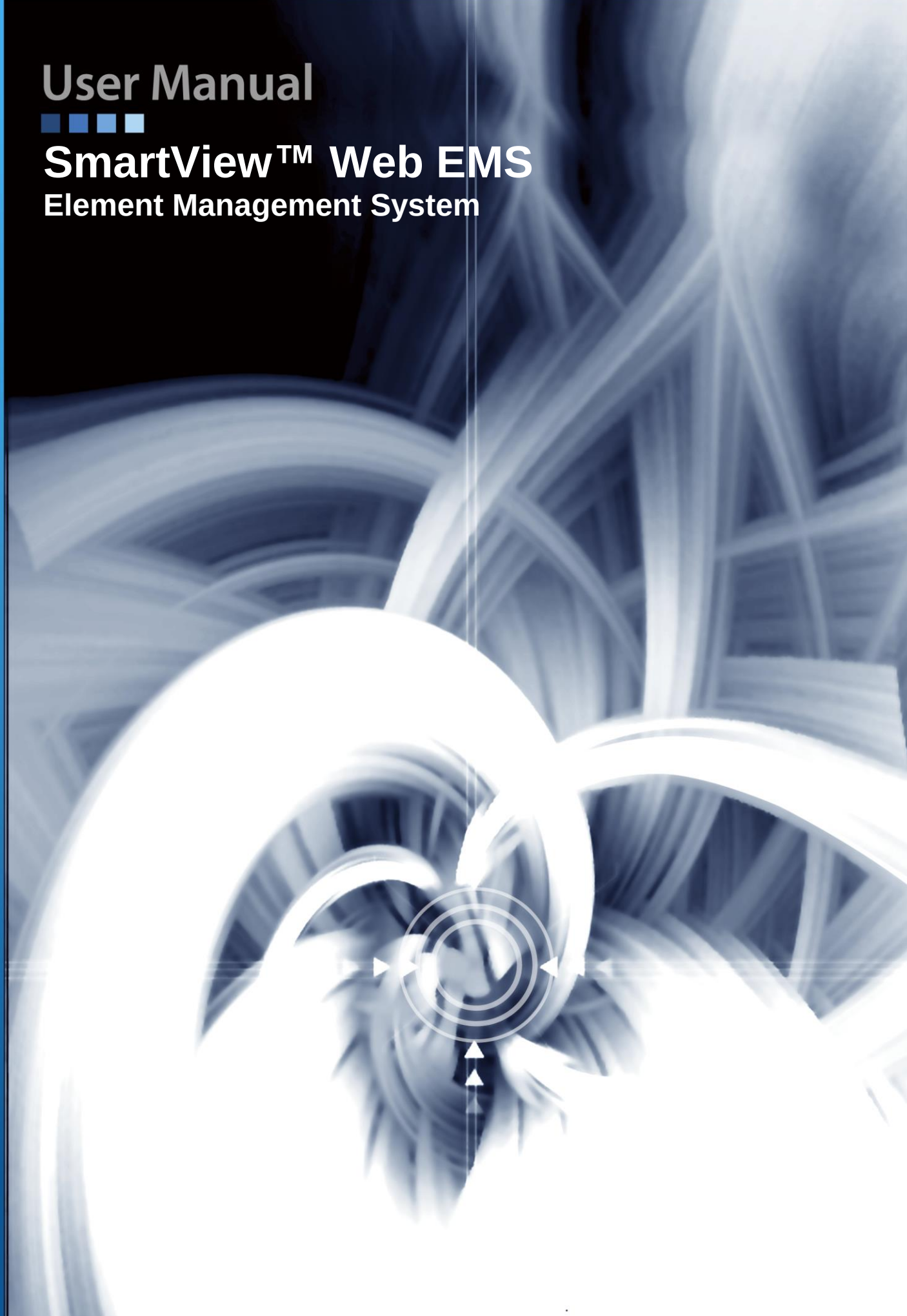
User Manual

SmartView™ Web 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® and MS-SQL® are registered trademark of Microsoft® Corporation
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™ Web EMS
(Element Management System).
Software Version 1.000 and above

User Manual
Version 0.99a December 21, 2022

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 download file 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 (Web based EMS), herein just called Web 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 WEB 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 WEB EMS
Step by step procedure for installing the WEB EMS system on a single PC platform.

Chapter 4 Admin Console
Explains how to setup the WEB EMS Service

Chapter 5 Using a standard browser as a manager
Configuration of the manager client for WEB EMS.

Chapter 6 Using the Topology Feature
Provides some details for maintenance and troubleshooting problems with WEB 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: Installing MS-SQL2014 SP2 Express
Provides a step by step instruction for installing Microsoft's SQL Server for use with WEB EMS.

1.2 The WEB EMS system

There are two opposing points of view for management system

Management system 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 (WEB 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 WEB 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)
- Zabbix (Open Source)
- PRTG (commercial)
- Cognos (IBM)
- SolarWinds (commercial)

Limitations

Universal management systems cannot fully present vendor specific features of Network Devices. One of WEB 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 WEB EMS design is based on the following considerations that comply with new requirements for management systems

- JAVA based

WEB EMS is purely 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 Web server support

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

- Open architecture

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

Web Service (http/https)

A web server is computer software and underlying hardware that accepts requests and sends responses via HTTP or its secure variant HTTPS. The network protocols were created to distribute web contents (web pages, etc.) to client user agents. A user agent, commonly a web browser, initiates communication by making a request for a specific resource using HTTP, and the web server responds with the content of that resource or an error message. The web server can also accept and store resources sent from the user agent if configured to do so All information for each Network Device in WEB EMS can be stored or loaded from the EMS database.

Embedded Agent (EA)

This is the major element for WEB 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/SSH). 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. Implementing new protocols in all components of WEB 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 parameters 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.

Web Based 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 WEB 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 user defined colors for each alarm severity level.

Chapter 2 WEB EMS Functional Specifications

2.1. General Description

This chapter is intended to describe the software design specification for the SmartView™ WEB EMS Server software for CTC Union Network Devices (ND). The WEB EMS Server is designed to provide all the configuration and maintenance functions for the network device. The method to access WEB EMS Server functions is via HTTP protocol according W3C Specifications. When a user opens browser software and sets up a link to the WEB EMS Server it will be possible to monitor and control Network Devices via web http actions. The WEB 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	WEB EMS	Web Based Element Management System	
2	EMC	Element Management Console	
3	API	Application Interface	
4	ND	Network Device	
5	JAVA	Just Another Virtual Accelerator	
6	JDBC	JAVA Database Connectivity	
7	JRE	Java Runtime Environment	
8	SNMP	Simple Network Management Protocol	
9	HW	Hardware	
10	IP	Internet Protocol	
11	OS	Operating System	
12	SW	Software	
13	TCP	Transmission Control Protocol	
14	UDP	User Datagram Protocol	
15	HTTP(S)	Hyper Text Transport Protocol (Secure)	

2.3. Requirement

- H/W: IBM Compatible PC, 64bit Processor (minimum Intel i5, >3.0G, 8G RAM (16G recommended), 20G Disk Space, 1024x768 minimum display resolution, FHD (1920x1080) recommended.
- OS: Microsoft Windows 10/11 Professional(64), MS-Server 2016, MS-Server 2019, MS-Server 2022.
- Network: IP over LAN/WAN (Gigabit Ethernet I/F)
- OpenJDK 1.8 (64 bit binaries included with WEB EMS)
- MS-SQL Server 2019 Express for Windows 10/11/MS-Server 2019 (included)

2.4. The Architecture of WEB EMS Server

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

2.4.1. Basic Server Architecture

Since HTTP is used as the communication protocol, the system will be compatible with all implementations of Web client software, i.e., Chrome, Firefox, Edge, Safari, etc. Obviously, you can use any SNMP browser to monitor and control the Network Devices. However, the advantage of using an WEB 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 WEB 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 a browser on the server (localhost or 127.0.0.1) to discover and add elements for management.

WEB EMS Server 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 HTTP(S) with clients (Web browsers)

The communication protocol between the management WEB 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.

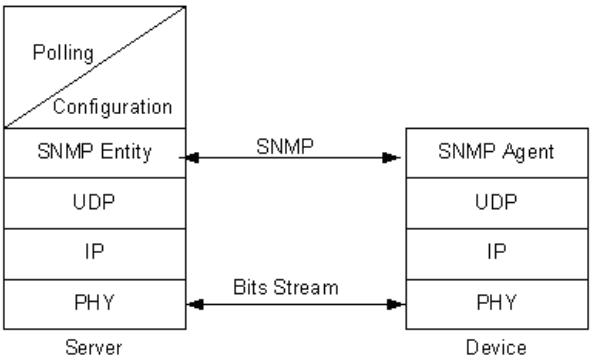


Figure 2-1 Communication between SNMP browser and device

The tasks performed by WEB 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 clients via HTTP(S)
- 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 WEB EMS Server works in close connection with the following external modules:

1. Web Server – Jetty 9.4.42
2. JDBC - mssql-jdbc-6.4.0.jre8 with OpenJDK 1.8 (64-bit)
2. Database Server - MS SQL 2019 Server Express (64-bit) from Microsoft Corp.

The database and Web EMS are installed on the same host for best performance.

The WEB 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
- Embedded Web Server
- Database

2.5 Functional Description of WEB EMS Server

2.5.1. Functions of 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 (i.e., Pollers)

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 Web Server (Jetty)

Realize HTTP(S) to interact with client browsers. Performs client registration message sending to clients and all SW calls from client. There is only one active thread per connection.

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 WEB 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 Web Server

The Web Server, in Web EMS, is an embedded, open-sourced, JAVA based module, called Jetty, which is part of the "Eclipse" open-source project. The Jetty version used, at the time of this printing, is 9.4.42. This is the oldest and most stable branch of Jetty, which runs alongside the new versions 10.x and 11.x. Jetty server is a super light weight embedded web server and serves as the interface between Network Administrator's web browsers and the actual Web EMS program. The user interface, being Web-Based, does not require that any clients install "special" software. Since Web EMS clients connect through the http common TCP port of 80, network admins will find it easy to configure and firewall(s) that could be between the Web clients and the Web server of Web EMS.

2.7 Network Structure

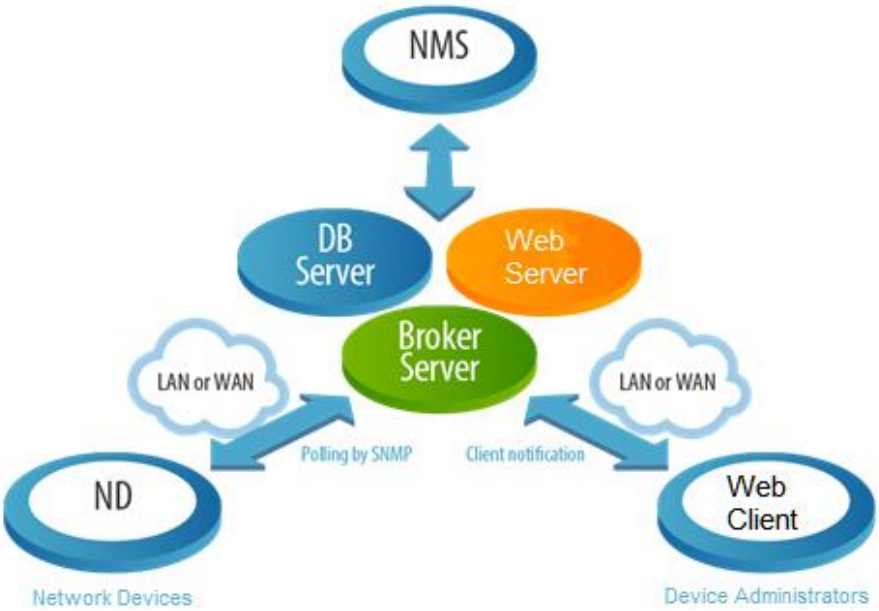


Figure 2-1 A block diagram of the WEB EMS network

2.7.1. Agents

The very first product brought into the SmartView WEB EMS was the IGS-803SM. The IGS-803SM is an Industrial Grade Ethernet switch in a compact DIN Rail mounted package, which features 8 x 10M/100M/1000M UTP ports on RJ-45 plus 3 x 100M/1000M/2.5G optical ports on SFPs. Other SNMP enabled products will be added to the WEB 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. Web Server

Jetty provides a web server and servlet container, additionally providing support for HTTP/2, WebSocket, OSGi, JMX, JNDI, JAAS and many other integrations. These components are open source and are freely available for commercial use and distribution.

Jetty is used in a wide variety of projects and products, both in development and production. Jetty has long been loved by developers due to its long history of being easily embedded in devices, tools, frameworks, application servers, and modern cloud services.

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 WEB 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 are Web browser clients which may connect via LAN or Internet (depending on how the Web EMS server is routed). All major Web browsers are supported. The number of simultaneously connected clients depends entirely on the performance of the hardware running Web EMS and the throughput of the network that connects to the Web EMS server.

This page left blank intentionally.

Chapter 3 Installing WEB EMS

3.1 Installation Description

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

3.2 Basic Requirements for WEB EMS

This document has been arranged in such a way, that there are only two major steps performed by the Web EMS installer. For a full installation on clean hardware, the installer will completely take care of installing SQL Server and WEB 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 WEB EMS ems_full.exe installer in just one easy step.

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. WEB EMS has been integrated into three components, the Broker Server, the SQL Database Server and the Jetty Web Server. Each component has its own task and purpose. All of these components will be placed on the same hardware to handle all those tasks.

WEB EMS has been developed under the JAVA environment; You could have WEB EMS running on different OS platforms. However, in its current form, WEB EMS relies on the MS-SQL database and therefore the database server and WEB EMS server must be running in a 64bit MS-Windows environment. The following section will describe how to setup your WEB EMS on MS-Windows.

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

WEB EMS Component	Hardware	Software	Operating System
WEB EMS Server	i5 3.0G or higher, 8192 MB RAM, HD >10GB (free).	OpenJDK v1.8.x.(64) Included in WEB EMS.	Windows 64 bit
SQL database Server	I5 3.0G or higher, 8GB RAM, HD >20GB (free).	MS-SQL Server 2019, including Express Edition WEB EMS Kit.	Windows 2016/19/22 Server, (64bit) Win 10/11 Pro
Workstation-Clients	Core-2 or higher, 2048MB RAM, HD >1GB.	Chrome, Firefox, Edge, Safari	Windows 32/64 bit (8, 8.1, 10, 11)
All-In-One (WEB EMS & SQL Server on one machine)	I5 or higher, 16GB or more RAM, HD >40GB (free)	OpenJDK, WEB EMS kit, MS-SQL Server, JDBC Driver ems_full.exe	Windows 2016/19/22 Server, (64 bit) Win 10/11 Pro

Table 3-1 Hardware & Software requirements for WEB EMS

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 dedicated hardware or a virtual machine (VM) for running the WEB EMS with MS-SQL Server, and no other services. If the server is freshly installed, an i7 3.40G CPU should show CPU utilization under 1%. 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 view utilization of individual processes and shut-down offending processes.

3.3 Install WEB EMS

3.3.1 Introduction

WEB EMS is delivered as a single ~300MB Windows "exe" file. The "ems_full.exe" is the complete installation file which includes the MS-SQL Server Express Edition 2019 and OpenJDK JAVA binaries. The "ems.exe" is an 'upgrade or patch' file which is incrementally released with new product support, function additions and/or fixes. WEB EMS may be delivered on USB Pen Drive (Physical Media) or it may be downloaded from CTC Union's servers. The installation process will follow these basic steps:

1. Run the "ems_full.exe" program as administrator. (right click, select 'run as administrator')
2. Ensure the check boxes are checked to install MS-SQL and to create a desktop shortcut.
3. Follow the prompts until the program is installed.
4. Start Web EMS server; Using a local browser, login to localhost (127.0.0.1)
5. Install license file or run in evaluation mode.

3.3.2 WEB EMS Windows Installer

Insert the USB flash drive into your PC's USB port. Open the drive folder and right-click the "ems_full.exe" icon, choose 'Run as administrator'. Optionally, if you have downloaded and unzipped the installation set to local disk, browse to and right-click the "ems_full.exe" program and choose 'Run as administrator'.

1. USB Distribution

The USB drive has the windows installation file which includes the 64bit 1.8 OpenJDK Runtime Environment Binaries and Microsoft's free MS-SQL Server 2019 Express in English. Open the USB drive and right-click the "ems_full.exe" icon and choose 'Run as administrator'.

2. Download

The download file is a ZIP file (the unzip process will ensure the download has no errors). Use extraction software, such as 7-Zip (or WinZip™), to extract the "ems_full.exe" file to the local drive. After being unzipped the "ems_full.exe" can be run (right-click and choose 'Run as administrator') directly.

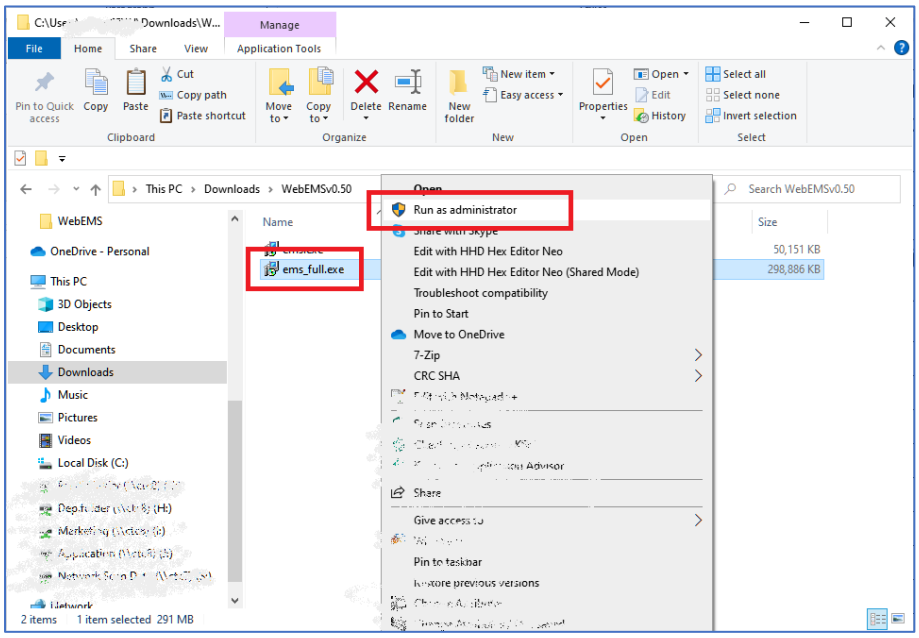


Fig. 3.1 Installation folder, ready to install Web EMS.

3.3.3 WEB EMS Install Screen

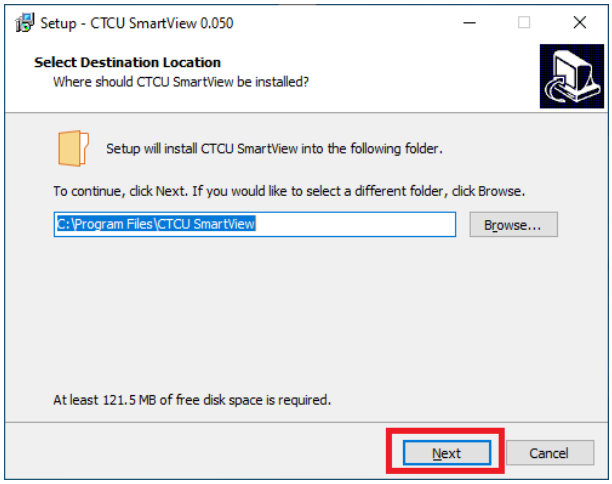


Fig. 3.2 The default installation folder is under Program Files.

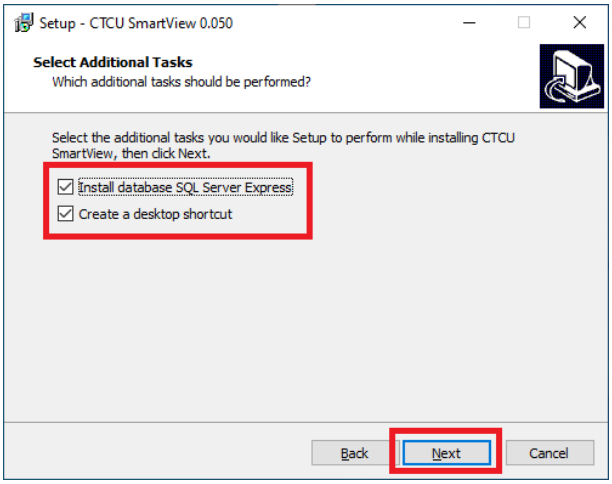


Fig. 3-3 Enable both checkboxes and click 'Next'.

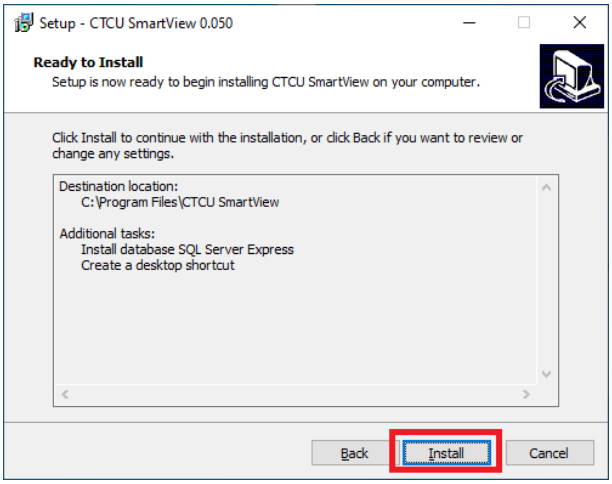


Fig. 3.4 Setup is ready, click 'Install'.

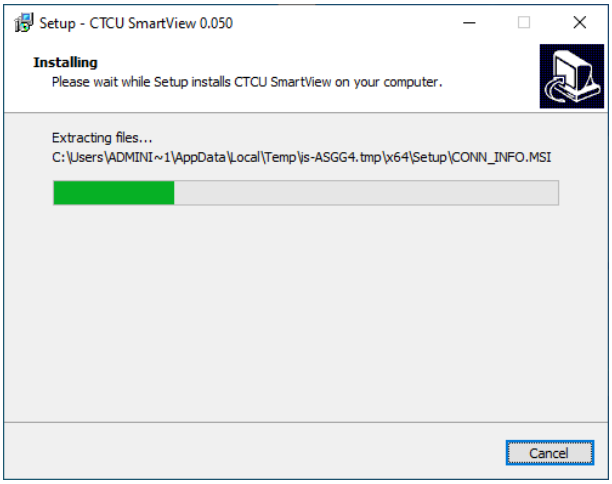


Fig. 3.5 Progress bar while installing.

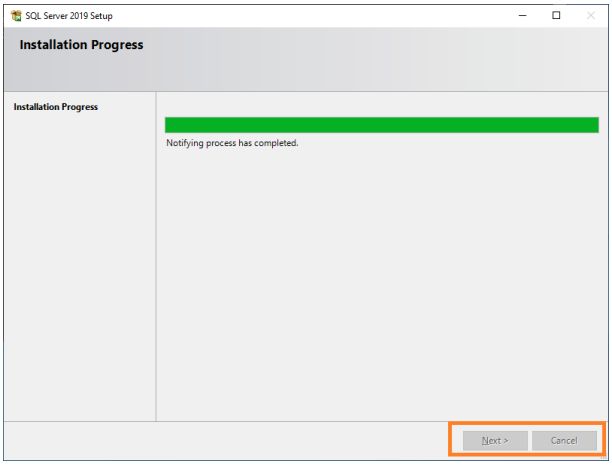


Fig. 3.6 MS-SQL Server is installed automatically.

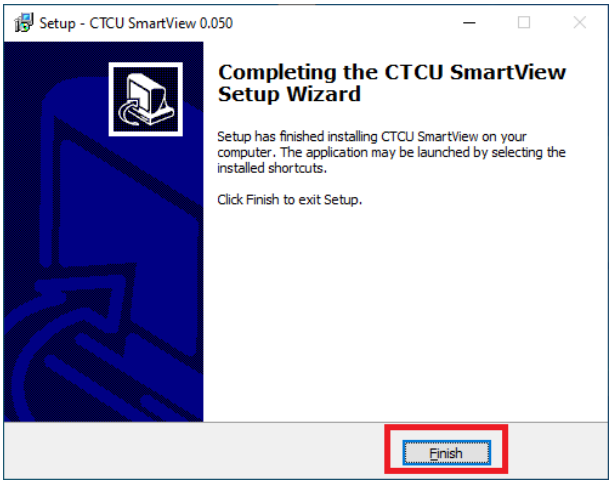


Fig. 3.7 When setup is complete, click 'Finish'.

3.3.4 About Java Run Time Environment

The EMS Broker (server) is 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 closed programming language, while the OpenJDK project continues the free open source JAVA originally released by Sun Microsystems in 2005.

SmartView Web EMS includes the 64-bit OpenJDK version "8.0.2820.8" and places the runtime binaries within the CTCU Smartview program folder. It doesn't matter if the host computer has Java or not or what the Java version installed is. Web EMS will always use its own 64bit OpenJDK version "8.0.2820.8" binaries for maximum stability and compatibility. There is no need to separately install Java JDK/JRE on the host computer.

3.3.5 SQL Server Install

Web EMS relies on ***Microsoft***® MS-SQL database to store all information. Unattended installation is the supported default. This means Web EMS installs MS-SQL Server when the "Install database SQL Server Express" checkbox is checked (default). Please refer to the detailed instructions in Appendix A for manual installation of SQL Express 2019. Refer to your Microsoft documentation when installing your own SQL Server and reference our installation procedures, as the server must be installed with a "Default Instance" and in "Mixed-Mode".

3.3.6 Updating

CAUTION: Web EMS version is tightly matched to firmware versions of CTC Union products. Prior to doing any upgrading of Web EMS, please ensure all ND (Network Devices) are properly upgraded and compatible with the new Web EMS version (refer to the included Product_Support.PDF with any SmartView version). There is no method to "down grade" the Web 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 Web EMS folder will aid in doing a quick recovery. Please see the Appendix on the methods to perform a complete backup of the Web EMS system and database before performing Web EMS upgrade.

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

IMPORTANT: Make sure all clients are logged and the Web EMS service is shutdown prior to doing any Upgrade.
Hint: Right-Click on the WebEMS taskbar icon and select Stop Service.

The Upgrade Tool will be distributed as a 'ZIP' file. After extraction, move the "ems.exe" file to the server. Next, 'right-click' on the 'ems.exe' file and select 'Run as Administrator'.

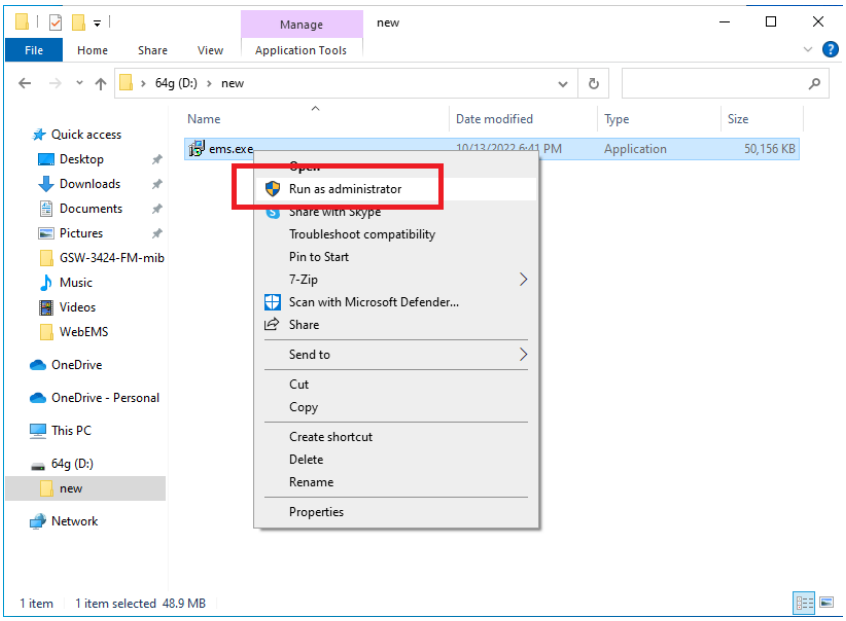


Fig. 3.8 Upgrade ems.exe file from extracted Upgrade ZIP file.

The Setup will start. Follow and click on the prompts.

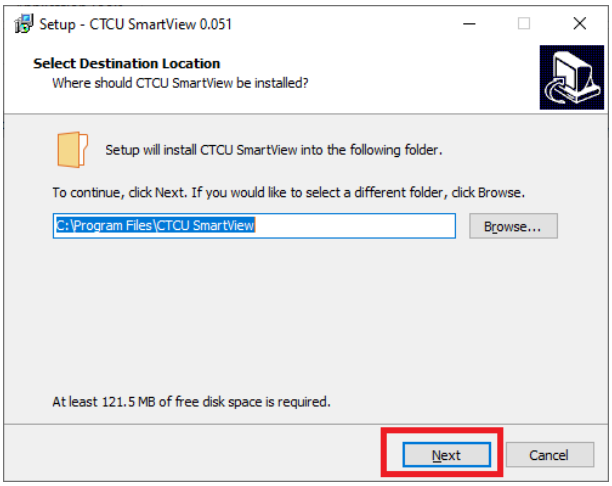


Fig. 3.9 Install to default folder, click 'Next'

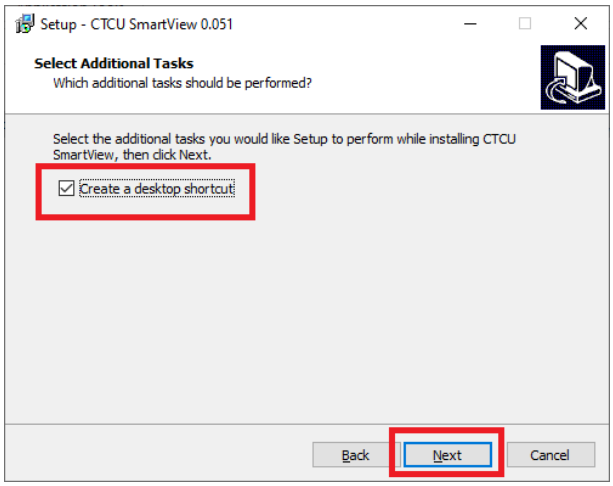


Fig. 3.10 Create shortcut and click 'Next'

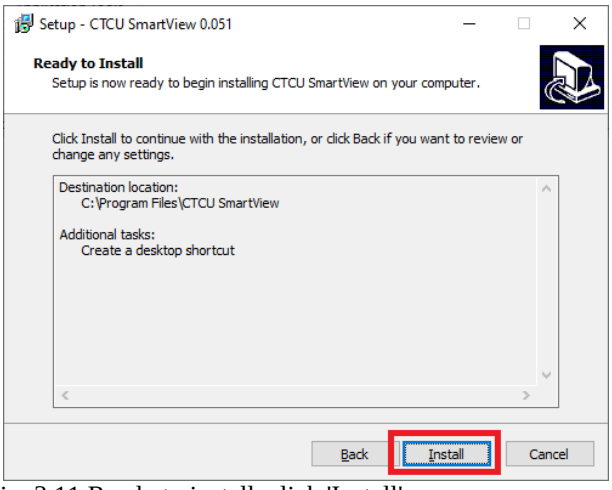


Fig. 3.11 Ready to install, click 'Install'

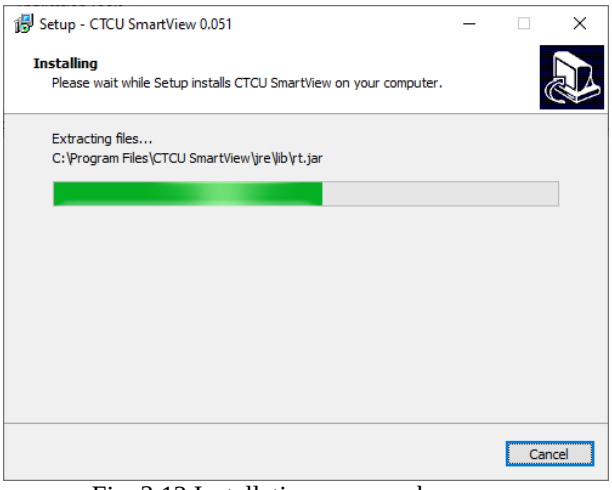


Fig. 3.12 Installation progress bar

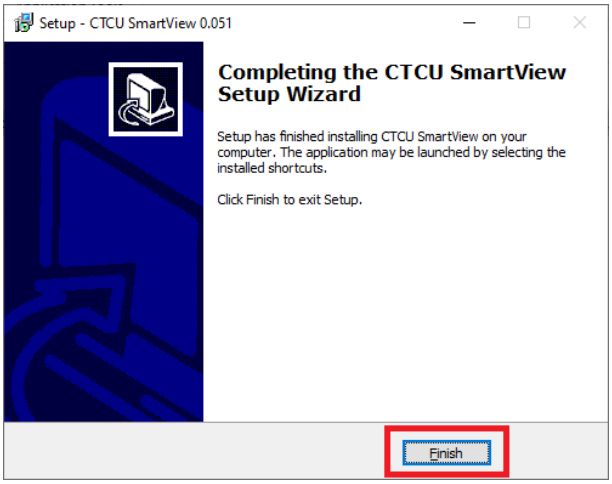


Fig. 3.13 Finish

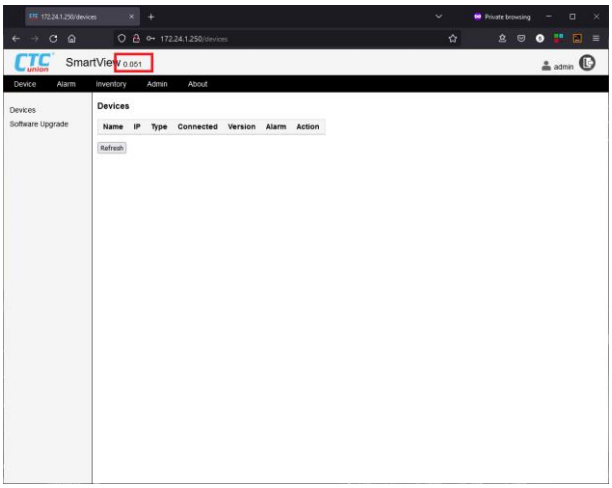


Fig. 3.14 Start server, open client, login, check version.

Warning: Under Windows Vista and above (Windows 7, 8, 8.1, 10, 11), unless the logged in user is the Administrator, or the upgrade is NOT run as the administrator, the upgrade may fail to write the new files into the protected program files folder.

3.3.7 Start the Web EMS Server

Located on the desktop is the SmartView icon. Double-click the icon to start the server.

Fig. 3.15 Desktop Icon

Alternately, click the 'Windows Start' button and browse to CTCU SmartView, click "Start Service".

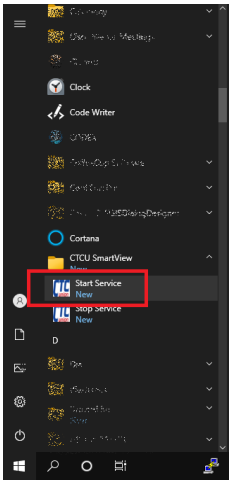


Fig. 3.16 Windows Start Menu

The first time that the SmartView Server is started, the *Windows Defender Firewall* will issue a pop-up. Be sure to allow the OpenJDK Platform binary to communicate on at least the Domain network and the Private network. Failure to do this will limit web browser client access to localhost only.

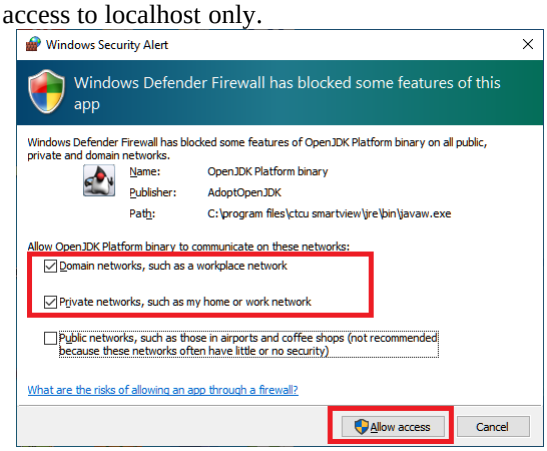


Fig. 3.17 Windows Security Alert

3.3.8 Stop Web EMS Server

Located on the Taskbar (bottom-right of desktop) is the "CTC" icon. Right-click it and select "Stop Service".

Fig. 3.18 Windows Taskbar

Alternately, click the 'Windows Start' button and browse to CTCU SmartView, click "Stop Service".

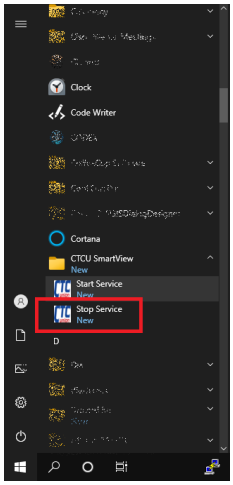


Fig. 3.19 Stop via Start Menu

3.3.9 Uninstalling SmartView WEB EMS

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

1. Prior to uninstalling, make a backup copy of the license file (SN.txt) located in the \Program Files\CTCU Smartview 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 uninstall. Stop the Web EMS Service (see 3.3.8)

2. Perform Uninstall through the Window's Control Panel.

Press the Windows key + R and in the popup type in 'control' and [Enter] (or click OK).

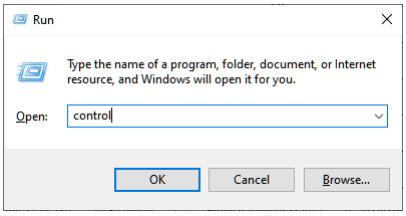


Fig. 3.20 Run 'popup'

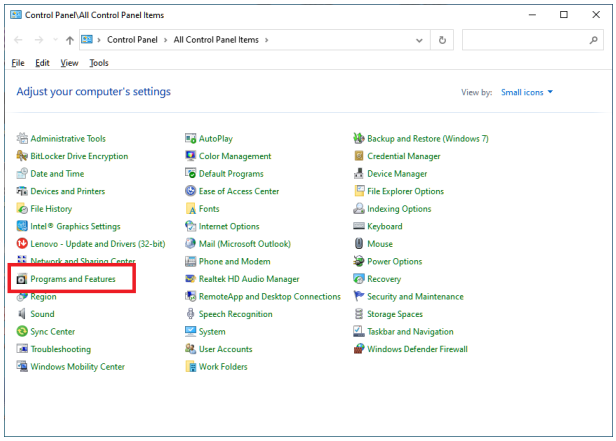


Fig. 3.21 Control Panel Items, select *Programs and Features*

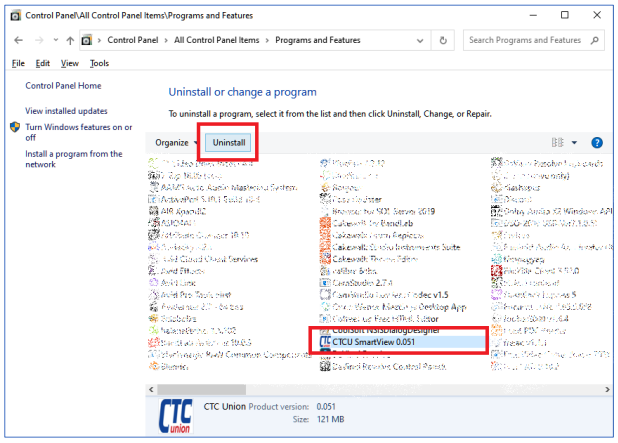


Fig. 3.22 Select the *CTCU SmartView* & Uninstall

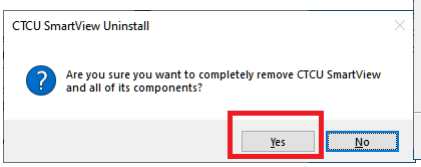


Fig. 3.23 Confirm
Click Yes to confirm.

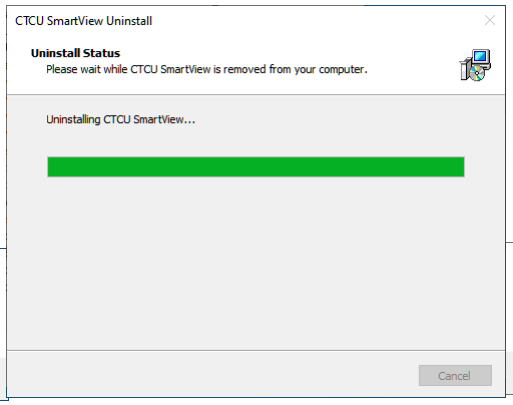


Fig. 3.24 Status
Observe the uninstall status.

Fig. 3.25 Success
Acknowledge the removal.

3. An alternate method is to browse to \Program File\CTCU SmartView and double-click unins000.exe

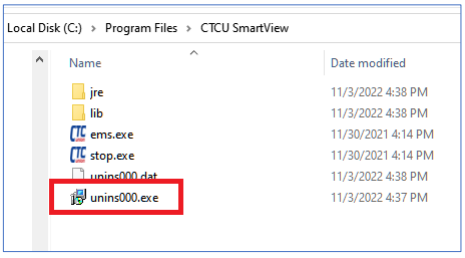


Fig. 3.26 Using unins000.exe

3.3.10 Uninstalling MS SQL Server 2019 Express

Use the *Control Panel* > *Programs and Feature*s again.
Uninstall all items related to the *SQL server*.
Reboot the computer and delete the \Program Files\Microsoft SQL Server folder.

3.3.11 Serial Number File

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

The license file is a simple text file that may be opened and viewed with any pure text editor, such as Windows Notepad. Included with the license file is a license-info.txt file. The file has a format like this:

```
File:         license
Version:      1.00
ID:           1665708567443
Valid Date:   2999/12/31
MAC Address:  78-24-AF-37-FB-11
Device:       1000
Product:      Telecom + Industrial
```

The MAC Address along with device agent number and product class are shown.
Important !! Make a copy or copies of this file and keep in a safe place. If you lose a license, a new one will most likely need to be purchased.

3.3.12 License Install

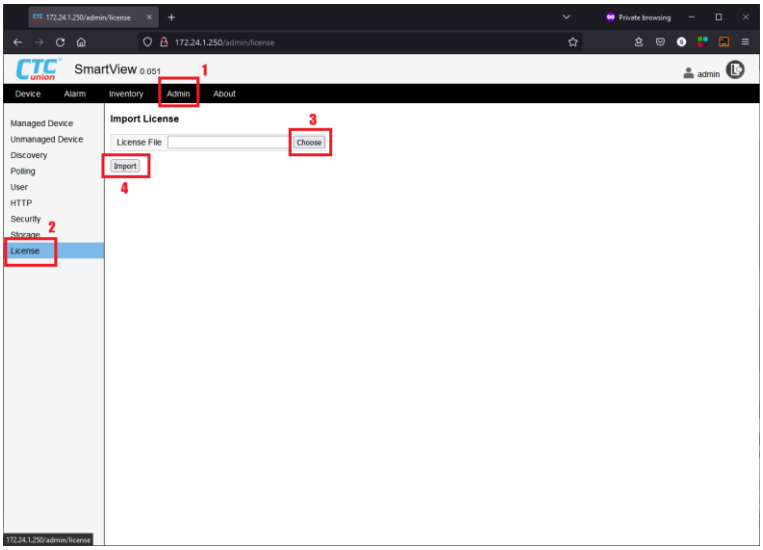


Fig. 3.27 Install license through Web GUI

After logging in as administrator:

1. Select the 'Admin' tab
2. Select 'License' from the left menu
3. Click the 'Choose' button and browse to the license file
4. Click 'Import' to install the license.

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

3.3.13 Evaluation Version WEB EMS

Version 1.00 of SmartView WEB EMS is a FULL FEATURED evaluation version which allows the WEB EMS to run in '**evaluation mode**' WITHOUT any serial key. The WEB EMS is one software, but with two different actions:

If WEB EMS detects a valid license, 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. Telecom & Industrial
- 1 only Login Client at a time. (local or remote)

3.3.14 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/
Click the "Search" icon, key-in "sql server express".
Valid downloads would include:
Microsoft® SQL Server® 2019 Express
WEB EMS ships with the 64 bit version of SQL Server Express 2019.

The free 'Express' version is more than capable of running Web EMS in a production environment, as it can support a database size up to 10GB.

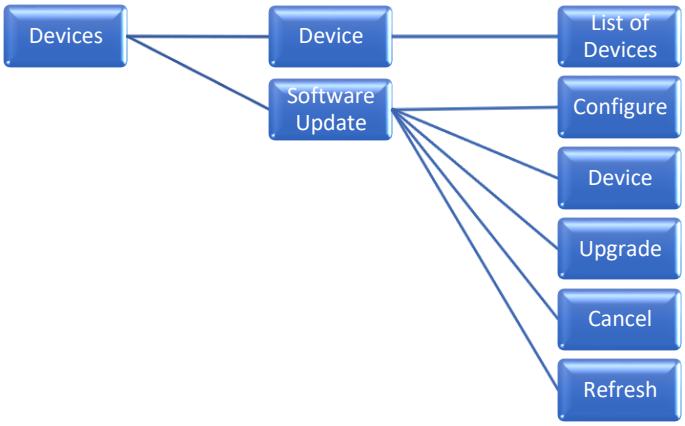
This page left blank intentionally.

4.1 Web EMS User Interface

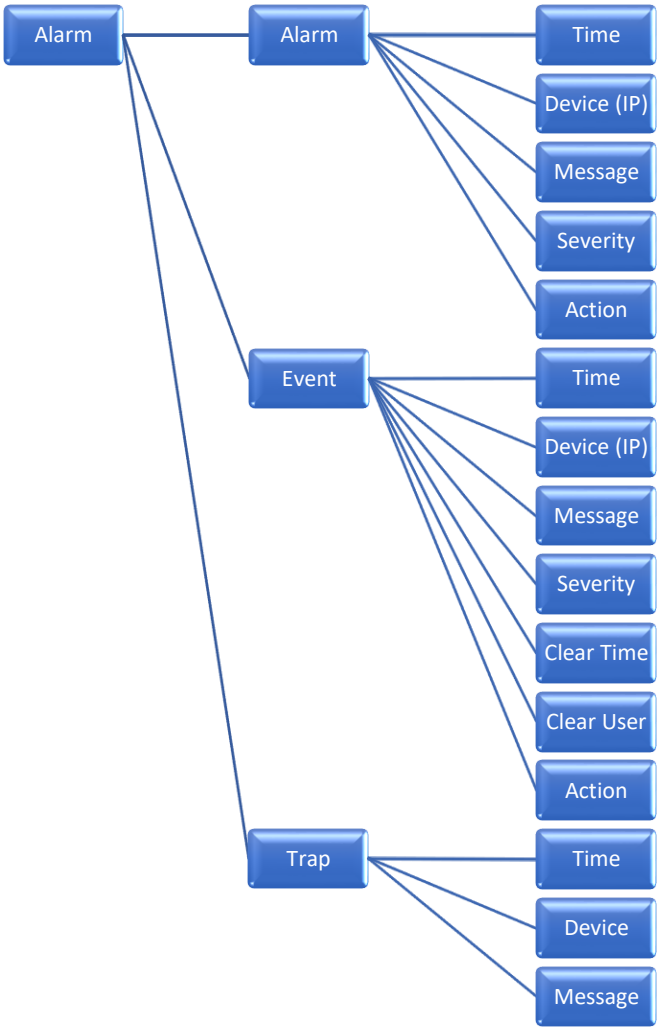
The following is a 'site map' of the Web EMS user interface.

4.1.0 Top Menu Items

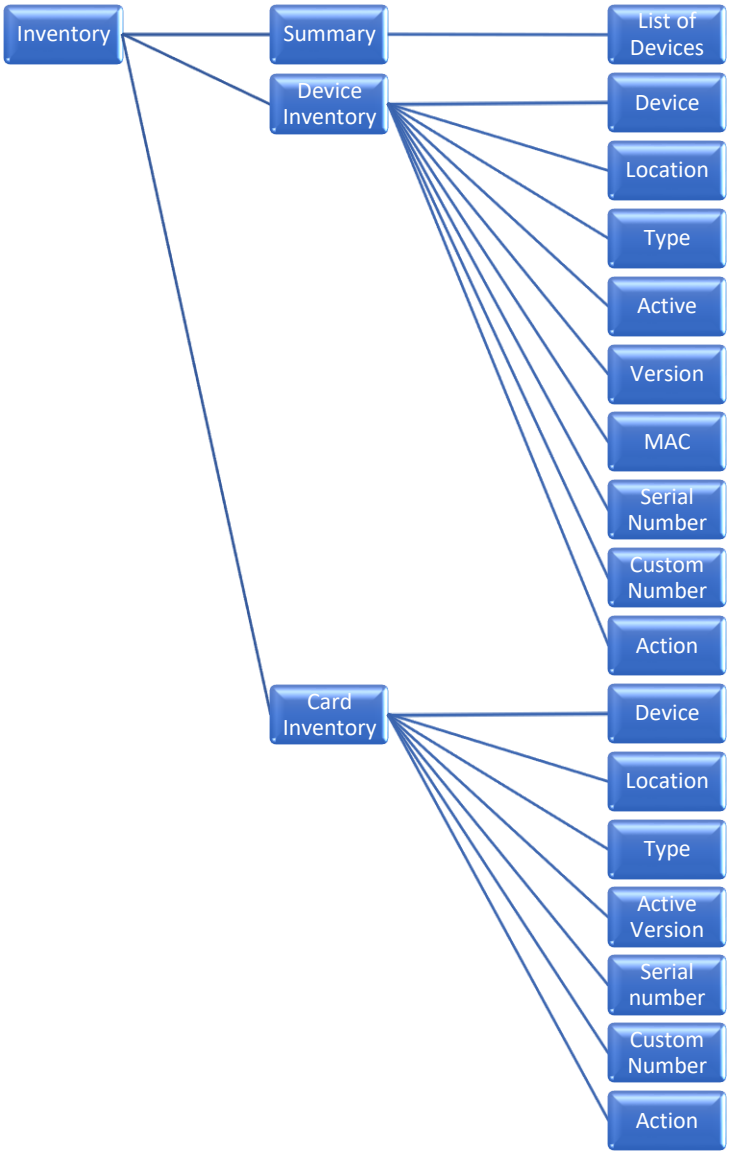
4.1.1 Devices



4.1.2 Alarm

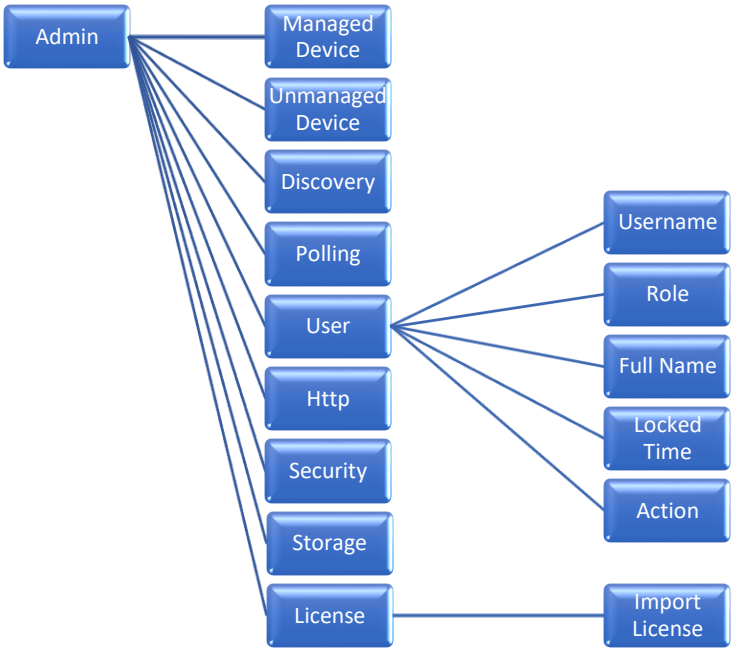


4.1.3 Inventory



4.1.4 Topology

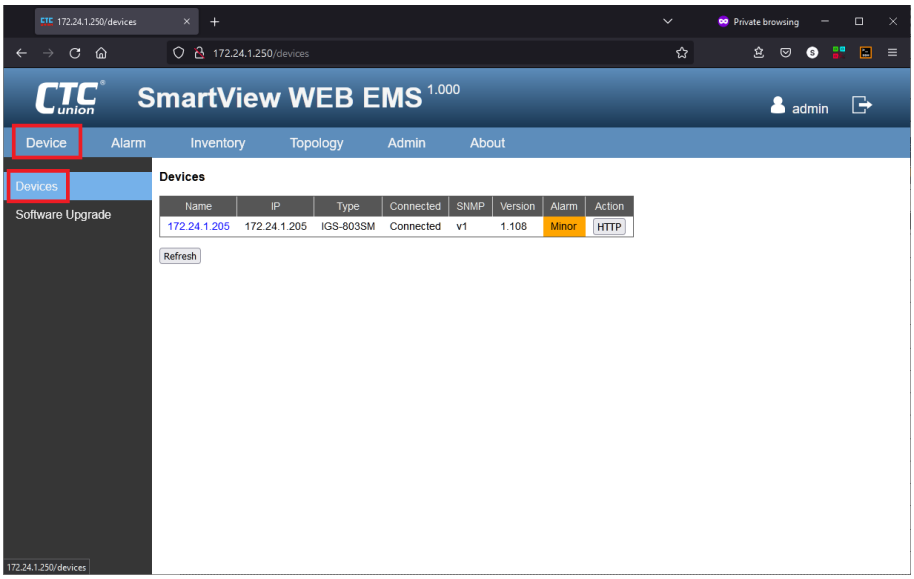
4.1.5 Admin



4.1.6 About

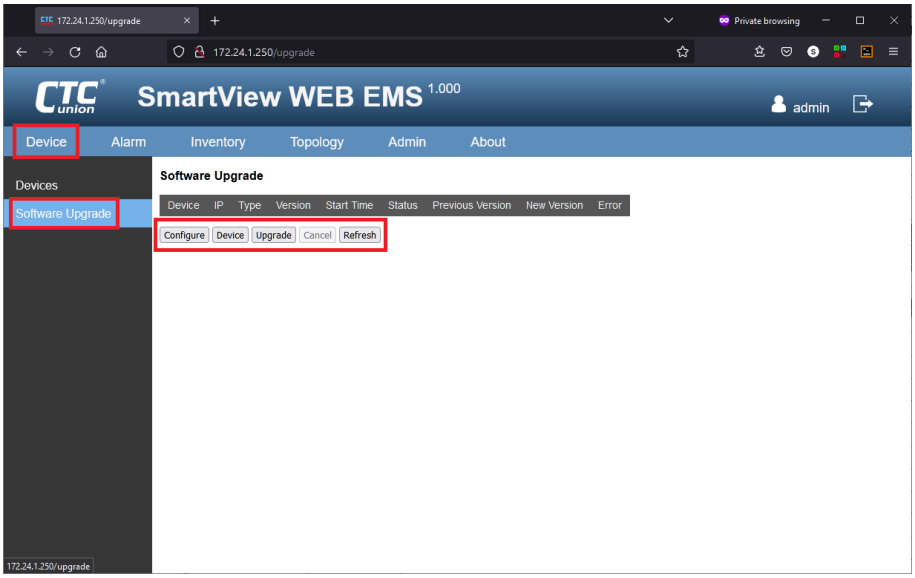
4.2 Menu Details

4.2.1 Devices



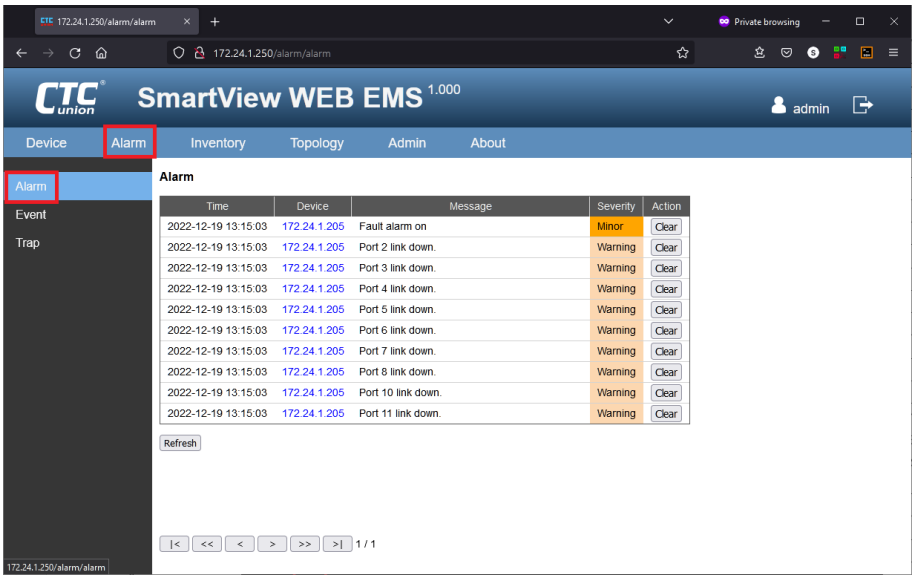
A list of all discovered devices is shown under the 'Device' menu. In the above, the Web EMS has been freshly installed and one device has been discovered.

4.2.2 Device – Software Upgrade



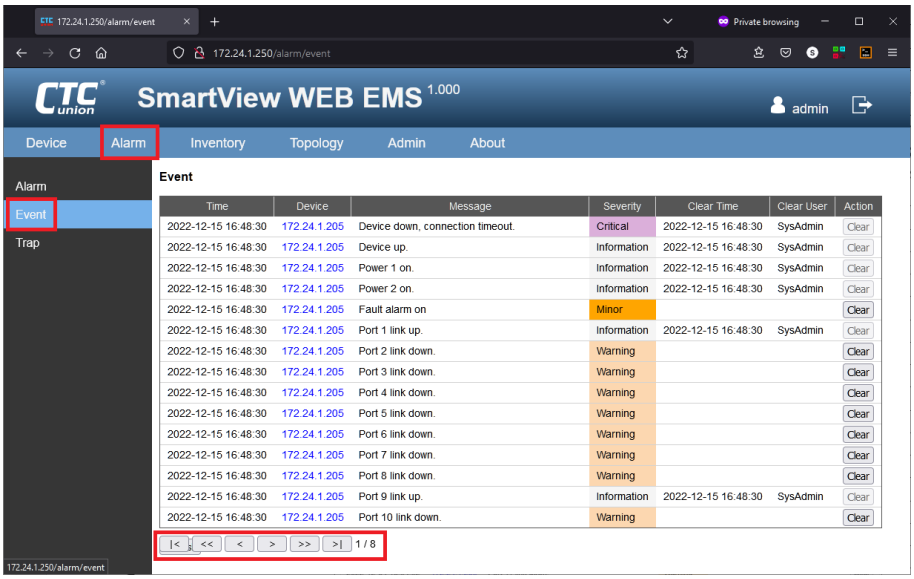
The Web EMS has the functions to upgrade network devices. The device(s) to be upgraded are first "Configured" (device type selected and software uploaded to Web EMS). Next the Device (single or multiple) are chosen for upgrade. Lastly the Upgrade is executed.

4.2.3 Alarms



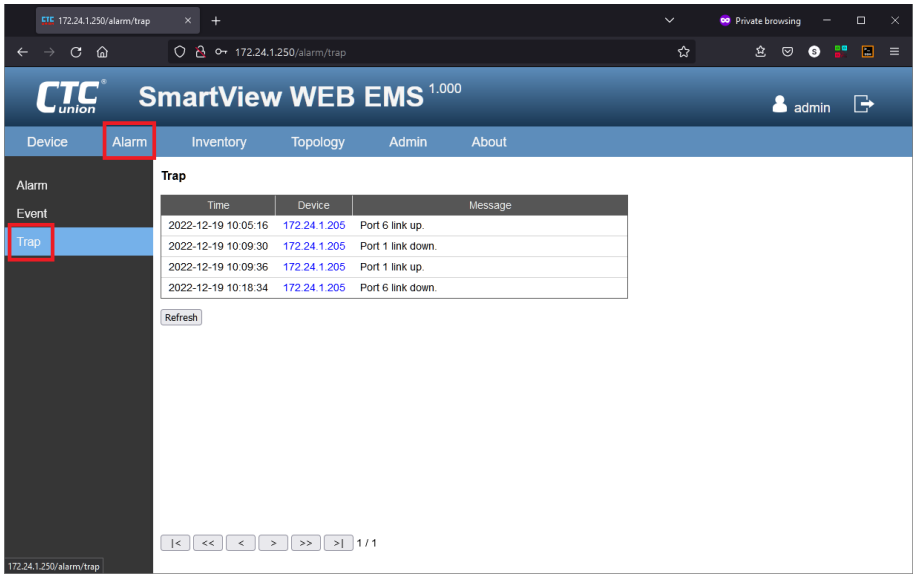
Alarms are faults discovered from devices during the polling cycle. They are shown with different severity, such as warnings, minor, major or severe alarms. If corrective action is performed, such as restoring a down link, the alarm will automatically be removed at the next polling cycle. (Note, web screens must be refreshed to reflect the current status.) The device can be clicked directly from the device's IP address.

4.2.4 Events



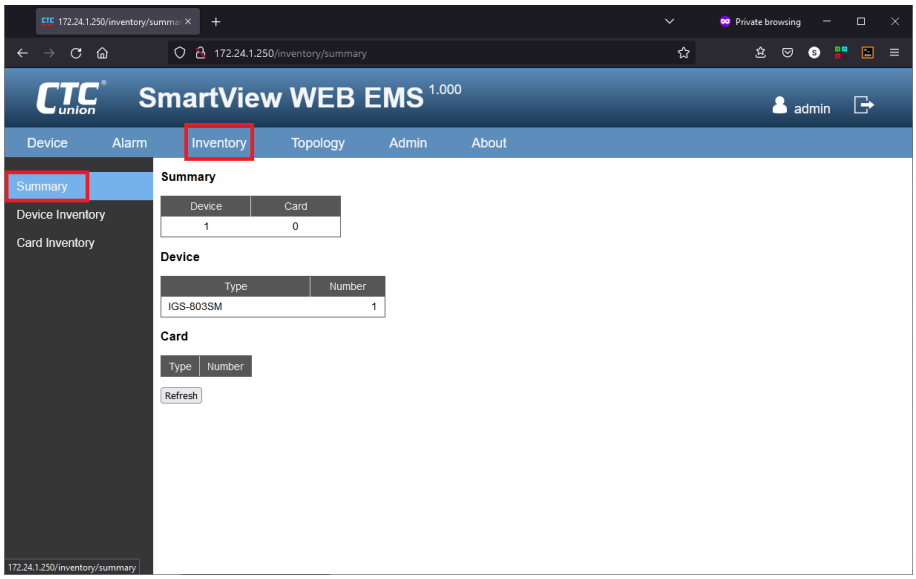
This is the Event log, basically a "system log" of all events, traps and user actions. Device alarms, their severity and time are displayed.

4.2.5 Traps



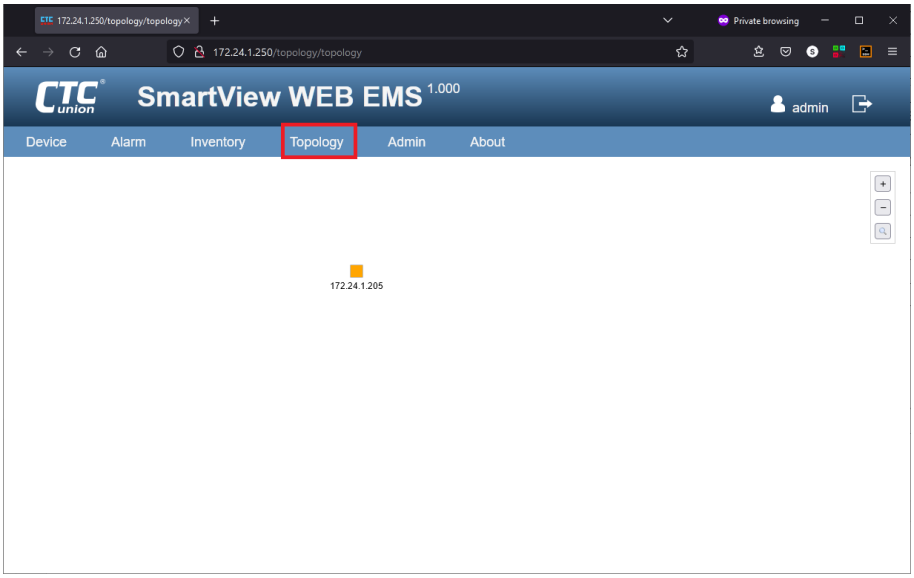
Traps are unsolicited SNMP messages which are sent by network devices to the Web EMS server, are captured via port 162, and then logged. The conditions for the trap messages are set in the devices themselves. The devices must send traps specifically to Web EMS server's IP address and the community strings must match between the devices and the trap receiver (server).

4.2.6 Inventory



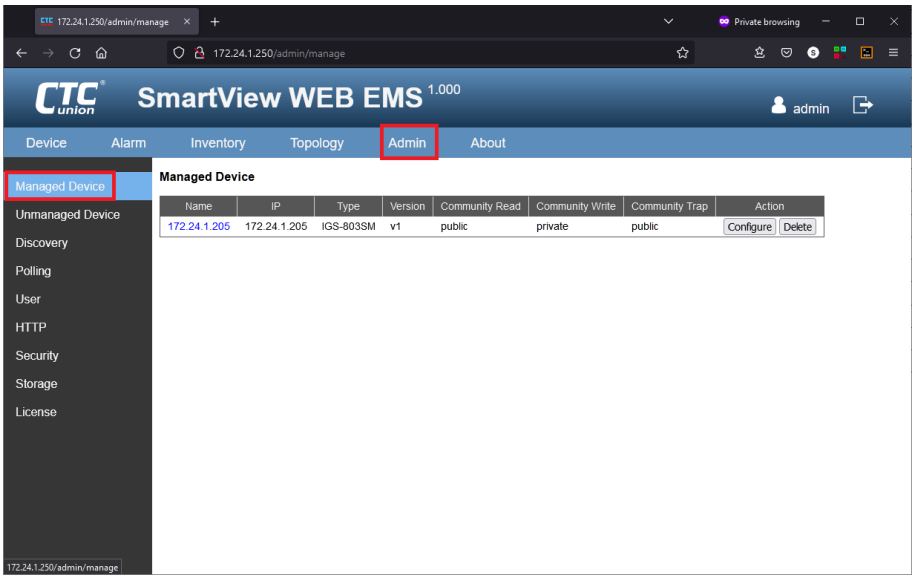
The 'Inventory' function allows listing all of the network devices which have been discovered and are being managed by the Web EMS. The 'Summary' gives a rough breakdown. 'Device Inventory' will display an inventory list of all devices. The 'Card Inventory' relates to chassis based devices and will list the card types and numbers installed in the managed chassis.

4.2.7 Topology



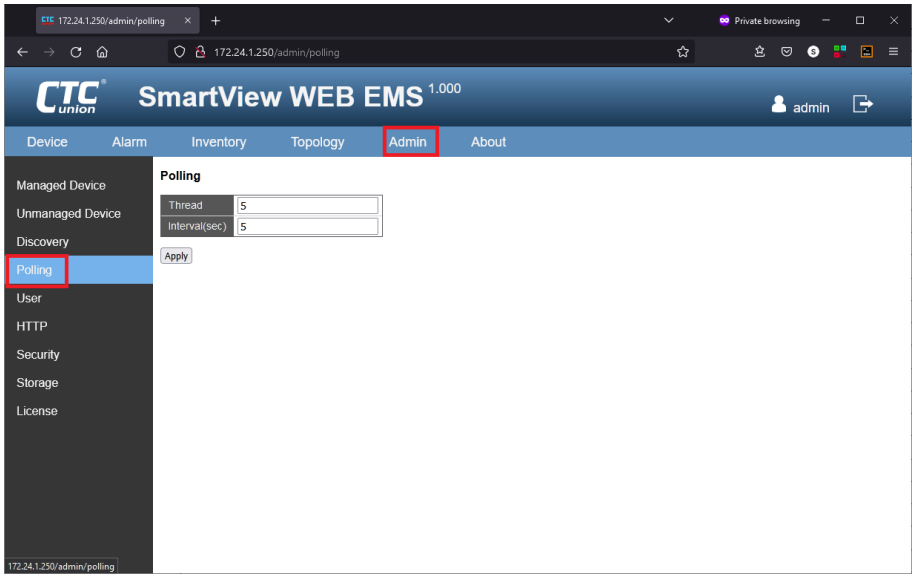
When many devices are being managed, they can be moved and connected in the 'Topology' screen. The screen may be zoomed in or out and a 'search' function may be used to quickly find a device.

4.2.8 Admin



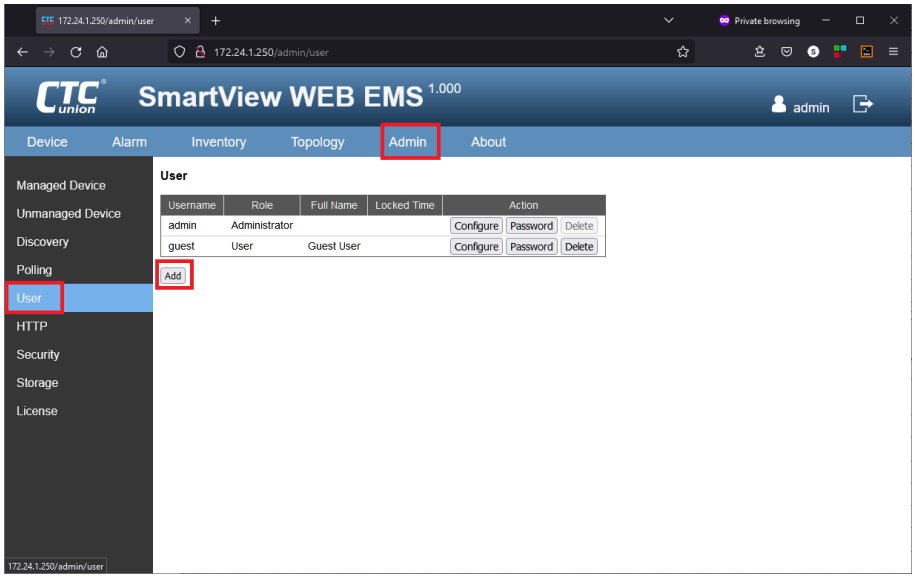
The 'Admin' tab provides a number of administrative functions. Under the 'Managed Device' menu, all devices which have been discovered and added to Web EMS management are displayed in a list. 'Unmanaged Device' are those SNMP agents found by discovery but are either not supported by Web EMS for management or have not yet been added to management.

4.2.9 Admin Polling



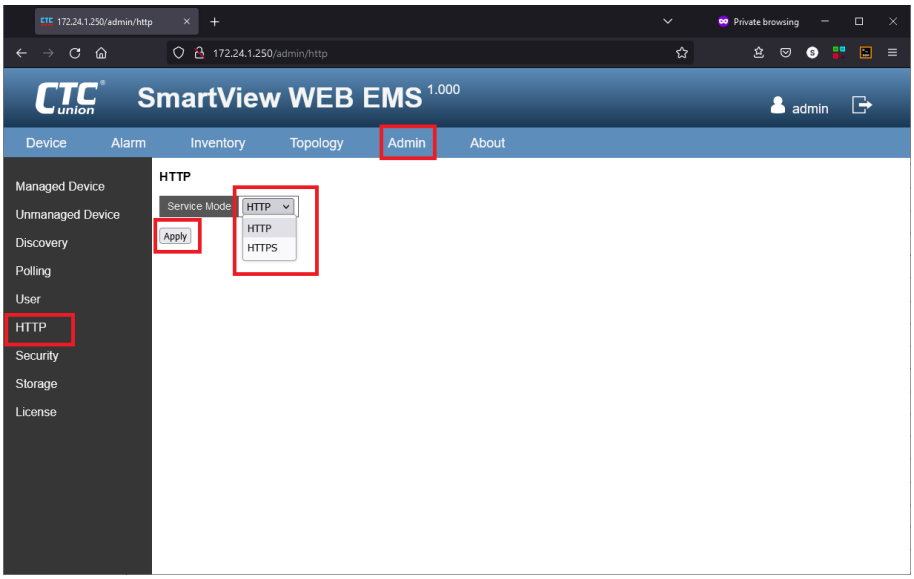
Web EMS uses "Pollers" to access devices under its management. The polling uses SNMP 'get' and 'get next' commands to gather relevant information on the device being polled. "Threads" allow Web EMS to run simultaneous pollers to query multiple devices at the same time. When all devices have been polled there is an interval "wait" period before polling starts all over again. The threads number and wait interval are both set here. (Defaults are 5 threads and 5 seconds interval.)

4.2.10 User



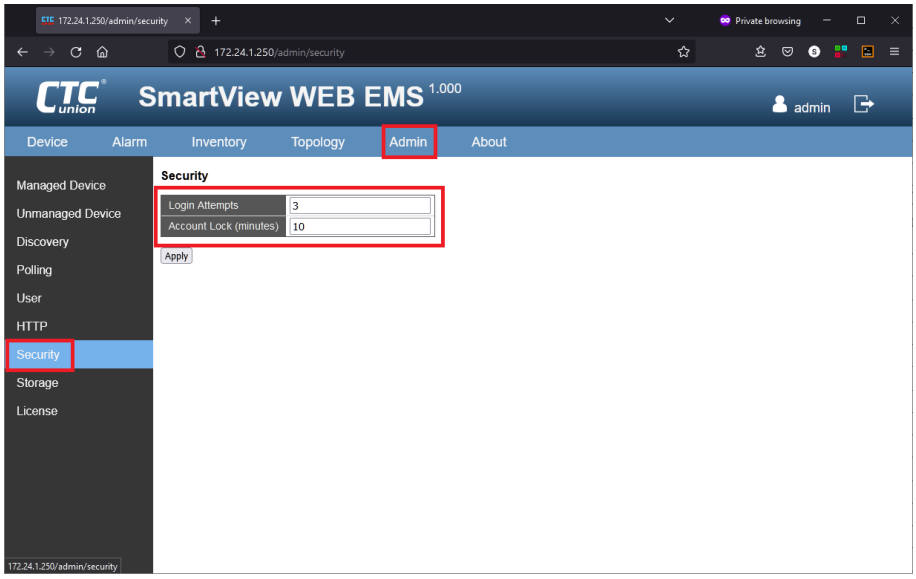
System users are added through the Admin->User menu. The admin user is the default user available following the installation of SmartView Web EMS. The default password is '00000000' (eight zeros). The admin account cannot be deleted. When creating new user accounts, the user may be assigned as a normal 'user' or as an 'administrator'. Passwords must be at least 8 characters and a user may be forced to change their password on first login. Only the admin or accounts that are assigned as administrators may add, remove or modify users.

4.2.11 HTTP



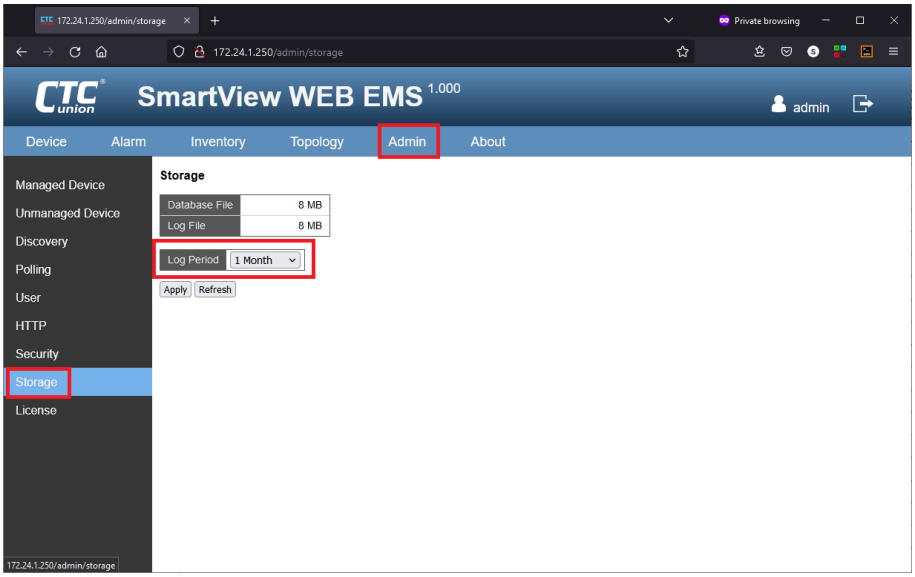
As the Web EMS uses its own embedded web server, the connection may be switched to the secure HTTPS protocol. With HTTPS enabled, any login or actions performed in the Web EMS will travel over the network as encrypted transmissions.

4.2.12 Security



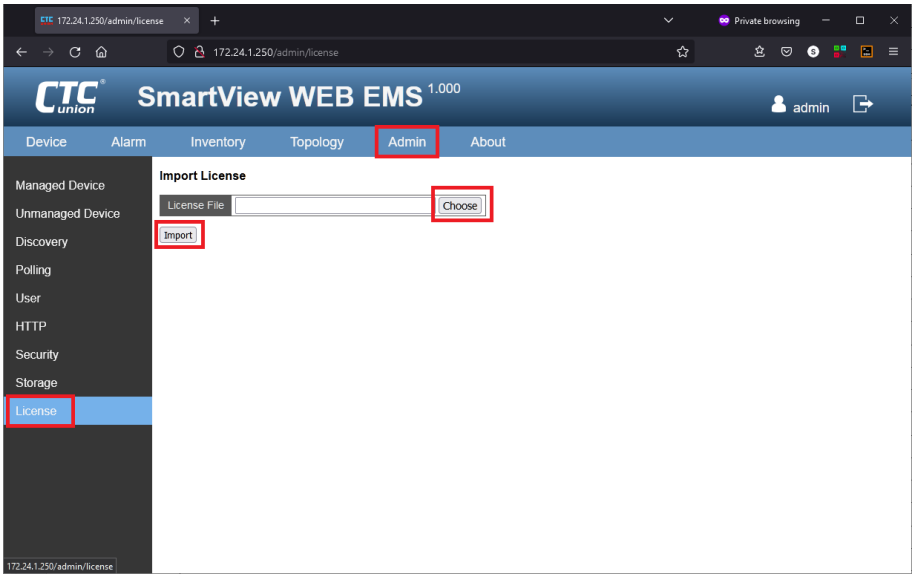
To prevent "Brute Force" attacks, the security settings may be adjusted to suit your environment. In the default settings, two failed login attempts are allowed. On the third failed attempt, the login account will be locked for ten minutes. After ten minutes, the user may then retry login.

4.2.13 Storage



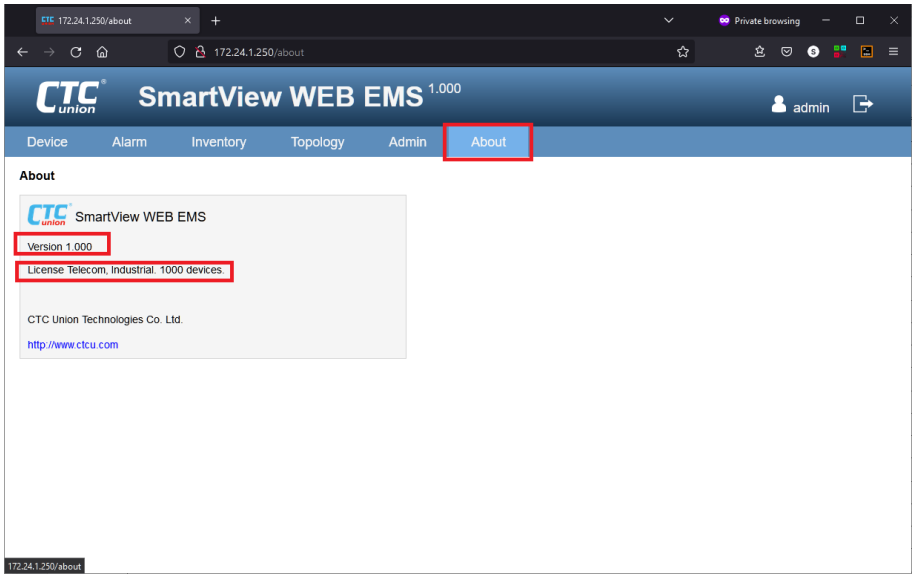
Under the Admin->Storage menu, the retention period for logs may be set to 1, 3, 6 or 12 months. The actual usage for the database and the log file is also displayed.

4.2.14 License



After the 90-day trial period, a license must be installed in order to continue to run SmartView Web EMS. The license is a "file" that is selected when clicking the "Choose" button. Once chosen, the license is then "Imported" by clicking the "Import" button. The Web EMS service must be stopped and restarted to read the license file.

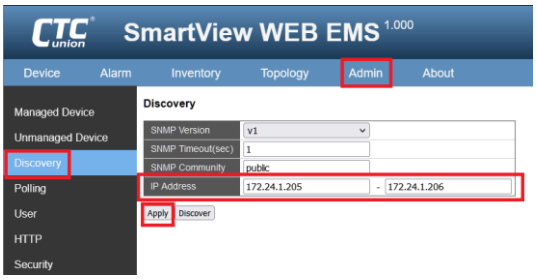
4.2.15 About



Under the "About" tab, the information regarding the SmartView Web EMS version and the details of the license are displayed. In the above example, the Web EMS version is 1.000 (first release) and the server is licensed for 1000 devices under both the 'Telecom' and 'Industrial' product lines.

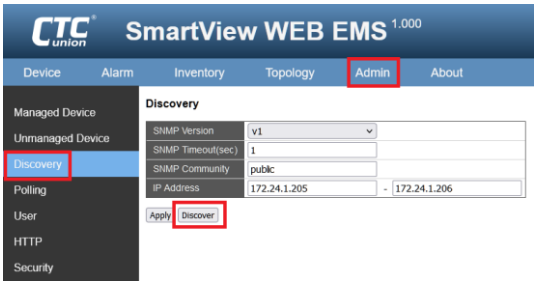
4.2.16 Discovery Procedure

1) Click the Admin menu tab and select the "Discovery" menu.

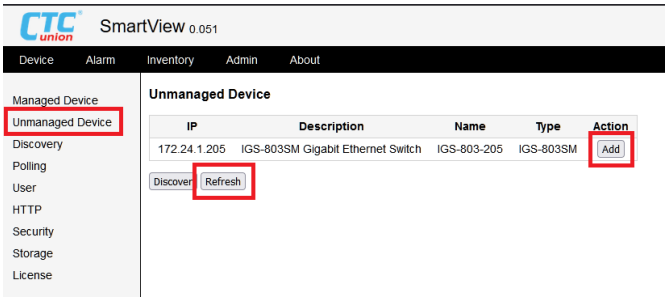


Key-in the SNMP version, community string, and IP range to discover. In this example, we are discovering a specific unit at a single IP address. Click "Apply" and the discovery parameters are set.

2) Start the actual discovery by clicking the Discover button.



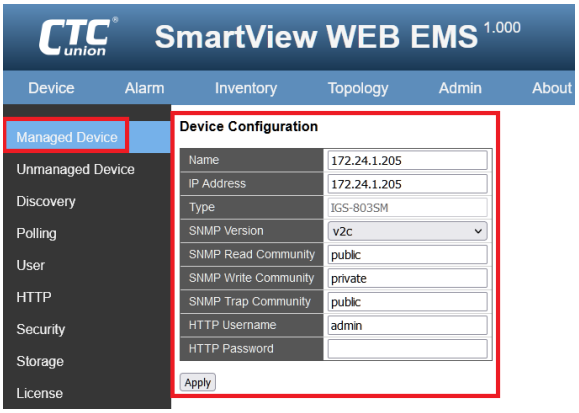
3) The "Unmanaged Device" screen should automatically be displayed.



If nothing is yet displayed, click the Refresh button. When the device is displayed, click the Add button to move the discovered device(s) to the Managed Device list.

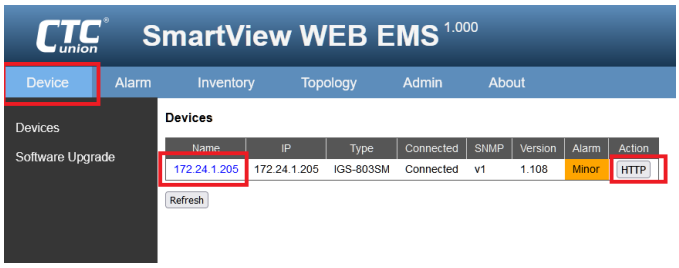
4) To configure this device through Web EMS, click Configure.

5) Configuring a device's network/SNMP



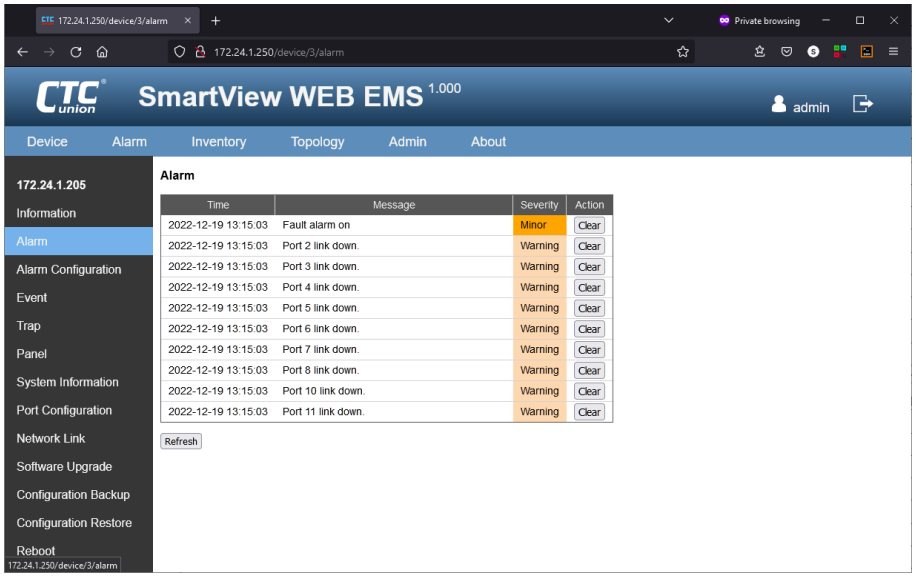
Make any changes here, then click the Apply button.

6) Manage a device



Bring up the "Device" tab to display all manageable devices. Click on the device's IP address to manage through Web EMS. Alternatively, click on the "HTTP" button to directly log into the device's Web management.

4.2.17 Device Managed via Web EMS



The first page displayed will be the 'Alarm' page. Other menu items will allow configuring the device or displaying information.

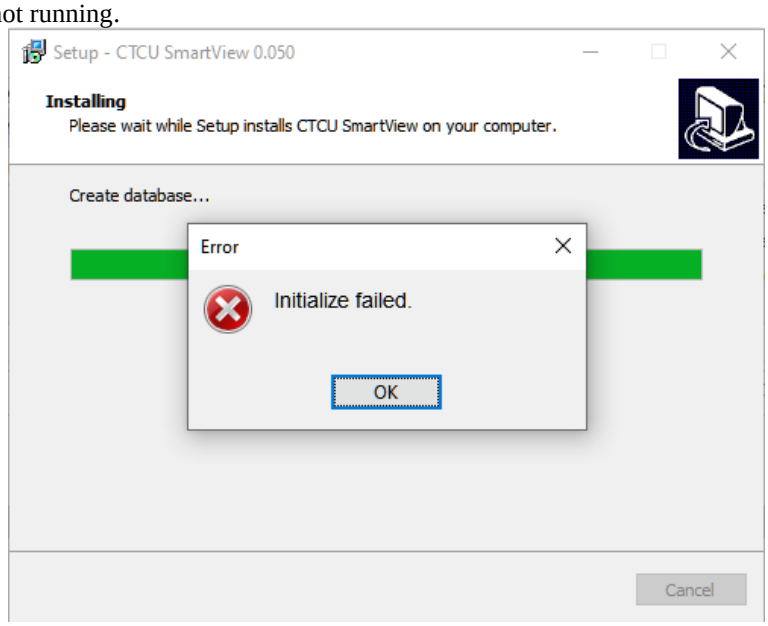
1) Information: This will display the device "Name", the "IP Address", the model "Type", the connection "Status", SNMP version, the device "Software Version" and the "Alarm Status".
2) Alarm Configuration: The alarm types available for this device will be listed. Interfaces are set by check boxes. Alarm severity is assigned from pull-down menus. Finally, an "Apply" button will accept the changes.
3) Event & Trap: These will display those events and traps specific for this selected device.
4) Panel: This will display a graphic representation of the device's front panel with all port and LED states.
5) System Information: This will display the device's MAC address, the hardware version, system date, system uptime, software version and the software compilation date.
6) Port Configuration: All of the ports for the device will have port status displayed and may have the ports configured as 'Auto' or 'Forced' or may be disabled.
7) Network Link: When devices deploy LLDP, all neighboring devices will be displayed on each port.
8) Software Upgrade: This supports updating the device's software.
9) Configuration Backup: The configuration for the device may be downloaded to the user's PC.
10) Configuration Restore: A previously saved configuration file may be uploaded and made active on the device.
11) Reboot: A cold boot for the device may be done remotely. Exercise care, as traffic will be blocked through a device while it reboots and reloads its configuration.

This page left blank intentionally.

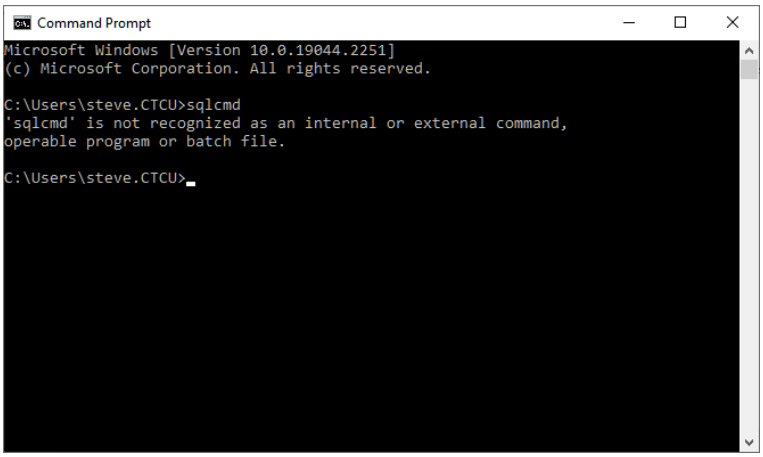
Chapter 5 Troubleshooting

5.1 Installation Errors

If you see this error message pop up during the "Create database" portion of the installation, chances are the MSSQL Server did not install or is not running.



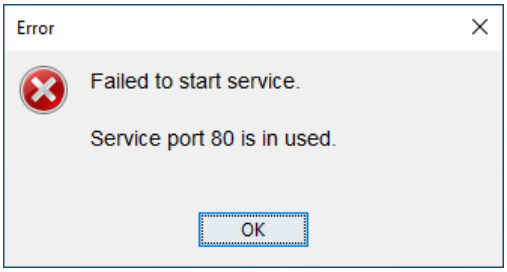
Open a command window and type the 'sqlcmd' command. If you see that the command is not recognized, then MSSQL has not been properly installed.



1. Check "Programs and Features" under the Control Panel. If the Microsoft SQL Server is not installed, do a manual installation as described in Appendix A.
2. If the program appears to be installed, it probably does not have a Default Instance or be in Mixed-Mode. Uninstall all the SQL programs via "Programs and Features", then reboot the system. Delete any Microsoft SQL Server folders under \Program Files. Either re-run ems_full installer or manually install MS-SQL Server following the guide in Appendix A and run ems_full while unchecking the "install database SQL Express" check box.

5.2 Startup Errors

When starting the Web EMS Server, the following message indicates that some other application is using the HTTP service port.



Open the Services panel in Windows (WinKey + R, services.msc). Search for the "World Wide Web Publishing Service" and click it. Stop the service and set the Startup type to disabled. If the IIS server is not enabled, find what program is using port 80.

1. From a command prompt type netstat -ano
2. Search the list to find port 80 (for TCP/UDP) and which PID is using it.
3. Open Taskmgr and find which process is using that PID.
4. Kill the process or look again for it in Services and Stop then disable the process startup.

5.3 Enable Administrator Account

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

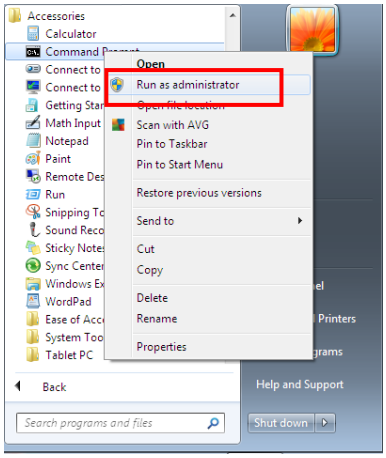
Note: Only Professional or Enterprise versions of Windows can support enabling the administrator user. In addition, this may cause a security issue if someone has physical access to the machine or if it should become compromised. For better security, it is still recommended to use a normal user account and follow the instructions in 8.1 Take Permission of WEB 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 WEB EMS on these flavors of Windows, it is best to place the WEB EMS installation folder into a writeable user location rather than in 'Program Files'.

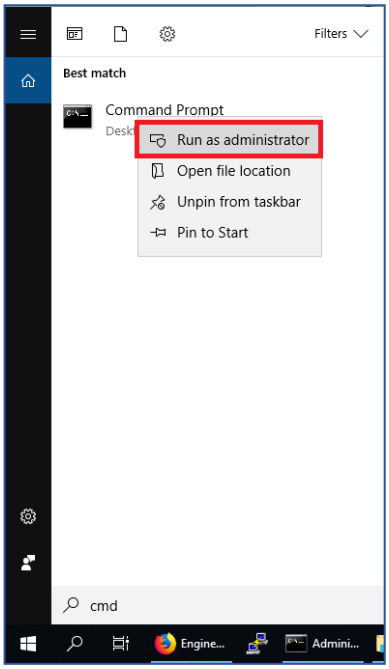
5.3.1 Enable Administrator using Command

This is the quickest way to enable the administrator account on Windows 7-10.

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.



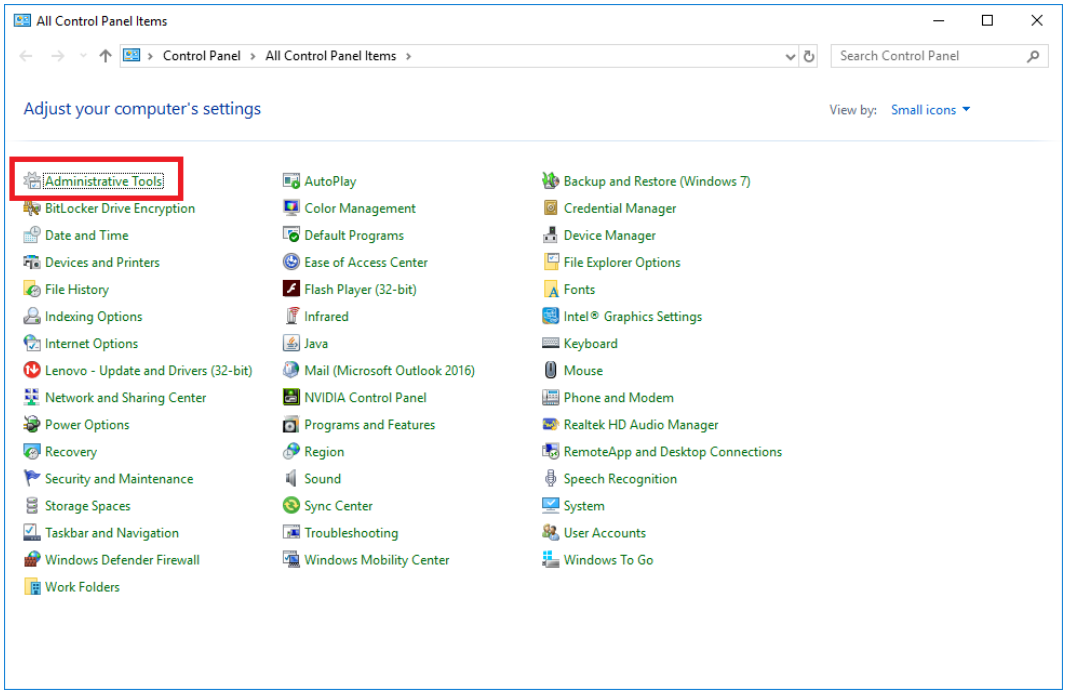
Step 2. In the command window type in the command exactly as below.

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

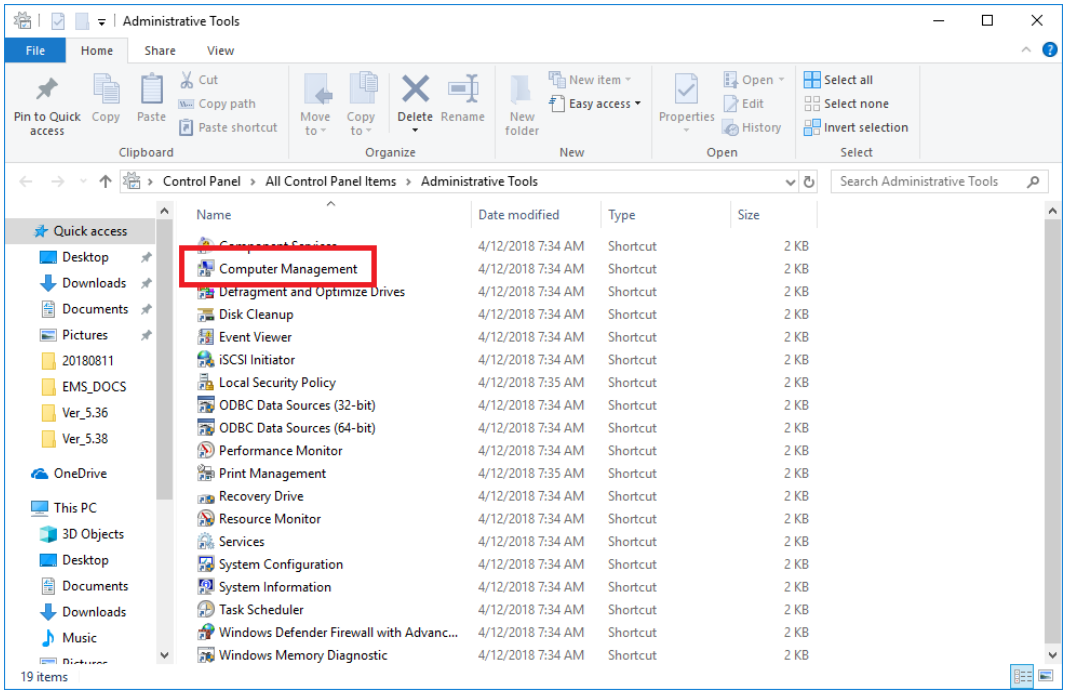
Step 3. Exit and logoff. Then login as administrator and set password.

5.3.2 Enable Administrator Account Using Control Panel

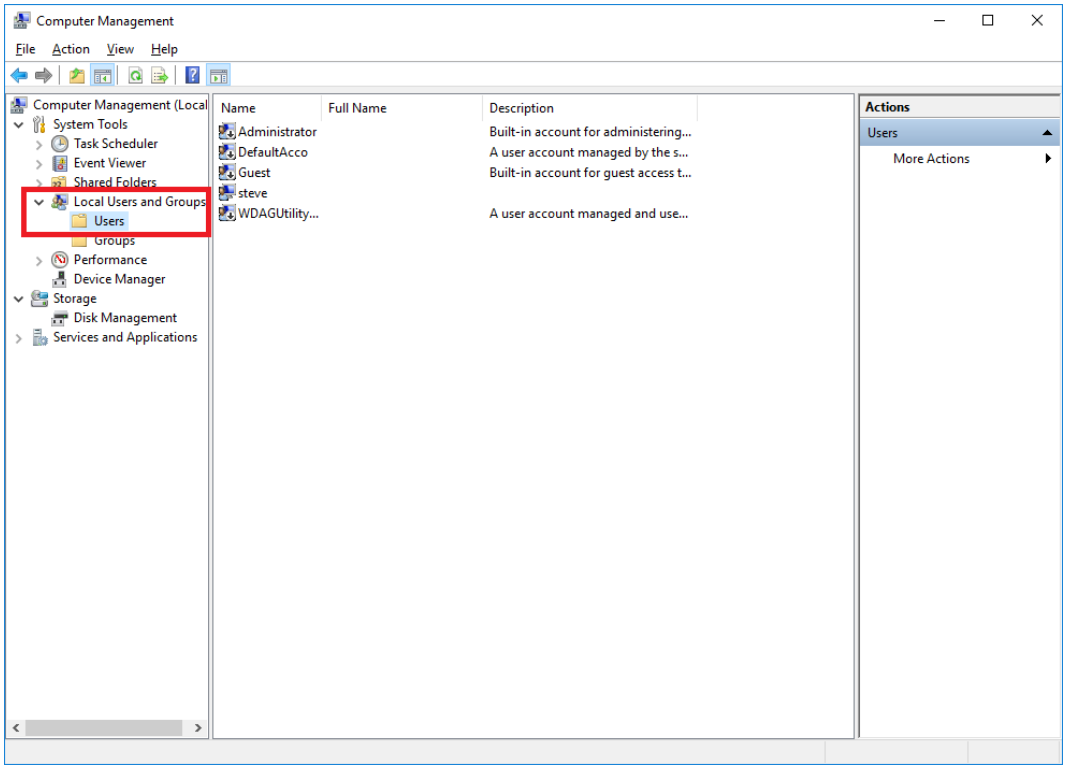
Step 1. Use **Windows Key + r** (Run) and key in **control**. Double click **Administrative Tools**.



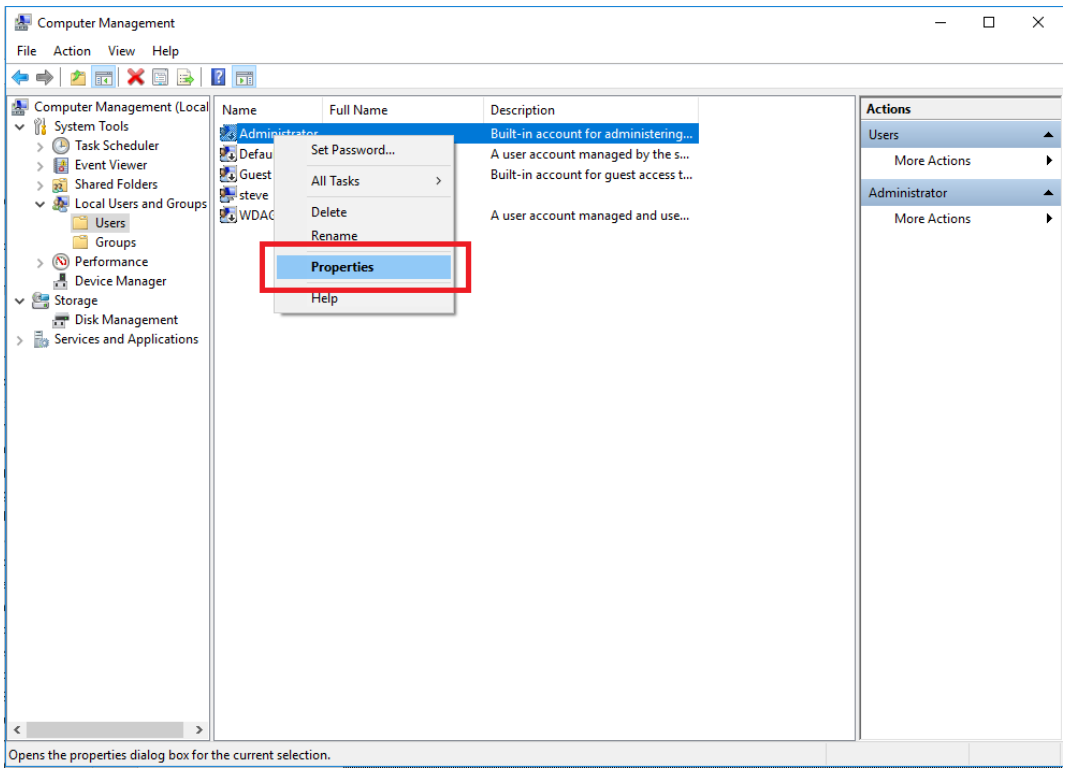
Step 2. Double click **Computer Management**.



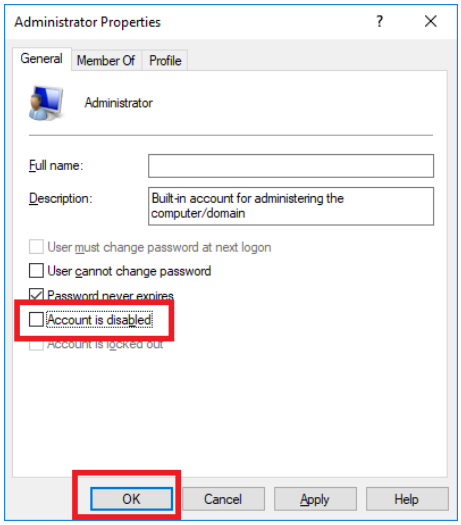
Step 3. Open up the "Local Users and Groups" and select "Users".



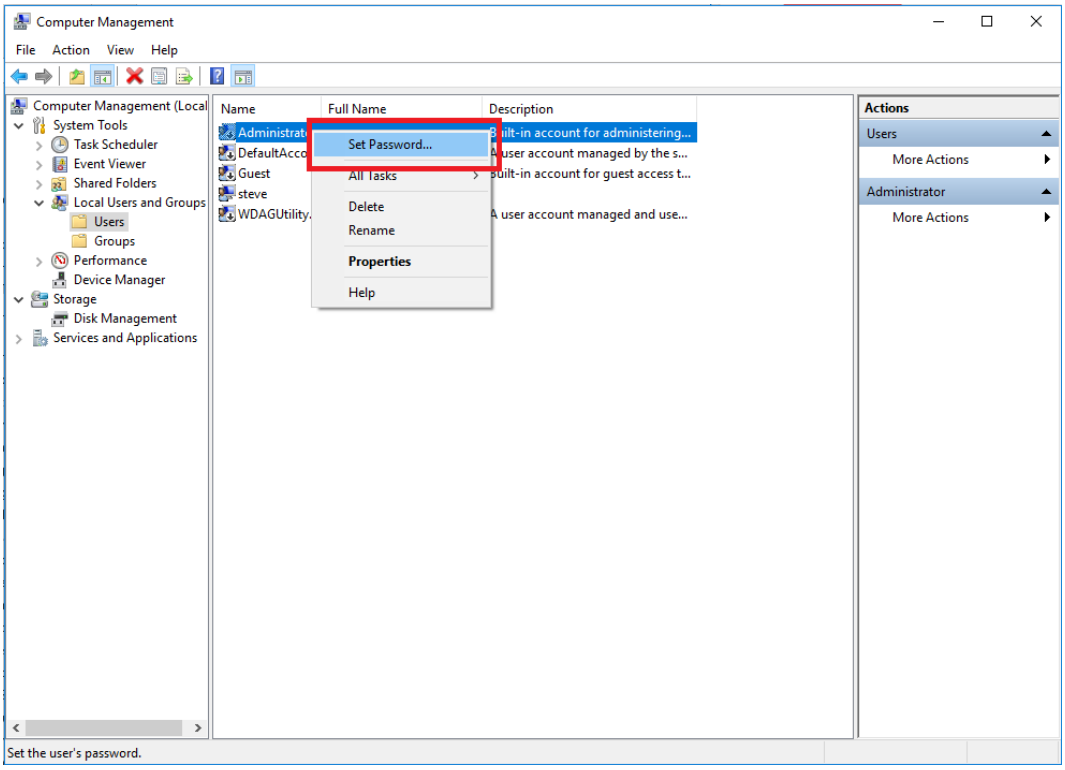
Step 4. Right-click on the user **Administrator** and click **Properties**.



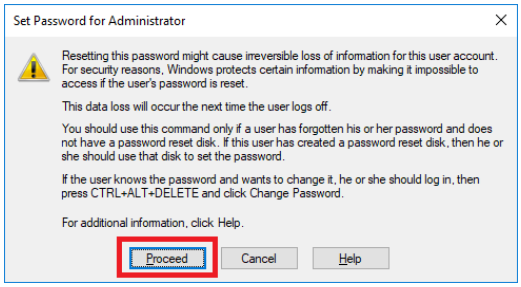
Step 5. Uncheck the "Account is disabled" check box and click OK.



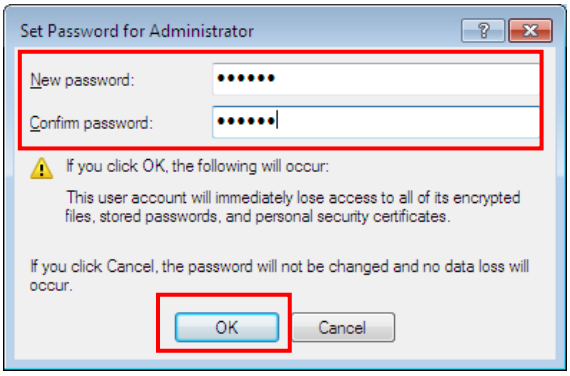
Step 6. Right-click the **Administrator** again and this time select **Set Password**.



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



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

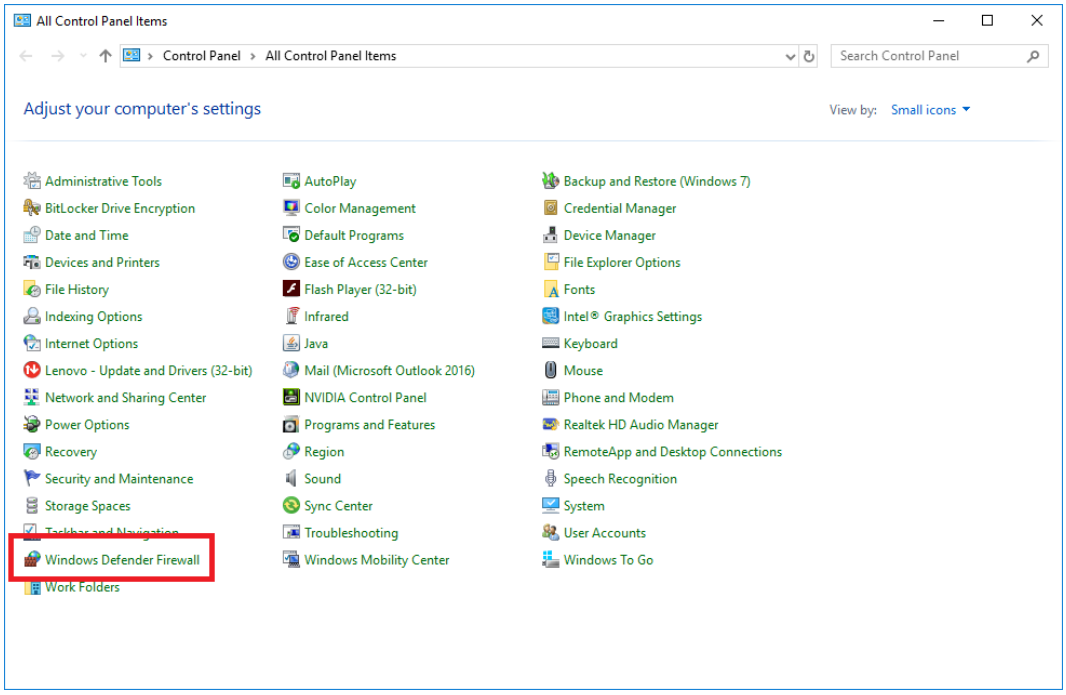


Now logout and log back in with the now activated administrator account.

5.4 Open Firewall for SNMP Traps

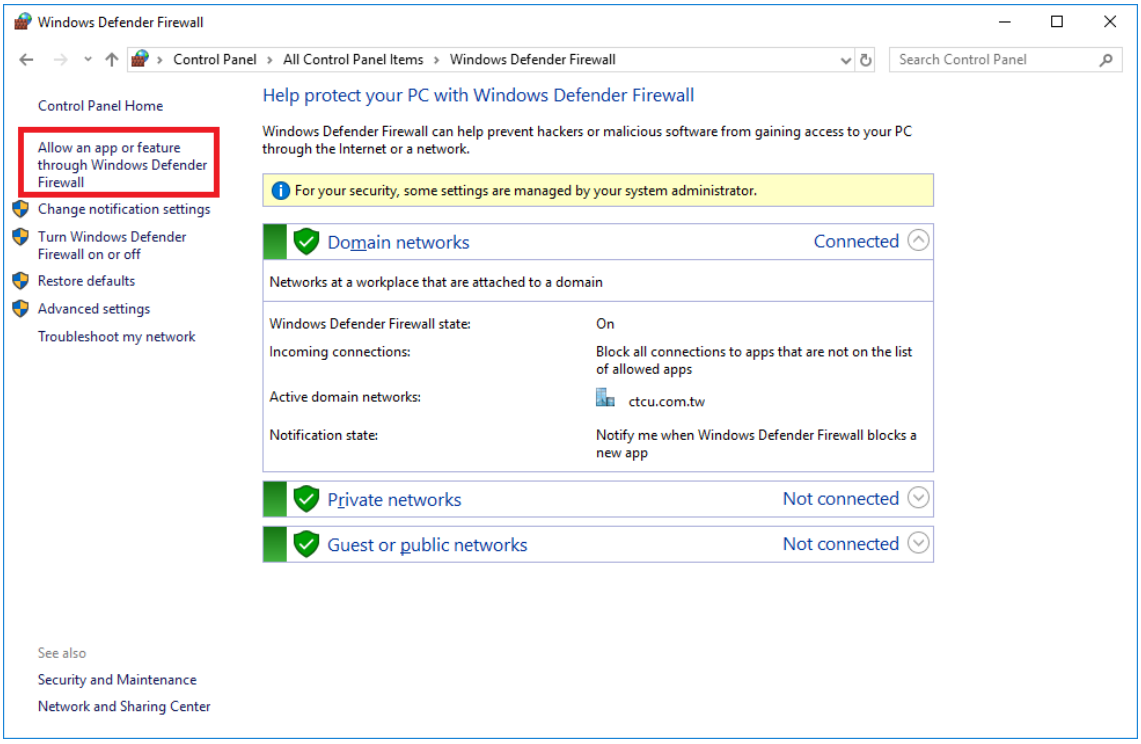
Both Windows 10 and Windows Server 2016 have SNMP Traps blocked by default. The WEB EMS server will not show any traps until the Firewall is opened for SNMP Traps.

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

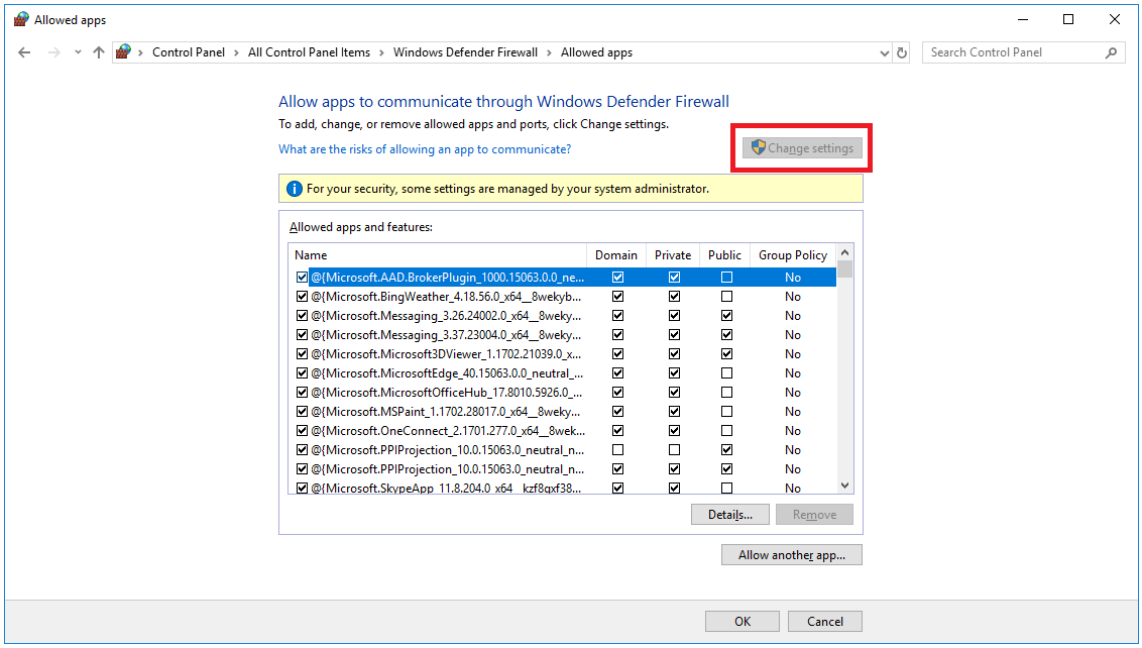


Step 2. Double click the **Windows Defender Firewall**

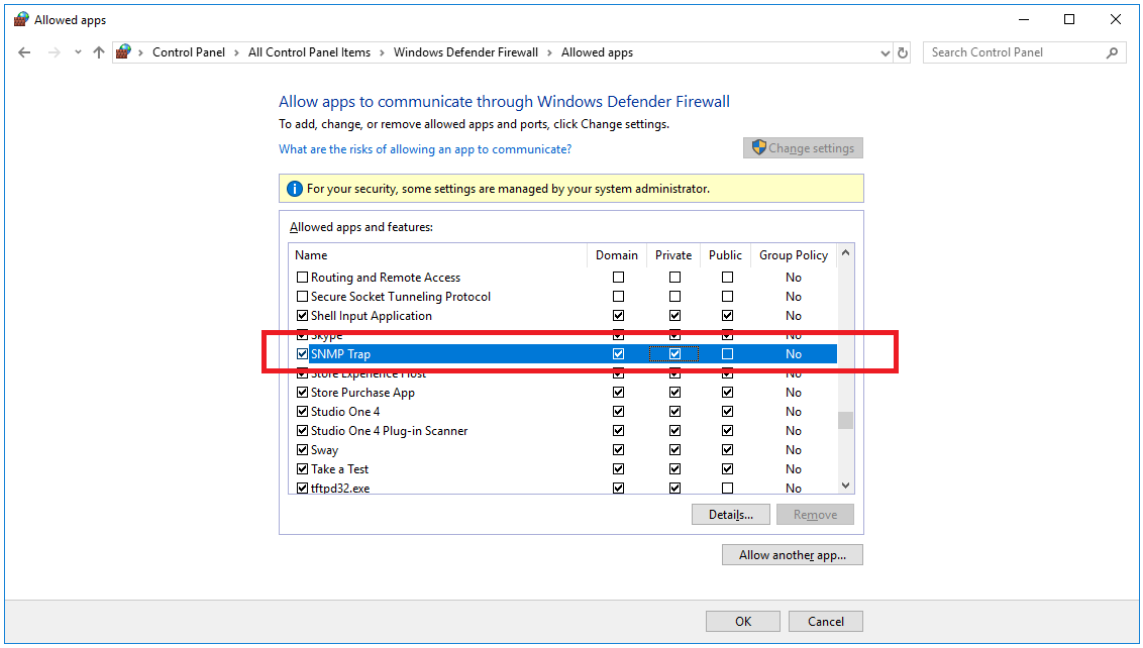
Step 3. Click the **Allow an app or feature….**



Step 4. Click **Change settings**



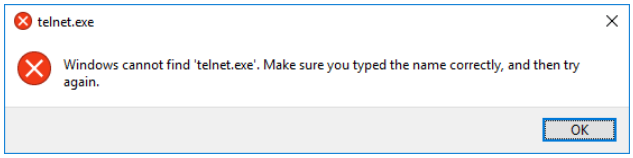
Step 5. Pull down and find **SNMP Trap**, then enable the check box. Finally, click **OK**.



SNMP traps will then be received by Smartview Web EMS.

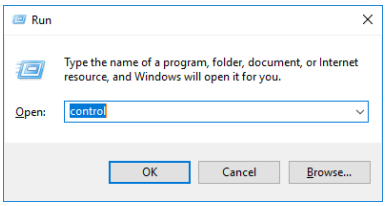
5.5 Telnet Won't Open when Right Clicking Device

Have you been presented with the following pop up window?

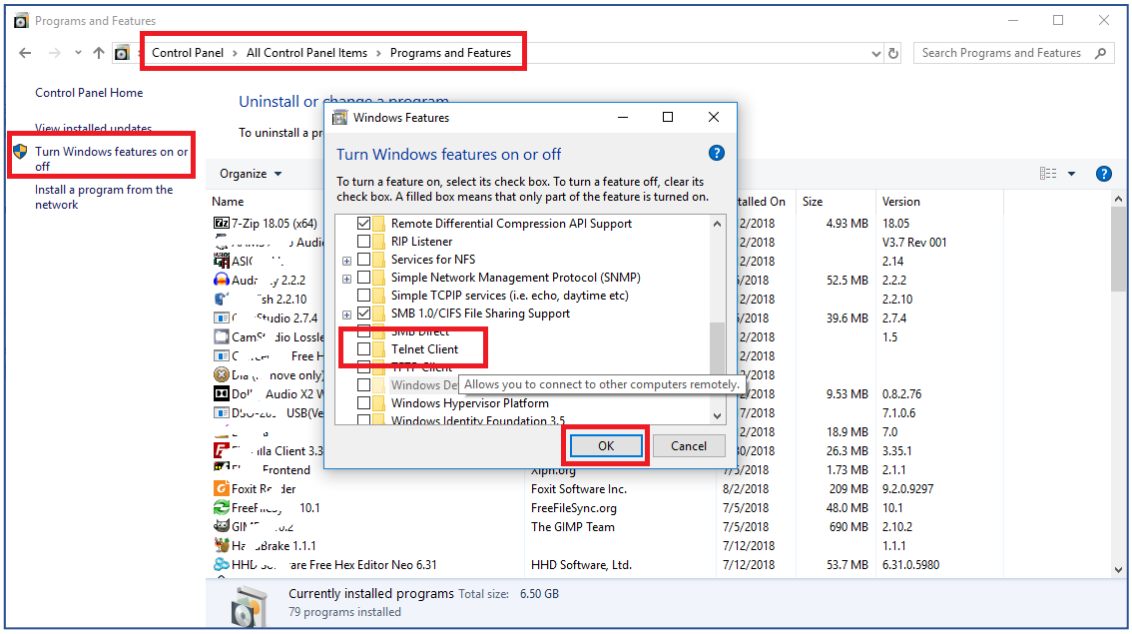


We have found that the Telnet client is NOT active by default for either Windows 10 or for Windows Server 2016.

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

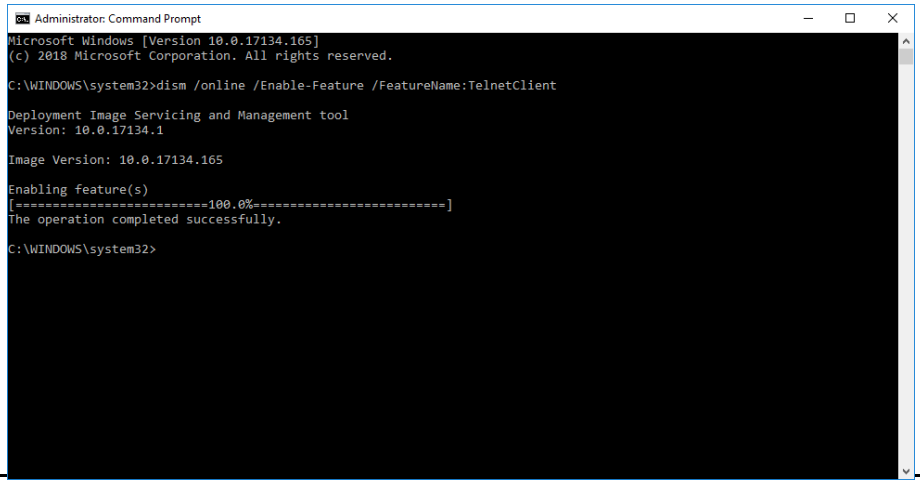


Step 2. Double click **Programs and Features**. Click **Turn Windows features on or off**.



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

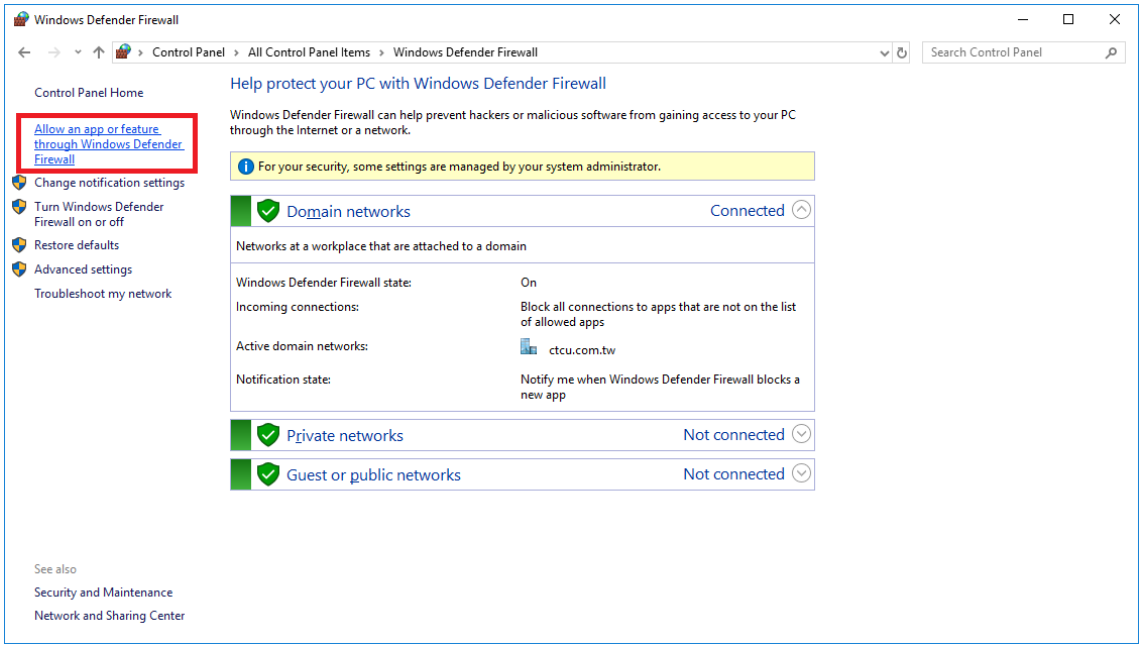
If you feel confident using the command prompt, it is possible to enable this feature with elevated privileges: **dism /online /Enable-Feature /FeatureName:TelnetClient**



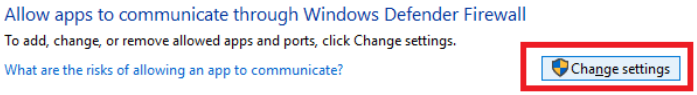
5.6 Modifying Firewall

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).

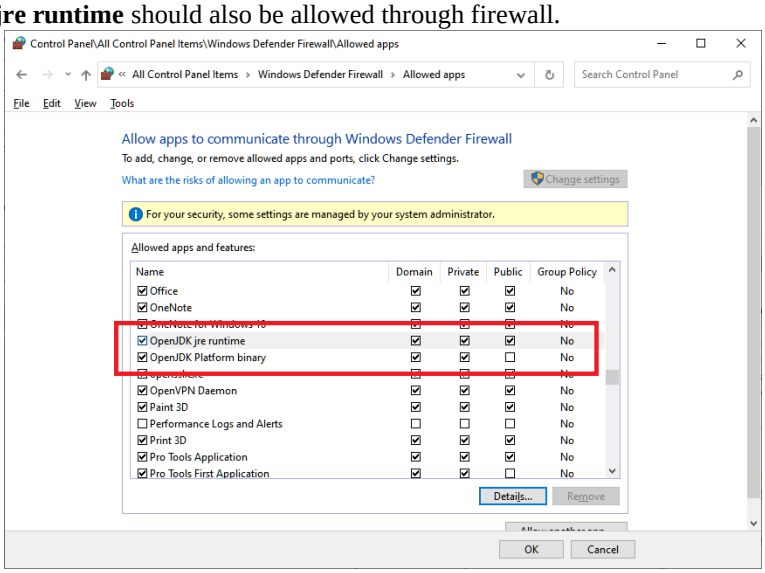
From **Windows Defender Firewall**, under **Control Panel**;
Step 1. Click 'Allow an app or feature…'



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



Step 3. Scroll down and find and highlight the app labeled **OpenJDK platform binary**. Click the **Details** button and confirm. The **OpenJDK jre runtime** should also be allowed through firewall.



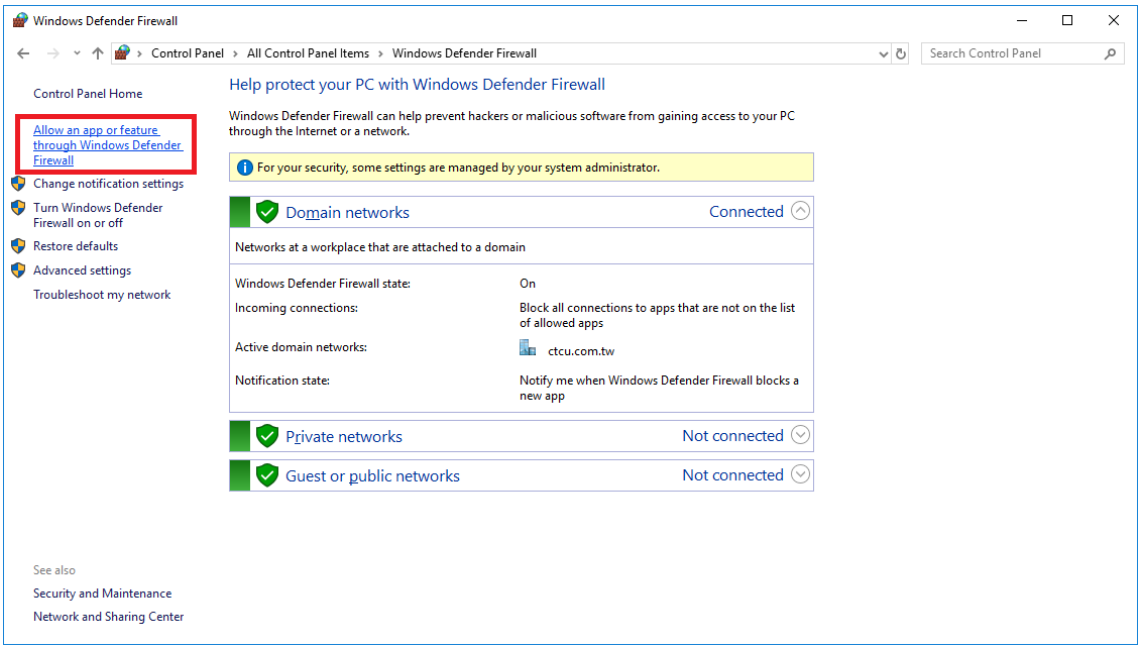
Step 4. The pop up has identified the name server app used by WEB EMS Server. Click OK and adjust the communications (Domain, Private, Public) accordingly.

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

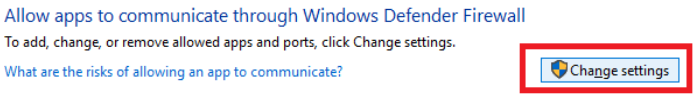
5.7 Adding App to Firewall

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.

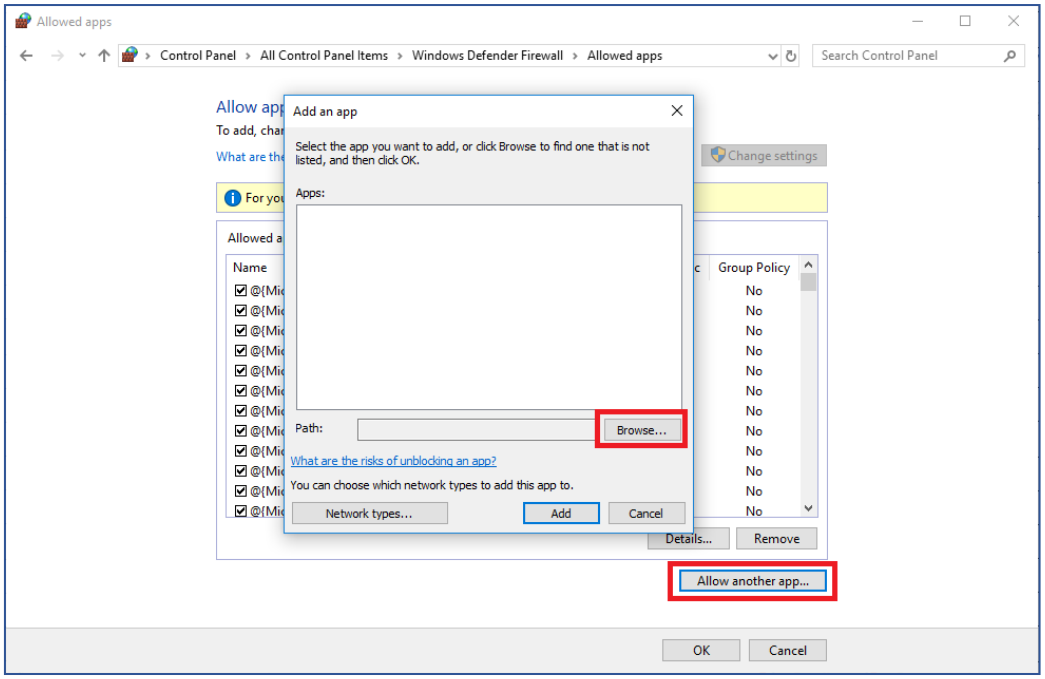
Step 1. Click 'Allow an app or feature…'



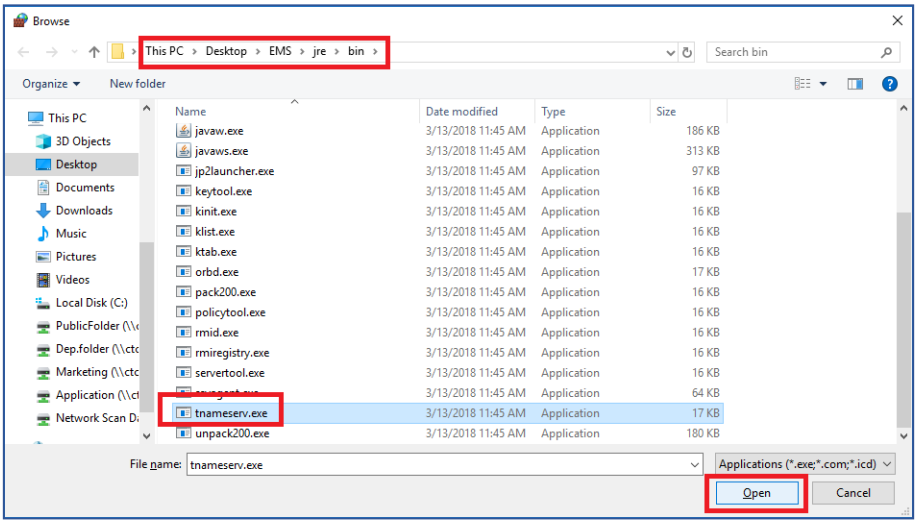
Step 2. Click the **Change settings** button.



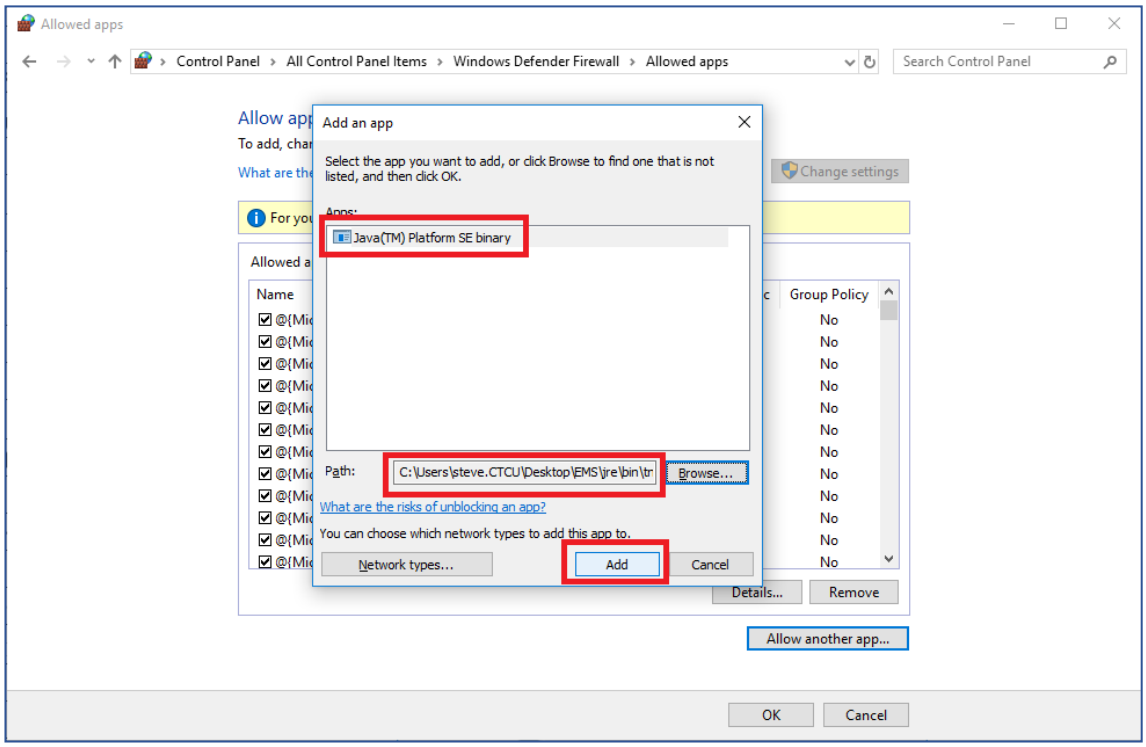
Step 3. Click the **Allow another app** button.



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



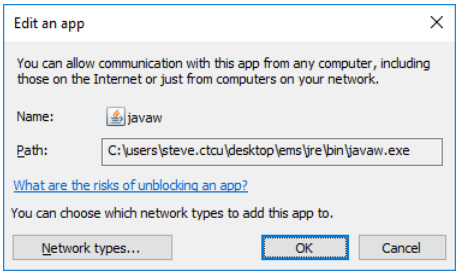
Step 5. Locate your client folder (example here is Desktop\WEB EMS) and find the binary file to open. Do this for both the **javaw.exe** file and the **tnameserv.exe** files.



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.

WEB EMS Java Client
(client on Desktop)



5.8 Database and Connection Issues

Most problems that arise with WEB 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.

5.8.1 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.

5.8.2 Network Issue

If SQL Server is running on the same machine as the WEB EMS Server, the network is NOT an issue. WEB EMS Server should always be able to make local connection without a working network, if *localhost* was chosen during Smartview WEB EMS installation. In our WEB EMS installation, we rely on a *localhost* connection (127.0.0.1), as it provides the best performance when the SQL Server and WEB 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.

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

SmartView WEB 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 WEB 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 **WEB 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 **WEB EMSinstaller** do the **MS-SQL Express** installation to avoid these pitfalls.

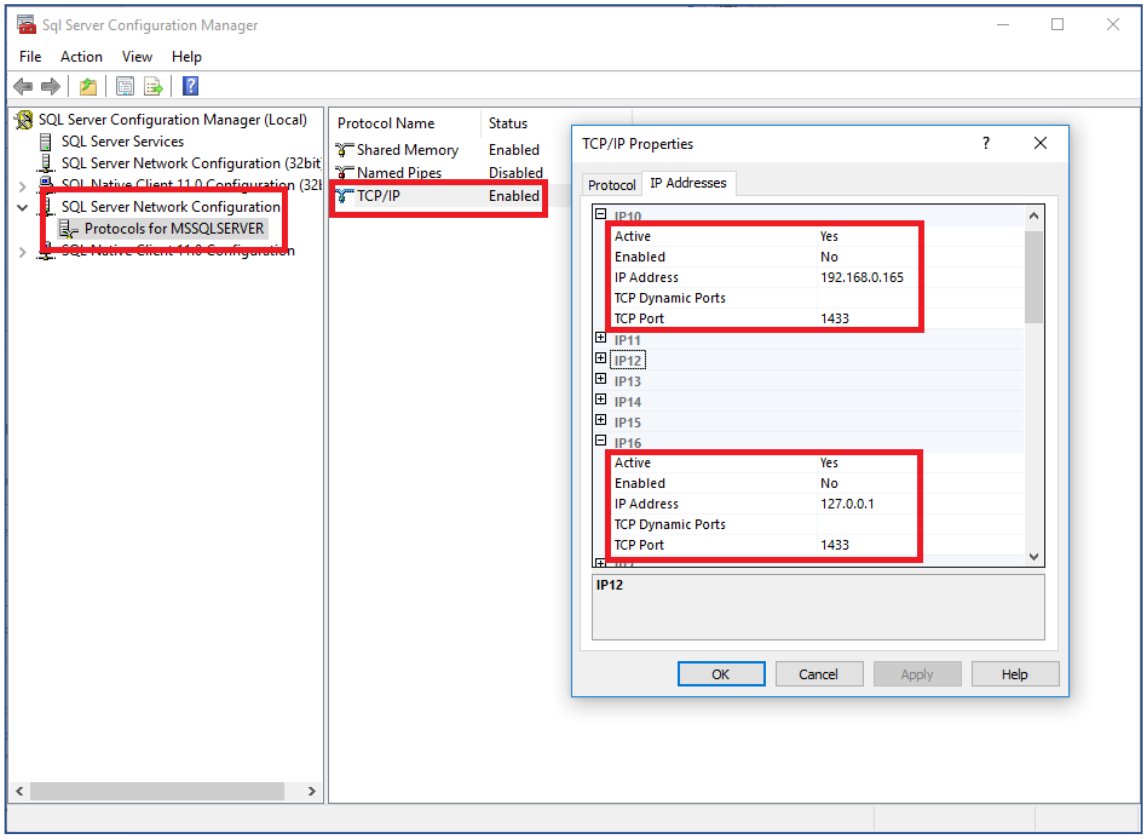
5.8.4 Must Restart WEB EMSinstaller

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

5.8.5 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 WEB 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 WEB 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.

5.8.6 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 WEB 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.

5.8.7 Connection Tests

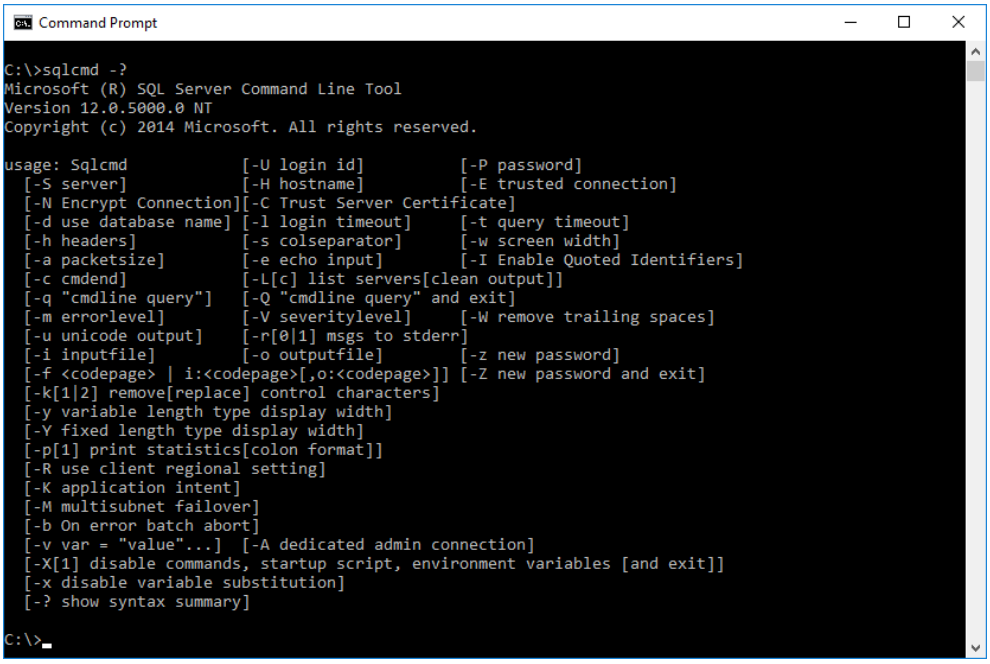
At this stage, you can test your connection using some tools. The tests need to be done on a client machine.

First try:

telnet <your_target_machine> <TCP_Port>

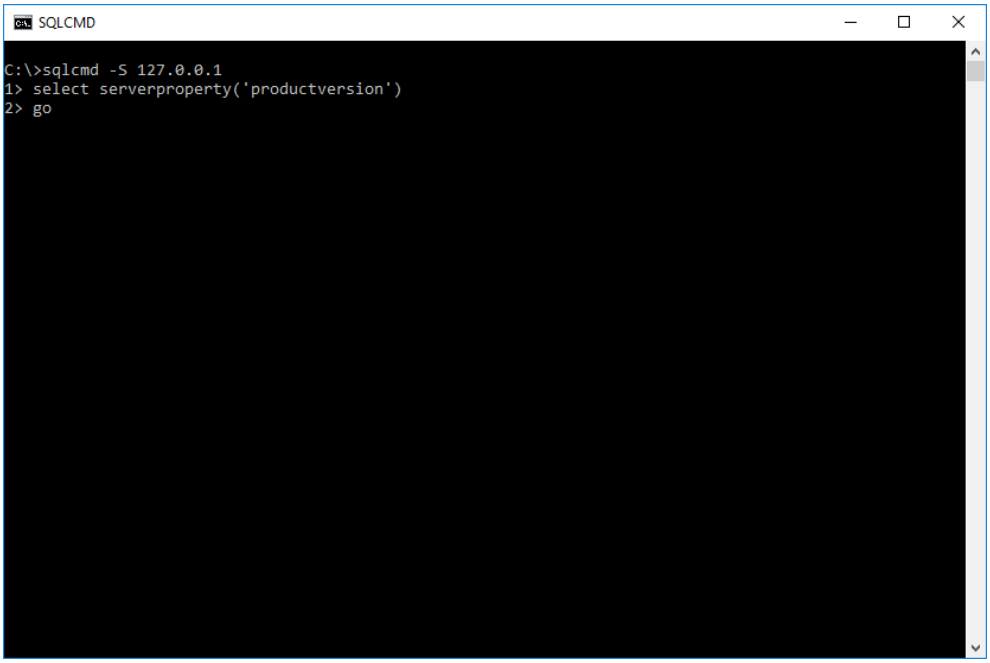
You should be able to telnet to the SQL server TCP port (1433) if TCP is enabled. Then, use SQLCMD and/or **SQL Management Studio** to test SQL connections. If you don't have those tools, please download SQL Express from Microsoft and you can get those tools for free. Another way to quickly troubleshoot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

sqlcmd -?



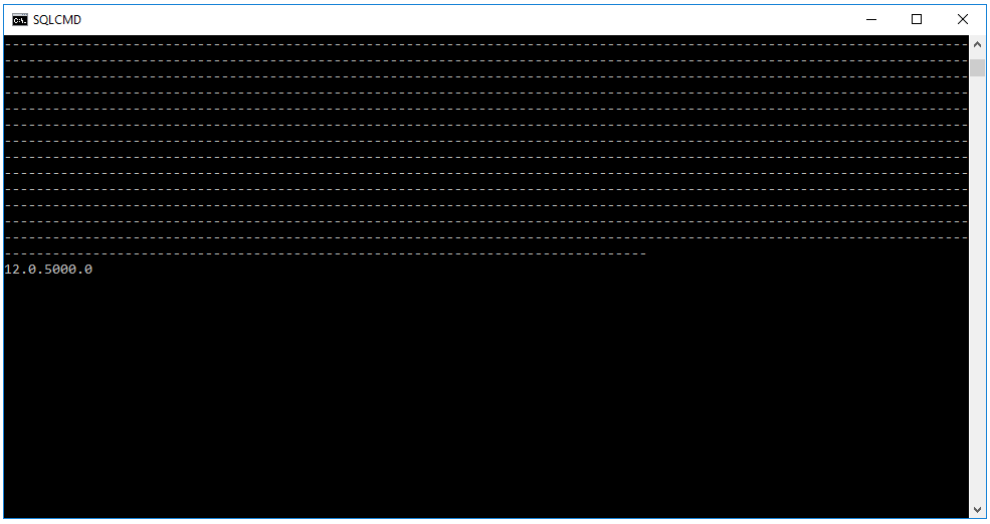
sqlcmd -S <your_target_machine>

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



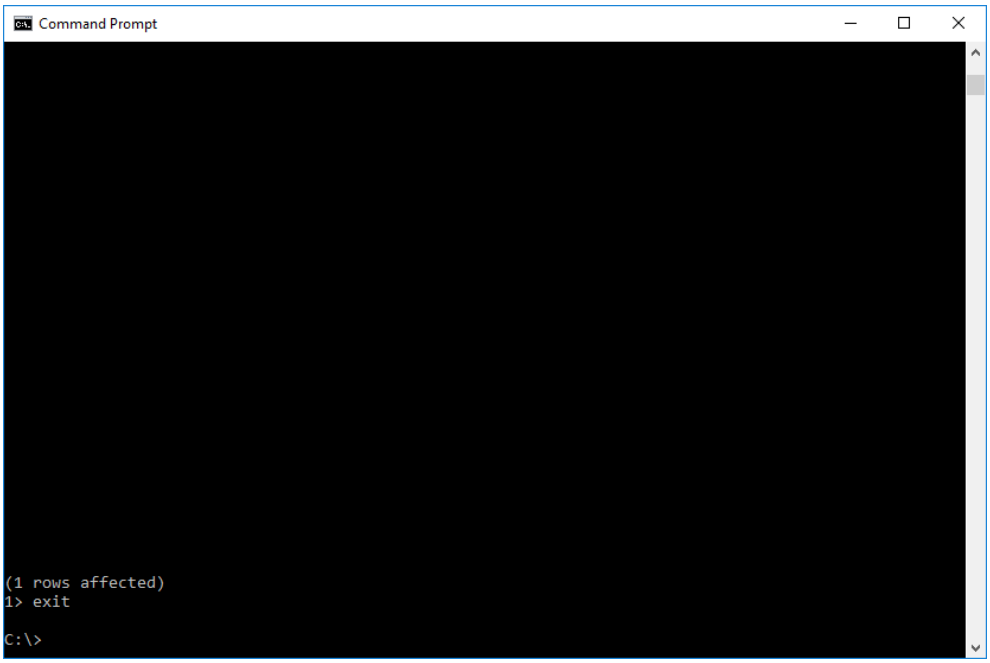
Example for finding your SQL Server version.

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.

5.8.8 Application Issue

If you succeed with steps 8.3.1~8.3.7 but still see failure in your WEB EMS application, 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.

5.8.9 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:

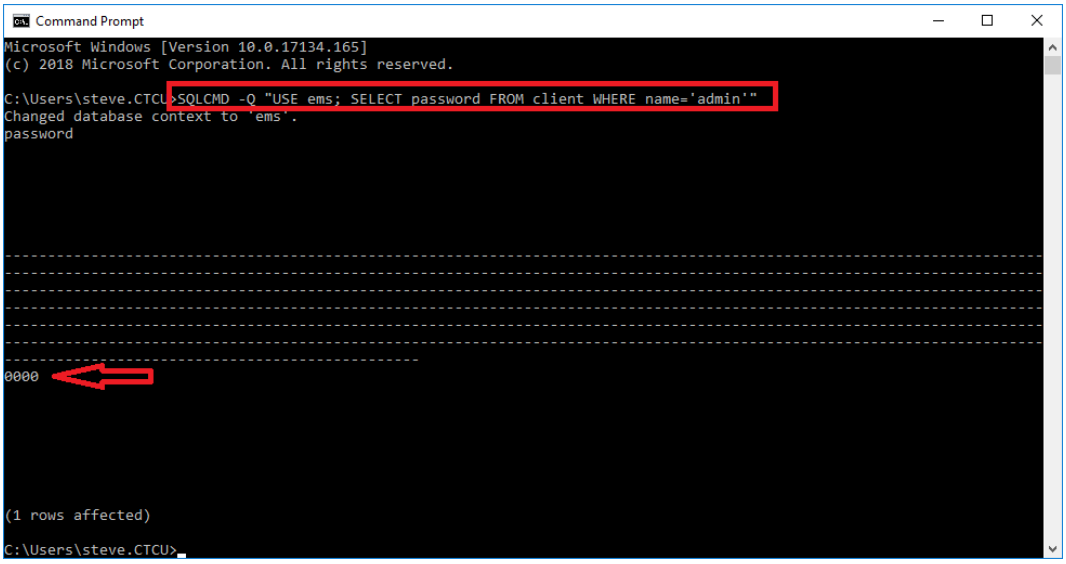
SmartView WEB EMS uses **SQL Auth**, therefore mixed authentication must be enabled. Check this page for reference http://msdn.microsoft.com/en-us/library/ms188670.aspx.

In our WEB 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 WEB EMS User Manual. Better yet, use the **ems_full installer** to install MS-SQL Server.

5.9 Forgot WEB EMS Admin Password

The default admin password for WEB EMS Server is 00000000 (eight 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 Web EMS; SELECT password FROM client WHERE name='admin'"
```

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

5.10 Complete WEB EMS System and Database Backup

It may be prudent to do occasional WEB 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 WEB EMS upgrade so that in case of trouble, the previously working system may be restored.

Backup:

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

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

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

Now that the WEB 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 WEB EMS.

These files may also be used to clone the WEB 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\WEB EMS and copy the old contents into the WEB EMS folder. Have all users take permission of the new WEB 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 Install MS-SQL Server 2019 Express

A.1 Introduction

This chapter will detail the installation steps for the Free Edition of MS-SQL, Microsoft SQL Server 2019 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 2019 Express can be installed on Windows Server 2016, Windows Server 2019, Windows Server 2022 and Windows 10/11

Note:

SQL Server 2019 Express Edition is differentiated from the rest of the SQL Server 2019 editions only by the following:

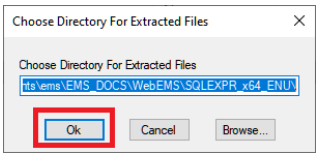
Lack of enterprise features support
Limited to one CPU socket or 4 CPU cores
One GB memory limit for the SQL Server Engine
Databases have a 10 GB maximum size

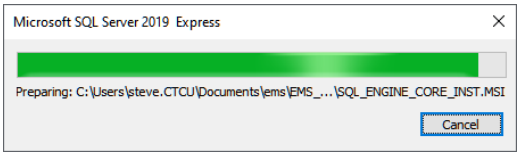
A.2 SQL Express Software Installation

In the following example, the step-by-step procedure is given for the free version of Microsoft® SQL Server 2019. The free version may be downloaded from Microsoft's Download Center website and is a good choice for demonstrating or for evaluating the WEB EMS in a non-production or production environment.

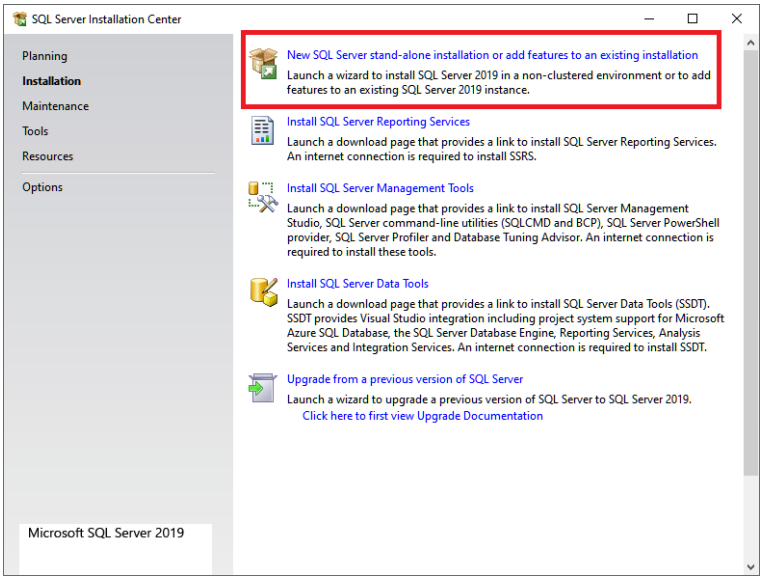
Find the location of your download files on the local disk and double-click into the ' SQLEXPR_x64_ENU.exe' icon.

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

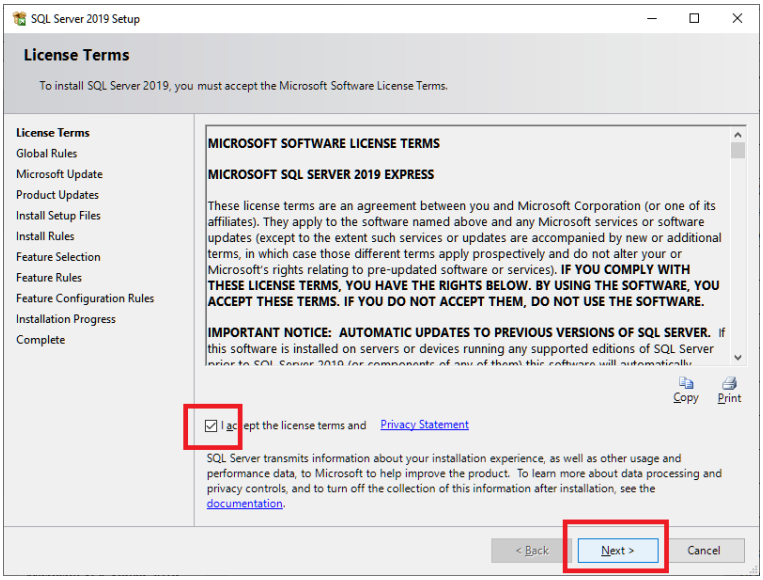




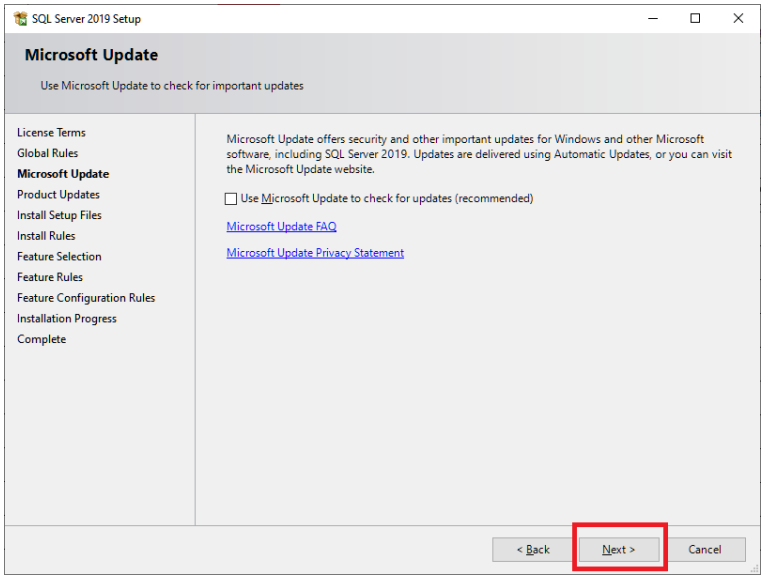
The 'SQL Server Installation Center' will be the starting point for either a fresh SQL Server installation or for upgrading from a previous SQL Server version.



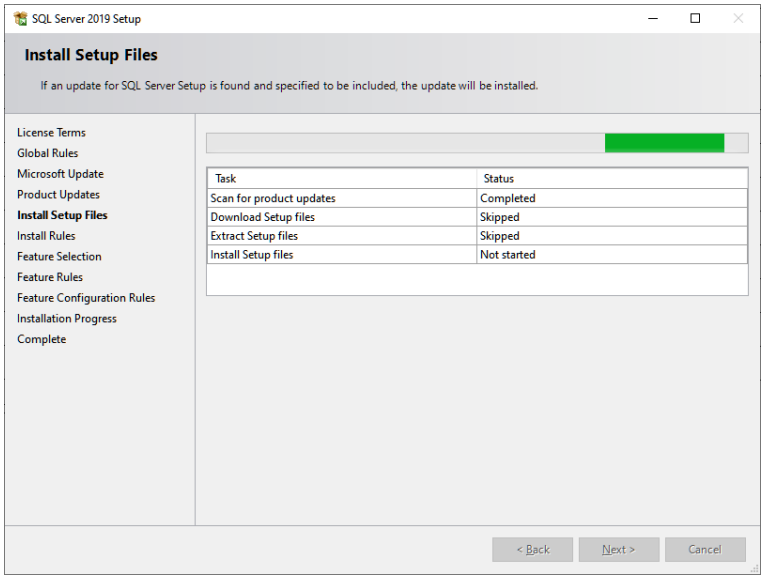
Double click the 'New SQL Server' to launch the installation wizard.



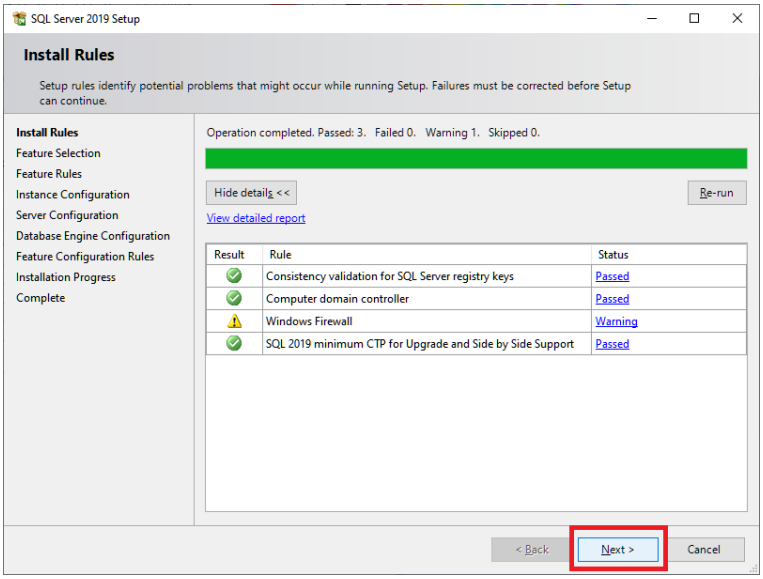
Check the "I accept the license terms." check-box and click the "Next" button.



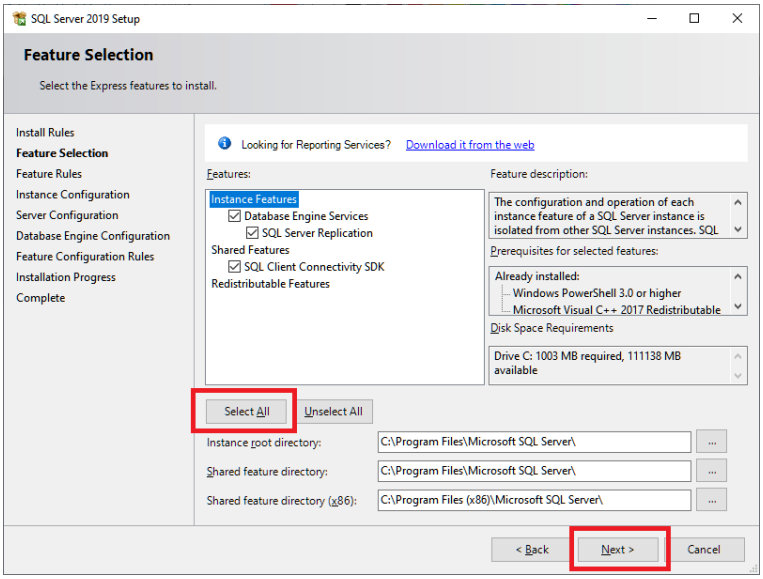
Click "Next" on this Microsoft Update page.



The following screen indicates the Install Rules check. Click "Next" to continue.

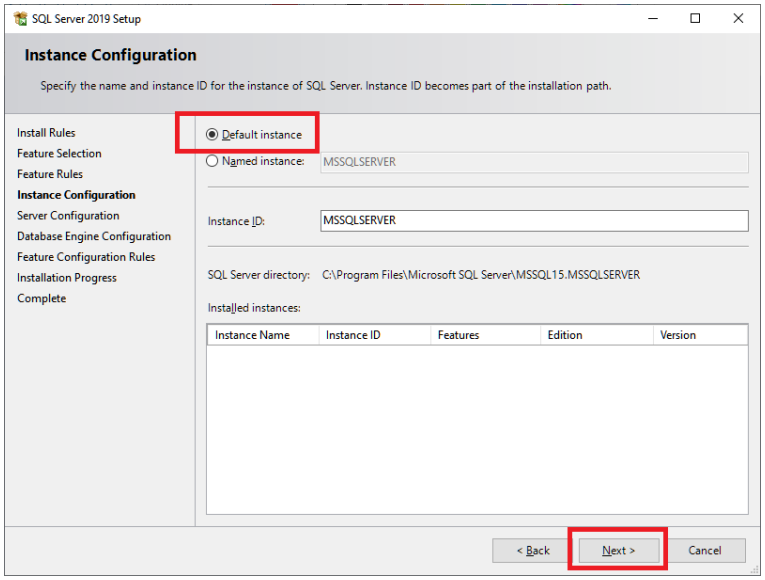


The following screen is for feature selection. Make sure all features are checked, then click "Next".

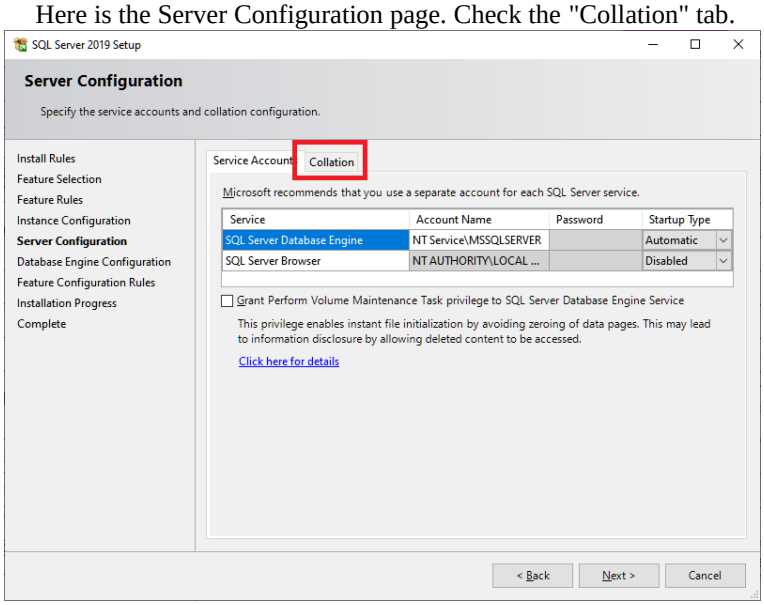


SQL Server 2019 requires MS Visual C++ 2017 Shell and if not on your system it will be installed from the installation files.

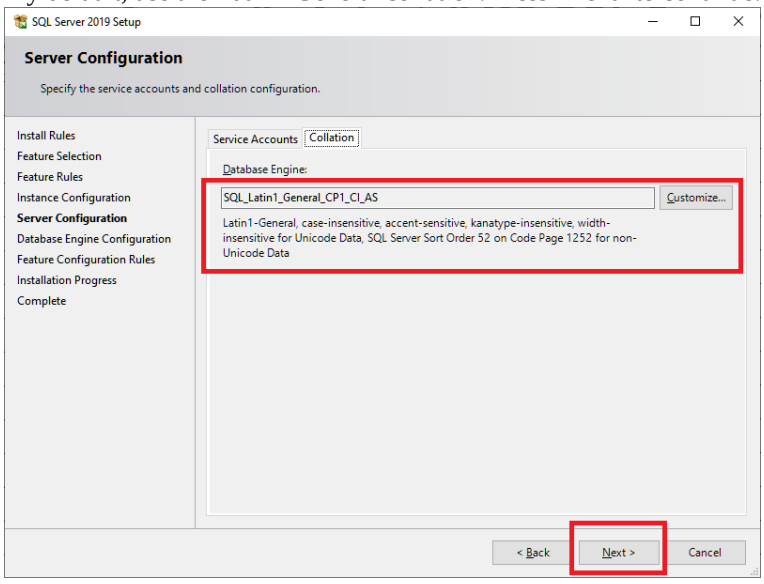
This screen shows the Instance Configuration. IMPORTANT!! Change the selection to "Default instance" then click "Next". Failure to choose the Default instance will result in incompatibility with Web EMS.



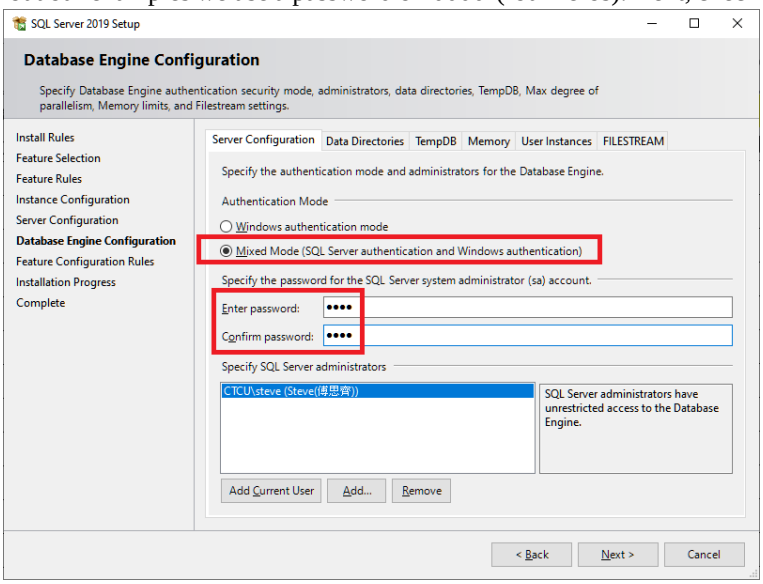
Here is the Server Configuration page. Check the "Collation" tab.



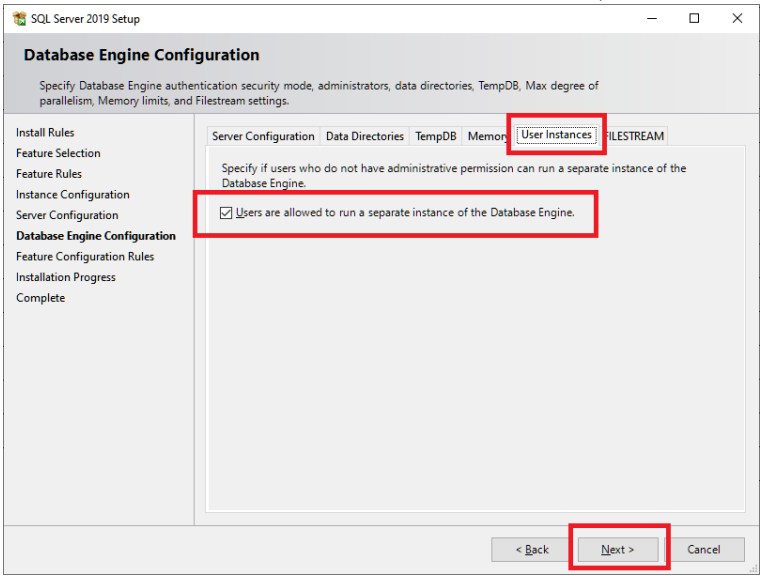
By default, use the Latin1-General collation. Press "Next" to continue.



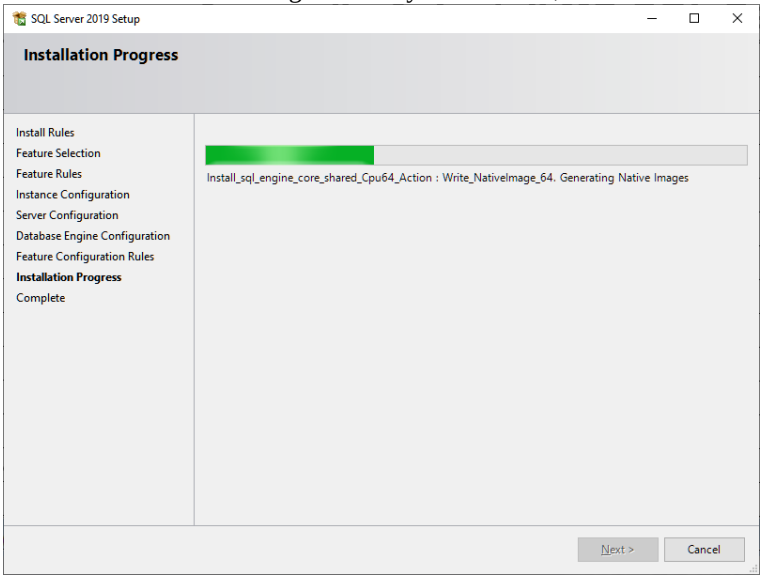
The following is the Database Engine Configuration. IMPORTANT!! Switch to "Mixed Mode" and enter the sa password twice. (throughout our examples we use a password of '0000' (four zeros). Next, check the "User Instances" tab.



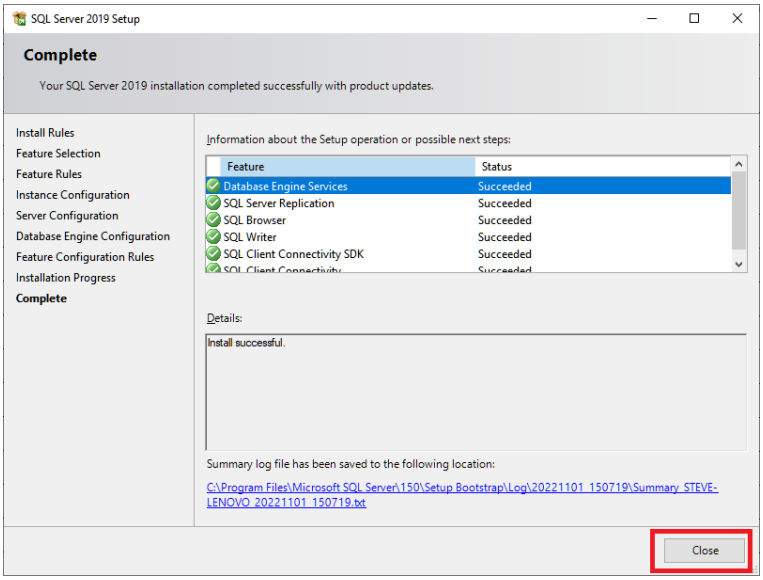
Make sure the check box is checked under "User Instances", then click "Next".



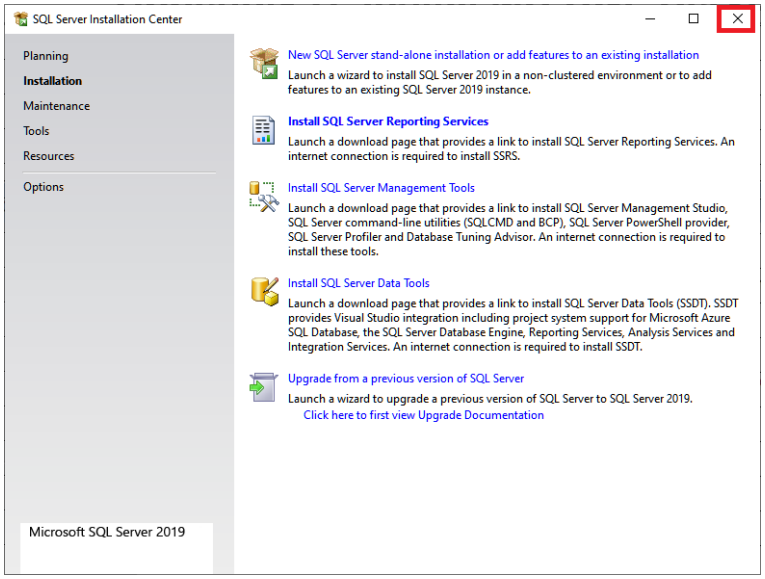
Now observe the Installation Progress. If any errors occur, click "OK" and "Retry".



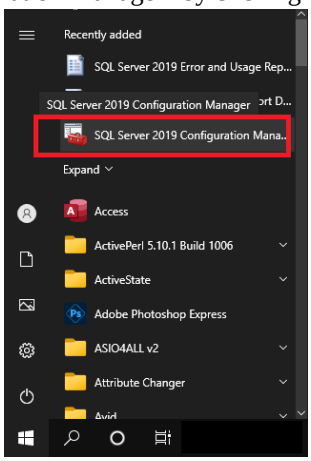
The application has now been installed. Click "Close".



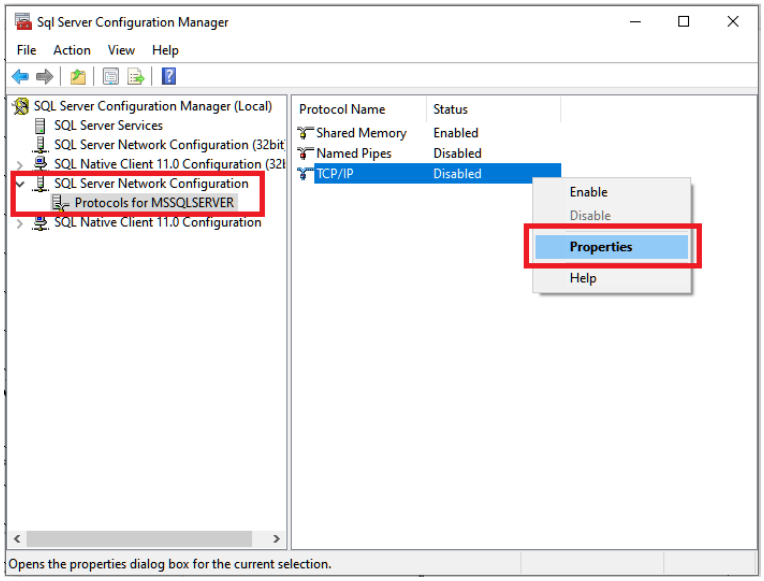
Close the Installation Center window.



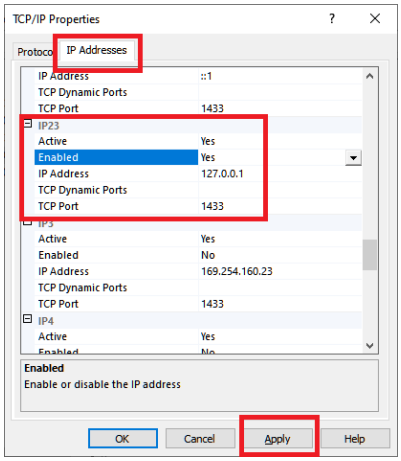
Open the "SQL Configuration Manager" by clicking "Start > SQL Server 2019 Configuration Manager".



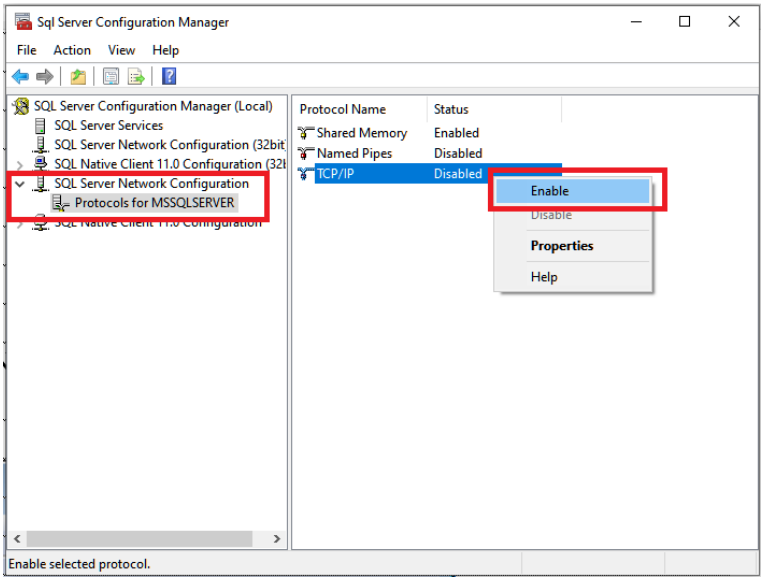
Find the "Protocols for MSSQLSERVER", under "SQL Server Network Configuration. Right-click on TCP/IP and select 'Properties'.



First, under the "IP Address" tab, make sure the Local Host connection is 'Active' and 'Enabled' and that the TCP Port is 1433. Web EMS connects to the database through the localhost IP (127.0.0.1). Click "Apply".

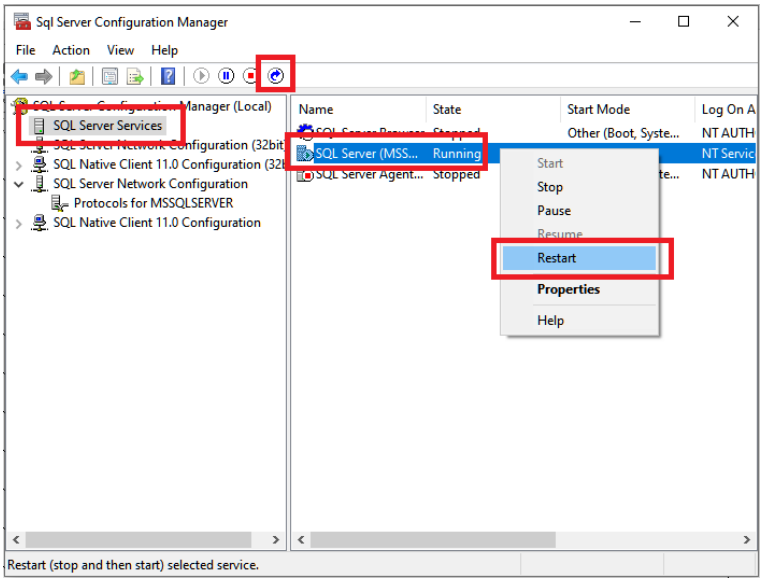


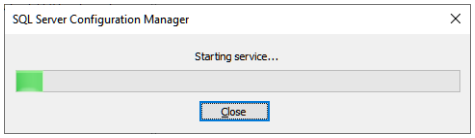
Next, right-click "TCP/IP" again and 'Enable' TCP/IP.



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 2019 Express.

CTC union®

www.ctcu.com

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