PacStar IQ-Core Software Getting Started Guide

The following guide is for viewing outside the IQ-Core Software help system and is suitable for printing. If you are using IQ-Core, open the Help Window (F1 anywhere) to view this same guide with access to all help information.

IQ-Core Software v3.9.40

Feb 2019

Army WIN-T Edition Overview

IQ-Core Software is a communication management application used on a variety of WIN-T nodes including:

- Joint Network Node (JNN)
- Battalion Command Post (BCP or CP)
- Single Shelter Switch (SSS)
- Tactical Hub Node (THN)
- Unit Hub Node (UHN)

The WIN-T edition of IQ-Core Software has all the base features of IQ-Core Software but also includes some unique capabilities relevant for managing WIN-T nodes. These include a Apply Profile Wizard which helps you quickly configure IQ-Core to match the node type you are on.

IQ-Core Software runs on Element, LAN, and Node Manager laptops. It consists of a Client (UI) and a Server application. When configured on a Node manager laptop, the Server is disabled and the Client points to the Element/LAN manager laptop. This done automatically for you when you use the Apply Profile Wizard.

Getting Started

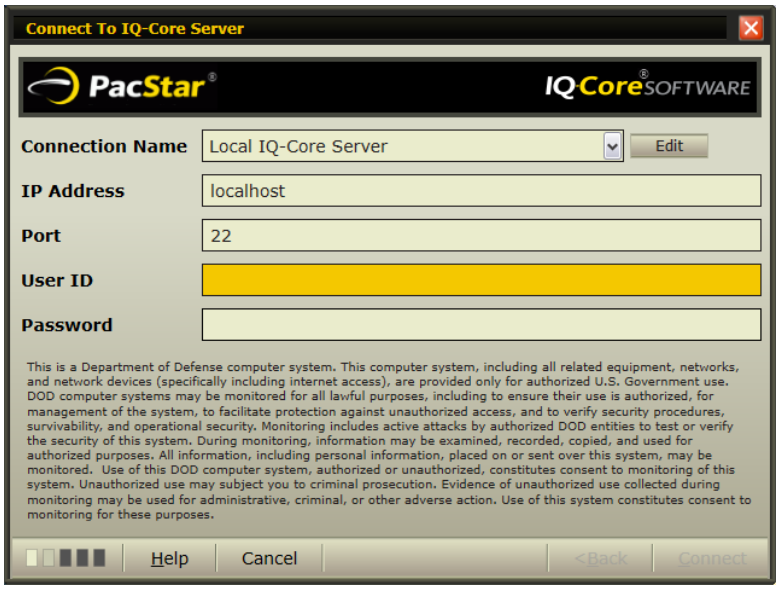
Follow the sections below to log into IQ-Core and get it configured to manage your node. If you have already done this, you can go to the generic Getting Started With PacStar IQ-Core Software to find out more information about IQ-Core Software and it's features.

Logging Into IQ-Core Software

The IQ-Core Client will auto-start when you log into the laptop but you can also start it manually if necessary. Follow these steps to log into IQ-Core Software:

1. Run the IQ-Core Client by double-clicking the desktop icon or by going to Start -> Programs -> PacStar IQ-Core Software -> IQ-Core Client
2. Wait for the 'Connection Wizard' to display. Verify that:
    - The Connection Name is 'Local IQ-Core Server'
    - The IP Address is 'localhost' for Element/LAN managers

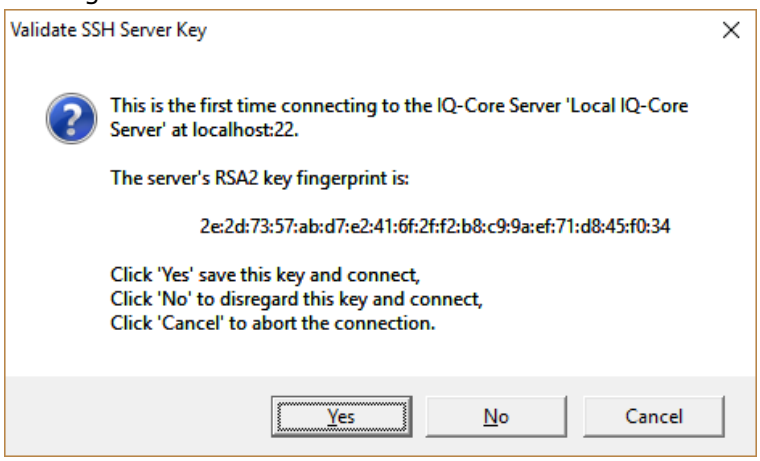
> ⚠ If you are on a Node Manager, this should be the IP address of the Element/LAN manager laptop, NOT localhost. The IQ-Core Server only runs on the Element and LAN Manager laptops.



3. You can log into the Server with a Windows user account. Enter the User ID and Password in the wizard. Use one of the following:
    1. The user account you installed with.
    So if you installed IQ-Core Software as 'jsmith', then you can log into IQ-Core with that same user and password.

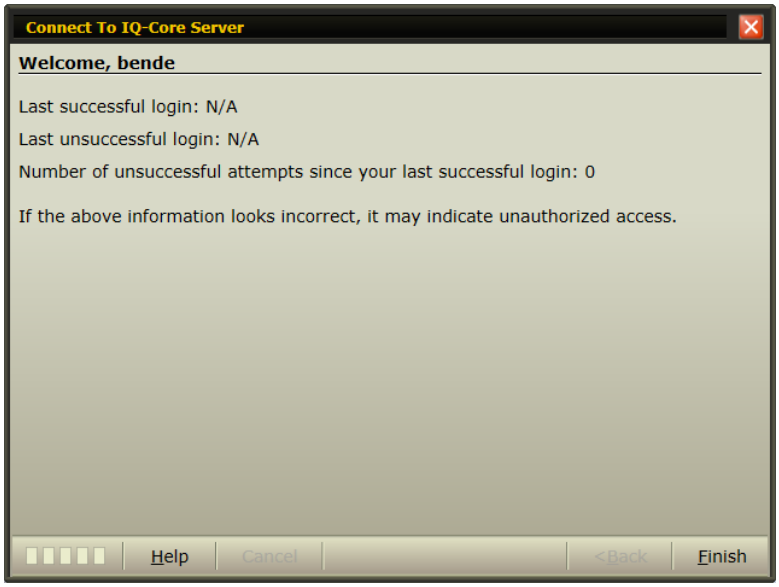
2. A special user account called 'iqcoreadmin'.
   This local Windows account was automatically set up by the installer and will have a password that you entered in the installer. You can also change this password using normal Windows methods in case you do not have the password used during install.
3. Any other user account that has been set up for your use.
   IQ-Core has a full role-based access system and it is possible to create other Windows user accounts and give them limited access to the IQ-Core feature set.

4. Click 'Connect' to continue
5. The first time you log in, you will see a 'Validate SSH Server Key' popup.
   This is telling you that the SSH key that the server is providing is not yet known by the client system. Just click 'Yes' to save this key and you will not see this popup again. If you click 'No', you will still be able to connect to the Server, but the key will not be saved on the client system and you will see the popup on the next Login.



> In future logins, if you see this popup and do not expect it, ensure that the IP Address/Host you are connecting to is correct and that there is not another server pretending to be the IQ-Core Server.

6. If the login is successful, you will see the final wizard page. The information shown gives a summary of any recent login activity.



7. Wait a few seconds and the main IQ-Core Client window will appear

Profile or Snapshot Application

You may see a **First Time** window appear if you have not yet configured IQ-Core Software for your node. If you don't see this window, you can always apply a profile or snapshot by clicking the **System** icon on the left-hand side of IQ-Core and going to the **Profiles and Snapshots** link.

1. **Apply Profile**
   This will bring up the Apply Profile Wizard which will guide you through configuring IQ-Core to manage your WIN-T node. **You should always do this first** unless you have an IQ-Core snapshot that you want to use so that this node is managed this same as another.
2. **Import Snapshot**
   This button will bring up a wizard that allows you to take a configuration snapshot from a different IQ-Core system and make this system identical to that.
3. **Manage Devices**
   This button takes you to the main devices page where you can manually add devices to be managed. This is the same as clicking the 'Device' menu item on the left-hand side of the IQ-Core window. You can always add/remove devices, even after applying a Profile or Snapshot. Follow the instructions in the Getting Started With PacStar IQ-Core Software assistance.
4. **Help**
   The help system is available throughout IQ-Core by clicking any 'Help' button or hitting 'F1' in any page or wizard.

Initial Configuration

After you have applied a Profile or Snapshot, you may need to adjust IP addresses or passwords to match your actual node device configurations. If your node type also has a Cisco Call Manager (JNN, BCP, SSS, etc.) then you will need to take some additional steps to configure that.

1. IP Address/Password Changes
   Use the **Change Device** wizard by clicking on the **Devices** icon on the left-hand side of IQ-Core and double-clicking on the device that needs tweaked. Follow the pages in the wizard to modify the pieces of information.
2. Cisco UCM Configuration
   IQ-Core Software manages Cisco Unified Call Manager via a secure web services interface. To do this, IQ-Core needs to communicate with the UCM by it's name and also have the UCM certificate installed. Follow the instructions in Cisco Call Manager Configuration Help.
3. REDCOM Configuration
   If you are actively using the REDCOM PBX, there is some additional configuration on that device so that IQ-Core can receive call detail records. Follow the instructions in REDCOMConfiguration.

WIN-T NMS Integration

The WIN-T program deploys a special Network Management System (NMS) at various Network Operating Centers (NOC) around the world. The NMS software provides advanced monitoring and configuration for WIN-T nodes. Many node types, like WIN-T INC1 nodes, use PacStar IQ-Core Software as the interface to this NMS system. When this NMS capability becomes available for your nodes, IQ-Core Software can be configured to interface with it. Contact your support or to learn more.

Support

Army operators should direct questions and problems to their first-tier support. This could be service representatives assisting in the configuration of the node or the Software Engineering Center (SEC) at Aberdeen Proving Ground. You can always , however, with any issue or comments you have.

Getting Started With PacStar IQ-Core Software

IQ-Core Software is a communications management application to help monitor, control, and configure devices in voice and data networks. It contains a broad set of easy-to-use management tools designed to reduce setup time, minimize configuration errors, and troubleshoot problems.

This guide will help you learn about IQ-Core capabilities, install and configure the software, and try out some of it's features. If you are already installed and configured, see the **'Try It Out'** section below.

Product Overview

View Army WIN-T Edition Overview first to see the unique features and initialization notes for this IQ-Core edition. This will help guide you to the best way to configure IQ-Core Software for your environment.

Feature Overview

View an Overview Of IQ-Core Software to get familiar with the capabilities of IQ-Core Software.

Architecture Overview

IQ-Core Software uses an efficient client-server model to communicate with devices in a variety of ways. View Architecture Overview Of IQ-Core Software to get an idea of how IQ-Core Software works.

Before You Install

You can install IQ-Core Software on almost any Windows computer or virtual machine. View the IQ-Core Resource Requirements for a list of supported environments.

Installation

See the IQ-Core Installation Guide for assistance in getting the software installed and logging in for the first time.

Try It Out

Once installed, follow the steps below to start using IQ-Core Software. These steps are designed to give you a high-level understanding of some of the basic features but there are many more features available once you are comfortable with the basics.

> When using IQ-Core Software, you can get guidance for any page, wizard, or tab by pressing F1 at any time. There are also 'Help' buttons in wizards that give you the same context-sensitive help. If you leave the resulting help window open, it will syncronize with the view you are at in the software.

How To: Manage A Device
Follow the Adding A Device Overview instructions to learn how to get IQ-Core Software to start communicating with a device.

How To: Device Monitoring Overview
Some of the basic device functionality is in the main Devices page. See the Device Tab Overview to learn about some of these features.

How To: Set Up The Dashboard
The IQ-Core dashboard has a network diagram which can be set up to give you at-a-glance status of important system information. See Dashboard Overview for initial setup instructions.

How To: Backup And Restore Device Configurations
IQ-Core has numerous capabilities to help manage your device configurations. See Configuration Management Overview for more information.

Next Steps

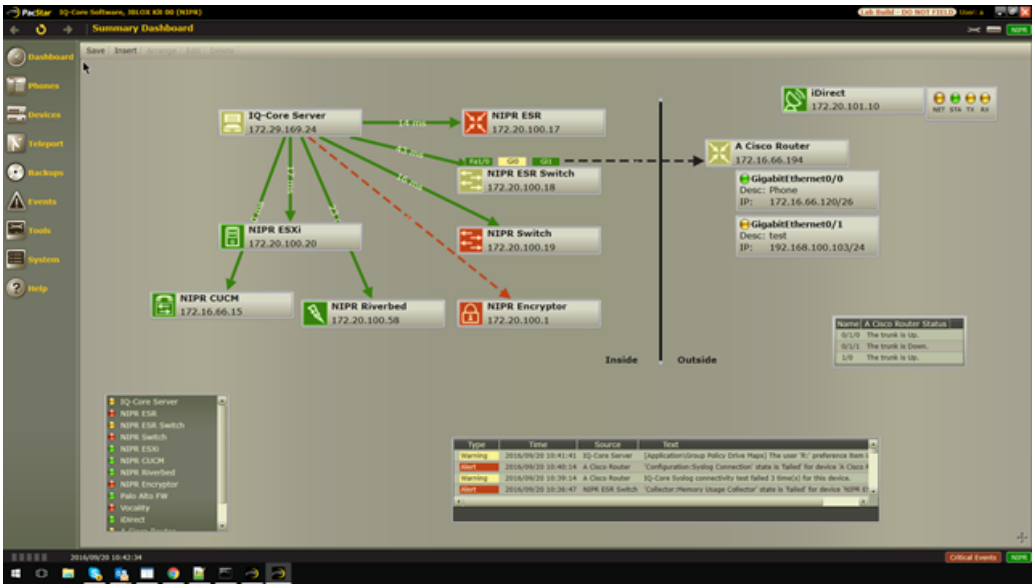
Explore IQ-Core Software with the Help Window open by clicking F1 or a help button anywhere. This help window will sync up with the current page or wizard that you have open and guide you on it's use.

Support

For any questions or issues, contact PacStar Technical Support.

Overview Of IQ-Core Software

IQ-Core Software is a communications management application to help monitor, control, and configure devices in voice and data networks. It contains a broad set of easy-to-use management tools designed to reduce setup time, minimize configuration errors, and troubleshoot problems.



The Software gives you both high-level workflow features as well as power-user features in a single interface. The capabilities fall largely into these categories:

- Monitoring
- Configuration Management
- Event Processing
- Voice Management
- File Services
- Certificate Management
- VPN Management
- User Provisioning
- System Tools

Nearly any network device can be managed through IQ-Core Software, including routers, switches, firewalls, modems, and phone systems. Additionally, the Software has system-level tools to assist in deployments of standard nodes or kits.

Here is a listing of some the features available in the above categories.

Monitoring

IQ-Core Software monitors devices, servers, and applications in numerous ways. Operational, environmental, and configuration status is made available in real-time. Thresholds can be set on most monitored values so that operators are alerted when data is not in an expected range.

1. **Critical Connectivity**
   IQ-Core monitors each device via ICMP, SNMP, SSH or other APIs such as REST to ensure that they are accessible on the network. This includes the ability to not only monitor networking devices, but also a myriad of applications as long as they provide an open interface.
2. **Interface Status**
   The Software monitors interface status for each device and can alert the operator when interface status changes. This includes the ability to monitor voice trunk interfaces.
3. **Network Diagram**
   IQ-Core has a graphical view of the status of the system. You can customize it by adding devices or widgets that represent various kinds of monitored status.
4. **Environmental Status**

The Software monitors temperature and fan metrics when the device has sensors to detect them. Alerts are generated when these environmental values exceed thresholds.

5. **Cisco IP SLA Creation/Monitoring**
   The Software includes integrated, wizard-driven support for Cisco IP SLA, enabling graphical analysis of connectivity and performance on supported devices.
6. **Time Monitoring**
   The Software monitors the current time and up-time of each device and can quickly alert the operator which devices are not time-synchronized. This novel capability is especially important in PKI environments.
7. **Version Compliance**
   The Software monitors device operating system/firmware versions and can alert the operator when they do not meet a specified baseline version, assisting NetOps in meeting configuration management and configuration monitoring requirements.
8. **Configuration Changes**
   The Software detects configuration changes on devices and automatically backs up running configurations. These configurations can be compared to a baseline and the operator can be alerted when they deviate.
9. **Any Value**
   The Software can be configured to monitor any other SNMP values data and compare to thresholds for alerting purposes.

Configuration Management

IQ-Core Software can retrieve and store device configurations. Any configuration can be pushed back onto a device. Configuration snippets with tokens are also supported.

1. **Backup**
   The Software can retrieve running device configurations manually, on a schedule, or when it detects that a configuration has changed. Multiple backups can be stored for use at any time.
2. **Restore**
   Any backed up configuration can be easily pushed back onto the device. IQ-Core will restart the device so it is using the new configuration.
3. **View/Search**
   Any configuration can be viewed and easily searched for values
4. **Compare**
   Two configurations from the same or different devices can be graphically compared for differences. This is especially useful for seeing how a configuration has changed from the baseline.
5. **Configuration Snippets**
   Any configuration file or snippet can be added to IQ-Core. These configuration files can have tokens within them so that the operator is prompted to provide values that will replace these tokens. This capability is very useful for initial device configuration or larger rollouts where configuration baselines need some deployment-specific data before applying to the device.
6. **Serial Support**
   Configuration snippets can be applied to the device via the serial port, which is useful when the device has not yet been configured.

Event Processing

IQ-Core Software stores events from devices and generates a number of events based on normal monitoring. Events have a severity level, typically generated by the device, so that it is easy to see warnings or errors.

1. **Syslog**
   IQ-Core is a syslog server and will receive and store syslog messages from devices. The Software can also automatically configure a device to send syslogs to itself.
2. **SNMP Traps**
   If configured, IQ-Core will receive SNMP traps from devices.
3. **Internally Generated Events**
   IQ-Core generates events having to do with both management and monitoring of devices. For example, you can be alerted if bandwidth on an interface is too high.
4. **Event Management**
   All events are stored and can be viewed, filtered, and forwarded to other syslog servers. Email alerts can be sent based on the occurence of critical events.

Voice Management

IQ-Core Software can manage multiple phone systems and has unique features for Cisco Unified Call Manager.

1. **Phone Provisioning**
   IQ-Core has views and wizards to help you manage phones, directory numbers, and important phone attributes. IQ-Core can also automatically configure a switch port that will have an IP phone plugged into it.
2. **Call Volume and Quality Reporting**
   IQ-Core can be configured to receive the necessary data to generate multiple types of call reports. These include call volume, call errors, and call quality including jitter and MOS.

File Services

IQ-Core Software is a fully functional SFTP, SCP, and TFTP server.

1. **File Management**
   IQ-Core has a file management view that allows you to manage the files on the server, including the ability to easily upload and download files, even from remote locations.
2. **Tool Support**
   You can use third-party tools like WinSCP against the IQ-Core file server. You can also drop files directly into the file server manually or via script.

Certificate Management

IQ-Core Software has unique capabilities to manage certificates in a PKI environment with one or more Certificate Authorities (CA).

1. **List, View, Export, Revoke Certificates**
   IQ-Core has a consolidated view of certificates with wizards that make it easy to view, export, or revoke individual certificates.
2. **Certificate Issuance**
   IQ-Core can tell a CA to sign a certificate based on a signing request.
3. **User Certificate Provisioning**
   For some environments it is useful to have the ability to generate certificates on behalf of an end-user device. IQ-Core can generate these certifiates and save them to a file for secure transport to the device.
4. **Expiration Monitoring**
   IQ-Core monitors certificate expiration dates and warns you when they are about to expire.
5. **Time Sync Monitoring**
   PKI environments require network devices to be syncronized in time. IQ-Core monitors the current time for all devices and alerts the operator if a CA is too far out-of-sync.

VPN Management

IQ-Core integrates it's certificate management capabilities into the creation and monitoring of secure VPNs. This is extremely useful in Commercial Solutions for Classified (CSfC) environments.

1. **Create VPN Configurations**
   IQ-Core has a step-by-step wizard to help you generate VPN configuration for a device from scratch. This can save you a lot of time and reduce errors as VPN configuration can be complicated. The Software also has wizards to create smaller pieces of configuration when you want to modify an existing VPN configuration.
2. **Certificate Support**
   IQ-Core will automatically generate certificate signing requests (CSR) on devices, get a certificate signed, and import it back onto the device. This is typically a laborious, error-prone process.
3. **User Provisioning**
   Some devices require configuration on a per-VPN-user basis. IQ-Core supports the creation of user certificates and will configure the device to be able to accept those certificates.
4. **VPN Monitoring**
   As VPN connections are made to a device managed by IQ-Core, they are detected and displayed with pertinent attributes.

User Provisioning

IQ-Core Software simplifies the management of users in Active Directory domains

1. **List, View Users**

IQ-Core makes it easy to see and filter the users in a domain.

2. **Add, Change, Remove Users**
   Wizards make it easy to add a user, assign them to Organization Units or Groups, and set up a user mailbox.

System Tools

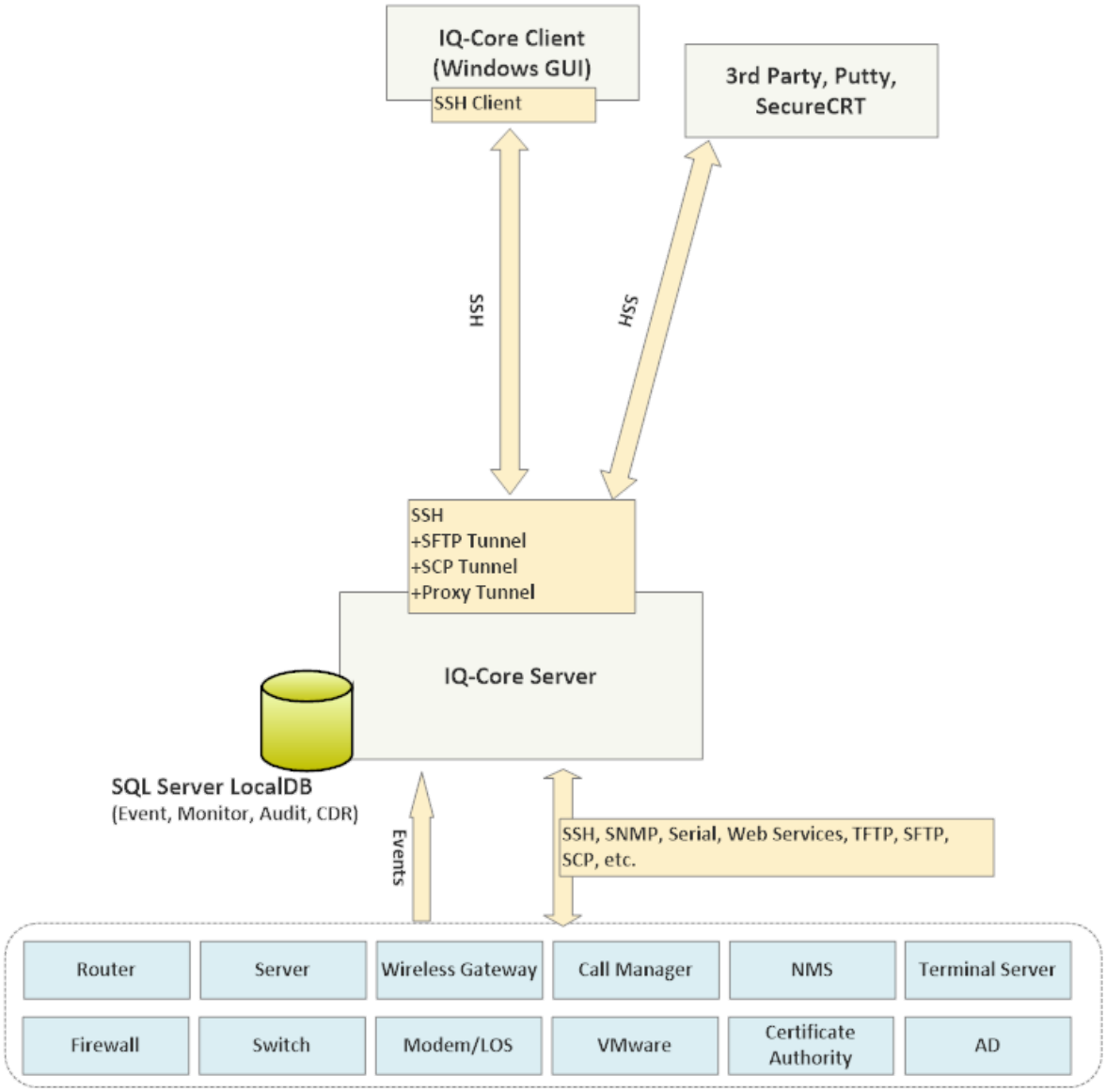
There are a number of other tools in IQ-Core to help operators. A couple of these are:

1. **RBAC Support**
   Nearly every page and wizard in IQ-Core is controlled by a role-based access system (RBAC). Users can be given restricted access to the IQ-Core feature set.
2. **System Reports**
   You can view and export basic reports on current system status, including operational status of each device.
3. **Named Credentials**
   You can store usernames and passwords in IQ-Core like a password vault. You can then easily use them by a descriptive name without having to constantly type them in.

Architecture Overview Of IQ-Core Software

IQ-Core Software consists of a Microsoft Windows Service called the IQ-Core Server, and a Microsoft Windows client application called the IQ-Core Client. You can have multiple Clients using a Server at the same time and the Clients can be local or remote.

The Client is just a user interface for the server, it does not communicate with devices directly. Here is a high-level drawing:



IQ-Core Server

The IQ-Core Server is named **PacStar.IQCore.Service.exe** and will be present in the '/Server' subfolder where the PacStar software has been installed. The Server is responsible for all the 'heavy-lifting' and communicates with the devices directly.

Device Communication

The Server is in constant communication with the devices it is managing to do things like retrieve status, monitor data flow, configure interfaces, restore configuration, and retrieve events. The IQ-Core Server uses a variety of protocols to communicate with devices. These include:

- SSH (with SFTP and SCP tunnels)
- SNMP
- Serial
- Web Services
- Device-specific libraries

Example: Cisco Router

- Use SSH to get status information, provide a terminal and run scripts
- Use SNMP for Bandwidth or Resource data
- Use SCP (over SSH) to retrieve configuration files
- Use Serial for initial configuration needs

You don't normally need to worry about which protocol the Server is using for a particular feature as long as that protocol communication channel is working correctly.

Event Server
In addition to communicating directly with devices, IQ-Core Server is also an 'Event Server'. It can receive syslog and SNMP traps from devices. By default, the Server will automatically ensure that most devices send their syslogs to the Server but will not enable SNMP traps. This is because many traps overlap their syslog counterparts. However, you can control this behavior when configuring a device within IQ-Core.

Events are stored as they come in. This allows you to be able to view and manage these events at any time. The event data is stored in an embedded SQL Server LocalDB database. This database is only for use by the IQ-Core Server and has no facility to receive data from any other application.

File Server
The IQ-Core Server is also a 'File Server' and can send and receive files over SCP, SFTP and TFTP. The Server uses these protocols in various ways:

- SCP and SFTP are used to get running configurations off devices and push them back on.
- TFTP is used for running configurations if necessary, but is especially useful for initial device configuration.
- You can use any SCP/SFTP/TFTP clients with IQ-Core to easily get files onto the Server for further use.

IQ-Core Client

The IQ-Core Client is named **PacStar.IQCore.Client.exe** and will be present in the '/Client' subfolder where the PacStar software has been installed. The Client is responsible for the User Interface (pages, wizards, tabs) and only communicates with the IQ-Core Server, not with any of the devices.

The Client communicates with the Server over a single SSH connection. When the Client wants to retrieve some information from the Server, it will call a function on the Server over that SSH connection, receive the data from the Server, and display it to you in various ways.

You can use the IQ-Core Client remotely, it does not have to be on the same machine as the Server. You can also use multiple Clients simultaneously.

Note that it may appear that the Client is communicating directly with devices when using the Terminal feature which provides access to device command-line interfaces (CLI). But these CLI connections are actually proxied through the IQ-Core Server, meaning that you do not need to worry about giving the Client special access to devices.

Ports And Protocols

For a summary of which ports and protocols IQ-Core Software uses, read the Ports And Protocols overview. This will help ensure that your system can run IQ-Core in a secure, efficient manner.

IQ-Core Resource Requirements

The operating system, memory, and processor requirements for using IQ-Core Software are listed below. The Software has a small footprint and low resource requirements, making it easy and cost-effective to host on even low-end computers. Also see Ports And Protocols for the specific network ports that need to be open.

IQ-Core Software consists of a Server (a single Microsoft Windows Service) and a Client (a Microsoft Windows application). Both can be installed on bare metal or in a virtualized environment. Additionally, the IQ-Core Crypto Manager add-on may use a Windows Agent, which is a trimmed-down version of the IQ-Core Server.

Supported Operating Systems

The Client, Server, and Agent will run on the following Microsoft operating systems:

- Windows 7
- Windows 8.1
- Windows 10
- Windows 2008
- Windows 2012
- Windows 2016

Note that a Windows VM running on a Linux server is also fully supported.

External Dependencies

IQ-Core Software applications are written using Microsoft .NET. The version of .NET required changes over time as new releases become available. The current version that IQ-Core uses is .NET 4.6.2.

The PacStar installers will automatically install the appropriate .NET version if it does not already exist on the system.

Processor Requirements

A dual-core CPU is recommended but small nodes can use a single-core CPU with no problem. There is no specific speed or cache requirement although hyper-threading is suggested when there are more than a few devices being managed. For larger nodes, a quad-core computer will provide increased performance.

Memory

The Server requires a minimum of 1GB to operate but 2GB is recommended. More memory will be required as the device count increases (more than 50 devices). The Client requires about 300MB free RAM. The Client and Agent need no more than 500MB free memory to operate.

Disk Space

The Server requires a minimum of 10GB of disk space. The Server stores data of various kinds and automatically archives and prunes older data as necessary. The Client requires 200MB of disk space. The Agent requires 1GB of disk space.

Graphics Card

There is no specific graphics card requirement for any of the IQ-Core applications although the Client benefits from more capable graphics processing.

Network Ports

IQ-Core Server needs a variety of network port access to communicate with devices via SSH, SNMP, and other protocols. The IQ-Core installer will automatically configure the appropriate local Windows firewall rules but you may need to adjust manually in some cases. See Ports And Protocols for more information.

Ports And Protocols

IQ-Core Server uses a variety of network-based communication, both to communicate with devices and to communicate with the IQ-Core Client.

Client/Server Connection

IQ-Core Client connects to the IQ-Core Server via an SSH connection. The Server normally listens on the default SSH port 22 for these connections, but this port number can be changed in a configuration file in IQ-Core Server. Contact PacStar Technical Support for information on how to change this.

The IQ-Core Client 'Connection Wizard' allows you to select the port so that you are matching what the IQ-Core Server is expecting.

Device Communication

IQ-Core Server uses SSH, SNMP, and web services to communicate with devices. Additionally, protocols like SCP, SFTP, and TFTP are used as necessary to manage device configurations. A full listing of the various ports and protocols in shown below.

If there are ACLs or firewall rules that are blocking these ports or protocols from the IQ-Core Server, then device communication may not work properly.

Port	Protocol	Direction
22	TCP (SSH)	In and Out
514	UDP (Syslog)	In
161	UDP (SNMP gets)	Out
162	UDP (SNMP traps)	Out
69	UDP (TFTP)	Out
60000-60010	UDP (TFTP Source)	Out
443	UDP (HTTPS)	Out

Windows Firewall

If you are running the Windows Firewall service on the machine that is running IQ-Core Server, you will need to ensure that all ports are open and available for IQ-Core Server to use. To do this, you can put in place rules for each port. Open the firewall management console and go to the create port rules for each of the ports listed above.

Administrators often shut off access to the Firewall settings. You may not be able to get to firewall management console and will need administrative assistance to do so.

Changing firewall settings can cause applications to appear to stop working or cause security holes in your system. The following is just an example of creating a firewall rule and you should understand the consequences of changing firewall rules.

Example Port Rule

As an example, to open up port 22 so that the IQ-Core Server can use SSH, do the following in the firewall management console:

1. Go to Windows Firewall With Advanced Security/Windows Firewall With Advanced Security - Local Group Policy Object
2. Right-click on Inbound or Outbound (use **Direction** column above) and click **New Rule...**
3. Select the **Port** radio button
4. Set the rule to use **TCP** and **Specific local ports** to 22
5. Set the rule to **Allow the connection**.
6. Leave all Apply checkboxes checked and click next.
7. Name the rule: (e.g. Allow IQ-Core SSH TCP 22)
8. Click Finish

IQ-Core Installation Guide

IQ-Core Software consists of a Windows **Server**, **Client**, and possibly an **Agent** (a trimmed-down version of the Server). There are various installers available for these applications. The filenames of the installers have a form that indicates their version. IQ-Core versioning is explained more fully in VersionOverview but the file forms are as follows:

Application	Filename Format
Server Installer	Setup_<ProductType>_<Version>.<Build>.<Revision>_<LabIdentifier>.exe
Client-Only Installer	Setup_<ProductType>_<Version>.<Build>.<Revision>_<LabIdentifier>.exe
Agent Installer	Setup_<ProductType>_<Version>.<Build>.<Revision>_<LabIdentifier>.exe

where <ProductType> is the name of the IQ-Core product (e.g. Standard, CSfC, etc.) and <Version>.<Build> is the full version of the IQ-Core Software to be installed (e.g. 3.9.17). The <Revision> field is for internal PacStar use.

The Server Installer actually installs both IQ-Core Server and IQ-Core Client. Only use the Client installer on remote systems that need access to the IQ-Core Server.

The Agent is currently only required for CSfC installations. However, it is also useful to install the Agent when managing remote Windows servers to gain some additional features.

Interactive vs. Unattended Install

You can run the installers in two different modes:

Interactive
This is the normal graphical mode where you will click through a wizard to install the software. If an issue is encountered you will be able to see information about it and suggestions on how to handle. See InteractiveInstall for instructions.

Unattended
This mode is used to install the software via script where there is no user available to view information or click buttons. See the UnattendedInstall document for information on how to use this mode.

Dependencies

IQ-Core Software is largely written in C# using Microsoft .NET libraries and contains most of the other libraries or modules that it needs to function. The two primary external dependencies are:

1. Microsoft .NET
   IQ-Core is built to use a specific minimum version of .NET. At the time of this writing, this version is .NET 4.6.2. This means that IQ-Core Software needs 4.6.2 at a minimum but can operate fine with 4.7 or 4.8 as well because the .NET libraries are backward compatible. Note that the IQ-Core Installer will notice if it does not have an appropriate .NET version and will install it automatically (interactive install) or gracefully error out (unattended install). Also, the IQ-Core installer itself requires .NET 3.5 and this cannot be installed automatically. If your system does not have that minimum version, it will need to be installed prior to running the installation
2. Microsoft SQL Server LocalDB
   This is an embedded form of SQL Server for use by applications. This is NOT a normal SQL Server install as the database access only exists when IQ-Core is running and can only be accessed by the IQ-Core service itself. Thus the security profile of this database server is much better than other typical database servers. You will never need to worry about this dependency as the IQ-Core installer will create the databases automatically, there are no additional components that can be added.

What Gets Installed

Here is a high-level overview of what will be placed on the computer during installation. Also see Ports And Protocols for information about the required network access needed.

Server Installer
The Setup_...exe installer will put both the IQ-Core Server and IQ-Core Client applications on the computer.

- The binary files are placed in C:\IQ-Core

- The data files (to store events, monitored data, etc.) are stored in a location of your choosing, usually C:\PacStar or D:\PacStar
- The embedded SQL Server database (Microsoft SQL Server LocalDB) is installed in the default Program Files folder
- The Server (PacStar.IQCore.Service.exe) gets installed as a Windows Service. You can start and stop this service from the Windows Service Manager
- The Client (PacStar.IQCore.Client.exe) will have desktop and start menu icons created for it
- The installer will create a new Windows Registry key at Computer/HKEY_LOCAL_MACHINE/Software/PacStar
- One local Windows user is created, **IQCoreSvc**. IQCoreSvc is the user that runs the Windows Service.
- Various registry entry permissions are altered so that the Server can read performance counters
- The installer will optionally modify the local Windows firewall with rules that allow the Server to use SSH, SNMP, and ICMP for network access

> Also see Ports And Protocols for the specific network ports needed. Note that your computer may be set up so that there is administrative (domain) control over the firewall rules. In this case, the local rules will be put in place, but may be overridden by the domain-specific rules. IQ-Core does not attempt to modify these domain rules.

Client Installer
The Client_...exe installer puts only the Client application on the computer. You use this only for remote systems that require access to the Server.

- The binary files are placed in the default Program Files folder
- The Client (PacStar.IQCore.Client.exe) will have desktop and start menu icons created for it
- The installer will create a new Windows Registry key at Computer/HKEY_LOCAL_MACHINE/Software/PacStar

Agent Installer
The Agent_...exe installer puts a slimmed-down version of IQ-Core Server on the computer. The installed artificats are similar to the Server Installer but the Agent does not need a database and does not come with a Client.

- The binary files are placed in C:\IQ-Core
- The Server (PacStar.IQCore.Service.exe) gets installed as a Windows Service. You can start and stop this service from the Windows Service Manager
- The installer will create a new Windows Registry key at Computer/HKEY_LOCAL_MACHINE/Software/PacStar
- Two local Windows users are created, IQCoreSvc and IQCoreAdmin.
  IQCoreSvc is the user that runs the Windows Service. IQCoreAdmin is a convenience user that you can use to log into IQ-Core with. It can be removed once other users are allowed to log into IQ-Core.
- Various registry entry permissions are altered so that the Server can read performance counters
- The installer will optionally modify the local Windows firewall with rules that allow the Server to use SSH, SNMP, and ICMP for network access

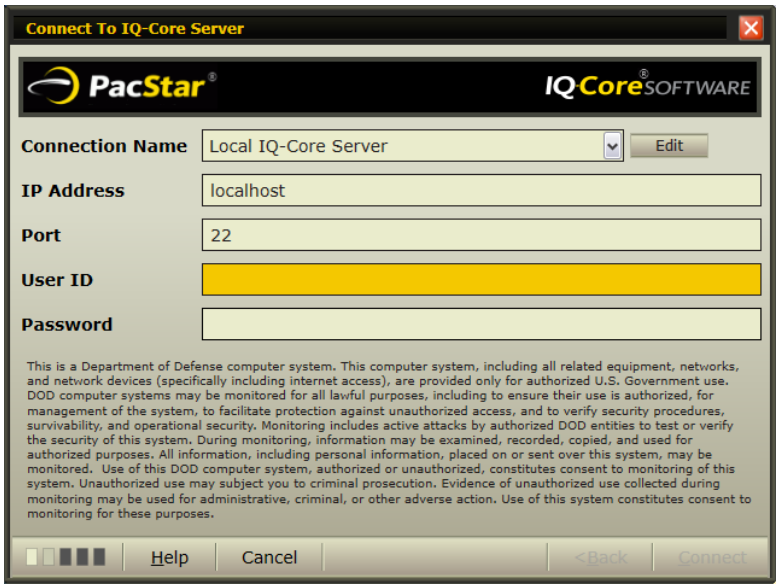
> Also see Ports And Protocols for the specific network ports needed. Note that your computer may be set up so that there is administrative (domain) control over the firewall rules. In this case, the local rules will be put in place, but may be overridden by the domain-specific rules. IQ-Core does not attempt to modify these domain rules.

Installation Instructions
For typical installation, see InteractiveInstall. If you need to script the installation in an unattended manner, see UnattendedInstall.

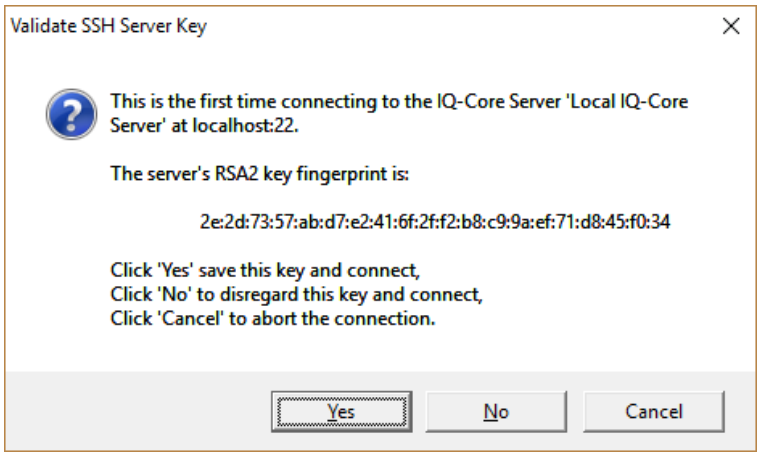
Logging Into IQ-Core and Validating Install
After installation of the Server, you can log into IQ-Core to start managing your communication system. To do so, follow these steps:

1. Run the IQ-Core Client by double-clicking the desktop icon or by going to Start -> Programs -> PacStar IQ-Core Software -> IQ-Core Client

2. Wait for the 'Connection Wizard' to display. Verify that:
   - The Connection Name is 'Local IQ-Core Server'
   - The IP Address is 'localhost'

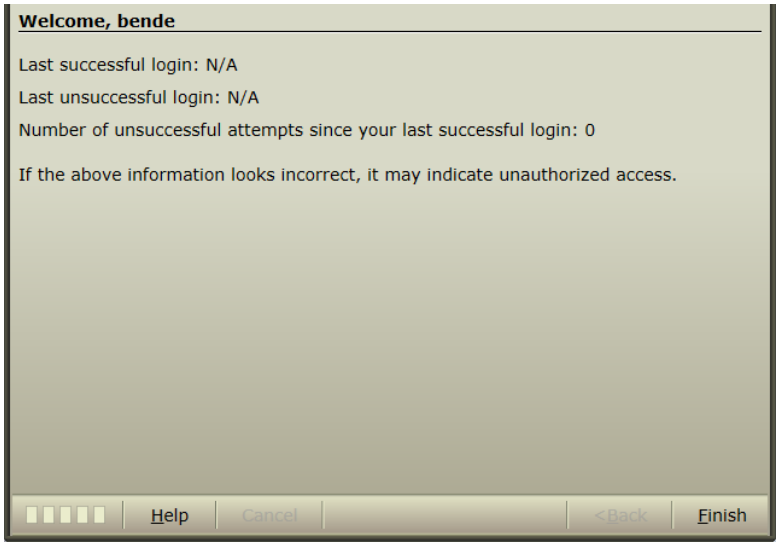


3. You can log into the Server with a Windows user account. Enter the User ID and Password in the wizard. Use one of the following:
   1. The user account you installed with.
      So if you installed IQ-Core Software as 'jsmith', then you can log into IQ-Core with that same user and password.
   2. Any other user account that has been set up for your use.
      IQ-Core has a full role-based access system and it is possible to create other Windows user accounts and give them limited access to the IQ-Core feature set. But this only works after upgrades since you must have previously been in IQ-Core Software to set up the user in a role.
4. Click 'Connect' to continue
5. The first time you log in, you will see a 'Validate SSH Server Key' popup.
   This is telling you that the SSH key that the server is providing is not yet known by the client system. Just click 'Yes' to save this key and you will not see this popup again. If you click 'No', you will still be able to connect to the Server, but the key will not be saved on the client system and you will see the popup on the next Login.



> In future logins, if you see this popup and do not expect it, ensure that the IP Address/Host you are connecting to is correct and that there is not another server pretending to be the IQ-Core Server.

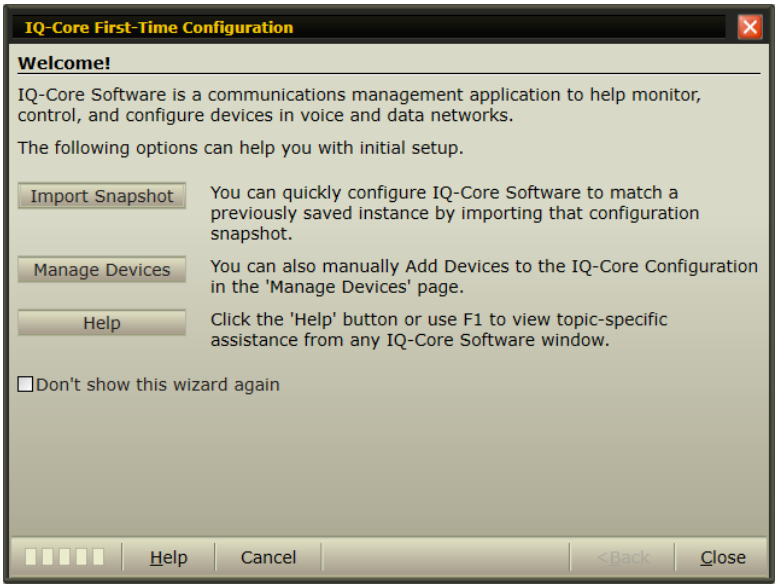
6. If the login is successful, you will see the final wizard page. The information shown gives a summary of any recent login activity.



7. Wait a few seconds and the main IQ-Core Client window will appear

Initial Configuration

After logging in, you will see a 'First Time Configuration' window like that shown below.



You can just close this window to get to the main IQ-Core Client workspace. But you can also use these buttons to help start configuring IQ-Core to manage your system. The options are:

1. **Apply Profile**
   The Profile Wizard helps you quickly set up a system for a specific node type by putting in appropriate devices, credentials, default values, and other settings. If you do not see this button, there is no Profile for your product type and you will need to manually add devices.
2. **Import Snapshot**
   This button will bring up a wizard that allows you to take a configuration snapshot from a different IQ-Core system and make this system identical to that.
3. **Manage Devices**
   This button takes you to the main devices page where you can manually add devices to be managed. This is the same as clicking the 'Device' menu item on the left-hand side of the IQ-Core window. Use this if you are evaluating IQ-Core for the first time and follow the instructions in the Getting Started With PacStar IQ-Core Software.
4. **Help**
   The help system is available throughout IQ-Core by clicking any 'Help' button or hitting 'F1' in any page or wizard.

Initial Configuration For Agent

If you are using the Agent on a Microsoft Certificate Authority, remember to follow the configuration steps in IQ-Core Agent Configuration after installing the Agent using the steps above.

Configuring and Using IQ-Core Software

Now that installation is complete, you can start configuring IQ-Core to manage your communication system. See the Getting Started With PacStar IQ-Core Software to learn how.

When using IQ-Core Software, you can get guidance for any page, wizard, or tab by pressing F1 at any time. There are also 'Help' buttons in wizards that give you the same context-sensitive help. If you leave the resulting help window open, it will synchronize with the view you are at in the software.

IQ-Core Agent Configuration

When IQ-Core Software is managing a Microsoft Certificate Authority (CA), an IQ-Core Agent must be installed to provide the IQ-Core Server with the appropriate CA access. See the IQ-Core Installation Guide for information on how to install the Agent. Once installed, follow the steps below to configure the CA to work with the Agent service.

> These configuration steps do not need to be done on the ISC CertAgent as there is no Agent in that case.

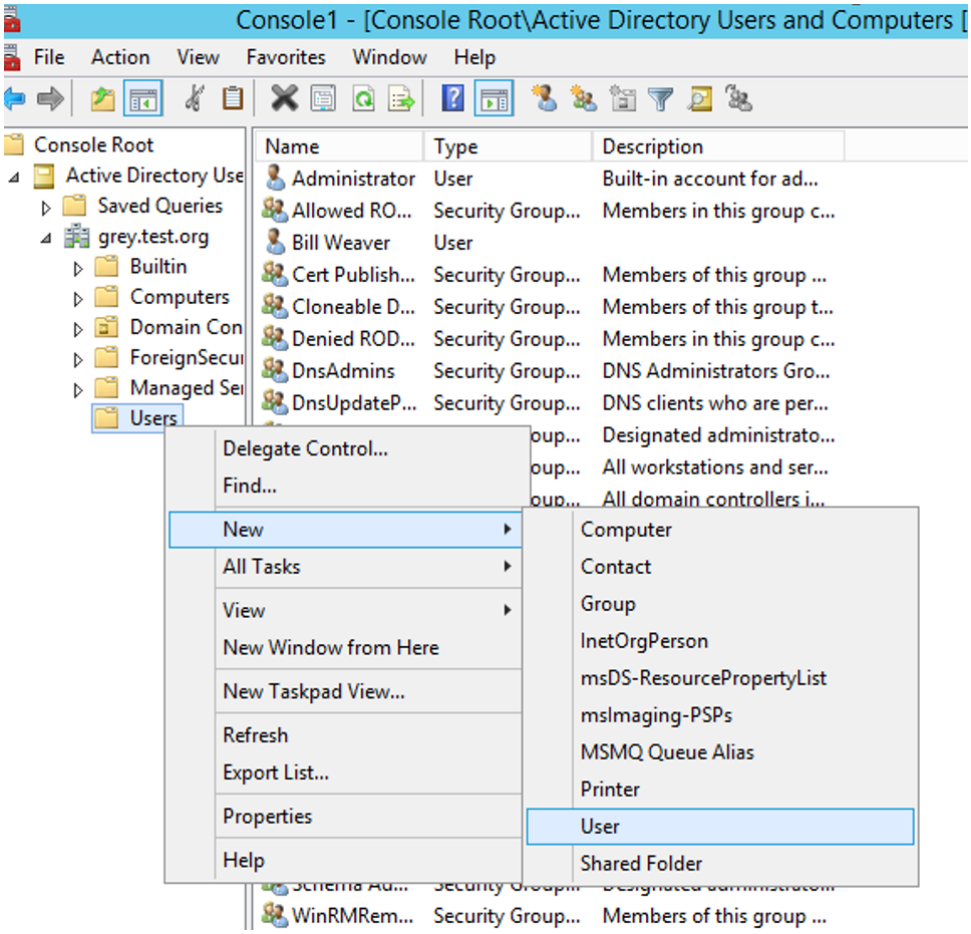
> These configuration steps do not need to be done after an *upgrade* to the IQ-Core Agent service, just after a clean install.

Configure Domain User

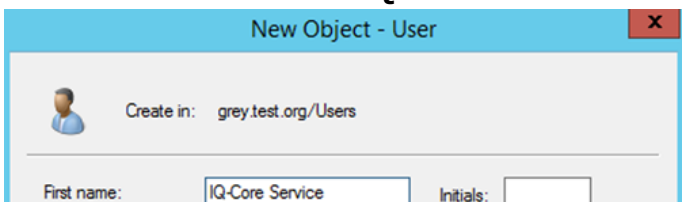
If you are installing the Agent on a CA that is a domain controller or member of a domain (which is likely), then you need to ensure that the Agent service user, called **IQCoreSvc**, is created as a ***domain*** user and that the Agent runs as that user. The Agent installer will install a ***local*** user called IQCoreSvc but cannot create the domain user.

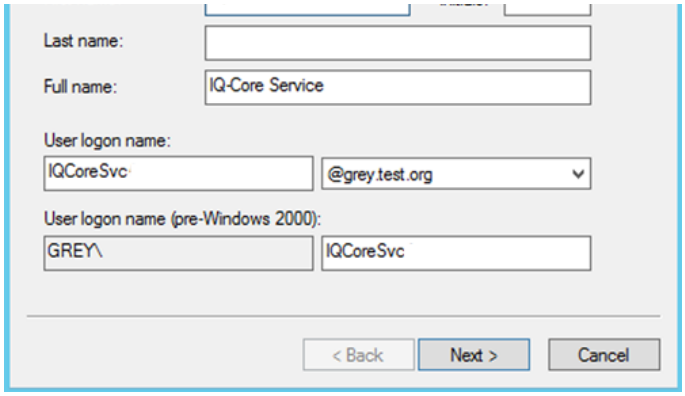
If this is your situation, then on the domain controller or CA:

1. Open the Active Directory Users And Computers applet
   Find the Users organizational unit and right-click to add a user

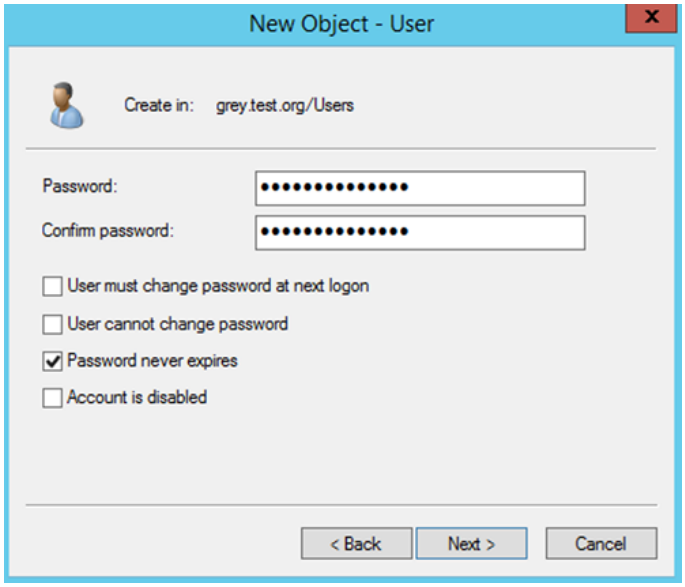


2. Create a domain user called **IQCoreSvc**

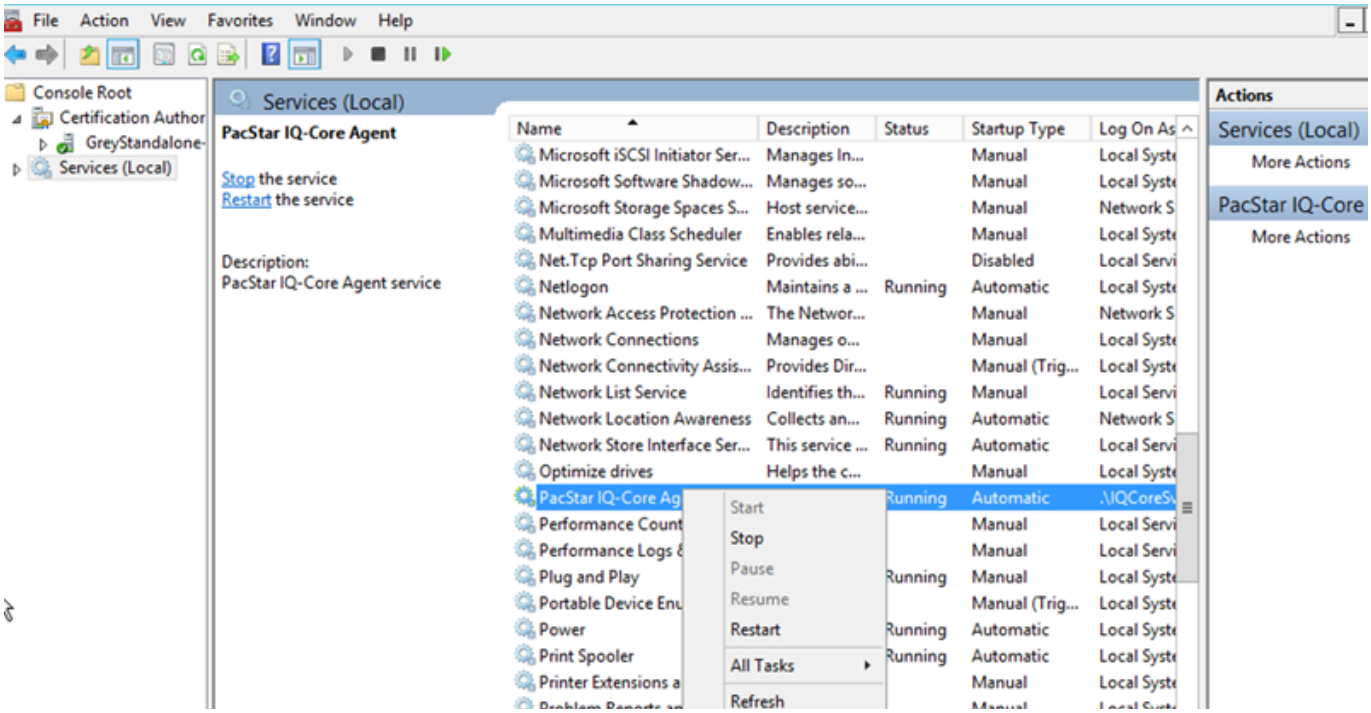


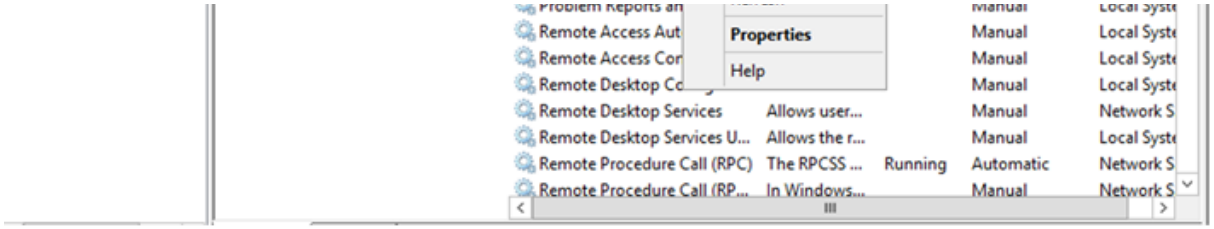


3. Click Next and give user a password
   Make sure to set 'Password never expires'

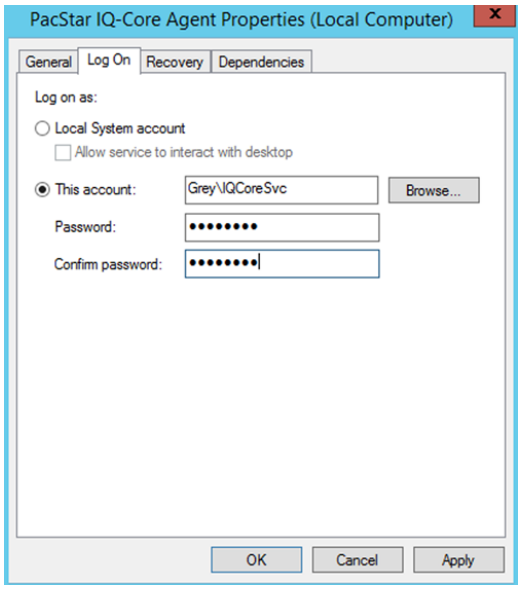


4. Click Next and OK to create user
5. On the CA with the IQ-Core Agent installed, open **C:\IQ-Core\tools\Certificate Management.msc**
   And click on Services (you can use File/Add Remove Snap In to get Services if you don't see it).
6. Find the 'PacStar IQ-Core Agent' service and right-click to get to Properties





7. Go to Logon tab and change account to newly created domain user
   You can use the 'Browse...' button to find IQCoreSvc user but just ensure you are picking the domain user and not a local user. For a password, enter the same password you used when creating the user above.

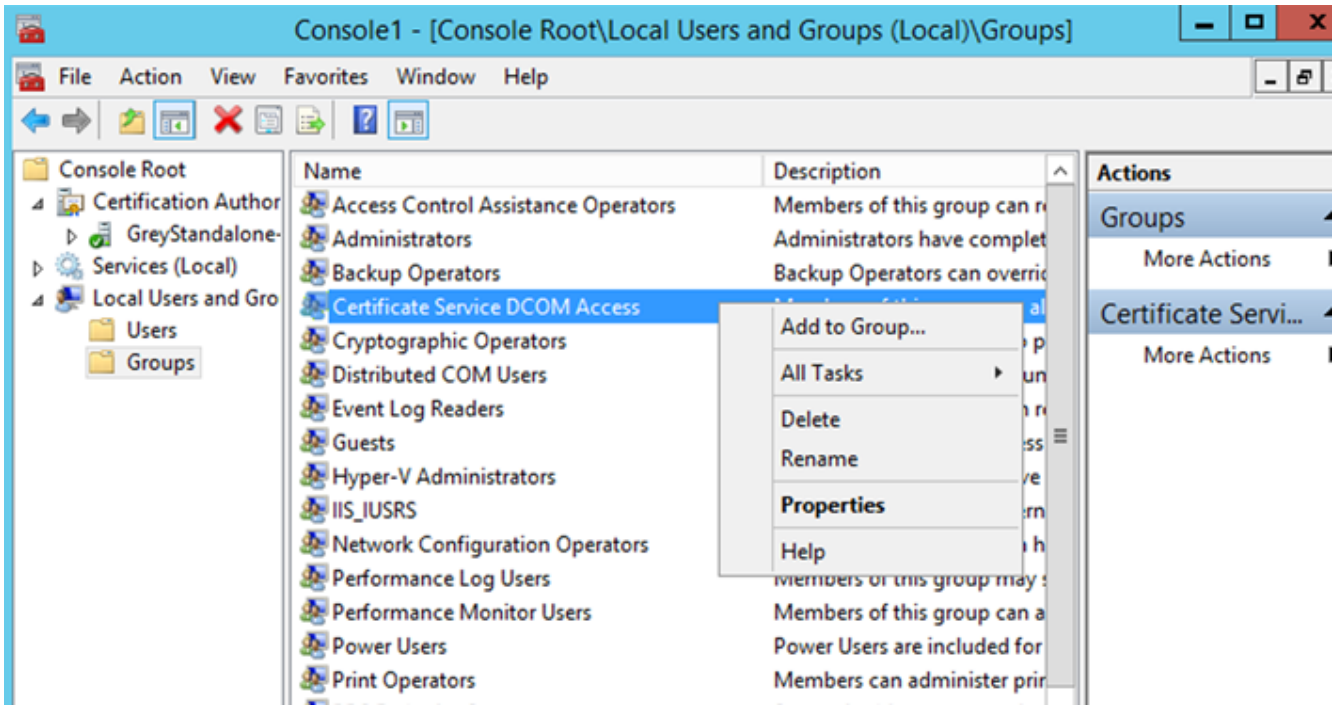


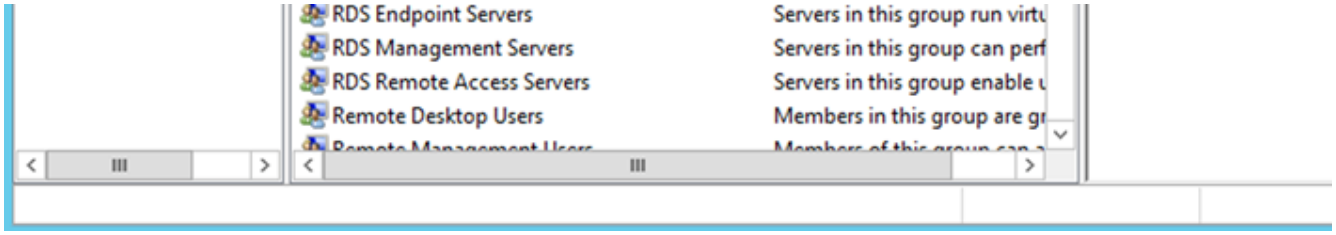
8. Click OK to finish.

Configure DCOM

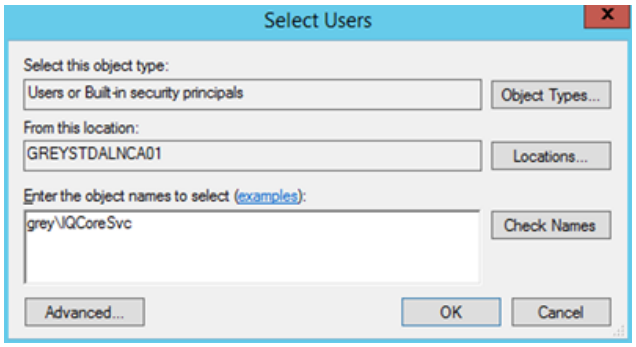
You will need to add the Agent service user (IQCoreSvc) to two local distributed COM groups. To do so:

1. On the CA with the IQ-Core Agent installed, open **C:\IQ-Core\tools\Certificate Management.msc** And go to the 'Local Users And Groups' add-in on the left. Select Groups and select 'Certificate Service DCOM Access'.

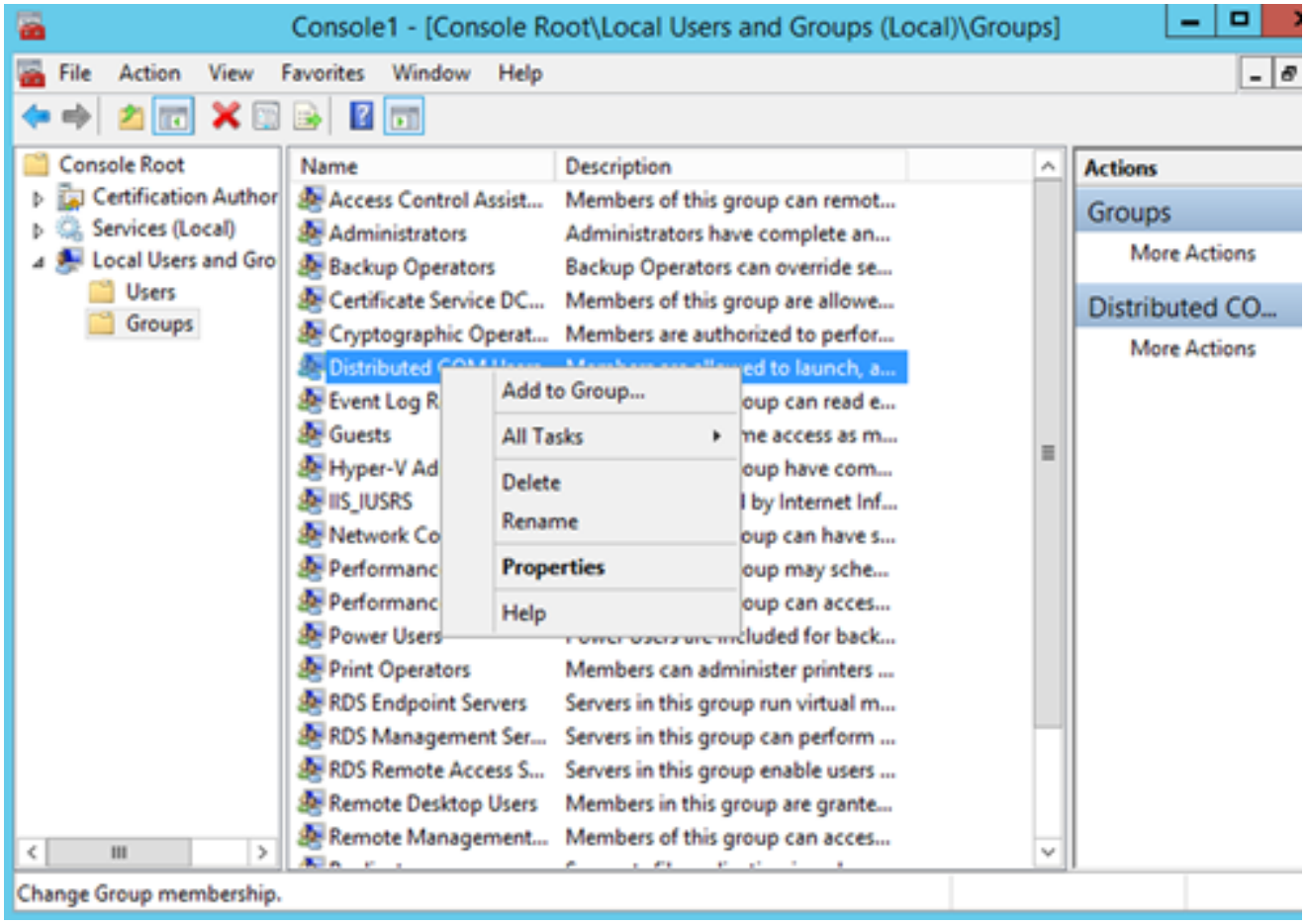




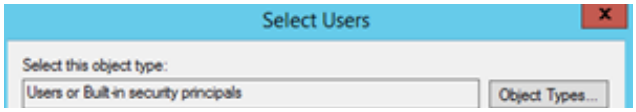
2. Right-click and click 'Add To Group...'
3. Add **IQCoreSvc** to the user member list and click 'OK'.
   If you're CA is in a domain, make sure to add the domain IQCoreSvc user, not the local IQCoreSvc user.

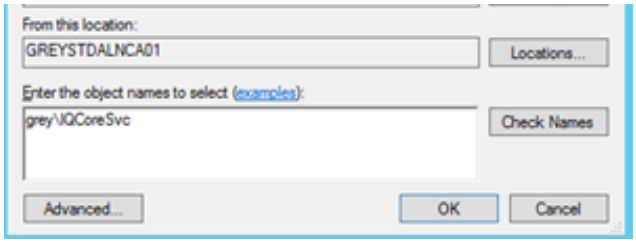


4. Now select 'Distributed COM Users' from the same Groups list



5. Right-click and click 'Add To Group...'
6. Add **IQCoreSvc** to tthe user member list and click 'OK'.
   If you're CA is in a domain, make sure to add the domain IQCoreSvc user, not the local IQCoreSvc user.

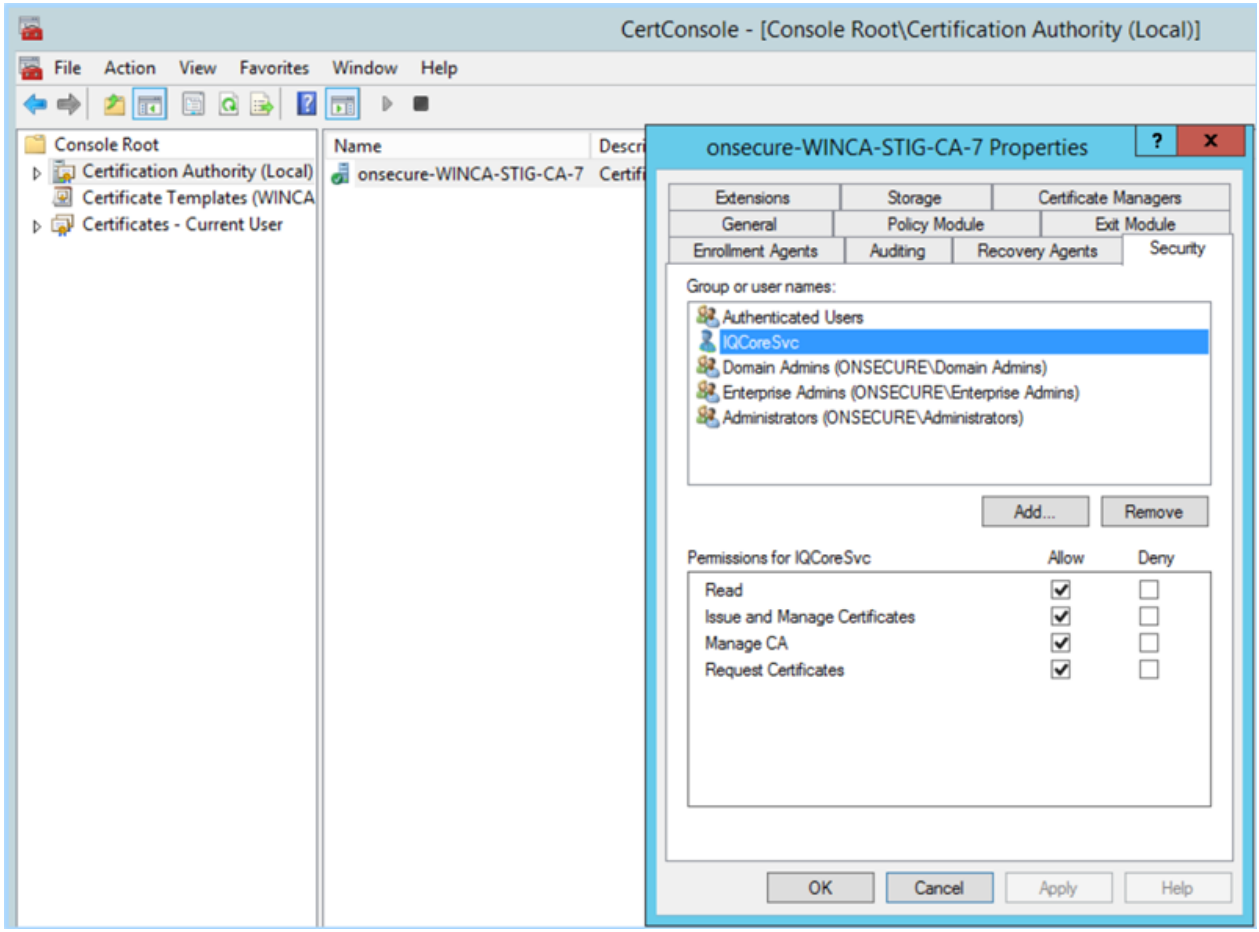




CA Permissions

After installing the Agent, follow these instructions to give the IQ-Core Agent permission to use the CA

1. Open the preset certificate console at **C:\IQ-Core\Tools\Certificate Management.msc**
   You can also open up mmc.exe and manually add the appropriate CA add ons.
2. Expand the 'Certification Authority' and right-click on the actual server CA name
3. Click Properties and go to the Security tab
4. Add **IQCoreSvc** as an authorized user and Allow all permissions (Read, Issue, Manage, Request)
   If you're CA is in a domain, make sure to add the domain IQCoreSvc user, not the local IQCoreSvc user.



> ⚠ If the CA is a domain controller or part of a domain, make sure you use the ***domain*** IQCoreSvc user and not the ***local*** IQCoreSvc user.

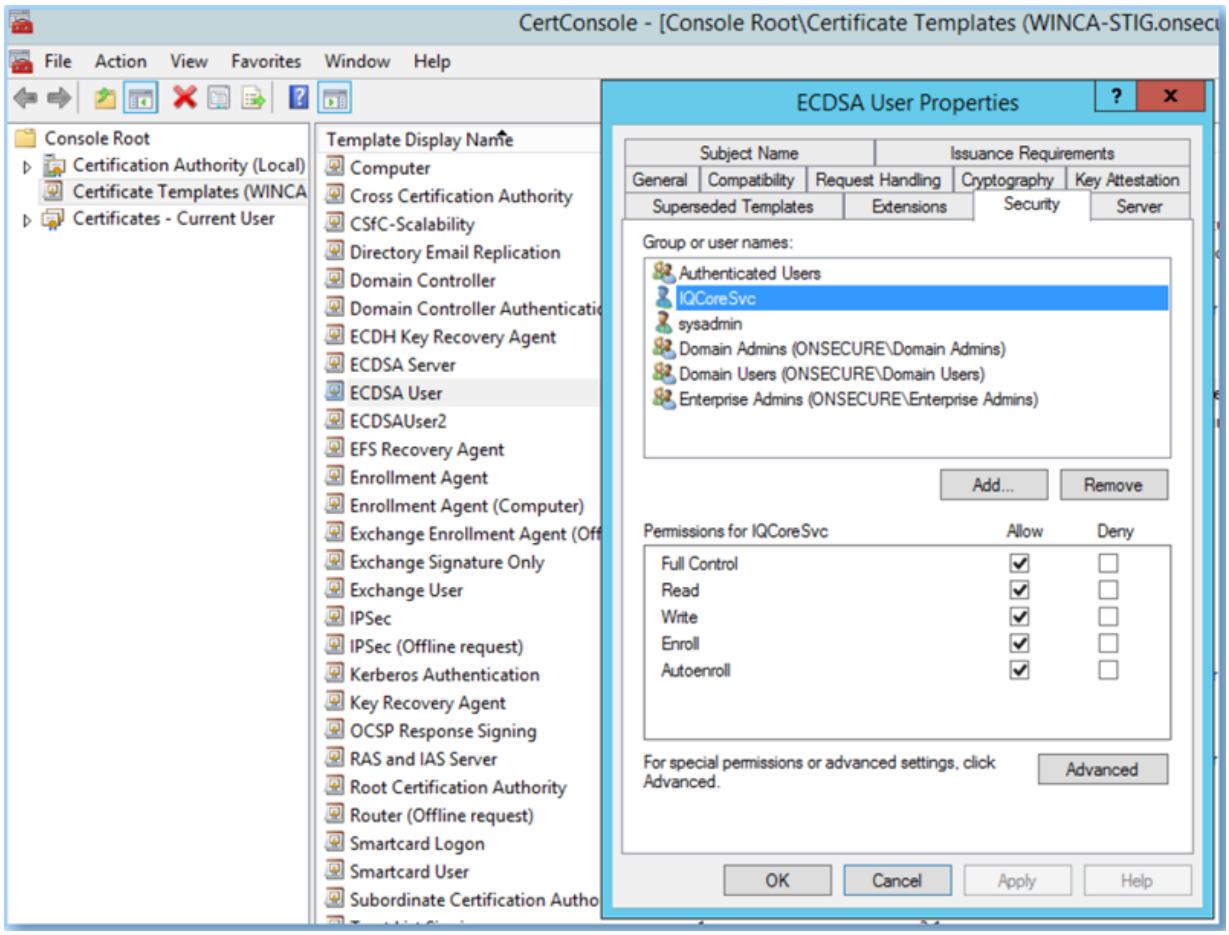
5. Click OK to accept and close all windows

CA Template Permissions

The IQ-Core Agent also needs permissions to access the Microsoft Certificate Templates that you will be using. To do so:

1. Open the preset certificate console at C:\IQ-Core\Tools\Certificate Management.msc
   You can also open up mmc.exe and manually add the appropriate CA add ons.

2. Click on Certificate Templates
3. For each Template you will use, right-click and select Properties
4. Add **IQCoreSvc** as an authorized user and Allow all permissions (Full Control, Read, Write, Enroll, Autoenroll)
   If you're CA is in a domain, make sure to add the domain IQCoreSvc user, not the local IQCoreSvc user.



> ⚠ If the CA is a domain controller or part of a domain, make sure you use the ***domain*** IQCoreSvc user and not the ***local*** IQCoreSvc user.

5. Click OK to accept and close all windows

Cisco Call Manager Configuration Help

IQ-Core Software has features with Cisco UCM that require some configuration in the Cisco UCM Web GUI. You will also need to configure IQ-Core Software to use the appropriate Cisco UCM name.

Certificate Installation

IQ-Core uses a secure web services interface to communicate with Cisco UCM. In order for this to work properly, the UCM certificate must be installed on the computer running IQ-Core Server. To do so:

1. Get and install certificate
   Follow the instructions in Certificate Configuration Help to get the certificate from Cisco UCM and install it.
2. Note certificate/host name
   IQ-Core needs to communicate with Cisco UCM with the **same name as the certificate name**. This will ensure the secure connection can be made. To do so, you'll need to note the name of the certificate in the step above and then use that in these subsequent steps.
3. Modify DNS/hosts file
   If the Cisco UCM host name is already in DNS, you do not need to do anything. If you are not running DNS you must modify the local **hosts file** to map the UCM host name (**certificate name**) to the IP address of UCM. To modify the hosts file:
   1. Run Notepad as administrator
      And open the following file: C:\Windows\System32\drivers\etc\hosts. You will need to view all files in the Open File dialog, not just TXT files.
   2. Add the IP to Host Mapping
      Follow the example in the file. Example:

      192.168.1.30 MyCUCMCertificateName
   3. Save the file.
      Note that it will take IQ-Core a minute or so to notice the change.
4. Manage UCM using the host/certificate name
   Finally you will use the **Change Device Wizard** for UCM to go and change the Management IP address. Change it to the certificate/host name noted above and identical to what is in DNS/hosts file.
5. Wait for IQ-Core to notice changes
   After a minute or so, IQ-Core will start using the changes above and be able to successfully connect to the Cisco UCM web services interface.

Syslog Server

IQ-Core can receive syslog messages from Cisco UCM as it does with other devices. To configure this:

1. Log into the Cisco UCM Web GUI
   You can always use the 'Web GUI' button in the **Mange Devices** page to quickly launch this.
2. Go to System/Enterprise Parameters menu
3. Set 'Remote Syslog Server Name'
   Put the IQ-Core Server IP address in this field.
4. Modify severity level
   If you would like, you can also change the severity level of messages that should be sent from Cisco UCM to IQ-Core Software.

Enable CDR/CMR Collection

These are the basic settings which configure Cisco UCM to collect call detail records.

1. Log into the UCM web GUI
   If IQ-Core is successfully managing Cisco UCM, you can quickly do this by clicking the 'Web GUI' button in the Manage Devices Page.
2. Go to System/Service Parameters
3. Set 'CDR Enabled' flag to true
4. Set 'CDR Log Calls With Zero Duration' to true
5. Set 'Call Diagnostics Enabled' flag to 'Enabled only when CDR Enabled flag is true'.

Billing Server For CDRs

IQ-Core uses Cisco Call Detail Records and Call Management Records for call reporting features. You will need to configure Cisco UCM to send this data to IQ-Core Server via SFTP.

1. Log into the UCM web GUI
   If IQ-Core is successfully managing Cisco UCM, you can quickly do this by clicking the 'Web GUI' button in the Manage Devices Page.
2. Go to 'Cisco Unified Servicability'
   This is at the top right of the page. Click 'Go'.
3. Go to 'Tools/CDRs' menu
4. Click 'Add New' and fill in the following fields:

   Host Name/IP
   IP address of the IQ-Core Server

   User
   A valid Windows user on the IQ-Core Server. The user must also be configured as an IQ-Core Software user. See ManageRoles.

   Password
   Password of the above user.

   Protocol
   Select SFTP

   Directory Path
   /cdrs/
5. Click 'Add'
   Cisco UCM will attempt to connect to the IQ-Core Server with the information you have entered. If there is a problem, it will display a message.

Certificate Configuration Help

IQ-Core Software manages some devices (like Cisco UCM) through a secure web services interface. For these kinds of interfaces, a device certificate must be installed on the IQ-Core Server computer, and the name of the certificate needs to be resolvable to an IP address through DNS or a hosts file.

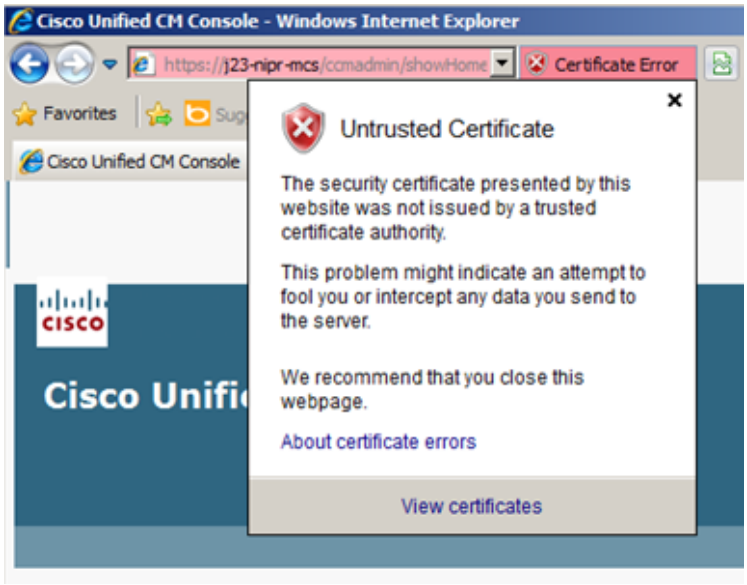
Certificate Installation

There are a couple different ways to install certificates on a Microsoft Windows machine. Here are the manual steps for devices that have a web GUI (like Cisco UCM).

1. Browse To Application
   Find the device in the Manage Devices Page and click on the 'Web GUI' button on the toolbar. This will open up a web browser to the site.

   > You may need to run the browser **as administrator** if the security settings of the browser do not allow viewing of certificates.

2. Click 'Continue to site'
   You will see text like 'There is a problem with this website's security'. Click the link that allows you to continue to the site and accept any warnings that appear.
3. Click Certificate Error Box
   At the top of the browser you will see a 'Certificate Error' box. Click on this to view the error. It will look like:



4. Click 'View Certificates'

   > Make a note of the certificate host name. You will need when setting up the hosts file (below) and in the Change Device Wizard.

5. Click 'Install Certificates'
   The Certificate Import wizard will appear. Click 'Next'.
6. Select 'Place all certificates in the following store'.
   And click the Browse button.
7. Check 'Show physical stores'.
   Then select the 'Trusted Root Certification Authorities' in the list box. Choose 'Local Computer' or 'Enterprise'. If you do not see these, choose 'Registry'.
8. Finish wizard
   The certificate will be imported and give a success message. It will take IQ-Core a minute or two to notice the newly installed certificate.

DNS or Host File

IQ-Core needs to communicate with a certificate-based device (like Cisco UCM) with a host name and not an IP address. The host name is the certificate name. You will need to make a mapping of the host name to IP

address in DNS or in the local hosts file. To set in the hosts file, follow these steps:

1. Run Notepad as administrator
   And open the following file: C:\Windows\System32\drivers\etc\hosts. You will need to view all files in the Open File dialog, not just TXT files.
2. Add the IP to Host Mapping
   Follow the example in the file. Example:

   192.168.1.30 MyCUCMCertificate.
3. Save the file.
   It will take IQ-Core a minute or so to notice the change.

Adding A Device Overview

IQ-Core Software supports many different kinds of devices. You can add, change, or remove a device at any time. Once added, IQ-Core will help monitor and configure devices and give you easy access to the underlying CLI or GUI. Device types that are supported include:

- Network routers and switches
- Firewalls
- Call managers
- Wireless controllers
- Servers and services
- VMware ESX hosts and VMs
- Terminal servers

Add Device

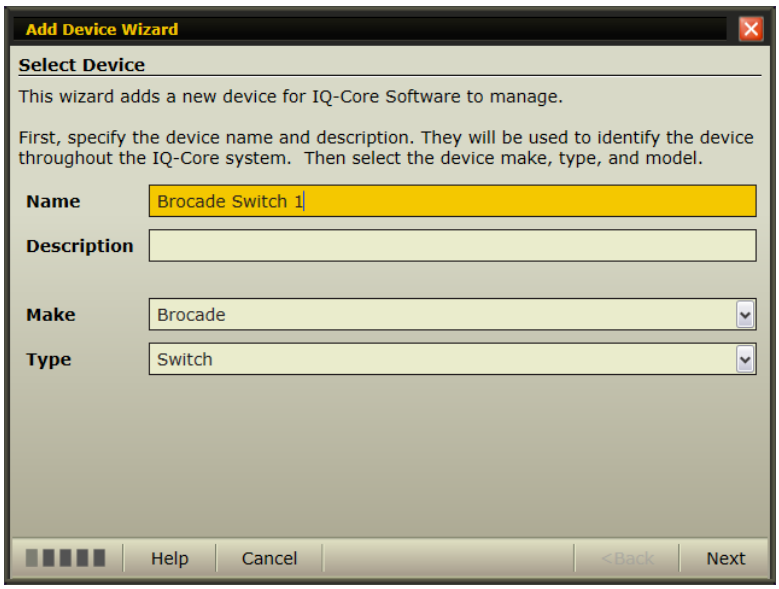
You add a device from the 'Devices' page by clicking 'Devices' in the main left-hand menu. You can also add a device directly from the Dashboard. Before you add a device you will need some information about how to communicate with the device. This includes:

- IP Address or hostname
- SSH credentials
- SNMP parameters and credentials
- Web URL if applicable

To add a device:

1. In the Devices page, click the 'Device' button in the top toolbar and select 'Add Device'
   This will bring up the 'Add Device Wizard'.

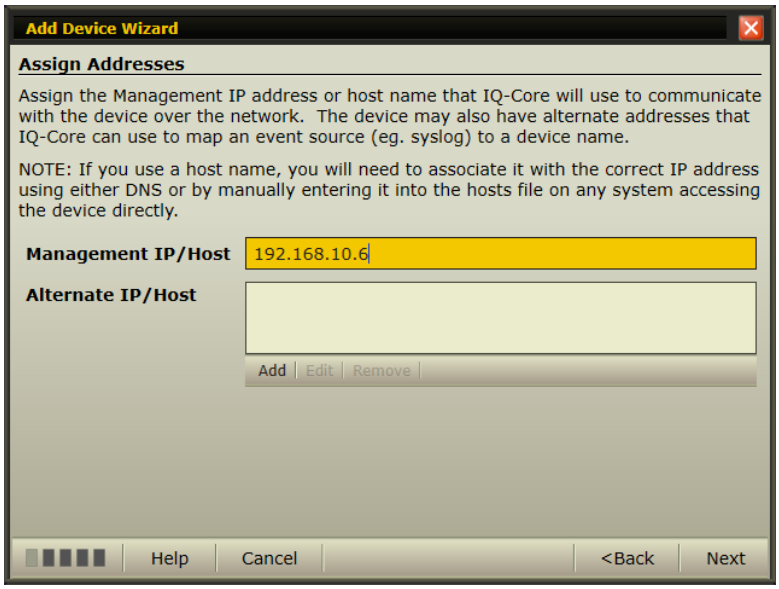
2. Type any Name and Description
   The Name and Description are used throughout the user interface. Use values that make sense for your system/deployment.



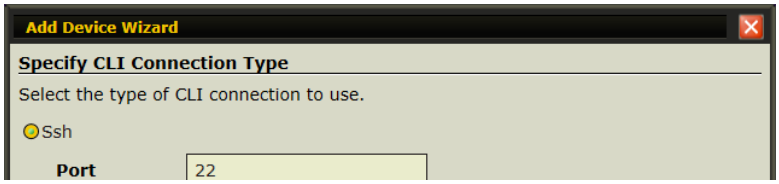
3. Select the Make and Model
   Choose the closest values for your device. If you do not see values that match your device you can always manage any device by selecting the 'Generic Device'

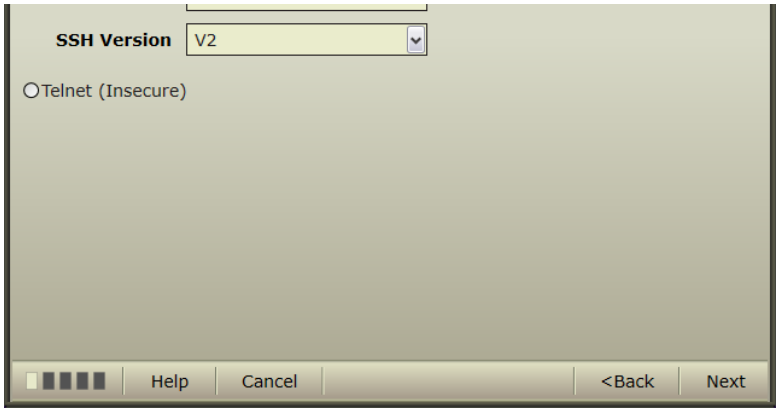
> The wizard pages that follow will vary slightly depending on the device type you select

4. Type in the management IP/Host
   IQ-Core will communicate with the device using this IP address or hostname. If you specify a hostname, you must be using DNS or have added an appropriate entry in the local hosts file. Some devices have IP addresses for other interfaces that are different than the management IP (e.g. for sourcing syslog messages). If you know these, you can add them here and IQ-Core will be able to map the IP to this device.

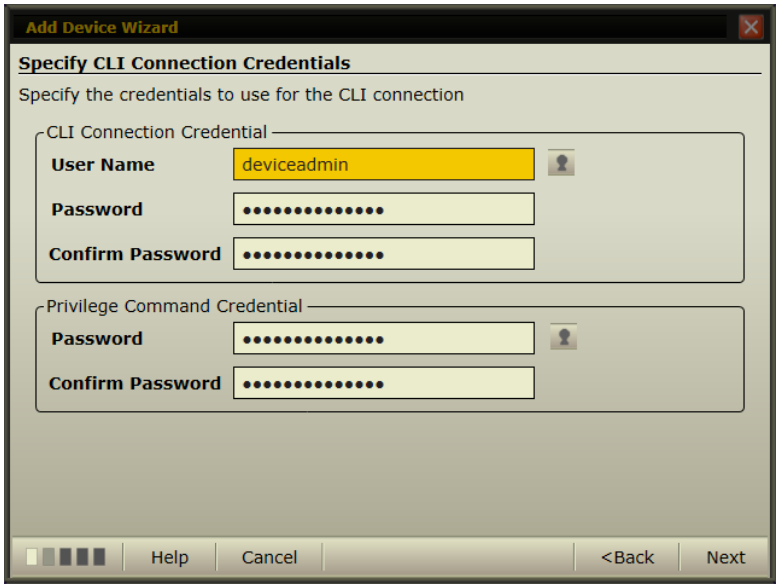


5. Select the CLI protocol
   IQ-Core communicates with most devices through SSH. Only select Telnet if you know that is the only way your device is configured to communicate. Telnet is insecure and should not be used in most environments.



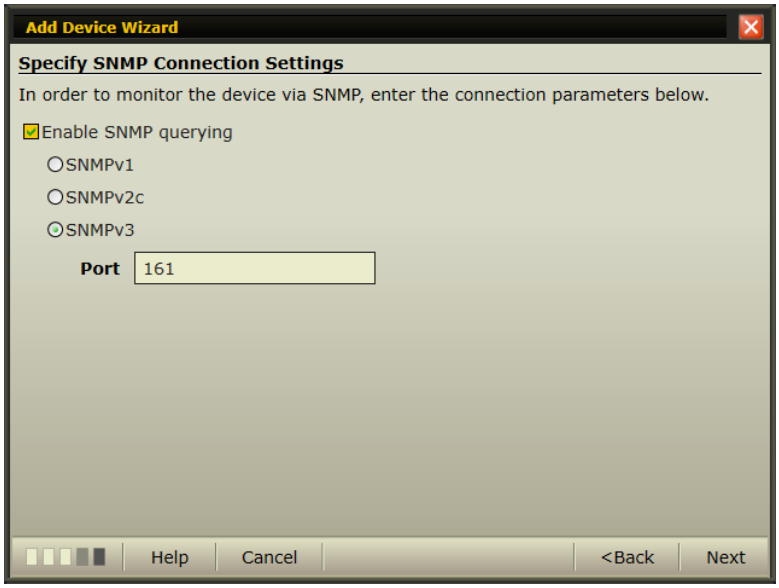


6. Enter the CLI (SSH) credentials
   IQ-Core will use these credentials to log into the device and keep a persistent connection. Use credentials that have administrative access so that IQ-Core can fully monitor and configure the device.

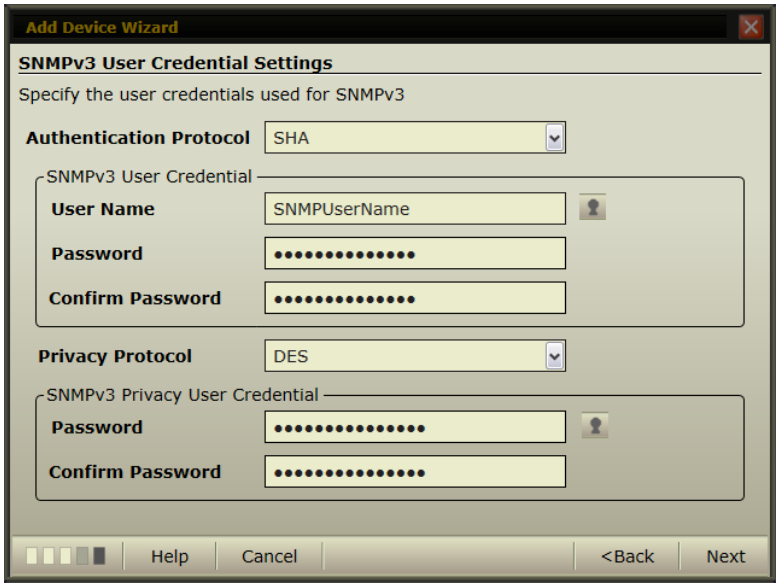


7. Select the SNMP protocol
   Only SNMPv3 is a secure protocol so use v1 or v2 only when necessary.

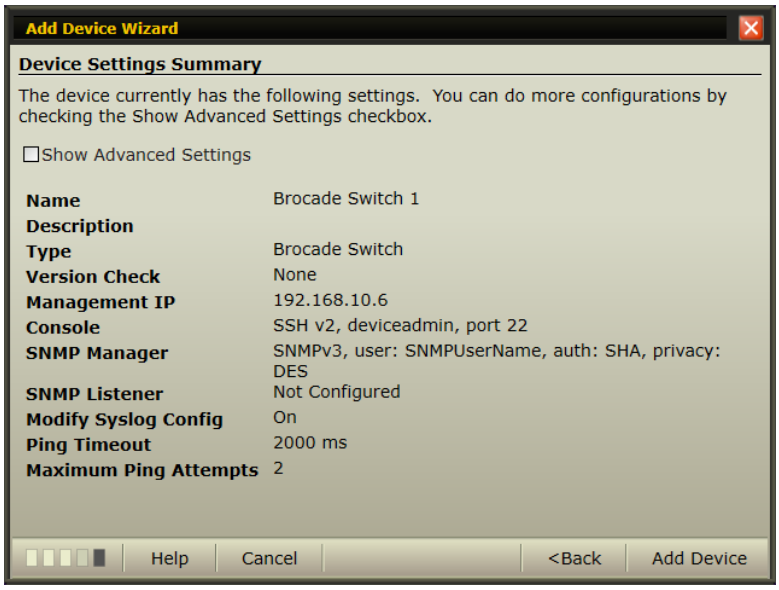
> SNMPv3 is sometimes difficult to configure on devices. You can tell IQ-Core to use SNMPv3 here and then later use the IQ-Core **Enable SNMP Wizard** to help configure the actual device. This wizard is accessed via the 'Enable SNMP' button on the Device page toolbar.



8. Enter SNMP security settings
   If you selected SNMPv1 or v2, enter the community string that your device is using. For SNMPv3 enter the authentication and privacy parameters that the device is, or will be, configured with.

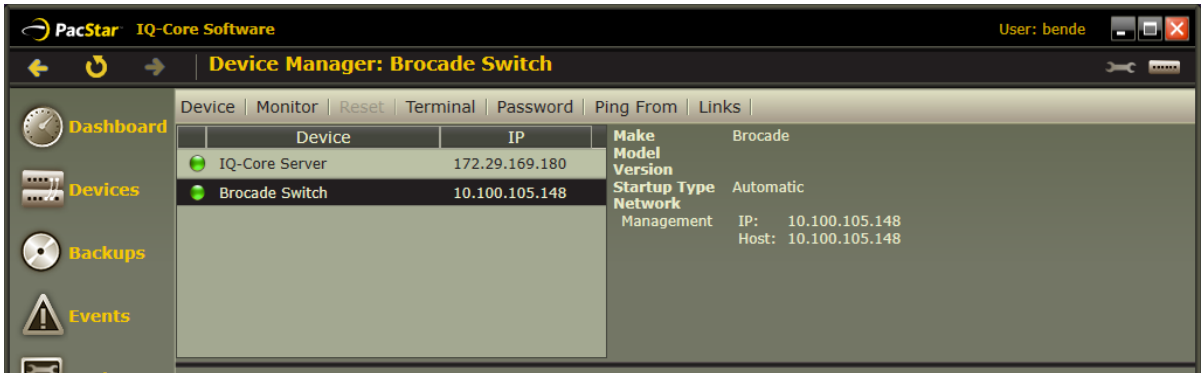


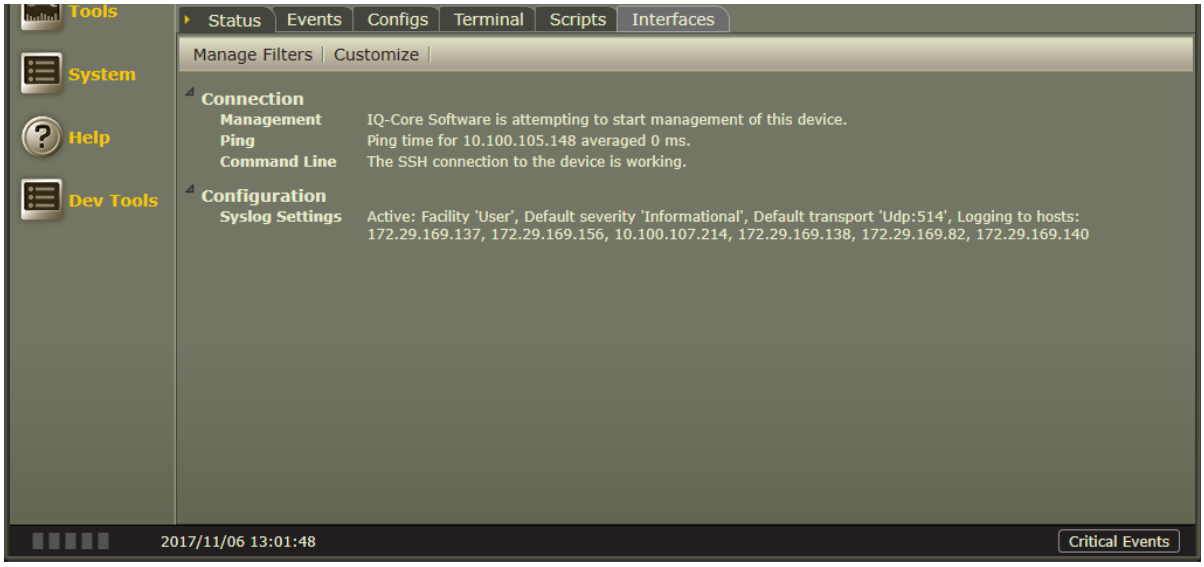
9. Review and Add
   Review the settings that were entered and click 'Add' to have IQ-Core start managing it.



After Device Is Added

You will see a new entry for the device in the Devices page. While IQ-Core is attempting to communicate with the device via SSH and SNMP, the device indicator will be yellow. The indicator will then turn green or red depending on whether the communication succeeds or fails.





Once the device is green, IQ-Core will be monitoring the device and you will have access to all the features available for that device.

Tips For Fixing Common Problems

If IQ-Core is displaying a red device indicator, then look in the 'Status' tab for any error messages. Common connection problems are:

1. **Ping failure**
   This means that the device cannot be seen on the network. Check the management IP address or hostname. If using a hostname, ensure that DNS is accessible or that there is a local hosts entry.
2. **Command Line failure**
   This means that the SSH (or Telnet) connection cannot be made. The error text will indicate what the problem might be. Common errors are:
   - No connection could be made because the target actively refused it
     This almost always means that the device is not configured to receive SSH connections. This involves configuring the device for SSH and setting up the cryptographic keys. Consult the device documentation for how to do this.

     This error can also mean there is an ACL or firewall that is blocking access. Check the rules for all devices in the network path.
   - Authorization failed
     This almost always means that IQ-Core is not using the correct username or password for the CLI connection. Use the 'Change Device Wizard' to sync IQ-Core with the existing device configuration.
   - Timeout Error
     Some devices have slow management CLIs. You may occasionally see a timeout error when the device does not respond to IQ-Core in a reasonable amount of time. Note that IQ-Core will periodically connect and maintain the CLI connection so timeouts often go away quickly.
3. **SNMP failure**
   You may see SNMP errors in the 'Status' tab. Some common errors are listed below.

   > If your device has not yet been configured for SNMP access or you want to quickly sync up the IQ-Core configuration with the actual device configuration, use the **Enable SNMP Wizard** accessed by a button on the Device page toolbar.

   - The connected party did not properly respond after a period of time
     This almost always means that IQ-Core is not using the SNMP credentials or hash/encryption types that the device is currently configured for. However, it can also mean a true timeout if the device is busy. Use the 'Change Device' Wizard to sync IQ-Core with the existing device configuration.
   - User not found
     This means that the SNMP hash/encryption types seem correct but that the SNMP user that IQ-Core is using does not exist on the device.
   - Invalid Engine Id

When connecting to a device via SNMPv3, IQ-Core will cache the underlying engine id of the device. The engine id is an attribute of the device and if IQ-Core receives a different engine identifier, it may be an indication of a security problem because the device appears to have changed. To clear this error, you can run the 'Restart Collectors' Wizard from the Device page toolbar.

4. **Management State failure**
   The 'Management' state is used to track the internal management of the device. You will see it change occasionally to indicate this state. If it is red, it is likely because of Ping, CLI, or SNMP failures.

Stop and Start Monitoring

Once a device is added, you can quickly tell IQ-Core to **stop** managing it without removing the device from the system. To do so, click the 'Monitor' button on the Devices page when the device is selected and click 'Stop'. The device health indicator will become Gray to indicate that IQ-Core is not communicating with it.

Device Tab Overview

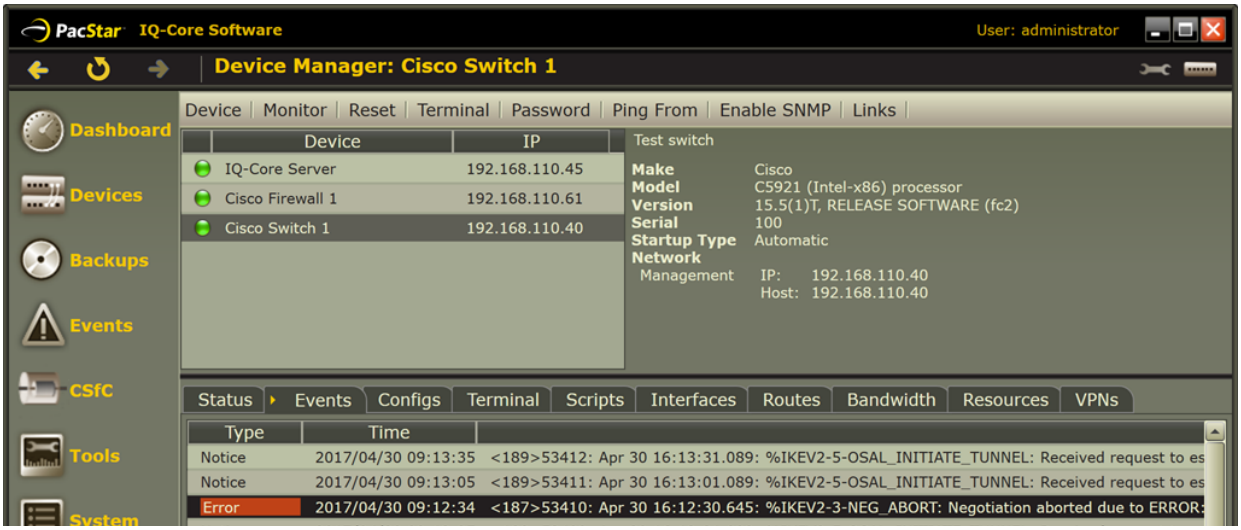
The Devices page is where the majority of the per-device functionality is available. Here are examples to navigate to and try out. Note that while devices have many common tabs, some devices have more or less tabs depending on features specific to that device.

Status Tab

The Status tab is where you will see information about device connectivity, health, and configuration. If the device icon indicator is not green, then the Status tab will have information about possible problems. You can also add your own custom status monitors to the Status tab by clicking the 'Custom' button.

Events Tab

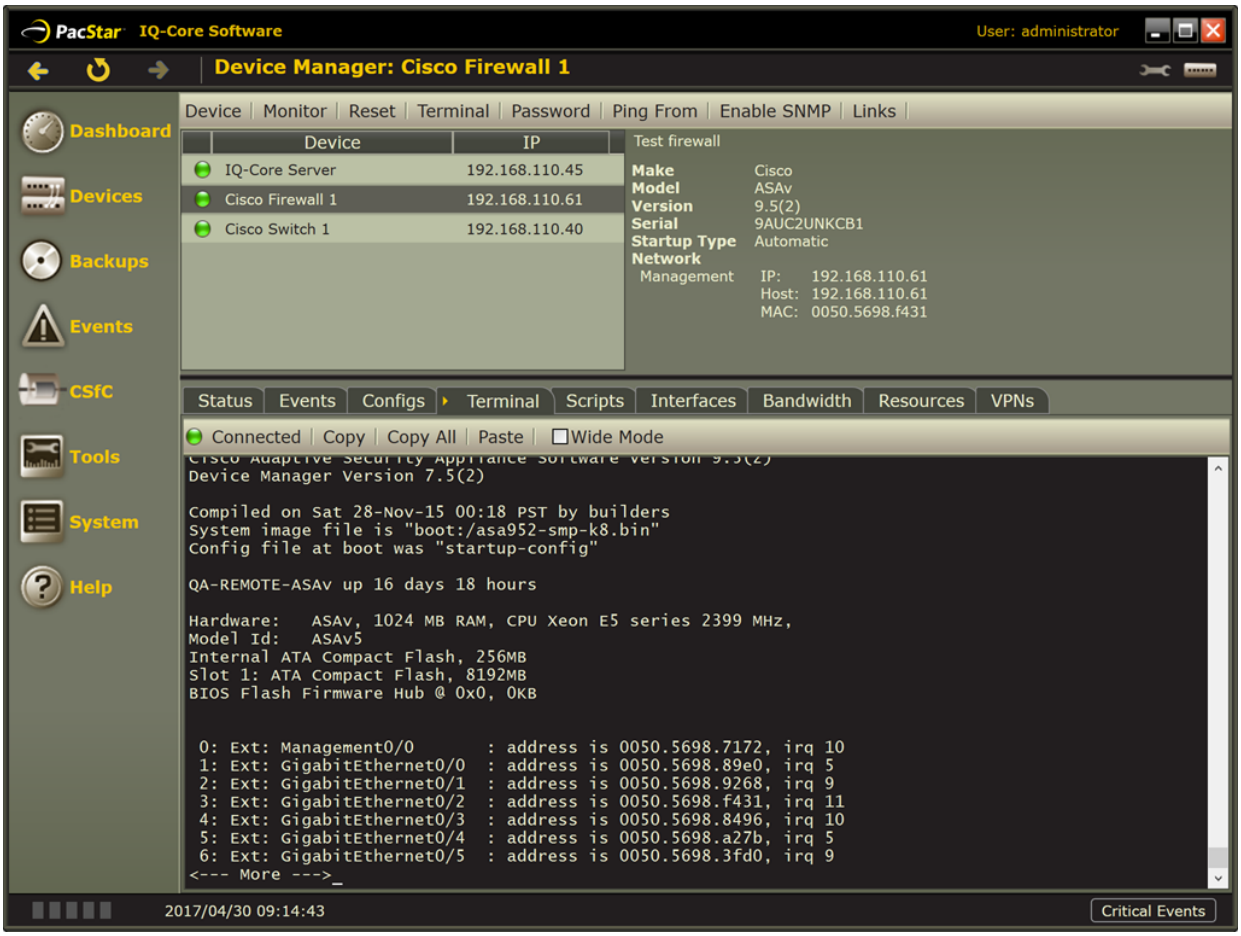
The Events tab shows a list of events already filtered for this device. This list will contain a combination of syslog, traps, and IQ-Core generated events, depending on device configuration. You can also click the main 'Events' menu item on the left-hand side of IQ-Core to manage all events from all devices.



Terminal Tab

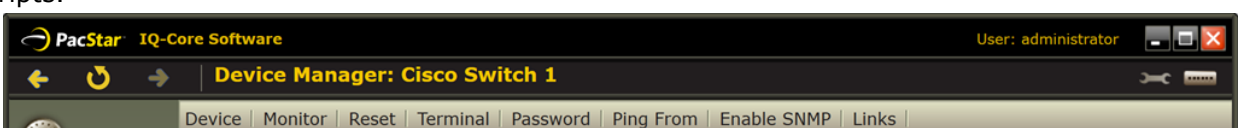
You can access the Command Line Interface (CLI) for a device if it has one. This provides the same behavior as applications like Putty.

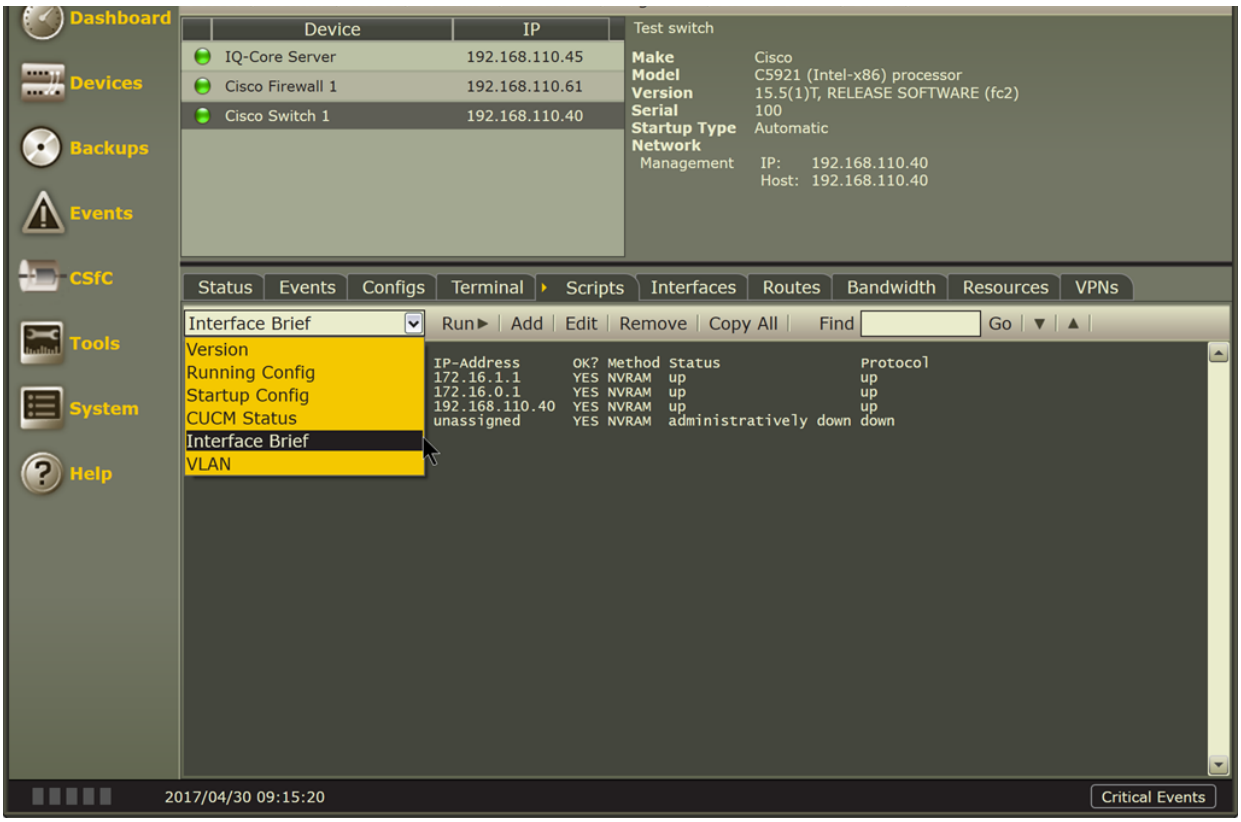
> IQ-Core also provided a separate Terminal window that you can access via the 'Terminal' toolbar button in the Devices page. Additionally, Putty is always available from the 'Links' button on that same page in case you need to troubleshoot connections.



Scripts Tab

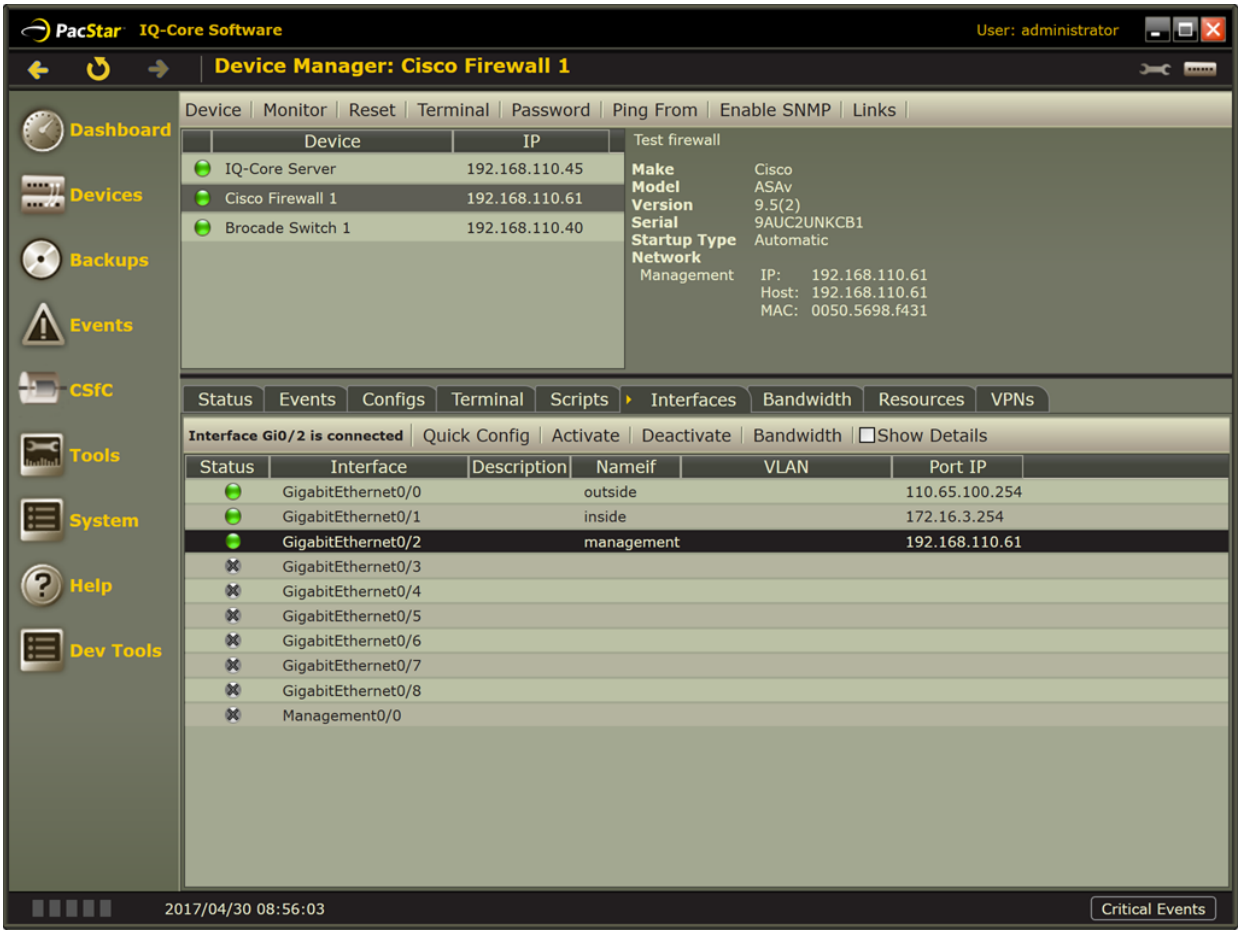
When interacting with the CLI, it is common to have commands you frequently enter. The Scripts tab is a place where you can put any CLI script that will execute and show output. IQ-Core comes with a number of useful scripts.





Interfaces Tab

This tab gives you at-a-glance status of each device interface. You can quickly view the underlying device interface configuration and metrics by double-clicking an interface or by clicking the 'Show Details' checkbox.



Bandwidth Tab

IQ-Core monitors the number of bytes in and out on each device interface and shows you this data in real-time or based on some date range. You can also arrange for IQ-Core to alert you when the bandwidth exceeds some value. Click the 'Thresholds' button to do this.

Resources Tab

IQ-Core monitors the CPU and memory usage of each device and shows you this data in real-time or based on some date range. You can also arrange for IQ-Core to alert you when the bandwidth exceeds some value. Click the 'Thresholds' button to do this.


30
20
10
0
09:14:00
09:14:50
09:15:40
09:16:30
09:17:20
09:18:10
2017/04/30 09:19:08
Critical Events

Dashboard Overview

The IQ-Core Dashboard consists of a network diagram and a list of events, both updated in real-time. The network diagram is customizable and serves as an 'at-a-glance' view of the system being managed. You can do the following with the diagram:

- View device health with pertinent information
- Connect devices to show latency, topology, interface status, or other device status
- View widgets for interface or other device status

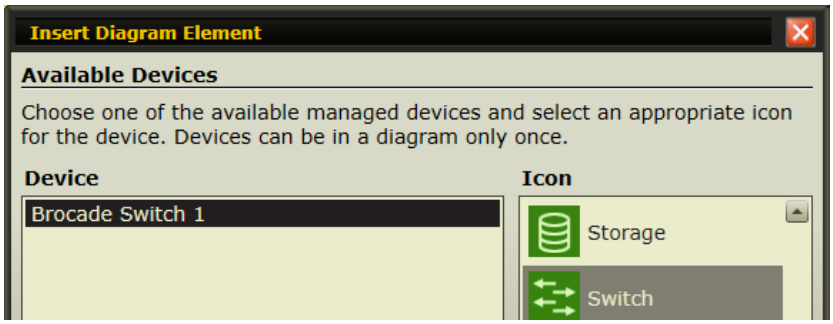
The event list below the diagram is updated as events come in with the latest shown first. These events are from the devices themselves (syslog, SNMP traps) and from IQ-Core itself. You can manage events by clicking on the 'Events' icon in the left-side menu.

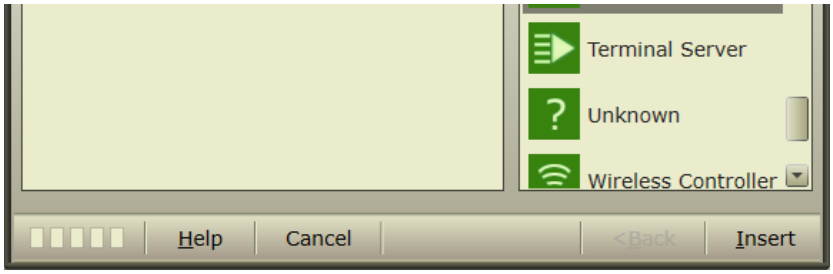
Add Device To Diagram

You can add either a new device or existing device to the diagram. To add an existing device:

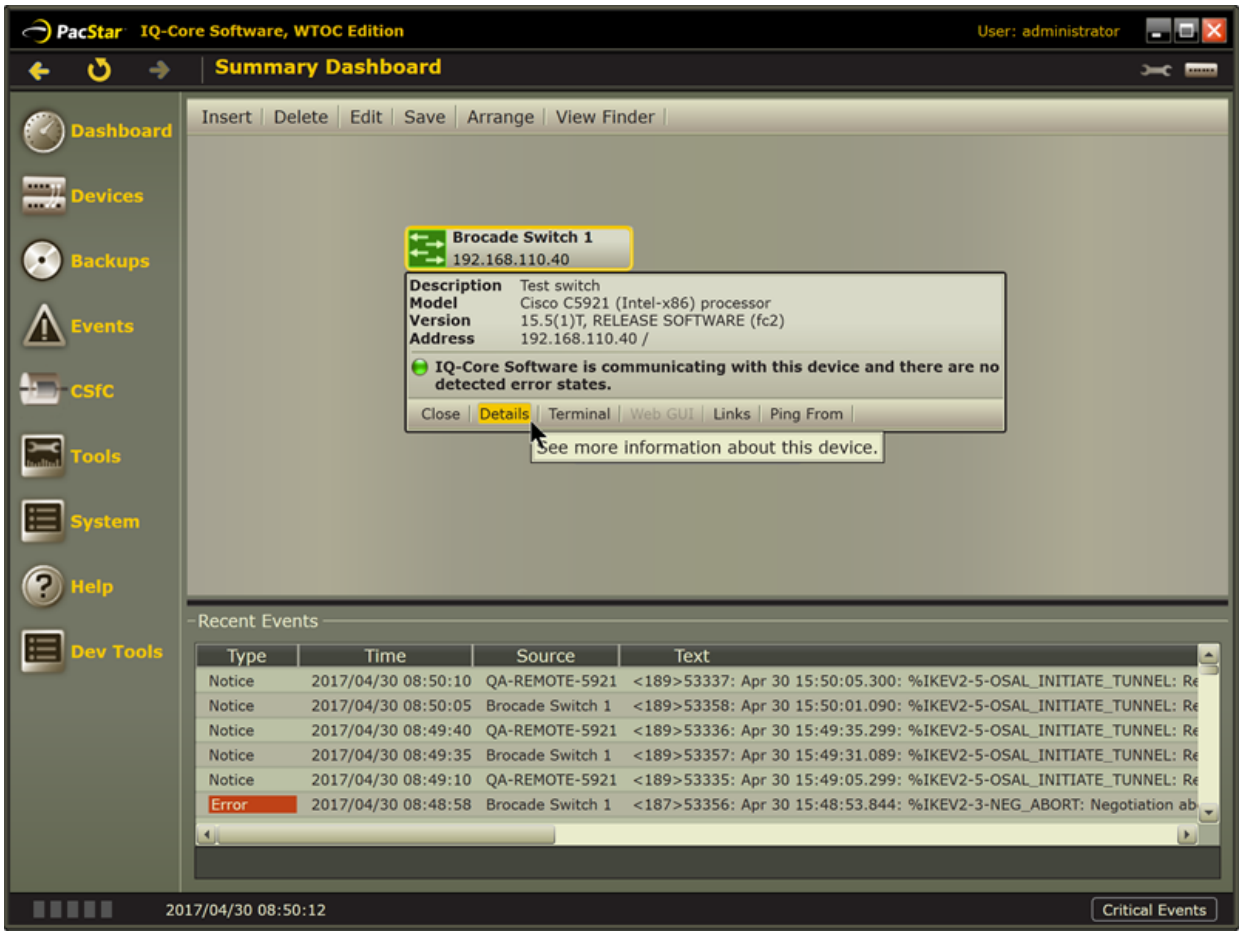
1. Click the 'Insert' button
   And select 'Device/Existing Device'.

2. Choose icon
   An appropriate default icon will be preselected but you can change to another to more closely match the device function.

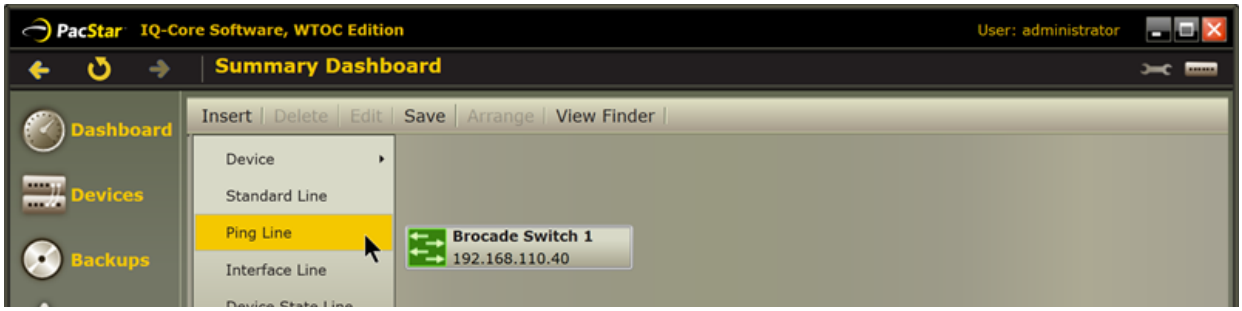


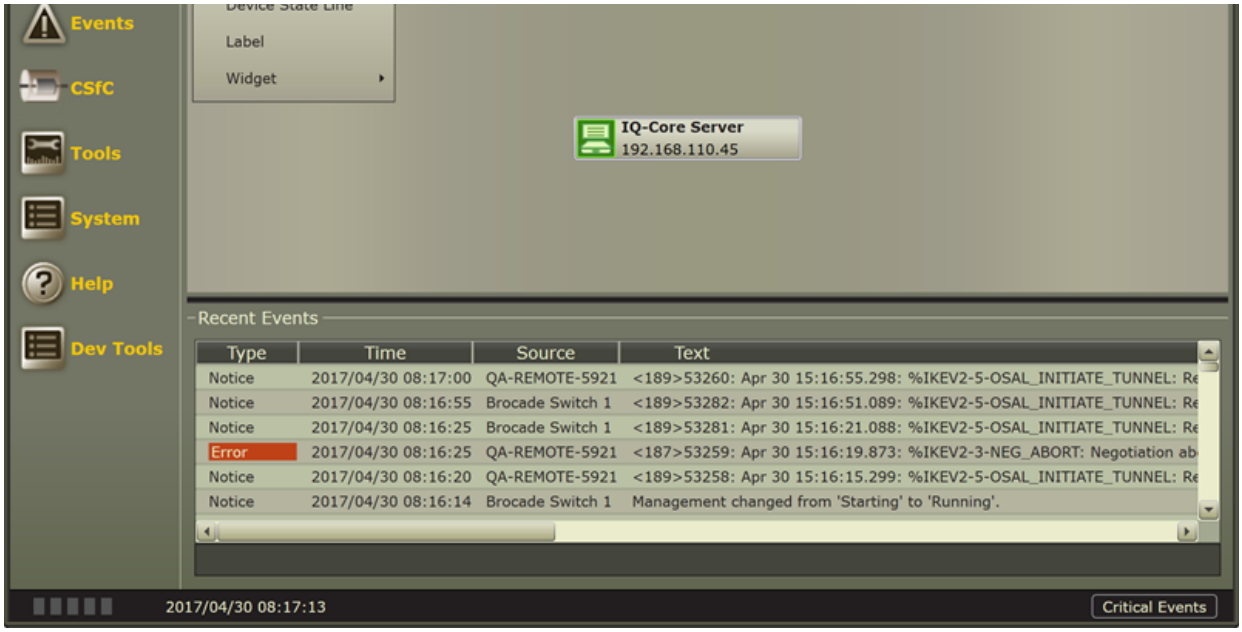


3. Device is now in diagram
   You can now click on the device to get a summary of status and quick links to common functionality like opening a CLI terminal or viewing a device Web GUI. Click the 'Details' button to go to the main device page where you can interact further with the device.

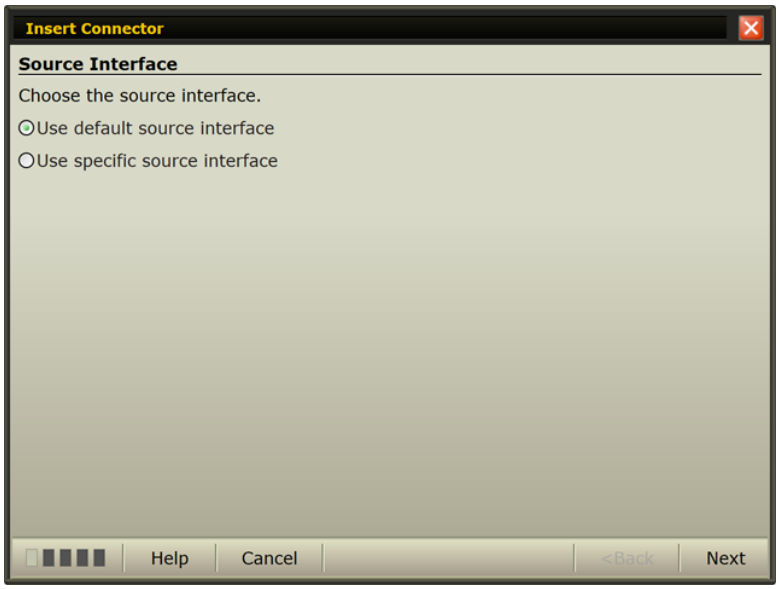


4. Connect two devices
   In this example, a 'Ping' connector is used so that you can view latency between devices. Note that IQ-Core can source pings from supported devices so that latency can be monitored throughout the network. You can also connect devices or widgets with lines that represent interface status, specific device states (like SNMP values), or other types of connectivity.
5. Click 'Insert/Ping Line' from the top toolbar
   This will put the diagram in a mode where you first click the device where the ping will be sourced and then click the destination device that will be pinged.

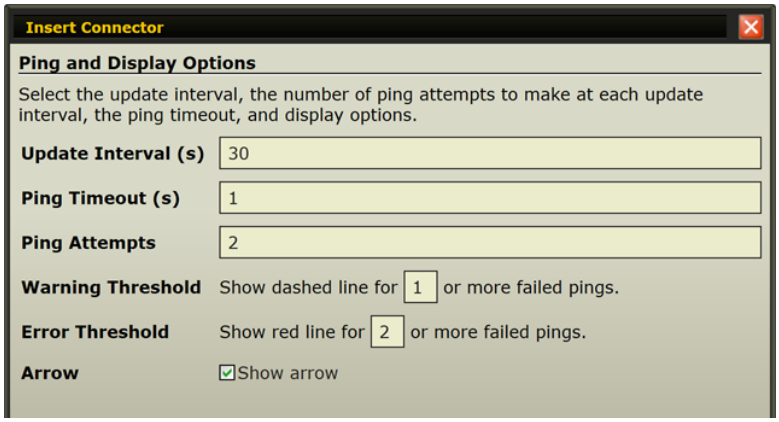


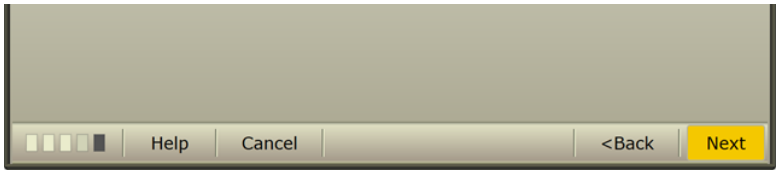


6. Click the Source device (1) and then click the Destination device (2)
   The mouse icon changes to indicate which device is the source and which is the destination.
7. Choose Source and Destination Interfaces
   For this example, leave as the default interfaces. You could also select a specific interface on the device to source your ping from and/or a specifc interface to send the ping to.

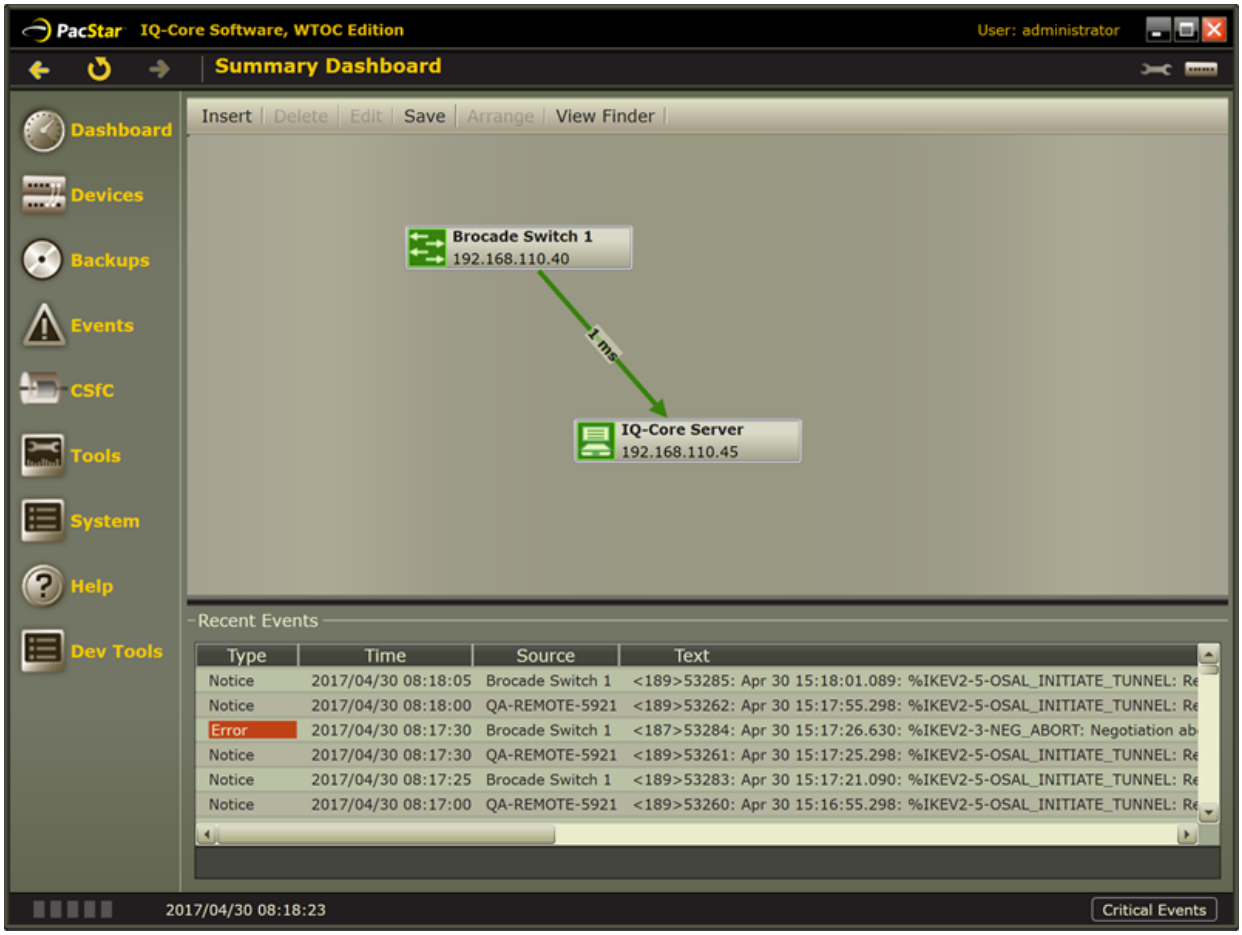


8. Modify Ping Settings
   For this example, leave as the defaults. But you can change how the newly created line will change based on the number and interval of ping attempts.





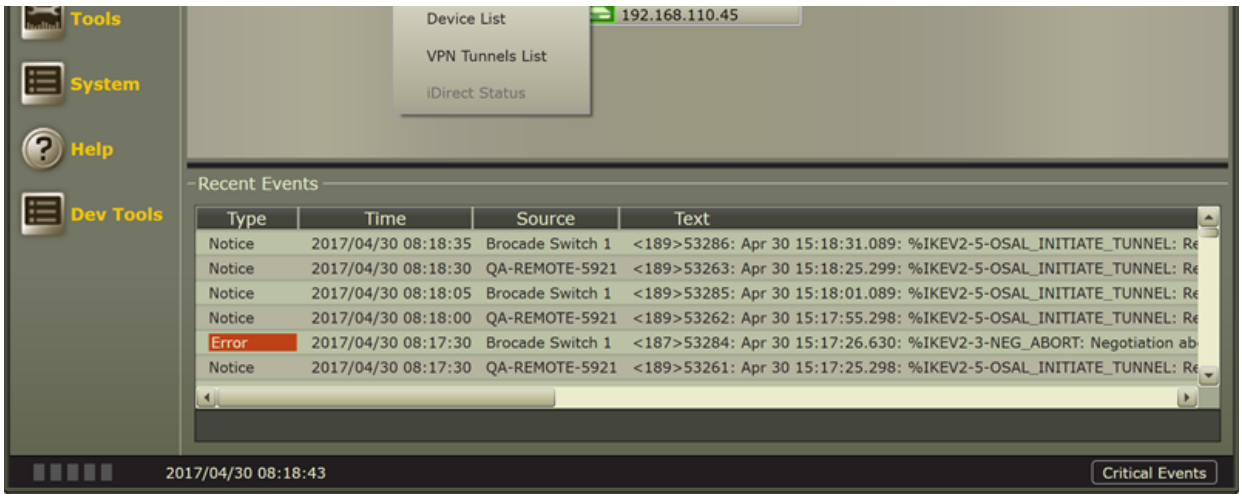
9. Ping (Latency) Line Appears
   The appearance of the line will change depending on ping status. You will also see the round-trip-time as the line label. When you source pings from various network devices, you will get a good sense of latency on the network paths.



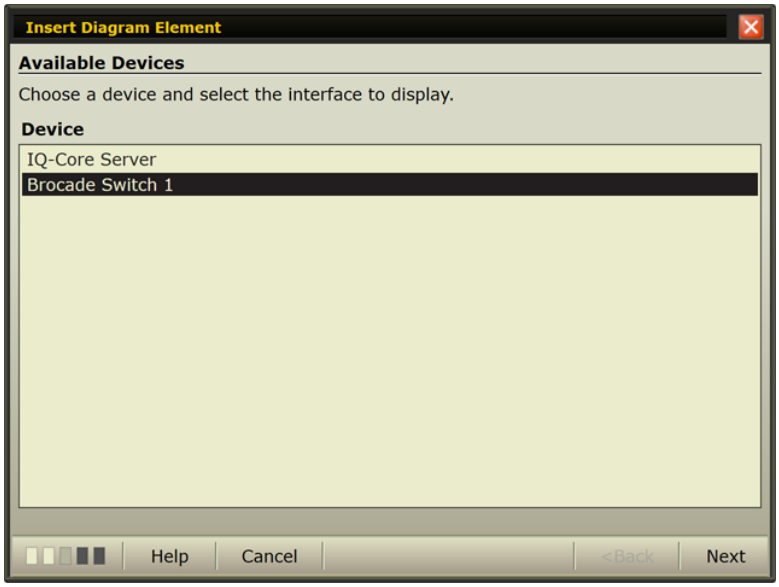
Add Interface Widget To Diagram

Another useful thing to add to the diagram is the status of a important device interfaces. This will give you an immediate indication if there is a problem with a port or interface.

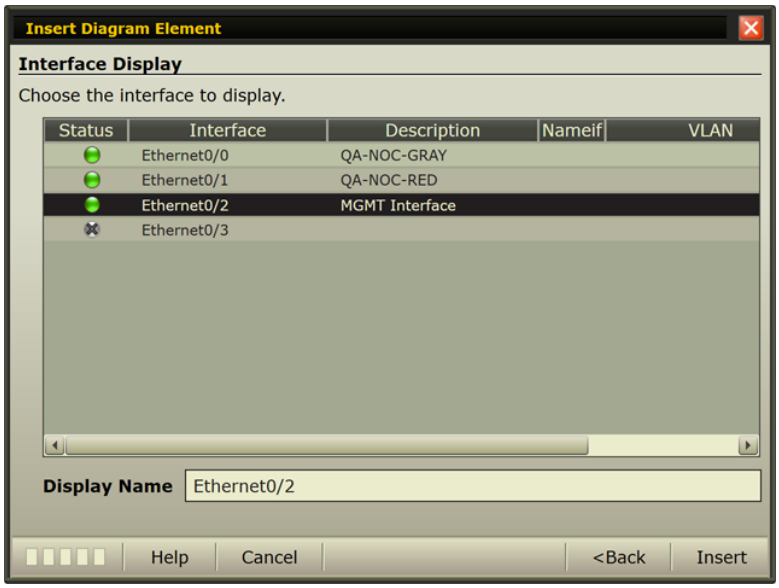
1. Click the 'Insert/Widget/Interface Status' option
   This will bring up a wizard that allows you to select the device and interface.



2. Choose the device

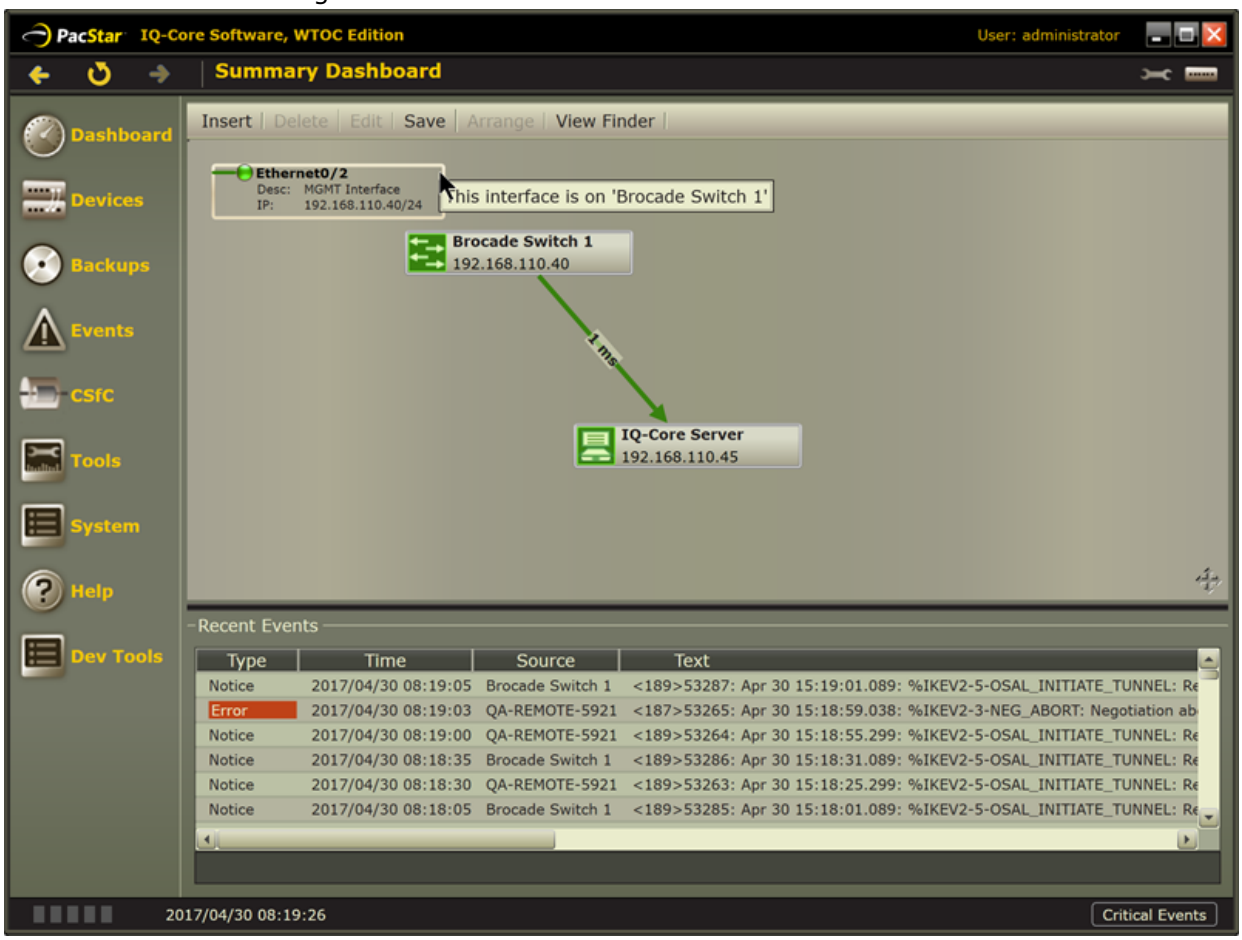


3. Choose the interface
   All the device interfaces that IQ-Core detects will be shown, along with the current connection status. Choose an interface and optionally change the name that will be displayed in the network diagram.



4. Interface widget now in diagram

You can resize and move this widget. You can also draw lines to and from this widget to show association with other devices or widgets.



Configuration Management Overview

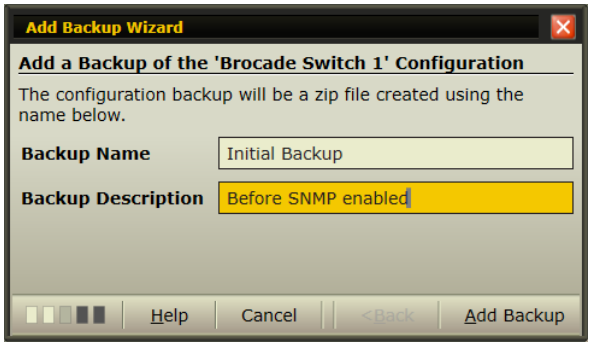
IQ-Core Software can back up and restore running configurations of devices. You can manually create a backup at any time but the software also automatically does a backup when it notices that a configuration has changed (when the device supports sending events when it's configuration changes). Additionally, one or more devices can be backed up on a daily schedule.

Back Up A Device

You can get the current running configuration (backup) for a device either by going to the 'Config' tab for the device or by clicking 'Backups' in the main left-hand menu. The main advantage of the 'Backups' page is that multiple device configurations can be retrieved at the same time, giving you a snapshot of the current system configuration. For most purposes, though, you will use the 'Configs' tab for the device as it has more per-device options. To manually create a backup:

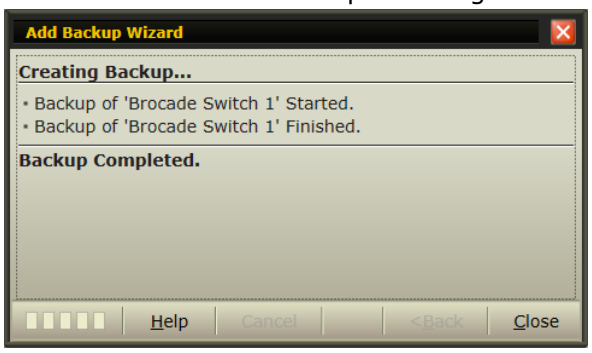
1. Go to the 'Configs' tab for the device
   Click the 'Backup' button to bring up the Backup Wizard

2. Enter any descriptive name
   The Name is used to identify the purpose of the backup. The Description is optional.



3. Complete the wizard

If there are any errors you will see them here. The primary reasons for a backup failing is that there are firewall rules or other ACLs preventing SCP or SFTP from the device.



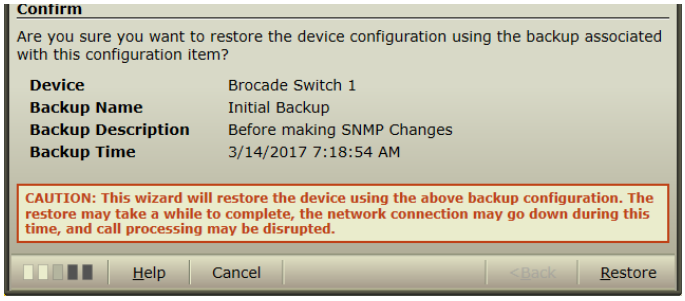
4. Backup shows in list
   The resulting backup file set shows up in the Configs tab list. Some devices (like Cisco routers and switches) have a single backup file while others may have multiple files. If the backed up files are readable (not all devices create readable files), you can double-click or click the 'View' button to see the configuration.

Restore A Configuration

Once you have a backup, you can push it back onto a device so that the device will start using that configuration. This is useful when undesirable configuration changes have been made and you want to get to a known state.

1. Go to the 'Configs' tab for the device
   Click the 'Restore' button after selecting the desired backup.

2. Confirm to continue
   Restoring a backup is 'destructive' in that the existing configuration will be deleted in favor of the new. Note that you can always take another backup before restoring.



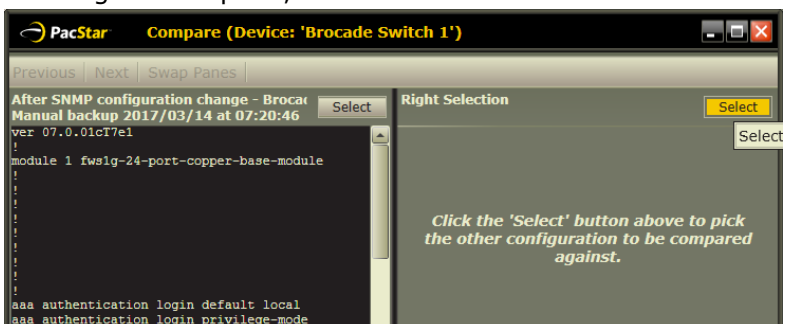
3. Wait for device to restart
   When complete, the device will usually reboot itself to start using the new configuration. This may take awhile and you'll see the IQ-Core monitoring system indicate that the device is offline.

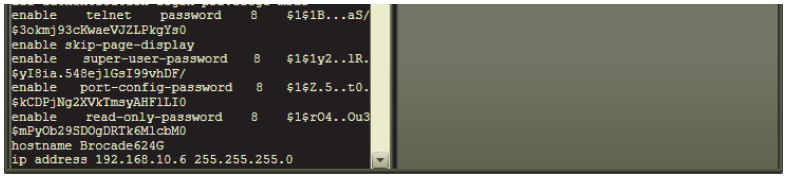
Comparing Configurations

It is often useful to see the differences between two configurations. To do so:

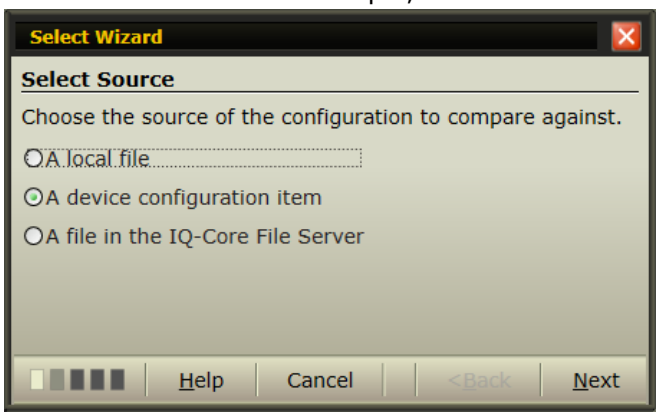
1. Go to the 'Configs' tab for the device
   Click the 'Compare' button after selecting one of the backups you would like to compare.

2. Select the file to compare to
   In the right-hand pane, click the 'Select' button

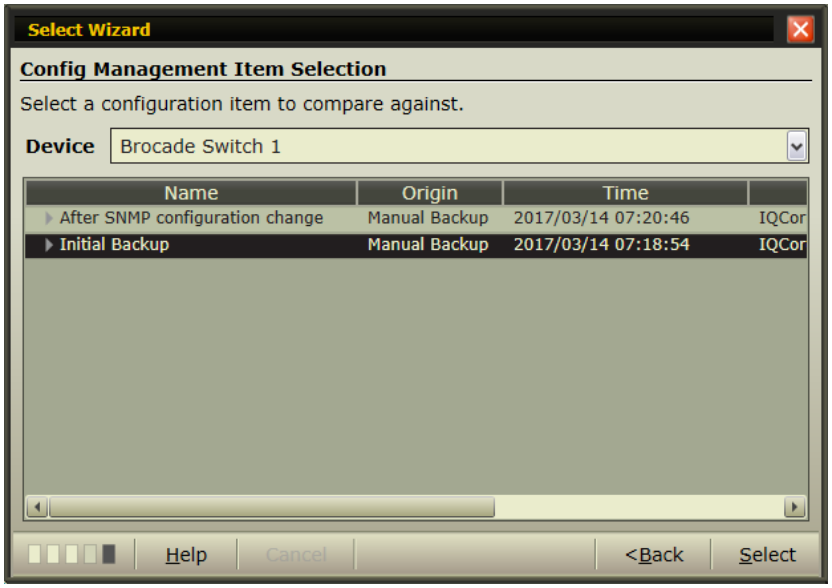




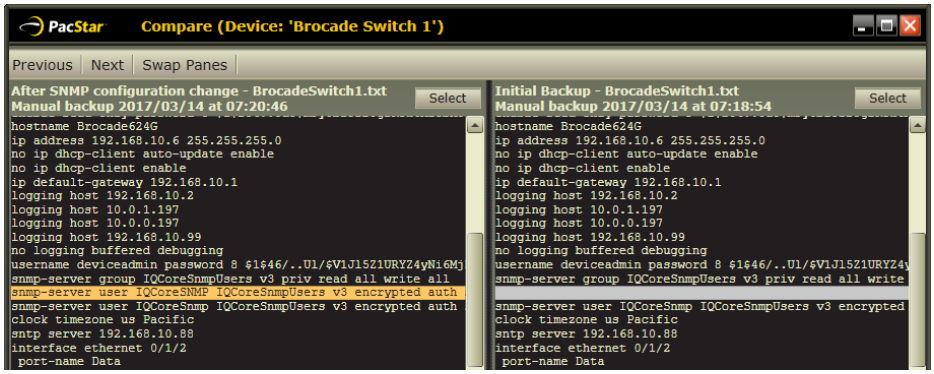
3. Choose the file source
   You can not only compare against backups you have taken, but also against any other configuration file you may have available. If the files are on the IQ-Core File Server (SFTP/SCP), you can select from that location as well. In this example, choose another device config (backup) item.

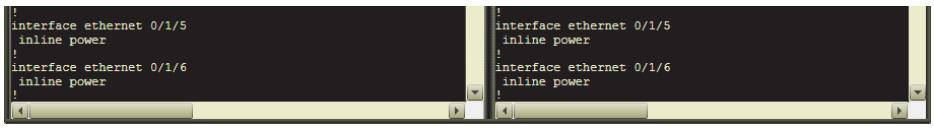


4. Choose the file
   The list will show you the same items that are in the Configs tab main listview. Note that you can also select items from another device.



5. Perform comparison
   The window will show both configurations side-by-side and color-code the lines that have been added, removed, or changed.




!
interface ethernet 0/1/5
 inline power
!
interface ethernet 0/1/6
 inline power
!
!
interface ethernet 0/1/5
 inline power
!
interface ethernet 0/1/6
 inline power
!

PacStar Technical Support

There may be various support tiers in your deployment which you should use for technical support. For assistance with any IQ-Core Sofware issue from PacStar directly, use the following information.

Contacts

Phone
+1.888.872.1512 or +1.503.906.7314

Service is available 24x7, 365 days a year. A PacStar support engineer will respond to your support request within a time frame that is based on the call's severity level.

For our U.S. DoD customers, our PacStar toll-free number is available world-wide via DSN - enabling you to contact PacStar support where ever you have DSN access.

Web
A support request can be entered here: http://www.pacstar.com/

Email
Send a request to **techsupport@pacstar.com**.

Apply Profile Wizard

This wizard helps you quickly customize the IQ-Core configuration for the system (node) you are managing. This is called a Profile. This wizard is accessible from the **System/Profiles and Snapshots** menu.

For Army WIN-T systems, the profile lets you select the node and enclave type, giving other basic IP and credential information that IQ-Core will use to manage the node devices. The application of the profile will reset IQ-Core to a default state, then build it up to configure IQ-Core to manage the node. For example, the Profile will add devices such as the Tier 2 Router, Tier 2 Switch, Call Manager, Host Firewall, etc. The devices will be added to IQ-Core with appropriate WIN-T display names.

While you can apply a profile at any time, you will primarily use it for initial system configuration. Use the Export IQ-Core Snapshot Wizard wizard to save off a copy of an IQ-Core configuration that you can later import to quickly configure a system.

After profile application, you will still likely need to modify specific IP addresses and passwords that do not match the patterns that the profile uses. To do so, use the Change Device Wizard in the Manage Devices Page.

> ⚠ Applying a profile will erase all of your existing IQ-Core configuration including device list, IP addresses, passwords, scripts, etc. If you want to make a copy of the existing configuration, use the Export IQ-Core Snapshot Wizard. You can then get back to the current state by importing that snapshot with the Import IQ-Core Snapshot Wizard.

> ⚠ Profile application can fail if another application is using one of the IQ-Core configuration files. Ensure that you have no editors nor Explorer windows open to the IQ-Core Server configuration folder (IQ-Core/Service/Config).

Laptop Type

While the same build is used for every management laptop, there are a couple unique configuration items on certain node types. This is because IQ-Core is a client-server application. Specify the type of the laptop you are running IQ-Core on and you will be presented with guidance on how to correctly configure it.

- For **Element** and **LAN Manager** laptops:
  The Profile will configure IQ-Core to actively manage the node. The IQ-Core Server service will run on these laptops and perform all device communication.
- For **Node Manager** laptops:
  The Profile will configure the IQ-Core Client to *point* to the IQ-Core Server that is running on the associated Element/LAN Manager laptop. The IQ-Core Server service will be disabled on this laptop and you will have only a client view. This keeps network traffic to a minimum by having only a single IQ-Core Server talking to devices.

Node Identification

Node Type
Select the WIN-T node type that you will be managing. If you have a customized node that isn't exactly one of the choices, just pick the closest one. You can modify it after the profile is applied.

Node Enclave
Select the security enclave type of the node, NIPR, SIPR, Colorless, etc.

Node Release
Select the release indicator so that IQ-Core will add the appropriate devices to be managed. The differences generally are:

- AO14
  This the original device payload.
- AO15
  Some devices and firmware versions changed, including the Tier 2 Switch becoming a Cisco NEXUS switch, Cisco UCM moving to v10.5, and Brocade User Access Cases added.
- AO16
  This is the latest incarnation of each node type which includes Palo Alto firewalls.

IP Address
WIN-T nodes use a patterned IP scheme, where the first three octets are generally the same, and the last octet is fixed for a particular device. Use the first three octets that are most common to your devices. This

scheme is not always adhered to however, so you will likely need to modify the IP addresses for some devices on the next wizard page. You can also use the Change Device Wizard in the Manage Devices Page at any time to change IP addresses.

User Access Cases

WIN-T nodes have network switches (either Cisco or Brocade) that are in a user access case. Select the type of each user access case that you currently have. You can always add/remove these later with the AddUACWizard from the Manage Devices Page.

Review Profile Devices

Each device that will be added to the system is shown in the 'Review Profile Devices' page with the ability to edit any of the individual IP addresses. It is very likely that the fourth octet of many of these devices will need to be changed to match the actual node configuration. You will also be able to change these later using the Change Device Wizard.

CLI Credentials

It is likely that many of your devices use the same username and password for CLI (SSH) access. Enter those common values here and IQ-Core will use these to try and communicate with the device. It is also likely that some of the devices have a unique username or password. You will need to set these per device after the profile application by going to the Change Device Wizard in the Manage Devices Page.

The usernames and passwords you enter in the Apply Profile Wizard are also used to create a . This allows you to quickly use them in various places in IQ-Core without having to type them in each time (like a password vault).

SNMP Credentials

It is likely that many of your devices use the same username and password for SNMPv3 access or the same community string for SNMPv2 access. Enter those common values here and IQ-Core will use these to try and communicate with the device. It is also likely that some of the devices have a unique username or password. You will need to set these per device after the profile application by going to the Change Device Wizard in the Manage Devices Page.

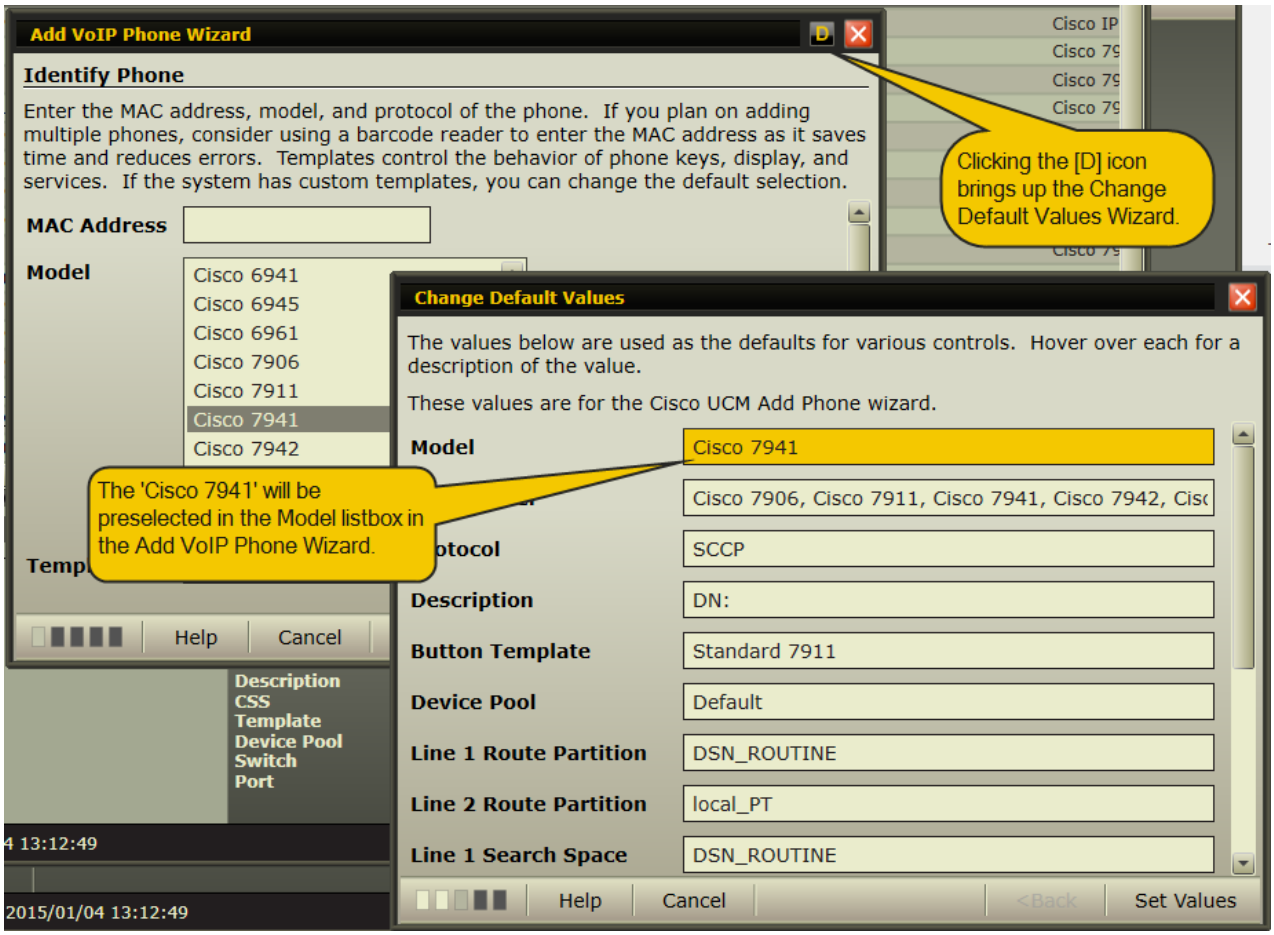
Change Default Values Wizard

IQ-Core Software contains numerous wizards and pages that allow control over the prepopulation or preselection of values. This facility makes it easier for an operator to choose the appropriate parameter values, which prevents errors and speeds up tasks.

As an example, the Help:addVoIPphone contains a list of phone models. The operator must choose one of these models. By using a Default Value for the model, the most appropriate phone model for a deployment can be preselected so that the operator does not have to think about finding the right model in the list.

Wizards or pages that have Default Values to set are denoted by a [D] icon in the title bar. Clicking this icon brings up the Default Values Wizard which will contain one or more parameters that you can set. The parameters have a name and value (and description if you hover over the value). Set the values to appropriate ones for a given deployment. If you leave a value blank, it generally means that no prepopulation or preselection will be performed.

The values are just text strings and you must know what the parameter expects. Future versions of IQ-Core Software may assist in the selection of values for using as defaults.



Occasionally, a Default Values is shared between wizards so that setting the value in one wizard will also set it in another. These will be denoted as such in the help documentation for the wizard.

Change Device Wizard

This wizard allows you to change how IQ-Core manages a device. You can change management IP address, SSH/SNMP credentials, and other device management parameters. Note that this wizard does NOT change the configuration of the device itself.

> Some devices have unique configuration needs in order for IQ-Core Software to properly manage them. See the main ConfigurationHelp page for configuration assistance.

Related

Manage Devices Page
AddDeviceWizard
deviceRemove
SSHConfiguration
SNMPConfiguration
ConfigurationHelp

Device Identification

Name
Enter a brief, descriptive name for the device. This will identify the device in all user interface views.

Alias
Enter an optional alias for the device. If provided, then certain views may display this value instead of the Name.

Description
Enter an optional description for the purpose/function of the device.

Make
This was set on device addition and cannot be changed.

Type
This was set on device addition and cannot be changed.

Assign Addresses

Management IP/Host
IQ-Core will communcicate with this device via this IP address or host name. If you enter a host name, the IP address must be set up through DNS or the hosts file on the IQ-Core Server. Note that network devices often have multiple IP addresses and VLANS associated with them. Select the one configured for management use.

Alternate IP/Host
Network devices are often configured to send syslog messages or use alternate IP addresses for some functions. If you enter these here, IQ-Core will use them to show the appropriate descriptive name/description (entered above) when it sees one of these IP addresses. This is optional.

CLI Connection Type

SSH
SSH is the primary mode in which IQ-Core communicates with devices. IQ-Core Server will keep one or more persistent SSH connections to the device to monitor and configure the device. You will rarely need to change the port and SSH version, but can do so if they differ from the defaults.

Telnet
Telnet is an insecure (clear text) way to communicate with devices. You should not normally use this connection type, but it is available for older devices or for troubleshooting when SSH is not available. You will rarely need to change the Telnet port but can do so if it differs from the default.

Terminal Server
For some device types, IQ-Core supports managing the device through a terminal server. The only terminal server currently supported is the MRV. The wizard will display any currently managed terminal servers and the available ports on them. Select the terminal server and the serial port that your device is connected to.

> If you need to manage a device through a terminal server, it must first be managed by IQ-Core so that it will show up in the options here.

Serial
With some device types, a serial port is the only way IQ-Core can communicate with the device. Set the serial port parameters as needed for this connection. They must match EXACTLY what the device is using for communication to work correctly.

CLI Connection Credentials

Network devices using SSH or Telnet require credentials. The main credential is a username and password. Many devices have a secondary 'Privileged' credential (enable mode) that IQ-Core also needs so that it can properly manage the device. See SSHConfiguration for more information.

> Many username/password boxes in IQ-Core have the ability to be quickly pre-populated with cached values (like a 'password vault' application). These are called 'Named Credentials'. You can enter these once and then quickly use them without having to re-enter them. Look for the icon next to a username or password box. See namedCredentialsWizard for more information.

CLI Credential
Enter the username and password that IQ-Core should use for the CLI (SSH/Telnet/Serial) connection. If your device is configured to authenticate via a RADIUS or TACACS server, check the 'User is authenticated from a server' box. If you are unsure, just leave the box unchecked.

Privilege Credential
This is the 'enable' password that many network devices use as a secondary protection mechanism. It is required so that IQ-Core features work correctly.

SNMP Connection

While IQ-Core uses a device CLI as it's primary management connection, there are some features that use SNMP. You can set up that connection here.

Enable SNMP Querying
Check this box to have IQ-Core manage the device with SNMP.

SNMP Version
SNMPv3 is the only secure version of SNMP. Use SNMP v2 or v1 only if your device does not support SNMPv3.

SNMPv2 Port/Community
If you select SNMPv1 or SNMPv2, enter the SNMP port and community string that matches what the device is using. You should rarely need to change the default port.

SNMPv3 Port
If you select SNMPv3, enter the SNMP port that matches what the device is using. You should rarely need to change the default port.

SNMP Credentials

While IQ-Core uses a device CLI as it's primary management connection, there are some features that use SNMP. See SNMPConfiguration for more information.

Authentication Protocol
Select 'SHA' or 'MD5'. MD5 is not sufficiently secure so you should select 'SHA' if at all possible. This must match the device configuration.

SNMPv3 User Credential
Enter the username and password that IQ-Core should use for SNMP authentication.

Privacy Protocol
Secure SNMPv3 requires an encrypted communication channel. Select the encryption protocol that matches the device configuration.

SNMPv3 Privacy Credential
Enter the password that will be used to encrypt/decrypt SNMP data with the device. This must match the device configuration.

Browser Application Settings

The Manage Devices Page has a **Web GUI** button that will bring up a web browser and navigate to the device's native web application. Note that if you are using the IQ-Core Client on a remote machine, you will need a routable path between the machine and the actual device.

> For many devices, these settings are in the 'Advanced Settings' at the end of the wizard.

Enable browser application
If left unchecked, IQ-Core will not display a 'Web GUI' button for the device in the Manage Devices Page. If checked, the IQ-Core Client will bring up a browser and navigate to the URL shown in the 'Preview' text.

Enter components/complete address
Normally you will only need to change the protocol or URL path and IQ-Core will construct the correct URL from the available information. But you can also enter a full URL if you would like to point to a different IP address or host.

Protocol
Select http or https.

Port
Change the port by checking the 'Custom' box and entering a new value. Most HTTP sites use port 80. Most HTTPS sites use port 443. But some devices will use a different port.

Host
Change the IP address or host name by checking the 'Custom' box and entering a new value. The value defaults to the current management IP address or hostname of the device and should rarely need to be changed.

Path
Leave blank for a default path or enter the path to the page that you want the 'Web GUI' button to take you to.

Preview
Shows the complete URL address that IQ-Core will use when the operator clicks the 'Web GUI' button.

Advanced Settings
Check the 'Show Advanced Settings' box to see settings that don't normally need to be changed.

Version Comparison
IQ-Core can audit the firmware/OS versions on the devices it manages. If enabled, IQ-Core will display a device state (DeviceStates) that indicates whether the device is in compliance with an expected firmware/OS version.

Comparison
Use 'Exact Match' if the device firmware/OS version string should match exactly what the 'Target String' specifies. Use 'Greater Than Or Equals' if the device firmware/OS version needs to meet a minumum version target.

Target
Enter a version string that IQ-Core will use to compare against the firmware/OS version that it obtains from the device.

Ping Check
IQ-Core normally uses ICMP pings as a basic check of device status (whether a device is up or down). Some devices may have ICMP turned off for security reasons so you can instruct IQ-Core to not try and ping the device as a check of device up or down status.

Addresses
Select one or more addresses to turn on/off ICMP ping checks.

Timeout
IQ-Core will allow ample time for an ICMP ping check to succeed. You can alter this time for slow links where it is known that latency will affect how long the check can take.

CLI Settings

Pool Limit
When IQ-Core is managing the device via SSH or Telnet, it will use multiple connections to increase performance. You can set how many connections should be allowed.

Privilege Command
Some devices use special 'enable' commands to enter privileged mode depending on how they are configured. The command that IQ-Core uses can be set here.

SNMP Traps

IQ-Core can receive SNMP traps from devices. When received, they are presented with all other Syslog and internal events in the user interface. If the device supports sending syslog messages, then traps are not often necessary (they will be duplicates of syslogs). But some devices use traps as their primary notification method.

SNMP Trap Version
Select the version that the device is configured with.

SNMP Trap Credentials

Authentication Protocol
Select 'SHA' or 'MD5'. MD5 is not sufficiently secure so you should select 'SHA' if at all possible. This must match what the device is configured for.

SNMPv3 User Credential
Enter the username and password that IQ-Core should use to communicate with SNMP traps.

Privacy Protocol
Secure SNMPv3 requires an encrypted communication channel. Select the protocol that matches what your device is configured for.

SNMPv3 Privacy Credential
Enter the password that will be used to decrypt SNMP traps coming from the device. This much match what the device is configured for.

Manage Devices Page

This is the main entry to device-specific information and control and is accessible by clicking the main **Devices** icon on the left side of the user interface. The page has a listing of all the basic device information and for more detailed information and interaction with the device. Common device actions are also presented on the main toolbar.

You can add and remove devices on this page with the **Device** button on the main toolbar.

When IQ-Core is first installed, go to the **System/Profiles and Snaphots** menu and use the Apply Profile Wizard or Import IQ-Core Snapshot Wizard to quickly set up management of devices.

Related

DeviceTabs
AddDeviceWizard
Apply Profile Wizard

Top View

Each device in the list has it's colored health indicator with name and primary management IP address. The currently selected device has device-specific Tabs in the Bottom View, and basic device information shown on the right. This information includes:

Make
The vendor of the device. This is static and set up when the device is added.

Model
The model string for the device. This is obtained directly from the device. For some devices, the model string may contain multiple pieces of information.

Version
The primary version of the firmware/software obtained directly from the device.

Serial
The primary serial number of the device obtained directly from the device.

Startup Type
Will be 'Automatic' if IQ-Core should start this device when the IQ-Core Service starts. Will be 'Manual' if IQ-Core put the device in 'Stop' mode but still show the device in the UI. Will be 'Disabled' if IQ-Core should do nothing with the device, including not showing it in the user interface. See for more information.

Network
Shows all the network interfaces used for IQ-Core management including the primary MAC address. For devices that are using a host name, both name and resolved IP address will be shown here.

Tool Bar

The toolbar contains buttons that modify the device list or act on the currently selected device.

Device

Add
Opens the AddDeviceWizard to add a new device to the list. IQ-Core will start managing this device after addition.

Change
Opens the Change Device Wizard to change information about the currently selected device. This includes device name, IP addresses, and passwords.

Remove
Opens the deviceRemove to confirm deletion of the device from the system.

Add UAC
Opens the AddUserSwitchWizard to add or remove user access case switches.

Monitor
Quick access to change how IQ-Core is managing the device. To fully control device management, use the menu item.

Start
Starts management of the device.

Restart

Attempts to stop management of the device, followed by a start.

Stop
Stops management of the device. The device will remain in the user interface with a gray icon.

Disable
Disables management of the device. This is the same as 'Stop', but the device will NOT remain in the user interface and can only be re-enabled by the menu item.

Wizard
Opens the changeInternalRunState for full control over device monitoring.

Reset
Opens the ResetDeviceWizard to confirm you want to reset or reinitialize the actual device. This will normally cause the device to go offline temporarily while it reloads it's configuration. Thus, the device indicator will likely be red for a while.

Terminal
Opens the TerminalWindow and opens a CLI session to the device. This is the same as using the TerminalTab but the session is in it's own window.

Web GUI
For devices that are managed primarily through a web interface, this button gives you a quick way to open that GUI. This button will not appear for devices with no web interface. You can control whether this button appears and which URL the browser will navigate to through the Change Device Wizard.

Password
Opens the changeDevicePassword which allows you to quickly change passwords on the actual device. This feature may not be available for all devices.

Ping From
Opens the ping so that you can ping from the device to any other device (sometimes called a proxy ping).

Shut Down
Some devices are complex enough that they require a proper shutdown to avoid problems associated with 'pulling the plug'. This opens the shutDown to instruct the device to shut down and power off.

SNMP

Enable SNMP
SNMPv3 configuration on certain devices can be complex. To aid this process IQ-Core provides the enableSNMP for some device types. This wizard is only for convenience to help configure SNMPv3 on a device when no such configuration currently exists.

Restart Collectors
IQ-Core collects some data like interface bandwidth via SNMP. There are times when you may be instructed to restart the collectors to sync them up to new SNMP configuration on a device.

Links
Quick access to device-specific links. You can create your own links associated with a device in the linkMenu. For example, a default link will open the CLI access application PuTTY to connect to the device.

Bottom View

A list of tabs with device-specific functionality. See DeviceTabs for help with each tab. You can resize this bottom view with the horizontal dark sizer bar.

Export IQ-Core Snapshot Wizard

This wizard compresses and encrypts all of the current IQ-Core configuration, then downloads to a client location. This snapshot can then be saved offline for later importing using the Import IQ-Core Snapshot Wizard.

This wizard will save all the IQ-Core configuration including the device list, device ip addresses, and device credentials. If you import the saved snapshot on another IQ-Core instance, it will be configured identically to the exported system.

Parameters

Save To
Choose a location and filename for the exported snapshot.

Passphrase
Enter the key that will be used to encrypt the snapshot contents. IQ-Core does not currently enforce any complexity rules on this passphrase but you should follow standard password best practices.

> ⚠ This passphrase must be entered by an operator using the Import IQ-Core Snapshot Wizard. There is no other way to access the contents of the backup.

Confirm Passphrase
Re-enter the passphrase to ensure you typed it correctly.

Import IQ-Core Snapshot Wizard

This wizard takes a previously exported snapshot (from the Export IQ-Core Snapshot Wizard), replaces the existing IQ-Core configuration with it, and restarts IQ-Core Server to start using the new configuration. This includes information about the device list, device ip addresses, and device credentials.

> ⚠ The entire IQ-Core configuration will be replaced, including device list, IP addresses, and credentials (with a couple possible exceptions described below). There is no way to undo this operation.

Parameters

Snapshot File
Choose the previously exported snapshot that you want to import.

Passphrase
Enter the key that will be used to encrypt the snapshot contents. IQ-Core does not currently enforce any complexity rules on this passphrase but you should follow standard password best practices.

> ⚠ This passphrase must be **EXACTLY** as entered in the Export IQ-Core Snapshot Wizard. There is no other way to access the contents of the backup.

Merge all security information
IQ-Core Server has a roles-based system that keeps track of the users who are allowed to log into IQ-Core, and the features that they are allowed access to. By default (the box is checked), the import will merge all existing users, roles, and directory services with those in the snapshot. If the box is unchecked, the import will merge only the *currently logged in* user and roles with those that are imported.

Keep current IQ-Core service credentials
There are a couple service credentials that are stored in the IQ-Core configuration including the credentials for the IQ-Core service itself. Normally you will want to leave these credentials alone as they are more up-to-date than those stored with the snapshot. You can overwrite the current credentials by unchecking the box.

Clear cached SNMP engine ids
When you are importing an IQ-Core snapshot onto a **different** system than the snapshot was taken on (different devices), you will get SNMP engine identification errors because IQ-Core is caching those identifiers for security reasons. Leave this box checked to clear these values on import. This will force IQ-Core to retrieve the engine identifiers again, avoiding the error but keeping the SNMP communications secure. It's OK to leave this checked even if the import is on the same system the export was taken.

Configuring the NMS Endpoint

Overview

There are four parts to the NMS configuration process: 1. Add the certificate you are going to use for secure communication between the NMS and IQ-Core Server to the personal certificate store on the computer hosting the IQ-Core Service. 2. Import the certificate into the IQ-Core service. 3. Enable the IQ-Core web server. 4. Update the network configuration of the computer hosting the IQ-Core Service.

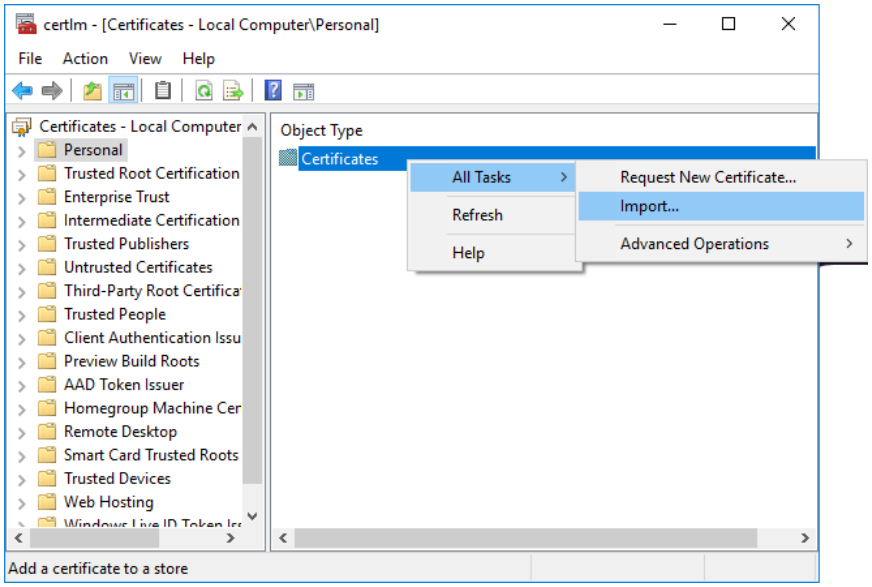
Before You Begin

To complete this setup you will need the certificate with its private key that will be used for secure communication between the NMS and the IQ-Core Service.

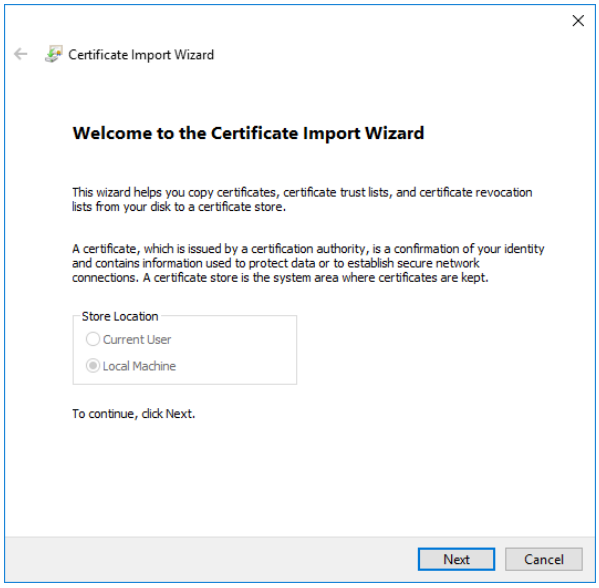
Part 1: - Add the Certificate to the Windows Certificate Store

1. Open the **Manage Computer Certificates** administrative tool. Verify that the title bar of the window you just opened shows that you are working with certificates for the Local Computer, not for the currently logged in user.

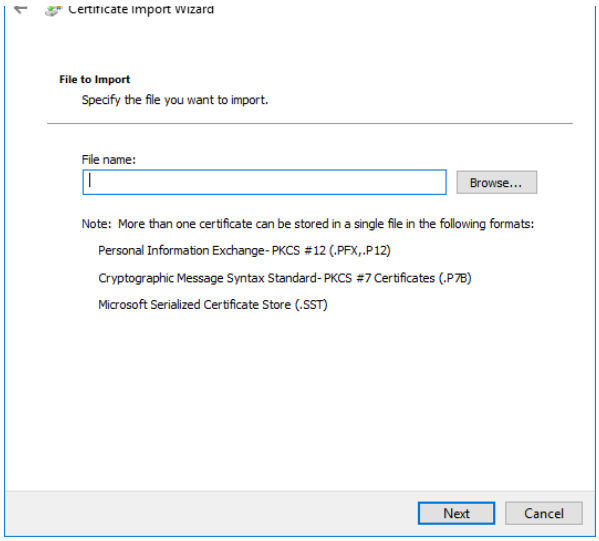
2. Select the **Personal** store then right click on **Certificates** then **All Tasks** and finally **Import**.



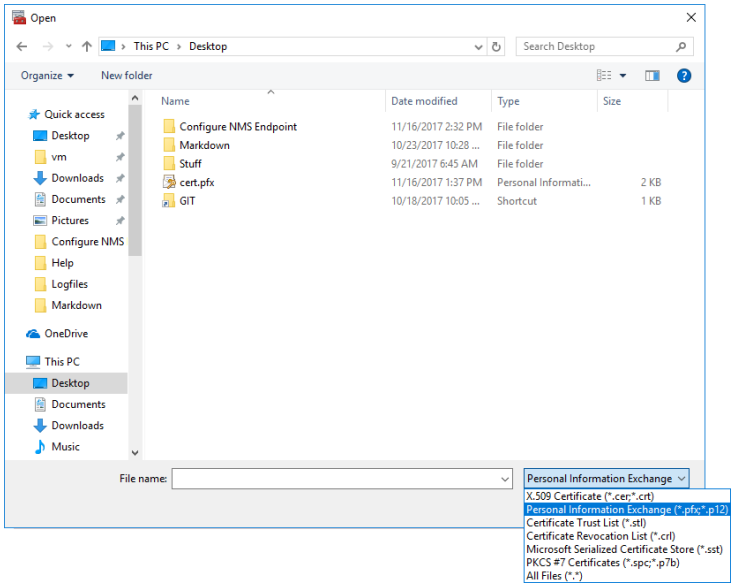
3. This opens the **Certificate Import Wizard**. Again, verify that the **Store Location** is the local computer.



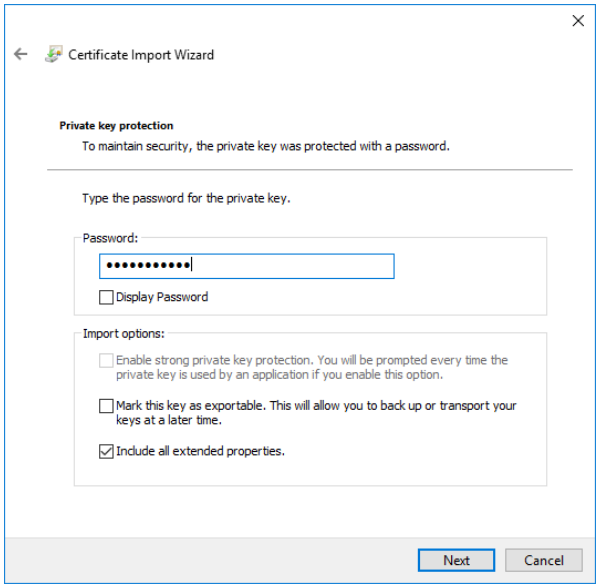
4. Browse to the certificate you want to secure NMS/IQ-Core communications.



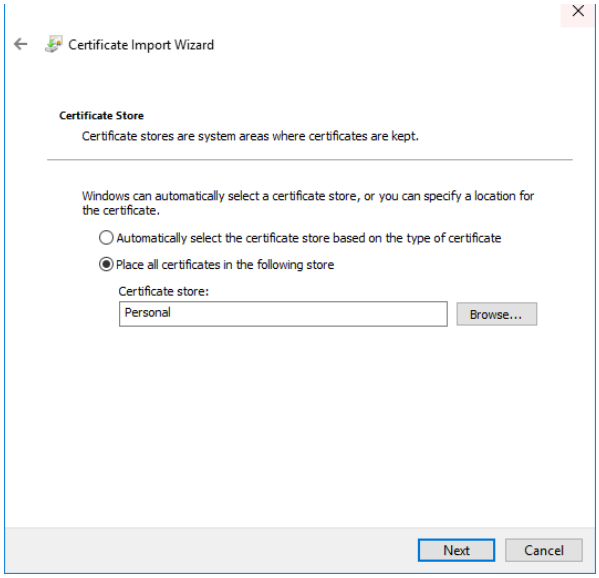
5. If you do not see the certificate listed in the Open File dialog, make sure the file type is set for the type of certificate you are importing (.pfx or .p12).



6. Once you select a certificate, click **Next** and enter the certificate password.



7. Click **Next** and insure the certificate is placed in the **Personal** store on the local computer.

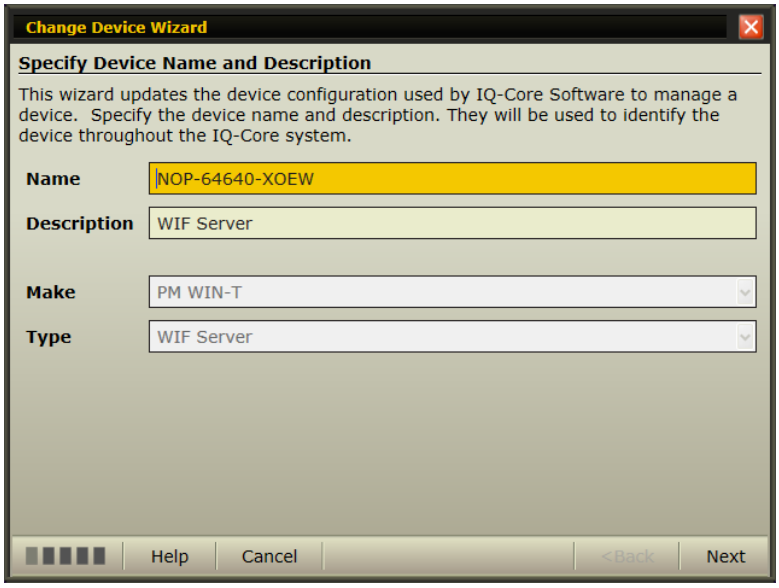


8. Click **Next** then **Finish** to complete the import.

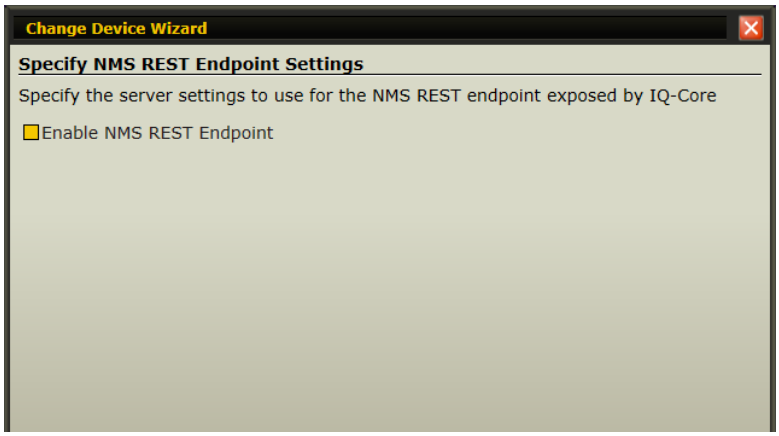
Part 2 - Import the Certificate into IQ-Core

1. Select the NMS device, from which this system will receive CommGoals, from the list of managed devices in the **Devices** page.

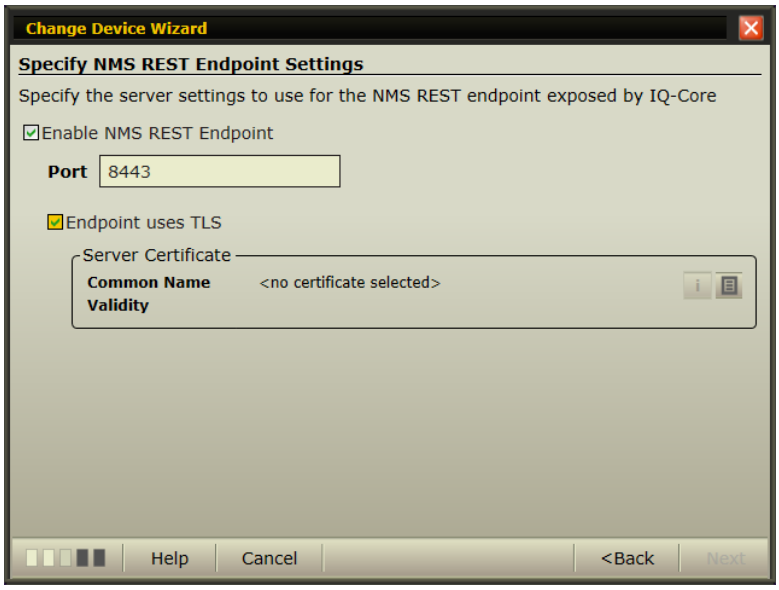
2. Next click the **Device** button in the toolbar and select **Change Device**. This opens the **Change Device Configuration Wizard**.



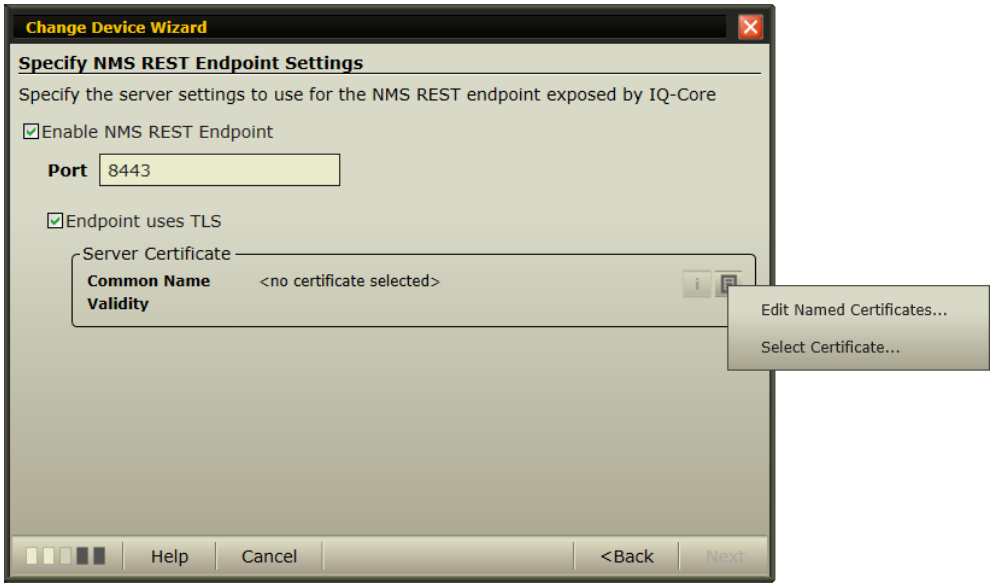
3. Page through (click the **Next** button at bottom right) until you get to the **Specify NMS REST Endpoint Settings** page.



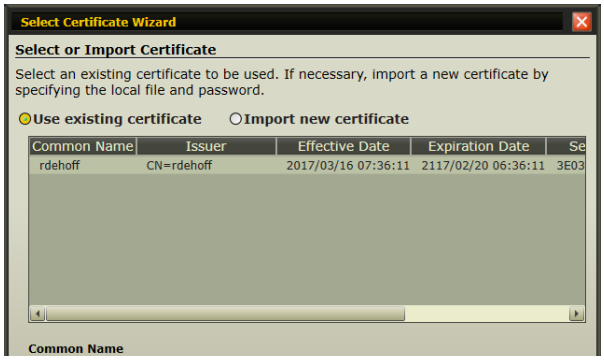
4. Check the **Enable NMS REST Endpoint** checkbox. This will show the **Port** setting and an **Endpoint uses TLS** checkbox.
5. Click the **Endpoint uses TLS checkbox**. This will show the **Server Certificate** settings.

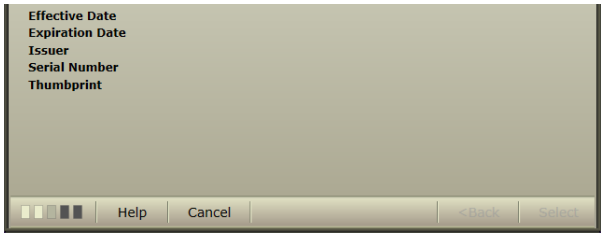


6. Click the **Certificate** button and then pick the **Select Certificate** item from the dropdown menu.



This shows the **Select Certificate Wizard**.





7. Click the **Import New Certificate** radio button and then the **Browse** button.

8. A file-open dialog will open. Browse to your certificate (a file with a .pfx or .p12 extension) and select it.
9. Fill in the certificate password and then click the **Import and Select** button at the lower left corner of the window. Click **Next** through the remaining pages and close the wizard.

Part 3 - Enable the IQ-Core Web Server

1. Select the IQ-Core server from the list of managed devices in the **Devices** page.
2. Click the **Device** button in the toolbar and select **Change Device**. This opens the **Change Device Configuration Wizard**.
3. Click Next until you get to the **Specify Web Server Settings** page and click the **Enable Web Server** checkbox. Port 80 will be selected by default.

4. Click **Next** through the remaining pages and close the wizard.

Part 4 - Update the Network Configuration of the Computer Hosting the IQ-Core Service

1. Open an elevated command prompt and navigate to the directory where the IQCore service (PacStar.IQCore.Service.exe) is located. By default this is C:\IQ-Core\Service.
2. Enter:

```
`PacStar.IQCore.Service.exe -netsh > websetup.cmd
```

This will copy a set of commands to a new file named websetup.cmd, located in the current folder.

3. Next enter:

```
`websetup.cmd > websetupResults.txt
```

which will setup and secure the NMS Rest endpoint and write the results to a file named websetupResults.txt.

Because this set of commands first attempts to remove any conflicting endpoints, you might see one or more errors in the results file if there were no existing endpoints to remove.
