

TANDBERG FieldView

The FieldView Management Suite (FMS) system allows administrators to view the status of remote FieldView System endpoints, create and apply system configurations, and manage and apply remote software updates.

Using the FMS, administrators can efficiently manage and maintain groups of FieldView endpoints, including both FieldView Device (FD) and FieldView Application (FA) endpoints.

Management Suite



**TANDBERG FieldView
FMS User manual
March 2008**

Copyright © 2007–2008, TANDBERG

The information in this document is furnished for informational purposes only, is subject to change without prior notice, and should not be construed as a commitment by TANDBERG.

TANDBERG reserves the right to amend any of the information given in this document in order to take account of new developments.

Every effort has been made to supply complete and accurate information, however, TANDBERG assumes no responsibility or liability for any errors or inaccuracies that may appear in this document, nor for any infringements of patents or other rights of third parties resulting from its use. No license is granted under any patents or patent rights of TANDBERG.

All rights reserved. This document contains information that is proprietary to TANDBERG. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronically, mechanically, by photocopying, or otherwise, without the prior written permission of TANDBERG. Nationally and internationally recognized trademarks and trade names are the property of their respective holders and are hereby acknowledged

The FMS software is subject to the following copyright:

Copyright © 2007–2008 LibreStream Technologies, Incorporated. All rights reserved. Patents Pending in Canada, the U.S. and other countries.

LibreStream, the LibreStream logo, n_sight, and the n_sight logo are either registered trademarks or trademarks of LibreStream Technologies, Incorporated in Canada, the United States, and/or other countries. All other trademarks are the property of their respective owners..

Table of Contents

FieldView Management Suite Overview	5
System Requirements	5
Installation	6
Server Firewall Configuration	6
Starting FMS for the First Time	7
Logging In	7
Configuring the FMS User Interface	7
Changing the Administrator Password	8
Changing the FMS Service Host Name and Port	8
Configuring the FMS Update Server	9
Activating the FMS Service	10
Online Activation	10
Manual Activation	11
Configuring the FMS Service	12
Preparing an Endpoint for Remote Management	14
Enabling Remote Management on an FD Endpoint	14
Enabling Remote Management on an FA Endpoint	14
Installing the SNMP Service	15
Configuring the SNMP Service	17
Client Host Firewall Configuration	19
Additional Configuration	19
Remote Monitoring Without the FMS Service	19
Managing Devices	21
Manually Adding a Managed Device	21
Troubleshooting Adding a New Device	22
Automatic Discovery of Managed Devices	22
View Existing Device Discovery Ranges	22
Creating a Device Discovery Range	23
Modify an Existing Device Discovery Range	24
Deleting a Device Discovery Range	24
Viewing Existing Managed Devices	24
Refreshing the Managed Devices Table	25
Device Administration	25
Software / Configuration Updates	26
Assigning an Update Group	26
Removing an Endpoint from an Update Group	27
Updating the Software/Configuration of an Endpoint	27
Viewing and Modifying an Existing Endpoint	28
Managing Device Details	29
Software / Configuration Updates	30
Viewing Endpoint Status	31
FD Configurations	33
Creating an FD Configuration Package	33
View Existing FD Configuration Packages	35
Modifying an Existing FD Configuration Package	35
Maintaining the Wireless Preferred Networks List	36
Create a Wireless Preferred Network	36
Modify an Existing Wireless Preferred Network	37
Deleting a Wireless Preferred Network	37
FA Configurations	38
Creating an FA Configuration Package	38

View Existing FA Configuration Packages	39
Modifying an Existing FA Configuration Package	40
Users/Contacts Packages	41
Creating a New Users/Contacts Package	41
View Existing Users/Contacts Packages	42
Modifying an Existing Users/Contacts Package	43
Maintaining the Users List	44
Create a New User	44
Modify an Existing User	45
Deleting a User.	46
Maintaining the Contacts List	46
Create a New Contact	46
Modify an Existing Contact.	46
Deleting a Contact	47
Importing Users and Contacts	47
Media Configurations.	48
Creating a New Media Configuration Package.	48
View Existing Media Configuration Packages	49
Modifying an Existing Media Configuration Package	49
Maintaining the Media Configurations List	50
Create a New Media Configuration	50
Modify an Existing Media Configuration	51
Deleting a Media Configuration.	52
Software Update Packages.	53
View Existing Software Packages	53
Adding a New Software Package.	53
Deleting an Existing Software Package	54

FieldView Management Suite Overview

The FieldView Management Suite (FMS) system allows administrators to view the status of remote FieldView System endpoints, create and apply system configurations, and manage and apply remote software updates. Using the FMS, administrators can efficiently manage and maintain groups of FieldView endpoints, including both FieldView Device (FD) and FieldView Application (FA) endpoints.

The FMS consists of two main software components. The first, the FMS Service, is a Microsoft Windows service that queries the status of FieldView endpoints and initiates software updates by SNMP GET and SET requests. The second, the FMS User Interface, is a web application that communicates with the FMS service. It allows administrators to view and manage FieldView endpoints, configuration update packages, and software update packages. The FMS User Interface application also hosts the software and configuration update packages that are downloaded and installed by the endpoints. Typically these two systems reside on the same physical machine.

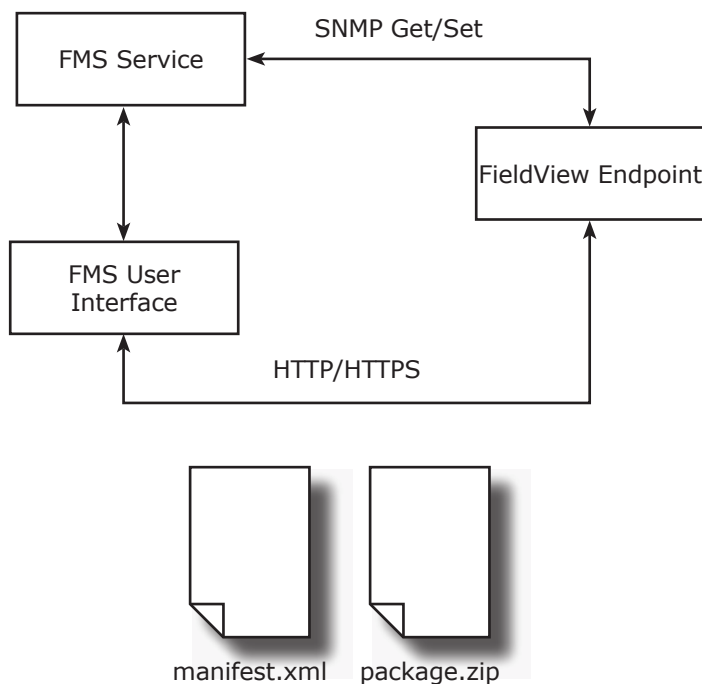


Figure 1 - FMS Architecture

System Requirements

The FMS has the following system requirements:

- Windows XP Professional SP2 or Windows Server 2003
- IIS 5.1 or later
- ASP.NET 2.0

Installation

To install FieldView Management Suite, put the installation CD into your CD drive. The installation program should automatically launch when the CD is inserted. If it doesn't, open an Explorer window (right-click on the Windows Start button and select Explore), locate the **FMS** directory on the CD, and run the **setup.exe** program.

Before the installation you may be prompted to install several pre-requisites that are required for the FMS to operate. These include:

- Visual C++ Runtime
- Microsoft Windows Installer 3.1
- Microsoft .NET Framework 2.0
- Microsoft ASP.NET 2.0 Ajax Extensions 1.0

After installing the pre-requisites, follow the onscreen prompts to complete the installation procedure.

During the installation process you will be presented with a window asking you to enter the TCP port that the FMS Service will use to communicate with the FMS User Interface. Once the FMS Service starts, it begins listening for TCP connections on this port, so it is important that you choose a port that is not already in use on your system. The default TCP port is **9090**. Enter the value of the port you wish to use, and click **OK** to accept the changes and complete the installation.

Take note of which TCP port you chose as you will be required to enter this again when configuring the FMS User Interface. You can view or change the selected TCP port at any time by choosing **Start→All Programs→TANDBERG FieldView Management Suite→Configure FMS Service**.

Server Firewall Configuration

If Windows Firewall, third party firewall software, or another Internet security suite is running on the server where you installed FMS, you need to configure firewall exceptions for the ports listed in Table 1.

Table 1 - Required Firewall Exceptions

TCP Port 80 (HTTP)	Required if the FMS server will be hosting software and configuration updates by HTTP. If your IIS configuration uses a port other than 80 , ensure that you have allowed that port instead.
TCP Port 443 (HTTPS)	Required if the FMS server will be hosting software and configuration updates by HTTPS. If your IIS configuration uses a port other than 443 , ensure that you have allowed that port instead.
UDP Port 162 (SNMP Traps)	Although not required for the FMS to function, if you are using third party monitoring software you will need to open port 162 to receive SNMP traps from FieldView endpoints.

Starting FMS for the First Time

Logging In

To login to the FMS system, you must first launch the user interface by choosing **Start→All Programs→ TANDBERG FieldView Management Suite→Login to FMS**. This starts the FMS User Interface in your default web browser and you will be presented with the screen in Figure 2.

Every web page in the FMS User Interface is laid out in a similar manner to the login screen in Figure 2. At the top of the page the name of the application is displayed, along with the product's activation status (see **Activating the FMS Service**). Immediately below the activation status is the menu bar which is used to navigate between sections of the user interface. Lastly, the title of the page/section that you are working on and the content of that section is displayed directly below the menu.

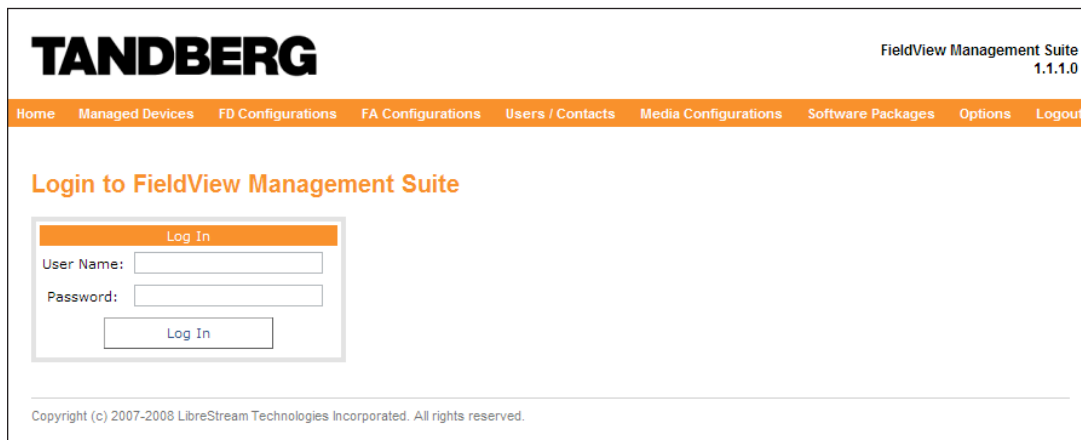


Figure 2 - Logging In to FMS

To log in, enter the default user name and password listed below:

Default User Name: **admin**

Default Password: **admin**

To avoid unauthorized access to the software, change this password immediately after logging in for the first time.

Configuring the FMS User Interface

After logging in for the first time, you need to configure the user interface. There are three steps required in the configuration process: changing the administrator password, configuring the FMS Service host name and port, and configuring the FMS configuration and software update server.

Changing the Administrator Password

On the menu bar located near the top of your screen, choose **Options→General Settings**. This will take you to the **General Settings** configuration page, shown in Figure 3. To change the administrator password, type the new password into both the password and confirmation fields, and click the **Save** button. If the passwords you enter do not match, an error message is displayed.

The screenshot shows the TANDBERG FieldView Management Suite interface. The top navigation bar includes 'Home', 'Managed Devices', 'FD Configurations', 'FA Configurations', 'Users / Contacts', 'Media Configurations', 'Software Packages', 'Options', and 'Logout'. The 'Options' menu is active, leading to the 'General Settings' page. The page title is 'General Settings'. The form is divided into two sections: 'General Configuration' and 'FMS Service Configuration'. Under 'General Configuration', there are two text input fields for 'Administrator Password' and 'Confirm Password'. Under 'FMS Service Configuration', there are two text input fields: 'Service Host Name' (containing 'localhost') and 'Service TCP Port' (containing '9090'). At the bottom of the form are 'Save' and 'Cancel' buttons. A copyright notice at the bottom reads: 'Copyright (c) 2007-2008 LibreStream Technologies Incorporated. All rights reserved.'

Figure 3 - General Settings

Changing the FMS Service Host Name and Port

The FMS User Interface communicates with the FMS Service over a TCP connection. If you install the FMS Service on the same machine as the FMS User Interface and use the default TCP port of **9090**, no further configuration is required.

Otherwise, open the **General Settings** configuration page by choosing **Options→General Settings** and locate the **FMS Service Configuration** section. In the field labeled **Service Host Name**, enter the host name of the server that the FMS Service is installed on. In the field labeled **Service TCP Port**, enter the TCP port that you selected during installation.

For example, if the FMS Service resides on the same physical computer as the FMS User Interface and communicates on port 9876, you would enter the following values into the service configuration fields:

Service Host Name:	localhost
Service TCP Port:	9876

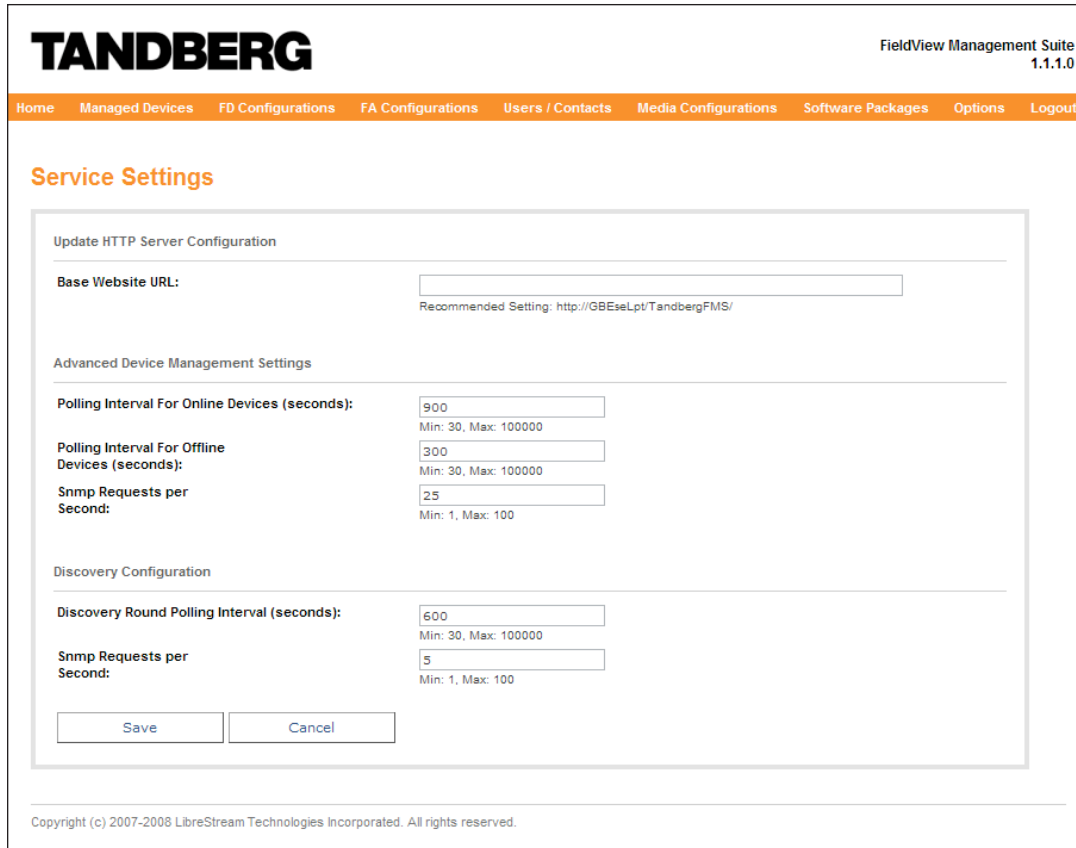
Once you have made your changes, click the **Save** button to save your changes.

Note: While navigating around the user interface, if the FMS Service is not running or the host name and port are configured incorrectly, an error page may be displayed stating that the user interface could not communicate with the FMS Service.

Configuring the FMS Update Server

FieldView endpoints retrieve software and configuration updates from the FMS User Interface server using either HTTP or HTTPS requests. When performing a check for updates, the FMS Service configures the FieldView endpoints with the URL to use when downloading updates from the server.

To configure the URL of the update server, choose **Options**→**FMS Service Settings**. You will be presented with the **FMS Service Settings** screen similar to the one shown in Figure 4.



TANDBERG FieldView Management Suite 1.1.1.0

Home Managed Devices FD Configurations FA Configurations Users / Contacts Media Configurations Software Packages Options Logout

Service Settings

Update HTTP Server Configuration

Base Website URL: Recommended Setting: http://GBEseLpt/TandbergFMS/

Advanced Device Management Settings

Polling Interval For Online Devices (seconds): Min: 30, Max: 100000

Polling Interval For Offline Devices (seconds): Min: 30, Max: 100000

Snmp Requests per Second: Min: 1, Max: 100

Discovery Configuration

Discovery Round Polling Interval (seconds): Min: 30, Max: 100000

Snmp Requests per Second: Min: 1, Max: 100

Copyright (c) 2007-2008 LibreStream Technologies Incorporated. All rights reserved.

Figure 4 - FMS Service Settings

To configure the update server, locate the field labeled **Base Website URL** and enter the fully qualified URL of the update server. The URL that you enter is similar to the URL that you use to navigate to the FMS User Interface, except that rather than using **localhost** as the server name, a publicly visible IP address or hostname should be used.

For example, if the host name of the machine that the user interface resides on is **bingo**, you would enter `http://bingo/TandbergFMS/` into the **Base Website URL** field. A recommended setting based on the hostname and installed directory of the server is shown below the **Base Website URL** field.

To apply your changes, click the **Save** button at the bottom of the screen.

Note: For security reasons, we recommended that you use secure HTTPS. If an SSL certificate is installed on your server, you may substitute **https** for **http** when entering the **Base Website URL**.

Note: If FieldView endpoints are not able to resolve the hostname of the update server, use the IP address of the machine instead.

Example: `http://192.168.2.1/TandbergFMS/`.

Activating the FMS Service

After installing the FieldView Management Suite system, you must activate the FMS Service. Activation can be done in one of two ways: online or manually. The online method is normally more convenient, but it requires that the FMS Service have access to the Internet. If this is not the case, use the manual activation method.

Regardless of which method you use, you need the license keys that you received when you purchased the FieldView Management Suite. Once the service has been properly activated, you can begin monitoring devices and creating and applying configuration packages.

Note: To use the user interface, even to perform tasks such as creating and modifying configurations, the FMS Service must be running and activated at all times.

Online Activation

To perform online activation of the FMS Service, choose the **Options**→**Activation** menu item. You will be presented with the **Activation** screen shown in Figure 5.

TANDBERG

FieldView Management Suite
 1.1.1.0
Demo: 30 day(s) left

Home Managed Devices FD Configurations FA Configurations Users / Contacts Media Configurations Software Packages Options Logout

Activation

Current Activation Status: Demo: 30 day(s) left

Support Expiry Date: n/a

Activation Instructions

When you purchase **TANDBERG FieldView Management Suite** you will receive an **Activation Key**. This key is made up of two parts as depicted below:

XXXXXXX - CCCCCCCCCC

- Group "X" is a **License ID** and will be a numeric value from 1 to 2147483648.
- Group "C" is the **Key Code** and will be an alphanumeric character sequence.

You can activate your product either online via the Internet, or manually.

Online
Manual

Please enter your two-part Activation Key, and press the **Online Activation** button:

-

Copyright (c) 2007-2008 LibreStream Technologies Incorporated. All rights reserved.

Figure 5 - Online Activation

On the tab labeled **Online Activation**, enter the two parts of the license key in the fields provided, press the **Online Activation** button, and wait for a response from the TANDBERG activation server. Online activation may take up to a minute to complete. If the activation is successful, it is indicated at the top of the screen in green.

Manual Activation

To manually activate the FMS Service, choose the **Options→Activation** menu item and select the **Manual Activation** tab shown in Figure 6.

Contact a TANDBERG customer service representative using the phone number displayed on the screen. You will be asked to provide the activation key from your CD in addition to two automatically generated codes. These codes are unique to the PC that the FMS Service is installed on, so ensure that you use the ones displayed on your screen rather than the example codes in Figure 6. The service representative will provide you with the two

activation codes needed for activation. Enter the codes into the boxes provided and press the **Manual Activation** button. If the activation is successful, it is indicated at the top of the screen in green.

Online Manual

Step 1

In order to do manual activation you must provide the following information to a support representative:

1. This generated key code: **294884590**
2. This generated computer ID: **114035273**
3. The two-part Activation Key that you purchased along with this program

Step 2

Once you have the above information, please contact a support representative to get a two part Activation Code:

Americas: 1-866-826-3237 EMEA: contact your TANDBERG reseller

Step 3

Once you have a two-part Activation Code, enter it below and press the **Manual Activation** button:

Activation Code 1:

Activation Code 2:

Manual Activation

Copyright (c) 2007-2008 LibreStream Technologies Incorporated. All rights reserved.

Figure 6 - Manual Activation

Configuring the FMS Service

After configuring the FMS User Interface and activating the FMS Service, the system is fully operational. However, you may also wish to tune the performance of the FMS Service to fit your network environment.

To configure the FMS Service performance, choose **Options**→**FMS Service Settings**. You will be presented with the **FMS Service Settings** screen, shown in Figure 4. Using this page, you can configure both device management and device discovery settings. The configurable settings for device management are described in Table 2, while the configurable settings for device discovery are described in Table 3.

Table 2 - Device Management Settings

Polling Interval For Online Devices	The interval (in seconds) at which the FMS Service refreshes the current state of all online devices.
Polling Interval For Offline Devices	The interval (in seconds) at which the FMS Service attempts to retrieve the state of all not responding or offline devices. Setting this to a lower value reduces the delay in detecting when an endpoint has come online.
Snmp Requests Per Second	Setting this value to a lower number decreases the number of SNMP packets being sent by the FMS Service every second.

Table 3 - Device Discovery Settings

Discovery Round Polling Interval	The time the FMS service waits between endpoint discovery rounds. A lower number here increases the frequency of discovery rounds, increasing the chance that a device will be discovered if it is online for a short period of time. See the Automatic Discovery of Managed Devices for more information.
Snmp Requests Per Second	The number of requests per second sent by the discovery manager in the FMS Service. A higher number increases the speed of discovery and a lower number reduces network traffic.

Preparing an Endpoint for Remote Management

In order for the FMS Service to manage and monitor an FieldView endpoint, the SNMP service on the endpoint must be configured correctly.

Enabling Remote Management on an FD Endpoint

To enable remote management on an FD Endpoint, you must configure the SNMP community of the device. In the **Configuration** screen on the FD, select the **Network** → **SNMP** tab and configure the SNMP community accordingly.

Note: For security reasons, we recommend that you use a community name other than **public**. The community name that you choose will be given both READ and WRITE privileges.

Note: Take note of the community name that you choose here as it will be used later when adding this endpoint to the FMS database.

You can also configure the hostname or IP address of the SNMP manager that is permitted to communicate with the device. Entering a value into the **Permitted Manager** field on the SNMP tab restricts incoming SNMP packets to a single remote server. If you leave this field blank, any host will be allowed to communicate with the device using SNMP.

Note: For security reasons, we recommend that you enter the host name or IP address of the computer that is running the FMS Service.

The changes you make on this tab will take effect when you click **Apply**.

Enabling Remote Management on an FA Endpoint

To enable remote management on an FA endpoint, you must first ensure that the SNMP service is installed and configured on the host computer. After the SNMP service is installed and configured, the FA endpoint will be manageable from the FMS. Additional configuration of the FA client software itself is not necessary.

Note: The FA client software must be installed on a host system before the FMS can manage it. The client software can be installed either before or after the SNMP service configuration.

Note: When uninstalling or upgrading FAs on Windows Vista computers where the SNMP service is already running, you may be presented with a dialog, similar to the one in Figure 7, asking if you wish to automatically stop the SNMP Service. If you choose the option "Automatically close the applications and attempt to restart them after setup is complete", it is possible that the SNMP service will not be restarted after the uninstall operation has completed. If you choose "Do not close applications (A Reboot will be required)", the uninstall process will correctly stop and restart the SNMP service. In either case, to ensure that the SNMP service is in the desired state after the uninstall/upgrade process, we recommend that you restart the computer.

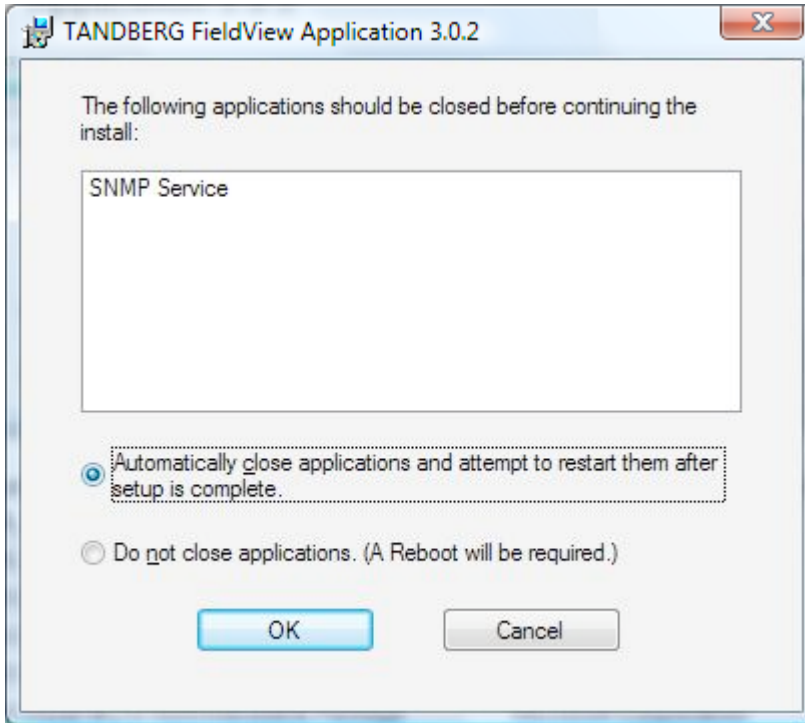


Figure 7 - SNMP Warning During FA Setup

Installing the SNMP Service

If the service is already installed, you may skip this section.

To install the SNMP service under Windows 2000/XP:

1. Choose **Start**→**Control Panel** to open the Windows Control Panel.
2. Double-click **Add/Remove Programs** to open the **Add or Remove Programs** dialog.
3. Click the **Add/Remove Windows Components** button on the left side of the dialog.

You will be presented with the Windows Components Wizard, as shown in Figure 8.

4. Click **Management and Monitoring Tools** in the list to select it and then click the **Details** button.

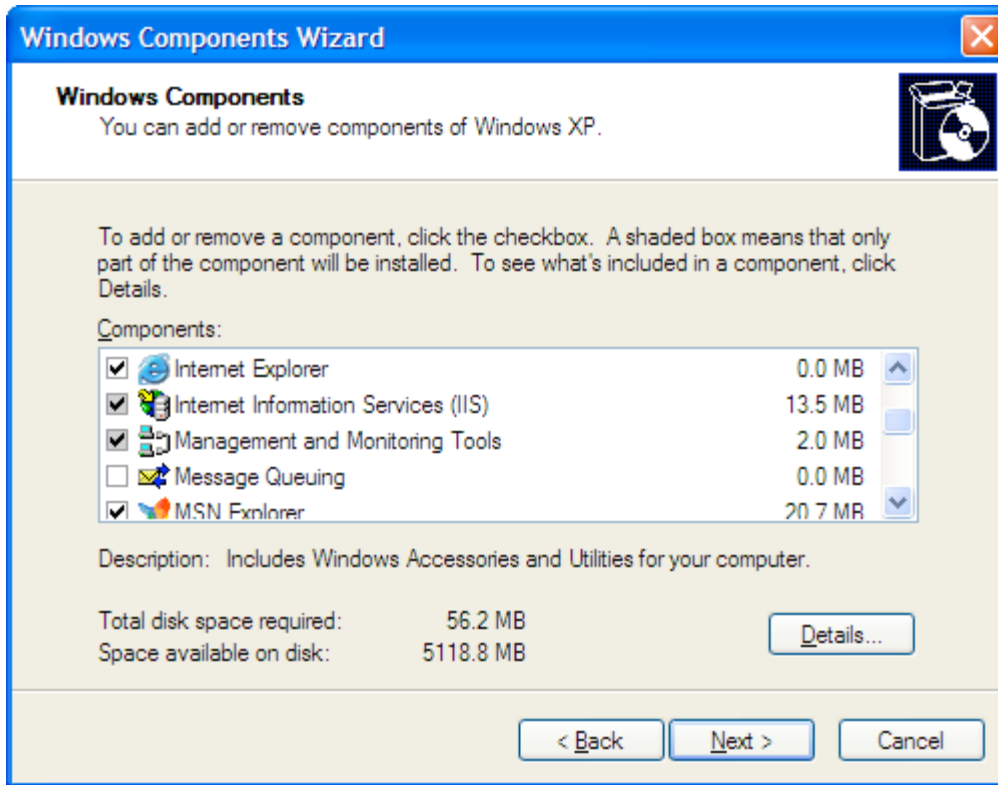


Figure 8 - Windows Components Wizard

You will be presented with the **Management and Monitoring Tools** dialog, as shown in Figure 9.

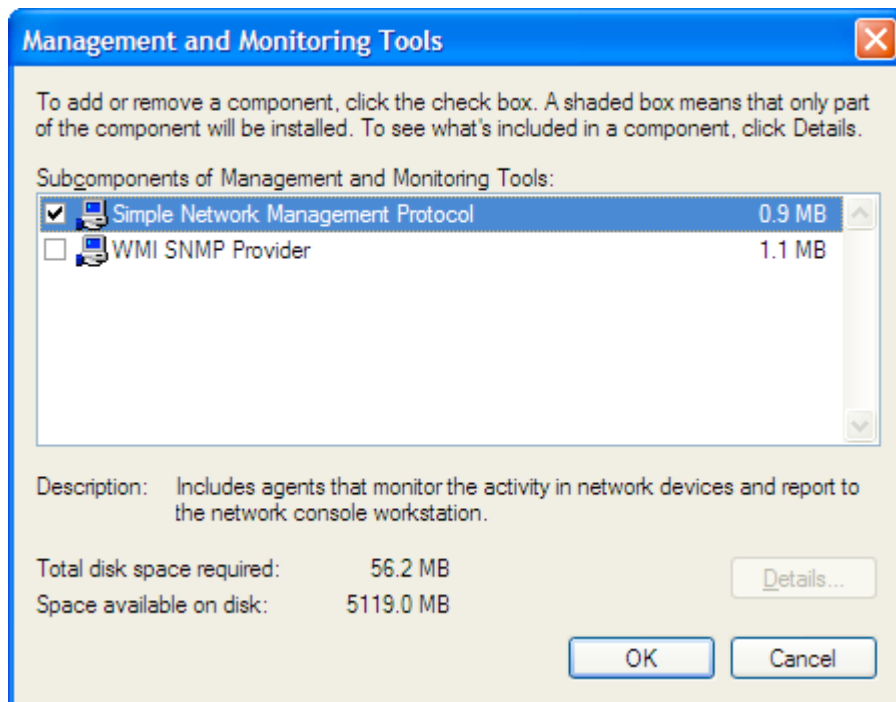


Figure 9 - Selecting SNMP from the Management and Monitoring Tools

5. Select the checkbox next to **Simple Network Management Protocol**.
6. Click **OK** to dismiss the **Management and Monitoring Tools** dialog.
7. Click **Next** to complete the installation. You may be asked for your Windows installation CD to complete the setup.
8. Click **Finish** when the wizard is finished.

After performing the steps above, the SNMP service is installed and running on your PC.

Configuring the SNMP Service

To configure the SNMP service to work with FMS:

1. Choose **Start** → **Control Panel** to open the Windows Control Panel.
2. Double-click **Administrative Tools** → **Services** to open the **Services** dialog.
3. Locate the **SNMP Service** entry in the list of services. The entry should indicate that the service is started. If it is not, start it by right-clicking on the entry and choosing **Start**.
4. Right-click on the **SNMP Service** entry and select **Properties**. You will be presented with the **SNMP Service Properties** dialog as shown in Figure 10.

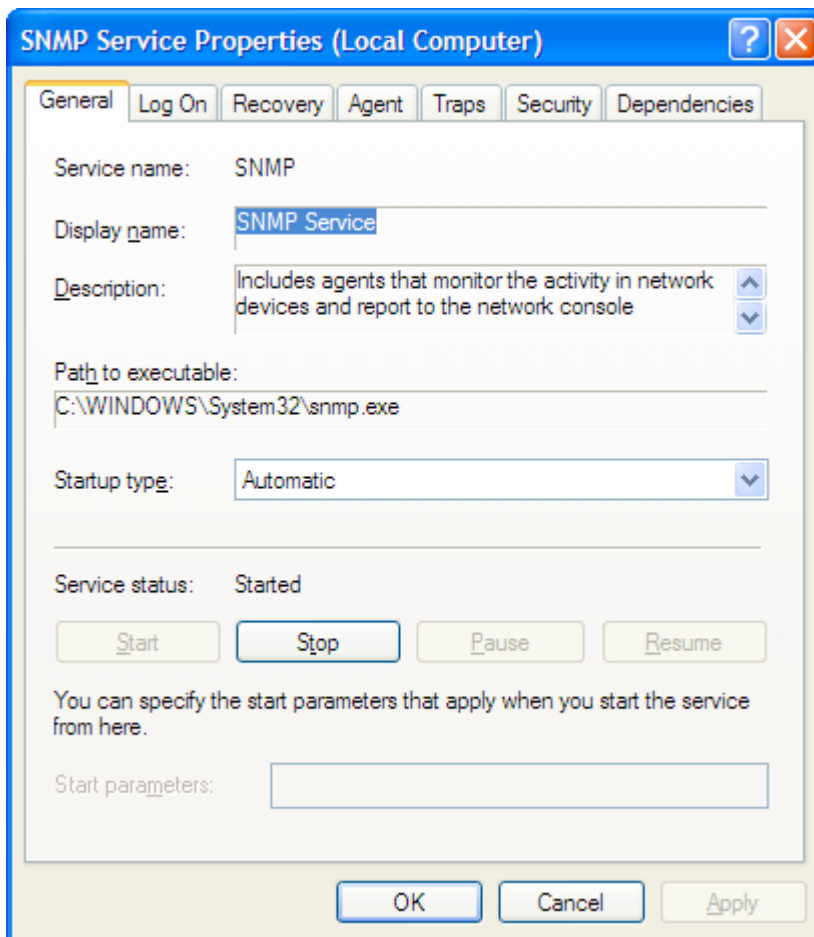


Figure 10 - SNMP Service Properties

5. On the **General** tab, to ensure that the SNMP service starts every time the host computer is restarted, select **Automatic** for the Startup Type. If you wish to start

the service manually each time, choose **Manual**.

6. Select the **Security** tab. You will be presented with a dialog similar to the one in Figure 11.

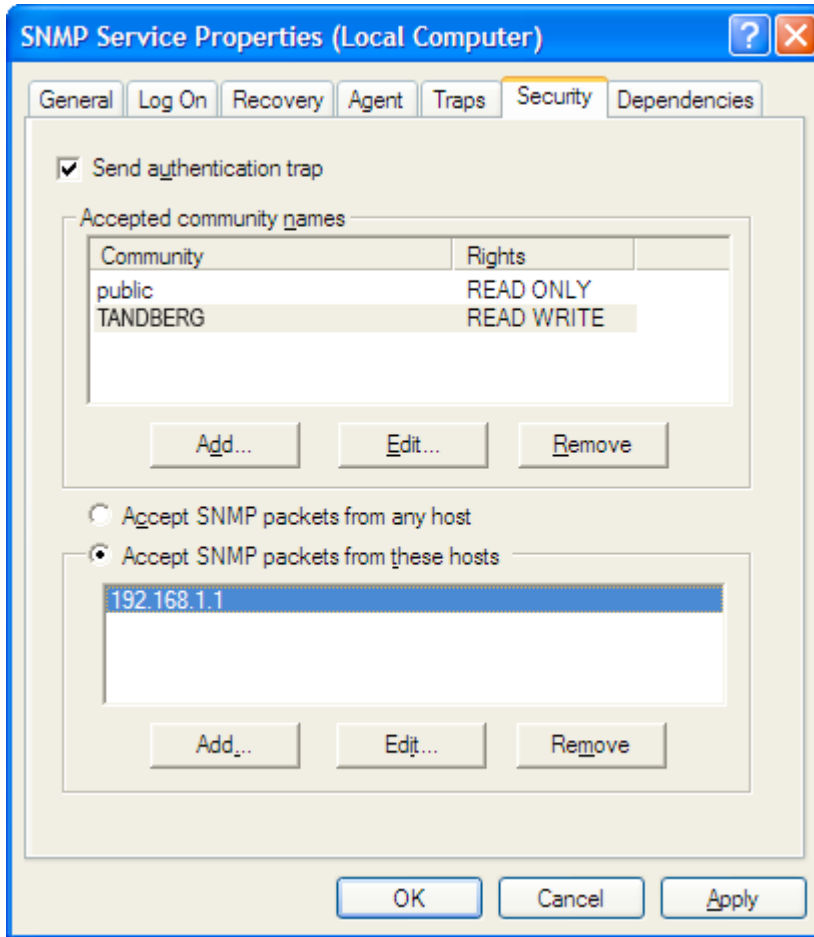


Figure 11 - SNMP Service Security Options

7. Configure the SNMP community. If this is the first time that you have installed the SNMP service, you may already see an entry in the accepted community names labeled **public**.

Note: For security reasons, we recommend that you either remove the public entry or ensure that it is set to READ ONLY under the Rights column.

- To delete the entry, select it and click the **Remove** button.
- To modify the entry, select it and click the **Edit** button.

8. Choose an SNMP community name to use to monitor and manage this device from the FMS and add it to the list of accepted community names. To add a community name, click **Add**. You will be presented with the **SNMP Service Community** dialog as shown in Figure 12, where you can set the community name and access rights for the community.

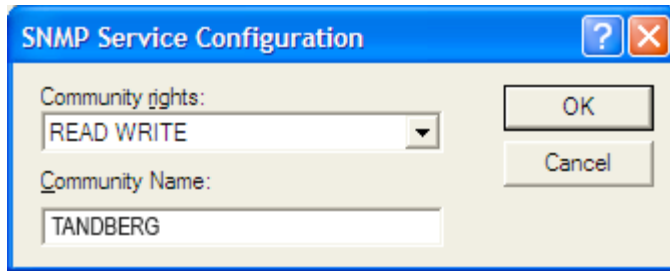


Figure 12 - SNMP Service Community

Note: In order to monitor the status of an endpoint, the community must be created with at least READ access. In order to apply software updates, the community must be created with READ/WRITE access.

Note: Take note of the community name that you choose here as it will be used later when adding this endpoint to the FMS database.

- Configure the list of permitted SNMP managers for the host computer. To do this, select **Accept SNMP Packets from these hosts** on the **Security** tab. To add the FMS server to the list of permitted hosts, click the **Add** button and enter the host name or IP address of the FMS server.

Note: By default, your host machine may already be accepting SNMP packets from all hosts. For security reasons, we recommend that you explicitly allow SNMP packets only from certain hosts.

Client Host Firewall Configuration

If Windows Firewall, third party firewall software, or another Internet security suite is running on the FA host machine, it may block SNMP packets from entering the system. You need to configure a firewall exception to allow UDP packets through on port 161.

Additional Configuration

No additional configuration is required provided the SNMP service is configured correctly. When the FA client software is installed, it sets up all necessary registry entries that are required for the FieldView SNMP agent to be loaded onto the system. However, if the SNMP service is removed and reinstalled later, these registry entries may need to be reapplied.

To apply the SNMP registry settings:

- Login to the FA host machine using an account with administrator privileges.
- Open the **C:\Program Files\TANDBERG\FA\Snp** folder and double-click the **SnpExtensionAgent.reg** file located in the folder.
- When prompted, click **Yes** to import the settings into the registry.
- Click **OK** when the import is complete.
- For the changes to take effect, either stop and restart the SNMP service through the **Administrative Tools**→**Services** dialog in the Control Panel or restart your computer.

Remote Monitoring Without the FMS Service

FA installations come with an SNMP Management Information Base (MIB) that can be imported into any third party SNMP monitoring and management application. Refer to the documentation for your SNMP management software for more information.

The MIB is located in the **C:\Program Files\TANDBERG\FA\Snmp** folder.

Managing Devices

The FMS can be used to monitor the status of FieldView endpoints as well as apply software and configuration updates to those endpoints. In order to perform monitoring and managements tasks on an endpoint, the endpoint must first be added to the system. The endpoint must also be correctly configured to support remote management, as described in **Preparing an Endpoint for Remote Management**.

Once an endpoint has been added, the FMS Service maintains it in a database of managed devices. This database persists even if the server is restarted, so endpoints only need to be added to the system once.

New devices can be added to the database in one of two ways: manually, by entering an IP address or hostname, or automatically through a discovery process.

Manually Adding a Managed Device

To manually add an endpoint to the system:

1. Choose **Managed Devices**→**Add Managed Device**. You will be presented with the **New Managed Device** screen, as shown in Figure 13.

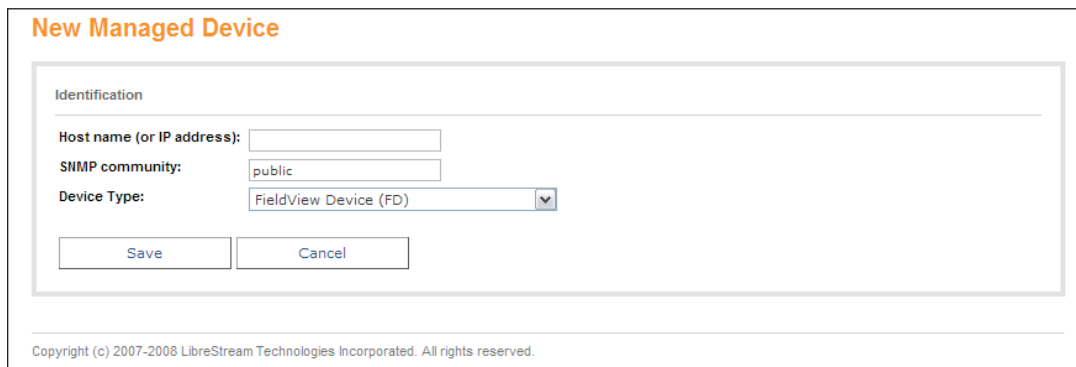


Figure 13 - Add a New Managed Device

2. Enter the information required to identify the device as listed in Table 4.

Table 4 – New Managed Device Identification

Host name / IP Address	<p>Enter the host name or IP address of the endpoint to monitor. This is used to identify the endpoint when performing monitoring or maintenance tasks. If an IP address is used, the FMS Service will attempt to resolve the host name of the endpoint once it has been added to the system.</p> <p>Note:</p> <p>The hostname you enter must not already exist in the FMS database.</p>
SNMP Community	<p>Enter the SNMP community name to be used to communicate with the device by SNMP. This should be the read/write community that you previously configured on the device.</p>
Device Type	<p>Choose whether the device is an FD or an FA endpoint. The type chosen determines what types of software configurations can be applied to the endpoint.</p>

3. Click the **Save** button to save your changes and add the endpoint to the system. You will be redirected to the **Managed Devices** page and the new endpoint appears in the list of managed devices.

Troubleshooting Adding a New Device

When a device is added to the database, the FMS Service will attempt to resolve the host name or IP address of the new device using the DNS lookup functionality built into Microsoft Windows.

If the server that the FMS resides on contains stale DNS records, it is possible that the resolved host name or IP address will be incorrect. In some cases, this may lead to either communication with a device other than the one that the administrator intended, or the inability to communicate with the device at all.

If the host name or IP address for a device appears incorrect, you should remove the device, clear the local DNS cache on the FMS server, and add the device again. On Windows XP Professional and Windows Server 2003 machines, this can be accomplished by going to a command prompt and entering the following command:

```
ipconfig /flushdns
```

This command will clear the local DNS cache on the FMS server, forcing the next DNS query for a device to go directly to the machine's configured DNS server.

Automatic Discovery of Managed Devices

Endpoints can also be added to the system automatically through a device discovery process. The FMS Service maintains a list of IP address ranges that it uses to search for new FieldView endpoints on the network. Periodically, the FMS Service will query every IP address included in each device discovery range to look for new endpoints. If a new endpoint that is not already present in the system is discovered, the endpoint will be added to the list of managed devices.

For an endpoint to be discovered, the following conditions must be met:

- The endpoint must be reachable by IP address on the network from the FMS server.
- The endpoint must have SNMP enabled and the FMS must be configured to discover devices using the endpoint's corresponding SNMP community.
- In the case of FA endpoints, the FA software client must be installed on the computer in order for the FMS to identify it as an FieldView endpoint.
- An endpoint with the same SNMP sysName or hostname as the one discovered must not already exist in the database.

View Existing Device Discovery Ranges

To view the list of current device discovery ranges in the system, choose **Managed Devices**→**Device Discovery**. You will be presented with a list of all of the device discovery ranges that were previously created, as shown in Figure 14.



Figure 14 - View Device Discovery List

Each item in the list displays the starting IP address of the range, the ending IP address of the range, and the SNMP community for the range. From here, you may perform a number of tasks on each item.

Modify opens a page allowing you to modify an existing discovery range. There, you can change all attributes of the existing discovery range.

Delete removes the discovery range from the system.

Creating a Device Discovery Range

To add an automatic discovery IP address range to the system:

1. Choose **Managed Devices**→**Device Discovery**. You will be presented with the **Device Discovery** screen, as shown in Figure 14.
2. Click the **Create New** button at the bottom of the device discovery list. You will be directed to an **Add Discovery Range** screen similar to the one in Figure 15.



Figure 15 - Add Device Discovery Range

3. Enter the information required to identify the discovery range listed in Table 5.

Table 5 - New Device Discovery Range Identification

Starting IP Address	Enter the first IP address in the discovery range.
Ending IP Address	Enter the final IP address in the discovery range.
SNMP Community	Enter the SNMP community to use when discovering devices for this range.

Note: To perform discovery on an IP address range using more than one SNMP community, add the same IP range multiple times with different community names.

- Click the **Save** button to save your changes and create the device discovery range. You will be redirected back to the **Device Discovery** page where the new range appears in the list.

Modify an Existing Device Discovery Range

To modify an existing device discovery range, open the **Device Discovery** page, locate the discovery range in the list, and click the **Modify** button.

Deleting a Device Discovery Range

To delete an existing device discovery range, open the **Device Discovery** page, locate the discovery range in the list, and click the **Delete** button.

Viewing Existing Managed Devices

To view a list of managed devices currently in the system, choose **Managed Devices**→**View Managed Devices**. You will be presented with a **Managed Devices** screen similar to the one shown in Figure 16.

Managed Devices

Device Administration :

[Add New Device](#) [Delete Selected](#) [Refresh Selected](#) [Check For Updates](#)

Assign Software / Configuration Groups :

[Software](#) [Configuration](#) [Users / Contacts](#) [Media Configurations](#)

[Refresh Table](#)

<input type="checkbox"/>	Name	Type	Status	Software Item	Version	(Update Group, Version)
Copyright (c) 2007-2008 LibreStream Technologies Incorporated. All rights reserved.						

Figure 16 - View Managed Devices List

The **Managed Devices** page contains a list of the endpoints currently managed by the FMS as well as their last known status. At regular polling intervals, the FMS Service queries each device in the database by the SNMP interface and records whether or not the device is online. It also updates the current hostname and IP address of each device, and retrieves the current versions of the software and configuration items on the endpoint. Each entry in the managed devices table will contain the information described in Table 6.

Table 6 - Managed Devices Table Columns

Name	The name used to identify the endpoint is displayed here. If the SNMP sysName of the endpoint has been successfully retrieved, it is used as the display name. Otherwise, the host name is displayed. Typically these two values are the same. Below the name of the device name, the current IP address of the endpoint is also shown.
Type	The type of device, either FD or FA .

Status	<p>The current status of the device is shown in addition to the last time the device was online. The possible status values are as follows:</p> <p>online – the endpoint is reachable by the FMS and is currently running.</p> <p>not responding – the endpoint is either not reachable by the network, is not turned on, or is not communicating for some other reason. Possible reasons could be that the SNMP community is configured incorrectly or the SNMP service (on FA endpoints) is not running.</p> <p>offline – the host is up and reachable by the network but the FieldView application software is not running. This only applies to FA endpoints.</p>
Software Item Version Update Group, Version	<p>These columns display the last known version of each type of software or configuration item installed on the FieldView endpoint. If the endpoint has been assigned to a software or configuration group, the latest version available for the group is displayed in parentheses. This is described further in Software / Configuration Updates.</p> <p>Note:</p> <p>If an endpoint's current software or configuration version does not match the version for the assigned group, the current version number is displayed in red.</p>

In addition to the information described above, action buttons are included that allow you to perform tasks on each endpoint in the table.

Details takes you to a page that allows you to view more detailed status for the endpoint and manage its assigned software and configuration groups.

Delete removes the device from the system.

Refreshing the Managed Devices Table

To refresh the list of managed devices and obtain a snapshot of the current state of the system from the FMS Service, you can either refresh the page in your browser or click **Refresh Table**, located at the top of the managed devices table.

Device Administration

At the top of the **Managed Devices** page there is a group of buttons that allow you to perform administrative tasks on the devices in the system. These are described in detail in Table 7. Note that some of the buttons perform the desired action only on devices that are currently selected. To select a device, click the checkbox in the managed devices table next to its name. You can also select or de-select all the devices in the table by clicking the checkbox in the title bar of the devices list.

Table 7 - Device Administration Commands

Add New Device	Clicking this button directs you to the New Managed Device page, where you can manually add a new device to the system.
----------------	--

Delete Selected	Use this button to remove all selected devices from the database.
Refresh Selected	Use this button to refresh the status of the selected devices. For performance reasons, this action is asynchronous, so results of the refresh are not displayed immediately in the table. You can refresh the table itself by clicking Refresh Table at the top of the managed devices table. You will know that a device's status has been refreshed when the Last Online time has been updated to match the current time of the server.
Check For Updates	Clicking this button tells the FMS Service to check for software and configuration updates on all selected devices. This is described further in Updating the Software/ Configuration of an Endpoint .

Software / Configuration Updates

In order to apply software and configuration updates to remote FieldView endpoints using the FMS system, you must assign endpoints to a software or configuration update group. An update group is a named software or configuration package that can be applied to an endpoint.

Assigning an endpoint to an update group does not immediately apply the corresponding software or configuration package to the device. Rather, the endpoint is marked as belonging to the assigned group allowing you to view, in the managed devices table, whether or not the software and configuration of each endpoint is up to date with respect to its assigned groups.

Applying a software or configuration package to an endpoint is a two-step process:

1. Assign the endpoint to the update group that corresponds to the package you wish to apply.
2. Check for updates on the endpoint. This will cause the endpoint to retrieve the latest versions of the software and configuration packages for each group it is assigned to and install them, if necessary.

Assigning an Update Group

Each FieldView endpoint can be assigned to multiple update groups: one for each type of software or configuration package that it supports. The available package types are outlined below.

Software packages are supported by both FD and FA endpoints. Assigning an endpoint to a Software group allows you to apply new versions of FD software or FA client software to remote endpoints. These are described further in the **Software Update Packages** section.

Configuration packages are supported by both FD and FA endpoints. Assigning an endpoint to a Configuration group allows you to push a configuration file to the endpoint. These are described further in **FD Configurations** and **FA Configurations**.

Users/Contacts packages are supported by both FD and FA endpoints. Assigning an endpoint to a Users/Contacts group allows you to apply users and shared contacts to a remote endpoint. These are described further in the **Users/Contacts** section.

Media Configurations packages are supported by FA endpoints only. Assigning an endpoint to a Media Configurations group allows you to apply video and audio profiles to a

remote FA. These are described further in the **Media Configurations** section.

To assign an endpoint to a particular update group:

1. Choose **Managed Devices** → **View Managed Devices**.
2. Select the devices that you wish to configure from the list by clicking their corresponding checkboxes.
3. Locate the **Assign Software / Configuration Groups** section, above the managed devices table.
4. Click the button that corresponds to the type of group you wish to assign. For example, if you are assigning the devices to a Software group, click the **Software** button.

A list of available group names for the type of group you wish to assign appears in a list below the button, as shown in Figure 17.

Figure 17 - Assigning an Update Group

5. Click the name of the group that you wish to assign to the selected devices. The devices will be assigned to the selected group. The managed devices table shows the name of the assigned group, as well as the current version number of the group for each of the selected devices. If a device is out of date, the current version number for the device is shown in red, as shown in Figure 18.

<input type="checkbox"/>	Name	Type	Status	Software Item	Version	(Update Group, Version)	
<input type="checkbox"/>	FD000B6B0BA723 192.168.1.137	FD	online Last online: 3/3/2008 9:59:20 AM	Software : Configuration : Users / Contacts :	3.62.0.0 Unknown Unknown	(FD 3.58, 3.58.0.0)	details

Figure 18 - A Device Requiring an Update

Note: The assigned groups for each endpoint are persistent in the FMS Service database.

Removing an Endpoint from an Update Group

To remove an endpoint from an update group, choose **[None]** when configuring the corresponding group name. Newly added devices have their configurations groups set to **[None]**.

Updating the Software/Configuration of an Endpoint

Once an endpoint is assigned to an update group, you can see in the **Managed Devices** table whether or not it is out of date. If an endpoint is out of date, you can check for updates for all assigned update groups.

To check for updates:

1. Choose **Managed Devices** → **View Managed Devices**.

2. Select the devices that you wish to update from the list by clicking their corresponding checkboxes.
3. Click the **Check for Updates** button located in the **Device Administration** section above the managed devices table. This causes the FMS Service to request that all selected devices check each configured update group for newer versions of software/configurations. If new versions exist, the endpoints download and apply the packages as necessary.
4. To see whether or not a device was updated successfully, refresh the managed devices table. If the software or configuration was applied correctly, the version numbers in the table matches the newly installed version.

Note: Only the version number of an update package is used to determine if an endpoint's configuration or software is out of date. The group name is used for display and identification purposes only, and is not a factor when an endpoint is checking for updates. In other words, an endpoint will not be able to distinguish between two differently named configuration packages of the same type if they also have the same version number.

When administering different groups of configurations, we therefore recommended that you assign a different major or minor version number for each configuration package that you create. This way, an endpoint will be able to correctly update its configuration when switching between update groups.

Example:	Warehouse Contacts	Internal Contacts
	2.0.0.1	3.0.0.1

Note: In order for a configuration or software update to succeed, the following conditions must be met:

- The device must not already be performing an update.
- The device must not be in a session or a call.
- If the device is an FD, it must be running on external power.

Note: To view a more detailed status of the last attempted check for updates, you can click the **details** link next to an endpoint in the **Managed Devices** table. See the **Viewing and Modifying an Existing Endpoint** section for more information.

Viewing and Modifying an Existing Endpoint

To modify an existing FieldView endpoint, locate it in the **Managed Devices** table and click its corresponding **details** link. You will be taken to the **Device Details** screen, similar to the one shown in Figure 19.

Figure 19 - Managed Device Details

The **Device Details** screen shows the current status of the selected FieldView endpoint. There are three tabs on the screen that are used to switch between the **Identification**, **Software**, and **Status** areas of the **Device Details** screen.

Managing Device Details

Click the **Identification** tab to view and modify the information used to identify the FieldView endpoint, as described in Table 8.

The **Identification** tab may also contain device specific configuration options. For example, administrators can lock or unlock call licenses on FA endpoints.

Table 8 - Identification Information

Hostname	The hostname of the endpoint.
IP Address	The IP address currently being used to communicate with the device.
Device Type	The type of device, either FD or FA .
Status	The current status of the device (see Viewing Existing Managed Devices)
Last Online	The last time the device was detected as being online.
SNMP sysName	The name returned by a request for the MIB-II sysName variable. This value is used for display purposes to identify the device. If the device has never been successfully reached by SNMP, this field is blank.
SNMP Community	The SNMP community being used to communicate with the device.

The device type and the SNMP community can be modified using this screen. Change the values and click **Save Changes** to apply the values to the FMS Service.

Note: Changing the SNMP community value only changes the value that the FMS service uses to communicate with the device. It does not change the actual community currently

set on the endpoint. Changing the community on the device itself must be done either manually or through the application on an FD configuration package.

Note: To refresh the information shown on the **Identification** tab, you can either refresh the page in your browser or click the **Refresh** link, located at the top right of the tab.

Software / Configuration Updates

In addition to being able to modify an endpoint's identification information, you can also apply software and configuration updates from the **Device Details** page. On the **Software** tab, you will see the list of software and configurations installed on the endpoint, the version numbers of each item, and the associated update groups that are assigned for each type of package, as shown in Figure 20.

Details for Device FD000B6B0BA723

Identification Software Status Refresh

Software Item	Version	Update Group (Version)
Software:	3.54.0.0	FD 3.57 (3.57.0.0)
Configuration:	1.0.0.1	[None]
Users / Contacts:	Unknown	[None]

Save Changes Check For Updates

Software / Configuration Update Status

Last Update Attempt: 1/4/2006 5:51:13 PM
Last Update Status: Successful

Figure 20 - Managed Device Software

Performing software and configuration updates from the **Device Details** page follows a similar process to updating from the managed devices table. Select the desired update groups from the corresponding drop down menus and click **Save Changes** to apply them to the device. To update an endpoint, click the **Check For Updates** button. This checks for updates on the endpoint.

If an endpoint is online, the status of the last update check performed on the endpoint is shown in the **Software / Configuration Update Status** section. The time of the last attempted update is shown, as well as the status of the last attempted update. The status will be one of those listed in Table 9.

Note: The last update time is the local time of the endpoint being monitored.

Table 9 - Last Update Status Description

Successful	The endpoint successfully detected, downloaded, and installed updated software and configurations.
Failed	Updates were detected, but one or more of them failed to either download or install. If there is more information regarding the reason for the failure, it is displayed as well.
No Updates Found	<p>The endpoint did not detect a newer version of software or configurations, either because the software on the endpoint was already up to date or the endpoint failed to detect the latest version of software from the FMS server.</p> <p>Note:</p> <p>If an endpoint shows No Updates Found after a check for updates, and the version numbers on the endpoint do match those in the assigned update groups, it is likely that there was a communication problem between the endpoint and the FMS server. If repeated attempts to update also fail, ensure that the Base Website URL for the FMS server is set correctly under Options→FMS Service Settings and that incoming HTTP requests from the endpoint are not blocked by any firewall software.</p>
Unknown	This is typically shown when a device has not previously attempted any updates.

Viewing Endpoint Status

The **Status** tab on the **Device Details** page displays the full list of an endpoint's software and configuration information, hardware information (FD only), and the details regarding the current session and media stream.

To view the current status of an endpoint, open the **Device Details** page and select the **Status** tab. You will be presented with a **Details for Device** screen similar to the one shown in Figure 21.

Details for Device FD000B6B0BA723

Identification Software **Status**

[Retrieve Status](#)

Software Versions

FD:	3.54.0.0
Application:	1.1.2952.28467
OS:	3.54.0.0
Monitor:	1.20.0.0
MCU:	2.14.0.0
Splash Screen:	Unknown

Registry Configuration: 1.0.0.1
Configuration: 1.0.0.1
Core Settings: 1.0.0.1
Preferred Networks: 1.0.0.1

Hardware

Device Name:	FD000B6B0BA723
Part Number:	200024
Board Number:	Version not available

Session

Status:	Disconnected
---------	--------------

Media Stream

No currently active media streams

Figure 21 - Managed Device Status

When the **Status** tab is first loaded, the status information is not displayed. To retrieve and display the current status of the endpoint, click the **Retrieve Status** link. This will send a request to the FMS Service for the current state of the endpoint by SNMP.

Note: If the FMS Service cannot retrieve the status of the device, an error message is shown in place of the endpoint's status. Failure to retrieve an endpoint's status could indicate a communication problem with the endpoint caused by either, incorrectly configured SNMP settings or heavy network traffic, which cause SNMP requests or responses to be lost.

FD Configurations

The FMS allows administrators to create FD configuration packages that can be applied to FD endpoints. An FD configuration package created by the FMS system is intended to be created offline and then applied to multiple FDs. As a result, items which are device specific, such as device name, static IP address and device specific SIP settings, cannot be configured by the FMS.

An FD configuration package actually consists of multiple configuration files. When viewing the currently installed version of the configuration package on the FD, you will notice four separate version numbers: Application Settings, Core Settings, Registry Settings, and Preferred Networks. When creating an FD configuration package, the same version number is applied to all four configuration files.

When an FD configuration package is applied to an FD endpoint, the following rules are applied:

- All configurations settings on the FD that also exist in the package will be replaced by the settings in the package.
- Any configuration settings that exist in the package that **do not** exist on the FD will be added to the FD.

The one exception to these rules is the management of wireless preferred networks, which are handled as follows:

- A preferred network that exists on the FD with the same SSID as one found in the package will be overwritten. Its position in the preferred networks list will not change.
- Preferred networks that **do not** exist on the FD, but exist in the package, will be added to the FD. They will be added to the top of the preferred networks list.
- None of the existing preferred networks on the FD will be deleted. They must be removed manually from the FD by an administrator.

Creating an FD Configuration Package

To create a new FD configuration package:

1. Choose **FD Configurations** → **Add FD Configuration Package**. You will be presented with the **New FD Configuration Package** screen as shown in Figure 22.

Figure 22 - Add FD Configuration Package

2. Enter the information that is required to identify the new FD configuration package in the **Identification** section, as shown in Table 10.

Table 10 - FD Configuration Package Identification

Group Name	Enter the name of the package. This name must be unique to all FD Configuration packages and be a valid Windows filename. This name is used to identify the package when assigning it to an FieldView endpoint.
Version	Enter the version of the FD Configuration package. This version number is used by endpoints to determine whether or not this package has already been installed. The default is 1.0.0.0.

3. In the **Configuration** section, create the actual FD configuration that can be applied to an FD endpoint. Navigate through the tabs and setup the desired configuration.

Note: For more information on FD configuration settings, refer to the **FieldView System Administration Manual**.

- Click the **Save** button to save your changes and create the FD Configuration package with default configuration settings.

View Existing FD Configuration Packages

To view the list of FD Configuration packages in the system, choose **FD Configurations** → **View FD Configuration Packages**. You will be presented with a list of all of the FD Configurations packages that were previously created, as shown in Figure 23. You can create a new FD configuration package by clicking the **Create New** button, located at the bottom of the list.



Group Name	Version	Last Modified	
Initial Configuration	2.0.0.0	17/12/2007 3:08:42 PM	save package modify delete
Warehouse Config	1.0.1.0	17/12/2007 3:08:54 PM	save package modify delete

[Create New](#)

Copyright (c) 2007-2008 LibreStream Technologies Incorporated. All rights reserved.

Figure 23 - View FD Configuration Package List

Each item in the list displays the name, the version number, and the last modified time of the package. From here, you may perform a number of tasks on each package.

Save Package allows you to download a ZIP file containing an FD configuration package. This ZIP file contains both the package manifest and the package archive. You can extract these two files to an SD card for manual installation of the package to FD endpoints.

Modify takes you to a page allowing you to modify an existing package. There, you can change the version number or name of an FD Configuration package, and modify the FD configuration in the package.

Delete removes the package from the system. Any endpoints that are currently assigned to the FD Configuration package will have their **Configuration** group set to **[None]**.

Modifying an Existing FD Configuration Package

To modify an existing FD configuration package, locate it in the list and click its corresponding **modify** link. You will be taken to a screen similar to the one shown in Figure 22.

The name of the package you are modifying is shown at the top of your screen. From here, you can change the name or version number of the FD configuration package, as well as modify the FD configuration itself. Modify the fields as required and click **Save** to save the changes.

Note: The version number of a FD configuration package must be changed whenever modifications are made to the package. If the version number is not incremented, an FD endpoint that is assigned to the package will not know that the configuration has changed and will fail to download and install it the next time the endpoint is asked to check for updates.

Maintaining the Wireless Preferred Networks List

The **Network** tab in **Configuration** section contains a list of wireless preferred networks in the current FD Configuration package, as shown in Figure 24.

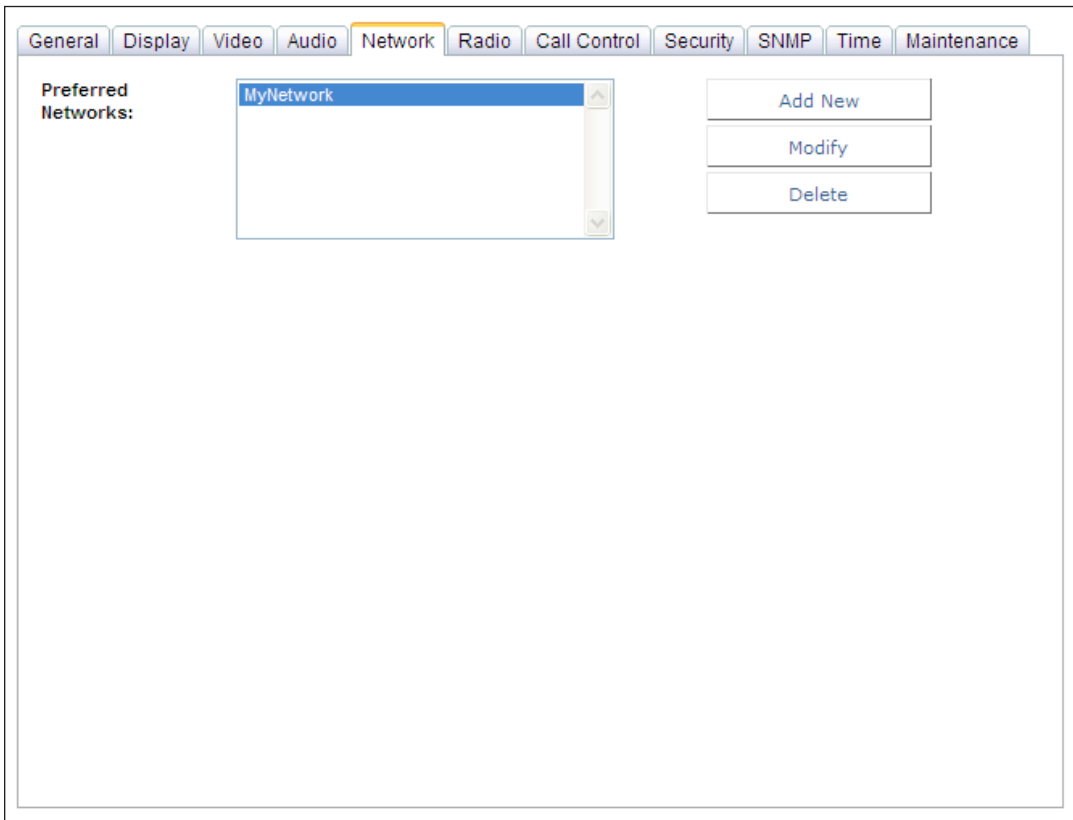


Figure 24 - View Preferred Networks List

Create a Wireless Preferred Network

To create a new wireless preferred network:

1. Click the **Add New** button, located to the right of the Wireless Preferred Networks table. You will be presented with a screen similar to the one in Figure 25.

General Display Video Audio **Network** Radio Call Control Security SNMP Time Maintenance

Network name (SSID): PrivateNetwork

Security

Authentication: Open

Encryption: Disabled

Network key:

Key index: 1

The key is provided automatically

IEEE 802.1x Authentication

IEEE 802.1x: Enabled

EAP Type: PEAP

User Certificate SHA1 Hash:

Validate server

Save Profile Cancel

Figure 25 - Add Preferred Network

- Fill in the details that identify the wireless preferred network. The available configuration settings are similar to what is found in the preferred network configuration on the FD. For more information on the available settings, refer to the **FieldView System Administration Manual**.
- Click **Save** to save your changes and return to the Wireless Preferred Networks list. The new preferred network is displayed in the list.

Note: The FMS system does not support remotely adding certificates to FD endpoints. If you are using IEEE 802.1x authentication, you can assign an existing certificate to a preferred network by filling in the **User Certificate SHA1 Hash** field. The hash must consist of HEX values separated by colons, similar to the following example:

```
69:b9:8d:ff:a1:c5:9b:8a:fc:71:0a:c9:04:8a:76:ce:4e:dd:06:13
```

If viewing a certificate in Internet Explorer, the required value can be found in the **Thumbprint** field of the **Details** tab.

Modify an Existing Wireless Preferred Network

To modify an existing wireless preferred network, select the **Network** tab, select the wireless network you wish to modify from the list of networks, and click the **Modify** button.

Deleting a Wireless Preferred Network

To delete an existing wireless preferred network, select the **Network** tab, select the wireless network you wish to delete from the list of networks, and click the **Delete** button

FA Configurations

The FMS allows administrators to create FA configuration packages that can be applied to FA endpoints.

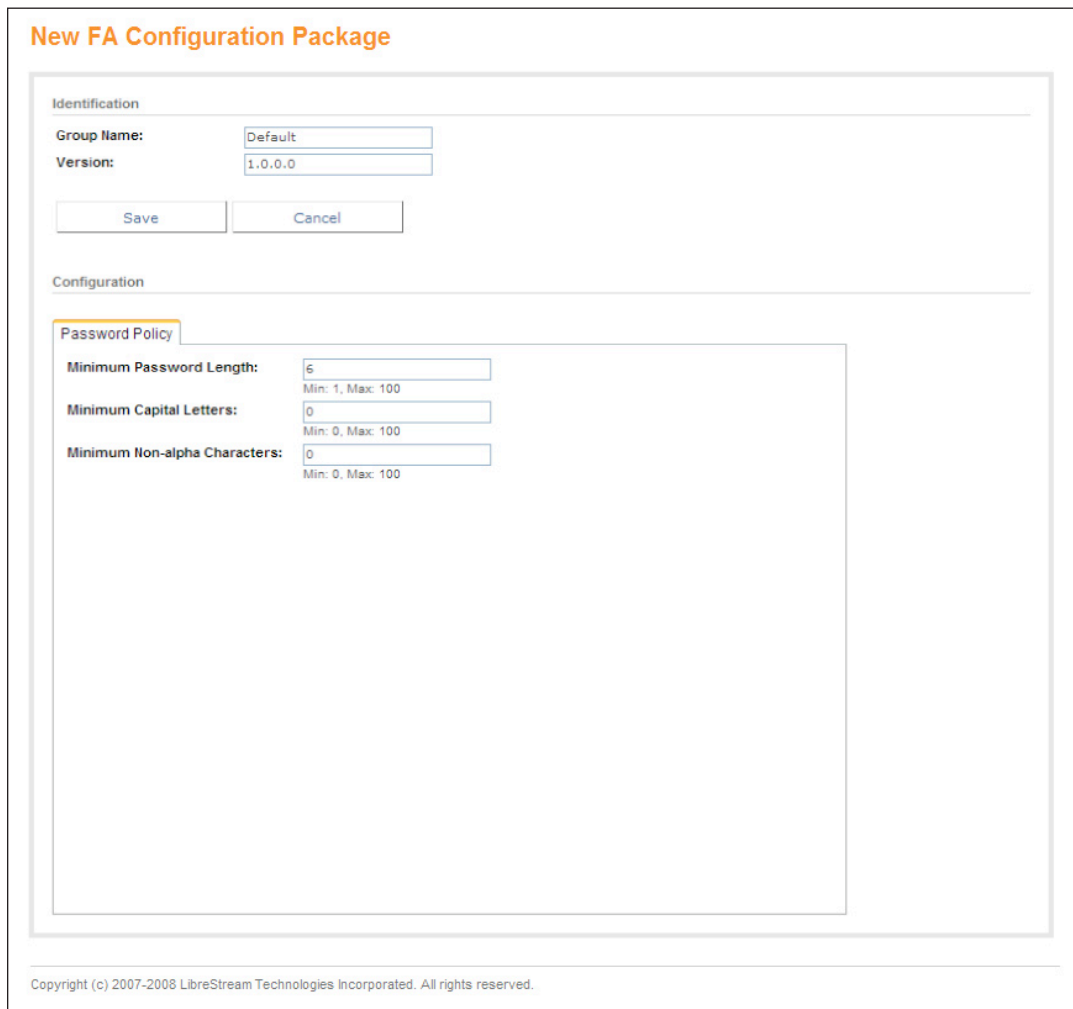
When an FA configuration package is applied to an FA endpoint, the following rules are applied:

- All configurations settings on the FA that also exist in the package will be replaced by the settings in the package.
- Any configuration settings that exist in the package that **do not** exist on the FA will be added to the FA.

Creating an FA Configuration Package

To create a new FA configuration package:

1. Choose **FA Configurations** → **Add FA Configuration Package**. You will be presented with the **New FA Configuration** screen as shown in Figure 26.



New FA Configuration Package

Identification

Group Name:

Version:

Configuration

Password Policy

Minimum Password Length:
Min: 1, Max: 100

Minimum Capital Letters:
Min: 0, Max: 100

Minimum Non-alpha Characters:
Min: 0, Max: 100

Copyright (c) 2007-2008 LibreStream Technologies Incorporated. All rights reserved.

Figure 26 - Add FA Configuration Package

- Enter the information that is required to identify the new FA configuration package in the **Identification** section, as shown in Table 11.

Table 11 - FA Configuration Package Identification

Group Name	Enter the name of the package. This name must be unique to all FA Configuration packages and be a valid Windows filename. This name is used to identify the package when assigning it to an FieldView endpoint.
Version	Enter the version of the FA Configuration package. This version number is used by endpoints to determine whether or not this package has already been installed. The default is 1.0.0.0.

- In the **Configuration** section, create the actual FA configuration that can be applied to an FA endpoint. Use the tabs to setup the desired configuration.

Note: For more information on FA configuration settings, refer to the **FieldView System Administration Manual**.

- Click the **Save** button to save your changes and create the FA Configuration package with default configuration settings.

View Existing FA Configuration Packages

To view the list of FA Configuration packages in the system, choose **FA Configurations** → **View FA Configuration Packages**. You will be presented with a list of all of the FA Configurations packages that were previously created, as shown in Figure 27. Additionally, you can create a new FA configuration package by clicking the **Create New** button located at the bottom of the list.

FA Configuration Packages			
Group Name	Version	Last Modified	
Warehouse	1.0.0.0	2/4/2008 3:36:57 PM	save package modify delete
<input type="button" value="Create New"/>			

Copyright (c) 2007-2008 LibreStream Technologies Incorporated. All rights reserved.

Figure 27 - View FA Configuration Package List

Each item in the list displays the name of the package, the version number of the package, and the last modified time of the package. From here, you may perform a number of tasks on each package.

Save Package allows you to download a ZIP file containing an FA configuration package. This ZIP file contains both the package manifest and the package archive. You can extract these two files to a standalone web server, which the FA client software can be configured to query.

Modify takes you to a page allowing you to modify an existing package. There, you can change the version number or name of an FA Configuration package, and modify the FA configuration in the package.

Delete removes the package from the system. Any endpoints that are currently assigned to the FA Configuration package will have their **Configuration** group set to **[None]**.

Modifying an Existing FA Configuration Package

To modify an existing FA configuration package, locate it in the list and click its corresponding **modify** link. You will be taken to a screen similar to the one shown in Figure 26.

The name of the package you are modifying is shown at the top of your screen. From here, you can change the name or version number of the FA configuration package, as well as modify the FA configuration itself. Modify the fields as required and click **Save** to save the changes.

Note: The version number of a FA configuration package must be changed whenever modifications are made to the package. If the version number is not incremented, an FA endpoint that is assigned to the package will not know that the configuration has changed and will fail to download and install it the next time the endpoint is asked to check for updates.

Users/Contacts Packages

The FMS allows administrators to create Users/Contacts packages. You can keep and maintain a centrally located list of users and shared contacts that can be distributed across multiple FieldView endpoints.

When a Users/Contacts package is applied to an FieldView endpoint, the following rules are applied:

- Any users that exist in the endpoint's directory that **do not** exist in the package will be deleted from the endpoint.
- Any users that exist in the endpoint's directory that **do** exist in the package will be modified to match the settings in the package. The passwords for each user on the endpoint will not be changed, regardless of the contents of the package. In addition, all personal contacts for existing users will be maintained.
- Any users that **do not** exist in the endpoint's directory that **do** exist in the package will be added to the endpoint's directory.
- The list of shared contacts on the endpoint will be replaced entirely with the contents of the package.

Creating a New Users/Contacts Package

To create a new Users/Contacts package:

1. Choose **Users / Contacts** → **Add Users / Contacts Package**. You will be presented with a **New Users / Contacts Package** screen similar to the one in Figure 28.

New Users / Contacts Package

Identification

Group Name:

Version:

Copy From: ▾

Password Policy

Minimum Length:
Min: 1, Max: 64

Minimum Capital Letters:
Min: 0, Max: 64

Minimum Non-alpha Characters:
Min: 0, Max: 64

Copyright (c) 2007-2008 LibreStream Technologies Incorporated. All rights reserved.

Figure 28 - Add Users/Contacts Package

2. Enter the information that is required to identify the new Users/Contacts package in the **Identification** section, as shown in Table 12.

Table 12 - Users/Contacts Package Identification

Group Name	Enter the name of the package. This name must be unique to all Users/Contacts packages and be a valid Windows filename. This name is used to identify the package when assigning it to an FieldView endpoint.
Version	Enter the version of the Users/Contacts package. This version number is used by endpoints to determine whether or not this package has already been installed. The default is 1.0.0.0.
Copy From	If you have existing Users/Contacts packages in the system, you can copy the users and contacts from an existing file by selecting it from the list.

3. Enter the password policy for the Users/Contacts package by filling in the required fields in the **Password Policy** section as described in Table 13.

Table 13 - Password Policy Settings

Minimum Length	Enter the minimum length of user passwords for the package.
Minimum Capital Letters	Enter the minimum number of capital letters required for user passwords.
Minimum Non-alpha Characters	Enter the minimum number of non-alpha characters required for each user password.

4. Click the **Save** button to save your changes and create the Users/Contacts package.

View Existing Users/Contacts Packages

To view the list of Users/Contacts files in the system, choose **Users / Contacts** → **View Users / Contacts Packages**. You will be presented with a list of all the Users/Contacts packages that were previously created, as shown in Figure 29. Additionally, you can create a new Users/Contacts package by clicking the **Create New** button, located at the bottom of the list.

Users / Contacts Packages					
Group Name	Version	Last Modified	# Users	# Contacts	
LibreStream Contacts	1.0.0.0	17/12/2007 3:06:58 PM	1	1	save package export to file modify delete
North American Contacts	1.0.0.0	17/12/2007 3:09:51 PM	1	0	save package export to file modify delete

Copyright (c) 2007-2008 LibreStream Technologies Incorporated. All rights reserved.

Figure 29 - View Users/Contacts Package List

Each item in the list displays the name of the package, the version number of the package, the last modified time of the package, and the number of users and contacts currently configured in the package. From here, you may perform a number of tasks on each package.

Save Package allows you to download a ZIP file containing a Users/Contacts package. This ZIP file contains both the package manifest and the package archive. You can extract these two files to an SD card for manual installation of the package to FD endpoints or to a standalone web server, which the FD or FA client software can be configured to query.

Export to File allows you to download an encrypted version of the Users/Contacts XML file for a package. This file can be imported into both FA and FD endpoints without using the software update interface.

Modify takes you to a page that allows you to modify an existing package. There, you can change the version number or password policy of a Users/Contacts package, and add users and shared contacts to the package.

Delete removes the package from the system. Any endpoints that are currently assigned to the Users/Contacts package will have their Users/Contacts group set to **[None]**.

Modifying an Existing Users/Contacts Package

To modify an existing Users/Contacts package, locate it in the list and click its corresponding **modify** link. You will be taken to a screen similar to the one shown in Figure 30.

Modify Users / Contacts Package TANDBERG Contacts

Identification

Group Name:

Version:

Password Policy

Minimum Length:
Min: 1, Max: 64

Minimum Capital Letters:
Min: 0, Max: 64

Minimum Non-alpha Characters:
Min: 0, Max: 64

Import Users and Contacts

Users

Full Name	User Name	
The Administrator	admin	modify delete

Shared Contacts

Name	Address	Type
Bob Smith	bob@192.168.1.100	Camera modify delete

Figure 30 - Modify Users/Contacts Package

The name of the package that you are modifying is shown at the top of your screen. From this screen, you can change the name, version number, and password policy of the Users/Contacts package. Modify the fields as required and click **Save** to save the changes.

Note: The version number of a Users/Contacts package must be changed whenever new users or shared contacts are added to the package. If the version number is not incremented, FieldView endpoints that are assigned to the package will not know that it has changed and will therefore fail to download and install it the next time the endpoints are asked to check for updates.

Note: Since user passwords are stored using a non-reversible hash, there is no way to tell if existing passwords meet the new password policy. It is up to administrators to ensure that all passwords are changed accordingly if a stricter password policy is being applied to an existing package.

Maintaining the Users List

Below the **Identification** section is a list of users that are configured for a Users/Contacts package. The table displays the Full Name of the user, the User Name, and a list of actions that can be performed for the user.

Create a New User

To create a new user:

1. Click the **Create New User** link, located below the Users table. You will be presented with the **Create New User** screen, shown in Figure 31.

Modify Users / Contacts Package TANDBERG Contacts

Create New User

Identification

User Name:

Initial Password:

First Name:

Last Name:

Administrator

URI:

SIP Server

Enable SIP Registration

Address:

User Name:

Password:

Type: Digest

Figure 31 - Add New User

2. In the **Identification** section, fill in the fields necessary for defining the new user, as shown in Table 14.

Table 14 - New User Identification

User Name	Use the name by which the user will be known on the system. The user will enter this string of characters during login.
Initial Password	Enter the user's password. Users can change their own passwords once they log in. Note: If a user already exists on an endpoint to which this package is being applied, this password will be ignored in favor of the one already configured on the system,
First Name	Enter the user's preferred first name.
Last Name	Enter the user's surname.
Administrator	If the user needs administrative access, click this checkbox. Only administrators can set up new users.
URI	Enter the user's SIP registration ID as listed on your SIP server, e.g.: bob@sip.domain.com.

- In the **SIP Server** section, enter the SIP server information necessary for routing calls through to the user as described in Table 15.

Table 15 - User SIP Settings

Enable SIP Registration	Check to enable the SIP Server fields.
Address	Enter the IP address of the SIP server on which this user has been defined.
Username	Enter the user name for this user as it has been defined on the SIP server.
Password	Enter the SIP server password for Digest authentication. This is different from the user's password.
Type	Digest authentication is selected by default and cannot be changed.
Transport	Select TCP or TLS.

- Click **Save** to save the changes and return to the **Modify Users / Contacts Package** screen. The new user is displayed in the Users table.

For a more detailed explanation of managing users and user lists, refer to the **User and Contact Management** section in the **FieldView System Administration Manual**.

Modify an Existing User

To modify an existing user, locate it in the Users table and click the corresponding **modify** link. You will be directed to the **Modify User** screen where you can change any of the details for the user.

Deleting a User

To delete a user from the package, locate it in the Users table and click the corresponding **delete** link.

Maintaining the Contacts List

Below the Users section is a list of Shared Contacts that are configured for the Users/Contacts package. This table displays the Name, Address and Type of each contact, as well as a list of actions that can be performed on each contact.

Create a New Contact

To create a new contact:

1. Click the **Create New Contact** link, located below the Contacts table. You will be presented with the **Create New Shared Contact** screen, shown in Figure 32.

The screenshot shows a web form titled "Create New Shared Contact" within a larger context of "Modify Users / Contacts Package TANDBERG Contacts". The form has three input fields: "Name" with the value "John", "Address" with the value "john@192.168.1.123", and "Type" with a dropdown menu showing "MCD". At the bottom of the form are two buttons: "Save" and "Cancel".

Figure 32 - Add New Contact

2. In the **Identification** section, fill in the fields necessary for defining the new contact as described in Table 16.

Table 16 - New Contact Identification

Name	This is the display name that identifies the contact in the directory.
Address	Enter the URI for the contact.
Type	Select the endpoint type, FD or Computer, from the drop-down list.

3. Click **Save** to save the changes and return to the **Modify Users / Contacts Package** screen. The new contact is displayed in the Contacts table.

For a more detailed explanation of Shared Contacts, refer to the **User and Contact Management** section in the **FieldView System Administration Manual**.

Modify an Existing Contact

To modify an existing contact, locate it in the Contacts table and click the corresponding **modify** link. You will be directed to the **Modify Contact** screen where you can change any of the details for the contact.

Deleting a Contact

To delete a contact from the package, locate it in the Contacts table and click the corresponding **delete** link.

Importing Users and Contacts

Users and contacts can also be imported into an existing package by using the **Import Users and Contacts** interface. To import an XML file containing users and contacts:

1. Click the **Browse** button. You will be presented with a file selection dialog.
2. Choose an XML file containing the users and contacts to import. This can be any users and contacts file previously exported by an FA client application or FMS system.
3. Click **Import**. The users and contacts are imported into the package using the same rules that apply when installing the package on an FD.

Note: Importing a file will replace all of the users and contacts in the existing package with the ones in the imported file using the rules described in **Users/Contacts Packages**.

Media Configurations

The FMS allows administrators to create Media Configuration packages that can be applied to FA software client endpoints. A media configuration defines a set of audio and video properties for a particular media stream.

When a Media Configuration package is applied to an FA software client endpoint the following rules are applied:

- Any configurations present on the endpoint with the same name as a profile in the package will be replaced with the settings defined in the package.
- Any configurations in the package that **do not** exist on the endpoint will be added to the endpoint.
- Any configurations on the endpoint that **do not** exist in the package will be maintained. It is up to the administrator of a particular endpoint to remove unwanted configurations manually.

Creating a New Media Configuration Package

To create a new Media Configuration package:

1. Choose **Media Configurations** → **Add Media Configuration**. You will be presented with the **New Custom Media Configuration Package** screen as shown in Figure 33.

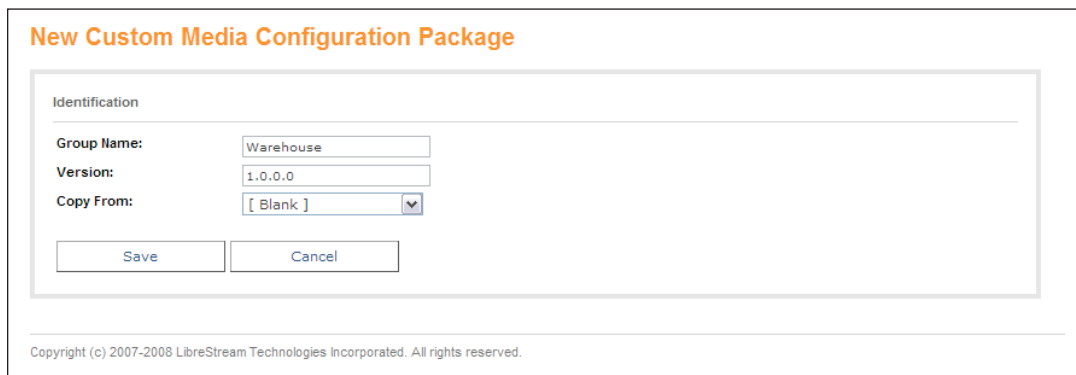


Figure 33 - Add Media Configuration Package

2. Enter the information that is required to identify the new Media Configuration package in the **Identification** section shown in Table 17.

Table 17 - Media Configuration Package Identification

Group Name	Enter the name of the package. This name must be unique to all Media Configuration packages and be a valid Windows filename. This name is used to identify the package when assigning it to an FA endpoint.
Version	Enter the version of the Media Configuration package. This version number is used by endpoints to determine whether or not this package has already been installed. The default is 1.0.0.0.

Copy From	If you have existing Media Configuration packages in the system, you can copy the individual configurations from an existing package into the new package by selecting it from the list.
-----------	--

- Click the **Save** button to save your changes and create the Media Configuration package.

View Existing Media Configuration Packages

To view the list of Media Configurations packages in the system, choose **Media Configurations** → **View Media Configurations**. You will be presented with a list of all the of Media Configuration packages that were previously created, as shown in Figure 34. You can create a new Media Configuration package by clicking the **Create New** button located at the bottom of the list.

Media Configuration Packages			
Group Name	Version	Last Modified	# Configurations
Intranet	1.0.0.0	17/12/2007 3:15:02 PM	0
Warehouse	2.0.0.0	17/12/2007 3:15:06 PM	1

[save package](#) [modify](#) [delete](#)
[save package](#) [modify](#) [delete](#)

Figure 34 - View Media Configuration Packages

Each item in the list displays the name of the package, the version number of the package, the date and time that the package was last modified, and the number of media configurations currently configured in the package. From here, you may perform a number of tasks on each package.

Save Package allows you to download a ZIP file containing a Media Configuration package. This ZIP file contains both the package manifest and the package archive. You can extract these two files to a standalone web server, which the FA client software can be configured to query.

Modify takes you to a page allowing you to modify an existing package. On this page, you can change the version number or name of a Media Configuration package, and add new configurations to the package.

Delete removes the package from the system. Any endpoints that are currently assigned to the Media Configurations package will have their Media Configuration group set to **[None]**.

Modifying an Existing Media Configuration Package

To modify an existing Media Configuration package, locate it in the list and click its corresponding **Modify** link. You will be taken to a screen similar to the one shown in Figure 35.

Modify Media Configuration Package Intranet

Identification

Group Name:

Version:

Configurations

Custom Profile Name

Low Bitrate [modify](#) [delete](#)

Figure 35 - Modify Media Configuration Package

The name of the package that you are modifying is shown at the top of your screen. From here, you can change the name or version number of the Media Configuration package. Modify the fields as required and click **Save** to save your changes.

Note: The version number of a Media Configuration package must be changed whenever new configurations are added to the package. If the version number is not incremented, FA software client endpoints that are assigned to the package will not know that it has changed and will fail to download and install it the next time the endpoint is asked to check for updates.

Maintaining the Media Configurations List

Below the **Identification** section is a list of configurations contained in the package. The table displays the name of the configuration and a list of actions that can be performed on each configuration.

Create a New Media Configuration

To create a new media configuration:

1. Click the **Create New** link located below the Configurations table. You will be presented with the **Create New Media Configuration** screen, shown in Figure 36.

Modify Media Configuration Package Intranet

Create New Media Configuration

Identification

Name:

Video

Device Type:

Resolution:

Frame Rate (fps):

Frame Sequence:

GOP:

Target Bitrate (kbps):
Min: 48, Max: 2500

Peak Bitrate (kbps):
Min: 48, Max: 2500

Audio

Enable Audio Configuration

Sample Size:

Sample Rate:

Separation:

Figure 36 - Create New Media Configuration

- In the **Identification** section, fill in the fields necessary to define the new configuration, as shown in Table 18.

Table 18 - New Media Configuration Identification

Name	The name used to identify the configuration in the FA client software. The names High Quality , Medium Quality , and Low Quality are reserved and cannot be used.
------	--

- In the Video section, fill in the video parameters for the configuration.
- In the Audio section, enable or disable the configuration of audio parameters by selecting the **Enable Audio Configuration** checkbox. If enabled, fill in the desired audio parameters for the configuration.
- Click **Save** to save your changes and return to the **Modify Media Configuration Package** screen. The new configuration is displayed in the Configurations table.

For a more detailed explanation of the configurable video and audio parameters, refer to the **Media Configuration** section in the **FieldView System Administration Manual**.

Modify an Existing Media Configuration

To modify an existing configuration, locate it in the Configurations table and click the corresponding **modify** link. You will be directed to the **Modify Media Configuration** screen where you can change any of the details for the configuration.

Deleting a Media Configuration

To delete a configuration from the package, locate it in the Configurations table and click the corresponding **delete** link.

Software Update Packages

Software update packages cannot be created using the FMS system. When new versions of FA or FD software are available, they will be pre-packaged and distributed by TANDBERG. Administrators can then add software packages to the FMS system and apply them remotely to FieldView endpoints.

When a software update package is applied to a FieldView endpoint, the following rules are applied:

- For FD endpoints, if the version of any software component does not match the version in the package, it will be applied to the endpoint.
- For FA endpoints, only newer versions of the FA client software will be downloaded and installed.

View Existing Software Packages

To view a list of the current software packages available in the system, choose **Software Packages** → **View Software Packages**. You will be presented with the **Software Update Packages** screen shown in Figure 37.

Software Update Packages			
Group Name	Version	Items	Comments
FD 3.57	3.57.0.0	3	Please see the release notes for more details.
FD 3.58	3.58.0.0	3	Please see the release notes for more details.

Packages can be added to the server manually by doing the following:

1. Create a new directory under C:\Documents and Settings\All Users\Documents\FMS\Packages\Software. The name of the directory will be the package name.
2. Copy the relevant package file and associated manifest XML file (if not already included in the package) to the newly created directory.

Figure 37 - View Software Packages

Each item in the list displays the name of the package, the version number of the package, the number of installable items in the package, and any comments contained in the package manifest.

Adding a New Software Package

To add a new software package to the system, it must be copied to the FMS software package repository.

To add a new software package:

1. In Windows Explorer, open the FMS software package repository by going to the following folder:
C:\Documents and Settings\All Users\Documents\FMS\Packages\Software\
2. Create a new folder in the ...Software folder to hold your new software package. The name you choose here is the name that will appear under **Group Name** in the software update packages list. We recommend that you choose a name that reflects the type of software (FA or FD) and version number for easy identification

when applying the update to an endpoint. For example, you could create a folder named **FD_4.0.0**.

- Copy the manifest.xml and the associated package ZIP file that you received from TANDBERG to the newly created folder as shown in Figure 38. It is important that you do not rename the package file as it is referenced by name within the manifest.

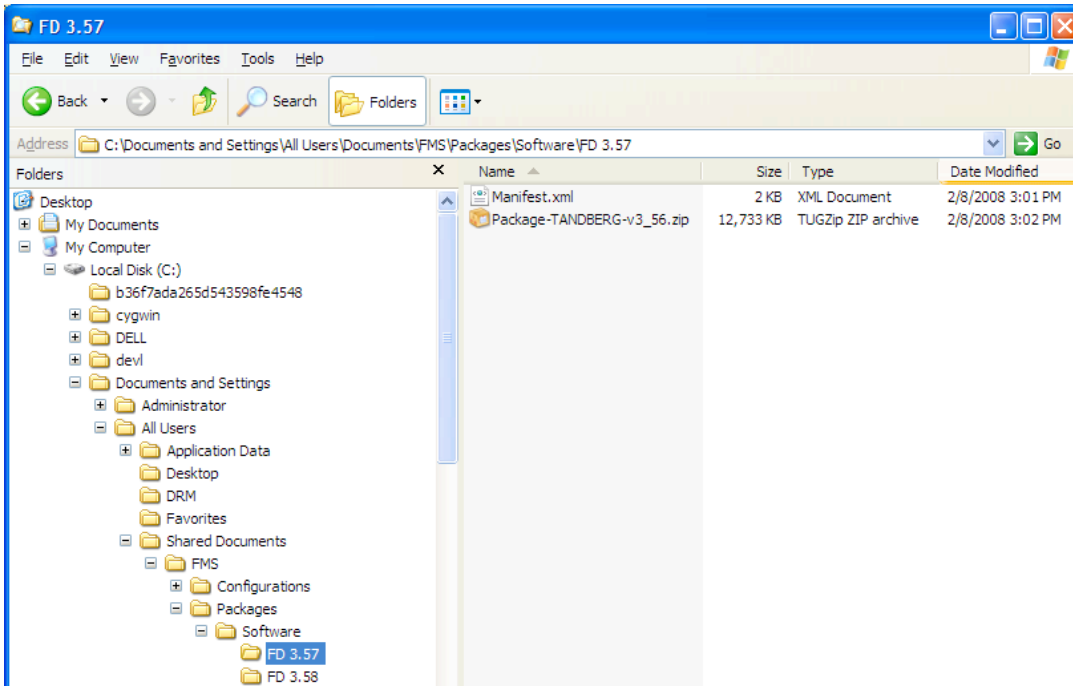


Figure 38 - Adding a New Software Package

- In the FMS User Interface, choose **Software Packages** → **View Software Packages**. Your software package appears in the list and can now be assigned to FieldView endpoints.

Deleting an Existing Software Package

To remove a software package from the system, remove the corresponding folder from the FMS software repository located in the following folder:

C:\Documents and Settings\All Users\Documents\FMS\Packages\Software\

Note: We recommend that you create a backup of a software package before deleting it in case you need to apply the software to FieldView endpoint at a later time.

TANDBERG

Philip Pedersens vei 20, 1366 Lysaker, Norway

Telephone: +47 67 125 125

Fax: +47 67 125 234

Video: +47 67 126 126

E-mail: tandberg@tandberg.com