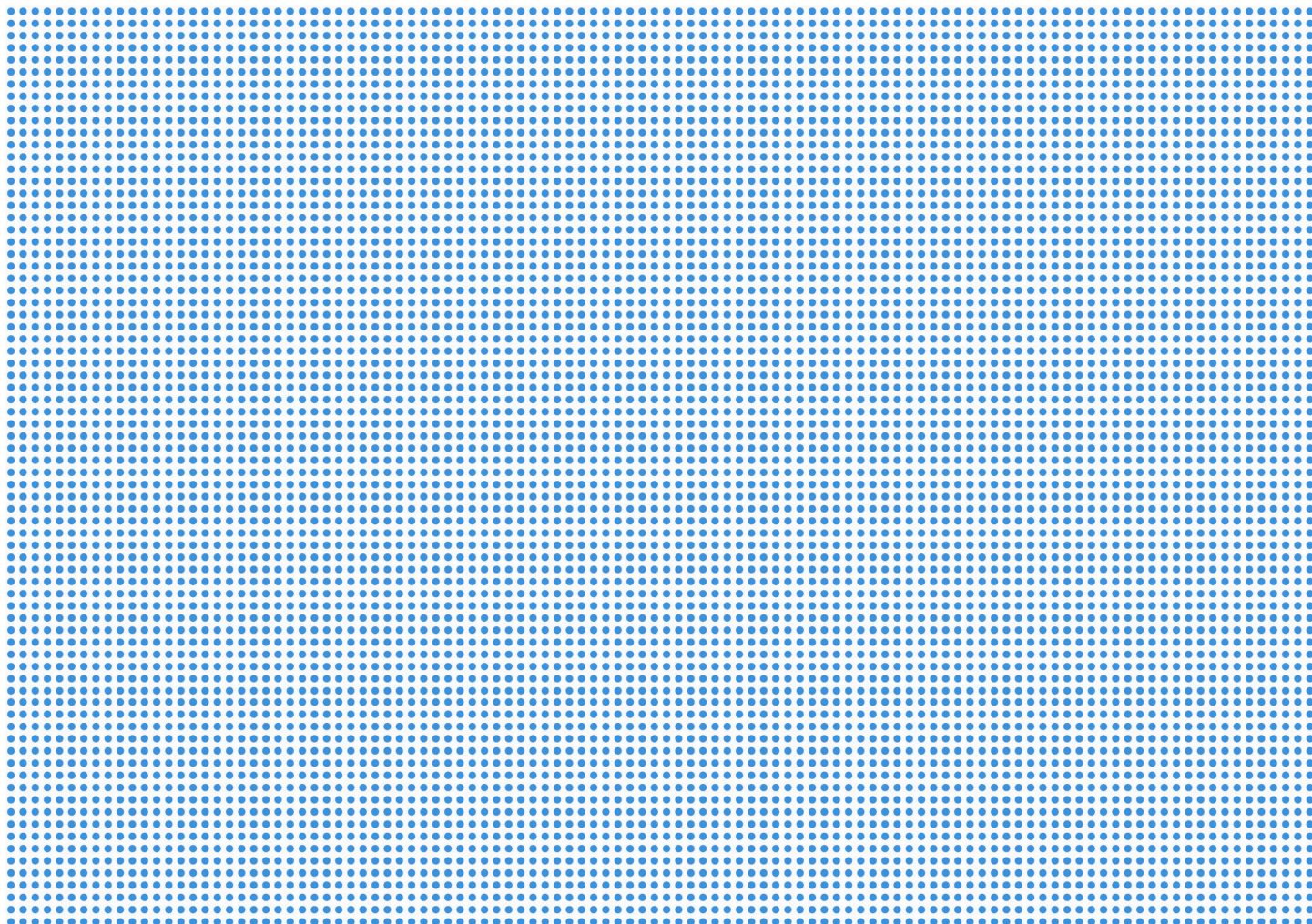


User Manual

Onsight Management Suite
Version 2.2



Another Innovation by [Librestream](#)



Librestream Onsite Management Suite

Doc #: 400075-05

July 2010

Information in this document is subject to change without notice.

Reproduction in any manner whatsoever without the written permission of Librestream is strictly forbidden.

Copyright © 2007–2010 Librestream Technologies Incorporated. All rights reserved.

Librestream, the Librestream logo, Onsite, Onsite Expert, Onsite Mobile, Onsite Enterprise, and Onsite Management Suite 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.

Name of Librestream Software:

Onsite Management Suite

Copyright Notice:

Copyright 2007 – 2010 Librestream Technologies Incorporated. All Rights Reserved.

Patents Notice: United States Patent # 7,221,386, together with additional patents pending in Canada, the United States and other countries, all of which are in the name of Librestream Technologies Inc.

Trademark Notice: Librestream, the Librestream logo, Onsite, Onsite Expert, Onsite Mobile, Onsite Enterprise, and Onsite Management Suite 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

1	Onsight Management Suite Overview.....	1
2	System Requirements	2
3	Installation.....	3
3.1	Server Firewall Configuration.....	4
3.2	Installation on Windows Server 2008 with IIS 7.0	5
4	Starting Onsight Management Suite for the First Time.....	8
4.1	Logging In	8
4.2	First Time Configuration.....	9
4.3	Activating Onsight Management Suite	11
5	Remote Management of Onsight Endpoints	14
5.1	Web Service Management.....	14
5.2	SNMP Management.....	16
6	Preparing Endpoints for Remote Management.....	19
6.1	Configuring Endpoints to use the Web Service Interface	19
6.2	Configuring Endpoints for SNMP Management	20
7	Adding Managed Endpoints	26
7.1	Identifying Managed Endpoints.....	26
7.2	Manually Adding a Managed Endpoint	26
7.3	Automatically Adding Managed Endpoints.....	29
8	Managing Endpoints	33
8.1	Managed Endpoints Table.....	33
8.2	Endpoint Groups.....	35
8.3	Modifying an Existing Endpoint.....	38
9	Software and Configuration Updates.....	43
9.1	Packages	43
9.2	Software Update Jobs.....	44
10	Onsight Device Configuration Packages.....	51
10.1	Creating an Onsight Device Configuration Package	51
10.2	View Existing Onsight Device Configuration Packages	53
10.3	Modifying an Existing Onsight Device Configuration Package.....	54
11	Onsight Expert Configuration Packages	55
11.1	Creating an Onsight Expert Configuration Package	55
11.2	View Existing Onsight Expert Configuration Packages.....	56
11.3	Modifying an Existing Onsight Expert Configuration Package	57
12	Users/Contacts Packages.....	58
12.1	Creating a New Users/Contacts Package.....	58
12.2	View Existing Users/Contacts Packages	59
12.3	Modifying an Existing Users/Contacts Package.....	59
12.4	Maintaining the Users List.....	60
12.5	Maintaining the Contacts List.....	63
12.6	Importing Users and Contacts	64
13	Media Configuration Packages	65

13.1	Creating a New Media Configuration Package	65
13.2	View Existing Media Configuration Packages	66
13.3	Modifying an Existing Media Configuration Package	67
13.4	Maintaining the Media Configurations List	67
14	Software Packages	69
14.1	Adding a New Software Package	69
14.2	View Existing Software Packages	70
14.3	Modifying an Existing Software Package	71
15	Statistics Collection	72
15.1	Enabling or Disabling Statistics Collection	72
15.2	Viewing Collected Statistics	73
15.3	Exporting Collected Statistics	75
15.4	Interpreting Statistics	76
15.5	Clearing Collected Statistics	80
16	Onsight Expert License Management.....	81
16.1	Onsight Expert Software Activation	81
16.2	Onsight Expert Release Keys	90
16.3	Onsight Expert Custom Installs.....	92
17	Configuration Access Control.....	96
17.1	Editing Configuration Access Control Files	96
17.2	Creating and Installing Configuration Access Control Packages	97
18	Maintenance	98
18.1	Backing up the Database	98
18.2	Restoring the Database	99
19	End User License Agreement.....	100
20	Librestream Contact Information	107

Figures

Figure 1 – Server Manager	5
Figure 2 – Add Roles Wizard	6
Figure 3 – Select Server Roles	6
Figure 4 – Select Role Services	7
Figure 5 – ASP.NET Role Services Confirmation	7
Figure 6 – Logging In to Onsight Management Suite	8
Figure 7 – General Settings	9
Figure 8 – Service Settings	10
Figure 9 – Web Service Settings	11
Figure 10 – Activation	12
Figure 11 – Manual Activation	13
Figure 12 – Activation Status	13
Figure 13 – Web Service Connection Settings	15
Figure 14 – Windows Components Wizard	21
Figure 15 – Management and Monitoring Tools	21
Figure 16 – SNMP Warning During Onsight Expert Setup	22
Figure 17 – SNMP Service Properties	23
Figure 18 – SNMP Service Security Options	24
Figure 19 – SNMP Service Community	25
Figure 20 – New Managed Endpoint Wizard	27
Figure 21 – SNMP Search Parameters	27
Figure 22 – New Managed Endpoint Identification	28
Figure 23 – View SNMP Discovery List	30
Figure 24 – Add SNMP Discovery Range	31
Figure 25 – Managed Endpoints	33
Figure 26 – Add Group	35
Figure 27 – Move Group	36
Figure 28 – Delete Group	37
Figure 29 – Move Selected Endpoints	38
Figure 30 – Endpoint Details Identification Tab	39
Figure 31 – Endpoint Details Software Tab	40
Figure 32 – Endpoint Details Update History Tab	41
Figure 33 – Endpoint Details Activation Tab	41
Figure 34 – Endpoint Details Status Tab	42
Figure 35 – Choose Update Job Details	45
Figure 36 – Select Endpoints	45
Figure 37 – Select Packages	46
Figure 38 – View Software Update Jobs	46
Figure 39 – Update Job Details	48
Figure 40 – Update Job History	50
Figure 41 – New Onsight Device Configuration Package	52
Figure 42 – Access Control Tab	53
Figure 43 – View Onsight Device Configuration Package List	54

Figure 44 – New Onsight Expert Configuration Package	55
Figure 45 – View Onsight Expert Configuration Package List.....	57
Figure 46 – New Users/Contacts Package	58
Figure 47 – View Users/Contacts Package List	59
Figure 48 – Modify Users/Contacts Package	60
Figure 49 – Create New User	61
Figure 50 – Create New Shared Contact	63
Figure 51 – New Media Configuration Package	65
Figure 52 – View Media Configuration Package List.....	66
Figure 53 – Modify Media Configuration Package.....	67
Figure 54 – Create New Media Configuration	68
Figure 55 – Add Software Package.....	69
Figure 56 – View Software Package List.....	70
Figure 57 - Statistics Settings	73
Figure 58 - View / Export Statistics	74
Figure 59 - Choose Endpoints	75
Figure 60 - Onsight Expert Activation Status	82
Figure 61 - Add Onsight Expert Activation Keys	83
Figure 62 - View Onsight Expert Activation Keys	84
Figure 63 – Select Onsight Experts.....	86
Figure 64 – Activation Conditions.....	86
Figure 65 – Select Activation Keys.....	87
Figure 66 - Confirm Activation Key Allocations	87
Figure 67 - Pending Activation Status	88
Figure 68 – Activation Job History.....	89
Figure 69 – Add Onsight Expert Release Keys	90
Figure 70 – View Onsight Expert Release Key List.....	91
Figure 71 –Custom Install Wizard	92
Figure 72 - Custom Install Remote Web Service Settings	93
Figure 73 - Custom Install Activation Settings.....	93
Figure 74 - Custom Install Release Key Settings	93
Figure 75 - Custom Install Export.....	94
Figure 76 – Sample Configuration Access Control File.....	96
Figure 77 - Services Control Panel	98

Tables

Table 1 – Installation Options.....	3
Table 2 – Windows Firewall Exceptions.....	4
Table 3 – Web Service Management Settings.....	16
Table 4 – SNMP Management Settings.....	17
Table 5 – Add New Managed Endpoint Methods.....	27
Table 6 – SNMP Search Parameters.....	27
Table 7 – New Managed Endpoint Identification.....	28
Table 8 – SNMP Discovery Configuration.....	30
Table 9 – New SNMP Discovery Range Identification.....	31
Table 10 – Managed Endpoints Table Columns.....	33
Table 11 – Managed Endpoints Actions.....	34
Table 12 – Endpoint Records.....	34
Table 13 – Supported Package Types.....	43
Table 14 – Update Job Settings.....	44
Table 15 – Update Jobs Table Columns.....	47
Table 16 – Update Jobs Actions.....	47
Table 17 – Update Job Endpoints Columns.....	49
Table 18 – Onsite Device Configuration Package Identification.....	52
Table 19 – Onsite Expert Configuration Package Identification.....	56
Table 20 – Users/Contacts Package Identification.....	58
Table 21 – New User Identification.....	62
Table 22 – User SIP Settings.....	62
Table 23 – User CUPS Settings.....	62
Table 24 – User FIPS Settings.....	62
Table 25 – New Contact Identification.....	63
Table 26 – Media Configuration Package Identification.....	65
Table 27 – New Media Configuration Identification.....	68
Table 28 – Software Package Identification.....	70
Table 29 – Statistics Filter Parameters.....	74
Table 30 – Call Records.....	76
Table 31 – Media Stream Records.....	78
Table 32 – Conference Records.....	79
Table 33 – Endpoint Event Records.....	79
Table 34 – Clear Statistics Filter Parameters.....	80
Table 35 – Onsite Expert Activation Status Table Columns.....	82
Table 36 – Onsite Expert Activation Status Table Actions.....	82
Table 37 – Onsite Expert Activation Keys Table Columns.....	84
Table 38 – Onsite Expert Activation Key Actions.....	84
Table 39 – Onsite Expert Activation Job Settings.....	85
Table 40 – Activation Conditions.....	87
Table 41 – Pending Activation Status Columns.....	88
Table 42 – Add Release Key Settings.....	90
Table 43 – Onsite Expert Release Key Actions.....	91

Table 44 – Release Key Import Options 91

Table 45 – Custom Install Release Key Actions..... 94

Table 46 – Access Control Levels..... 96

1 Onsight Management Suite Overview

Onsight Management Suite allows administrators to view the status of remote Onsight endpoints, create and apply system configurations and users/contacts lists, manage and apply remote software updates, maintain endpoint software licenses and collect endpoint usage statistics. Using Onsight Management Suite, administrators can efficiently manage and maintain groups of Onsight endpoints, including Onsight device and Onsight Expert endpoints.

Onsight Management Suite consists of three main software components:

- **Windows Service** – The Onsight Management Suite Service is a Windows Service, named **Librestream Onsight Management Suite**, which runs in the background on the server. The Windows Service is responsible for discovering new endpoints, the monitoring and management of endpoints using SNMP and deploying software and configuration updates. The Windows Service also maintains the Onsight Management Suite database, which stores the list of managed Onsight endpoints, software update and activation jobs, service settings and collected endpoint usage statistics.
- **Web Service** – The Onsight Management Suite Web Service is an ASP.NET web service. Remote endpoints can connect to the Web Service interface to periodically report their status, download and install any available software and configuration updates and retrieve assigned activation keys required for software activation. The Web Service is installed to Internet Information Services (IIS) under the **OnsightWebService** virtual directory, by default.
- **User Interface** - The Onsight Management Suite User Interface is an ASP.NET web application. The User Interface communicates with the Windows Service to allow an administrator to add and view managed endpoints, create configuration and users/contacts packages, create software update jobs, manage and maintain Onsight Expert software licensing and view and export reported endpoint usage statistics. The User Interface also acts as the web server from which endpoints download software and configuration update packages. The User Interface is installed to IIS under the **OnsightManagementSuite** virtual directory, by default.

2 System Requirements

The software is meant to be installed on a server with these minimum requirements:

Operating System	Windows Server 2003 SP2 (recommended) Windows Server 2008 SP1 ¹ Windows Server 2008 R2 Windows XP Professional SP2 (minimum) ²
Web Server	IIS 5.1 or higher
Processor speed	1 GHz (1.5 GHz recommended)
Disk space	Up to 120 MB required for initial installation (if Microsoft .NET Framework components are not already installed). Additional space is required for storage of software and configuration update packages and collected endpoint usage statistics.
Network	A wired 10/100 Ethernet port is recommended.

¹ Installation on Windows Server 2008 requires that your server be configured for the **Web Server (IIS)** role, with both the **ASP.NET** and **IIS 6 Management Compatibility** roles services installed. For more information, see the **Installation on Windows Server 2008 with IIS 7.0** section on page 5.

² Windows XP Professional SP2 allows only a limited number of simultaneous connections to IIS, and is therefore recommended only for smaller installations or in environments where software updates will be applied to only a few remote endpoints at a time.

3 Installation

→ To install Onsight Management Suite:



*If you are installing Onsight Management Suite on Windows Server 2008, please refer to **Installation on Windows Server 2008 with IIS 7.0** on page 5 to ensure that you have properly configured Internet Information Services (IIS).*

1. Insert the installation CD into your CD drive.
2. 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 **OnsightManagementSuite** directory on the CD, and run the **setup.exe** program.
3. At this time, you may be prompted to install a number of prerequisite programs such as the Microsoft .NET Framework. Simply follow the prompts as they appear, and re-boot the machine as required.
4. Once the prerequisites have been installed, the main Onsight Management Suite installer will appear. Follow the onscreen prompts to complete the installation process. A summary of the settings that you will be asked to configure during installation is shown in Table 1.

Table 1 – Installation Options

Setting	Description
Web Site	The IIS web site where the User Interface and Web Service will be installed. You will be prompted to choose from a list of available web sites on your server. The choice of web site will ultimately determine the URL that endpoints will use to access the Web Service interface and package server.
User Interface Application Pool	<p>The IIS application pool where the User Interface will be installed. You will be prompted to either choose from a list of available application pools under the chosen web site, or to create a new application pool named OMSUserInterfaceAppPool.</p> <p>It is strongly recommended that the User Interface and Web Service be installed to their own application pools.</p>
Web Service Application Pool	<p>The IIS application pool where the Web Service will be installed. You will be prompted to either choose from a list of available application pools under the chosen web site, or to create a new application pool named OMSWebServiceAppPool.</p> <p>It is strongly recommended that the User Interface and Web Service be installed to their own application pools.</p>
Installation Folder	<p>The folder where the Onsight Management Suite components will be installed.</p> <p>The default folder is C:\Program Files\Librestream Technologies\Onsight Management Suite.</p>
Configuration and Database Folder	The folder where the Onsight Management Suite configuration files, license file and database will be stored. If you are upgrading an existing version of Onsight Management Suite and change the Configuration and Database Folder setting, the installer will attempt to move your existing configuration files, license file and database to the specified folder.

	<p>The default folder is:</p> <ul style="list-style-type: none"> Windows XP / Windows Server 2003: C:\Documents and Settings\All Users\Application Data\MCA Windows Server 2008: C:\Program Data\MCA
Packages Folder	<p>The folder where software and configuration update packages will be stored. If you are upgrading an existing version of Onsite Management Suite and change the Packages Folder setting, the installer will not move your existing packages to the specified folder. Packages can be moved manually after the installation has completed.</p> <p>The default folder is:</p> <ul style="list-style-type: none"> Windows XP / Windows Server 2003: C:\Documents and Settings\All Users\Documents\Onsite Management Suite Windows Server 2008: C:\Users\Public\Documents\Onsite Management Suite
Service TCP Port	<p>The TCP port that the Windows Service will use to communicate with the User Interface and the Web Service. Once the Windows Service starts, it will begin 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.</p> <p>The default TCP port is 9090.</p>



The configured Configuration and Database Folder can be viewed after installation by navigating to **Options > General Settings** within the Onsite Management Suite User Interface; however, it cannot be changed without re-installing Onsite Management Suite.



The configured Packages Folder can be viewed or changed after installation by navigating to **Options > General Settings** within the Onsite Management Suite User Interface.



The configured TCP port can be viewed or changed after installation by choosing **Start > All Programs > Librestream Onsite Management Suite > Configure Onsite Management Suite Service**.

- When the installation completes, you will have the option of placing icons on your desktop or Quick Launch bar that can be used to launch the User Interface.

3.1 Server Firewall Configuration

If Windows Firewall or other third party firewall software is running on the server where you installed Onsite Management Suite, you may need to add firewall exceptions for the ports listed in Table 2.

Table 2 – Windows Firewall Exceptions

Name	Protocol	Port	Description
HTTP	TCP	80	Required if remote endpoints will access the package server or Web Service interface over HTTP. If your IIS configuration uses a port other than 80, ensure that you have allowed that port instead.
HTTPS	TCP	443	Required if remote endpoints will access the package server or Web Service interface over HTTPS. If your IIS configuration uses a port other than 443, ensure that you have allowed that port instead.

3.2 Installation on Windows Server 2008 with IIS 7.0

Installing Onsight Management Suite on Windows Server 2008 requires that the server first be properly configured to host ASP.NET web applications. In addition, Onsight Management Suite requires that the server be configured for IIS 6 Management Compatibility.

→ To install IIS 7.0 with ASP.NET support on Windows Server 2008:

1. Click **Start > All Programs > Administrative Tools > Server Manager**. The Server Manager dialog will appear, as shown in Figure 1.

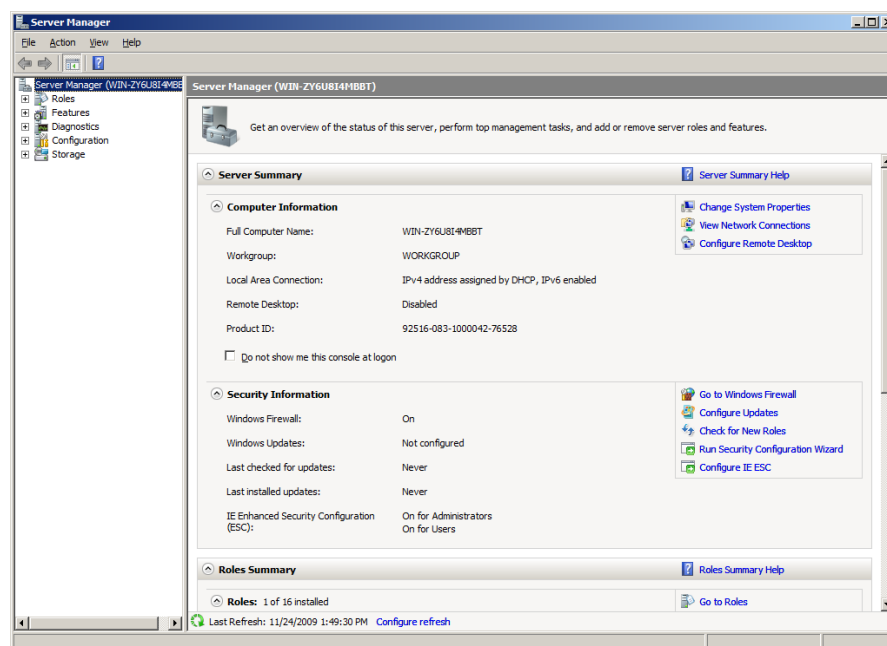


Figure 1 – Server Manager

2. Select the **Action > Add Roles** menu item to bring up the **Add Roles Wizard**, as shown in Figure 2.

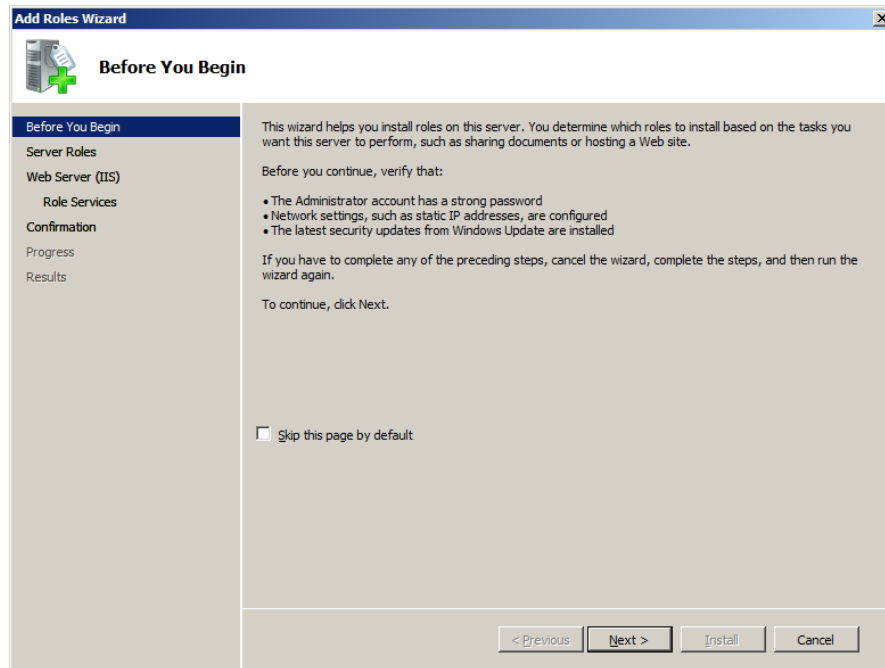


Figure 2 – Add Roles Wizard

3. Follow the prompts to the **Select Server Roles** step, and enable the **Web Server (IIS)** option in the list of available server roles, as shown in Figure 3.

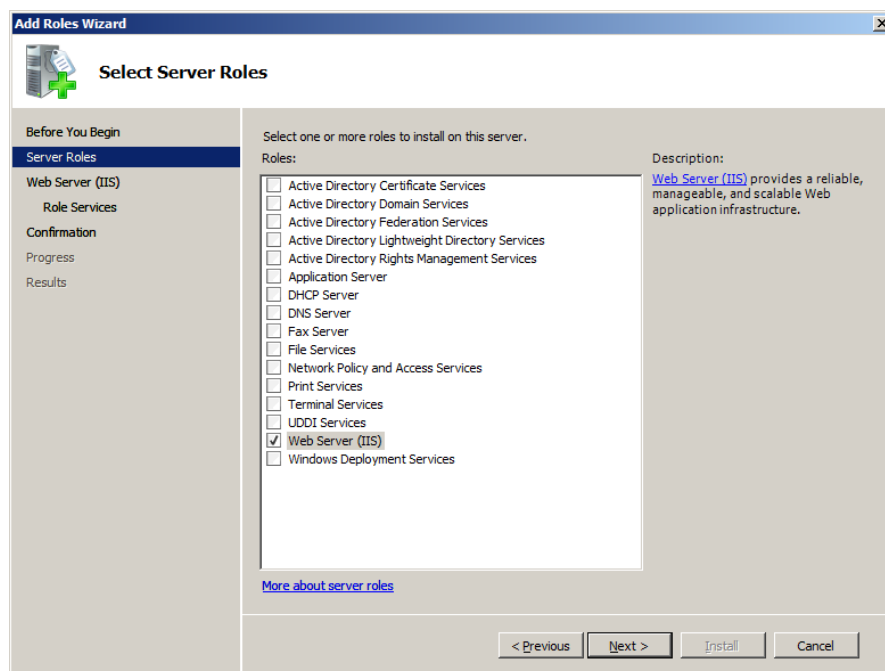


Figure 3 – Select Server Roles

4. Click the **Next** until you reach the **Select Role Services** page, as shown in Figure 4.

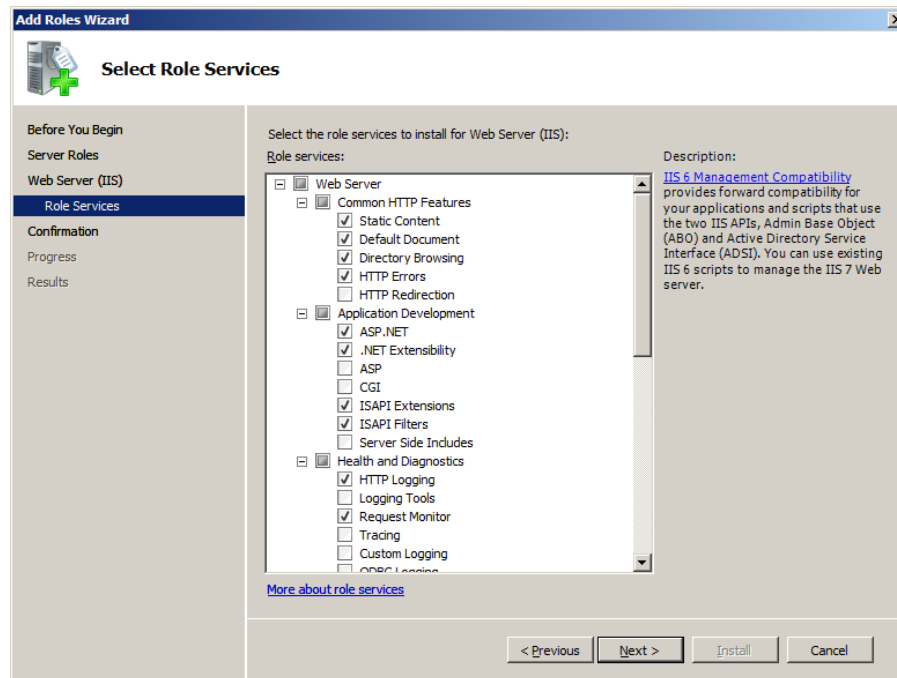


Figure 4 – Select Role Services

5. Some role services will already be checked off by default. Leave those role services selected.
6. Under the **Application Development** tree node, select the **ASP.NET** item to enable ASP.NET support on the server. You will be prompted to install additional role services that ASP.NET depends on, as shown in Figure 5. Click the **Add Required Role Services** button to add the necessary dependencies.

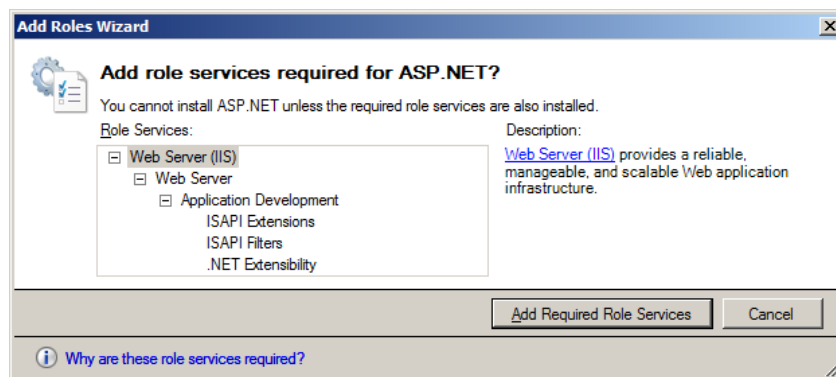


Figure 5 – ASP.NET Role Services Confirmation

7. Under the **Management Tools** tree node, select the **IIS 6 Management Compatibility** node. The role services under the **IIS 6 Management Compatibility** node will be selected automatically.
8. Click the **Next** button to proceed to the confirmation screen.
9. Click the **Install** button. The Web Server (IIS) role and required role services will be installed on your server.
10. When the installation completes, click the **Close** button to complete the wizard.

4 Starting Onsight Management Suite for the First Time

4.1 Logging In

To login to Onsight Management Suite, launch the User Interface by choosing **Start > All Programs > Librestream Onsight Management Suite > Login to Onsight Management Suite**, or by double-clicking the Onsight Management Suite icon that was installed to your desktop. This starts the User Interface in your default web browser and you will be presented with the login screen shown in Figure 6.

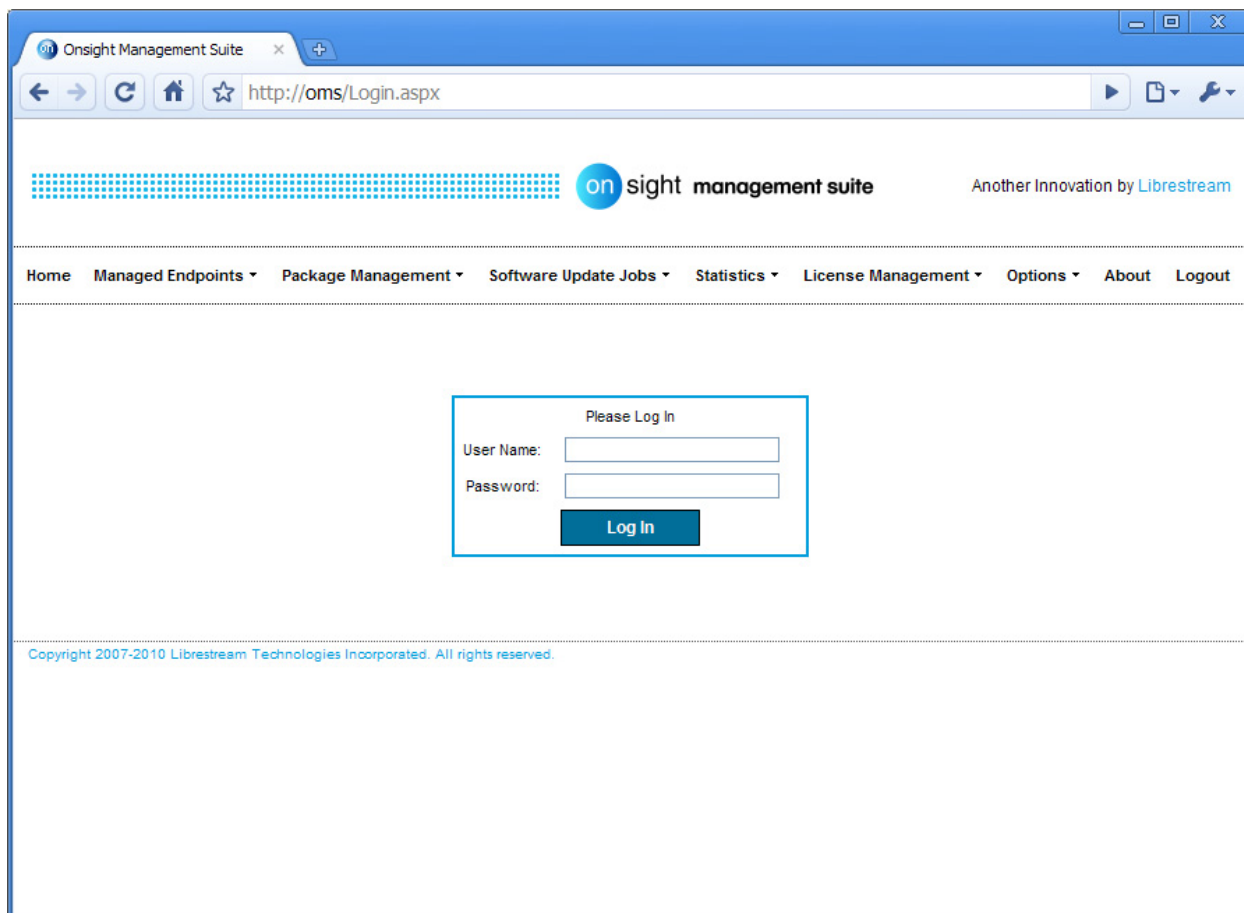


Figure 6 – Logging In to Onsight Management Suite

Every page in the User Interface is laid out in a similar manner to the login screen in Figure 6. At the top of the page, the name of the application is displayed along with the product's activation status (see **Activating Onsight Management Suite** on page 11). 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 or section that you are working on and the content of that section will be displayed directly below the menu.

To get started with the software, log in to the User Interface using the default user name and password, as follows:

User Name: **admin**
Password: **admin**

To avoid unauthorized access to the software, you should change this password immediately after logging in for the first time, as described in **Changing the Administrator Password** on page 9.

4.2 First Time Configuration

After logging in for the first time, you will need to configure a few items within Onsight Management Suite before it will become fully operational. There are three steps required in the configuration process: changing the administrator password, configuring the package server URL and configuring the Windows Service host name and port.

4.2.1 Changing the Administrator Password

→ To change the administrator password:

1. Choose **Options > General Settings**. This will take you to the **General Settings** configuration page, shown in Figure 7.
2. Locate the **Change Password** section, and enter the new password into both provided fields.
3. Click the **Save** button to save your changes.

General Settings

Change Password

Administrator Password:

Confirm Password:

Data Folders

Configuration File Root Path: C:\Documents and Settings\All Users\Application Data\MCA

Package Folder Root Path:

Windows Service Connection Settings

Service Host Name:

Service TCP Port:

Figure 7 – General Settings

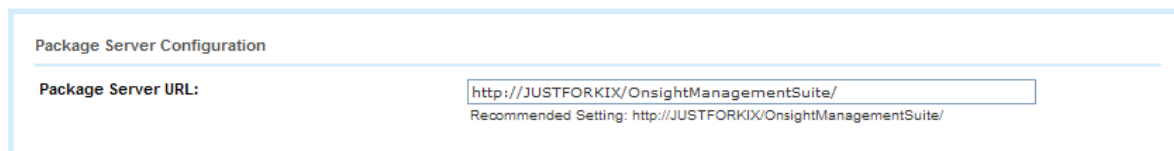
4.2.2 Configuring the Package Server

Onsight endpoints retrieve software and configuration updates from Onsight Management Suite using either an HTTP or HTTPS connection to the package server. When a software or configuration update is issued to an endpoint, the endpoint will be provided with the configured package server URL so that it can download any necessary update packages.

→ To configure the package server:

1. Choose **Options > Service Settings**. You will be presented with the **Service Settings** screen similar to the one shown in Figure 8.

Service Settings



Package Server Configuration

Package Server URL:

Recommended Setting: http://JUSTFORKIX/OnsightManagementSuite/

Figure 8 – Service Settings

2. Locate the field labeled **Package Server URL** in the **Package Server Configuration** section and enter the URL of the package server. The value entered should be the URL that an endpoint would use to access the **OnsightManagementSuite** virtual directory on the server. A recommended setting based on the host name of the server will be shown below the edit box.
3. To apply your changes, click the **Save** button at the bottom of the screen.



*For security reasons, the use of HTTPS is recommended. If an SSL certificate is installed on your server, you may substitute **https** for **http** when entering the **Package Server URL**.*



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

4.2.3 Configuring the Windows Service Port

The User Interface and Web Service components of Onsight Management Suite communicate with the Windows Service over a local TCP port. If you used the default port of 9090 during installation, as described in the **Installation** section on page 3, no further configuration should be required. However, if a TCP port other than the default was used, you will need to configure the User Interface and Web Service so that they will be able to communicate with the Windows Service.

→ To configure the User Interface to connect to the Windows Service:

1. Choose **Options > General Settings**. You will be presented with the **General Settings** screen, shown in Figure 7.
2. Locate the **Windows Service Connection Settings** section.
3. In the field labeled **Service TCP Port**, enter the TCP port you selected during installation.
4. Click the **Save** button to save your changes.

→ To configure the Web Service to connect to the Windows Service:

1. Choose **Options > Web Service Settings**. You will be presented with the **Web Service Settings** screen, shown in Figure 9.

Web Service Settings

Encryption Key

Encryption Key:
 Default encryption key: PqojYOjHe5MwTuB9Az178pNKcnk4ZJ3fD5xe

Remember to update configuration packages with the new encryption key.

Windows Service Connection Settings

Service Host Name:
 Service TCP Port:

Save **Cancel**

Figure 9 – Web Service Settings

2. Locate the **Windows Service Connection Settings** section.
3. In the field labeled **Service TCP Port**, enter the TCP port you selected during installation.
4. Click the **Save** button to save your changes.



Since the User Interface and Web Service will be running on the same server as the Windows Service, the **Service Host Name** should typically be left at the default setting of **localhost**.

4.3 Activating Onsite Management Suite

The first time you install Onsite Management Suite it will run in trial mode for a limited time. After that time you must activate the product in order to continue using it. Activation can be done in one of two ways: online or manually. The online method is normally more convenient, but requires that the server running Onsite Management Suite have access to the Internet. If this is not the case, use the manual activation method.

Regardless of which method you use, you will need the activation keys that you received when you purchased the product.



To operate the User Interface, even to perform tasks such as creating and modifying configuration packages, the Windows Service must be running and activated at all times.

4.3.1 Online Activation

→ To perform online activation of Onsite Management Suite:

1. Choose the **Options > Activation** menu item. You will be presented with the **Activate** screen shown in Figure 10.

Activate

Activation Instructions

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

XXXXXXX - CCCCCCCCCCCC

- 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:

- - X -

Online Activation

Figure 10 – Activation

2. On the tab labeled **Online**, enter the two parts of the activation key in the fields provided.
3. Press the **Online Activation** button, and wait for a response from the activation server. Online activation may take up to a minute to complete.
4. If the activation was successful, the activation status at the top of the screen will change to **Activated**.

4.3.2 Manual Activation

➔ To perform manual activation of Onsight Management Suite:

1. Choose the **Options > Activation** menu item and select the **Manual** tab shown in Figure 11.
2. Contact a Librestream 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 Onsight Management Suite was installed on, so ensure that you use the ones displayed on your screen rather than the example codes in Figure 11. The service representative will provide you with the two activation codes needed for activation.
3. Enter the codes into the boxes provided and press the **Manual Activation** button.
4. If the activation was successful, the activation status at the top of the screen will change to **Activated**.

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: **324776781**
2. This generated computer ID: **37987169**
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:

1-800-849-5507

Step 3
Once you have a two part Activation Code, enter it below along with the two part Activation Key that you purchased with this program, then press the **Manual Activation** button:

Activation Key: - - X -
Activation Code: -

Manual Activation

Figure 11 – Manual Activation

4.3.3 Viewing Activation Status

After activating, the status of Onsite Management Suite activation can be viewed by navigating to the **Options > Activation Status** menu item, which will display the **Activation Status** screen shown in Figure 12.

Activation Status

Status: **Activated**
Version: 2.0.4
Serial Number: 123456-Abcdefghijkl

Date	Version	Key
10/16/2009	2.0.2	123456-Abcdefghijkl-1-A1B2C3D4
10/19/2009	2.0.3	123456-Abcdefghijkl-1-E1F2G3H4
11/3/2009	2.0.4	123456-Abcdefghijkl-1-I1J2K3L4

Figure 12 – Activation Status

The **Activation Status** screen displays the status of the activation, the supported version number and the serial number that was used to activate the product. In addition, the list of release keys that were used to install each version of the product will be displayed for reference.

5 Remote Management of Onsight Endpoints

After configuring and activating the Onsight Management Suite for the first time, the system will be fully operational and can be used to monitor and manage Onsight endpoints. Endpoints can communicate with Onsight Management Suite using one or both of the following two methods: the built in Web Service interface, or the Simple Network Management Protocol (SNMP).

5.1 Web Service Management

Onsight Management Suite can accept connections from remote endpoints over the ASP.NET Web Service interface that was installed with the product. Advantages of the Web Service interface over the SNMP management interface include:

- The Web Service interface can be used in network environments that do not support the use of SNMP, such as those environments where SNMP traffic is blocked by firewalls.
- Since all communication is initiated from the endpoint to the Onsight Management Suite server, changes in an endpoint's IP address (whether occurring as a result of a DHCP renewal, a change in physical location, or a switch between the endpoint's wired and wireless network interfaces) can be detected faster and more reliably.
- Endpoint usage statistics and activation jobs are supported exclusively over the Web Service interface, and are not supported over the SNMP interface.

When configured to connect to the Web Service interface, endpoints will periodically report back to Onsight Management Suite. Each periodic report will include:

- Identification information for the endpoint, including the Device / Computer name and type of endpoint.
- A list of network interfaces on the endpoint, including each interface's MAC and IP addresses.
- The current version numbers of all software and configuration items installed on the endpoint.
- The endpoint's detailed system status, including call status, SIP registration and media streaming information.

If there is a pending software update or activation job configured for an endpoint, Onsight Management Suite will inform the endpoint during the next periodic report.



If the detailed status of endpoint changes between periodic reports (if, for example, the endpoint enters or leaves a call), the endpoint will communicate its new status immediately without waiting for the next reporting interval. Software update and activation jobs are not initiated during these intermediate status reports.

5.1.1 Configuring the Web Service Connection Settings

In order to be able to configure certain Web Service options using the User Interface, you must first configure the Web Service connection settings. Once configured, the connection settings can also be automatically applied to newly created Onsight device or Onsight Expert configuration packages.

→ To configure the Web Service Connection Settings:

1. Choose **Options > Web Service Connection**. You will be presented with the **Web Service Connection Settings** screen similar to the one shown in Figure 13.

Web Service Connection Settings

Remote Web Service Connection Settings

Service URI:

Encryption Key:

☒ Use as default when creating new Onsight Device Configuration packages

Figure 13 – Web Service Connection Settings

2. Locate the field labeled **Service URI** in the **Remote Web Service Connection Settings** section and enter the fully qualified URI of the Web Service. The value entered should be the URI that the User Interface and any Onsight endpoints will use to access the **OnsightWebService/RemoteEndpointService.asmx** file on the server.
3. Enter the encryption key required to communicate with the Web Service interface in the **Encryption Key** field.



*Enter the encryption key that is required to communicate with the Web Service interface in its current configuration. On a newly installed Onsight Management Suite, this should typically be left at the default value until the configured Web Service encryption key is changed, as described in **Changing the Web Service Encryption Key** section on page 15.*

4. Select the **Use as default when creating new Onsight Device Configuration packages** option to automatically fill these settings into the appropriate fields when creating a new Onsight device or Onsight Expert configuration package.
5. To test the connection settings, click the **Test** button to attempt a connection from the User Interface to the Web Service using the configured settings. The result of the test will be displayed when the test has completed.
6. Click the **Save** button to save your changes.

5.1.2 Changing the Web Service Encryption Key

Traffic sent over the Web Service interface is encrypted using a shared encryption key. When Onsight Management Suite is installed, it will use the following encryption key by default:

PqojYOjHe5MwTuB9Az178pNKCnk4ZJ3fD5xe

It is strongly recommended that you change the encryption key to prevent unauthorized access to the Web Service interface.

→ To change the Web Service encryption key:

1. Choose **Options > Web Service Settings**. You will be presented with the **Web Service Settings** screen, shown in Figure 9.
2. Enter the new encryption key into the **Encryption Key** field.
3. Click the **Save** button to save your changes.



You will have to manually change existing Onsight device and Onsight Expert configuration packages to use the new encryption key.



The encryption key on the **Web Service Connection Settings** screen will automatically be changed to match the newly configured key.

5.1.3 Configuring Web Service Management Settings

→ To configure the Web Service management settings:

1. Choose **Options > Service Settings**. You will be presented with the **Service Settings** screen, as shown in Figure 8.
2. Locate the **Web Service Management Configuration** section.
3. Configure the Web Service management settings described in Table 3.

Table 3 – Web Service Management Settings

Auto-register Unrecognized Endpoints	Enable this option to automatically add endpoints that connect over the Web Service interface to the database.
Endpoint Identification	The identification method to use for endpoints that are added automatically over the Web Service interface.
SNMP Manage New Web Service Clients	Enable this option to enable SNMP management by default for auto-registered endpoints.
Default SNMP Community	The SNMP community to use for endpoints that are auto-registered over the Web Service interface.
Reporting Interval	The interval (in seconds) at which clients will report over the Web Service interface. Clients will read this value from the server the first time they report.

4. Click **Save** to save your changes.

5.2 SNMP Management

Onsight Management Suite can also manage endpoints using the Simple Network Management Protocol (SNMP). SNMP management is more suited to endpoints that are on the same Intranet as the Onsight Management Suite server, as SNMP traffic is typically blocked by corporate firewalls and will not function for endpoints that operate in an environment where Network Address Translation (NAT) is used. The advantage of using SNMP is that all communication is initiated by Onsight Management Suite, so actions such as initiating software update jobs can be performed immediately without waiting for the endpoint to report over the Web Service interface.

All SNMP communication is performed by the Onsight Management Suite Windows Service. Periodically, the SNMP manager component of the Windows Service will attempt to refresh the status of each SNMP-managed endpoint in the database using SNMP requests. The information collected during each SNMP polling interval includes:

- Identification information for the endpoint, including the Device / Computer Name and type of endpoint.
- A list of network interfaces on the endpoint, including each interface's MAC and IP addresses.
- The current version numbers of all software and configuration items installed on the endpoint.



To reduce SNMP traffic on the network, the detailed system status of an endpoint is not collected during the regular SNMP polling interval. Detailed system status must be retrieved manually, as described in the **Status** section on page 42.

If there is an active software update job configured for an endpoint at the time of the regular SNMP polling interval, Onsight Management Suite will command the endpoint to immediately download and install the update.

5.2.1 SNMP Communication

Onsight Management Suite must know the IP address and SNMP community of an endpoint in order to communicate with it using SNMP. When communicating with an endpoint, Onsight Management Suite will attempt to resolve the address of the endpoint in the following order:

- The currently configured IP address. Usually this will be the last IP address that was successfully used to communicate with the endpoint via SNMP.
- The IP address resulting from a DNS lookup of the endpoint's Device / Computer name, if available.
- The IP address resulting from a DNS lookup of the endpoint's fully qualified DNS name, if available.
- Each IP address listed in the endpoint's last reported network interfaces table.



In environments where an endpoint's address is likely to change often, it is recommended that you use the Web Service interface in addition to SNMP. This will allow the endpoint to communicate any changes in its IP addresses to Onsight Management Suite immediately.



IP addresses and host names are resolved using the DNS lookup functionality built into Microsoft Windows, which caches DNS records for a period of time. If Onsight Management Suite is not able to resolve the IP address of an endpoint due to stale DNS records, you can clear the local DNS cache on the server by entering a Windows command prompt and typing the following command: `ipconfig /flushdns`.

5.2.2 Configuring SNMP Management Settings

→ To configure the SNMP management settings:

1. Choose **Options > Service Settings**. You will be presented with the **Service Settings** screen, shown in Figure 8.
2. Locate the **SNMP Management Configuration** section.
3. Configure the SNMP management settings described in Table 4.

Table 4 – SNMP Management Settings

Polling Interval For Online Endpoints	The interval (in seconds) at which the SNMP management component refreshes the current state of all online endpoints.
Polling Interval For Offline Endpoints	The interval (in seconds) at which the SNMP management component attempts to retrieve the state of all not responding or offline endpoints. Setting this to a lower value reduces the delay in detecting when an endpoint has come online.
Maximum SNMP Requests Per Second	The maximum number of requests per second sent by the SNMP management component. Use a lower number to reduce network traffic, and a higher number to reduce the time it takes to refresh the status of each managed endpoint.

4. Click **Save** to save your changes.

5.2.3 SNMP Management without Onsight Management Suite

Onsight Expert 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\Librestream Technologies\Onsight Expert\Snmp** folder.

6 Preparing Endpoints for Remote Management

In order for Onsight Management Suite to manage and monitor Onsight endpoints, the endpoints must first be configured to communicate with the server.

6.1 Configuring Endpoints to use the Web Service Interface

6.1.1 Configuring the Web Service Interface on an Onsight device

→ To configure the Web Service interface on an Onsight device endpoint:

1. Log on to the Onsight device with administrator privileges.
2. Open the main menu on the Onsight device and select **Configuration**.
3. Navigate to the **Network > Management** tab.
4. Select the **Enable Remote Management Web Service** option.
5. Enter the **Server URI** and **Encryption Key** of the Web Service interface.
6. Click the **Connect** button to apply the settings and connect to the Web Service. If the settings are entered correctly and the server is reachable by the endpoint, the status label on the **Management** tab should change to **Connected**.



*If the **Auto-register Unrecognized Endpoints** option on the server is disabled and the endpoint has not already been added to the server's database, the Onsight device will be unable to connect to the Web Service interface.*

6.1.2 Configuring the Web Service Interface on an Onsight Expert

→ To configure the Web Service interface on an Onsight Expert endpoint:

1. From the Onsight Expert main window, select **File > Preferences**.
2. Click the **Remote Management** tab.
3. Select the **Enable Remote Management Web Service** option.
4. Enter the **Server URI** and **Encryption Key** of the Web Service interface.
5. Click the **Connect** button to apply the settings and connect to the Web Service. If the settings are entered correctly and the server is reachable by the endpoint, the status label on the **Remote Management** tab should change to **Connected**.



*If the **Auto-register Unrecognized Endpoints** option on the server is disabled and the endpoint has not already been added to the server's database, the Onsight Expert will be unable to connect to the Web Service interface.*



*Onsight Expert endpoints can also be automatically configured to communicate with the Web Service Interface upon installation. See the **Onsight Expert Custom Installs** section on page 92 for more information.*

6.2 Configuring Endpoints for SNMP Management

6.2.1 Configuring SNMP Management on an Onsight device

→ To configure SNMP management on an Onsight device endpoint:

1. Open the main menu on the Onsight device and select **Configuration**.
2. Navigate to the **Network > SNMP** tab.
3. Configure the **Community** setting that will be used to communicate with the device over SNMP. Take note of the community name that you choose here as it will be used later when adding this endpoint to Onsight Management Suite.



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

4. You can also optionally configure a 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.



For security reasons, we recommend that you enter the host name or IP address of the Onsight Management Suite server.

5. Click the **Apply** button to apply the settings.

6.2.2 Configuring SNMP Management on an Onsight Expert

→ To configure SNMP management on an Onsight Expert endpoint:

1. Install the Windows SNMP service on the client computer. More information on installing the SNMP service is included in the **Installing the SNMP Service** section on page 20.
2. Configure the SNMP service to communicate with Onsight Management Suite. More information on configuring the SNMP service can be found in the **Configuring the SNMP Service** section on page 22.
3. Configure the firewall software on the client computer. See the **Firewall Configuration** section on page 25 for more information.
4. Install the Onsight Expert software on the client computer. Additional configuration of the Onsight Expert client software itself is not necessary.



The Onsight Expert software can be installed either before or after the SNMP service is installed and configured.

6.2.2.1 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 14.

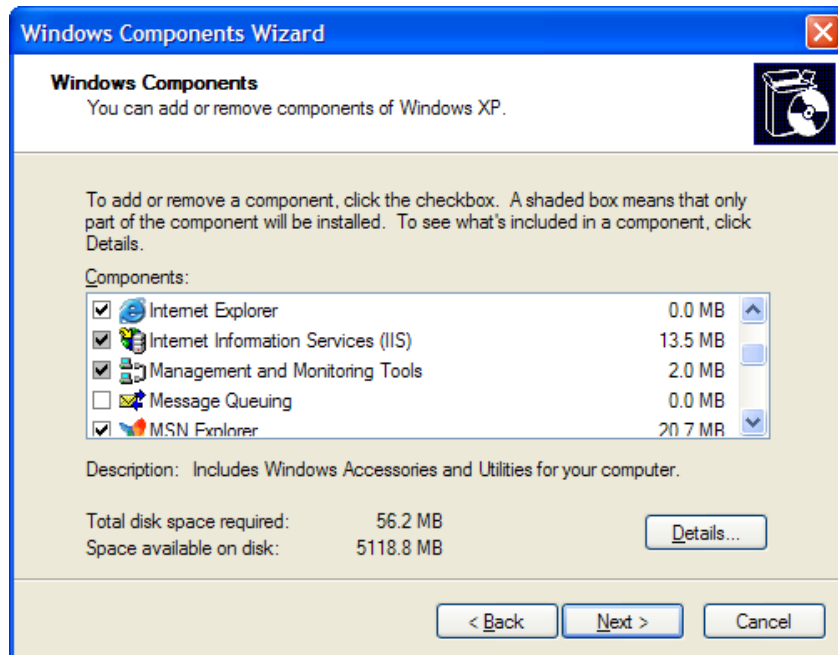


Figure 14 – Windows Components Wizard

4. Click **Management and Monitoring Tools** in the list to select it and then click the **Details** button. You will be presented with the **Management and Monitoring Tools** dialog, as shown in Figure 15.

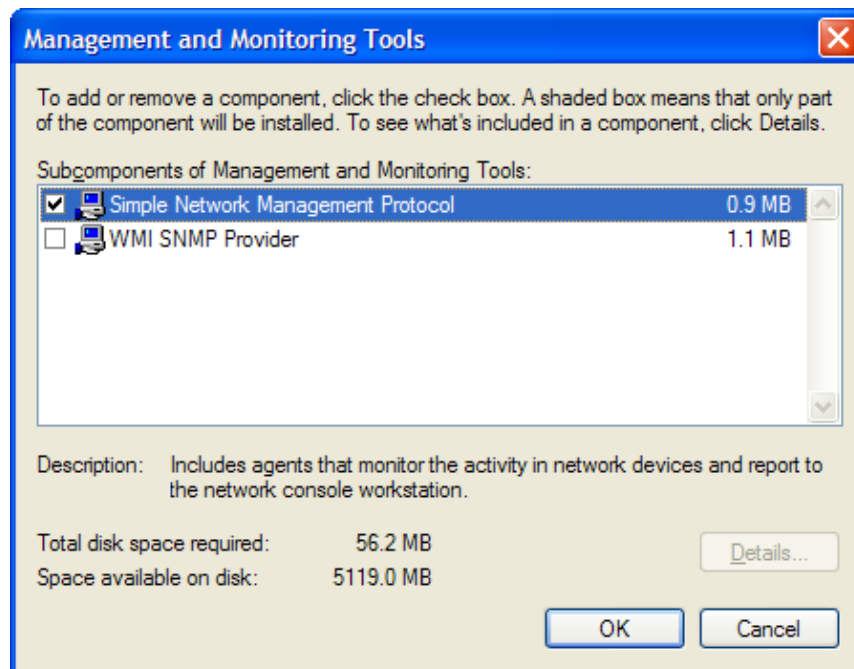


Figure 15 – Management and Monitoring Tools

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 will be installed and running on your PC.



When uninstalling or upgrading the Onsight Expert software on Windows Vista computers where the SNMP service is already running, you may be presented with a dialog similar to the one in Figure 16, asking if you wish to automatically stop the SNMP Service.

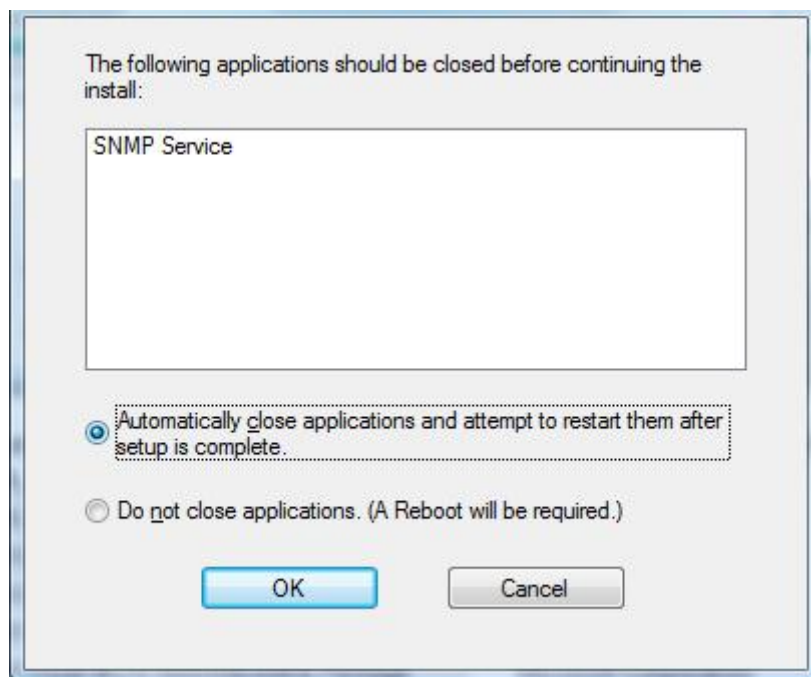


Figure 16 – SNMP Warning During Onsight Expert Setup

*If you choose the **Automatically close the applications and attempt to restart them after setup is complete** option, 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.*

6.2.2.2 Configuring the SNMP Service

→ To configure the SNMP service to communicate with Onsight Management Suite:

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 17.

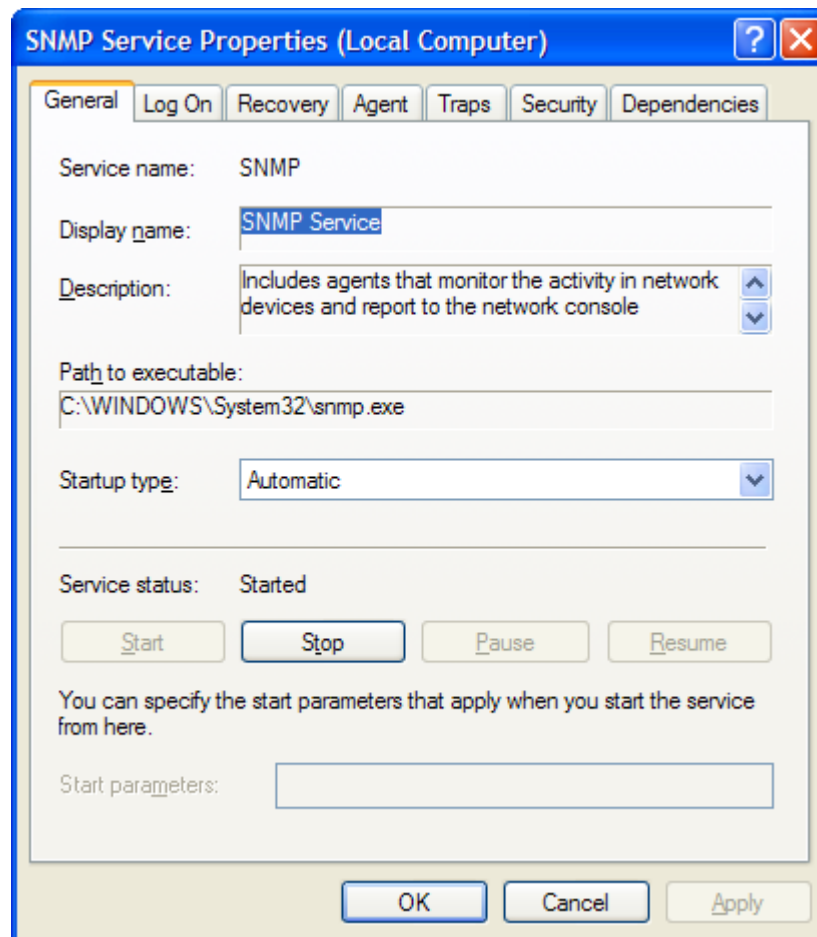


Figure 17 – SNMP Service Properties

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 18.

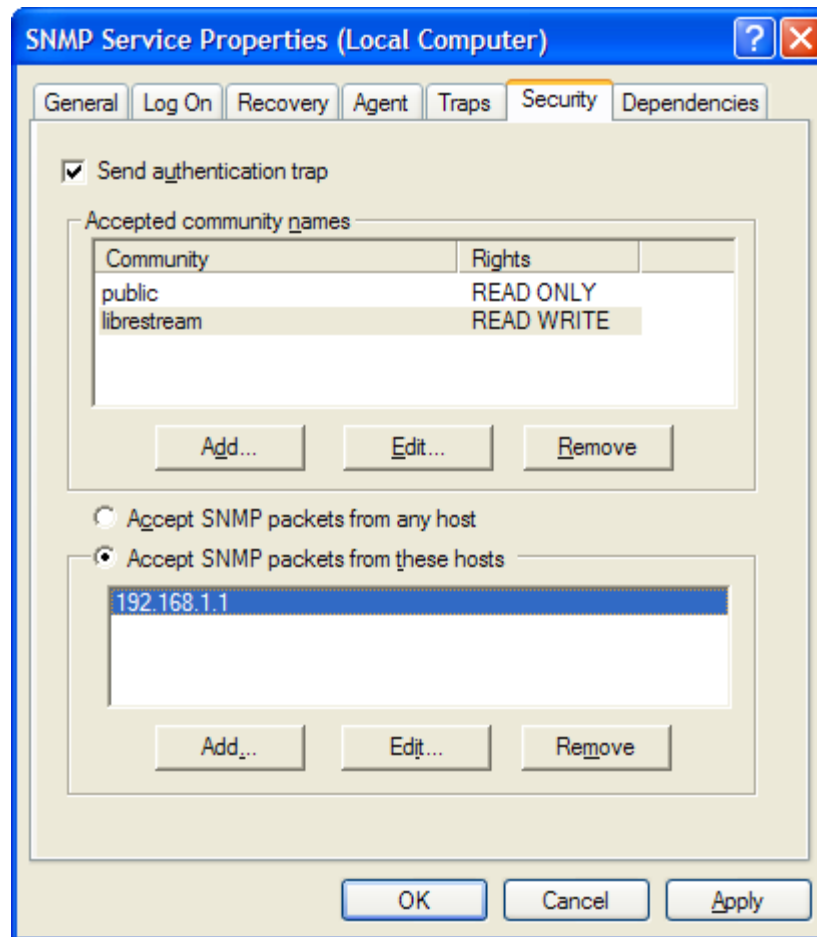


Figure 18 – SNMP Service Security Options

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**.



*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. To add a community name, click **Add**. You will be presented with the **SNMP Service Community** dialog as shown in Figure 19, where you can set the community name and access rights for the community. Take note of the community name that you choose here as it will be used later when adding this endpoint to Onsight Management Suite.

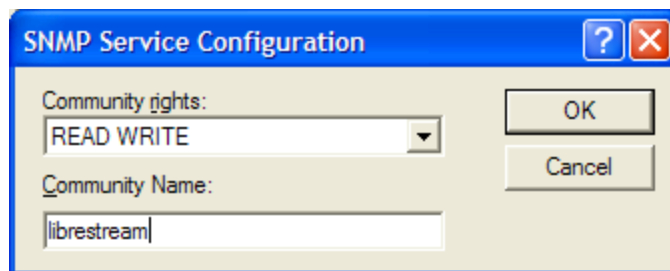


Figure 19 – SNMP Service Community



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.

9. 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 Onsite Management Suite server to the list of permitted hosts, click the **Add** button and enter the host name or IP address of the server.



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.

6.2.2.3 Firewall Configuration

If Windows Firewall, third party firewall software, or another Internet security suite is running on the Onsite Expert computer, SNMP packets may be blocked from entering the system. You will need to configure a firewall exception to allow UDP packets through on port 161.

6.2.2.4 SNMP Service Registry Settings

When the Onsite Expert client software is installed, it sets up all necessary registry entries that are required for the Librestream SNMP agent to be loaded onto the system. However, if the SNMP service is removed and reinstalled at a later date these registry entries may need to be reapplied manually.

→ To re-apply the SNMP registry settings:

1. Login to the Onsite Expert computer using an account with administrator privileges.
2. Open the **C:\Program Files\Librestream Technologies\Onsite Expert\Snmp** folder and double-click the **SnmpExtensionAgent.reg** file located in the folder.
3. When prompted, click **Yes** to import the settings into the registry.
4. Click **OK** when the import is complete.
5. For the changes to take effect, either restart the SNMP service through the **Administrative Tools > Services** dialog in the Control Panel or restart your computer.

7 Adding Managed Endpoints

→ To manage an endpoint with Onsight Management Suite:

1. Configure the endpoint for remote management, as described in **Preparing Endpoints for Remote Management** on page 19.
2. Add the endpoint to the system. The endpoint can be added either manually, as described in **Manually Adding a Managed Endpoint** on page 26, or automatically, as described in **Automatically Adding Managed Endpoints** on page 29.

Onsight Management Suite Service maintains a persistent database of managed endpoints, so an endpoint only needs to be added to the system once.

7.1 Identifying Managed Endpoints

In order to distinguish one endpoint from another, Onsight Management Suite must be able to uniquely identify endpoints in the system. There are currently two supported methods of endpoint identification: Device / Computer Name and MAC Address.

7.1.1 Device / Computer Name Identification

Onsight Management Suite will use the Device / Computer Name of an endpoint to uniquely identify it by default. Each time the server communicates with an endpoint, it will check that the reported Device / Computer Name of the endpoint matches what is stored in the database to ensure it is talking to the correct endpoint.



If the Device / Computer Name of an endpoint changes, you will need to manually change the Device / Computer Name within Onsight Management Suite in order to identify it as the same endpoint.

7.1.2 MAC Address Identification

If the Device / Computer Name of endpoints changes frequently, or endpoints on the network do not have unique names, an administrator also has the option of identifying endpoints using one or more MAC addresses. Each time the server communicates with an endpoint, it will retrieve the list of network interfaces on the endpoint. If at least one of the MAC addresses of the retrieved interfaces matches at least one of the configured MAC addresses for the endpoint, the server will assume that it is talking to the correct endpoint.



If a network interface on an endpoint is disabled, its MAC address will not be reported to Onsight Management Suite. It is recommended that only MAC addresses of interfaces that are not likely to be disabled be used for identification purposes.



Network adapters that are shared between multiple computers, such as a wireless USB network adapter, should not be used to identify endpoints.

7.2 Manually Adding a Managed Endpoint

→ To manually add an endpoint to the system:

1. Choose **Managed Endpoints > Add Managed Endpoint**. You will be presented with the **New Managed Endpoint** wizard, as shown in Figure 20.

New Managed Endpoint

Add New Managed Endpoint Method

☒ Search for an endpoint using SNMP

☐ Register an endpoint that is not reachable by SNMP

Next

Cancel

Figure 20 – New Managed Endpoint Wizard

2. In the **Add New Managed Endpoint Method** section, choose the method you wish to use to add the new endpoint from the options listed in Table 5. Once you have selected the method you wish to use, click **Next**.

Table 5 – Add New Managed Endpoint Methods

Search for an endpoint using SNMP	This option allows you to search for an SNMP-enabled Onsight endpoint on the network using either its hostname or IP address.
Register an endpoint that is not reachable by SNMP	This option allows you to manually add an endpoint that either is not currently online, or one that is not SNMP-enabled.

3. If you chose to search for an SNMP-enabled endpoint, you will be presented with the **SNMP Search Parameters** screen, as shown in Figure 21. Otherwise, proceed to step 5.

SNMP Search Parameters

IP Address / DNS name:

192.168.1.88

SNMP community:

librestream

Figure 21 – SNMP Search Parameters

4. Enter the information required to communicate with the endpoint using SNMP, as listed in Table 6. Click **Next** to search for the endpoint.

Table 6 – SNMP Search Parameters

IP Address / DNS Name	Enter the IP address, DNS name or host name of the endpoint to search for.
-----------------------	--

SNMP Community	Enter the SNMP community name to be used to communicate with the endpoint by SNMP. This should be the read/write community that you previously configured on the endpoint.
----------------	--

5. After the SNMP search has been completed, or if you chose the **Register an endpoint that is not reachable by SNMP** method, you will be presented with the **New Managed Endpoint Identification** screen, as shown in Figure 22.

Identification

Endpoint Type:

Identification Method:

Device / Computer Name:

MAC Addresses:

Endpoint Group: [change](#)

SNMP Management (optional)

☒ Enable SNMP Management

IP Address:

DNS Name:

Community:

Figure 22 – New Managed Endpoint Identification

6. Enter the information required to identify the endpoint, as listed in Table 7.

Table 7 – New Managed Endpoint Identification

Endpoint Type	Choose whether the endpoint is an Onsight device or Onsight Expert endpoint.
Identification Method	Choose to identify the endpoint by either the Device / Computer Name or by MAC Address.
Device / Computer Name	Enter the Device / Computer Name of the endpoint. This is required if the endpoint is being identified by Device / Computer Name, otherwise this setting is optional.
MAC Addresses	Enter one or more MAC addresses for the endpoint, one per line. This is required if the endpoint is being identified by MAC Address, otherwise this setting is optional.
Endpoint Group	Select the change link to choose the endpoint group that the new endpoint will belong to. The default is All Endpoints . For more information on endpoint groups, see the Endpoint Groups section on page 35.
Enable SNMP Management	Select this option if you wish to be able to manage the endpoint using SNMP.

IP Address	Enter the initial IP address to use when communicating with the endpoint using SNMP. If you choose not to enter an IP address, Onsight Management Suite will attempt to resolve an IP address for the endpoint using its Device / Computer Name or DNS Name.
DNS Name	Enter a fully-qualified DNS name for the endpoint. Use this setting if Onsight Management Suite will not be able to resolve an IP address for the endpoint using the Device / Computer Name.
SNMP Community	Enter the SNMP community name to be used to communicate with the endpoint using SNMP. This should be the read/write community that you previously configured on the endpoint.



*If the endpoint was found during the **Search for an endpoint using SNMP** method, the details for the endpoint will be automatically filled into the **New Managed Endpoint Identification** form. If an SNMP search was performed but failed to locate an endpoint at the specified address, only the IP Address / DNS Name and SNMP Community used for the search will be filled in.*

- Click the **Next** button to save your changes and add the endpoint to the system. You will be redirected to the **Managed Endpoints** page and the new endpoint will appear in the list of managed endpoints.

7.3 Automatically Adding Managed Endpoints

In addition to being added to the system manually, endpoints can also be automatically discovered and added to Onsight Management Suite.

7.3.1 Web Service Discovery

Onsight endpoints that were previously configured to connect to the Onsight Management Suite Web Service interface can be automatically added to the system the first time they connect.

To enable or disable this functionality, refer to the **Configuring Web Service Management Settings** section on page 16.

7.3.2 SNMP Discovery

Endpoints can also be added to the system automatically through an SNMP discovery process. The Onsight Management Suite Windows Service maintains a list of IP address ranges that it uses to search for new SNMP-enabled Onsight endpoints on the network. If a new endpoint that is not already present in the system is discovered, the endpoint will be added to the list of managed endpoints.

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

- The endpoint must be reachable by IP address on the network.
- The endpoint must have SNMP enabled and Onsight Management Suite must be configured to discover endpoints using the corresponding SNMP community.
- In the case of Onsight Expert endpoints, the Onsight Expert software must be installed on the computer in order for it to be identified as an Onsight endpoint.

7.3.2.1 Configuring SNMP Discovery

→ To configure SNMP discovery:

- Choose **Options > Service Settings**. You will be presented with the **Service Settings** screen, as shown in Figure 8.

2. Locate the **SNMP Discovery Configuration** section and configure the SNMP discovery configuration settings described in Table 8.

Table 8 – SNMP Discovery Configuration

Periodic SNMP Discovery	Enable or disable periodic discovery. If periodic SNMP discovery is disabled, discovery rounds will have to be performed manually.
Endpoint Identification	The default identification method to use for endpoints discovered over SNMP.
Discovery Interval	The time between periodic SNMP discovery rounds. A lower number increases the frequency of discovery rounds, increasing the chance that an endpoint will be discovered if it is online for a short period of time.
Maximum SNMP Requests Per Second	The maximum number of requests per second sent during SNMP discovery. A higher number increases the speed of discovery and a lower number reduces network traffic.

3. Click the **Save** button to save your changes.

7.3.2.2 Creating an SNMP Discovery Range

→ To add an SNMP discovery range to the system:

1. Choose **Managed Endpoints > SNMP Discovery**. You will be presented with the **SNMP Discovery** screen, as shown in Figure 23.

SNMP Discovery

Status: **Running**
 Last Discovery Started: 11/18/2009 10:38:28 AM
 Addresses Searched: 4
 Next Discovery Round: -

[Start Discovery](#)

Add	Delete	Reload Table		
<input type="checkbox"/>	Starting IP Address	Ending IP Address	SNMP Community	
<input type="checkbox"/>	192.168.1.1	192.168.1.100	public	modify delete
<input type="checkbox"/>	192.168.1.1	192.168.1.100	librestream	modify delete

Figure 23 – View SNMP Discovery List

2. Click the **Add** button at the top of the SNMP discovery list. You will be directed to an **Add SNMP Discovery Range** screen similar to the one in Figure 24.

Add SNMP Discovery Range

SNMP Discovery Range

Starting IP Address: 192.168.2.1

Ending IP Address: 192.168.2.100

SNMP Community: librestream

Save Cancel

Figure 24 – Add SNMP Discovery Range

- Enter the information required to identify the discovery range, listed in Table 9.

Table 9 – New SNMP 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 endpoints for this range.



To perform discovery on an IP address range using more than one SNMP community, the same range of addresses can be added multiple times with different community names.

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

7.3.2.3 View Existing SNMP Discovery Ranges

To view the list of current SNMP discovery ranges in the system, choose **Managed Endpoints > SNMP Discovery**. You will be presented with a list of all of the SNMP discovery ranges that were previously created, as shown in Figure 23. In addition, the status of current SNMP discovery round, the time of the last discovery round, the number of IP addresses searched and the time of the next scheduled discovery round are shown at the top of the page.

Each item in the discovery range 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 SNMP discovery range.
- Delete** removes the discovery range from the system.

7.3.2.4 Modify an Existing SNMP Discovery Range

To modify an existing SNMP discovery range, open the **SNMP Discovery** page, locate the discovery range in the list, and click the **modify** link.

7.3.2.5 Performing SNMP Discovery Rounds

Once you have configured the desired SNMP discovery ranges, you may perform an SNMP discovery round. During an SNMP discovery round, the Windows Service will query each IP address in each configured SNMP discovery range to attempt to discover new SNMP-enabled Onsite endpoints.

To begin a new SNMP discovery round, perform one of the following:

- Navigate to **Managed Endpoints > SNMP Discovery** and click the **Start Discovery** button.

- If periodic SNMP discovery is enabled, simply wait for the next scheduled discovery round. The time of the next discovery round is indicated by the **Next Discovery Round** field at the top of the **SNMP Discovery** page.

8 Managing Endpoints

To view a list of managed endpoints currently in the system, choose **Managed Endpoints > View Managed Endpoints**. You will be presented with the **Managed Endpoints** screen, similar to the one shown in Figure 25.

Managed Endpoints

Endpoint Group: **All Endpoints** Selected: 0 [Clear Selected](#)

[Add](#) [Rename](#) [Delete](#) [Move](#)

- All Endpoints
 - Lab

[Add](#) [Delete](#) [Move](#) [SNMP Refresh](#) [Create Update Job](#) [Export to CSV](#) [Reload Table](#)

<input type="checkbox"/>	Name	Type	Address	Remote Address	Online Status	Last Online	Sub-Group	
<input type="checkbox"/>	MCD0023A7000244	Onsight Device	-	192.168.1.158	not responding	6/29/2010 4:14:01 PM	-	delete
<input type="checkbox"/>	MCD000B6B0BA69D	Onsight Device	-	192.168.1.165	online	6/29/2010 4:14:38 PM	-	delete
<input type="checkbox"/>	ONSIGHTEXPERTPC	Onsight Expert	-	192.168.1.174	online	6/29/2010 4:14:23 PM	Lab	delete

Figure 25 – Managed Endpoints

8.1 Managed Endpoints Table

The **Managed Endpoints** screen contains a table of all endpoints currently managed by Onsight Management Suite. Each entry in the table will contain the information described in Table 10.

Table 10 – Managed Endpoints Table Columns

Name	The name of the endpoint. This will typically be the Device / Computer Name of the endpoint.
Type	The type of endpoint: Onsight device or Onsight Expert.
Address	The IP address used to communicate with the endpoint using SNMP.
Remote Address	The IP address that the endpoint last used to communicate with Onsight Management Suite over the Web Service interface.
Online Status	The current status of the endpoint, which will be one of the following: <ul style="list-style-type: none"> online – the endpoint is reachable by the Onsight Management Suite and is currently running. not responding – the endpoint is either not reachable by the network, is not turned on, or is not communicating for some other reason. offline – the endpoint is reachable by the network but the Onsight software is not running.
Last Online	The last date and time the endpoint was online.
Sub-Group	The sub-group the endpoint is a member of, with respect to the currently selected endpoint group.

In addition to the information described above, action buttons are included at the top of the table, allowing you to perform various tasks on the **Managed Endpoints** table. These are described in detail in Table 11.

Table 11 – Managed Endpoints Actions

Add	Directs you to the New Managed Endpoint Wizard page, where you can manually add a new endpoint.
Delete	Deletes the selected endpoints. You can also delete an individual endpoint by clicking its corresponding delete link in the table.
Move	Move the selected endpoints to a different endpoint group.
SNMP Refresh	Commands the Onsight Management Suite Service to immediately perform a background SNMP refresh on the selected endpoints.
Create Update Job	Create a software update job for the selected endpoints. More information on creating a software update job can be found in Creating a New Software Update Job on page 45.
Export to CSV	Export the Managed Endpoints table to a comma-separated values (CSV) file. The format of the exported data is described in Table 12.
Reload Table	Reload the table and display the current information for all endpoints.



*When an endpoint is deleted it will no longer be visible in the **Managed Endpoints** table. However, in order to preserve collected statistics and software update job history, deleted endpoints will not be removed from the database. When viewing collected statistics or software update job status, a deleted endpoint will be shown using a strikethrough font to indicate that it is no longer being managed.*



An endpoint that was deleted from the database must be re-added to Onsight Management Suite in order to resume managing it.

Table 12 – Endpoint Records

EndpointId	When an endpoint is added to Onsight Management Suite, it is automatically assigned an auto-incrementing Endpoint ID. This identifier can be used to correlate endpoints with their reported usage statistics, as described in the Interpreting Statistics section on page 76.
EndpointName	The name of the endpoint. This will typically be the Device / Computer Name of the endpoint.
EndpointType	The type of endpoint: Onsight device or Onsight Expert.
WiredMacAddress	The MAC address of the wired network interface (Onsight devices only).
Address	The IP address used to communicate with the endpoint using SNMP.
RemoteAddress	The IP address that the endpoint last used to communicate with Onsight Management Suite over the Web Service interface.
LastOnline	The last date and time the endpoint was online.



If an endpoint is deleted from Onsight Management Suite and added again at a later time, it will be assigned a new Endpoint ID.

8.1.1 Filtering the Managed Endpoints Table by Column

The **Managed Endpoints** table can be filtered by any column in order to assist in locating an endpoint in the table. Filtering is performed using the filter row, located just below the column headings in the table.

→ To filter the Managed Endpoints table:

1. Locate the column you wish to filter the table by.

2. In some cases, the list of available filter values for that column will be provided in a drop-down list. If so, choose the desired value from the list. The filter will be applied and only endpoints that match the filter will be displayed in the table.
3. If the column does not provide a list of available values to filter by, you must type a filter value into the corresponding edit box. Type the first few characters of the value you wish to filter by, and either press the **Enter** key, or wait for a moment for the filter to be applied automatically.
4. Once the table has been filtered by the chosen column, you can further refine the filter using additional columns by repeating steps 1-3.
5. Click the **Clear** link in the filter row to clear the filter when you are finished.



Filtering the **Managed Endpoints** table will not clear which endpoints in the table are selected. To view the number of currently selected endpoints, locate the **Selected** count to the top right of the table.



When manually entering a filter value, the '%' or '*' characters can be used as wildcards.

8.2 Endpoint Groups

In addition to filtering the **Managed Endpoints** table, endpoints can be further organized into endpoint groups. An endpoint group acts simply as another filter that can be applied to the table in order to manage groups of endpoints whose properties might be similar.

Endpoint groups are organized into a hierarchical tree, similar to folders on a computer's file system. Although an endpoint can only be directly assigned to a single endpoint group, the tree structure allows an administrator to further organize endpoints by assigning them to different sub-groups within the tree.

The root of the **Endpoint Group** tree is the **All Endpoints** node. All groups added to the system will be a sub-group of **All Endpoints**.

8.2.1 Creating a New Endpoint Group

→ To create a new endpoint group:

1. Select the node in the **Endpoint Group** tree that you wish to add a sub-group to.
2. Click the **Add** link at the top of the **Endpoint Group** tree. You will be presented with the **Add Group** screen shown in Figure 26.

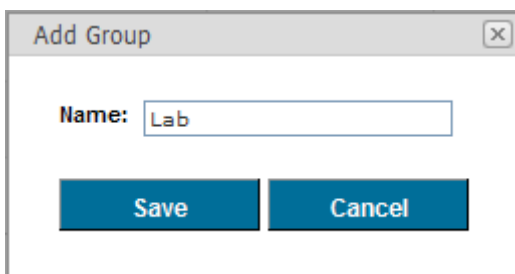


Figure 26 – Add Group

3. Enter a name for the endpoint group, and click the **Save** button.



Endpoint group names must be unique across the entire endpoint group tree.

4. The group will be added to the **Endpoint Group** tree.

8.2.2 Renaming an Endpoint Group

→ To rename an endpoint group:

1. Select the group in the **Endpoint Group** tree that you wish to rename.
2. Click the **Rename** link at the top of the **Endpoint Group** tree. You will be presented with the **Rename Group** screen.
3. Enter the new name for the endpoint group, and click the **Save** button.



*The **All Endpoints** group cannot be renamed.*

8.2.3 Moving an Endpoint Group

An endpoint group can also be moved within the **Endpoint Group** tree. When you move an endpoint group, all of its sub-groups will be moved with it.

→ To move an endpoint group:

1. Select the group in the **Endpoint Group** tree that you wish to move.
2. Click the **Move** link at the top of the **Endpoint Group** tree. You will be presented with the **Move Group** screen shown in Figure 27.

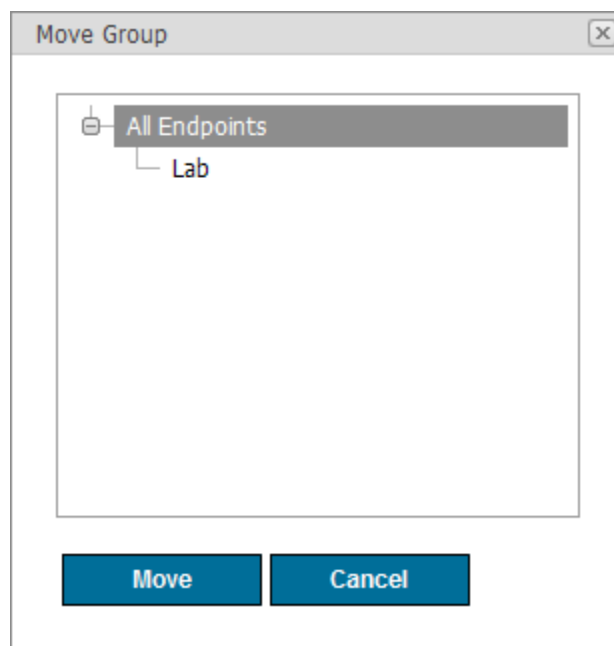


Figure 27 – Move Group

3. Select the group name from the tree that you wish to move the group to, and click the **Move** button. Note that a group cannot be moved to itself or any of its sub-groups.

4. The group and all its sub-groups will be moved to the specified group.

8.2.4 Deleting an Endpoint Group

→ To delete an endpoint group:

1. Select the group in the **Endpoint Group** tree that you wish to delete.
2. Click the **Delete** link at the top of the **Endpoint Group** tree. You will be presented with the **Delete Group** screen shown in Figure 28.

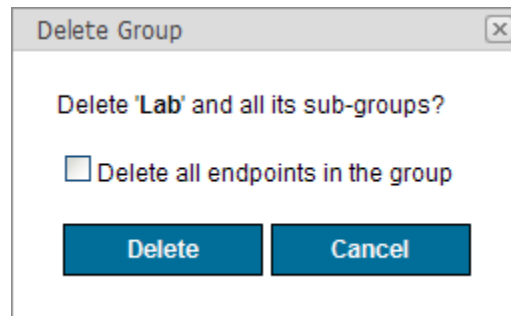


Figure 28 – Delete Group

3. To delete all of the endpoints that belong to that portion of the tree, select the **Delete all endpoints in the group** option. If this option is not selected, endpoints that belong to the selected group and its sub-groups will be moved to the **All Endpoints** group.
4. Click the **Delete** button to delete the group and all of its sub-groups.

8.2.5 Moving Endpoints to an Endpoint Group

→ To move endpoints to an endpoint group:

1. Select the endpoints in the **Managed Endpoints** table that you wish to move.
2. Click the **Move** link at the top of the **Managed Endpoints** table. You will be presented with the **Move Selected Endpoints** screen shown in Figure 29.

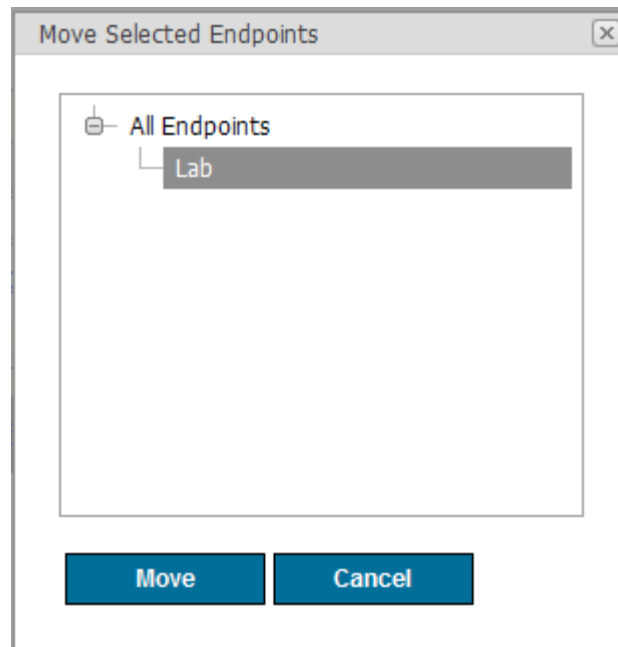


Figure 29 – Move Selected Endpoints

3. Select the group name from the tree that you wish to move the endpoints to, and click the **Move** button.
4. The endpoints will be moved to the specified group.

8.2.6 Filtering the Managed Endpoints Table by Group

To filter the **Managed Endpoints** table by endpoint group, select the group name from the **Endpoint Group** tree. The table will reload to display all endpoints that belong either directly to that group or one of its sub-groups. If an endpoint belongs directly to the chosen group, its Sub-Group column in the **Managed Endpoints** table will be blank. If an endpoint belongs to one of the sub-groups within the selected group, the group name will be displayed in the Sub-Group column.

To clear the filter and view all endpoints in the system, select the **All Endpoints** group in the tree.

8.3 Modifying an Existing Endpoint

To view or modify an existing Onsight endpoint, locate it in the **Managed Endpoints** table and click on its name. You will be taken to the **Endpoint Details** screen, similar to the one shown in Figure 30.

Details for Endpoint **ONSIGHTEXPERTPC**

Status: **online**
 Last Online: 7/6/2010 11:52:48 AM (9 seconds ago)
 Updated Source: Web Service

[SNMP Refresh](#) [Reload Page](#)

Identification	Software	Update History	Activation	Status						
Identification										
Endpoint Type: <input type="text" value="Onsight Expert"/>										
Identification Method: <input type="text" value="Device / Computer Name"/>										
Device / Computer Name: <input type="text" value="ONSIGHTEXPERTPC"/>										
MAC Addresses: <input type="text"/>										
Endpoint Group: <input type="text" value="All Endpoints"/> change										
Network Interfaces										
<table border="1"> <thead> <tr> <th>MAC Address</th> <th>IP Address</th> <th>Type</th> </tr> </thead> <tbody> <tr> <td>08-00-27-6B-7A-8D</td> <td>192.168.1.174</td> <td>Ethernet</td> </tr> </tbody> </table>					MAC Address	IP Address	Type	08-00-27-6B-7A-8D	192.168.1.174	Ethernet
MAC Address	IP Address	Type								
08-00-27-6B-7A-8D	192.168.1.174	Ethernet								
SNMP Management										
<input checked="" type="checkbox"/> Enable SNMP Management										
IP Address: <input type="text" value="192.168.1.174"/>										
DNS Name: <input type="text"/>										
Community: <input type="text" value="public"/>										
Last Online: <input type="text" value="never"/>										
Web Service Management										
Remote Address: <input type="text" value="192.168.1.174"/>										
Last Online: <input type="text" value="7/6/2010 11:52:48 AM (9 seconds ago)"/>										
<input type="button" value="Save Changes"/>										

Figure 30 – Endpoint Details Identification Tab

The current status of the endpoint and the time the endpoint was last online will be shown at the top of the screen. In addition, the protocol (Web Service or SNMP) last used to communicate with the endpoint is also shown. There are also two action buttons at the top of the screen:

- **SNMP Refresh** can be used to immediately communicate with the endpoint using SNMP to retrieve its latest status.
- **Reload Page** will reload the page to display any information that has been updated since the last time the **Endpoint Details** page was loaded.

The tabs at the top of the **Endpoint Details** page can be used to navigate between its five sections: **Identification**, **Software**, **Update History**, **Activation** and **Status**.



*The **Activation** tab will only be visible when viewing the details of Onsight Expert endpoints.*

8.3.1 Identification

The **Identification** tab on the **Endpoint Details** page, as shown in Figure 30, displays the information used to identify an Onsite endpoint, as described in **Manually Adding a Managed Endpoint** on page 26. Here you can make changes to the information used to identify the endpoint. When you have made the necessary changes, click **Save Changes** to save them to the database.



Changing the SNMP community value only changes the value that Onsite Management Suite uses to communicate with the endpoint. It does not change the actual SNMP community configured on the endpoint, which must be done either manually on the endpoint itself, or by installing a new configuration package containing the desired community.

8.3.1.1 Network Interfaces

The **Identification** tab also contains the **Network Interfaces** table, which contains a list of network adapters that were active on the endpoint the last time it was online. The MAC address, IP addresses and type of each network interface are displayed in the table.



*Only IPv4 addresses will be displayed in the **Network Interfaces** table.*

8.3.2 Software

The **Software** tab on the **Endpoint Details** page displays an endpoint's software and configuration version information, as well as the status of active software update jobs for that endpoint, as shown in Figure 31.

The screenshot shows the 'Software' tab selected in the 'Endpoint Details' page. It contains two main sections: 'Installed Software' and 'Active Update Jobs'.

Installed Software

Name	Version
Software	4.0.2.0
Configuration	1.0.0.0
Media Configurations	1.0.0.0
Users / Contacts	13.0.0.0

Active Update Jobs

Name	Status	Last Attempt Initiated	Next Attempt	Attempts	
Update Contacts to Latest	Waiting for Device (Offline)	-	-	0	Cancel
Revert Config to Default	Queued	-	-	0	Cancel

At the bottom of the 'Active Update Jobs' section, there are two buttons: 'Create Update Job' and 'SNMP Initiate Update'.

Figure 31 – Endpoint Details Software Tab

The **Installed Software** table lists the version numbers of all software and configuration items installed on the endpoint. In some cases, an item in the table can be expanded by clicking the + button to reveal more detailed version information. For example, expanding the **Software** item for an Onsite device will reveal the version numbers of the OS, Application, Monitor, MCU and Splash Screen.



*If a package of a particular type has never been installed on an endpoint, the installed version number for that package type will appear as **Unknown**.*

The **Active Update Jobs** table lists all of the active or queued software update jobs for the endpoint. Administrators can also create a new update job for an endpoint by clicking the **Create Update Job** button below the table. If there

is a pending update job that is waiting to be initiated, you can attempt to initiate it immediately by pressing the **SNMP Initiate Update** button.

More information about creating and managing software update jobs can be found in the **Software and Configuration Updates** section on page 43.

8.3.3 Update History

The **Update History** tab on the **Endpoint Details** page displays a table of all previously completed or cancelled update jobs for an endpoint, as shown in Figure 32.

Update Job History				
	Name	Status	Last Attempt Initiated	Attempts
⊕	Update to Latest Software	Cancelled	-	0
⊕	New Software Update Job	Succeeded	11/16/2009 2:57:19 PM	2

Figure 32 – Endpoint Details Update History Tab

8.3.4 Activation

The **Activation** tab on the **Endpoint Details** page displays the software activation status of Onsite Expert endpoints, as shown in Figure 33.

Activation Status

Status: **Activated**

Days Remaining: -

Serial Number: **XXXXXXXXXXXX**

Server Licensing: Disabled

Locked Call License ID: -

Pending Activation Status

Activation Key: 123456-Abcdefgh

Type: Activation

Status: **Waiting for Endpoint**

Last Attempt Initiated: -

Last Attempt Result: -

Next Attempt: -

Attempts: 0

Conditions: Trial mode

Cancel

Figure 33 – Endpoint Details Activation Tab

The **Activation Status** section displays the last reported software activation state of the Onsite Expert endpoint. For more information on the activation status of Onsite Expert endpoints, refer to **Onsite Expert Activation Status** on page 81.

The **Pending Activation Status** section lists the status of any pending activation job for the endpoint. Pending activation jobs can be cancelled from this screen by clicking the **Cancel** button. More information about creating and managing activation jobs can be found in the **Onsite Expert Activation Jobs** section on page 85.

8.3.5 Status

The **Status** tab on the **Endpoint Details** page displays an endpoint's detailed system status, including hardware information, call and conference status, SIP registration status and media streaming status.

→ To view the detailed system status of an endpoint:

1. Open the **Endpoint Details** page for the endpoint you wish to view, and select the **Status** tab, as shown in Figure 34.

Identification **Software** **Update History** **Status**

Summary

Timestamp: 11/17/2009 11:36:54 AM (1 second ago)

Hardware

Part Number: 200024
Board Number: Version not available
Serial Number: 001613010030

Call Status

Call Status: Not in a call

SIP Status

Status: Unregistered

Call Participants

Status	ID	Name	Site	Duration	Endpoint Type	Voice Codec	Picture Sharing
This endpoint	0	admin	-	-	-	-	Disabled

Stream Status

No currently active media streams

Figure 34 – Endpoint Details Status Tab

2. If the endpoint is online and detailed system status is available, the status will be displayed in the **Status** tab. A timestamp indicating when the status information was obtained will be shown in the **Summary** section.
3. If the endpoint's detailed system status is not available, or you wish to refresh the displayed status information, click the **SNMP Refresh** link at the top of the **Endpoint Details** page. This will command the Windows Service to attempt to communicate with the endpoint using SNMP to obtain updated status information.



If an endpoint is configured to use the Web Service interface it will periodically report its detailed system status every reporting interval, as well as every time its status changes between reporting intervals.



*Detailed system status is not retrieved during background SNMP polling. If an endpoint is online and the detailed system status is not displayed, you must click **SNMP Refresh** to retrieve it.*

9 Software and Configuration Updates

Onsight Management Suite can be used to push software and configuration updates to remote Onsight endpoints.

→ To apply software or configuration updates to remote Onsight endpoints:

1. Add the endpoints to Onsight Management Suite. For more information, refer to the **Adding Managed Endpoints** section on page 26.
2. Create or add the software and configuration packages you wish to apply.
3. Create a software update job containing the endpoints you wish to update, and the packages you wish to install to those endpoints.

9.1 Packages

Software and configuration updates are distributed to Onsight endpoints using packages. A package in Onsight Management Suite consists mainly of two components: a manifest, which is an XML file describing the version number and contents of the package, and a package archive, which holds the actual contents of the package. Onsight Management Suite currently supports the package types listed in Table 13.

Table 13 – Supported Package Types

Package Type	Endpoints	Description
Software	Onsight device Onsight Expert	Created and distributed by Librestream whenever new software releases become available. These are described further in Software Packages on page 69.
Configuration	Onsight device Onsight Expert	Allows you to apply configuration settings to remote endpoints. These are described further in Onsight Device Configuration Packages on page 51 and Onsight Expert Configuration Packages on page 55.
Users/Contacts	Onsight device Onsight Expert	Allows you to apply a list of users and shared contacts to remote endpoints. These are described further in the Users/Contacts Packages section on page 58.
Media Configuration	Onsight Expert	Allows you to apply a list of media configuration profiles to Onsight Expert endpoints. These are described further in the Media Configuration Packages section on page 65.

When an endpoint attempts to install a package, it first retrieves the associated manifest file to determine whether the package contains any applicable software or configuration updates. An endpoint will determine that a package needs to be installed if it meets the following conditions:

- The package contains software or configuration items that are supported by the endpoint.
- The individual version numbers of the items in the package differ from the currently installed items on the endpoint.



Although packages can be assigned names within Onsight Management Suite, only the version number and type of a package are used by the endpoint to determine whether or not a package needs to be installed. An endpoint will not be able to distinguish between two packages with the same version number and type, even if they have different names.

9.2 Software Update Jobs

Software and configuration packages are distributed to Onsight endpoints through the creation of software update jobs. A software update job defines a number of endpoints to be updated, along with the packages to install to those endpoints. When a software update job is created for an endpoint, the endpoint will attempt to contact the package server to download and install the update the next time it communicates with the server over either the Web Service or SNMP interfaces.

For a software or configuration update to proceed:

- The endpoint must not already be performing a software update or activation job.
- The endpoint must not be in a call, recording or playing back a recording.
- If the endpoint is an Onsight device, it must be connected to an external power source.

A software update job will be considered successful if, upon completion, the version numbers of the installed software and configuration items on an endpoint match the version numbers of all items in the packages assigned to the update job. If for some reason the update job should fail for an endpoint, the update job will be reattempted up to a configurable number of times.

9.2.1 Configuring Software Update Job Settings

→ To configure software update job settings:

1. Choose **Options > Service Settings**. You will be presented with the **Service Settings** screen as shown in Figure 8.
2. Locate the **Update Job Configuration** section.
3. Configure the software update jobs settings described in Table 14, as required.

Table 14 – Update Job Settings

Update Retry Interval	The time to wait between failed update job attempts, in seconds.
Maximum Retry Attempts	The number of times to automatically attempt an update job.

4. Click **Save** to save your changes.



*After the **Update Retry Interval** expires, the software update job will be reattempted the next time an endpoint connects over the Web Service or SNMP interfaces.*

9.2.2 Creating a New Software Update Job

→ To create a new software update job:

1. Choose **Software Update Jobs > Create Software Update Job**. You will be presented with the **Create Software Update Job Wizard** as shown in Figure 35.

Create Software Update Job

Step 1 - Choose Update Job Details

Details

Name:

Next Cancel

Figure 35 – Choose Update Job Details

2. In the **Details** section, enter a name for the software update job. This name will be used to identify the software update job at a later time. Once you have entered a name, click **Next**.
3. You will be presented with the **Select Endpoints** step, as shown in Figure 36.

Step 2 - Select Endpoints

Endpoint Group: All Endpoints Lab

All Endpoints

Selected: 2 [Clear Selected](#)

<input type="checkbox"/>	Name	Type	Address	Remote Address	Software	Config.	Users / Contacts	Media Config.	Sub-Group
<input checked="" type="checkbox"/>	MCD00086B0BA69D	Onsight Device	-	192.168.1.141	4.2.10.3	1.0.0.3	Unknown	Unknown	-
<input checked="" type="checkbox"/>	MCD0023A7000253	Onsight Device	-	192.168.1.159	4.2.10.3	Unknown	Unknown	Unknown	-
<input type="checkbox"/>	ONSIGHTEXPERTPC	Onsight Expert	192.168.1.174	192.168.1.174	4.2.5.0	Unknown	Unknown	Unknown	-

Figure 36 – Select Endpoints

4. The list of managed endpoints in the system, along with their current software and configuration version numbers, will be displayed. Select the endpoints from the list that you wish to add to the software update job and click **Next**.



*If you navigated to the **Create Software Update Job Wizard** from the **Managed Endpoints** page, the endpoints selected on that page will be pre-selected for you in the **Select Endpoints** table.*

5. You will be presented with the **Select Packages** step, as shown in Figure 37.

Step 3 - Select Packages

Software Update Packages

Onsight Expert:

[None]

Onsight Device:

[None]

Configuration Packages

Onsight Expert:

[None]

Onsight Device:

[None]

Users / Contacts Packages

Users / Contacts:

Default Contacts (1.0.0.0)

Media Configuration Packages

Media Configurations:

[None]

Figure 37 – Select Packages

- Select the packages you wish to add to the software update job. You can choose one of each type of available package.



Selected packages will be installed on every supported endpoint assigned to the update job. If a particular package is not installable on an endpoint (for example, attempting to install an Onsight Expert configuration package onto an Onsight device endpoint), it will be ignored by that endpoint when the update job is initiated.

- Click **Finish** to create the software update job. You will be redirected to the **Update Jobs** page where you can view the status of your software update job.

9.2.3 Viewing Existing Software Update Jobs

To view the list of software update jobs in the system, choose **Software Update Jobs > View Software Update Jobs**. You will be presented with a list of all of the previously created software update jobs, as shown in Figure 38.

Update Jobs

Add Delete Reload Table									
<input type="checkbox"/>	Name	Created Date	Packages	Endpoints	Succeeded	Cancelled	Failed	Status	
<input type="checkbox"/>	Update to Latest Software	11/16/2009 12:43:56 PM	1	1	0	1	0	Completed	delete
<input type="checkbox"/>	New Software Update Job	11/16/2009 12:43:23 PM	2	2	0	0	0	Active	delete

Figure 38 – View Software Update Jobs

Each entry in the Update Jobs table will contain the information described in Table 15.

Table 15 – Update Jobs Table Columns

Name	The name used to identify the software update job.
Created Date	The date and time the software update job was created.
Packages	The number of packages assigned to the software update job.
Endpoints	The number of endpoints assigned to the software update job.
Succeeded	The number of endpoints that have successfully installed all applicable packages in the software update job, or for which there were no updates available.
Cancelled	The number of endpoints for which the software update job was cancelled.
Failed	The number of endpoints that reached the maximum number of failed update attempts, and are waiting for administrator input to proceed.
Status	The status of the software update job, either Completed or Active .

In addition to the information described above, action buttons are included at the top of the table, as described in Table 16.

Table 16 – Update Jobs Actions

Add	Directs you to the Create Software Update Job Wizard where you can create a new software update job.
Delete	Cancels and deletes the selected software update jobs from the system. You can also delete an individual software update job by clicking its corresponding delete link in the table.
Reload Table	Refresh the page to display the current status of each software update job in the table.

9.2.4 Modify an Existing Software Update Job

To modify an existing software update job, locate it in the list and click on its name. You will be taken to the **Update Job Details** screen, as shown in Figure 39. The name of the update job you are viewing will be shown at the top of your screen. The **Update Job Details** screen is divided into three main sections: Details, Packages and Endpoints.

Details for Update Job New Software Update Job

Details

Name:

New Software Update Job

Created:

11/16/2009 12:43:23 PM

Status:

Active

Save

Cancel

Packages

Package Name	Type	Version
Warehouse Contacts	Users / Contacts	2.0.0.0
Onsight Device 3.98	Onsight Device Software	3.98.0.0

Endpoints

	Name	Type	Status	Last Attempt Initiated	Next Attempt	Attempts	
⊕	MCD12345678	Onsight Device	Waiting for Device	-	-	0	Cancel
⊕	LABPC	Onsight Expert	Succeeded	11/16/2009 2:57:19 PM	-	2	

Figure 39 – Update Job Details**9.2.4.1 Details**

The **Details** section of the **Update Job Details** page displays the name of the update job, the date it was created, and the overall status of the update job. To change the name of an update job, enter a new name for the update job in the **Name** field, and click **Save** to save your changes.

9.2.4.2 Packages

The **Packages** section of the **Update Job Details** page displays a table of packages that were assigned to the update job. The name, type and version number of each package is displayed in the table. The version numbers of the displayed packages will correspond to the version numbers of the packages at the time the software update job was created. To view a package's current contents, click its name in the table to be taken to the details page for that package.

9.2.4.3 Endpoints

The **Endpoints** section of the **Update Job Details** page displays a table of endpoints that were assigned to the update job. Each entry in the table will contain the information described in Table 17.

Table 17 – Update Job Endpoints Columns

Name	The name of the endpoint. Clicking the name of an endpoint in the table will take you to the Endpoint Details page for that endpoint. If an endpoint was deleted after the software update job was created, its name will be shown using a strikethrough font.
Type	The type of endpoint.
Status	<p>The status of the software update job for that endpoint, which will be one of the following:</p> <ul style="list-style-type: none"> • Queued – The job is waiting in the queue for one or more update jobs to complete. • Waiting for Endpoint – Onsight Management Suite is ready to initiate the next update attempt, and is waiting for the endpoint to be ready. • Initiated – Onsight Management Suite has communicated the details of the update job to the endpoint, and is waiting for it to report further status. • In Progress – The endpoint reports that the update is in progress. • Attempt Failed – The previous attempt failed. Onsight Management Suite is waiting until the time indicated by the Next Attempt column before it will initiate a new attempt. • Max Attempts Reached – The maximum number of failed attempts was reached for the update. Administrator intervention is required to proceed. • Cancelled – The update was cancelled by the administrator. • Succeeded – The update completed successfully. • No Updates Found – The version numbers of the endpoint already match those of the packages assigned to the update job. • Unknown – The status of the update job for the endpoint is unknown.
Last Attempt Initiated	The date and time the last update attempt was initiated.
Next Attempt	The date and time of the next update attempt.
Attempts	The total number of update attempts.



*The status of an update job for an endpoint can only be updated only when the endpoint is online. If an endpoint's status changes to either offline or not responding while an update job is in progress, the status of the update job for that endpoint will remain **In Progress** until the next time the endpoint comes online.*

If the update job you are viewing is still active for an endpoint, the final column in the table will display one or more actions that can be performed on the update job, depending on its current status:

- **Cancel** allows the administrator to cancel the update job for a particular endpoint at any time. Cancelling an update job for an endpoint will have no effect on the other endpoints assigned to the update job.

- **Retry Now** allows the administrator to command Onsight Management Suite to begin the next update attempt if it is in the **Attempt Failed** state. This initiates the update job as soon as the endpoint is ready, without waiting for the time displayed in the **Next Attempt** column.
- **Reset** allows the administrator to reset the attempt count of an endpoint if it is in the **Max Attempts Reached** state. This will set the attempt count back to zero, allowing Onsight Management Suite to re-attempt the update job on that endpoint.

The logged history of update attempts for an endpoint can also be viewed by clicking the **+** button next to its name in the **Endpoints** table on the **Update Job Details** page. This will reveal a log of update events for that endpoint, including the date and time of each attempt, as shown in Figure 40. If an update attempt has failed, the update job history log will display the reason for the failure, allowing you to diagnose the problem before the next scheduled attempt.

⊟ LABPC	Onsight Expert	Succeeded	11/16/2009 2:57:19 PM	-	2
Update Job History:					
Timestamp		Status			
11/16/2009 2:57:34 PM		Update job completed successfully.			
11/16/2009 2:57:20 PM		Update is in progress.			
11/16/2009 2:57:19 PM		Update attempt initiated by server.			
11/16/2009 2:57:18 PM		Next attempt requested by administrator. Waiting for device.			
11/16/2009 2:57:12 PM		The device reports that the update failed for the following reason: 'Failed - There was a problem downloading the manifest. Check the Base Website URL setting on the Service Settings page.'			
11/16/2009 2:55:06 PM		Update is in progress.			
11/16/2009 2:55:06 PM		Update attempt initiated by server.			
11/16/2009 12:43:23 PM		Update job dequeued. Waiting for device.			
11/16/2009 12:43:23 PM		Update job created.			

Figure 40 – Update Job History

10 Onsight Device Configuration Packages

Onsight Management Suite allows administrators to create Onsight device configuration packages that can be applied to Onsight device endpoints. An Onsight device configuration package created by Onsight Management Suite is intended to be created offline and then applied to multiple Onsight devices. As a result, items which are device-specific, such as device name, static IP address and device specific SIP settings cannot currently be configured by Onsight device configuration packages.

An Onsight device configuration package consists of multiple configuration files. When viewing the currently installed version of a configuration package on an Onsight device you will notice five separate version numbers: Access Control, Application Settings, Core Settings, Registry Configuration and Preferred Networks.



When installing an Onsight device configuration package onto an Onsight device, the version number of the package will be applied to all five configuration files. However, if Access Control settings are not present in the package, its version number will remain unchanged.

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

- All configuration settings on the Onsight device 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 Onsight device will be added to the Onsight device.

The exception to this is the installation of wireless preferred networks and VPN connections, which are handled as follows:

- A preferred network or VPN connection that exists on the Onsight device with the same SSID or name as one found in the package will be overwritten.
- Preferred networks or VPN connections that **do not** exist on the Onsight device, but exist in the package, will be added to the Onsight device.
- None of the existing preferred networks or VPN connections on the Onsight device will be deleted. They must be removed manually from the Onsight device by an administrator.

10.1 Creating an Onsight Device Configuration Package

→ To create a new Onsight device configuration package:

1. Choose **Package Management > Onsight Device Configurations > Add Onsight Device Configuration Package**. You will be presented with the **New Onsight Device Configuration Package** screen as shown in Figure 41.

New Onsight Device Configuration Package

Identification

Package Name:

Version:

Save **Cancel**

Configuration

General **Display** **Video** **Audio** **Call Control** **Network** **Radio** **Security** **Remote Management** **Time** **Maintenance** **Access Control**

Power

Standby Timeout (minutes):
(0 to disable) Min: 0, Max: 120

Media

Media Path:
Example: \\Storage Card\\Media

While sharing an image, the video:

☒ Continues
☐ Pauses
☐ Stops

Figure 41 – New Onsight Device Configuration Package

- Enter the information that is required to identify the new Onsight device configuration package in the **Identification** section, as shown in Table 18.

Table 18 – Onsight Device Configuration Package Identification

Package Name	Enter the name of the package. This name must be unique to all Onsight device configuration packages and must be a valid Windows filename. This name is used to identify the package when assigning it to an Onsight endpoint.
Version	Enter the version of the Onsight device configuration package. The 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, navigate through the tabs and set up the desired Onsight device configuration.
- Click the **Save** button to save your changes and create the Onsight device configuration package.

10.1.1 Importing Access Control Settings

An Onsight device configuration package can contain an Access Control settings file, which allows an administrator to control which Onsight device settings can be configured by users and administrators. For more information on maintaining Access Control settings files, refer to the **Configuration Access Control** section on page 96.

→ To include Access Control in an Onsight device configuration package:

- Navigate to the **Access Control** tab in the **Configuration** section, as shown in Figure 42.

Figure 42 - Access Control Tab

2. Select the **Include Access Control settings in this package** checkbox.
3. Click the **Browse** button and select the Access Control settings file that you wish to include.
4. Press the **Import** button to upload the file to the server. Your selected Access Control settings file will now be shown in the **Access Control Settings** box.
5. Click **Save** to save the configuration package.



If you choose not to include Access Control settings in an Onsight device configuration package, the Onsight device's currently installed Access Control settings will remain unchanged when the package is installed. To remove an Onsight device's Access Control settings and revert them to their default values, include a default settings file in a new Onsight device configuration package and install it to the device.

10.2 View Existing Onsight Device Configuration Packages

To view the list of Onsight device configuration packages in the system, choose **Package Management > Onsight Device Configurations > View Onsight Device Configuration Packages**. You will be presented with a list of all of the Onsight device configuration packages that were previously created, as shown in Figure 43. Each item in the list displays the name, the version number, and the last modified time of the package. You can also create a new Onsight device configuration package by clicking the **Create New** button, located at the bottom of the list.


Onsight Device Configuration Packages

Package Name	Version	Last Modified	
Default	1.0.0.0	10/14/2009 9:01:00 AM	save package delete
NewDeviceConfig	2.0.0.0	11/26/2009 11:31:35 AM	save package delete
Telestration	3.0.0.1	11/26/2009 11:31:45 AM	save package delete

[Create New](#)

Figure 43 – View Onsight Device Configuration Package List

From here, you may perform a number of tasks on each package.

- **Save Package** allows you to download a ZIP file containing an Onsight device 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 Onsight device endpoints.
- **Delete** removes the package from the system. If an Onsight device configuration package is a member of an active update job it cannot be deleted and its **delete** link will be replaced by the  icon.

10.3 Modifying an Existing Onsight Device Configuration Package

To modify an existing Onsight device configuration package, locate it in the list and click on its package name. You will be taken to a screen similar to the one shown in Figure 41.

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 Onsight device configuration package, as well as modify the Onsight device configuration settings. Modify the fields as required and click **Save** to save the changes.



The version number of an Onsight device configuration package should be changed whenever modifications are made to the package. If the version number is not changed, an Onsight device endpoint with the same version number will fail to download and install it if an update is attempted.



If an Onsight device configuration package is a member of an active update job it cannot be modified. You can still view the package by clicking its package name in the Onsight device configuration package list, but you will not be able to make or save changes to the package.

11 Onsight Expert Configuration Packages

Onsight Management Suite allows administrators to create Onsight Expert configuration packages that can be applied to Onsight Expert endpoints.

An Onsight Expert configuration package consists of multiple configuration files. When viewing the currently installed version of a configuration package on an Onsight Expert you will notice two separate version numbers: Access Control and Configuration.



When installing an Onsight Expert configuration package onto an Onsight Expert, the version number of the package will be applied to both configuration files. However, if Access Control settings are not present in the package, the version number of Access Control will remain unchanged.

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

- All configuration settings on the Onsight Expert application 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 Onsight Expert application will be added to the Onsight Expert application.

11.1 Creating an Onsight Expert Configuration Package

→ To create a new Onsight Expert configuration package:

1. Choose **Package Management > Onsight Expert Configurations > Add Onsight Expert Configuration Package**. You will be presented with the **New Onsight Expert Configuration** screen as shown in Figure 44.

New Onsight Expert Configuration Package

Figure 44 – New Onsight Expert Configuration Package

2. Enter the information that is required to identify the new Onsight Expert configuration package in the **Identification** section, as shown in Table 19.

Table 19 – Onsight Expert Configuration Package Identification

Package Name	Enter the name of the package. This name must be unique to all Onsight Expert Configuration packages and must be a valid Windows filename. This name is used to identify the package when assigning it to an Onsight endpoint.
Version	Enter the version of the Onsight Expert configuration package. The 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, navigate through the tabs and set up the desired Onsight Expert configuration.
4. Click the **Save** button to save your changes and create the Onsight Expert configuration package.

11.1.1 Importing Access Control Settings

An Onsight Expert configuration package can contain an Access Control settings file, which allows an administrator to control which Onsight Expert settings can be configured by users and administrators. For more information on maintaining Access Control settings files, refer to the **Configuration Access Control** section on page 96.

→ To include Access Control in an Onsight Expert configuration package:

1. Navigate to the **Access Control** tab in the **Configuration** section, similar to one displayed while editing Onsight device configuration packages shown in Figure 42.
2. Select the **Include Access Control settings in this package** checkbox.
3. Click the **Browse** button and select the Access Control settings file that you wish to include.
4. Press the **Import** button to upload the file to the server. Your selected Access Control settings file will now be shown in the **Access Control Settings** box.
5. Click **Save** to save the configuration package.



If you choose not to include Access Control settings in an Onsight Expert configuration package, the Onsight Expert's currently installed Access Control settings will remain unchanged when the package is installed. To remove an Onsight Expert's Access Control settings and revert them to their default values, include a default settings file in a new Onsight Expert configuration package and install it to the endpoint.

11.2 View Existing Onsight Expert Configuration Packages

To view the list of Onsight Expert configuration packages in the system, choose **Package Management > Onsight Expert Configurations > View Onsight Expert Configuration Packages**. You will be presented with a list of all of the Onsight Expert configuration packages that were previously created, as shown in Figure 45. 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. You can also create a new Onsight Expert configuration package by clicking the **Create New** button located at the bottom of the list.


Onsight Expert Configuration Packages

Package Name	Version	Last Modified	
Default	1.0.0.0	11/26/2009 11:49:30 AM	save package delete
SetAccessControl	2.0.0.1	11/26/2009 11:49:44 AM	save package delete

[Create New](#)

Figure 45 – View Onsight Expert Configuration Package List

From here, you may perform a number of tasks on each package:

- **Save Package** allows you to download a ZIP file containing an Onsight Expert 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 Onsight Expert client software can be configured to query.
- **Delete** removes the package from the system. If an Onsight Expert configuration package is a member of an active update job it cannot be deleted and its **delete** link will be replaced by the  icon.

11.3 Modifying an Existing Onsight Expert Configuration Package

To modify an existing Onsight Expert configuration package, locate it in the list and click on its package name. You will be taken to a screen similar to the one shown in Figure 44.

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 Onsight Expert configuration package, as well as modify the Onsight Expert configuration settings. Modify the fields as required and click **Save** to save the changes.



The version number of an Onsight Expert configuration package should be changed whenever modifications are made to the package. If the version number is not changed, an Onsight Expert endpoint with the same version number will fail to download and install the package if an update is attempted.



If an Onsight Expert configuration package is a member of an active update job it cannot be modified. You can still view the package by clicking its package name in the Onsight Expert configuration package list, but you will not be able to make or save changes to the package.

12 Users/Contacts Packages

Onsight Management Suite 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 Onsight endpoints.

When a Users/Contacts package is applied to an Onsight 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 of existing users will either be changed or be maintained, depending on the **Reset Existing Password** setting for each user. 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.

12.1 Creating a New Users/Contacts Package

→ To create a new Users/Contacts package:

1. Choose **Package Management > Users / Contacts > Add Users / Contacts Package**. You will be presented with a **New Users / Contacts Package** screen similar to the one in Figure 46.

New Users / Contacts Package



Figure 46 – New 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 20.

Table 20 – Users/Contacts Package Identification

Package Name	Enter the name of the package. This name must be unique to all Users/Contacts packages and must be a valid Windows filename. This name is used to identify the package when assigning it to an Onsight endpoint.
Version	Enter the version of the Users/Contacts package. The 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 package by

	selecting it from the list.
--	-----------------------------

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

12.2 View Existing Users/Contacts Packages

To view the list of Users/Contacts packages in the system, choose **Package Management > 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 47. 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. You can also create a new Users/Contacts package by clicking the **Create New** button, located at the bottom of the list.


Users / Contacts Packages

Package Name	Version	Last Modified	# Users	# Contacts	
Default Contacts	1.0.0.0	11/26/2009 11:53:38 AM	1	0	save package export to file delete
Warehouse Contacts	2.0.0.0	11/16/2009 12:31:16 PM	1	0	save package export to file delete

Create New

Figure 47 – View Users/Contacts Package List

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 Onsite endpoints or to a standalone web server, which Onsite endpoints can be configured to query.
- Export to File** allows you to download an encrypted version of a package's Users/Contacts XML file. This file can be imported into Onsite endpoints without using the software update interface.
- Delete** removes the package from the system. If a Users/Contacts package is a member of an active update job it cannot be deleted and its **delete** link will be replaced by the  icon.

12.3 Modifying an Existing Users/Contacts Package

To modify an existing Users/Contacts package, locate it in the list and click its package name. You will be taken to a screen similar to the one shown in Figure 48.

Modify Users / Contacts Package Default Contacts

Identification

Package Name:
Version:

Save Cancel

Import Users and Contacts

Browse...

Import

Users

User Name	Full Name	Reset Existing Password	
admin	The Administrator	<input type="checkbox"/>	

Create New User

Shared Contacts

Name	Address	Type	
John Smith	192.168.1.44	Onsight Device	delete

Create New Contact

Figure 48 – 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 and version number of the Users/Contacts package. Modify the fields as required and click **Save** to save the changes.



The version number of a Users/Contacts package should be changed whenever new users or shared contacts are added to the package. If the version number is not changed, Onsight endpoints with the same version number will fail to download and install the package if an update is attempted.



If a Users/Contacts package is a member of an active update job it cannot be modified. You can still view the package by clicking its package name in the Users/Contacts package list, but you will not be able to make or save changes to the package.

12.4 Maintaining the Users List

Below the **Identification** section is the list of users that are configured for the Users/Contacts package. The table displays the User Name of each user, the Full Name of the user, column indicating whether or not a user's password or FIPS settings will be reset when the package is installed, and a list of actions that can be performed on the user.

12.4.1 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 49.

Modify Users / Contacts Package Default Contacts

Modify user john

Identification

User Name:

john

Password:

☒ Reset Existing Password

First Name:

John

Last Name:

Smith

☐ Administrator

URI:

john@mydomain

💡 When modifying a user's password, ensure that it meets the password policy on all endpoints where this package will be installed.

SIP Server

☐ Enable SIP Registration

Address:

User Name:

Password:

Type:

☒ Digest

Transport:

TCP

Cisco Presence

☐ Connect to Cisco Unified Presence Server

Address:

SIP Proxy Domain:

FIPS Encryption

User ID:

Password:

☐ Reset Existing FIPS Settings

Save

Cancel

Figure 49 – Create New User

2. In the **Identification** section, fill in the fields necessary for defining the new user, as shown in Table 21.

Table 21 – 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.
Password	Enter the user's password.
Reset Existing Password	If this option is selected, the user's password will be replaced with the one configured in the package if the user already exists on the endpoint. If this option is not selected, the user's password will remain unchanged on the endpoint, regardless of what is set in the package.
First Name	Enter the user's 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.



When modifying a user's password, ensure that it meets the password policy on all endpoints where this package will be installed.

3. In the **SIP Server** section, enter the SIP server information necessary for routing calls through to the user as described in Table 22.

Table 22 – 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.

4. In the **Cisco Presence** section, enter the information necessary for connecting to a Cisco Unified Presence Server (CUPS) as described in Table 23.

Table 23 – User CUPS Settings

Connect to Cisco Unified Presence Server	Check to connect to a CUPS server.
Address	Enter the address of the CUPS server.
SIP Proxy Domain	Enter the SIP Proxy Domain.

5. In the **FIPS Encryption** section, enter the information necessary for enabling FIPS encryption as described in Table 24.

Table 24 - User FIPS Settings

User ID	Enter the user's FIPS user ID.
Password	Enter the user's FIPD password.
Reset Existing FIPS	If this option is selected, the user's FIPS settings will be replaced

Password	with the settings configured in the package if the user already exists on the endpoint. If this option is not selected, the user's FIPS settings will remain unchanged on the endpoint, regardless of what is set in the package.
----------	---

- 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 **Onsight System Administration Manual**.

12.4.2 Modify an Existing User

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

12.4.3 Deleting a User

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

12.5 Maintaining the Contacts List

Below the **Users** section is the 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.

12.5.1 Create a New Contact

→ To create a new contact:

- Click the **Create New Contact** link, located below the Shared Contacts table. You will be presented with the **Create New Shared Contact** screen, shown in Figure 50.

Modify Users / Contacts Package Default Contacts

Create New Shared Contact

Name:

Address:

Type:

Figure 50 – Create New Shared Contact

- In the **Identification** section, fill in the fields necessary for defining the new contact as described in Table 25.

Table 25 – 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: Onsight Expert, Onsight device or 3 rd Party Device.

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

For a more detailed explanation of Shared Contacts, refer to the **Onsight System Administration Manual**.

12.5.2 Modify an Existing Contact

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

12.5.3 Deleting a Contact

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

12.6 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 Onsight Expert application or Onsight Management Suite.
3. Click **Import**. The users and contacts are imported into the package using the rules described on page 58.

13 Media Configuration Packages

Onsight Management Suite allows administrators to create Media Configuration packages that can be applied to Onsight Expert software client endpoints. A media configuration defines a set of video properties for a particular media stream.

When a Media Configuration package is applied to an Onsight Expert endpoint the following rules are applied, by default:

- Any configurations present on the endpoint with the same name as a configuration 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.

Deleting configurations on an endpoint before the above rules are applied can be accomplished by configuring the package's **Merge Method** setting, as described in Table 26.

13.1 Creating a New Media Configuration Package

→ To create a new Media Configuration package:

1. Choose **Package Management > Media Configurations > Add Media Configuration Package**. You will be presented with the **New Custom Media Configuration Package** screen as shown in Figure 51.

New Custom Media Configuration Package

Figure 51 – New Media Configuration Package

2. Enter the information that is required to identify the new Media Configuration package in the **Identification** section shown in Table 26.

Table 26 – Media Configuration Package Identification

Package Name	Enter the name of the package. This name must be unique to all Media Configuration packages and must be a valid Windows filename. This name is used to identify the package when assigning it to an Onsight Expert endpoint.
Version	Enter the version of the Media Configuration package. The version number is used by endpoints to determine whether or not this package has already been installed. The default is 1.0.0.0.
Merge Method	Choose how the configurations will be merged onto the endpoint:

	<ul style="list-style-type: none"> • Merge Only – Configurations will be merged onto the endpoint as described on page 65. • Delete Remote Profiles Before Merge – Before performing the merge operation, delete any profiles that were previously added to the endpoint as a result of installing a Media Configuration package. This has the effect of replacing the entire list of remotely created configurations with the ones in the package, while maintaining any configurations that were created locally. • Delete All Profiles Before Merge – Before performing the merge operation, delete all configurations from the endpoint. This has the effect of replacing the entire list of custom configurations on the endpoint (other than the predefined Low, Medium and High configurations) with the ones in the package.
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.

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

13.2 View Existing Media Configuration Packages

To view the list of Media Configuration packages in the system, choose **Media Configurations > View Media Configuration Packages**. You will be presented with a list of all the of Media Configuration packages that were previously created, as shown in Figure 52. 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. You can also create a new Media Configuration package by clicking the **Create New** button located at the bottom of the list.


Media Configuration Packages

Package Name	Version	Last Modified	# Configurations	Merge Method	
Low Bandwidth Profiles	3.0.0.1	11/26/2009 11:58:36 AM	2	Merge Only	save package delete
Reset to Default	1.0.0.0	11/26/2009 11:59:06 AM	1	Delete All	save package delete

Create New

Figure 52 – View Media Configuration Package List

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 Onsite Expert client software can be configured to query.
- **Delete** removes the package from the system. If a Media Configuration package is a member of an active update job it cannot be deleted and its **delete** link will be replaced by the  icon.

13.3 Modifying an Existing Media Configuration Package

To modify an existing Media Configuration package, locate it in the list and click its name. You will be taken to a screen similar to the one shown in Figure 53.

Modify Media Configuration Package Low Bandwidth Profiles

Identification

Package Name:

Low Bandwidth Profiles

Version:

3.0.0.1

Merge Method:

Merge Only

Save

Cancel


Configurations


Custom Profile Name	
LowBitrate	delete

Create New

Figure 53 – 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.

- 

The version number of a Media Configuration package should be changed whenever new configurations are added to the package. If the version number is not changed, Onsite Expert endpoints with the same version number will fail to download and install the package if an update is attempted.
- 

If a Media Configuration package is a member of an active update job it cannot be modified. You can still view the package by clicking its package name in the Media Configuration package list, but you will not be able to make or save changes to the package.

13.4 Maintaining the Media Configurations List

Below the **Identification** section is the 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.

13.4.1 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 54.

Modify Media Configuration Package Low Bandwidth Profiles

Create New Media Configuration

Identification

Name:

LowBitrate

Video

Device Type:

NTSC

Resolution:

640 x 480 - VGA

Frame Rate (fps):

10

GOP:

5

Target Bitrate (kbps):

256

Min: 8, Max: 2500

☐ Hard Limit

☒ Soft Limit

Choose higher **Frame Rate** values to optimize the video for smooth motion, and lower values to optimize for increased detail.

Choose higher **GOP** values to optimize the video for quality, and lower values to optimize for reliability.

Save

Cancel

Figure 54 – Create New Media Configuration

2. In the **Identification** section, fill in the fields necessary to define the new configuration, as shown in Table 27.

Table 27 – New Media Configuration Identification

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

3. In the **Video** section, fill in the video parameters for the configuration.
4. 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 configurable video parameters, refer to the **Onsite System Administration Manual**.

13.4.2 Modify an Existing Media Configuration

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

13.4.3 Deleting a Media Configuration

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

14 Software Packages

When new versions of Onsight device or Onsight Expert software are available, they will be pre-packaged and distributed by Librestream. Administrators can add these software packages to Onsight Management Suite and apply them remotely to Onsight endpoints.

When a software package is applied to an Onsight endpoint, the following rules are applied:

- For Onsight device endpoints, if the version of software does not match the version in the package, the software will be installed on the endpoint.
- For Onsight Expert endpoints, only newer versions of the Onsight Expert software will be downloaded and installed.



*Installing an Onsight Expert software package may require that a release key be entered during the installation process. Rather than requiring that the end user enter a release key manually, Onsight Management Suite can provide it to the installer automatically. Refer to the **Onsight Expert Release Keys** section on page 90 for more information.*

14.1 Adding a New Software Package

→ To add a software package:

1. Choose **Package Management > Software Updates > Add Software Update Package**. You will be presented with the **Add Software Package** screen as shown in Figure 55.

Add Software Package

Identification

Package Name:

Software Package

No file chosen

The uploaded file must be a valid Librestream software update package ZIP file.
If you obtained the software release in the form of an archive containing both a Manifest.xml file and <PackageName>.zip file, you must unpack the archive and upload only the contained software update package ZIP file.

Figure 55 – Add Software Package

2. Enter the information that is required to identify the new Software package in the **Identification** section shown in Table 28.

Table 28 – Software Package Identification

Package Name	Enter the name of the package. This name must be unique to all Software packages and must be a valid Windows filename. This name is used to identify the package when assigning it to an Onsite Expert endpoint.
--------------	--

- In the **Upload New Software Package** section, click the **Browse** button and select the ZIP archive of the software package you want to upload.
- Click the **Upload** button to upload the package to the server. Once the package has been uploaded successfully, you will see its details listed in the **Package Details** section.



Depending on its size, uploading a package may take up to a few minutes. The progress of the upload will be shown in a popup window.

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

14.2 View Existing Software Packages

To view the list of Software packages in the system, choose **Package Management > Software Updates > View Software Update Packages**. You will be presented with a list of all the Software packages that were previously created, as shown in Figure 56. Each item in the list displays the name of the package, the type of endpoint the package can be installed on, the version number of the package, the last modified time of the package and any comments contained in the package manifest. You can also add a new Software package by clicking the **Add Package** button, located at the bottom of the list.

Software Update Packages

Package Name	Type	Version	Last Modified	Comments	
OE 4.0.0	Onsite Expert Software	4.0.0.0	11/3/2009 4:39:13 PM	Please see the release notes for more details.	delete
Onsite Device 3.98	Onsite Device Software	3.98.0.0	10/9/2009 2:08:03 PM	Please see the release notes for more details.	
Onsite Device 3.98.54.3	Onsite Device Software	3.98.54.3	10/9/2009 2:41:10 PM	Please see the release notes for more details.	delete
Onsite Device 3.99.5.74	Onsite Device Software	3.99.5.74	9/21/2009 4:19:48 PM	Please see the release notes for more details.	delete

Add Package

Figure 56 – View Software Package List

From here, you may perform the following of tasks on each package:

- Delete** removes the package from the system. If a Software package is a member of an active update job it cannot be deleted and its **delete** link will be replaced by the icon.

14.3 Modifying an Existing Software Package

To modify an existing Software package, locate it in the list and click its package name. You will be taken to a screen similar to the one shown in Figure 55.

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 of the Software package. Modify the fields as required and click **Save** to save the changes.



If a Software package is a member of an active update job it cannot be modified. You can still view the package by clicking its package name in the Software package list, but you will not be able to make or save changes to the package.

15 Statistics Collection

Onsight Management Suite can be configured to collect usage statistics from Onsight endpoints over the Web Service interface. Collected statistics include conference, call, media stream and endpoint event statistics. Statistics are stored in the Onsight Management Suite database until they are explicitly cleared by an administrator. Statistics can either be viewed directly using the Onsight Management Suite User Interface, or exported to comma-separated values (CSV) files for further analysis.



Endpoints do not support reporting statistics over the SNMP management interface.

In order for an endpoint to report statistics to Onsight Management Suite:

- Statistics collection must be enabled in Onsight Management Suite.
- The statistics reporting setting on the endpoint must be enabled
- The endpoint must be communicating with Onsight Management Suite over the Web Service interface.

If an endpoint is not able to connect to the Web Service interface to report statistics, it will cache them locally until either the next time the connection is successful or until there is no remaining space available in its local statistics cache. The local statistics cache on an endpoint will store roughly fifty unreported call records and their associated media stream records. When the cache is filled, older records will be purged to make room for newer ones. Any statistics that are cleared from the cache before they are reported to Onsight Management Suite will be lost.



The number of calls stored in the local statistics cache depends on the nature of the calls being recorded. Hosted conferences with many participants or calls where streaming is started and stopped multiple times will take up more space in the cache, reducing the total number of calls that can be stored on an endpoint.

15.1 Enabling or Disabling Statistics Collection

→ To enable or disable statistics collection in Onsight Management Suite:

1. Navigate to **Options > Statistics Settings**. You will be presented with the **Statistics Settings** screen, as shown in Figure 57.

Statistics Settings

Collection Settings

Statistics Collection: **Enabled**

Disable Collection

Clear Statistics

Date Range:

☒ Any date
 ☐ Recorded by endpoint before: 7/6/2010
 ☐ Reported to server before: 7/6/2010

Dates are assumed to be in Coordinated Universal Time (UTC).

Statistics Type:

☐ Calls / Conferences / Media Streams
 ☐ Endpoint Events

Endpoints:

Any Endpoint

Choose Endpoints

Clear Statistics

Figure 57 - Statistics Settings

- The current state of statistics collection will be displayed in the **Collection Settings** section.
- If statistics collection is disabled, click the **Enable Collection** button to enable statistics collection on the server.
- If statistics collection is enabled, click the **Disable Collection** button to disable statistics collection on the server.



Enabling or disabling statistics collection will not clear any previously collected statistics from the database.



When statistics collection is enabled, endpoints will report all unreported statistics that were cached while statistics collection was disabled.

15.2 Viewing Collected Statistics

→ To view collected statistics:

- Navigate to **Statistics > View / Export Statistics**. You will be presented with the **View / Export Statistics** screen, as shown in Figure 58.

View / Export Statistics

Filter Parameters

Statistics Type
[Conferences](#)
[Calls](#)
[Media Streams](#)
[Endpoint Events](#)

Date Range: ☒ Date recorded by endpoint ☐ Date reported to server
Start Date: 7/6/2010 Start Time: 12:00 AM
End Date: 7/7/2010 End Time: 12:00 AM
Time Zone: ☒ Server (Central Daylight Time) ☐ UTC
User Names:
Endpoints: Any Endpoint
[Choose Endpoints](#)

Calls

[Export to CSV](#) | [Reload Table](#)

	Start Time	Call GUID	Endpoint Name	Endpoint Type	User Name	Duration	Direction	Local IP
<input checked="" type="checkbox"/>	7/6/2010 2:36:40 PM	1664B1E732A841DD86C845DC863AAC31	ONSIGHTEXPERTPC	Onsight Expert	admin	00:01:06	Outgoing	192.168.1.174
<input checked="" type="checkbox"/>	7/6/2010 2:36:55 PM	1664B1E732A841DD86C845DC863AAC31	MCD0023A7000253	Onsight Device	admin	00:01:05	Incoming	192.168.1.159
<input checked="" type="checkbox"/>	7/6/2010 2:39:18 PM	DD8AC3E3906B48548343609C15D34B95	ONSIGHTEXPERTPC	Onsight Expert	admin	00:00:49	Outgoing	192.168.1.174
<input checked="" type="checkbox"/>	7/6/2010 2:39:33 PM	DD8AC3E3906B48548343609C15D34B95	MCD0023A7000253	Onsight Device	admin	00:00:49	Incoming	192.168.1.159
<input checked="" type="checkbox"/>	7/6/2010 2:39:49 PM	393A0B3D18AC4DAEB1138C46620284A9	MCD000B6B0BA69D	Onsight Device	admin	00:00:16	Incoming	192.168.1.141
<input checked="" type="checkbox"/>	7/6/2010 2:39:50 PM	393A0B3D18AC4DAEB1138C46620284A9	ONSIGHTEXPERTPC	Onsight Expert	admin	00:00:18	Outgoing	192.168.1.174

Page 1 of 1 (6 items) [1] Records per page: 15

Figure 58 - View / Export Statistics

- Select which type of statistics to view from the **Statistics Type** section. These are described in more detail in the **Interpreting Statistics** section on page 76.
- From the **Filter Parameters** section, setup the filter parameters that will be used to display the collected statistics, as described in Table 29.

Table 29 – Statistics Filter Parameters

Date Range	<p>The range of dates to view statistics for. The date range can be specified in one of two ways:</p> <ul style="list-style-type: none"> Date recorded by endpoint – display statistics that were recorded by the endpoint between the specified dates. Date reported to server – display statistics that were reported to Onsight Management Suite between the specified dates.
Time Zone	Display statistics using either the Onsight Management Suite server's time zone or Coordinated Universal Time (UTC).
User Names	Enter a comma separated list of user names to filter statistics by.

Endpoints	Only display statistics that were reported by the specified endpoints. The default is to view statistics reported by any endpoint.
-----------	--



If both the endpoint and user name filter parameters are specified, they will be combined using the Boolean AND operator.

- If you are filtering statistics by endpoint, click the **Choose Endpoints** button. You will be presented with the **Choose Endpoints** screen shown in Figure 59.

Figure 59 - Choose Endpoints

- Choose the endpoints you wish to view reported statistics for by selecting the checkbox next to their names in the displayed table, and click the **Accept** button.



*Deleted endpoints can be selected from the **Deleted Endpoints** group. To view statistics reported by all endpoints, including deleted endpoints, click the **Clear Selected** link to the top right of the table.*

- Once all filter parameters have been chosen, click the **Apply Filter** button to display the desired statistics in the table at the bottom of the page. For more information on interpreting the displayed statistics, see **Interpreting Statistics** on page 76.

15.3 Exporting Collected Statistics

→ To export collected statistics to a CSV file:

- View the statistics you wish to export by following the instructions in **Viewing Collected Statistics** on page 73.
- Click the **Export to CSV** link at the top of the displayed statistics table.

- You will be prompted by your web browser to save a CSV file containing the displayed statistics. For more information on interpreting the exported statistics, see **Interpreting Statistics** on page 76.



*Statistics will be exported to the CSV file in the order in which they appear in the **View / Export Statistics** table. If you have sorted the displayed statistics using one of the table columns, they will be sorted by the same column in the exported file.*

15.4 Interpreting Statistics

There are currently four types of statistics reported to Onsight Management Suite by Onsight endpoints: Calls, Media Streams, Conferences and Endpoint Events. More information on each statistics type is provided in the following sections.

15.4.1 Call Statistics

Call statistics keep track of all the calls that an Onsight endpoint has participated in. They are reported to Onsight Management Suite after a call has disconnected. A call record includes the start time and length of the call, the parameters used to connect the call, and the details of the other participant in the call. For a full list of the reported data contained in a call record, refer to Table 30.

When a call takes place between two Onsight endpoints, both participants will report the call to Onsight Management Suite, resulting in two records of the same call being stored in the database. For this reason, each call reported to Onsight Management Suite includes a unique identifier called a Call GUID, which is passed between the two endpoints when the call is connected. When viewing call statistics in Onsight Management Suite, call records with the same Call GUID reported by different endpoints can be considered to be both ends of the same call. The Direction field in a call record will indicate that the call is either outgoing, for the endpoint that originated the call, or incoming, for the endpoint that received the call.



The Call GUID is generated by Onsight endpoints only, and should not be confused with the SIP Call-ID, which can be used to correlate call statistics with statistics recorded by third party equipment.



Endpoints will report the Start Time and Duration of a call independently according to their individual system clock settings. If the system clocks of endpoints involved in a call are not synchronized, they may report different Start Time values for the same call.

Call statistics can be viewed by selecting **Calls** from the **Statistics Type** section shown in Figure 58. To view the media streams that took place during a given call, press the **+** button next to the call in the **Calls** table.

Table 30 – Call Records

StartTime	Start time of the call, in the server's time zone.
StartTimeUTC	Start time of the call, in UTC.
CallGuid	A uniquely generated call identifier. Call records reported by endpoints at both ends of the same call will have the same Call GUID.
EndpointId	The Endpoint ID of the endpoint that reported the call, as described in Table 12 on page 34.
EndpointName	The name of the endpoint. This will typically be the Device / Computer Name of the endpoint.
EndpointType	The type of endpoint: Onsight device or Onsight Expert.
UserName	The user name of the user logged into the endpoint when the call took place.
Duration	The duration of the call in hh:mm:ss.
DurationSeconds	The duration of the call in seconds.
Direction	The direction of the call: Incoming or Outgoing.

LocalIp	The IP address of the reporting endpoint.
LocalPid	The conference participant ID of the reporting endpoint.
RemoteIp	The IP address of the remote endpoint.
RemotePid	The conference participant ID of the remote endpoint.
RemoteName	The name of the remote endpoint.
RemoteSite	The URI of the remote endpoint.
RemoteEndpointType	The type of the remote endpoint: Onsight device, Onsight Expert, or Unknown.
VoiceCodec	The voice codec used for the call: G.711 ALAW, GSM6.10, PCM or G7.11 ULAW.
SipCallId	The SIP Call-ID.
SipRegistered	Whether or not the reporting endpoint was registered to a SIP server at the time of the call.
SipServer	The SIP server the reporting endpoint was registered to.
SipUserName	The SIP user name of the reporting endpoint.
SipTransportType	The SIP transport type: TLS, TCP, or UDP.
SipUri	The SIP URI of the reporting endpoint.
ImageSharingMode	Whether or not the call was in image sharing mode.
VoiceOnly	Whether or not the call was voice only.
Encryption	Whether or not the call was encrypted.
TerminationReason	The reason the call was terminated: NORMAL or NETWORK_LOSS.
ReportedTime	The time the call was reported to Onsight Management Suite, in the server's time zone.
ReportedTimeUTC	The time the call was reported to Onsight Management Suite, in UTC.

15.4.2 Media Stream Statistics

Media stream statistics keep track of all media streams that were sent or received by an endpoint during a call. They are reported along with the call record after the call has disconnected. A new media stream record will be created each time streaming is started, including cases where a change in the media configuration parameters causes the stream to be restarted automatically. Media stream records include the start time, duration, and configured video and audio parameters that were used for the stream. For a full list of the reported data contained in a media stream record, refer to Table 31.



Reported video parameters such as target and peak bitrate correspond to the configured settings used for the stream. The reported values may vary from the actual observed bitrates during the stream, depending on factors such as network conditions and the nature of the video being sent.

Onsight endpoints at either end of a stream will each report a record of the stream to Onsight Management Suite. The Direction field will indicate that a stream is either outgoing, for the endpoint that sent the stream, or incoming, for the endpoint that received the stream. In order to correlate reported media streams to a particular call, each media stream record will include the Call GUID of its corresponding call, as well as the Endpoint ID of the endpoint that reported it.

Media stream statistics can be viewed by selecting **Media Streams** from the **Statistics Type** section shown in Figure 58.

Table 31 – Media Stream Records

StartTime	Start time of the media stream, in the server's time zone.
StartTimeUTC	Start time of the media stream, in UTC.
CallGuid	The Call GUID of the call the stream belongs to.
EndpointId	The Endpoint ID of the endpoint that reported the media stream, as described in Table 12 on page 34.
EndpointName	The name of the endpoint. This will typically be the Device / Computer Name of the endpoint.
EndpointType	The type of endpoint: Onsight device or Onsight Expert.
UserName	The user name of the user logged into the endpoint when the stream took place.
Duration	The duration of the stream in hh:mm:ss.
DurationSeconds	The duration of the stream in seconds.
Direction	The direction of the stream: Incoming or Outgoing.
SourcePid	The conference participant ID of the endpoint from which the stream originated.
VideoSource	The source of the video: Internal Video, S-Video or File.
VideoSourceStandard	The video standard: NTSC or PAL.
Quality	The quality setting used: Low, Medium, High or Custom.
VideoTargetBitrate	The configured target video bitrate in Kbps.
VideoPeakBitrate	The configured peak video bitrate in Kbps.
VideoFrameRate	The configured video frame rate in frames per second.
VideoResolution	The configured video resolution.
VideoGOP	The configured video GOP.
VideoCodec	The video codec.
AudioCodec	The subject audio codec: G.711 ALAW, GSM6.10, PCM or G7.11 ULAW.
AudioResolution	The subject audio resolution: 8-bit or 16-bit.
AudioSeparation	The audio separation: Mono or Stereo.
AudioSampleRate	The audio sample rate in Hz.
ReportedTime	The time the media stream was reported to Onsight Management Suite, in the server's time zone.
ReportedTimeUTC	The time the media stream was reported to Onsight Management Suite, in UTC.

15.4.3 Conference Statistics

Conference statistics keep track of hosted conferences that contain three or more participants (including the conference host). The Onsight Expert endpoint that hosted the conference will report the details of the conference to Onsight Management once all of its calls have been disconnected. For a full list of the reported data contained in a conference record, refer to Table 32.

In addition to reporting a record of the conference, the conference host will also report a call record for each call that made up the conference. In order to correlate call records to a particular conference, conference records will contain the Call GUID of each call that was part of the conference.

Conference statistics can be viewed by selecting **Conferences** from the **Statistics Type** section shown in Figure 58. To view the calls that were part of a conference, press the + button next to the conference in the **Conferences** table.

Table 32 – Conference Records

StartTime	Start time of the conference, in the server's time zone.
StartTimeUTC	Start time of the conference, in UTC.
ConferenceGuid	A uniquely generated conference identifier. Currently this is only reported by the conference host, and is not communicated to other endpoints in the conference.
HostEndpointId	The Endpoint ID of the endpoint that hosted the conference, as described in Table 12 on page 34.
HostEndpointName	The name of the endpoint that hosted the conference. This will typically be the Device / Computer Name of the endpoint.
HostUserName	The user name of the user logged into the conference host when the conference took place.
Duration	The total duration of the conference in hh:mm:ss.
DurationSeconds	The total duration of the conference in seconds.
HostPid	The conference participant ID (PID) of the host endpoint.
Participants	The number of conference participants.
CallGuids	A list of each Call GUID of the calls that were part of the conference, separated by the ' ' character.
ReportedTime	The time the conference was reported to Onsight Management Suite, in the server's time zone.
ReportedTimeUTC	The time the conference was reported to Onsight Management Suite, in UTC.

15.4.4 Endpoint Event Statistics

Endpoint event statistics keep track of certain events on Onsight device endpoints, including power on, power off and battery events. Endpoint events are reported to Onsight Management Suite as soon as they occur. For a full list of the reported data contained in an endpoint event record, see Table 33.



Power off events may not be reported until the next time the endpoint is powered back on.

Endpoint event statistics can be viewed by selecting **Endpoint Events** from the **Statistics Type** section shown in Figure 58.

Table 33 – Endpoint Event Records

EventTime	Date and time the event occurred, in the server's time zone.
EventTimeUTC	Date and time the event occurred, in UTC.
EndpointId	The Endpoint ID of the endpoint that reported the event, as described in Table 12 on page 34.
EndpointName	The name of the endpoint. This will typically be the Device / Computer Name of the endpoint.
EndpointType	The type of endpoint: Onsight device or Onsight Expert.
EventType	The type of event: BatteryCritical, BatteryLow, PowerOff, PowerOn, or Unknown.
ReportedTime	The time the event was reported to Onsight Management Suite, in the server's time zone.
ReportedTimeUTC	The time the event was reported to Onsight Management Suite, in UTC.

15.5 Clearing Collected Statistics

→ To clear collected statistics from the database:

1. Navigate to **Options > Statistics Settings**. You will be presented with the **Statistics Settings** screen, as shown in Figure 57.
2. Setup the filter parameters to use when clearing statistics from the options described in Table 34.

Table 34 - Clear Statistics Filter Parameters

Date Range	<p>The date range to use when clearing statistics, specified in one of the following ways:</p> <ul style="list-style-type: none"> • Any date – do not use the recorded or reported date to determine which statistics to clear. • Recorded by endpoint before – clear statistics that were recorded by the endpoint before the specified date. • Reported to server before – clear statistics that were reported to Onsight Management Suite before the specified date.
Statistics Type	The type of statistics to clear.
Endpoints	Clear statistics reported by the specified endpoints. Click the Choose Endpoints link to bring up a popup window allowing you to choose from the list of available endpoints.



*The **Date Range** specified when clearing statistics is assumed to be in Coordinated Universal Time (UTC).*

3. Click the **Clear Statistics** button to clear collected statistics according to the selected filter parameters. The number of calls, conferences, media streams and endpoint events that were removed from the database will be displayed at the top of the page.

16 Onsight Expert License Management

Onsight Management Suite can be used to manage and maintain Onsight Expert software licensing. This includes the ability to:

- View the current software activation status of managed Onsight Expert endpoints.
- Remotely assign activation keys to Onsight Expert endpoints to perform software activation.
- Automatically provide release keys required for software upgrades to Onsight Expert endpoints (if the software upgrade is performed through an Onsight Management Suite software update job).
- Create Onsight Expert custom install files that can be packaged with the Onsight Expert setup files, allowing for automatic configuration or activation of an Onsight Expert during installation.

16.1 Onsight Expert Software Activation

Onsight Management Suite can remotely assign activation keys to Onsight Expert endpoints, allowing an administrator to activate an Onsight Expert running in trial mode, convert a server licensed Onsight Expert to a standalone license, or re-activate an Onsight Expert with a new activation key.

→ To activate an Onsight Expert using Onsight Management Suite:

1. Add the Onsight Expert endpoint to Onsight Management Suite. For more information, refer to the **Adding Managed Endpoints** section on page 26.
2. Add the activation key to the database. For more information, refer to the **Adding Onsight Expert Activation Keys** section on page 83.
3. Create an activation job to assign the activation key to the Onsight Expert. For more information, refer to the **Creating a New Onsight Expert Activation Job** section on page 85.



Onsight Expert activation keys can be assigned over the Web Service interface only.



Onsight Management Suite simply supplies the assigned activation keys to the Onsight Expert endpoints, which in turn must communicate with the activation server in order to perform software activation with their assigned keys. Onsight Expert endpoints are therefore required to have a valid Internet connection in order for software activation to succeed.

16.1.1 Onsight Expert Activation Status

To view the current activation status of Onsight Expert endpoints, choose **License Management > Onsight Expert Software Activation > View Onsight Expert Activation Status**. You will be presented with the **Onsight Expert Activation Status** page, as shown in Figure 60.

Onsight Expert Activation Status

Endpoint Group: All Endpoints Selected: 0 [Clear Selected](#)

[Create Activation Job](#) | [SNMP Refresh](#) | [Cancel](#) | [Retry Now](#) | [Reset Attempt Count](#) | [Export to CSV](#) | [Reload Table](#)

<input type="checkbox"/>	Name	Activation Status	Days Remaining	Serial Number	Server Licensed	Locked Call License	Pending Activation	Sub-Group
<input type="checkbox"/>	ONSIGHTEXPERTPC	Activated	-	9 - A	<input type="checkbox"/>			-
<input type="checkbox"/>	JOHNPC	Activated	-	9 - D	<input checked="" type="checkbox"/>		Waiting for Endpoint	- Cancel

Figure 60 - Onsight Expert Activation Status

The **Onsight Expert Activation Status** page contains a table of all Onsight Expert endpoints currently managed by Onsight Management Suite, along with their current software activation status. Each entry in the table will contain the information described in Table 35.

Table 35 - Onsight Expert Activation Status Table Columns

Name	The name of the endpoint. This will typically be the Device / Computer Name of the endpoint.
Activation Status	The current activation status of the endpoint: Activated, Trial or Unknown.
Days Remaining	The number of trial days remaining, if the endpoint is in trial mode.
Serial Number	The serial number of the Onsight Expert endpoint. This will typically be the activation key that was used to activate the endpoint.
Server Licensed	Whether or not the endpoint is server licensed.
Locked Call License	If the endpoint is server licensed and has locked a call license, the icon will be displayed. Hovering over the icon with the mouse pointer will display the locked call license ID.
Pending Activation	If there is a pending activation job scheduled for the endpoint, the status of the activation job will be displayed. Clicking the icon next to the pending activation status will display a popup window containing more detailed information, as shown in Figure 67 on page 88.

In addition to the information described in Table 35, action buttons are included at the top of the table, allowing you to perform various tasks on the **Onsight Expert Activation Status** table. These are described in detail in Table 36.

Table 36 – Onsight Expert Activation Status Table Actions

Create Activation Job	Create an activation job for the selected endpoints. More information on creating an activation job can be found in Creating a New Onsight Expert Activation Job on page 85.
SNMP Refresh	Commands the Onsight Management Suite Service to immediately perform a background SNMP refresh on the selected endpoints.
Cancel	Cancel any pending activation job for the selected endpoints.
Retry Now	Retry the activation job for the selected endpoints as soon as they are ready.
Reset Attempt Count	Reset the activation job attempt count for the selected endpoints.
Export to CSV	Export the table to a comma-separated values (CSV) file.

Reload Table	Reload the table and display the current information for all endpoints.
--------------	---

16.1.2 Onsight Expert Activation Keys

In order to remotely assign activation keys to Onsight Expert endpoints, they must first be added to the Onsight Management Suite database.

16.1.2.1 Adding Onsight Expert Activation Keys

→ To add a new Onsight Expert activation key:

1. Choose **License Management > Onsight Expert Activation Keys > Add Onsight Expert Activation Keys**. You will be presented with the **Add Onsight Expert Activation Keys** screen as shown in Figure 61.

Add Onsight Expert Activation Keys

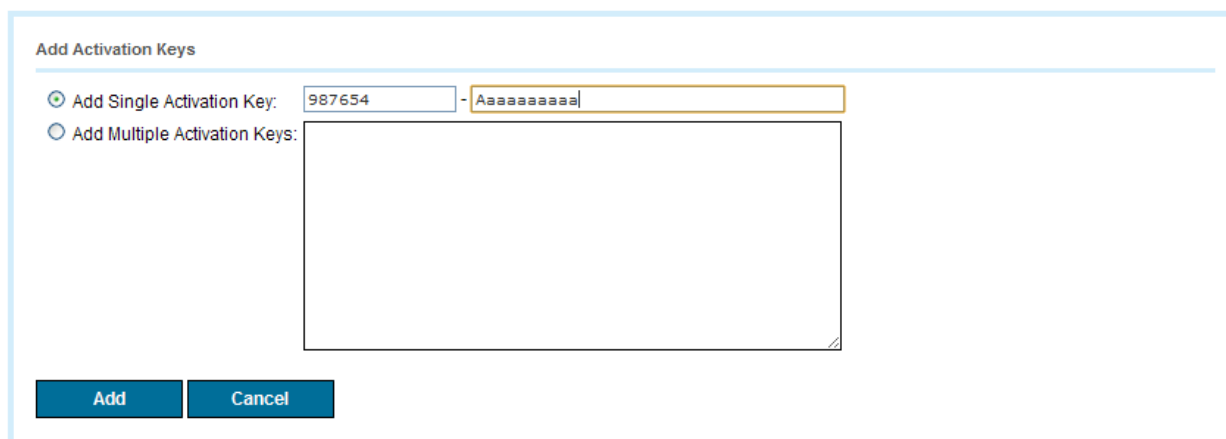


Figure 61 - Add Onsight Expert Activation Keys

2. In the **Add Activation Keys** section, select the appropriate radio button to enter either a single activation key or multiple activation keys. If you are adding multiple activation keys, each key must begin on a new line.
3. Click the **Add** button to add the activation keys to the database. You will be redirected to the **View Onsight Expert Activation Keys** page where you can view all of the activations keys that have been added to the system.

16.1.2.2 Viewing Existing Onsight Expert Activation Keys

To view the list of Onsight Expert activation keys in the database, choose **License Management > Onsight Expert Activation Keys > View Onsight Expert Activation Keys**. You will be presented with a list of all the activation keys that were previously added, as shown in Figure 62.

Onsight Expert Activation Keys

Add Delete Change Status Export to CSV Reload Table				
<input type="checkbox"/>	Activation Key	Type	Status	Date Added
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	987654-Aaaaaaaaaa	Activation	Available	6/29/2010 3:53:23 PM
<input type="checkbox"/>	123456-Abcdefghijkl	Activation	Activation Pending	6/29/2010 3:53:34 PM
<input type="checkbox"/>	999999-Azzzzzzzzzz	Activation	Used	6/29/2010 4:18:17 PM

Figure 62 - View Onsight Expert Activation Keys

Each entry in the **Onsight Expert Activation Keys** table will contain the information described in Table 37.

Table 37 – Onsight Expert Activation Keys Table Columns

Activation Key	The activation key.
Type	The type of key. Currently only keys of type Activation are supported.
Status	<p>The status of the activation key, which will be one of the following:</p> <ul style="list-style-type: none"> • Available – the activation key has not yet been used, and can be assigned to an Onsight Expert as part of an activation job. This is the default status assigned to an activation key when it is added to the database. • Activation Pending – the activation key belongs to a pending Onsight Expert activation job. Clicking the Activation Pending link will direct you to the Onsight Expert Activation Status page where you can view the status of the activation job. • Used – the activation key has been used, and is not available to be assigned to an Onsight Expert as part of an activation job.
Date Added	The date the activation key was added to the database.



*Onsight Management Suite does not communicate with the activation server to determine the status of activation keys in the database. If an activation key has been used to activate an Onsight Expert without the use of Onsight Management Suite, you will need to manually update the status of the key to Used by clicking the **Change Status** link, as described in Table 38.*

In addition to the information described in Table 37, action buttons are included at the top of the table, allowing you to perform the various tasks described in Table 38.

Table 38 – Onsight Expert Activation Key Actions

Add	Directs you to the Add Onsight Expert Activation Keys page, where you can add new activation keys to the database.
Delete	Deletes the selected activation keys from the database. Activation keys that are part of pending activation jobs cannot be deleted.
Change Status	Change the status of the selected activation keys to either Available or Used. The status of activation keys that are part of pending activation jobs

	cannot be changed.
Export to CSV	Export the table to a comma-separated values (CSV) file.
Reload Table	Reload the table to display the current list of keys in the database.



*You should only change the status of an activation key from **Used** to **Available** if you are sure that the activation key has not already been used to activate an Onsight Expert. If a used activation key is assigned to an Onsight Expert through Onsight Management Suite, the activation job will simply fail after the Onsight Expert attempts to contact the activation server to activate itself with the new key. The reason for the failure will be reported to Onsight Management Suite as 'No activations remaining'.*

16.1.3 Onsight Expert Activation Jobs

Activation keys are assigned to Onsight Expert endpoints through the creation of activation jobs. For an activation job to proceed:

- The endpoint must not already be performing a software update or activation job.
- The endpoint must not be in a call, recording or playing back a recording.
- The endpoint must be communicating with Onsight Management Suite over the Web Service interface.

When an activation job is initiated for an Onsight Expert endpoint, Onsight Management Suite will provide the endpoint with its assigned activation key. The Onsight Expert endpoint will then communicate over the Internet with the activation server to attempt to activate itself with the new key. If for some reason activation should fail, the activation job will be re-attempted up to a configurable number of times.

16.1.3.1 Configuring Onsight Expert Activation Job Settings

→ To configure Onsight Expert activation job settings:

1. Choose **Options > Service Settings**. You will be presented with the **Service Settings** screen as shown in Figure 8.
2. Locate the **Activation Job Configuration** section.
3. Configure the Onsight Expert activation job settings described in Table 39, as required.

Table 39 – Onsight Expert Activation Job Settings

Activation Retry Interval	The time to wait between failed activation job attempts, in seconds. The default value is 86400 seconds (24 hours).
Maximum Retry Attempts	The number of times to automatically attempt an activation job.

4. Click **Save** to save your changes.



*After the **Activation Retry Interval** expires, the activation update job will be reattempted the next time an Onsight Expert endpoint connects over the Web Service.*

16.1.3.2 Creating a New Onsight Expert Activation Job

→ To create a new Onsight Expert activation job:

1. Choose **License Management > Onsite Expert Software Activation > Create Onsite Expert Activation Job**. You will be presented with the **Create Onsite Expert Activation Job Wizard** as shown in Figure 63.

Create Onsite Expert Activation Job

Step 1 - Select Onsite Experts

Onsite Experts with pending activation jobs are not shown.

Endpoint Group: **All Endpoints** Selected: 1 [Clear Selected](#)

All Endpoints

- Lab

<input type="checkbox"/>	Name	Activation Status	Days Remaining	Serial Number	Server Licensed	Locked Call License	Sub-Group
<input checked="" type="checkbox"/>	ONSIGHTEXPERTPC	Activated	-	9-11111111-1111111111111111	<input checked="" type="checkbox"/>		Lab

[Next](#) [Cancel](#)

Figure 63 – Select Onsite Experts

2. The list of managed Onsite Expert endpoints in the system along with their current activation status will be displayed. Select the Onsite Experts from the list that you wish to add to the activation job and click **Next**.



If you navigated to the **Create Onsite Expert Activation Job Wizard** from the **View Onsite Expert Activation Status** page, the Onsite Expert endpoints selected on that page will be pre-selected for you in the **Select Onsite Experts** table.



Onsite Expert with pending activation jobs will not be shown in the **Select Onsite Experts** table.

3. You will be presented with the **Activation Conditions** step, as shown in Figure 64.

Step 2 - Activation Conditions

Activate the Onsite Expert if it meets at least one of the following conditions:

- ☒ Activate if the Onsite Expert is in **Trial Mode**
- ☐ Activate if the Onsite Expert is **Server Licensed**
- ☐ Activate if the Onsite Expert is already **Activated** (change the existing serial number)

Figure 64 – Activation Conditions

4. Select the conditions under which the Onsite Experts should be activated with their assigned activation keys and click **Next**. The conditions are described in detail in Table 40.



The selected activation conditions will be evaluated against the status of the selected Onsite Expert endpoints the next time they report to Onsite Management Suite over the Web Service

interface. If none of the selected conditions are met by an endpoint, the activation job will be marked completed and the message 'Activation of this endpoint was not required' will be added to the endpoint's activation job history log.

Table 40 – Activation Conditions

Activate if the Onsight Expert is in Trial Mode	This option can be used to activate a newly installed Onsight Expert (one that is running in trial mode).
Activate if the Onsight Expert is Server Licensed	This option can be used to convert a server licensed Onsight Expert to a standalone license. If the Onsight Expert has a locked call license, it will attempt to unlock the license before proceeding with the activation.
Activate if the Onsight Expert is already Activated	This option can be used to re-activate an Onsight Expert (one that has already been activated) with a new activation key.

5. You will be presented with the **Select Activation Keys** step, as shown in Figure 65.

Step 3 - Select Activation Keys

Activation Keys

☐ Auto-assign from all available activation keys
☒ Assign from selected activation keys

<input type="checkbox"/>	Activation Key	Type	Status	Date Added
<input type="checkbox"/>				
<input type="checkbox"/>	987654-Aaaaaaaaaa	Activation	Available	6/29/2010 3:53:23 PM
<input checked="" type="checkbox"/>	123456-Abcdefghijkl	Activation	Available	6/29/2010 3:53:34 PM

Figure 65 – Select Activation Keys

6. Choose the activation keys that you wish to allocate to the previously selected Onsight Experts. You can choose to either automatically assign keys from all available activation keys in the database, or automatically assign keys from a subset of selected activation keys. Click **Next** to continue to the next step.



Activation keys will be assigned to the Onsight Expert endpoints in the order in which they were added to the database. To assign a specific key to a specific Onsight Expert, create a new activation job for only the desired Onsight Expert and choose **Assign from selected activation keys** to assign the desired key.

7. You will be presented with the **Confirm Activation Key Allocations** step, as shown in Figure 66.

Step 4 - Confirm Activation Key Allocations

Allocated Activation Keys

Name	Allocated Activation Key	Type	Result
ONSIGHTEXPERTPC	123456-Abcdefghijkl	Activation	Activation key allocated

Figure 66 - Confirm Activation Key Allocations

8. The **Allocated Activation Keys** table will provide a summary of each selected Onsight Expert along with its newly allocated activation key.




*If there were not enough available activation keys in the database to allocate to all of the selected Onsight Expert endpoints, those endpoints that could not be assigned a key will have 'Not enough available activations' displayed in the **Result** column.*

9. Click **Confirm and Assign Keys** to create the activation job. The next time the selected Onsight Expert endpoints report to Onsight Management Suite over the Web Service interface they will attempt to communicate with the activation server to perform software activation with their assigned keys.

16.1.3.3 Viewing Pending Onsight Expert Activation Jobs

To view a list of pending activations jobs, navigate to **License Management > Onsight Expert Software Activation > View Onsight Expert Activation Status**. You will be presented with the **Onsight Expert Activation Status** page, as shown in Figure 60.

If an Onsight Expert endpoint has a pending activation job scheduled for it, the status of the activation job will be displayed in the **Pending Activation** column of the **Onsight Expert Activation Status** table. Clicking the  icon next to the pending activation status will display a popup window containing more detailed information, as shown in Figure 67.

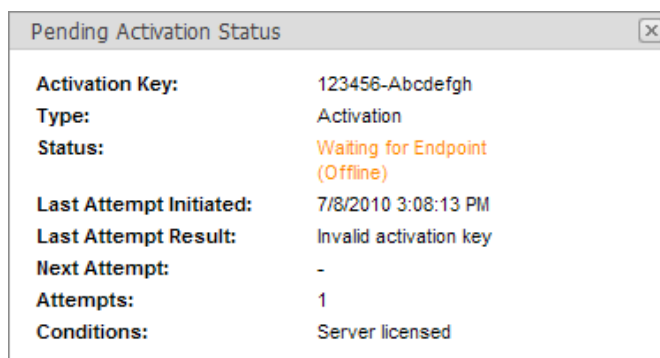


Figure 67 - Pending Activation Status

The **Pending Activation Status** window displays detailed information about a pending activation job for an endpoint, as described in Table 41.



*Detailed activation job status can also be viewed on **Activation** tab of the **Endpoint Details** page for an endpoint, as described in the **Activation** section on page 41.*

Table 41 – Pending Activation Status Columns

Activation Key	The activation key assigned to the endpoint.
Type	The type of activation key. Currently only keys of type Activation are supported.
Status	The status of the activation job for that endpoint, which will be one of the following: <ul style="list-style-type: none"> Waiting for Endpoint – Onsight Management Suite is ready to initiate the next activation attempt, and is waiting for the endpoint to be ready. Initiated – Onsight Management Suite has communicated the details of the activation job to the endpoint, and is waiting for it to report further

	<p>status.</p> <ul style="list-style-type: none"> • In Progress – The endpoint reports that the activation job is in progress. • Attempt Failed – The previous attempt failed. Onsight Management Suite is waiting until the time indicated by Next Attempt before it will initiate a new attempt. • Max Attempts Reached – The maximum number of failed attempts was reached for the activation job. Administrator intervention is required to proceed. • Cancelled – The activation job was cancelled by the administrator. • Unknown – The status of the activation job is unknown.
Last Attempt Initiated	The date and time the last activation attempt was initiated.
Last Attempt Result	If the last activation attempt failed, the reason for the failure will be displayed.
Next Attempt	The date and time of the next activation attempt.
Attempts	The total number of activation attempts.
Conditions	The conditions under which the Onsight Expert should be activated with the assigned activation key.

While an activation job is pending for an endpoint, the last column in **Onsight Expert Activation Status** table will display one or more actions that can be performed on the activation job:

- **Cancel** allows the administrator to cancel the activation job.
- **Retry Now** commands Onsight Management Suite to retry the activation job as soon as the endpoint is ready without waiting for the time indicated by **Next Attempt**.
- **Reset** allows the administrator to reset the activation job attempt count for the endpoint if it is in the **Max Attempts Reached** state. This will set the attempt count back to zero, allowing Onsight Management Suite to re-attempt the activation job on that endpoint.

The logged history of activation job attempts for an endpoint can also be viewed by clicking the **+** button next to its name in the **Onsight Expert Activation Status** table. This will reveal a log of activation job events for that endpoint, including the date and time of each event along with the assigned activation key, as shown in Figure 68. If an activation attempt has failed, the log will display the reason for the failure, allowing you to diagnose the problem before the next scheduled attempt.

		JOHNPC	Activated	-	9:00:00 AM -D			Waiting for Endpoint		-	Cancel
Activation History:											
Timestamp	Activation Key	Status									
7/8/2010 3:11:06 PM	123456-Abcdefgh	Next attempt requested by administrator. Waiting for endpoint.									
7/8/2010 3:08:19 PM	123456-Abcdefgh	The activation attempt failed: Invalid activation key									
7/8/2010 3:08:13 PM	123456-Abcdefgh	Activation initiated by server.									
7/8/2010 3:07:29 PM	123456-Abcdefgh	Activation key assigned. Conditions: Server licensed. Waiting for endpoint.									

Figure 68 – Activation Job History

16.2 Onsite Expert Release Keys

Onsite Management Suite can maintain a database of Onsite Expert release keys, which may be required when upgrading the Onsite Expert software. When an Onsite Expert software update is initiated remotely using Onsite Management Suite, the server can provide the endpoint with the necessary release key based on the activated serial number of the Onsite Expert and the version number of the software package that is being installed. If a corresponding release key does not exist in the database, the user of the Onsite Expert computer will need to enter the release key manually during the installation process.

16.2.1 Adding Onsite Expert Release Keys

→ To add a new Onsite Expert Release Key:

1. Choose **License Management > Onsite Expert Release Keys > Add Onsite Expert Release Keys**. You will be presented with the **Add Onsite Expert Release Keys** screen as shown in Figure 69.

Add Onsite Expert Release Keys

Figure 69 – Add Onsite Expert Release Keys

2. In the **Add Release Key** section, enter the information required for the new release key, as described in Table 42.

Table 42 – Add Release Key Settings

Onsite Expert Version	The version number of Onsite Expert the release key corresponds to.
Activation Key	The activation key that was used to activate the Onsite Expert that is being upgraded.
Release Key	The release key required to update the Onsite Expert to the specified version.

3. Click the **Add** button to add the release key.
4. Once the release key has been added, you can continue adding additional keys, or click the **View** button to view the list of release keys currently in the database.

16.2.2 Viewing Existing Onsite Expert Release Keys

To view the list of Onsite Expert release keys in the database, choose **License Management > Onsite Expert Release Keys > View Onsite Expert Release Keys**. You will be presented with a list of all the release keys that were previously added, as shown in Figure 70. Each item in the list displays the version number, activation key, release key and the date the item was added.

View Onsite Expert Release Keys

Add Delete Export Reload Table				
<input type="checkbox"/>	Version	Activation Key	Release Key	Date Added
<input type="checkbox"/>	4.0.0	123456-Abcdefghijkl	123456-Abcdefghijkl-1-A1B2C3D4	11/19/2009 9:09:59 PM

Figure 70 – View Onsite Expert Release Key List

In addition to the information described above, action buttons are included at the top of the table, allowing you to perform the various tasks described in Table 43.

Table 43 – Onsite Expert Release Key Actions

Add	Directs you to the Add Onsite Expert Release Keys page, where you can add new release keys to the database.
Delete	Delete the selected release keys from the database.
Export to XML	Export the selected release keys to an XML file. The exported file can either be used as a backup, or imported into another Onsite Management Suite.
Export to CSV	Export the table to a comma-separated values (CSV) file.
Reload Table	Reload the table to display the current list of keys in the database.

16.2.3 Importing Onsite Expert Release Keys

A list of release keys that was previously exported to XML can be imported back into Onsite Management Suite.

→ To import an XML file containing release keys:

1. Choose **License Management > Onsite Expert Release Keys > Add Onsite Expert Release Keys**. You will be presented with the **Add Onsite Expert Release Keys** screen as shown in Figure 69.
2. In the **Import Release Keys** section, choose the **Import Options** to use while importing the release keys from the options listed in Table 44.

Table 44 – Release Key Import Options

Skip duplicate records found in the imported file	If a release key for a particular version number and activation key already exists in the database, release keys in the file for the same version number and activation key will be ignored.
Replace duplicate records with those in the imported file	If a release key for a particular version number and activation key already exists in the database, it will be replaced with release keys in the file for the same version number and activation key.

3. Click the **Browse** button. You will be presented with a file selection dialog.
4. Choose the XML file containing the release keys to import.

5. Click **Import**. The release keys will be imported into the database using the selected import options.

16.3 Onsign Expert Custom Installs

Onsign Management Suite allows you to create an Onsign Expert custom install file that can be packaged with the Onsign Expert setup files, allowing you to automatically configure or activate an Onsign Expert during installation. Using Onsign Expert custom install files you can:

- Activate a single Onsign Expert after installation, without the need for Onsign Management Suite.
- Provide release keys to Onsign Expert endpoints that are upgraded using some means other than Onsign Management Suite, such as installing from a shared network drive or third party software distribution system.
- Configure Onsign Expert endpoints to automatically communicate with Onsign Management Suite over the Web Service interface after installation, allowing an administrator to immediately assign activation keys, monitor system status and collect usage statistics from newly installed Onsign Expert endpoints.

16.3.1 Creating an Onsign Expert Custom Install File

➔ To create an Onsign Expert custom install file:

1. Choose **License Management > Create Onsign Expert Custom Install**. You will be presented with the **Create Onsign Expert Custom Install** wizard as shown in Figure 71.

Create Onsign Expert Custom Install

Generate Custom Install for Onsign Expert

This feature allows you to package Onsign Expert settings that will be automatically applied when the product is installed.

Step 1

Choose which features to include in the Custom Onsign Expert Installer and hit the **Export** button.

Step 2

Save the resulting file to a convenient location and place it in the same folder as the Onsign Expert setup files.

Next **Cancel**

Figure 71 –Custom Install Wizard

2. After reviewing the instructions, click the **Next** button to continue.
3. Select whether to automatically configure the Onsign Expert to connect to the Web Service interface. Choose **Skip** if you do not wish to add Web Service settings to the file, otherwise choose **Configure Remote Web Service** and click **Next** to continue.

If you chose **Skip**, proceed to step 5.
4. You will be presented with the screen shown in Figure 72. Enter the settings that the Onsign Expert will use to connect to the Web Service, and click **Next** to continue.

Remote Web Service

Enter the URI of the Remote Web Service to automatically configure the Onsight Expert for remote management upon installation.

Server URI:
http://oms/OnsightWebService/RemoteEndpointService.asmx

Encryption Key:
PqojY0jHe5MwTuB9Az178pNKcnk4ZJ3fD5xe

Reporting:
☒ Report statistics over Remote Management Web Service

Figure 72 - Custom Install Remote Web Service Settings

- Select whether to add an activation key for automatic product activation. Choose **Skip** if you do not wish to add activation settings to the file, otherwise choose **Add Activation Key** and click **Next** to continue.

If you chose **Skip**, proceed to step 7.

- You will be presented with the screen shown in Figure 73. Enter the activation key required to activate the Onsight Expert into the provided fields, and click **Next** to continue.

Automatic Product Activation

Enter activation key(s) to include with the Onsight Expert installation files to allow the product to be automatically licensed for the user during installation.

Activation Key:
123456 - Abcdefghijkl

Figure 73 - Custom Install Activation Settings



Only a single activation key can be added to an Onsight Expert custom install file. If the file will be used to install Onsight Expert onto multiple client computers, only the first computer to install Onsight Expert will activate successfully, since the key will no longer be available for subsequent activations.

- Select whether to add release keys required for product upgrades. Choose **Skip** if you do not wish to add release keys to the file, otherwise choose **Add Release Keys** and click **Next** to continue.

If you chose **Skip**, proceed to step 9.

- You will be presented with the screen shown in Figure 74. Add release keys to the custom install file by using the action buttons located at the top of the displayed table, as described in Table 44, and click **Next** to continue.

Automatic Product Activation

Enter release key(s) to include with the Onsight Expert installation file to allow the product to be automatically licensed for the user during installation.

Add Key | Add Multiple Keys | Import from Database | Delete

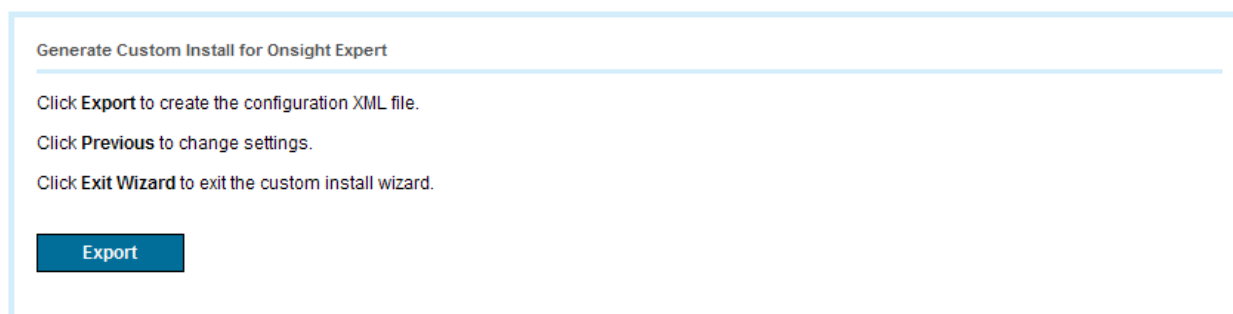
<input type="checkbox"/>	Release Key
<input type="checkbox"/>	123456-Abcdefghijkl-3-ABCDEFGH

Figure 74 - Custom Install Release Key Settings

Table 45 – Custom Install Release Key Actions

Add Key	Enter a single release key to add to the file.
Add Multiple Keys	Enter multiple release keys at a time, one release key per line.
Import from Database	Select release keys from the database to add to the file. For more information on adding release keys to the Onsite Management Suite database, see the Onsite Expert Release Keys section on page 90.
Delete	Remove the selected release keys from the file.

9. You will be presented with the screen shown in Figure 75. Click the **Export** button to generate the Onsite Expert custom install file.

**Figure 75 - Custom Install Export**

10. You will be prompted by your browser to save the resulting Onsite Expert custom install file, named `mca_config.xml`. Take note of the location where the file is saved, since you will need to copy it alongside the Onsite Expert setup files, as described in the **Deploying an Onsite Expert Custom Install File** section on page 94.

16.3.2 Deploying an Onsite Expert Custom Install File

To apply the settings contained in an Onsite Expert custom install file, the file must be copied alongside the Onsite Expert installation files. This can be done in either one of two ways: by creating a shared network directory from which client computers will install the Onsite Expert, or by creating a custom installation CD.

→ To create a shared network directory for installing Onsite Expert:

1. Create a shared installation directory on a server from which the client computers can install Onsite Expert.
2. Copy the contents of the **OnsiteExpert** subdirectory from a standard Onsite Expert installation CD to the shared installation directory.
3. Copy the `mca_config.xml` file that was created using the steps described in the **Creating an Onsite Expert Custom Install File** section on page 92 to the shared installation directory.
4. Client computers can now install Onsite Expert by running `setup.exe` from the shared installation directory.

→ To create a custom installation CD:

1. Create a temporary installation directory.
2. Copy the entire file system tree from a standard Onsite Expert installation CD to the temporary installation directory.

3. Copy the mca_config.xml file that was created using the steps described in the **Creating an Onsight Expert Custom Install File** section on page 92 to the **OnsightExpert** subdirectory within the temporary installation directory.
4. Use a CD image-creation tool to create an ISO file from the contents of the temporary installation directory.
5. Burn the ISO file to a CD.
6. Delete the temporary installation directory.
7. Client computers can now install Onsight Expert from the custom installation CD by running setup.exe from the **OnsightExpert** subdirectory.

17 Configuration Access Control

Access to Onsight device and Onsight Expert configuration parameters can be restricted through the use of Configuration Access Control files. Configuration Access Control files allow an administrator to restrict which features can be configured or changed by end users of Onsight device or Onsight Expert endpoints.

Some examples of when it might be appropriate to restrict access to certain configuration settings include:

- **Network Security** – If wireless networks are not permitted, you may want to restrict access to the Enable Radio feature. If you wish to control which channels are used by the radio, access to the Channel Configuration settings can be restricted.
- **Bandwidth Control** – Administrators can lock down the bandwidth configuration of endpoints.
- **Privacy** – Control whether or not users can change the configured privacy setting of an endpoint.

17.1 Editing Configuration Access Control Files

Configuration Access Control settings are maintained by editing the sample files that are distributed with Onsight Expert, starting with release 3.4. They are located on the Onsight Expert installation CD in the **AccessControl** folder. There are two sample files: one for the Onsight device, and one for Onsight Expert. Each file contains editing instructions, as well as a description of the available permission settings. Review the two sample files to learn which parameters you can control access to.

A portion of a sample Onsight device Configuration Access Control file is shown in Figure 76.

```
<!--
Call Control - General
-->
    <permission id="5001" version="1.0.0">
        <description>Enable auto answer</description>
        <access>open</access>
    </permission>
    <permission id="5002" version="1.0.0">
        <description>Start video on connection</description>
        <access>open</access>
    </permission>
    <permission id="12004" version="1.0.0">
        <description>Call History Maximum</description>
        <access>open</access>
    </permission>
```

Figure 76 – Sample Configuration Access Control File

Each <permission> element in the file contains a description of each configuration setting and the default access control level for that setting. In the example in Figure 76, the **Enable auto answer** setting has been given an access level of **open**. To restrict access to a given setting, the administrator can modify the value of the <access> element to one of the values shown in Table 46.

Table 46 – Access Control Levels

open	All logged in users can modify the setting.
admin	Only users with Administrator privileges can modify the setting.
locked	The setting cannot be edited by a user. It can only be modified by an installed configuration package

17.2 Creating and Installing Configuration Access Control Packages

→ To install Configuration Access Control settings to an endpoint using Onsite Management Suite:

1. Locate the sample Configuration Access Control file for the endpoint you wish to configure.
2. Using a text editor such as Notepad, edit the sample file to restrict access to certain configuration items.
3. Create a new configuration package for the endpoint. For more information, refer to **Creating an Onsite Device Configuration Package** on page 51 and **Creating an Onsite Expert Configuration Package** on page 55.
4. Import the edited Configuration Access Control file into the created package. For further information, refer to **Importing Access Control Settings** on page 52 and page 56.
5. Install the package containing the new Configuration Access Control settings onto the Onsite device or Onsite Expert endpoint. For more information regarding remotely installing packages to an endpoint, refer to the **Software and Configuration Updates** section on page 43.



*Once a particular setting has been set to an access control level of **locked**, it can only be modified by installing a configuration package.*

→ To install a Configuration Access Control package directly to an Onsite device endpoint:

1. Navigate to **Package Management > Onsite Device Configuration Packages > View Onsite Device Configuration Packages**.
2. Locate the package containing the Configuration Access Control file you wish to install, and click the **Save Package** link. This will allow you to download a ZIP file containing the manifest file and package archive.
3. Extract the manifest file and package archive to an SD card.
4. Insert the SD card containing the manifest file and package archive into the Onsite device.
5. Open the main menu on the Onsite device and select **Configuration**.
6. Navigate to the **Maintenance > Update** tab.
7. Select **file:** from the **Package Server** dropdown list.
8. Browse for the created Configuration Access Control package by pressing the ... (browse) button.
9. Select the manifest.xml file that corresponds to the package and press **Select File**.
10. Press the **Search** button. The Configuration Access Control package will be listed in the available packages window.
11. Press the **Download** button to download the package.
12. Press the **Install** button to install the package to the device.

18 Maintenance

The Onsite Management Suite database contains the list of managed endpoints, software update and activation jobs, service settings and collected endpoint usage statistics. You may wish to create a backup copy of the database that can be restored in the case of a hardware failure on the server.

18.1 Backing up the Database

→ To create a backup of the Onsite Management Suite database:



The Onsite Management Suite Windows Service must be stopped in order to create a backup of the database. During that time the User Interface will be inaccessible and Onsite endpoints will not be able to report system status or usage statistics to Onsite Management Suite. It is recommended that database backups be performed during off-peak hours.

1. Navigate to **Control Panel > Administrative Tools > Services**. This will bring up the Services control panel, as shown in Figure 77.

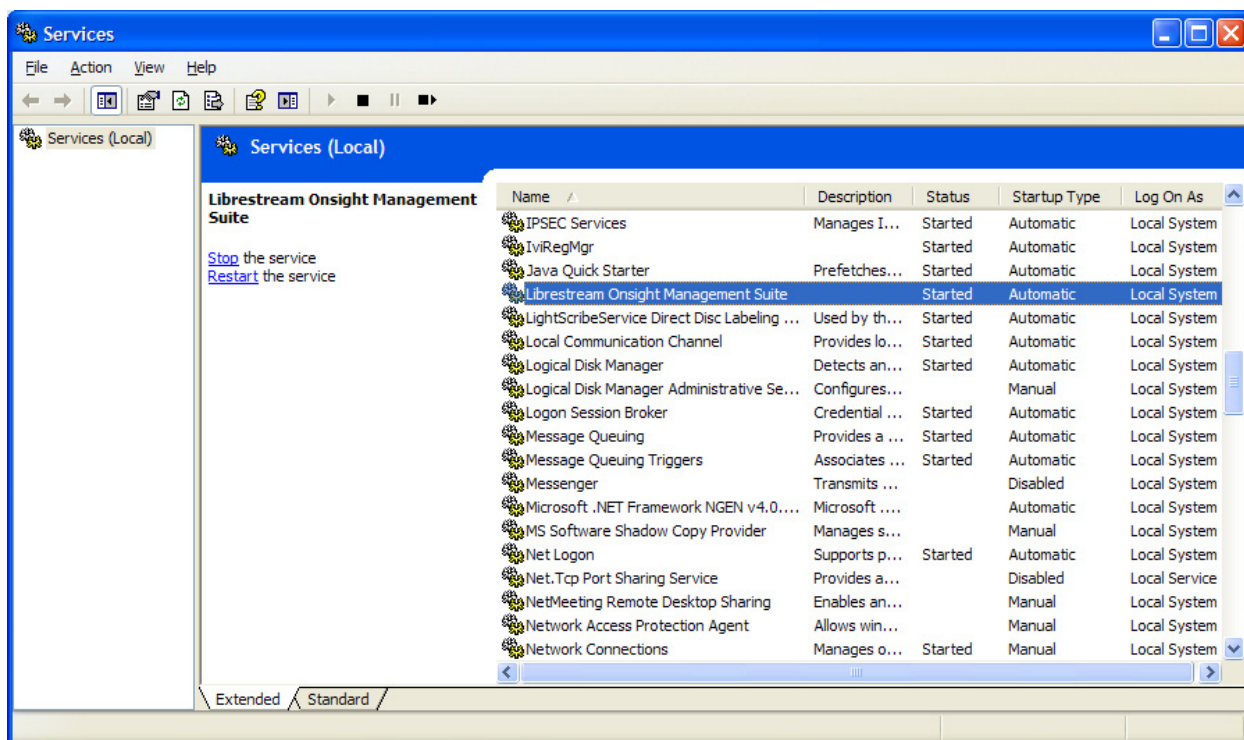


Figure 77 - Services Control Panel

2. Right-click on the item named **Librestream Onsite Management Suite**, and select **Stop**. This will stop the Windows Service.
3. Locate the folder where the database is stored. This is the folder that you configured during installation, as described in the **Installation** section on page 3. The default folders are:
 - Windows XP / Windows Server 2003: C:\Documents and Settings\All Users\Application Data\MCA
 - Windows Server 2008: C:\Program Data\MCA

4. Create a copy of the ManagementSuite.db file located in the folder and save it to the location where it will be stored as a backup.



Ensure that you do not delete or rename the original ManagementSuite.db.

5. Restart the Windows Service by right-clicking on **Librestream Onsight Management Suite** in the services control panel shown in Figure 77, and selecting **Start**.

18.2 Restoring the Database

→ To restore a backup copy of the database:

1. Navigate to **Control Panel > Administrative Tools > Services**. This will bring up the services control panel, as shown in Figure 77.
2. Right-click on the item named **Librestream Onsight Management Suite**, and select **Stop**. This will stop the Windows Service.
3. Locate the folder where the database is stored. This is the folder that you configured during installation, as described in the **Installation** section on page 3. The default folders are:
 - Windows XP / Windows Server 2003: C:\Documents and Settings\All Users\Application Data\MCA
 - Windows Server 2008: C:\Program Data\MCA
4. Restore the database by copying the backup database file into the folder. Ensure that the database file is named ManagementSuite.db.
5. Set the file permissions on the restored database (ManagementSuite.db) by granting **Full Control** access to the **Everyone** user group.
6. Restart the Windows Service by right-clicking on **Librestream Onsight Management Suite** in the services control panel shown in Figure 77, and selecting **Start**.



Ensure that the database being restored was not created with a version of Onsight Management Suite that is newer than the version of Onsight Management Suite that is currently running.

19 End User License Agreement

IMPORTANT – PLEASE READ THIS AGREEMENT CAREFULLY.

LIBRESTREAM IS WILLING TO LICENSE THE SOFTWARE TO LICENSEES AND ALLOW LICENSEES TO USE THE SOFTWARE AND LIBRESTREAM PRODUCTS ONLY UPON THE CONDITION THAT EACH LICENSEE ACCEPTS AND AGREES TO BE BOUND BY ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT.

FOR ALL INTENTS AND PURPOSES, EACH PERSON WHO DOWNLOADS OR INSTALLS ANY SOFTWARE, OR WHO USES ANY OF THE SOFTWARE OR ANY LIBRESTREAM PRODUCT, IS DEEMED TO BE A LICENSEE, WITH SUCH DOWNLOADING, INSTALLATION AND/OR USE CONSTITUTING IMMEDIATE AND AUTOMATIC ACCEPTANCE OF ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT, WHICH WILL BE BINDING ON, AND ENFORCEABLE AGAINST, THAT LICENSEE.

IF ANY POTENTIAL LICENSEE DOES NOT AGREE TO ALL OF THESE TERMS AND CONDITIONS, THEN LIBRESTREAM IS NOT WILLING TO LICENSE ANY OF THE SOFTWARE TO THAT LICENSEE OR TO ALLOW THAT LICENSEE TO USE ANY OF THE SOFTWARE OR ANY LIBRESTREAM PRODUCT. IN SUCH A CASE:

(a) DO NOT DOWNLOAD, INSTALL OR USE ANY SOFTWARE, AND

(b) IF YOU HAVE ALREADY ACQUIRED THE SOFTWARE, RETURN THE SOFTWARE FOR A FULL REFUND OR, IF THE SOFTWARE IS SUPPLIED AS PART OF A LIBRESTREAM PRODUCT, RETURN THAT LIBRESTREAM PRODUCT FOR A FULL REFUND.

1. DEFINITIONS.

1.1 “Agreement” means this End User License Agreement, including any Schedule attached hereto.

1.2 “Computer” means any electronic device that accepts information in digital or similar form and manipulates it for a specific result based on a sequence of instructions.

1.3 “Confidential Information” means (a) the Software and any portions, components or sub-files thereof; (b) the structure, sequence, internal design and organization of the Software and the concepts, methods of operations and ideas disclosed therein, together with all associated interface information; (c) any trade secrets relating to the Software and/or any Librestream Product; (d) any tangible items marked “confidential” or with a similar designation by Librestream or any of its distributors or other representatives or by any Third Party Licensor, and/or any information disclosed visually or verbally and identified by Librestream or any such distributor or other representative as confidential at the time of disclosure; and (e) the terms and conditions of this Agreement.

1.4 “Intellectual Property” means any patents, patent rights, trademarks, service marks, registered designs, topography and semiconductor mask work rights, applications for any of the foregoing, copyrights, know-how, unregistered design rights, trade secrets and any other similar protected rights in any country.

1.5 “Librestream” means Librestream Technologies Inc.

1.6 “Librestream Product” means any product developed by or for Librestream that incorporates any of the Software in any manner whatsoever.

1.7 “Librestream Software” means any software that is proprietary to Librestream and that is not Third Party Software, and includes in particular the Librestream software identified in Schedule A hereto.

1.8 “Licensee” means, collectively, each and every person who downloads, installs and/or uses any of the Software and/or any Librestream Product.

1.9 “party” means each of Licensee and Librestream, and “parties” means both the Licensee and Librestream.

1.10 “person” includes an individual, a sole proprietor, a partnership, a corporation, a trust, a syndicate, a joint venture and any other business or legal entity of any nature or kind whatsoever.

1.11 “Purchase Order” means the purchase order or other documentary evidence of any nature or kind whatsoever that

is related to this Agreement and that was submitted to and accepted in writing by Librestream.

1.12 "Software" means, collectively, the Librestream Software and the Third Party Software, and includes:

(a) all of the contents of the files, disk(s), CD-ROM(s) or other media with which this Agreement is provided or which are installed on any Librestream Product (including firmware) or which are made available online by Librestream or any Third Party Licensor including:

(i) all Librestream or Third Party Licensor computer information or software; and

(ii) any and all related instructional or supplementary documentation in human or machine readable form supplied or otherwise made available by Librestream or any Third Party Licensor; and

(b) all Upgrades in respect of which Licensee has paid the applicable license, maintenance and/or support fee.

Some of the Software may require activation – Licensees should consult the Purchase Order, the documentation that accompanies the Software and/or the Librestream website at www.librestream.com for further information in this regard.

1.13 "Third Party Licensors" means, collectively, those third parties who are the respective owners of the Third Party Software, and "Third Party Licensor" means any such third party.

1.14 "Third Party Software" means the software of a person other than Librestream that is embedded with the Librestream Software or that is otherwise provided to a Licensee by Librestream along with the Librestream Software.

1.15 "Third Party Software License Agreement" means a license agreement for a particular Third Party Software product, in the form attached to this End User License Agreement as a Schedule or in the form expressly referenced in any such Schedule.

1.16 "Upgrades" means all upgrades, modified versions, updates, additions and copies of any Software (including related documentation) which are provided, installed or made available online or otherwise by Librestream or any Third Party Licensor.

1.17 "use" or "using" includes accessing, downloading, installing or copying any of the Software or otherwise benefiting from the functionality of any of the Software and/or any Librestream Product.

2. LIMITED LICENSE.

2.1 Subject to Licensee's strict compliance with the terms and conditions of this Agreement, Librestream hereby grants to Licensee, during the term of this Agreement, a worldwide, non-transferable, non-exclusive, revocable, royalty-free limited license to use the Software for Licensee's internal business purposes and for no other purpose whatsoever. For greater certainty:

(a) some of the Third Party Software is licensed to Licensee in accordance with the provisions of the Third Party Software License Agreement applicable thereto, which Licensee acknowledges reading and agrees is binding on Licensee;

(b) all of the Librestream Software and all Third Party Software that is not subject to a Third Party Software License Agreement is licensed to Licensee in accordance with the terms and conditions of this End User License Agreement; and

(c) any default or non-compliance on the part of Licensee or those for whom it is responsible in law with the terms and conditions of this End User License Agreement or with the provisions of any Third Party Software License Agreement shall constitute default and non-compliance by Licensee with this End User License Agreement and all Third Party Software License Agreements.

2.2 Use of the Software pursuant to this Agreement shall be limited to the single Librestream Product and to a single Computer as set forth in the applicable Purchase Order and for which Licensee has paid to the Librestream the required license fee.

2.3 Any use of the Software which is not expressly authorized by this Agreement is strictly prohibited. Without limiting the generality of the foregoing and notwithstanding any other provision of this Agreement, in no event may Licensee do any of the following or permit any third party to do any of the following:

(a) transfer, assign or sublicense any of its license rights to any other person, or use the Software or any portion thereof on any unauthorized or secondhand Librestream Product or on any Computer(s) other than the specific Computer(s) on which the Software is licensed to be used - any such transfer, assignment, sublicense or use shall be null and void; or

(b) distribute, license, sublicense, rent, lease or sell the Software or any portion thereof as a standalone product - any such distribution, license, sublicense, rent, lease or sale shall be null and void; or

(c) make error corrections to or otherwise modify or adapt the Software or any portion thereof; or

(d) reverse engineer, decrypt, disassemble or decompile the Software or any portion thereof, or otherwise reduce the Software of any portion thereof to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this prohibition; or

(e) create any derivative works based upon the Software or any portion thereof or take any actions that would cause the Software or any portion thereof to become subject to the GPL, the LGPL or any other open source license (unless that portion is already expressly subject to the GPL, the LGPL or any other open source license, as expressly noted in any Third Party Software License Agreement); or

(f) use the Software or any portion thereof to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the prior express written consent of Librestream.

2.4 The Software is licensed, not sold, and is protected by the copyright laws of Canada and other countries and by international treaty provisions. All right, title and interest in and to the Software and any copies thereof, regardless of form or media, shall remain solely with Librestream or the Third Party Licensors, as the case may be. Except as expressly provided herein, this Agreement does not grant Licensee any rights under any of Librestream's or any Third Party Licensors' patents, copyrights, trade secrets, trademarks or other Intellectual Property rights. Librestream and each Third Party Licensors retain all rights not explicitly granted herein.

2.5 Licensee may make such limited copies of the Software as are strictly necessary for backup purposes only, provided that Licensee will not remove, obscure or destroy, and will reproduce on all copies of the Software so made, any Librestream and any Third Party Licensors names, logos, copyright or other notices, trademarks and other proprietary markings which appear on the Software.

2.6 Licensee is solely responsible for any use by Licensee or by any third party of any password issued to Licensee by Librestream or any Librestream distributor or other representative, regardless of whether or not any such third party use was authorized by Licensee.

2.7 Licensee may provide Librestream or any Librestream distributor or other representative with suggestions, comments or other feedback regarding Licensee's evaluation or use of the Software, including but not limited to suggested performance improvements to the Software and/or any Librestream Product, code enhancements and/or error corrections ("Feedback"). Licensee agrees that any Feedback shall be voluntarily given and that any and all Feedback will immediately and automatically become the property of Librestream, and that Librestream shall be entitled to incorporate any Feedback into the Software and/or any Librestream Product without any compensation or other liability or obligation of any nature or kind whatsoever to Licensee.

3. UPGRADES.

3.1 Notwithstanding any other provision of this Agreement:

(a) Licensee has no license or other right to use any Upgrade unless Licensee, at the time of acquiring that Upgrade, already holds a valid license to use the Software that is the subject of that Upgrade and has paid to Librestream the applicable license, maintenance and/or support fee to use that Upgrade; and

(b) use of Upgrades is limited to the Librestream Product in respect of which Licensee is the original end user purchaser or lessee and/or to the specific Computer(s) on which the Software is licensed to be used, unless Licensee is otherwise validly licensed to use that Upgrade and complies with Section 3.1(a).

4. AUDIT RIGHTS AND INDEMNITY.

4.1 Licensee shall, within thirty (30) days following Licensee's receipt of written request from Librestream or any Librestream distributor or other representative, fully document and certify all uses of the Software that Licensee has made within the period of twelve (12) months prior to the date of receipt of such request. In addition, Licensee shall, upon reasonable advance written notice and during normal business hours, provide access and allow Librestream or any Librestream distributor or other representative to inspect Licensee's books, records and computer systems in order to confirm Licensee's compliance with this Agreement.

4.2 In the event that any such request response or audit determines that Licensee is or was using the Software in a manner that exceeds or exceeded its license rights, Licensee shall immediately pay to Librestream on demand any amount(s) that are required to rectify such excessive use. This remedy shall be in addition to, and not in lieu of, any other right or remedy that Librestream may have pursuant to this Agreement or otherwise with respect to such excessive use.

4.3 In the event that any such request response or audit determines that Licensee is otherwise not in compliance with this Agreement, this Agreement shall immediately terminate as contemplated in Section 10.1. Such termination shall be in addition to, and not in lieu of, any other right or remedy that Librestream may have pursuant to this Agreement or

otherwise with respect to such non-compliance.

4.4 Licensee shall indemnify Librestream and save Librestream harmless from and against any and all losses, damages, liabilities, costs and expenses (including, without limitation, reasonable attorneys' fees) that arise out of or are attributable in any manner whatsoever to any non-compliance on the part of Licensee or those for whom it is in law responsible with any provision of this Agreement.

5. CONFIDENTIAL INFORMATION. Licensee shall not disclose to any third party, or use for any purpose not expressly permitted herein, any Confidential Information. Licensee agrees to take all reasonable measures to protect the Confidential Information and to prevent unauthorized disclosure thereof, which measures shall be at least as stringent as those measures Licensee takes to protect its own confidential information of like kind and which shall in no event be less than would be taken by a prudent business person in similar circumstances. Without in any way limiting the foregoing, Licensee shall restrict access to Confidential Information, including the Software, to Licensee employees and individual third party contractors who have executed a written agreement with Licensee sufficient to protect the Confidential Information in accordance with the provisions of this Agreement and who have a "need-to-know" to carry out the licenses granted herein. Notwithstanding the foregoing, all Confidential Information, any and all documents and other tangible material and/or objects containing or representing Confidential Information and any and all copies thereof shall be and always remain the property of Librestream or the Third Party Licensors, as the case may be.

6. REPRESENTATIONS AND WARRANTIES.

6.1 Librestream warrants that the Librestream Software will perform in substantial conformance to the applicable Librestream published specifications for that Librestream Software for a period of 12 months from the date of shipment from Librestream or from the date of downloading by Licensee, whichever is earlier, provided that (a) the Librestream Software remains unmodified by anyone other than Librestream; (b) the Librestream Software is and has always been operated under normal and proper conditions on the authorized Librestream Product and/or Computer on which that Librestream Software is licensed to be used; (c) the Librestream Software has not been used in any manner for which it was not designed; (d) the Librestream Software has not been used with any unauthorized software, hardware or third party equipment; (e) Licensee is not in breach of this Agreement; and (f) notice of any claim under this limited warranty is received in writing by Librestream within the 12 month limited warranty period.

6.2 Licensee's sole and exclusive remedy (at law, in equity or otherwise), and the sole and entire responsibility and liability of Librestream, with respect to any claim under the limited warranty set forth in Section 6.1 is for Librestream, at its sole option and discretion, to either (a) use commercially reasonable efforts to bring the non-warranty-compliant Librestream Software into substantial conformance with its published specifications; or (b) refund to Licensee the purchase price paid for the non-warranty-compliant Librestream Software.

6.3 NO REPRESENTATION OR WARRANTY OF ANY NATURE OR KIND WHATSOEVER IS PROVIDED BY LIBRESTREAM REGARDING ANY THIRD PARTY SOFTWARE. IF AND TO THE EXTENT THAT ANY THIRD PARTY SOFTWARE LICENSE AGREEMENT IS ATTACHED TO THIS AGREEMENT AS A SCHEDULE OR IS EXPRESSLY REFERENCED IN ANY SCHEDULE TO THIS AGREEMENT, LICENSEES SHOULD CAREFULLY REVIEW ANY SUCH THIRD PARTY SOFTWARE LICENSE AGREEMENT TO DETERMINE WHETHER OR NOT ANY REPRESENTATION OR WARRANTY IS PROVIDED TO LICENSEE IN RESPECT OF THE THIRD PARTY SOFTWARE THAT IS THE SUBJECT OF SUCH THIRD PARTY SOFTWARE LICENSE AGREEMENT. OTHERWISE, ALL THIRD PARTY SOFTWARE IS PROVIDED "AS IS", WITHOUT ANY REPRESENTATION, WARRANTY OR CONDITION OF ANY NATURE OR KIND WHATSOEVER.

6.4 TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND SUBJECT ONLY TO THE LIMITED WARRANTY IN SECTION 6.1 IN THE CASE OF THE LIBRESTREAM SOFTWARE AND TO ANY EXPRESS PROVISION TO THE CONTRARY IN ANY THIRD PARTY SOFTWARE LICENSE AGREEMENT (WHICH SUCH PROVISION SHALL BE CONFINED TO THE THIRD PARTY SOFTWARE AND THE THIRD PARTY LICENSOR THAT ARE THE SUBJECT OF THAT THIRD PARTY SOFTWARE LICENSE AGREEMENT), LIBRESTREAM AND THE THIRD PARTY LICENSORS EXPRESSLY DISCLAIM ALL OTHER REPRESENTATIONS, WARRANTIES AND CONDITIONS, WHETHER EXPRESS OR IMPLIED, IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION QUIET ENJOYMENT, NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS AND THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, MERCHANTABLE QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. IN PARTICULAR, NEITHER LIBRESTREAM NOR ANY THIRD PARTY LICENSOR REPRESENTS OR WARRANTS THAT THE FUNCTIONALITY OF THE SOFTWARE WILL SATISFY ANY OR ALL OF LICENSEE'S REQUIREMENTS, THAT THE SOFTWARE WILL WORK IN COMBINATION WITH ANY HARDWARE OR SOFTWARE PRODUCTS

PROVIDED BY THIRD PARTIES, THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT ALL ERRORS OR DEFECTS IN THE SOFTWARE WILL BE CORRECTED. SOFTWARE UPDATES, IF ANY, WILL BE PROVIDED AT THE SOLE DISCRETION OF LIBRESTREAM. LICENSEE ACKNOWLEDGES AND AGREES THAT SOFTWARE IN GENERAL IS NOT ERROR-FREE, AND THAT THE EXISTENCE OF MINOR ERRORS OR DEFECTS IN THE SOFTWARE DOES NOT MEAN THAT THE SOFTWARE DOES NOT PERFORM IN SUBSTANTIAL CONFORMANCE WITH ITS APPLICABLE PUBLISHED SPECIFICATIONS. NEITHER LIBRESTREAM NOR ANY THIRD PARTY LICENSOR SHALL BE RESPONSIBLE FOR THE RECONSTRUCTION OF ANY CORRUPTED OR LOST DATA FILES.

6.5 Librestream reserves the right to at any time provide a limited warranty for any Librestream Software that is different from the limited warranty set forth in Sections 6.1 and 6.2. The text of any such different limited warranty will be included with that Librestream Software, regardless of whether that Librestream Software is embedded in a Librestream Product, is provided to Licensee on CDROM or is downloaded by Licensee. In the event of any inconsistency between any such other limited warranty and the limited warranty set forth in Sections 6.1 and 6.2, the inconsistency shall be resolved in favor of such other limited warranty.

6.6 Librestream may also provide a separate limited warranty with respect to the hardware components of a Librestream Product.

7. NO LIABILITY FOR INDIRECT DAMAGES. REGARDLESS OF CIRCUMSTANCES AND REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT UNDER THIS AGREEMENT OR IN TORT, INCLUDING NEGLIGENCE OR PRODUCTS LIABILITY, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL LIBRESTREAM OR ANY THIRD PARTY LICENSOR HAVE ANY LIABILITY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE OR EXEMPLARY LOSSES OR DAMAGES OF ANY NATURE OR KIND WHATSOEVER, ARISING OUT OF THIS AGREEMENT AND/OR LICENSEE'S USE OF, DELAY IN USING OR INABILITY TO USE THE SOFTWARE, ANY CONFIDENTIAL INFORMATION AND/OR ANY LIBRESTREAM PRODUCT, INCLUDING BUT NOT LIMITED TO LOST OR CORRUPTED DATA OF LICENSEE OR ANY THIRD PARTY, LOST PROFITS OR LOST GOODWILL, BUSINESS INTERRUPTION OR LOSS OF INFORMATION, FAILURE TO REALIZE SAVINGS, OR FOR ANY CLAIM OR DEMAND AGAINST LICENSEE BY ANY THIRD PARTY, EVEN IF LIBRESTREAM OR ANY THIRD PARTY LICENSOR MAY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSSES OR DAMAGES OR EVEN IF SUCH LOSSES OR DAMAGES WERE REASONABLY FORESEEABLE.

8. LIMITED LIABILITY FOR DIRECT DAMAGES. REGARDLESS OF CIRCUMSTANCES AND REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT UNDER THIS AGREEMENT OR IN TORT, INCLUDING NEGLIGENCE OR PRODUCTS LIABILITY, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE CUMULATIVE LIABILITY OF LIBRESTREAM AND THE THIRD PARTY LICENSORS FOR LICENSEE'S DIRECT DAMAGES ARISING OUT OF OR RESULTING IN ANY MANNER WHATSOEVER FROM THIS AGREEMENT AND/OR LICENSEE'S USE OF, DELAY IN USING OR INABILITY TO USE THE SOFTWARE, ANY CONFIDENTIAL INFORMATION AND/OR ANY LIBRESTREAM PRODUCT, INCLUDING WITHOUT LIMITATION ANY UNCURED MATERIAL DEFAULT, BREACH OR FAILURE ON THE PART OF LIBRESTREAM OR ANY THIRD PARTY LICENSOR UNDER THIS AGREEMENT, SHALL IN NO EVENT EXCEED THE GREATER OF THE LICENSE FEE INITIALLY PAID BY LICENSEE FOR THE SOFTWARE OR ONE DOLLAR (\$1.00), IN CANADIAN CURRENCY.

9. FUNDAMENTAL UNDERSTANDING REGARDING RISK ALLOCATION. LICENSEE ACKNOWLEDGES AND AGREES THAT THE FEES PAYABLE BY LICENSEE PURSUANT TO THIS AGREEMENT OR ANY PURCHASE ORDER HAVE BEEN DETERMINED BY LIBRESTREAM BASED UPON A SPECIFIC RISK ALLOCATION BETWEEN LIBRESTREAM AND THE THIRD PARTY LICENSORS, ON THE ONE HAND, AND LICENSEE, ON THE OTHER HAND, AND THAT LIBRESTREAM WOULD NOT HAVE ACCEPTED ANY PURCHASE ORDER THAT RELATES TO LICENSEE AND WOULD NOT HAVE LICENSED THE SOFTWARE TO LICENSEE PURSUANT TO THIS AGREEMENT IN THE ABSENCE OF SECTIONS 6, 7 AND 8. LICENSEE FURTHER ACKNOWLEDGES AND AGREES THAT THESE SECTIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. IN JURISDICTIONS THAT PROHIBIT EXCLUSION OF LIABILITY OR LIMITATION OF IMPLIED WARRANTIES, SECTIONS 6, 7 AND 8 MAY BE LIMITED IN THEIR APPLICATION TO LICENSEE AND, DEPENDING ON LOCAL LAW, LICENSEE MAY HAVE OTHER SPECIFIC LEGAL RIGHTS.

10. TERM AND TERMINATION.

10.1 The licenses granted pursuant to this Agreement are perpetual unless terminated earlier as specified herein. Licensee may terminate the licenses and this Agreement at any time upon the provision of written notice to Librestream.

Without prejudice to any other right or remedy which may be available to Librestream, the licenses and this Agreement shall immediately terminate without the necessity of any notice from Librestream in the event that Licensee:

- (a) fails to comply with any provision of this Agreement; or
- (b) makes any voluntary arrangement with its creditors for the general settlement of its debts or becomes subject to the supervision of a bankruptcy tribunal; or
- (c) has an order made against it, or passes a resolution, for its winding-up, or has a lien holder take possession of, or has a receiver or similar officer appointed over, all or substantially all of its property or assets.

10.2 Upon termination of this Agreement for any reason, Licensee agrees to immediately cease use of, and to return or destroy, at Librestream's sole option, the Software and any other Confidential Information in Licensee's possession, custody or control, together with all copies, including but not limited to deletion of the foregoing from the Computer and any other computer on which the Software or any portion thereof may have been installed, and to certify such return or destruction in writing.

10.3 Notwithstanding anything to the contrary contained herein, the bold faced and capitalized wording at the beginning of this Agreement and Sections 2.1(c), 2.3, 2.4, 2.6, 2.7, 4, 5, 6, 7, 8, 9, 10, 11, 12 and 13 (and the relevant definitions in Section 1) shall survive any termination of this Agreement for any reason whatsoever.

11. **EXPORT.** Some of the Software and Confidential Information is subject to United States export control laws and regulations, and some or all of the Software may be subject to export or import regulations in other countries as well. Licensee agrees that it will not export, re-export, transfer or import any of the Software, any of the Confidential Information or any Librestream Product in violation of any applicable laws or regulations of the United States or any other country. Licensee is responsible for obtaining any licenses or authorizations required to export, re-export, transfer or import all or any portion of the Software and Confidential Information or any Librestream Product.

12. **GOVERNMENT DEPARTMENTS.** In the event that Licensee is a governmental entity, only the department(s) or agency(s) specifically licensed in the Purchase Order to use the Software shall have the right to use the Software. Governmental departments or agencies not so specifically licensed must have a separate license and must pay additional license fees.

13. **GENERAL PROVISIONS.**

13.1 Licensee shall not assign or otherwise transfer this Agreement or any of its rights and/or obligations hereunder, whether in whole or in part, including by operation of law, without the prior express written consent of Librestream.

13.2 Licensee hereby acknowledges that its breach of this Agreement may cause irreparable harm and significant injury to Librestream and/or one or more of the Third Party Licensors in an amount that may be difficult to ascertain and for which a remedy at law may be inadequate. Accordingly, Licensee agrees that, in addition to any other rights and remedies it may have, Librestream shall have the right to seek injunctive relief in any court of competent jurisdiction to enforce Licensee's obligations under this Agreement.

13.3 This Agreement shall be construed and governed by the laws in force in the province of Manitoba, excluding its conflict of laws rules. The parties consent to the jurisdiction of all the courts in Manitoba, and agree that, except for requests for injunctive relief pursuant to Section 13.2, venue shall lie exclusively in Manitoba. **THE PARTIES EXCLUDE IN ITS ENTIRETY THE APPLICATION TO THIS AGREEMENT OF THE UNITED NATIONS CONVENTION ON CONTRACTS FOR THE INTERNATIONAL SALE OF GOODS.**

13.4 When any notice is required or authorized hereunder, such notice shall be given in writing by recognized delivery service or personal delivery addressed to the other party. Notices shall be sent to Licensee at the address set forth in the Purchase Order and to Librestream at Suite 110, 895 Waverley Street, Winnipeg, Manitoba, Canada R3T 5P4. Either party may change its address for notice hereunder by providing the other party with ten (10) days written notice thereof. Notices shall be effective upon receipt by the recipient.

13.5 The original of this Agreement has been written in the English language, and the governing language of this Agreement shall be English. Licensee hereby waives and agrees not to assert any right to have this Agreement written in the language of Licensee's place of residence.

13.6 A waiver of any default hereunder or of any of the terms or conditions of this Agreement shall not be deemed to be a continuing waiver or a waiver of any other default or of any other term or condition, but shall apply solely to the instance to which such waiver is directed. The exercise of any right or remedy provided in this Agreement shall be without prejudice to the right to exercise any other right or remedy provided at law or in equity.

13.7 In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall not in any way be affected or impaired, and a valid, legal and enforceable

provision of similar intent and effect shall be substituted for such invalid, illegal or unenforceable provision.

13.8 This Agreement constitutes the entire agreement between the parties with respect to the license of the Software and the other subject matter of this Agreement, and supersedes and terminates all other prior and/or contemporaneous verbal and/or written agreements and understandings with respect thereto. No modifications to this Agreement shall be enforceable except when in writing and signed by an authorized signatory of the party to be bound thereby. Without limiting the generality of the foregoing, the terms and conditions of any purchase order or other document submitted by Licensee to Librestream or to any Librestream distributor or other representative shall not be binding on Librestream unless definitively accepted in writing by Librestream.

13.9 THIS AGREEMENT SHALL IMMEDIATELY AND AUTOMATICALLY BE EFFECTIVE AND ENFORCEABLE UPON ANY DOWNLOADING OR INSTALLATION OF ANY OF THE SOFTWARE OR UPON ANY USE OF ANY OF THE SOFTWARE OR ANY LIBRESTREAM PRODUCT. It shall not be a requirement to the effectiveness and enforceability of this Agreement that any Licensee or Librestream execute this Agreement.

SCHEDULE A – LIBRESTREAM SOFTWARE AND LIBRESTREAM NOTICES

Name of Librestream Software – Onsight Enterprise and Onsight Management Suite

Copyright Notice: Copyright 2007-2010 Librestream Technologies Incorporated. All Rights Reserved.

Patents Notice: United States Patent # 7,221,386, together with additional patents pending in Canada, the United States and other countries, all of which are in the name of Librestream Technologies Inc.

Trademark Notice: Librestream, the Librestream logo, Onsight, Onsight Expert, Onsight Mobile, Onsight Enterprise, and Onsight Management Suite 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.

SCHEDULE B – THIRD PARTY SOFTWARE AND THIRD PARTY LICENSOR NOTICES

Not applicable.

20 Librestream Contact Information

Website

www.librestream.com

Head Office

Librestream Technologies Inc.

895 Waverley St., Suite 110

Winnipeg, Manitoba

Canada, R3T 5P4

General Inquiries:

Email information@Librestream.com

Phone +1.204.487.0612

Fax +1.204.487.0914

Support:

Email support@Librestream.com

Phone +1.204.487.0612

Fax +1.204.487.0914



Librestream