OptiView Console Installation Guide

Version 6.5

Table of Contents

Introduction to the OptiView Console Application

OptiView Console Overview

The OptiView™ Console application (also referred to as "the application") provides you with the ability to monitor the performance of your network, generate reports, map your network configuration, and generate a notification if problems with your network devices arise. With the integration of OptiView Console software agents and Fluke Networks hardware agents, you can quickly and easily get detailed information about your enterprise network from your desktop.

The application is a Microsoft Windows based software tool that provides Network Supervision™ capabilities for network engineers, LAN administrators, and network technicians who maintain local area networks. By deploying software agents or Fluke Networks OptiView™ analyzers acting as hardware agents on the broadcast domains of your network, the application allows you to monitor your complete network, generate network configuration maps and performance reports, and troubleshoot LAN segments that may consist of servers, routers, switches, printers, managed hubs, and clients (hosts and other network devices). You can also use the application to monitor and control Fluke Networks diagnostic tools (such as an OptiView™ analyzer or OneTouch™ Series II network assistant) that may be located on your network.

Prior to beginning the installation and configuration of the OptiView Console application, you should read and understand the document *Using OptiView Console – Usage and Deployment Guide* that is available on the Fluke Networks OptiView Console web site (http://www.flukenetworks.com/optiviewconsole) under **Literature**. This document discusses important issues regarding the size of the network being monitored, PC disk space, memory, and processor speed requirements, network bandwidth consumed by the application, and configuration issues relating to the master and remote software agents.

Main Components of the Application

Viewer is the main user interface of the OptiView Console application and provides the Vision into your Enterprise Network and access to all components of the application.

Service Manager allows you to configure and start the four services (**Discovery**, **Analysis**, **Import**, and **Notification**) that comprise the OptiView Console application. The four services are also referred to as the Agent.

MSDE Database is a Microsoft Desktop Engine (MSDE) SQL Server database that the Agent uses to store the information it has discovered about the network and its devices. The Viewer then displays the information from the database.

Network Maps (part of the **Viewer**) provides you with the ability to document your network configuration by drawing network diagrams using your Microsoft Visio application.

Reports (part of the **Viewer**) provides multiple reports that document the device types on your network and its performance.

SwitchTap™ Port Mirroring application (a separate application accessible from the **Viewer)** provides a convenient method of configuring mirror sessions on network switch ports, allowing you to easily monitor network traffic going through your switches.

RMON Inspector application is an optional application (accessible from the **Viewer)** that works with the OptiView Console application and allows you to run RMON measurements on your RMON enabled network devices.

Logo Tool (a separate application accessible from the **Viewer**) provides a way to substitute your own custom logo on OptiView Console application network maps.

Monitoring Your Network

Note

The Service Manager is comprised of four services (Discovery, Analysis, Import and Notification). Depending on the context, the four services are also referred to as the "Agent" .

The Discovery service discovers devices in the same local broadcast domain on which the PC that is running the service resides. The OptiView Console Viewer can display the results of data collected from multiple agents in different broadcast domains. In order to accomplish this, you need to install and run Remote Agents (hardware or software) in each broadcast domain that you want to monitor. You can direct each remote Agent to advertise itself to the master OptiView Console Viewer so that a full view of your network can be achieved.

Minimum Requirements

The minimum system requirements needed to run the application on your PC are:

Note

The requirements listed here are the minimum necessary to run the basic application on a small or medium size network. A very large network or other factors (e.g. the number of database archives stored) would require increased processing power, disk space, or system memory for acceptable performance of the application. For information on PC requirements for larger networks or other high use applications, refer to the ***Using OptiView Console – Usage and Deployment Guide*** *that is available on the OptiView Console application CD or on the Fluke Networks OptiView Console web site under Literature.*

Operating System

Any of the following:
Windows 2000 Professional SP2 or later
Windows 2000 Server SP2 or later
Windows 2000 Advanced Server SP2 or later
Windows XP Professional SP1 or later
Windows 2003 Server
Windows 2003 Advanced Server

Note

You must have administrative user privileges on the PC in order to install the application.

Operating System Languages

On any of the supported Operating Systems:

- English
- German
- Japanese
- Simplified Chinese

System RAM

384 MB

Processor

400 MHz

Browser

Windows Internet Explorer 5.00.2314.1003 or later

Disk Space

Installation Type	**System Disk** (for MSDE and swap file)	**Install Disk** (for Program and databases)	**Total Disk Space**
Complete Master	400 MB	850 MB	1250 MB
Agent Only	150 MB	100 MB	250 MB
Viewer Only	200 MB	75 MB	275 MB
Complete Remote	350 MB	175 MB	525 MB

Note

MSDE and the swap file will always be installed to the system disk and cannot be changed. However, during installation, you can select an alternate installation location for the OptiView Console program files and databases.

Network Mapping Software

Microsoft Visio® 5.0 English, Service Release 1 (SR1)

Visio® 2002 English

Microsoft Visio® 2003

Note

Visio is not included with the application. You must purchase the application separately and install it on your PC. Refer to the ***Introduction to Network Maps online*** *topic for more information on configuring Visio.*

Minimum Requirement Check

The installation program will perform a minimum requirements check to ensure that your PC meets the criteria necessary to run the application. If any of the requirements have not been met, the **Status** field will indicate **Fail**. You cannot install the application if any of the minimum requirements have not been met.

Use Remote Agents to Enhance Network Discovery

Each OptiView Console Agent discovers devices in the same local broadcast domain on which the PC that is running the agent resides. The OptiView Console Viewer can display the results of data collected from agents in different broadcast domains. The OptiView Console application supports two types of remote agents:

- **Remote Software Agents** are OptiView Console agents installed on PCs that are located on remote broadcast domains and designated as remote agents. You can install multiple remote Agents on your network and then direct each remote Agent to the IP address of the PC running the master Viewer and Agent. A remote agent will advertise itself by sending a UDP packet to the master Agent.

  Note

  If you are using DHCP to assign the IP address of the PC that is running the master Viewer/Agent and the IP address of the PC changes, then the remote Agent may no longer be "seen" by the master Agent. It is recommended that you use a static IP address for the PC that is running the master Viewer/Agent.

- **Hardware Agents** are Fluke Networks OptiView analyzers serving as remote agents to enhance network discovery. The master software Agent will discover all hardware agents in the local broadcast domain and any outside of the local broadcast domain up to N router hops away. You can specify the number of hops on the Advanced Tab of the Service Manager. In addition, you can direct an OptiView analyzer to advertise its presence on the network by entering the IP address of the master Viewer in the **OptiView Console** field of the **Security Tab** of the analyzer. This will cause the OptiView Console application to discover the analyzer on a remote broadcast domain, regardless of the number of hops specified on the **Advanced** tab.

  Notes

  Hardware Agents (OptiView analyzers) use Port 2359 to send the UDP packet. The OptiView Console application uses TCP Port 1695 to import data from hardware agents. If there is a firewall between the PC that is running the OptiView Console application and the remote hardware agent, then these ports must be open in order for the application to discover and import data from the agent.

  The discovery and import of data from a hardware agent could take a few minutes to an hour or more depending on the size of your network.

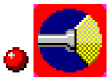
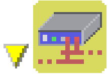
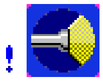
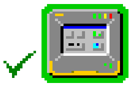
  When using remote software agents, there must be an account with administrator privileges on the PC that is running the remote agent that has the same userid and password as the logon account of the PC that is running the master agent. Refer to the topic Configure and Start a Remote Software Agent for more information.

  If you are using 8 or more hardware Agents on your network, then it may be necessary for you to install an upgraded version of SQL Server 2000. Contact Fluke Networks for assistance with determining computer specifications and which version of SQL Server 2000 you will need and for installation and configuration information.

  When you first start the Viewer, it may take up to 90 seconds to activate and display data from each hardware Agent. This is a sequential process and is designed to keep all of the hardware agents from simultaneously trying to connect to the master database.

  The Service Manager Import Service must be running to import a remote agent database.

Remote Agents will appear as separate icons in the Overview Tab of the **Viewer**. A software agent is represented by the icon and hardware agents are represented by a device icon that is representative of type of device it is (e.g. an OptiView Workgroup Analyzer hardware agent is represented as . The background color of the agent icon and the problem icon next to it gives a quick indication of the error status of the remote agent:

-  Indicates a software agent that has one or more reported error.
-  Indicates a hardware agent that has one or more reported warning.
-  Indicates a software agent that has one or more reported information notices.
- Indicates a hardware agent that has no reported errors, warnings, or information notices.

All of the application features can be used with a remote software agent database. An imported hardware agent has some limitations:

- Only one device can be trended at time and the number of ports is limited to 32.

Installation, Configuration, and Operation

Install the Application

The two main pieces of the OptiView Console application consist of the Viewer and Service Manager. After installing a master Viewer and Service Manager on a single PC, you can install any number of remote Viewers and/or Service Managers (Agents) on PCs located in remote broadcast domains on your network to monitor your complete network. You can monitor any number of devices (nodes) up to the limit as specified in the Software License agreement that you purchased with the application. You can purchase additional node licenses as needed to increase the node limit.

Note

You must purchase an additional software license to install a remote Viewer. Refer to your license agreement for more information.

The options for installing the OptiView Console application are:

- **Complete Master** - Install the Viewer and Service Manager on a PC. A master installation is required. Only one installation per software license agreement can be designated as a master.
- **Complete Remote** - Install the Viewer and Service Manager on a PC located on a different broadcast domain than the master. The first time that you run the remote Viewer, you will have to enter the IP address or computer name of the PC that is running the master Agent. The first time that you run the remote Agent, you will be prompted to enter the IP address of the PC that is running the master agent. You can change the master database that the remote Agent reports to by selecting the Remote Agent button on the **Service Tab** of the **Service Manager**.
- **Viewer Only** - Install the Viewer on a PC located on a different PC than the master. The first time that you run the remote Viewer, you will have to enter the IP address or computer name of the PC that is running the Agent whose database you want to see. You can direct the Viewer to look at different master Agent databases by selecting **Set Master Database...** from the File menu of the Viewer **Menu Bar** and entering a new IP address or computer name. You must purchase an additional software license for each remote Viewer that you install.
- **Agent Only** - Install the Service Manager on a PC located in a different broadcast domain than the master. The first time that you run the remote Agent, you will be prompted to enter the IP address of the PC that is running the master agent. You can change the master database that the remote Agent reports to by selecting the Remote Agent button on the **Service Tab** of the **Service Manager**. You may install any number of remote Agents, but you can only monitor the number of devices (nodes) up to the limit as specified in the Software License agreement that you purchased with the application. You can purchase additional node licenses as needed to increase the node limit.

  Note

  *Even though all four services will be installed in **Agent Only** installation, only the **Discovery** service will run when the **start** button is selected. The master Agent handles the tasks of analysis, notification, and import for remote Agents.*

Installing the Application

1. Select the computer on which you want to install the application. The PC that you select must meet the minimum requirements for the application.

   Notes

   The logon userid that you use for the PC must have administrator privileges in order to install the application.

   *You must remove any previous versions of OptiView Console or Fluke Networks Network Inspector application prior to installing OptiView Console. You can do this from the **Add or Remove Programs** selection on the Windows Control Panel. It is not necessary to remove the OptiView Console MSDE instance that was installed with OptiView Console 6.0.*

   While it is a good idea to back up your version 6.0 databases prior to beginning the installation, *they will be converted during the installation process to make them compatible with version 6.5.*

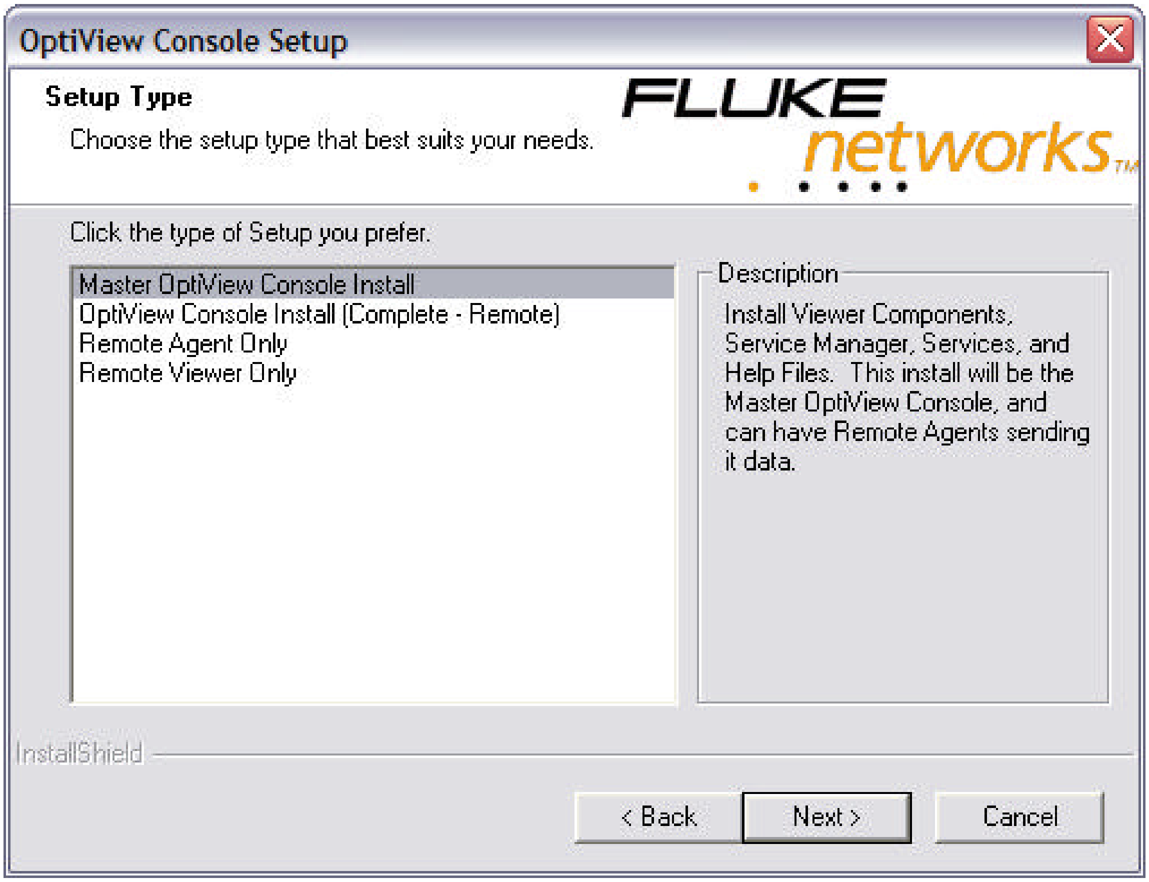
2. Verify that the **Server** service is installed and running on the PC. You can accomplish this by doing the following:
   a. From the Windows **Control Panel**, open **Administrative Tools**.
   b. Select **Services**.
   c. Verify that the **Server** service exists, is started, and that the **Startup Type** is set to **Automatic**.

Notes

*You may have to add the columns for **Startup Type** and **Status**. You can do this by selecting **View** | **Add/Remove Columns**.*

   d. If the **Server** service does not exist in the **Services** applet, install **File and Printer Sharing** by doing the following:
      i. From the Windows desktop, right-click on **My Network Places** and select **Properties**.
      ii. Double-click on network connection that is enabled in **Network Connections**.
      iii. Select **Properties** and then **Install**.
      iv. On the **Select Network Component Type** dialog select **Service** and click the **Add…** button.
      v. On the **Select Network Service** dialog select **Microsoft** under Manufacturer and select **File and Printer Sharing for Microsoft Networks** under **Network Service** and click the **OK** button.
3. If other instances of MSDE (Microsoft SQL Server Desktop Engine) are installed and running on the PC, they may cause a conflict that prevents the OptiView Console instance of MSDE from properly installing. Other applications may install their own instance of MSDE on the PC, however, there is no way to know whether the OptiView Console instance of MSDE will install and run properly with other instances on the system.

   You can check for other instances of MSDE by doing the following:
   a. From the Windows **Control Panel**, select Add/Remove Programs.
   b. Look for any entries titled **MSDE**, **Microsoft SQL Server** or **Microsoft SQL Server Desktop Engine**.
   c. If any entries with those names exist, you can either leave them and see if the OptiView Console application installs and runs correctly or you can uninstall them.
   d. Close all other programs on the PC prior to installing the OptiView Console application.
   e. Run the **Setup.exe** file found in the root directory of the OptiView Console application's CD-ROM (or double-click the self-extracting OptiViewConsoleV65.exe file, if you downloaded from the Web) and follow the instructions on your screen.
   f. When you come to the OptiView Console Setup screen, choose the Setup type that you want.



OptiView Console Setup

Setup Type

Choose the setup type that best suits your needs.

Click the type of Setup you prefer.

- Master OptiView Console Install
- OptiView Console Install (Complete - Remote)
- Remote Agent Only
- Remote Viewer Only

Description

Install Viewer Components, Service Manager, Services, and Help Files. This install will be the Master OptiView Console, and can have Remote Agents sending it data.

Note

You must remove any previous installations of the application before you can install a new one. Only one instance of the application can be installed on a single PC at any time.

4. Follow the instructions on the screen to complete the installation.
5. After you have installed the master Viewer and Agent, you can install any number of remote Agents on your network. You can then use the Viewer to access the remote Agent's database.

Configure and Start the Master Software Agent

To configure the master Agent, do the following:

1. Start the Service Manager.

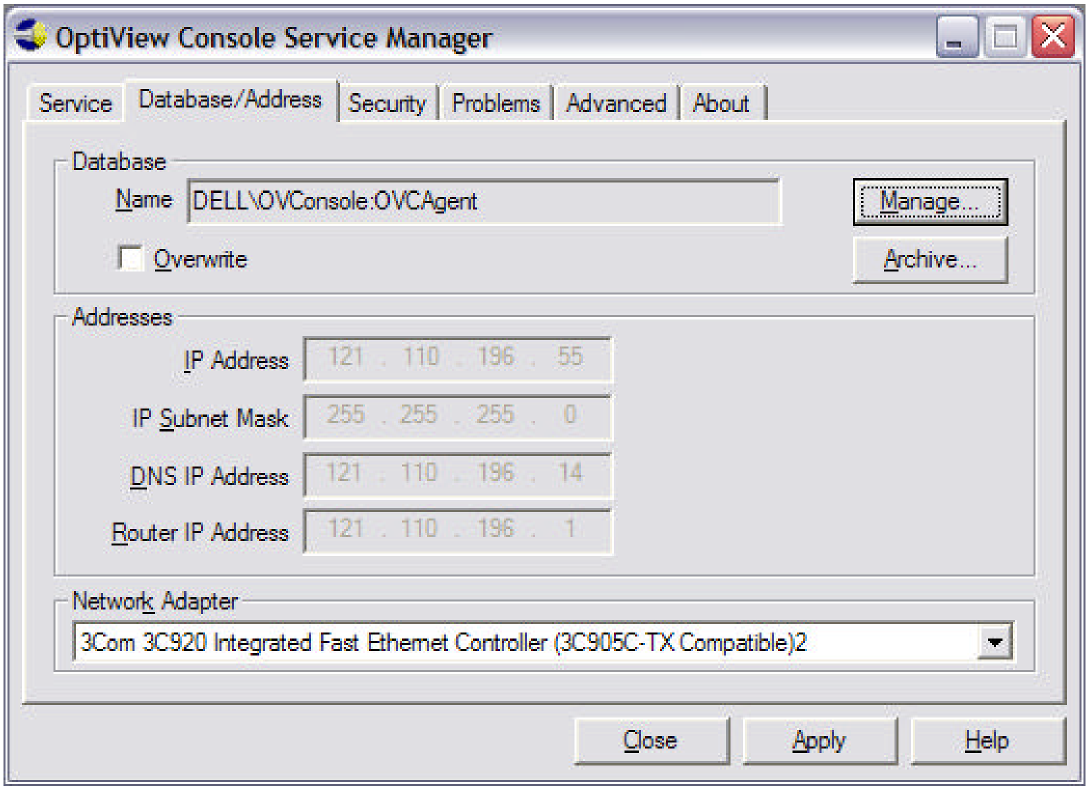
   On the computer on which you installed the Master Agent, select **Start** | **Programs** | **Fluke Networks** | **OptiView Console** (or, if you did not accept the default Program folder during installation, point to the folder that you chose) and then select **Service Manager**. Or you can select the OptiView Console Service Manager icon from your Windows desktop.
2. A dialog box labeled **OptiView Console License** opens.
3. Enter your license key and press the **Continue** button. If you are evaluating the application and wish to run in trial mode (30 days), just press the **Continue** button.

   Notes

   You can obtain your license key by registering the product at http://www.flukenetworks.com/optiviewconsoleregistration. You will need the serial number of the product in order to register it. It is located on the box and CD case.

   *Trial mode gives you all of the features of the OptiView Console application with the exception that you can only generate the **Server Connections in a Switched Network** map.*

5. The **OptiView Console Service Manager** dialog box opens. It is necessary to configure the application for your network.
6. Select the **Database/Address** tab.



Database

Name DELL\OVConsole:OVCAgent

☐ Overwrite

Addresses

IP Address 121 . 110 . 196 . 55

IP Subnet Mask 255 . 255 . 255 . 0

DNS IP Address 121 . 110 . 196 . 14

Router IP Address 121 . 110 . 196 . 1

Network Adapter

3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible)2

7. Verify that the **IP Address**, **IP Subnet Mask**, **DNS IP Address**, and **Router IP Address** are correct for the PC and broadcast domain on which the PC is located.

   With a few exceptions, you cannot change the IP settings. The OptiView Console application automatically manages (through the Microsoft TCP/IP stack) the IP Address to be the same as the IP address for the Agent's computer. The application attempts to autodetect your machine's IP configuration information; however, certain situations limit the accuracy of this autodetection.

Removal of TCP/IP, multiple NICs, moving from DHCP to fixed IP addressing (or vice-versa) may result in incorrect IP autodetection. If this happens, you must manually configure the IP for your machine in the Windows Control Panel. For more information, refer to Microsoft online help available from Windows Control Panel.

The **IP Subnet Mask** field lets you view the IP subnet mask for the Agent. You cannot change this field. The OptiView Console application automatically manages the IP subnet mask to be the same as the IP subnet mask for the Agent's computer.

The **DNS IP Address** field lets you view the IP address of the DNS server the Agent will query when it attempts to discover a device's DNS name. When possible, the OptiView Console application automatically manages the DNS IP address to be the same as the DNS IP address for the Agent's computer. You cannot change this field from the Service Manager's dialog box. If the sub-network where the Agent resides does not have a DNS server, this field will be blank, but be aware that the Agent will not be able to resolve the devices IP addresses to their DNS names.

The **Router IP Address** field lets you view the IP address of a router that is on the sub-network where the Agent's computer resides. The Agent uses that router as its default router. When possible, the OptiView Console application automatically manages the router's IP address to be the same as the default router IP address for the Agent's computer. You cannot change this field from the Service Manager's dialog box.

Note

Normally, if you have the required Microsoft TCP/IP stack properly running on your computer, you will not need to specify any of the IP addresses. However, there are some situations where you may need to specify an IP address. Refer to Microsoft online help available from Windows Control Panel (look under Network or Network Connections).

8. Make sure the **Network Adapter** field lists the proper NIC card (if there is more than one).
9. If you want the Agent to overwrite the current contents of the specified database, select the **Overwrite** check box. If you want to keep the current contents of the specified database and have the Agent use it as a baseline and just add new or changed information (append mode), make sure the **Overwrite** check box is disabled.

Caution

If you enable overwrite, any notes in the database (which you entered in the Notes tab of Device Properties) will be lost. In addition, any new devices that you manually added to the database (using the Add New… item in the Device menu) will be lost.

Note

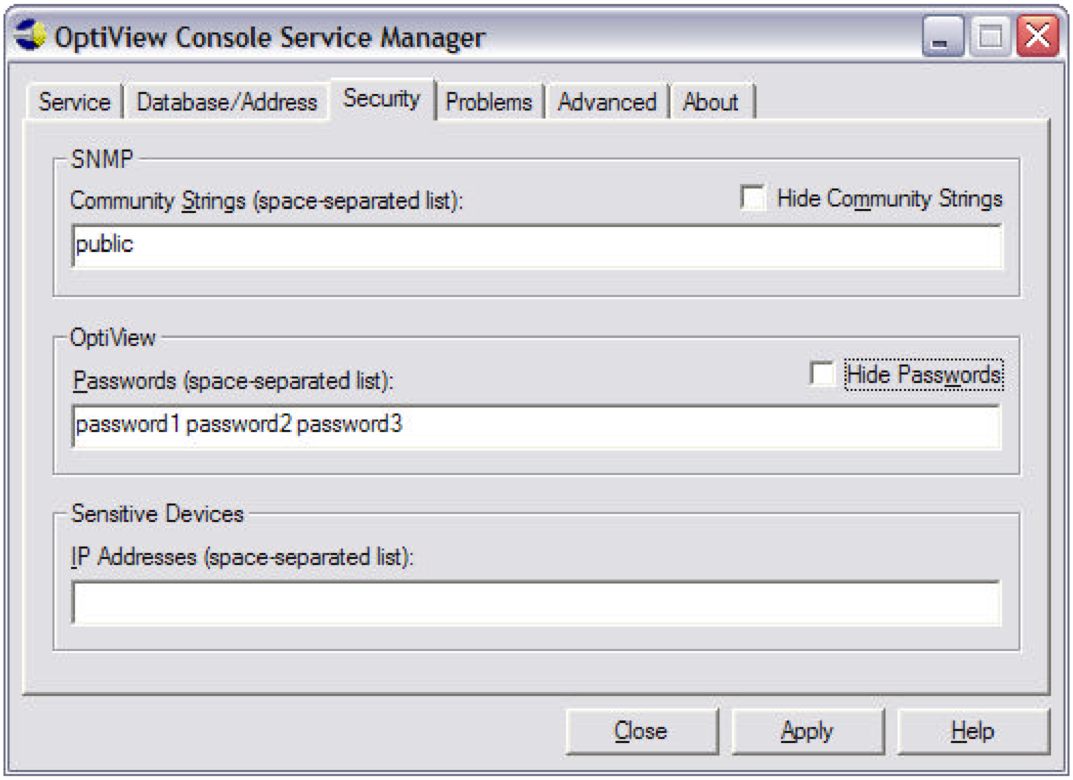
*If you are installing the application for the first time on the PC, there is no database to overwrite. If you enable **Overwrite**, the database will be overwritten each time the services are started. With **Overwrite** enabled, you will not lose information on discovered Agents, Notification settings, the Problem Log, archived databases, or the information on the **Key Devices** tab.*

10. Select the **Apply** button if you made any changes. Changes will take effect the next time the services are started.

Note

*You can wait and use the **Apply** button after you have made all of your configuration changes.*

11. Select the **Security** tab.



SNMP

Community Strings (space-separated list): public

□ Hide Community Strings

OptiView

Passwords (space-separated list): password1 password2 password3

□ Hide Passwords

Sensitive Devices

IP Addresses (space-separated list):

12. Enter SNMP community strings for your network devices. Use a space-separated list for multiple strings (e.g. string1 string2 string3).

Note

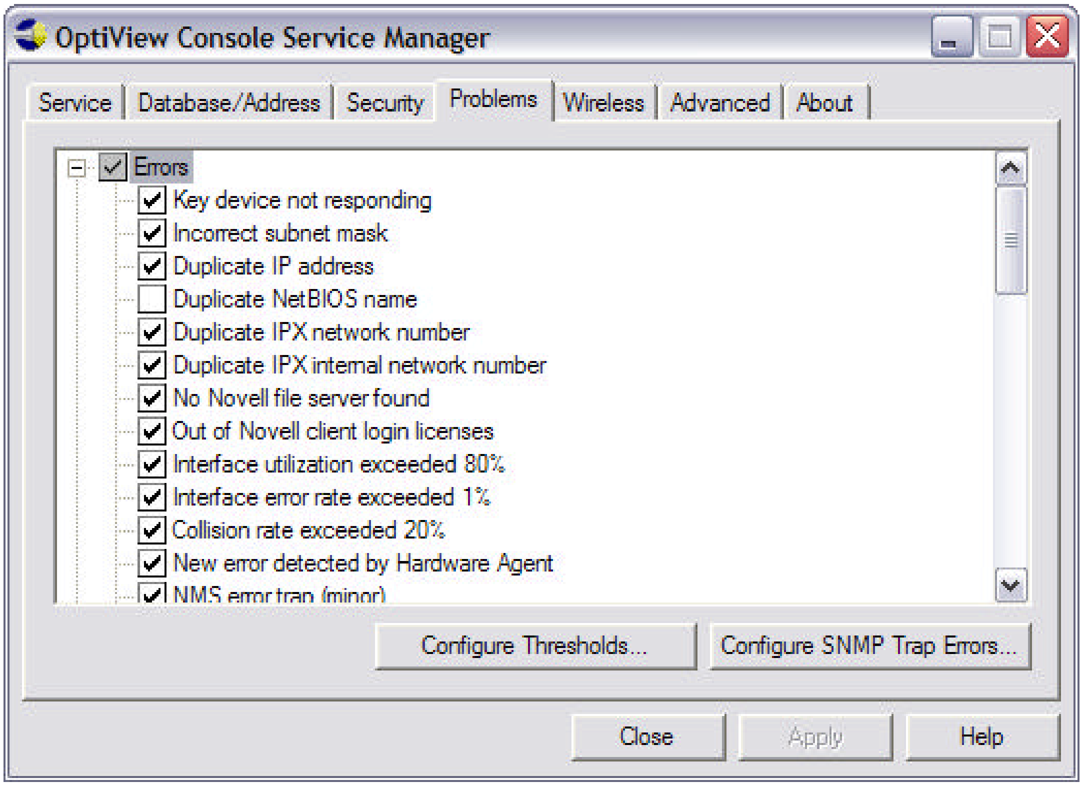
The application uses SNMP for discovery of network devices. Entering SNMP community strings for your network devices enables a more complete discovery of your network.

13. Select the **Hide Community Strings** checkbox if you want to hide the strings from view. The strings will be replaced with *****'s.
14. Enter passwords for any OptiView analyzers (that are being used as hardware agent and have their password feature enabled) on your network (s). Use a space-separated list for multiple devices.
15. Select the **Hide Passwords** checkbox to remove the passwords from view. The passwords will be replaced with *****'s.
16. Some devices are set to generate alarms if they are queried. In the **Sensitive Devices** window, enter the IP address of any device on your network that you do not want the application to use its active discovery methods on. Enter multiple IP addresses using a space-separated list. All devices designated as sensitive will not be actively queried by the application.
17. Select the **Apply** button if you made any changes. Changes will take effect the next time the services are started.

Note

*You can wait and use the **Apply** button after you have made all of your configuration changes.*

18. Select the **Problems** tab.



- ☑ Errors
  - ☑ Key device not responding
  - ☑ Incorrect subnet mask
  - ☑ Duplicate IP address
  - ☐ Duplicate NetBIOS name
  - ☑ Duplicate IPX network number
  - ☑ Duplicate IPX internal network number
  - ☑ No Novell file server found
  - ☑ Out of Novell client login licenses
  - ☑ Interface utilization exceeded 80%
  - ☑ Interface error rate exceeded 1%
  - ☑ Collision rate exceeded 20%
  - ☑ New error detected by Hardware Agent
  - ☑ NMS error trap (minor)

19. You can use this tab to select the problems (**Errors**, **Warnings**, and **Information**), which will be stored in the database and displayed in the **Problem Log**. The default selections are already entered. A white check box ☑ with a check in it means that all of the items in that category are selected and a gray check box ☑ with a check in it means that the some, but not all, of the items in that category are selected.
20. Select the **Configure Thresholds…** button to change thresholds that will generate a problem (error or warning) for **Network Utilization**, **Network Errors**, or **Collisions**.

Note

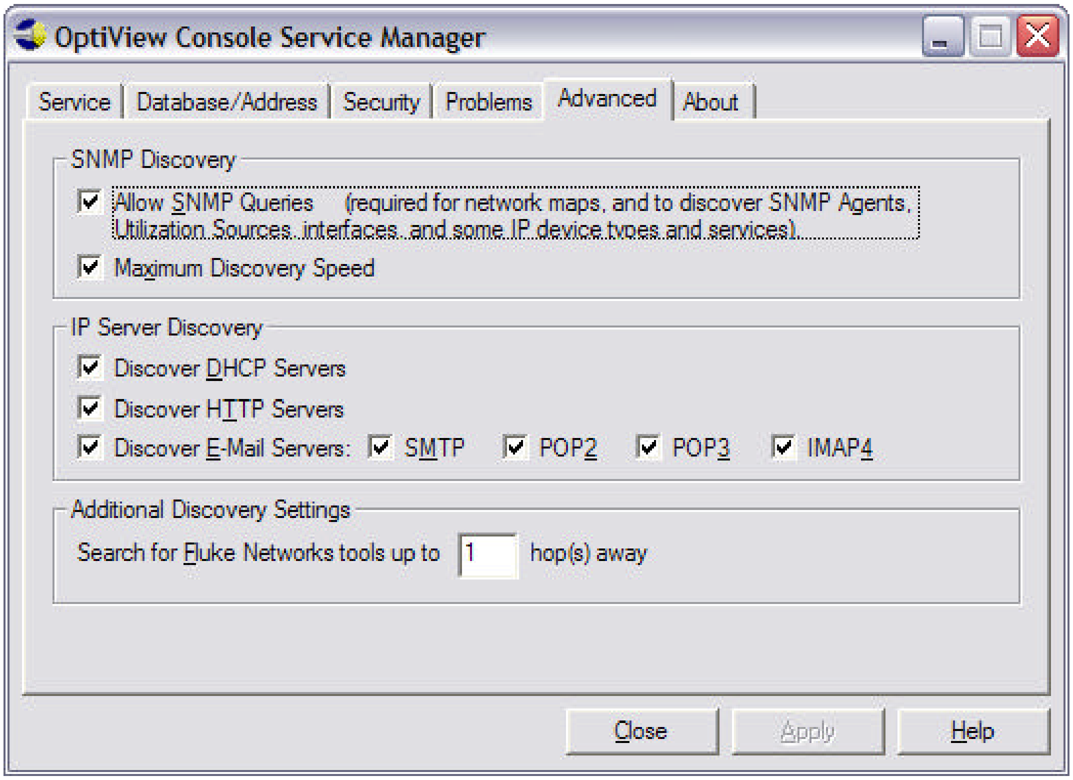
These are global thresholds for the devices discovered by the Agent. You can set individual interface thresholds. Refer to the topic Set Individual Interface Threshold Levels in the online help.

21. Select the **Configure SNMP Trap Errors** button to configure which SNMP Traps sent by other devices or Network Management Systems should be reported in the Problem Log. Refer to the topic **Configure SNMP Trap Errors** in the online help for more information on configuring SNMP traps.
22. Select the **Apply** button if you made any changes. Changes will take effect the next time the services are started.

Note

*You can wait and use the **Apply** button after you have made all of your configuration changes.*

23. Select the **Advanced** tab, where you can fine-tune the agent discovery process for your network.



SNMP Discovery

☑ Allow SNMP Queries (required for network maps, and to discover SNMP Agents, Utilization Sources, interfaces, and some IP device types and services).

☑ Maximum Discovery Speed

IP Server Discovery

☑ Discover DHCP Servers

☑ Discover HTTP Servers

☑ Discover E-Mail Servers: ☑ SMTP ☑ POP2 ☑ POP3 ☑ IMAP4

Additional Discovery Settings

Search for Fluke Networks tools up to 1 hop(s) away

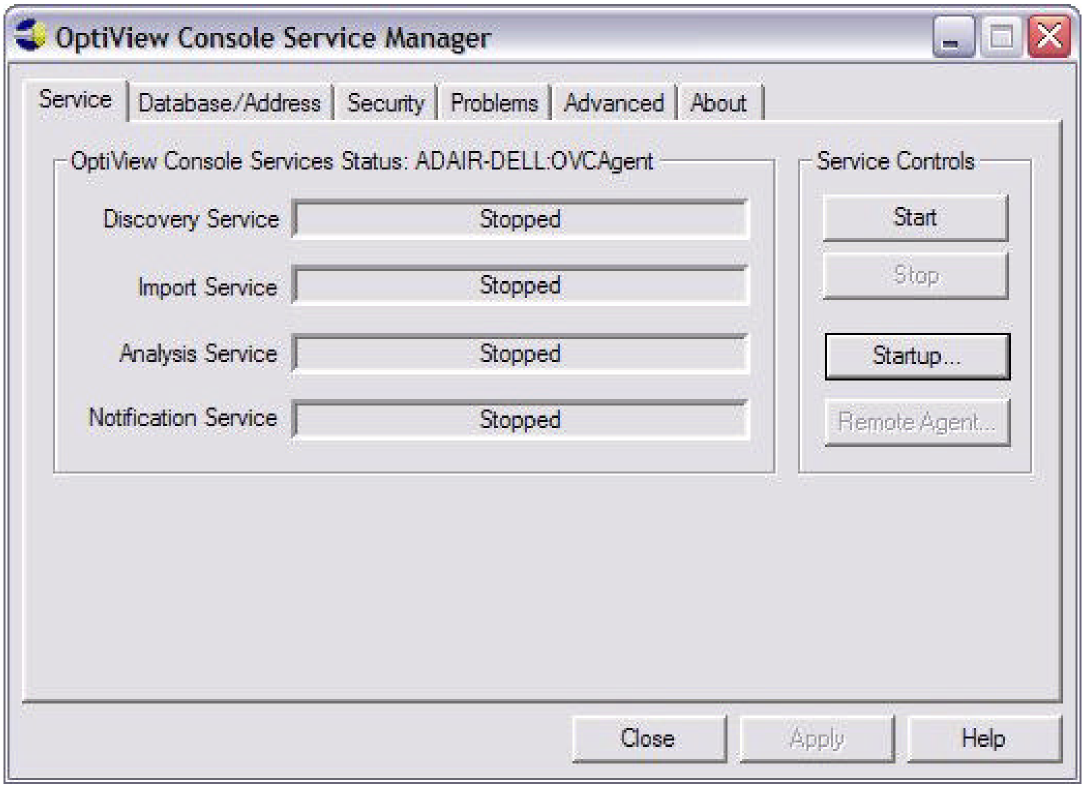
The default selections made on the **Advanced** tab are chosen to maximize the network discovery performance of the application. However, occasionally there may be a negative effect on your network performance that may cause you to need to turn one or more of these selections off. Refer to the Advanced Tab topic for more information.

24. Select the **Apply** button if you made any changes. Changes will take effect the next time the services are started.

Note

*You can wait and use the **Apply** button after you have made all of your configuration changes.*

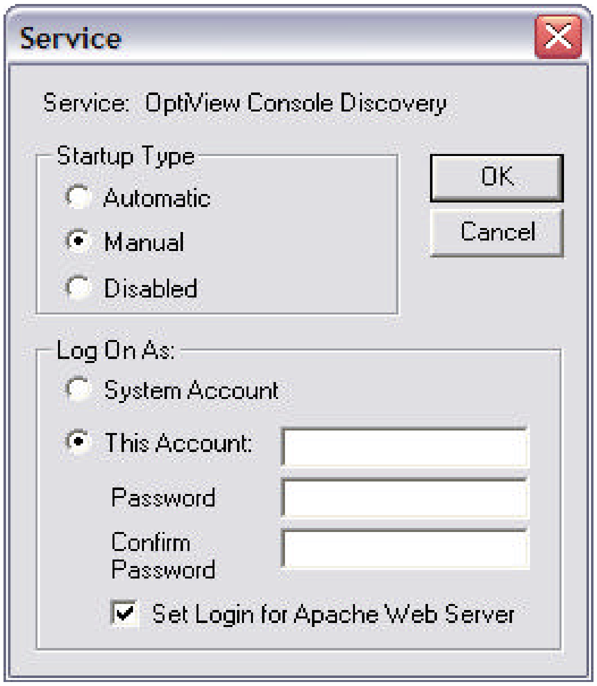
25. Select the **Service** tab.



OptiView Console Services Status: ADAIR-DELL:OVCAgent

Discovery Service	Stopped
Import Service	Stopped
Analysis Service	Stopped
Notification Service	Stopped

26. Select the **Startup…** button.
27. The Service dialog box opens:



Service: OptiView Console Discovery

Startup Type
○ Automatic
● Manual
○ Disabled

Log On As:
○ System Account
● This Account:
Password
Confirm Password
☑ Set Login for Apache Web Server

28. Select the **Automatic** radio button if you want the Agent to start automatically each time Windows is started, or select the **Manual** radio button if you prefer to start the Agent manually using the **Start** button.

Notes

*Selecting the **Automatic** radio button may add up to 30 seconds to the time it takes Windows to boot after you log in.*

*Regardless of whether you select the **Automatic** radio button or the **Manual** radio button, you can still manually start the Agent whenever you want by clicking the **Start** button. The automatic-start option merely gives you a way to ensure that if the computer reboots, the Agent will be started again automatically.*

29. Select the **This Account:** radio button and enter a valid Windows user account in the **This Account:** field of the **Log On As:** section if any of the following apply:
    - You will be using remote software Agents.
    - You are using the Agent to monitor an IPX network (required so that the Analysis service can properly determine IPX names).
    - You selected the **Automatic** startup type.

    Enter a password in the **Password** and **Confirm Password** fields.

    The Windows user account and password you enter must meet the following criteria:
    - It must have administrator privileges for the PC that is running the application.
    - It must be a valid Windows user account for the PC.
    - It must match a valid Novell account and password (if monitoring an IPX network).
30. Select **OK** to close the **Service** dialog box. Any changes made in the **Service** dialog box will take effect immediately.
31. Select the **Apply** button if you have made configuration changes on other tabs but have not yet applied the changes.
32. Select the **Start** button.
33. The services will now start.

Notes

The services can take up to 30 seconds to start.

The services will run until you click the Stop button in the Service Manager's dialog box. Because they are Windows services, closing the Service Manager's dialog box will not stop the services.

You can start the Agent and leave it running for a long time. If you do this, the Agent first creates a baseline of the network and its devices, and stores this information in the database. The Agent then continually compares the current state of the network to the baseline, and updates the database as necessary. You can then either open the Viewer and leave it open to monitor your network, or just open it when you want to check the status and close it when you are done. The Agent will continue to collect data until the services are stopped.

Configure and Start a Remote Software Agent

To configure a remote software Agent, do the following:

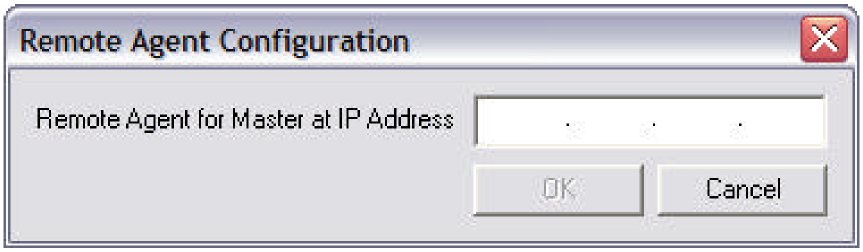
1. Start the Service Manager (remote Agent):

   On the computer on which you installed the remote Agent, select

   Start | **Programs** | **Fluke Networks** | **OptiView Console** (or, if you did not accept the default Program folder during installation, point to the folder you chose) and then select **Service Manager**. Or you can select the OptiView Console Service Manager icon from your Windows desktop.
2. A dialog box labeled **OptiView Console License** opens.
3. Enter your license key and press the **Continue** button. If you are evaluating the application and wish to run in trial mode (30 days), just press the **Continue** button.

   Note

   You can obtain your license key by registering the product at http://www.flukenetworks.com/optiviewconsoleregistration. You will need the serial number of the product in order to register it. It is located on the box and CD case.
4. The **Remote Agent Configuration** dialog box opens.



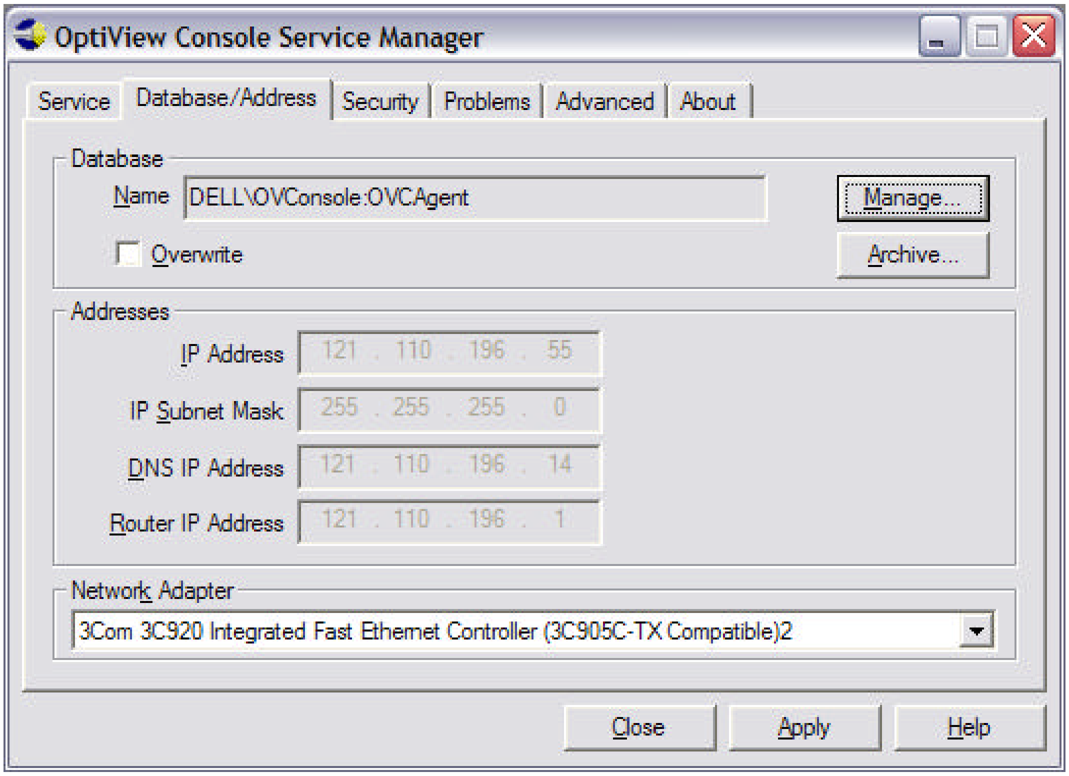
Remote Agent Configuration

Remote Agent for Master at IP Address . . .

5. Enter the IP address for the PC on which the master Viewer/Agent resides. This causes the remote agent to send a UDP packet to the master Agent, which advertises the remote Agent's presence on the network.

   Note

   If you are using DHCP to assign the IP address of the PC that is running the master Viewer/Agent and the IP address of the PC changes, then the remote Agent may no longer be "seen" by the master Agent. It is recommended that you use a static IP address for the PC that is running the master Viewer/Agent.
6. The OptiView Console Service Manager dialog box opens. It is necessary to configure the application for your network.
7. Select the **Database/Address** tab.



Database

Name DELL\OVConsole:OVCAgent

□ Overwrite

Addresses

IP Address 121 . 110 . 196 . 55

IP Subnet Mask 255 . 255 . 255 . 0

DNS IP Address 121 . 110 . 196 . 14

Router IP Address 121 . 110 . 196 . 1

Network Adapter

3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible)2

8. Verify that the **IP Address**, **IP Subnet Mask**, **DNS IP Address**, and **Router IP Address** are correct for the PC and broadcast domain on which the PC is located.

   With a few exceptions, you cannot (nor is it necessary) change the IP settings. The OptiView Console application automatically manages (through the Microsoft TCP/IP stack) the IP Address to be the same as the IP address for the Agent's computer. The application attempts to autodetect your machine's IP configuration information; however, certain situations limit the accuracy of this autodetection. Removal of TCP/IP, multiple NICs, moving from DHCP to fixed IP addressing (or vice-versa) may result in incorrect IP autodetection. If this happens, you must manually configure the IP for your machine in the Windows Control Panel. For more information on configuring your machine's IP settings, refer to Microsoft online help available from Windows Control Panel.

   The **IP Subnet Mask** field lets you view the IP subnet mask for the Agent. You cannot change this field. The OptiView Console application automatically manages the IP subnet mask to be the same as the IP subnet mask for the Agent's computer.

   The **DNS IP Address** field lets you view the IP address of the DNS server the Agent will query when it attempts to discover a device's DNS name. When possible, the OptiView Console application automatically manages the DNS IP address to be the same as the DNS IP address for the Agent's computer. You cannot change this field from the Service Manager's dialog box. If the sub-network where the Agent resides does not have a DNS server, this field will be blank, but be aware that the Agent will not be able to resolve the devices IP addresses to their DNS names.

   The **Router IP Address** field lets you view the IP address of a router that is on the sub-network where the Agent's computer resides. The Agent uses that router as its default router. When possible, the OptiView Console application automatically manages the router's IP address to be the same as the default router IP address for the Agent's computer.

Note

Normally, if you have the required Microsoft TCP/IP stack properly running on your computer, you will not need to specify any of the IP addresses. However, there are some situations where you may need to specify an IP address. Refer to Microsoft online help available from Windows Control Panel (look under Network or Network Connections).

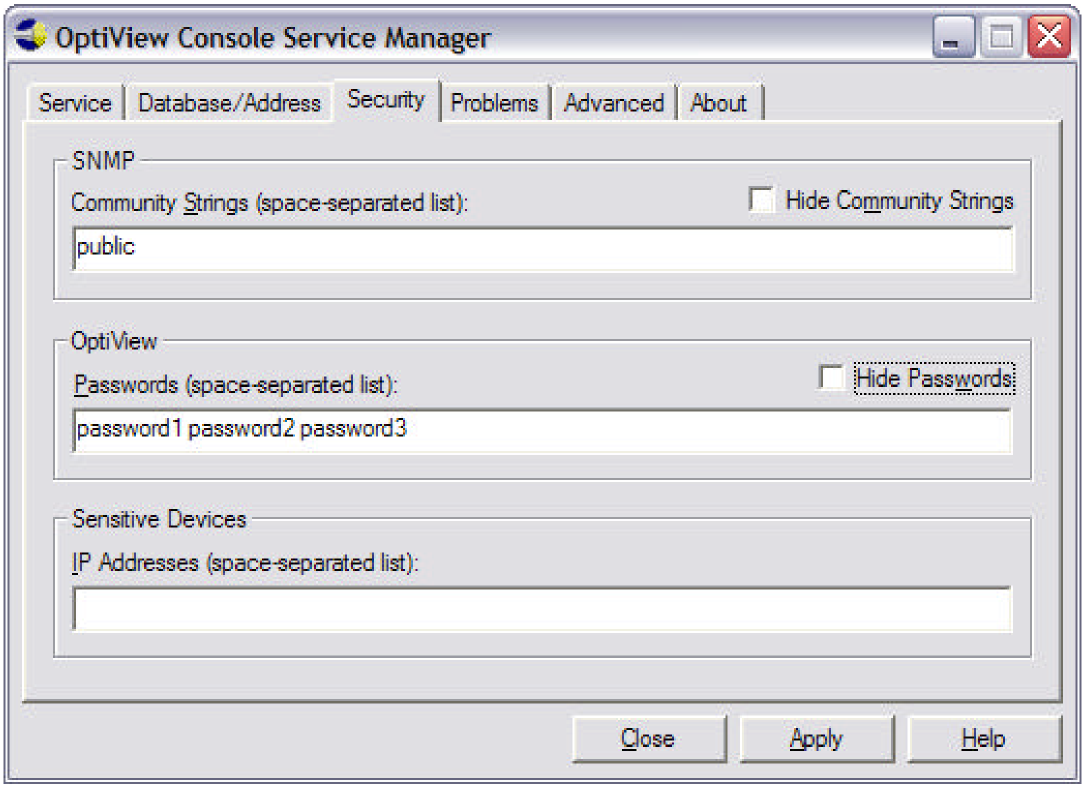
9. Make sure the **Network Adapter** field lists the proper NIC card (if there is more than one).
10. If you want the Agent to overwrite the current contents of the specified database, select the

Overwrite check box. If you enable **Overwrite**, the agent database will be overwritten each time the services are started. With **Overwrite** enabled, you will not lose information on discovered Agents, Notification settings, the Problem Log, archived databases, or the information on the **Key Devices** tab. If you want to keep the current contents of the specified database and have the Agent use it as a baseline and just add new or changed information (append mode), make sure the **Overwrite** check box is disabled.

Caution

If you enable overwrite, any notes in the database (which you entered in the Notes tab of Device Properties) will be lost. In addition, any new devices that you manually added to the database (using the Add New… item in the Device menu) will be lost.

11. Select the **Security** tab.



Community Strings (space-separated list): public

□ Hide Community Strings

Passwords (space-separated list): password1 password2 password3

□ Hide Passwords

IP Addresses (space-separated list):

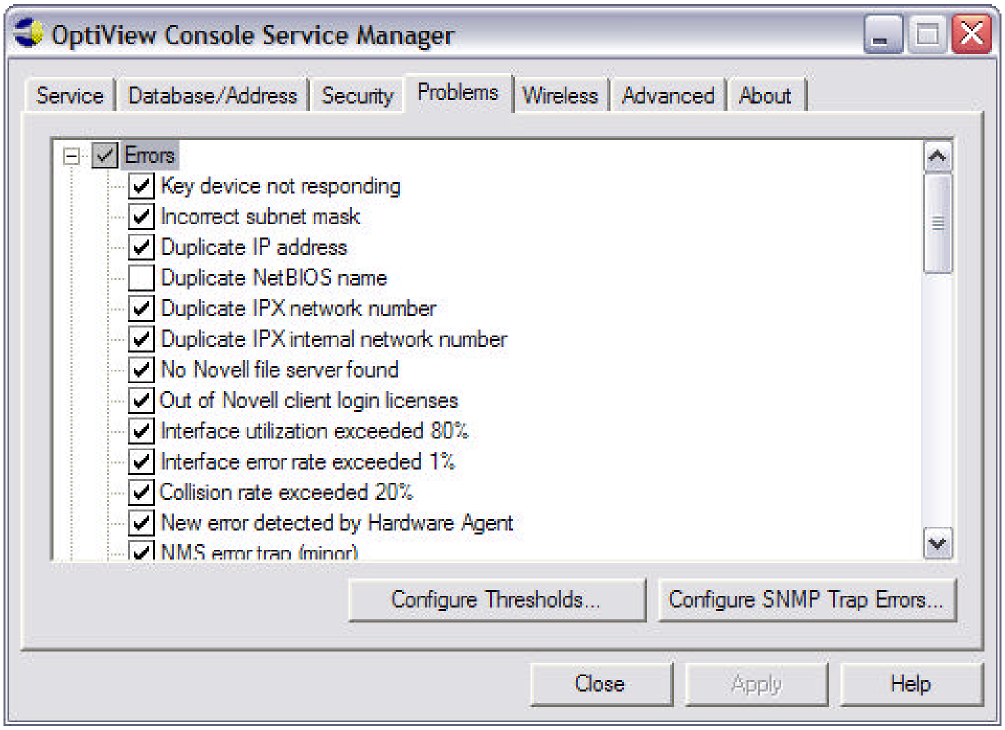
12. Enter SNMP community strings for your network devices. Use a space-separated list for multiple strings (e.g. string1 string2 string3).

Note

The application uses SNMP for discovery of network devices. Entering SNMP community strings for your network devices enables a more complete discovery of your network.

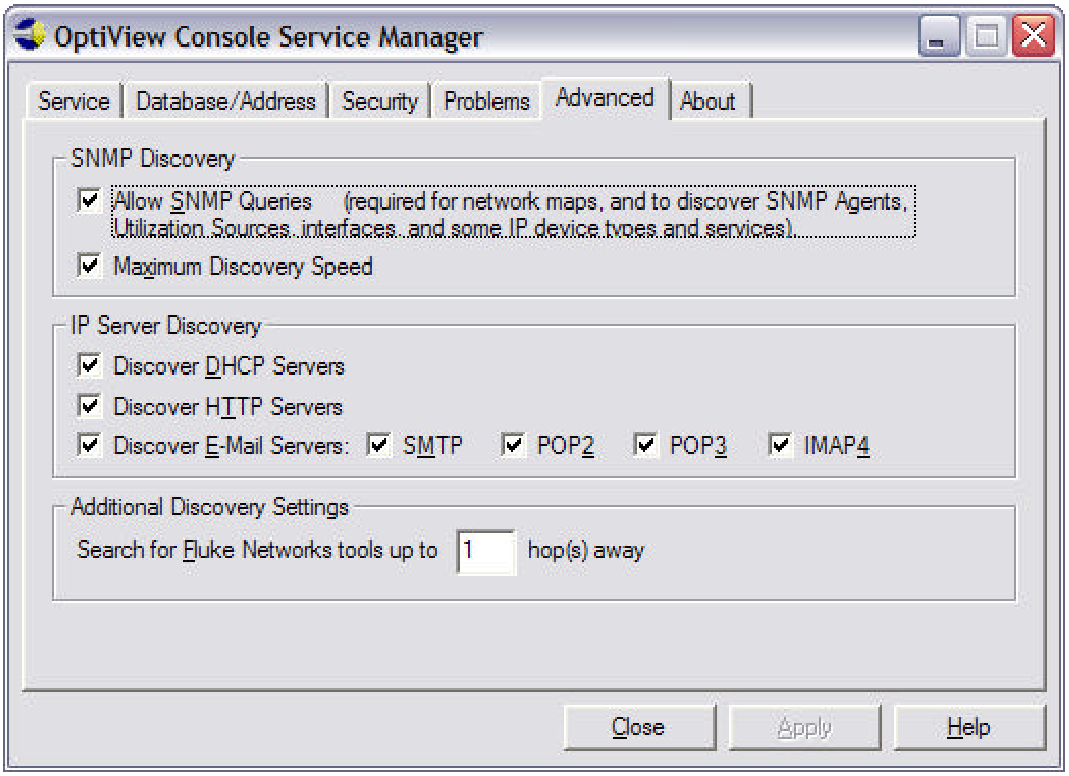
13. Select the **Hide Community Strings** checkbox to remove the strings from view. The strings will be replaced with *'s.
14. Enter passwords for any OptiView analyzers on your network (that are being used as hardware agents). Use a space-separated list for multiple devices.
15. Select the **Hide Passwords** checkbox to remove the passwords from view. The passwords will be replaced with *'s.
16. Some devices are set to generate alarms if they are queried. In the **Sensitive Devices** window, enter the IP address of any device on your network that you do not want the application to use its active discovery methods on to discover it. Enter multiple IP addresses using a space-separated list. All devices designated as sensitive will not be actively queried by the application.

17. Select the **Problems** tab.



- ☑ Errors
  - ☑ Key device not responding
  - ☑ Incorrect subnet mask
  - ☑ Duplicate IP address
  - □ Duplicate NetBIOS name
  - ☑ Duplicate IPX network number
  - ☑ Duplicate IPX internal network number
  - ☑ No Novell file server found
  - ☑ Out of Novell client login licenses
  - ☑ Interface utilization exceeded 80%
  - ☑ Interface error rate exceeded 1%
  - ☑ Collision rate exceeded 20%
  - ☑ New error detected by Hardware Agent
  - ☑ NMS error trap (minor)

18. You can use this tab to select the problems (**Errors**, **Warnings**, and **Information**), which will be stored in the database and displayed in the **Problem Log**. The default selections are already entered. A white check box ☑ with a check in it means that all of the items in that category are selected and a gray check box ☑ with a check in it means that the some, but not all, of the items in that category are selected.
19. Select the **Configure Thresholds…** button to change thresholds that will generate a problem (error or warning) for Network Utilization, Network Errors, or Collisions.
20. Select the **Configure SNMP Trap Errors** button to configure which SNMP Traps sent by other devices or Network Management Systems should be reported in the Problem Log. Refer to the topic Configure SNMP Trap Errors for more information on configuring SNMP traps.
21. Select the **Advanced** tab, where you can fine-tune the agent discovery process for your network.



SNMP Discovery

☑ Allow SNMP Queries (required for network maps, and to discover SNMP Agents, Utilization Sources, interfaces, and some IP device types and services)

☑ Maximum Discovery Speed

IP Server Discovery

☑ Discover DHCP Servers

☑ Discover HTTP Servers

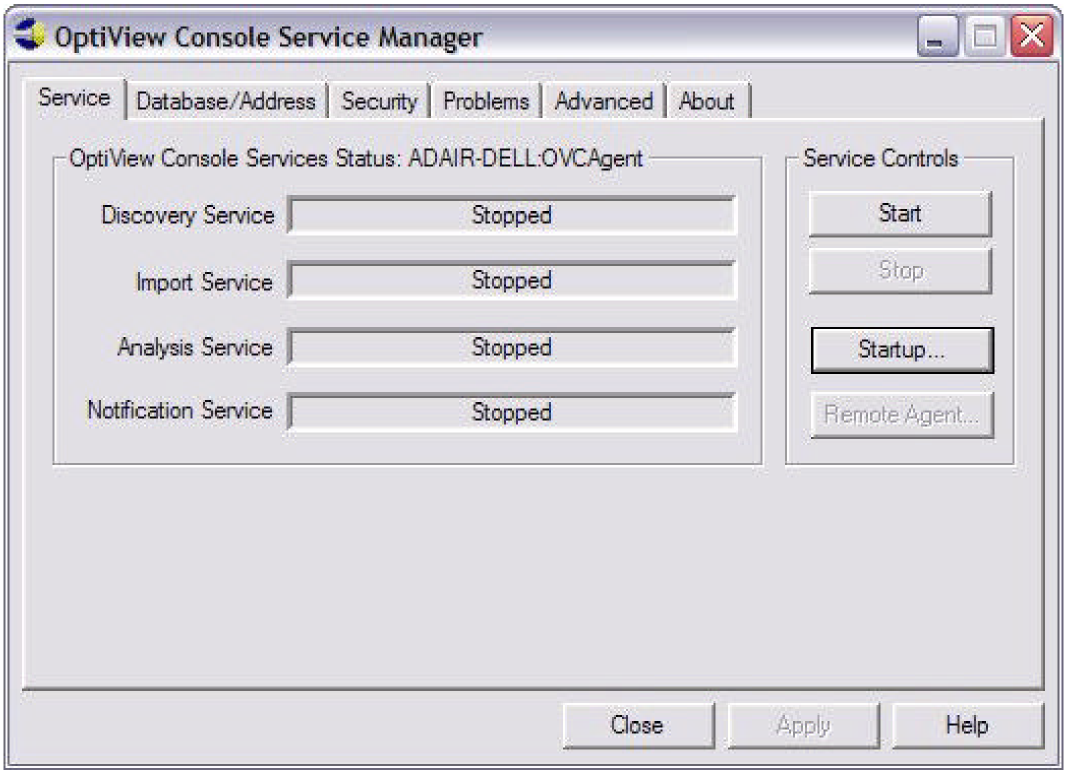
☑ Discover E-Mail Servers: ☑ SMTP ☑ POP2 ☑ POP3 ☑ IMAP4

Additional Discovery Settings

Search for Fluke Networks tools up to 1 hop(s) away

The default selections made on the **Advanced** tab are chosen to maximize the network discovery performance of the application. However, occasionally there may be a negative effect on your network performance that may cause you to need to turn one or more of these selections off. Refer to the Advanced Tab topic for more information.

22. Select the **Service** tab.



OptiView Console Services Status: ADAIR-DELL:OVCAgent

Discovery Service: Stopped

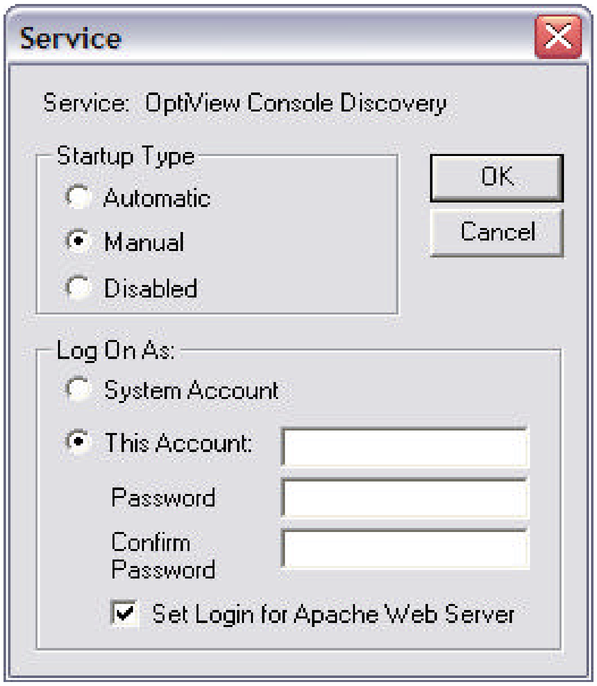
Import Service: Stopped

Analysis Service: Stopped

Notification Service: Stopped

Notice that the **Import**, **Analysis**, and **Notification** services are disabled for a remote Agent. The master Agent handles these tasks. Also, notice that the **Remote Agent…** button is enabled. You can use the **Remote Agent…** button to designate a different IP address for the master Agent to which the remote Agent reports.

23. Select the **Startup…** button.
24. The **Service** dialog box opens:



Service: OptiView Console Discovery

Startup Type
○ Automatic
● Manual
○ Disabled

Log On As:
○ System Account
● This Account:
Password
Confirm Password
☑ Set Login for Apache Web Server

25. Select the **Automatic** radio button if you want the Agent to start automatically each time Windows is started, or select the **Manual** radio button if you prefer to start the Agent manually using the **Start** button.

Notes

*Selecting the **Automatic** radio button may add up to 30 seconds to the time it takes Windows to boot after you log in.*

Regardless of whether you select the Automatic radio button or the Manual radio button, you can still manually start the Agent whenever you want by clicking the Start button. The automatic-start option merely gives you a way to ensure that if the computer reboots, the Agent will be started again automatically.

26. Select the **This Account:** radio button and enter a valid Windows user account in the **This Account:** field of the **Log On As:** section if you selected the **Automatic** startup type.

The Windows user account and password you enter must meet the following criteria:

- It must have administrator privileges for the PC that is running the application.
- It must be a valid Windows user account for the PC.

Notes

*A Windows user account must exist on the PC running the remote Agent that has the same user name and password as the logon account of the PC that is running the master Agent. The account must have administrator privileges for the PC (running the remote Agent). While in most cases this account is the one that will be used in the **This Account:** field, it is not a requirement. As long as the account exists on the remote PC, the system account can be used in the **Log On As:** field or a different Windows user account can be used.*

*If the accounts authenticate to domains, then there must be an account on the remote PC that has the same domain/account name and password as the logon account of the PC that is running the master Viewer/Agent. For example, the user logged on to the master PC using account **User1**. **User1** is in domain **Domain1**. In order to access the database on the PC that is running the remote software Agent, the account **Domain1\User1** must exist on the remote PC and have administrator privileges. The passwords for the accounts on both PCs must match.*

If the remote Agent is installed on a PC that is running Windows XP, either:

The login account of the PC running the master Viewer/Agent must authenticate to a domain and an account with the same name and password that authenticates to the same domain must exist on the PC that is running the remote Agent.

or

*If the PC is not in a domain, then you **must** turn on local user authentication for the PC.*

Turn on local user authentication for Windows XP as follows:

*a. From the Windows Control Panel select **Administrative Tools**.*

*b. Select **Local Security Policy**. The **Local Security Settings** window opens.*

*c. Select the **Network Access: Sharing and security model for local accounts** policy. The **Network Access** dialog box opens.*

*d. Select the **Classic – local users authenticate as themselves** security policy.*

*e. Select **Apply** and then **OK**.*

If any of the above information regarding accounts and passwords is confusing, please consult your network administrator or someone who has knowledge of Windows security. Correct setup of the account and password is critical for the master agent to be able to access remote software agents.

26. Enter a password in the **Password** and **Confirm Password** fields.
27. Select **OK**.
28. The **Service** dialog box closes.
29. Press the **Apply** button to save any changes made in the previous steps. The changes will take effect the next time the services are started.
30. Select the **Start** button.

31. The **Agent** service will now start.

Notes

The service can take up to 30 seconds to start.

*The service will run until you click the **Stop** button in the Service Manager’s dialog box. Because this is a Windows service, closing the Service Manager’s dialog box will not stop it.*

Configure and Start a Remote Hardware Agent

Configure a Hardware Agent

Hardware Agents are Fluke Networks OptiView analyzers (Workgroup Analyzers, Integrated Networks Analyzers, or WAN Analyzers) serving as remote agents to enhance network discovery. The master Agent will discover all hardware agents within N router hops of the PC that is running the agent. You can specify the number of router hops on the Advanced Tab of the Service Manager.

Note

Each router must have SNMP turned on in order for the application to discover OptiView analyzers that are more than one hop away from the PC that is running the application.

If an OptiView analyzer is not being discovered on the network, you can direct it to advertise its presence on the network to the master Agent. Enter the IP address of the PC that is running the master Agent in the **OptiView Console** field of the **Security** tab of the OptiView analyzer. This will cause the OptiView analyzer to send a UDP packet to UDP port 2359 of the PC that is running the master Viewer/Agent. This "Phone Home" feature will cause the Agent to discover an OptiView analyzer anywhere on the network.

Note

If UDP port 2359 on a firewall that is located between an OptiView analyzer and the PC that is running the master Viewer/Agent has been turned off, then the "Phone Home" feature will not work. If this is the case and the master Agent is not discovering the OptiView analyzer, then you can manually add the analyzer to the database.

You can add an OptiView analyzer to the database by doing the following:

1. *Select the **Detail** tab on the master Viewer.*
2. *Select **Device|Add New…** from the Menu bar.*
3. *When the **Add New Device** dialog box appears, enter the IP address of the OptiView analyzer and select **OK**.*
4. *It may take several minutes for the application to discover the device, but it will appear in the **Hosts** category of the **Detail** tab.*
5. *Select the device in the **Hosts** category, right-click on it, and select **Modify Type…**.*
6. *When the **Modify Device Type** dialog box appears, select the **Fluke Tool** checkbox and use the pull-down menu next to it to select the correct type of Fluke tool. Select **OK** when done.*
7. *The analyzer will now appear in the **Fluke Networks Tools** category of the **Detail** tab and it will appear as an agent in the **Overview** tab of the Viewer.*

If you are using the password feature on your OptiView analyzer, verify that the password is entered in the **Passwords** list on the Security tab of the **Service Manager**.

If Remote Control Encryption is enabled on your OptiView analyzer then you must enter the same encryption key in the same format (ASCII or Hexadecimal) as was entered on the OptiView analyzer. Enter it in the **Import Encryption Key** field of the Manage Agents dialog box. You can access the **Manage Agents** dialog box by selecting **File | Manage Agents** from the Menu bar.

Start a Hardware Agent

Normally, auto-import of data from a hardware agent is turned on automatically when the hardware agent is discovered. You can turn auto-import on or off by either right-clicking on the Agent in the **Overview** tab or by selecting **File | Manage Agents...** on the Menu bar and selecting or de-selecting **Enable Auto-Imports from Agent**.

Notes

When you first start the Viewer, it may take up to 90 seconds to activate and display data from each hardware Agent. This is a sequential process and is designed to keep all of the hardware agents from simultaneously trying to connect to the master database.

When you enable auto-import for an OptiView WAN analyzer, you will be prompted to select whether to enable imports with or without RMON2 Trending. With RMON2 Trending enabled, the counters on *the OptiView WAN analyzer are reset every hour. This allows a device that has relatively low counts (e.g. in the Top Talkers category) over a long period of time, but has recently seen a lot of activity, to overcome a device that has seen a consistent high level of activity. Without RMON2 Trending, the counters are not reset.*

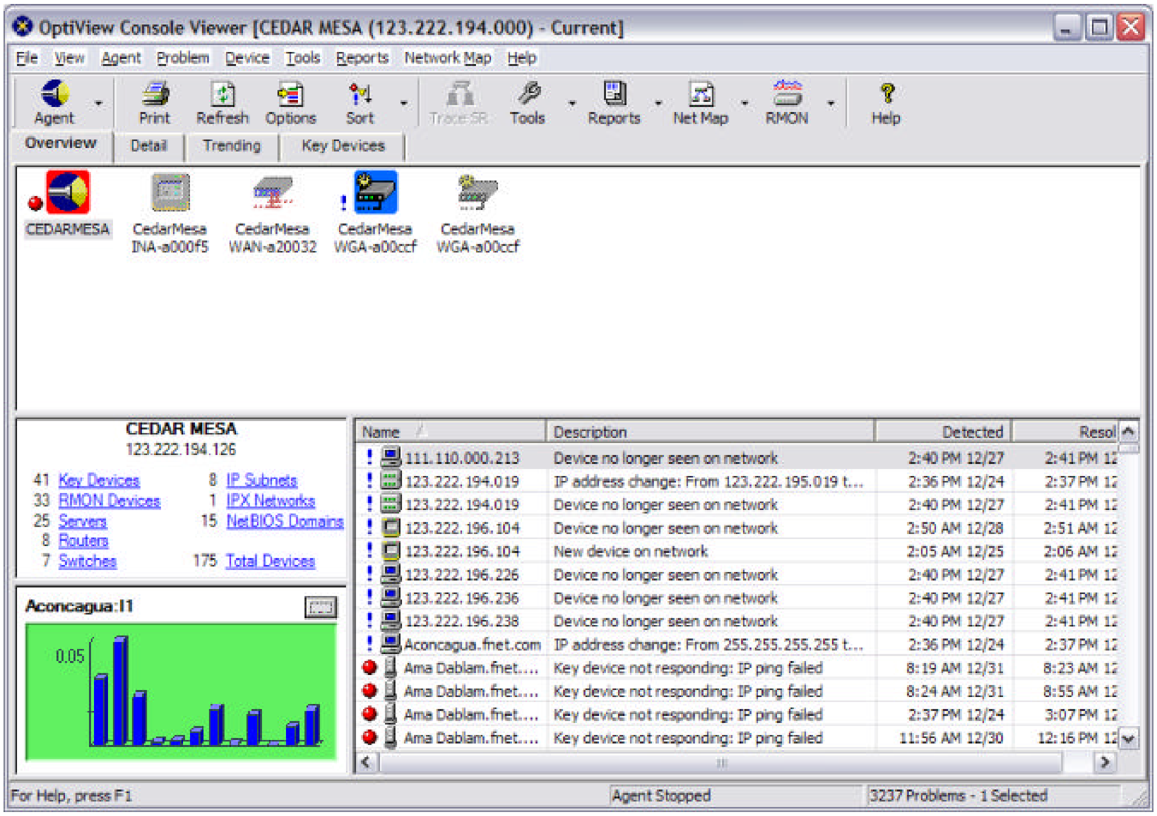
Two or more OptiView Console applications importing from the same OptiView WAN analyzer with RMON2 Trending turned on may invalidate the results, because the counters are being set asynchronously.

Configure and Start the Master Viewer

Note

There is no configuration necessary to start and run the master Viewer.

1. On the computer on which you installed the application, select **Start** | **Programs** | **Fluke Networks** | **OptiView Console** (or, if you did not accept the default Program folder name during installation, point to the folder you chose).
2. Select **Viewer**.



CEDAR MESA
123.222.194.126

41	Key Devices	8	IP Subnets
33	RMON Devices	1	IPX Networks
25	Servers	15	NetBIOS Domains
8	Routers		
7	Switches	175	Total Devices

	Name	Description	Detected	Resol
!	111.110.000.213	Device no longer seen on network	2:40 PM 12/27	2:41 PM 12
!	123.222.194.019	IP address change: From 123.222.195.019 t...	2:36 PM 12/24	2:37 PM 12
!	123.222.194.019	Device no longer seen on network	2:40 PM 12/27	2:41 PM 12
!	123.222.196.104	Device no longer seen on network	2:50 AM 12/28	2:51 AM 12
!	123.222.196.104	New device on network	2:05 AM 12/25	2:06 AM 12
!	123.222.196.226	Device no longer seen on network	2:40 PM 12/27	2:41 PM 12
!	123.222.196.236	Device no longer seen on network	2:40 PM 12/27	2:41 PM 12
!	123.222.196.238	Device no longer seen on network	2:40 PM 12/27	2:41 PM 12
!	Aconcagua.fnet.com	IP address change: From 255.255.255.255 t...	2:36 PM 12/24	2:37 PM 12
●	Ama Dablam.fnet....	Key device not responding: IP ping failed	8:19 AM 12/31	8:23 AM 12
●	Ama Dablam.fnet....	Key device not responding: IP ping failed	8:24 AM 12/31	8:55 AM 12
●	Ama Dablam.fnet....	Key device not responding: IP ping failed	2:37 PM 12/24	3:07 PM 12
●	Ama Dablam.fnet....	Key device not responding: IP ping failed	11:56 AM 12/30	12:16 PM 12

For Help, press F1 | Agent Stopped | 3237 Problems - 1 Selected

The Viewer opens to the **Overview** tab. The Viewer shows discovered hardware and software agents, the problem log, a summary of discovered devices for the selected agent, and a current utilization chart for a user selected interface. Refer to the **Introduction to the Viewer** topic in the online help for more information.

Notes

Opening and closing the Viewer has no effect on the Agent and other services. If the Agent is running, it continues to run, and if the Agent is stopped, it remains stopped.

You can open the Service Manager from the Viewer by selecting the Agent *button on the Toolbar and then selecting **Configure Local Agent...**, or you can use **Ctrl-A**.*

Configure and Start a Remote Viewer

With the purchase of an additional license, you can install a Viewer on a remote PC and direct the Viewer to read the master database. You can then perform all the same functions with the remote Viewer as the master Viewer with the exception that you cannot restore and view archived databases.

The first time that you run the remote Viewer, you will be prompted to enter the IP address or computer name of the PC that is running the master Agent. You can direct the Viewer to look at different master databases by selecting **Set Master Database...** from the File menu of the Viewer Menu Bar and entering a new IP address or computer name.

In order to use a remote viewer, a Windows user account with the same userid and password as the logon account of the remote viewer PC must exist on the master PC. Both accounts must have administrator privileges for the PC on which they are running. The master PC can be logged on as a different user, as long as the account exists on the master PC.

Example – Remote Viewer

A remote Viewer is installed and directed to a PC running the master Viewer/Agent. The remote PC is logged on as *RemoteUse*r with a password of *Viewer*. The *RemoteUser* userid has administrator privileges for the PC on which it is running.

The PC that is running the master Viewer/Agent must have an account *RemoteUser* with password *Viewer*. The account must have administrator privileges for the master PC. A different userid can be used to log on to the master PC, as long as the *RemoteUser* account exists on the master PC.

Remotely Access the OptiView Console Application

There are three options for remotely accessing the OptiView Console application:

- **Remote Viewer** - With the purchase of an additional license, you can install a Viewer on a remote PC and direct the Viewer to read the master database. You can then perform all the same functions with the remote Viewer as the master Viewer with the exception that you cannot restore and view archived databases. Refer to the topic Configure and Start a Remote Viewer for more information.
- **Web Reporter** - You can use your web browser and the included Web Reporter application to remotely access reports and maps that have been archived by the OptiView Console application.
- **Thin Client** - You can use HOBLink JWT to remotely access and run the OptiView Console application. HOBLink JWT is a Web-based solution for multi-user, multi-platform access to applications and data on Windows Terminal Servers. Refer to the HOBLink web site for more information.

Other Information

How To Contact Fluke Networks

To find out more about Fluke Networks and our products, visit us on the World Wide Web at http://www.flukenetworks.com or call us at 1-800-28-FLUKE (1-800-283-5853). You can also request information via email at `info@flukenetworks.com`.

You can visit the OptiView Console home page at http://www.flukenetworks.com/optiviewconsole . For technical support on the OptiView Console application you can review the Fluke Networks Knowledge base for the OptiView Console application at http://www.flukenetworks.com/knowledgebase. You can also send an email to `support@flukenetworks.com` or call 1-800-28-FLUKE (1-800-283-5853). For access to the Fluke Networks Support Solutions, visit http://www.flukenetworks.com/support .

Our offices are located at the following addresses:

Fluke Networks
P.O. Box 9090
Everett, Washington, USA
98206-9090

Fluke Europe B.V.
P.O. Box 1186
5602 B.D. Eindhoven
The Netherlands

Trademarks and Copyrights

OptiView Console Copyright © 1998, 1999, 2000, 2001, 2003, 2004 Fluke Corporation. All rights reserved.

RMON Inspector Copyright © 1992-1999 Apptitude, Inc. Copyright © 2003, 2004 Fluke Corporation.

Fluke Networks and LANMeter are registered trademarks of Fluke Corporation.

OptiView Console, OptiView, Protocol Inspector, OneTouch, SwitchTap, SwitchRoute, and Network Supervision are trademarks of Fluke Corporation

Visio is a registered trademark of Visio Corporation and Microsoft Corporation.

Microsoft, Windows, and NT are registered trademarks of Microsoft Corporation.

Windows 2003, Windows 2000, and Windows XP are trademarks of Microsoft Corporation.

Pentium is a registered trademark of Intel Corporation.

NetBIOS is a registered trademark of International Business Machines Corporation.

Novell, IPX, and NetWare are registered trademarks of Novell Inc.

Sniffer is a registered trademark of Network Associates, Inc.

CiscoWorks is a registered trademark of Cisco Systems, Inc.

Crystal Decisions, Crystal Reports, Crystal Enterprise, Crystal Analysis, Seagate Info and Seagate Holos are trademarks or registered trademarks of Crystal Decisions, Inc.

MG-Soft MIB Browser is a copyright of MG-Soft Corporation.

All product names mentioned in the OptiView Console application and help files are trademarks of their respective manufacturers. While Fluke Networks has made a reasonable effort to identify trademarks and trademark owners, we may have missed some, and our failure to identify them is unintentional.

Index