

Sightline Assure

User's Guide

Version 2.0.8

February 2017



© Copyright 2017 Sightline Systems Corp. All rights reserved.

Sightline, the Sightline logo, Sightline Assure, Sightline EDM, Sightline Agent, Sightline Expert Advisor/Vision, Sightline ACE, Sightline *Clairvor* and Sightline SupportWeb are trademarks or trade names of Sightline Systems Corporation. All other trademarks and trade names are the property of their respective owners.

Disclaimer

This manual describes how to install and use the Sightline™ Enterprise Data Manager software. The Sightline software suite is comprised of proprietary products offered for licensing by Sightline Systems Corporation. Use of this software requires that a license agreement be signed with Sightline Systems Corporation. No part of this document may be copied, distributed, or transmitted in any form or by any means, mechanical or electronic, without the express written permission of SightLine Systems Corporation.

Sightline Systems Corporation believes the information presented in this guide is accurate and reliable. Sightline Systems Corporation assumes no responsibility for any consequences arising from the use of the guide. SightLine Systems Corporation reserves the right to revise the contents of this publication without obligation to notify any person of such revisions.

All questions and comments concerning this document should be directed to:

Sightline Systems Customer Support
4035 Ridge Top Road
Suite 510
Fairfax, VA 22030

Phone: 703-563-3000
Fax: 703-563-4000
E-mail: support@sightlinesystems.com

Table of Contents

Chapter 1	Introduction	1-1
Chapter 2	Installing and Upgrading Sightline Assure	2-1
2.1	Installing Assure on a Windows System.....	2-1
2.1.1	Minimum Windows System Requirements	2-1
2.1.2	Installation Steps	2-2
2.1.3	Updating the Windows Power Agent AccessKey.....	2-4
2.1.4	Start the Assure UI	2-9
2.1.5	Upgrading Assure on a Windows System.....	2-10
2.2	Installing Assure on a Linux System.....	2-10
2.2.1	Minimum Linux Host Hardware Requirements.....	2-10
2.2.2	Installation Steps	2-11
2.2.3	Update the Linux Power Agent AccessKey.....	2-11
2.2.4	Start the Assure UI	2-13
2.2.5	Upgrading Assure on a Linux System.....	2-13
2.3	Installing the Assure Virtual Appliance on VMware.....	2-14
2.3.1	Assure Appliance Hardware Specifications.....	2-14
2.3.2	Installation Steps	2-14
2.3.3	Post-Install Configuration (Optional)	2-19
2.3.4	Configuring the Sightline Power Agent	2-24
2.4	Assure Communication Ports.....	2-26
2.5	Uninstalling Assure.....	2-27
2.5.1	Uninstalling Assure on a Windows System	2-27
2.5.2	Uninstalling Assure on a Linux System	2-29
2.6	Assure Memory Allocation	2-30
2.6.1	Increasing Memory on Windows Systems	2-30
2.6.2	Increasing Memory on Linux Systems	2-31
Chapter 3	Getting Started with Sightline Assure	3-1
3.1	Accessing Assure through your Browser	3-1
3.2	Logging into Assure.....	3-1
3.3	Entering the AccessKey.....	3-2
3.4	The Assure Setup Wizard.....	3-2
Chapter 4	Using Assure	4-1
4.1	The Assure Dashboard.....	4-1
4.2	Assure Server Overview Page	4-2
4.2.1	System Health Checks.....	4-3
4.2.2	Monitored Applications	4-4
4.2.3	Active Alerts and Alert History	4-4
4.2.4	Utilization Charts.....	4-5
4.3	VMware Host Overview Page.....	4-10
4.4	System Overview Page for a VMware Guest.....	4-11

4.5	Monitoring Options for VMware Guests	4-12
4.6	System Overview Page for everRun Systems	4-13
4.7	Creating and Monitoring Applications	4-14
4.7.1	Creating Applications.....	4-15
4.7.2	Managing Credentials	4-18
4.8	Alert Notification Emails	4-19
4.9	Scheduled Reports	4-19
4.10	Assure Mobile	4-20
Chapter 5 Assure Settings Menu		5-1
5.1	Dashboard	5-2
5.2	Add Server	5-2
5.3	Add Devices	5-5
5.4	Additional Monitoring.....	5-6
5.5	Email Settings	5-7
5.5	Report Settings.....	5-9
5.6	Update AccessKey	5-10
5.7	Manage Users.....	5-11
5.8	Manage Views	5-12
5.9	Download All Logs	5-15
5.10	Assure User's Guide.....	5-15
Appendix A Sightline OPC Server.....		A-1
Appendix B Monitoring Stratus everRun Systems.....		B-1
B.1	Installing the Sightline Power Agent for Linux Systems on everRun nodes.....	B-1
B.1.1	Retrieve your AccessKey string.....	B-1
B.1.2	Download the Power Agent Installation Kit.....	B-2
B.1.3	Transfer the Power Agent Installation Kit to the target system	B-2
B.1.4	Unzip the install file.....	B-3
B.1.5	Untar the install file	B-3
B.1.6	Execute the install script	B-3
B.1.7	Supply the requested information.....	B-3
B.1.8	Add the system to Assure.....	B-4
B.2	Monitoring KVM guests on everRun systems.....	B-4
B.3	Configure SNMP Settings.....	B-4
Appendix C Prerequisites for Hardware Monitoring		C-1
C.1	Cisco	C-1
C.2	Dell iDRAC 6.....	C-2
C.3	HP ilo	C-2
C.4	Windows 2012 Systems	C-3
C.5	Windows 2008 R2 Systems.....	C-4

Chapter 1

Introduction

Sightline Assure is designed to provide you the assurance that your mission-critical systems and applications are both available and healthy.

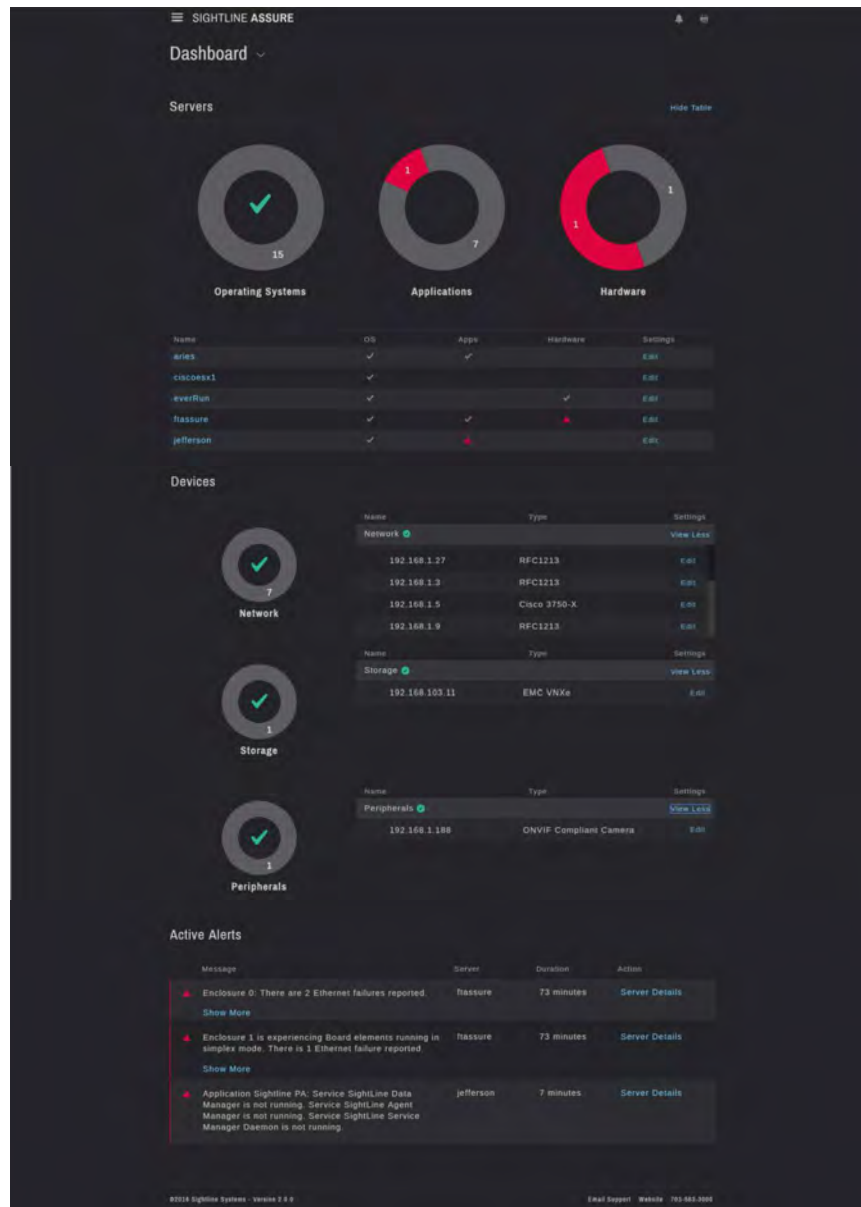


Figure 1-1. Assure Main Dashboard

Assure provides a single, unified view of system health that includes hardware, system software and applications. Assure's easy-to-use interface shows when systems are running well, or generates alerts when there are issues that require attention.

Easy to install and configure, Sightline Assure is a lightweight, scalable solution that provides the information and answers you need without IT complexity. You can configure Assure to provide summary reports and even access the Assure UI via your mobile device.

Chapter 2

Installing and Upgrading Sightline Assure

This chapter describes Sightline Assure application deployment and the prerequisites for deploying and running Assure.

Sightline Assure is supported on servers running the VMware, Microsoft Windows or Red Hat Linux operating systems. These instructions assume that you have some knowledge of Windows and Linux system administration.



BEFORE INSTALLING ASSURE Before installing Assure, confirm that the system on which you are installing the Assure software has the following:

- ◆ a valid hostname that is *not* localhost.
- ◆ the hostname cannot contain an underscore (_). The EDM component of Sightline Assure will not start when installed on a server whose computer name contains an underscore (_). If your server has an underscore in the name, and the system cannot be renamed, contact your Assure support representative for a possible workaround.
- ◆ an IP address that can reach the intended monitored objects (servers, devices, storage arrays, etc). For information about configuring a static IP address or DNS, see Section 2.3.3, *Post-Install Configuration*.



The Assure installation process should open the local firewall ports required for internal communication and communication to monitored objects. See Section 2.4, *Assure Communication Ports*, for details.



The minimum system requirements listed below support Assure implementations with fewer than five or six monitored objects (servers, devices, storage arrays, etc). If you are monitoring more objects, or if Assure's UI response seems sluggish, you may need to allocate more memory to Assure. See Section 2.6, *Assure Memory Allocation*, for details.

2.1 Installing Assure on a Windows System

2.1.1 Minimum Windows System Requirements

Operating system: Windows 2008 R2, Windows 2012

Processor: 1000 MHz

Memory: 2 GB

HDD Free space: 50 GB

Assure Installation File Size: 50 MB

Network Speed: 100 Mbit/second

2.1.2 Installation Steps



Sightline Assure accepts an AccessKey string for licensing. If you do not have an AccessKey, Assure will run for 45 days in trial mode; during this time, an AccessKey can be applied to extend the expiration of the software. Contact your support representative for a valid AccessKey string.

Log in as a user with **Administrator** privileges on the target Windows system, and transfer the Windows Assure installation zip file (`Assure_Windows.zip`) to a temporary directory.

Unzip the file by right-clicking on it and selecting either **Extract All** or **Extract here**, depending on the option available.

If you select **Extract All**, a window will appear prompting you to select a path to save the contents of the zip folder. The default location provided should be the same location as the downloaded zip file. Sightline recommends using the default directory. Ensure the **Show extracted files when complete** box is checked, then click **Extract** (Figure 2-1).

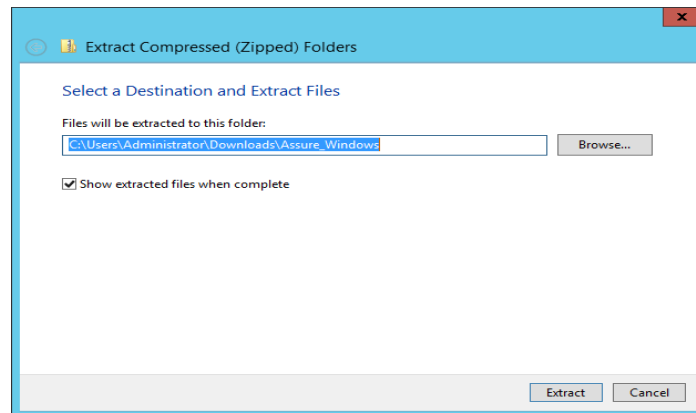


Figure 2-1. Extract Assure Windows Install Zip File

An `Assure_Windows` folder will be created, as shown in Figure 2-2.

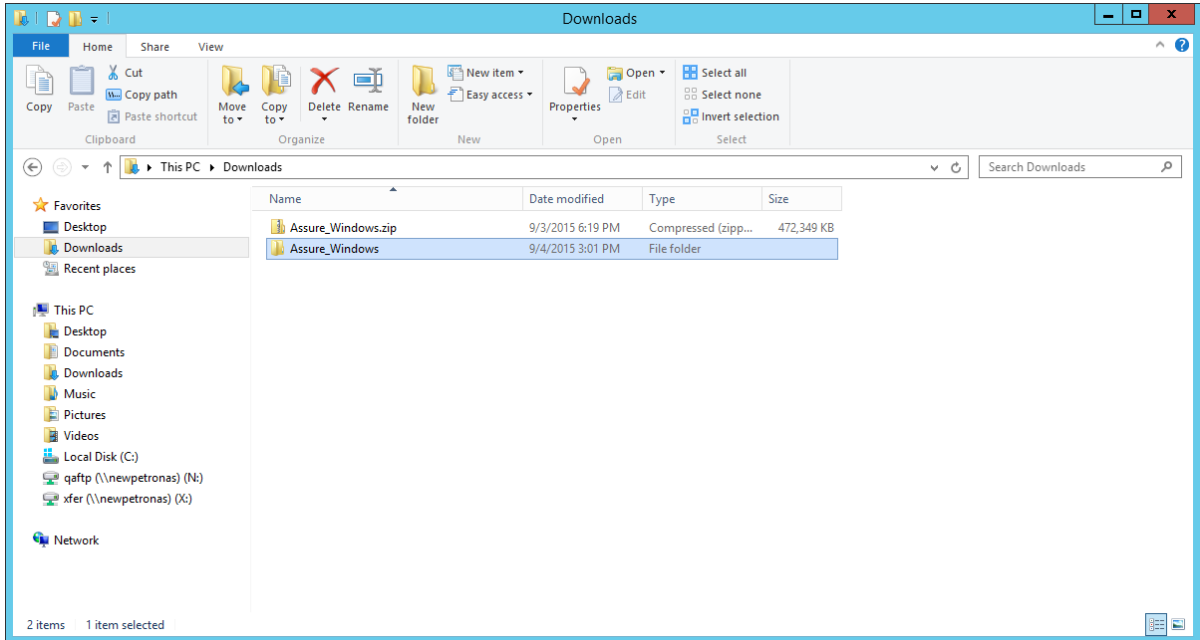


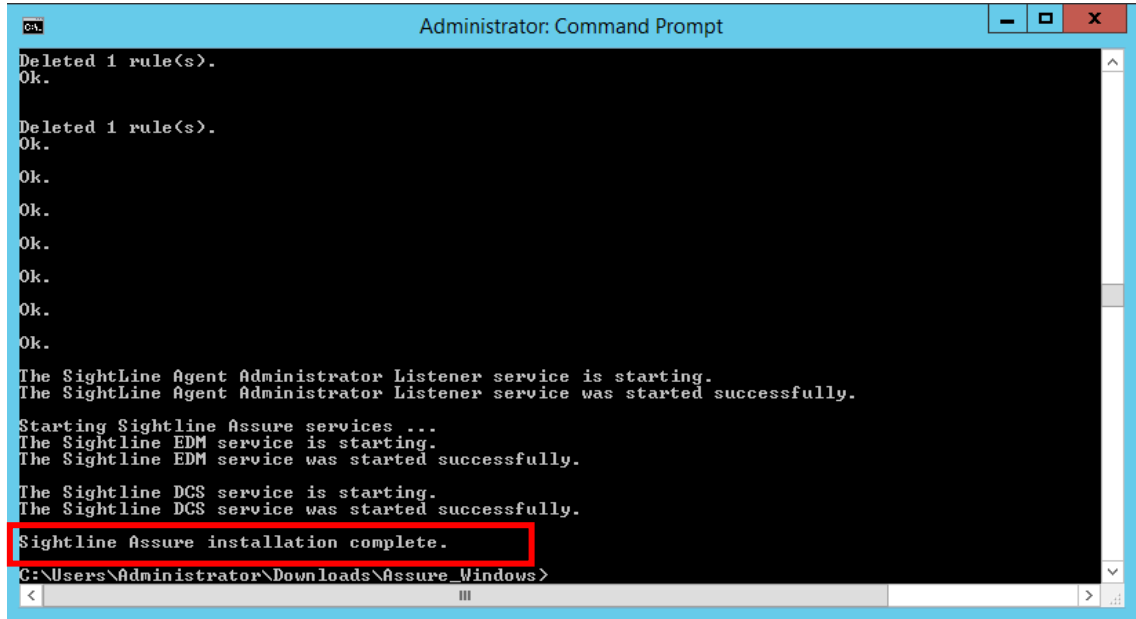
Figure 2-2. Extracted Assure Windows Directory.

- ◆ For machines running Windows 8 Desktop, or Windows Server 2012 and up, right-click on the **Start** menu and select **Command Prompt (Admin)**.
- ◆ For machines running Windows 7 desktop, or any version of Windows Server 2008, open a command prompt with Administrator privileges by clicking **Start | All Programs | Accessories** then right-click on **Command Prompt** and select **Run as Administrator**.

Once a command prompt opens, navigate to the `Assure_Windows` directory that was just unzipped, and initiate the installation batch file:

```
C:\...\Assure_Windows\Assure_install.bat
```

The command prompt output will update you on the progress of the installation; the entire install takes approximately 3-4 minutes. When installation is complete, a message will be displayed (Figure 2-3).



```
Administrator: Command Prompt
Deleted 1 rule(s).
Ok.

Deleted 1 rule(s).
Ok.
Ok.
Ok.
Ok.
Ok.
Ok.
Ok.
Ok.

The SightLine Agent Administrator Listener service is starting.
The SightLine Agent Administrator Listener service was started successfully.

Starting Sightline Assure services ...
The Sightline EDM service is starting.
The Sightline EDM service was started successfully.

The Sightline DCS service is starting.
The Sightline DCS service was started successfully.
Sightline Assure installation complete.
C:\Users\Administrator\Downloads\Assure_Windows>
```

Figure 2-3. Assure Installation Status Output

2.1.3 Updating the Windows Power Agent AccessKey

The installation process for Sightline Assure on a Windows system also installs a Power Agent. The Power Agent must be enabled with an AccessKey string; there are three places you might refer to for the AccessKey string.

- If you received an email with the Assure AccessKey, then it will include the AccessKey string for the Power Agent.
- If you are running Assure in trial mode, then the AccessKey string will be shown in the **Additional Monitoring** dialog box; simply copy this string and use it during the Power Agent installation.



Figure 2-4. Additional Monitoring Dialog Box

- If you have entered an AccessKey string into your Assure implementation, the **Monitored Servers** section of the AccessKey string should be used for the Power Agent. Select **Settings | Update AccessKey** and make a note of the AccessKey string to the right of the **Monitored Servers** entry.

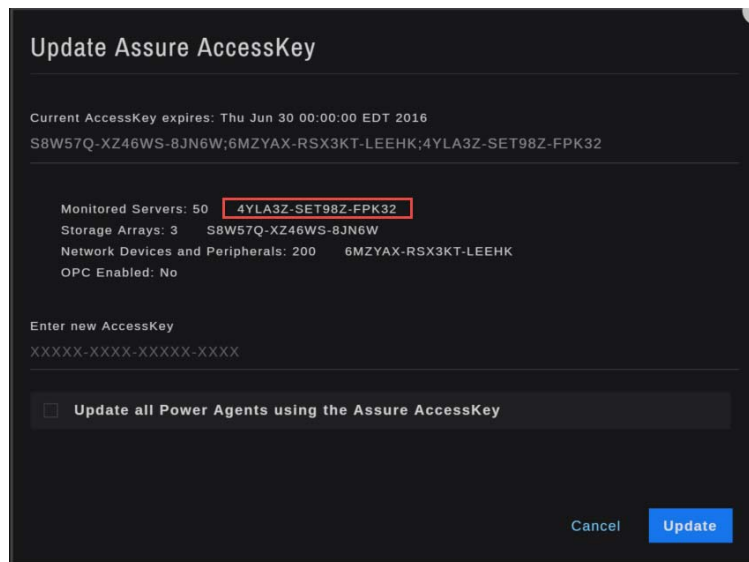


Figure 2-5. Update Assure AccessKey Dialog Box

To update the Power Agent AccessKey on a Windows 7 desktop or Windows Server 2008 system, refer to Section 2.1.3.1, *Windows 7 / Windows Server 2008, 2008 R2*. For a Windows 8 desktop or Windows Server 2012 system, see Section 2.1.3.2, *Windows 8 / Windows Server 2012, 2012R2*.

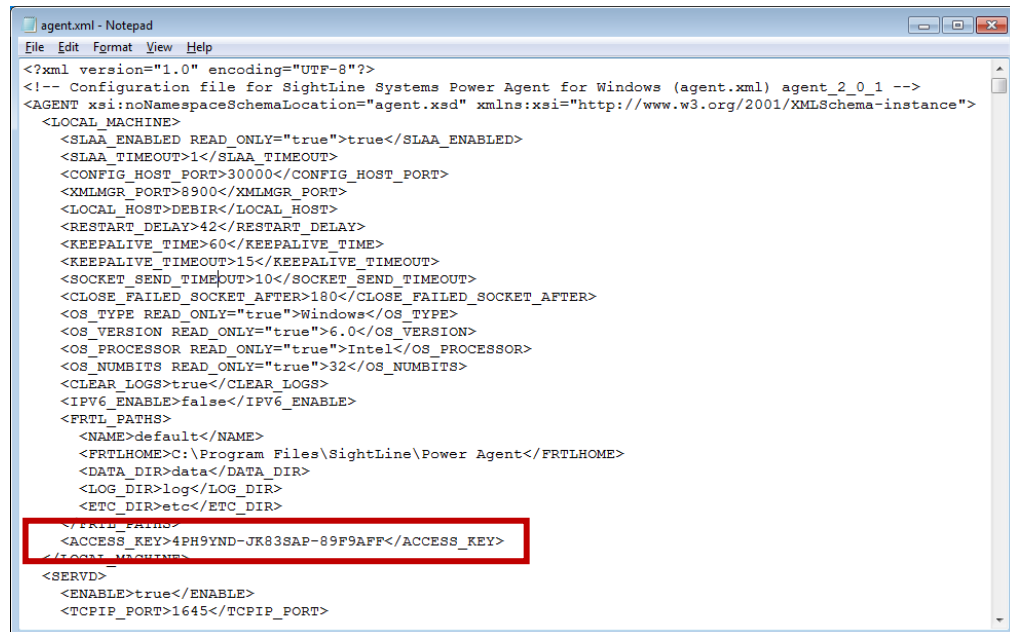
2.1.3.1 Windows 7 / Windows Server 2008, 2008R2

Run **notepad** as Administrator:

- ◆ Select **Start | All Programs | Accessories**
- ◆ Right-click on **Notepad** and select **Run as administrator**.

Once notepad is open:

- ◆ Select **File | Open**
- ◆ Navigate to the **Program Files \ Assure \ PowerAgent \ etc** directory
- ◆ Open the **agent.xml** file
- ◆ Insert a valid AccessKey string into the ACCESS_KEY element as shown in Figure 2-6.



```
agent.xml - Notepad
File Edit Format View Help
<?xml version="1.0" encoding="UTF-8"?>
<!-- Configuration file for SightLine Systems Power Agent for Windows (agent.xml) agent_2_0_1 -->
<AGENT xsi:noNamespaceSchemaLocation="agent.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <LOCAL_MACHINE>
    <SLAA_ENABLED READ_ONLY="true">true</SLAA_ENABLED>
    <SLAA_TIMEOUT>1</SLAA_TIMEOUT>
    <CONFIG_HOST_PORT>30000</CONFIG_HOST_PORT>
    <XMLMGR_PORT>8900</XMLMGR_PORT>
    <LOCAL_HOST>DEBIR</LOCAL_HOST>
    <RESTART_DELAY>42</RESTART_DELAY>
    <KEEPALIVE_TIME>60</KEEPALIVE_TIME>
    <KEEPALIVE_TIMEOUT>15</KEEPALIVE_TIMEOUT>
    <SOCKET_SEND_TIMEOUT>10</SOCKET_SEND_TIMEOUT>
    <CLOSE_FAILED_SOCKET_AFTER>180</CLOSE_FAILED_SOCKET_AFTER>
    <OS_TYPE READ_ONLY="true">Windows</OS_TYPE>
    <OS_VERSION READ_ONLY="true">6.0</OS_VERSION>
    <OS_PROCESSOR READ_ONLY="true">Intel</OS_PROCESSOR>
    <OS_NUMBITS READ_ONLY="true">32</OS_NUMBITS>
    <CLEAR_LOGS>true</CLEAR_LOGS>
    <IPV6_ENABLE>false</IPV6_ENABLE>
    <FRTL_PATHS>
      <NAME>default</NAME>
      <FRTLHOME>C:\Program Files\SightLine\Power Agent</FRTLHOME>
      <DATA_DIR>data</DATA_DIR>
      <LOG_DIR>log</LOG_DIR>
      <ETC_DIR>etc</ETC_DIR>
    </FRTL_PATHS>
    <ACCESS_KEY>4FH9YND-JK83SAP-89F9AFF</ACCESS_KEY>
  </LOCAL_MACHINE>
  <SERVD>
    <ENABLE>true</ENABLE>
    <TCPIP_PORT>1645</TCPIP_PORT>
  </SERVD>
</AGENT>
```

Figure 2-6. ACCESS_KEY element in the agent.xml configuration file

Save your changes, close Notepad, then start the Power Agent as follows:

- ◆ Select **Start | All Programs | Sightline | Power Agent**
- ◆ Right-click on **Start Agents**
- ◆ Select **Run as administrator** (Figure 2-7).

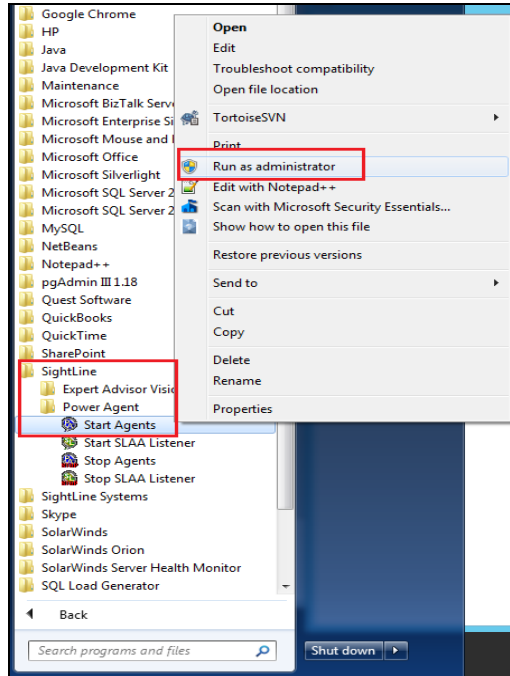


Figure 2-7. Starting Sightline Power Agent on Windows Server 2008

A command window will display with startup progress. It will take a few minutes for the Power Agent processes to start, and then a successful startup message will appear (Figure 2-8).

 A screenshot of a command window titled 'SightLine Console'. The window shows the following text:


```

FRTLHOME is C:\Program Files\SightLine\Power Agent
1 file(s) moved.
Starting "SightLine Agent Manager"
The service was started.
Starting "SightLine Data Manager"
The service was started.
Starting "SightLine Service Manager Daemon"
The service was started.
Starting "SightLine Threshold Manager Daemon"
The service was started.
SightLine Power Agent is starting, please wait...
...Waiting for the power agent to start...
...Waiting for the power agent to start...
...Waiting for the power agent to start...
SightLine Power Agent has started.
Press any key to continue . . . _
  
```

Figure 2-8. Sightline Power Agent Startup Console

Press the **Enter** key to close the console.

2.1.3.2 Windows 8 / Windows Server 2012, 2012R2

Run **notepad** as Administrator:

- ◆ Click on the **Start** menu
- ◆ Click on the **Apps** icon (the circled arrow icon located at the bottom left section)

- ◆ Locate the **Windows Accessories** section
- ◆ Right-click on **Notepad** and select **Run as administrator** (Figure 2-9).

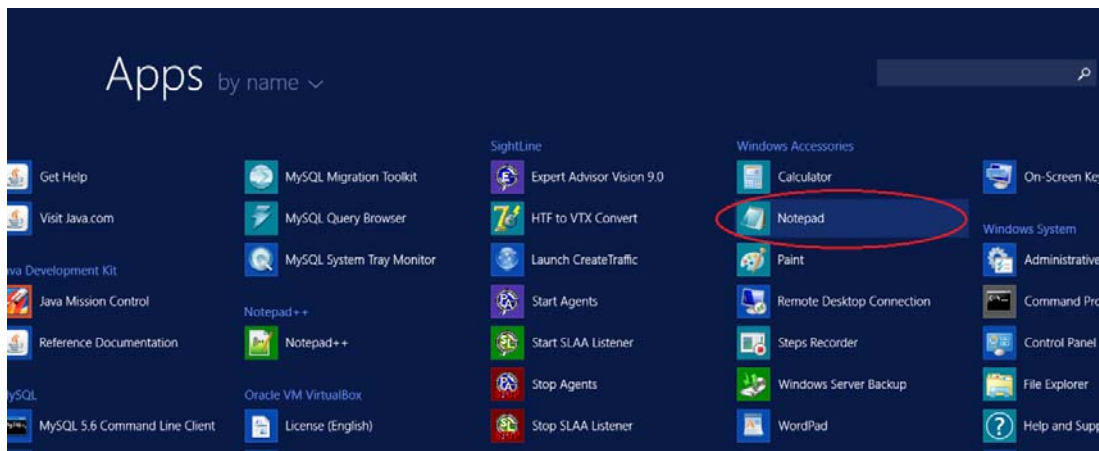


Figure 2-9. Starting Notepad, Windows Server 2012

Once notepad is open:

- ◆ Select **File | Open**
- ◆ Navigate to the **Program Files \ Assure \ PowerAgent \ etc** directory
- ◆ Open the **agent.xml** file
- ◆ Insert a valid AccessKey string into the ACCESS_KEY element as shown in Figure 2-10.

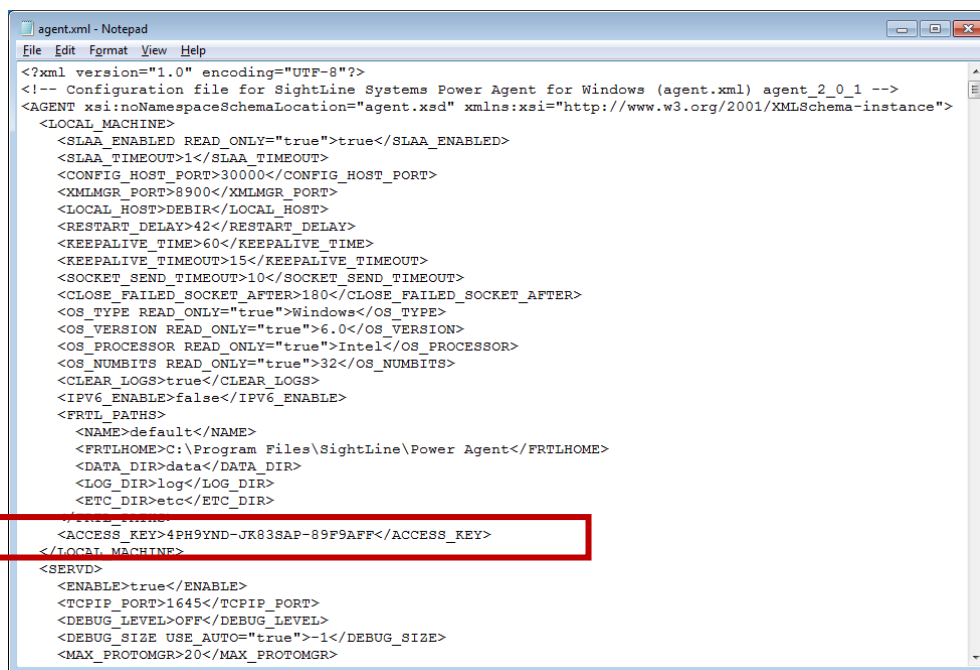


Figure 2-10. ACCESS_KEY section in agent.xml

Save your changes, close Notepad, then start the Power Agent as follows:

- ◆ Click the **Start** menu, then click on the **Apps** icon (the circled arrow icon located at the bottom left section)
- ◆ Locate the **Sightline** section
- ◆ Right-click on **Start Agents** and select **Run as administrator** (Figure 2-11).

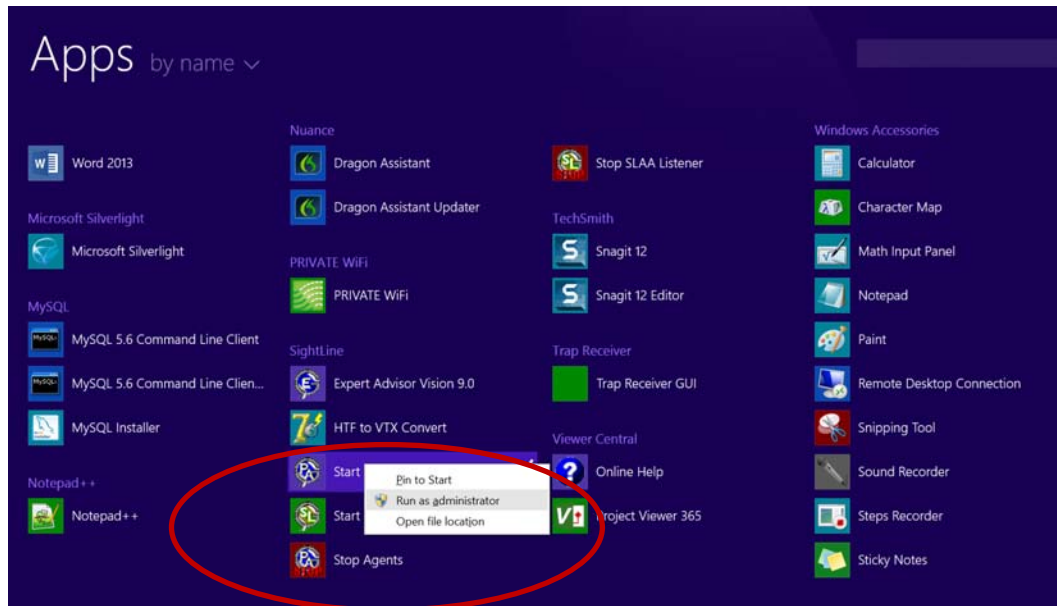


Figure 2-11. Starting the SightLine Power Agent on Windows Server 2012

2.1.4 Start the Assure UI

On your desktop, point your browser to `http://server_hostname:8080/edm`, where **server_hostname** is the computer name. The server's IP Address can be used in place of the server hostname. For example:

```
http://myserver:8080/edm
http://192.168.1.50:8080/edm
```

The login screen should appear. The default credentials are as follows:

Username: **admin**
 Password: **admin**

Click **Login** to enter the configuration wizard; see Chapter 3, *Getting Started*, for information about the Assure startup wizard.

2.1.5 Upgrading Assure on a Windows System

The upgrade process for Assure is similar to a clean installation, with the only difference being the argument included during upgrade process. The previous version of Assure does not have to be shutdown prior to the upgrade. Once the latest Assure installation kit has been obtained, follow the upgrade instructions below:

Log in to the target Windows system as a user with **Administrator** privileges.

Transfer the latest Windows Assure installation zip file (`Assure_Windows_x.x.zip`) to a temporary directory. Unzip the file by right-clicking on it and selecting either **Extract All** or **Extract here**, depending on the option available.

If you select **Extract All**, a window will appear prompting you to select a path to save the contents of the zip folder. The default location provided should be the same location as the Assure zip file. Sightline recommends extracting to this default directory. Ensure the **Show extracted files when complete** box is checked, then click **Extract**

An `Assure_Windows_x.x` folder will be created.

Open a command prompt with **Administrative** privileges, and navigate to the `Assure_Windows_x.x` directory.

Once in the directory, run the following command:

```
C:\Assure_windows_x.x>Assure.bat upgrade
```

The progress of the upgrade progress will be displayed in the command prompt window, and will notify users once the upgrade is complete.

Upon completion of the upgrade, log into the Assure UI and verify the latest Assure version number at the bottom of the Main Dashboard page.

2.2 Installing Assure on a Linux System



An AccessKey will be required for the final step of the installation. Contact your Sightline representative for an AccessKey.

2.2.1 Minimum Linux Host Hardware Requirements

Operating system: Red Hat Linux, Oracle Linux

Processor: 1000 MHz

Memory: 2 GB

HDD Free space: 50 GB

Assure Installation File Size: 50 MB

Network Speed: 100 Mbit/second

2.2.2 Installation Steps

Transfer the Linux Assure installation file, `assure_linux.tar.gz`, to the `/usr/local` folder on the system where it will be installed.

Log in as root, or a user that has root privileges, and then change directory to `/usr/local`:

```
#cd /usr/local
```

Unzip the file and extract the contents of the tar file:

```
#gunzip assure_linux.tar.gz
#tar -xvf assure_linux.tar -o
```

This will create a `/usr/local/assure_linux_x.x` folder.

Change directory to `/usr/local/assure_linux_x.x`:

```
#cd /usr/local/assure_linux_x.x
```

Enter the following command, which will install Sightline Assure (you must be root or a user with root privileges to perform this step):

```
./assure.sh install or sudo assure.sh install (the latter command should be used by a non-root user with root privileges).
```

The command prompt output will update you on the progress of the installation. The install is complete when the following message is displayed on the console:

```
#Sightline Assure was successfully installed.
```

The install process should generate a `sightline` directory, which contains Assure component sub-directories. This directory does not need to be accessed in order to start Assure.

2.2.3 Update the Linux Power Agent AccessKey

The installation process for Sightline Assure installs a Power Agent on the system. The Power Agent must be enabled with an AccessKey string; There are three places you might refer to for the AccessKey string. Even if the strings are different, they should all be valid.

- If you received an email with the Assure AccessKey, then it will include the AccessKey string for the Power Agent.
- If you are running Assure in trial mode, then the AccessKey string will be shown in the **Additional Monitoring** dialog box; simply copy this string and use it during the Power Agent installation.



Figure 2-12. Additional Monitoring Dialog Box

- If you have entered an AccessKey string into your Assure implementation, the **Monitored Servers** section of the AccessKey string should be used for the Power Agent. Select **Settings | Update AccessKey** and make a note of the AccessKey string to the right of the **Monitored Servers** entry.

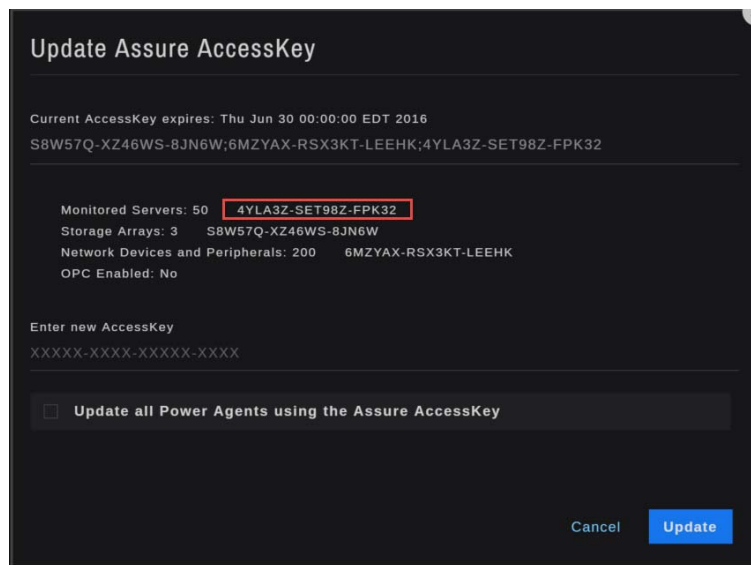


Figure 2-13. Update Assure AccessKey Dialog Box

To update the AccessKey, navigate to `/usr/local/sightline/sightlinePA/etc` and open the agent `.xml` file. Insert a valid AccessKey in the `ACCESS_KEY` field:

```
<ACCESS_KEY>insert_accesskey_here</ACCESS_KEY>
```

Save changes, and then start the Power Agent from the Power Agent’s bin folder by running the `./slagent start` script. Monitor startup progress from the console.

A successful startup message would look like the following in the console:

```
[root@edmfootprint ~]# /usr/local/sightline/sightlinePA/bin/slagent start
uid=0(root) gid=0(root) groups=0(root)
FRTLHOME is /usr/sightlinePA
Warning: TimeZone is not set in /etc/timezone
Removed agentmgr.log file
Removed datamgr.log file
Removed servd.log file
Removed protomgr.log file
Removed datamgr.Local.log log file
Removed slaaListener.log file
SightLine Agent Manager system started.
SightLine Service Daemon started.
SightLine Data Manager started.
SightLine Agent Administrator started.
```

2.2.4 Start the Assure UI

On your desktop, point your browser to `http://server_hostname:8080/edm`, where **server_hostname** is the computer name. The server's IP Address can be used in place of the server hostname. For example:

```
http://myserver:8080/edm
http://192.168.1.50:8080/edm
```

The login screen should appear. The default credentials are as follows:

Username: **admin**
Password: **admin**

Click **Login** to enter the configuration wizard; see *Chapter 3, Getting Started*, for information about the Assure startup wizard.

2.2.5 Upgrading Assure on a Linux System

The Assure upgrade process is similar to a clean installation, with the difference being the argument included when initiating the upgrade process. Note that the currently installed version of Assure does not have to be shutdown prior to the upgrade.

Once the latest Assure installation kit has been obtained and transferred to the target server, follow the following upgrade instructions:

Log in as root, or a user that has root privileges, and then change directory to `/usr/local`:

```
#cd /usr/local
```

Unzip the file and extract the contents of the tar file:

```
#gunzip assure_linux.tar.gz
#tar -xvf assure_linux.tar -o
```

This will create a `/usr/local/assure_linux_x.x` folder.

Change directory to `/usr/local/assure_linux_x.x`:

```
#cd /usr/local/assure_linux_x.x
```

Enter the following command, which will install Sightline Assure (you must be root or a user with root privileges to perform this step):

```
./assure.sh upgrade or sudo assure.sh upgrade (the latter command should be used by a non-root user with root privileges).
```

The command prompt will display the progress of the upgrade, and will notify the user once the upgrade is complete. Upon completion of the upgrade, log into the Assure UI and verify the version number at the bottom of the Main Dashboard page.

2.3 Installing the Assure Virtual Appliance on VMware



An AccessKey will be required to complete the installation. Contact your support representative for a valid AccessKey string.

2.3.1 Assure Appliance Hardware Specifications

Processor: 4 vCPU (Virtual Quad-Core)

Memory: 2 GB

Disk space: 175 GB (thin provisioned)

Assure Installation File Size: 50MB

Network Speed: 100 Mbit/second

During the installation process, Oracle Linux 7.1 will be installed as the operating system on the VMware guest. The default hostname is **sightline-assure**.

2.3.2 Installation Steps

Retrieve the current Sightline Assure Appliance (.ova file) from your Sightline software distributor.

Once downloaded, the .ova file can be deployed to an ESXi host using the vSphere client.

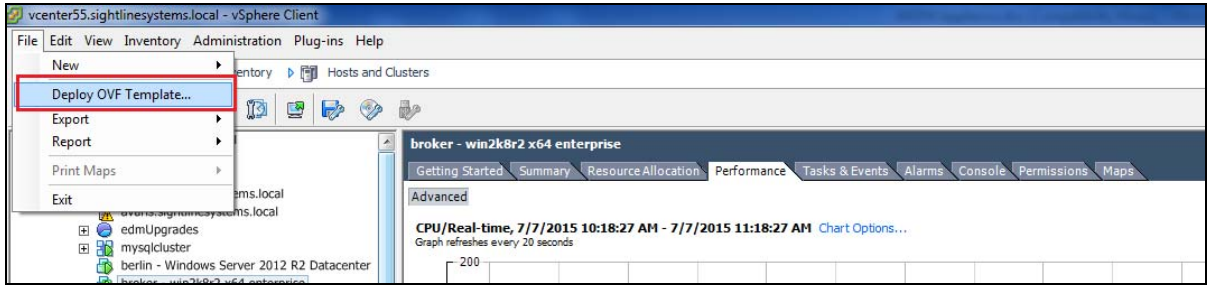


Figure 2-14. Deploying Sightline Assure Appliance

Navigate to the download location where the appliance file is stored. Click **Next**.

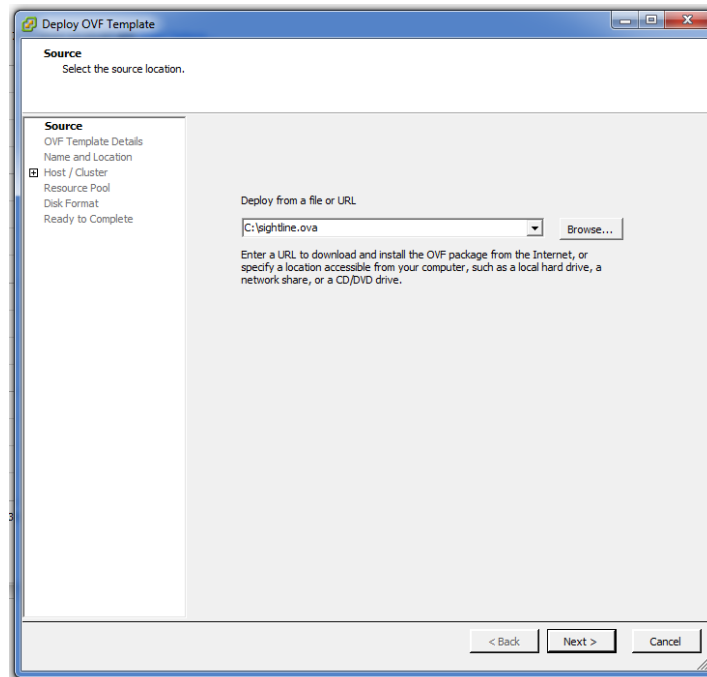


Figure 2-15. Browse to the Appliance File Location

The next screen is a summary of the appliance file. No action is required. Click **Next**.

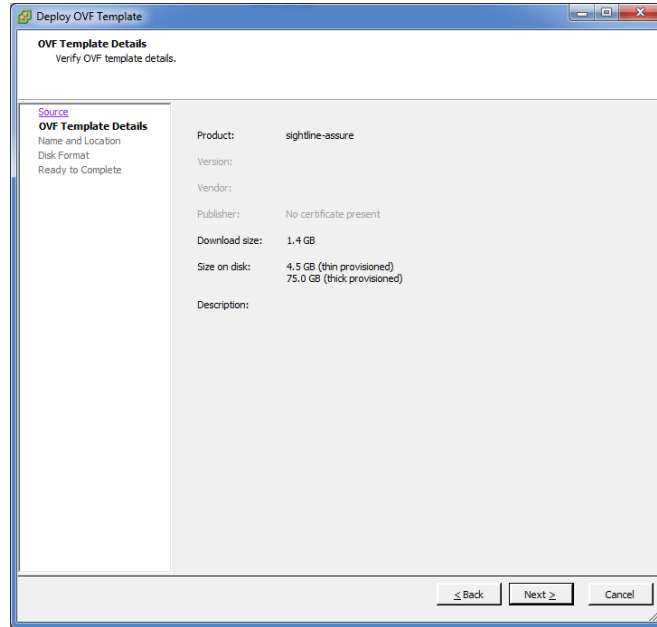


Figure 2-16. Verify Appliance Details.

The next screen allows the user to name the appliance. By default, the name **sightline-assure** is set. You can choose any name, although we recommend that you keep **sightline-assure** because there are other Assure settings that depend on this name.

Select the path to the `.ova` file. Click **Next**.

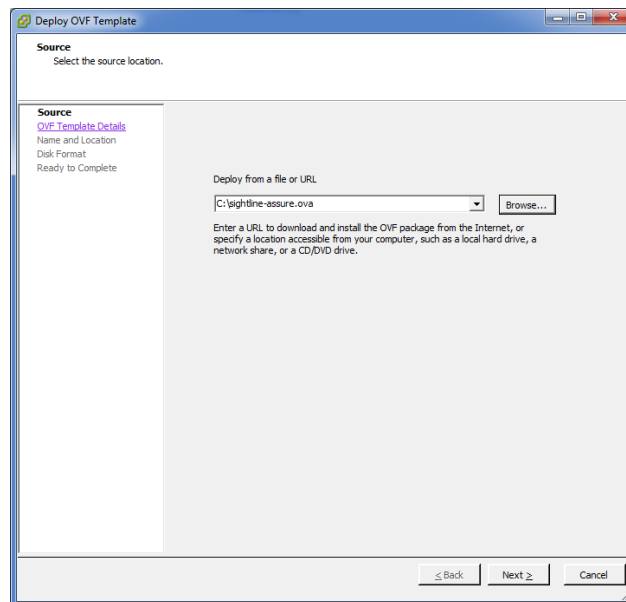


Figure 2-17. Appliance File Location

The next screen allows you to select a particular format to store the appliance's virtual disks. Once a particular format is selected, click **Next**.

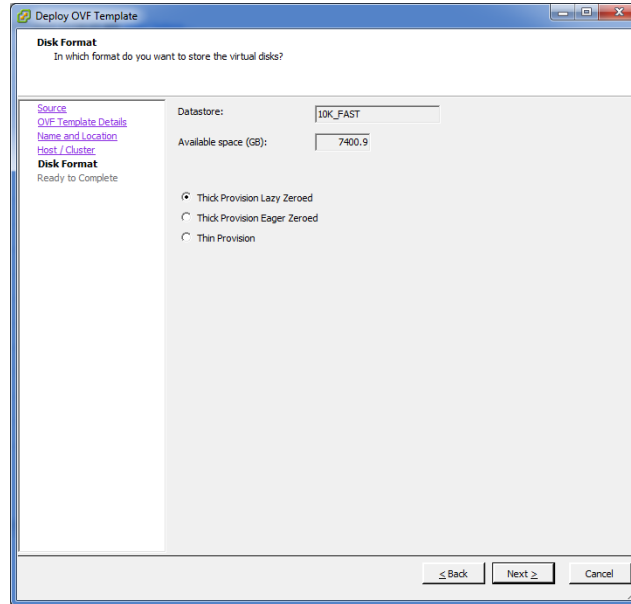


Figure 2-18. Selecting Disk Format

The final screen displays a summary of the input that was provided. If all information is satisfactory, click **Finish** to begin the deployment.

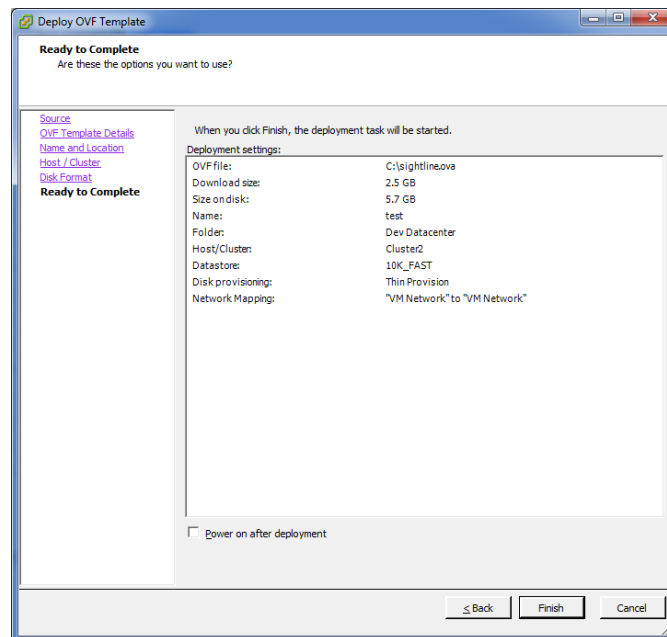


Figure 2-19. Summary of Assure Appliance

The appliance will begin to deploy to the designated ESXi host or cluster chosen during the appliance setup. Deployment can be monitored via the vSphere progress bar window.

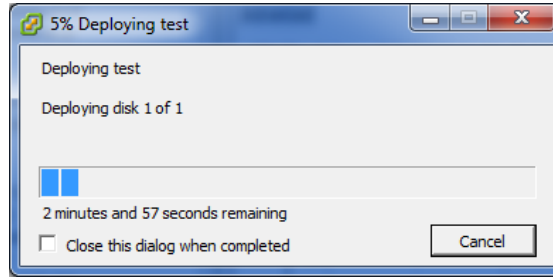


Figure 2-20. Deployment Status Window.

Close the deployment status window once the appliance has successfully deployed. The appliance should now be created under the selected host or cluster.

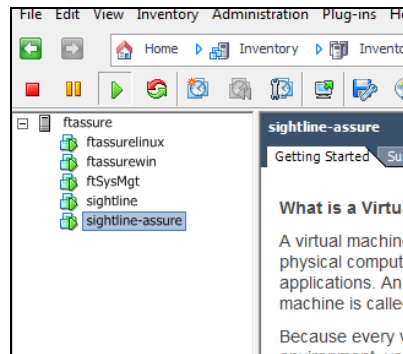


Figure 2-21. Appliance Created Under Selected Host or Cluster

Power on the appliance by right-clicking on the appliance name. Select **Power**, then **Power On**. The startup progress can be viewed from the vSphere console. Once the login prompt has been reached, Assure can be accessed via the web browser.

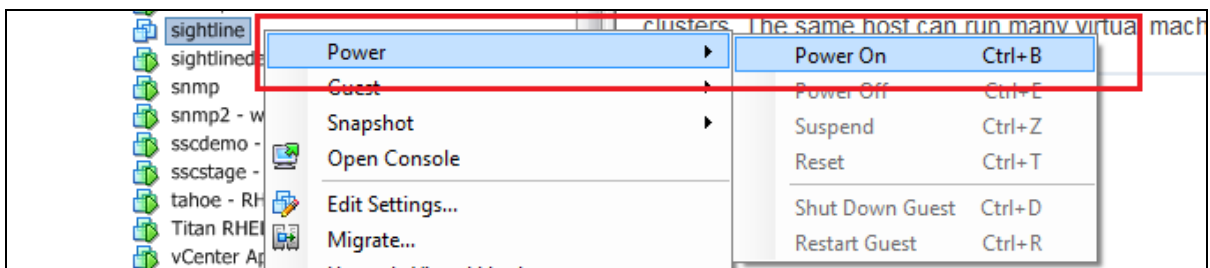


Figure 2-22. Powering on the Assure Appliance

The appliance network settings are configured for DHCP IP addressing, by default. The assigned IP address for the appliance is displayed on the same screen as the login prompt.

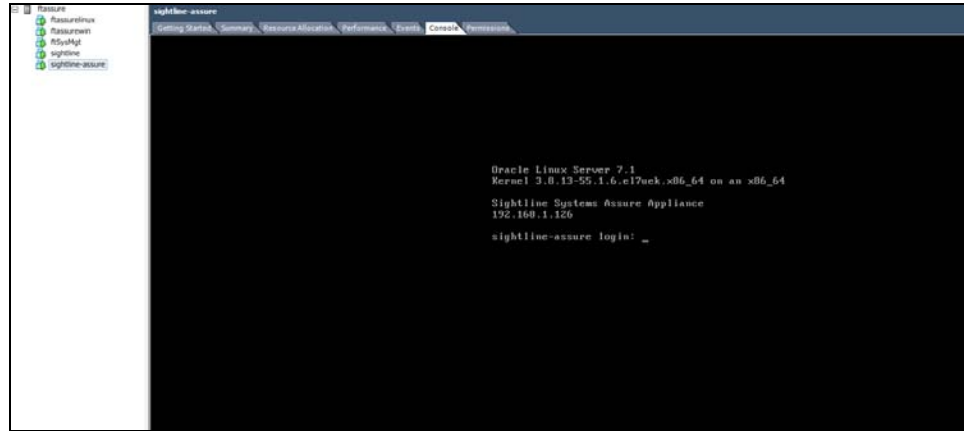


Figure 2-23. Appliance Login Prompt



If DHCP is not configured in your environment, see Section 2.3.3.1, *Configuring a Static IP Address*.

The assigned IP address or the hostname **sightline-assure** (if DNS is set on your network) can be used to access Assure via web browser. For example:

```
http://192.168.1.126:8080/edm  
http://sightline-assure:8080/edm
```

2.3.3 Post-Install Configuration (Optional)

2.3.3.1 Configuring a Static IP Address

The Sightline Assure appliance uses DHCP by default to obtain IP address. To assign a static IP address:

1. From the vSphere console, log into the **sightline-assure** guest as **root**:

Username: **root**

Password: **Sightline#1**

2. Run the network text graphical interface by entering the following command:

```
nmtui
```

3. A graphical network configuration screen should appear.



Figure 2-24. NetworkManager TUI (Text User Interface)

You can use either the **Tab** key or arrow keys to navigate. Select **Edit a connection**.

4. The next screen will present a list of all the available network interfaces. In Figure 2-25, only one interface is present, **ens160**

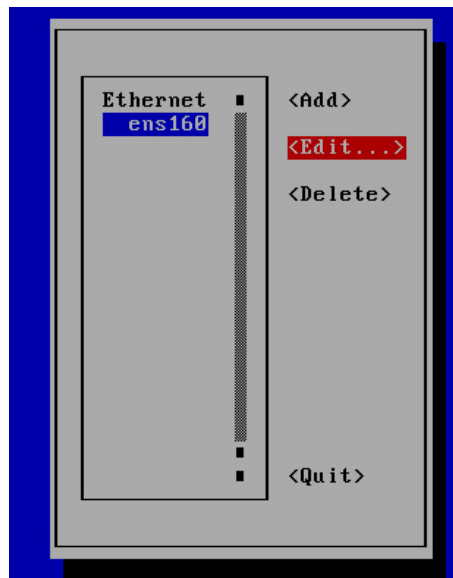


Figure 2-25. Network Interface Options

Select the **Edit** options and press **Enter**.

5. From the **Edit Connection** screen navigate to the **IPv4 CONFIGURATION** line, and select **<Automatic>**.

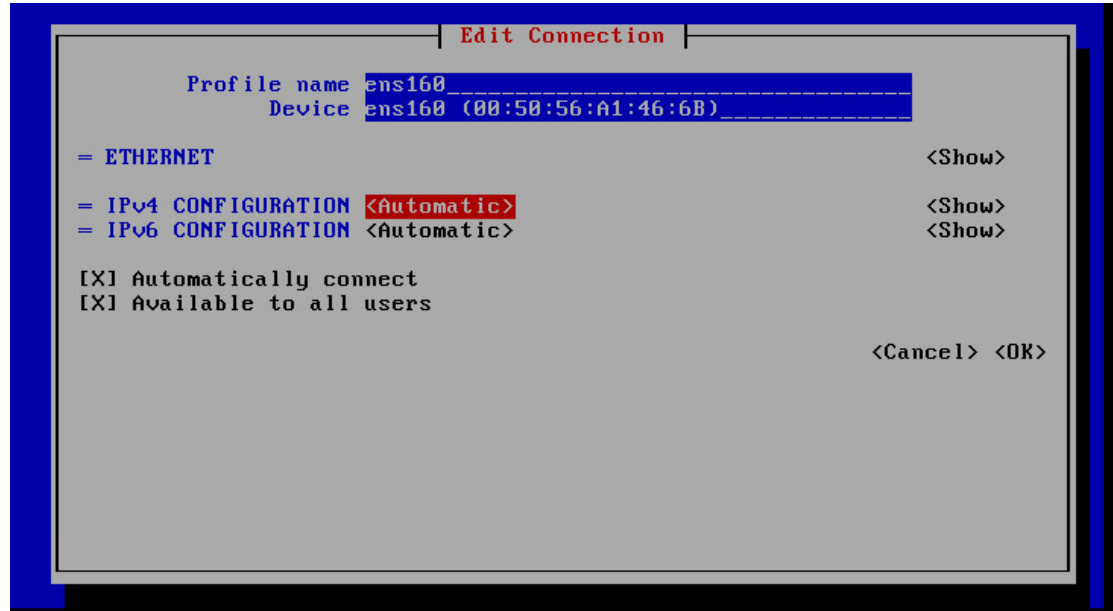


Figure 2-26. Edit Connection IPv4 Configuration

6. Select **Manual** from the list of configuration options, then select **Show**.

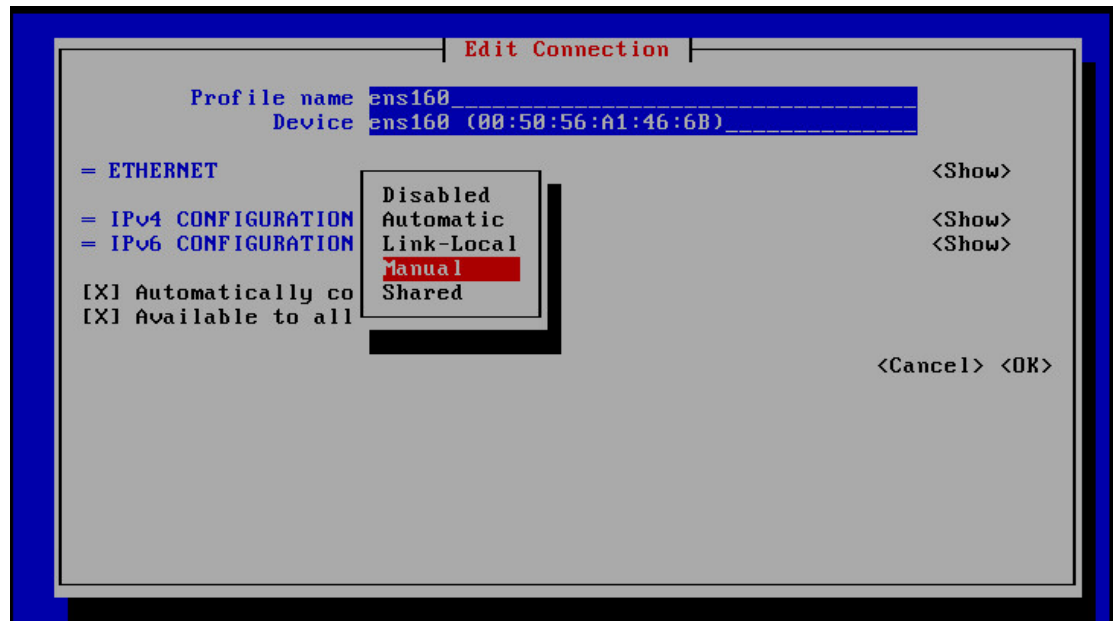


Figure 2-27. Manual Selection of IPv4 Configuration

7. The next screen presents a list of fields required to configure a static IP Address. Select **<Add>** to add a static IP address.

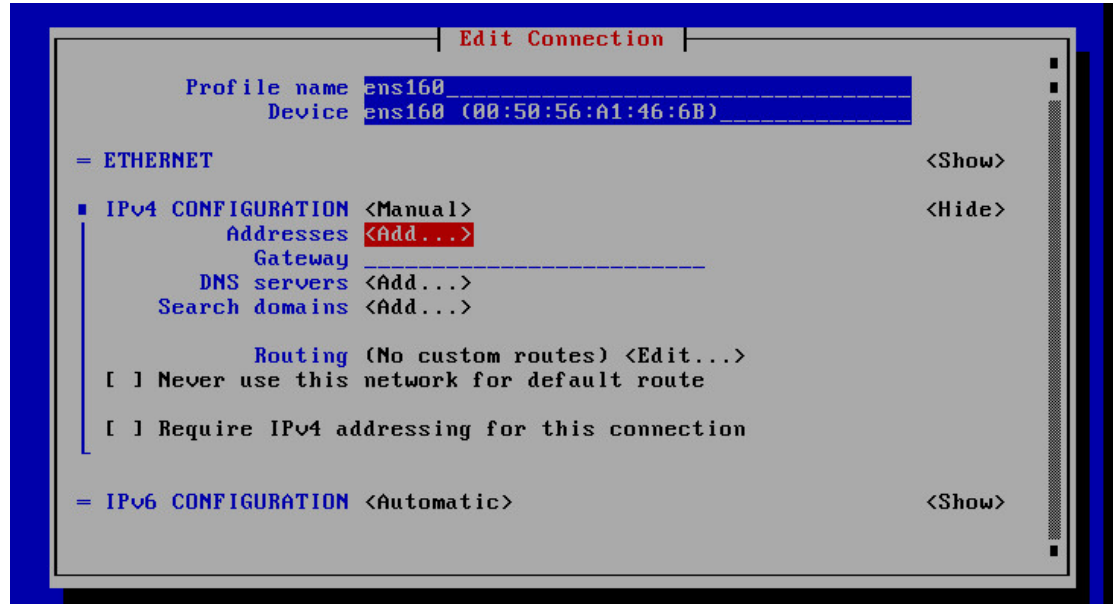


Figure 2-28. Manual IPv4 Configuration

Enter the following information:

- **IP Address**

Be sure to include the proper CIDR Prefix at the end of the IP address. The CIDR prefix is a different subnet mask format rather than the usual 255.x.x.x format. For example:

192.168.1.172/24

This format indicates an IP address tied to a subnet mask of 255.255.255.0.

Below are some common prefix values with their respective Subnet Masks:

255.255.255.255 = /32

255.255.255.0 = /24

255.255.0.0 = /16

If you are unsure about the correct prefix for your network, please contact your System Administrator.

- **Gateway**
- **DNS servers (if applicable)**
- **Search domains (if applicable)**

Automatically connect and **Available to all Users** are also available options. Sightline recommends keeping these options at their default values.

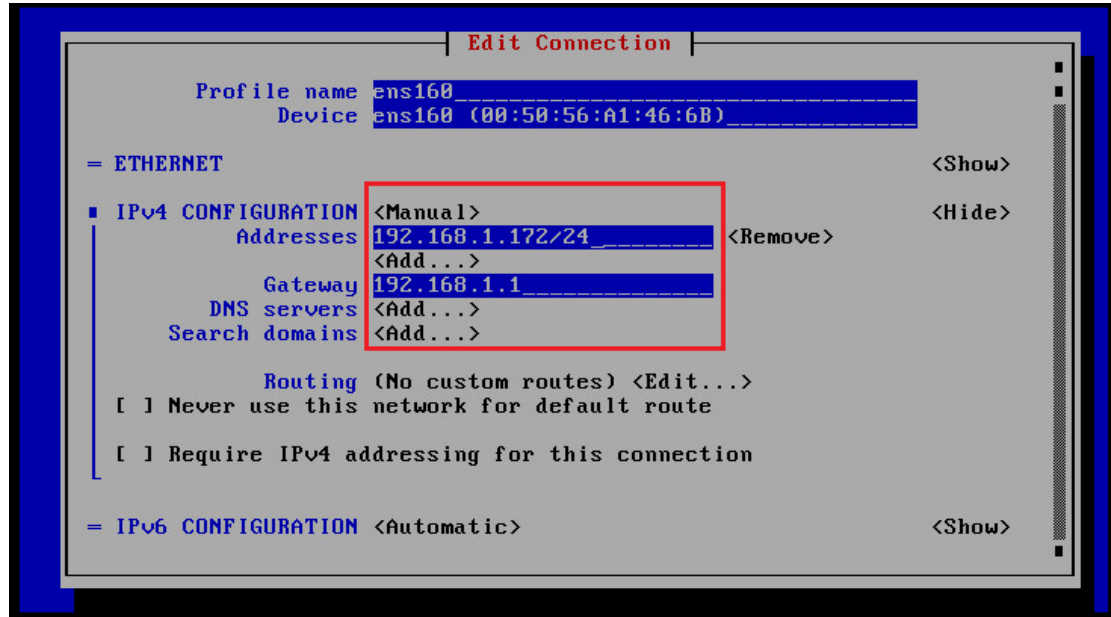


Figure 2-29. Manual IPv4 Configuration, continued.

Once all information and options have been set, select **OK**.

8. Select **Quit** from the Network Interface Screen.

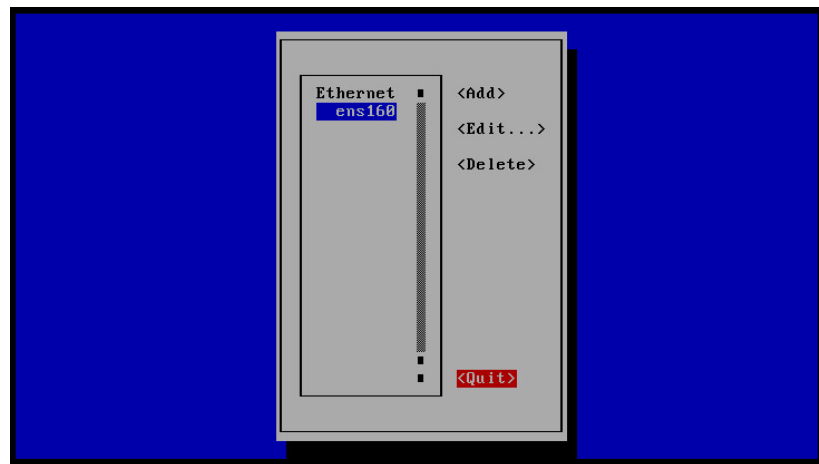


Figure 2-30. Quit Network Interface Screen.

9. When you are back at the command prompt, type the command `reboot`.
10. After the server has re-booted, verify from the login prompt that the static IP address has been set:

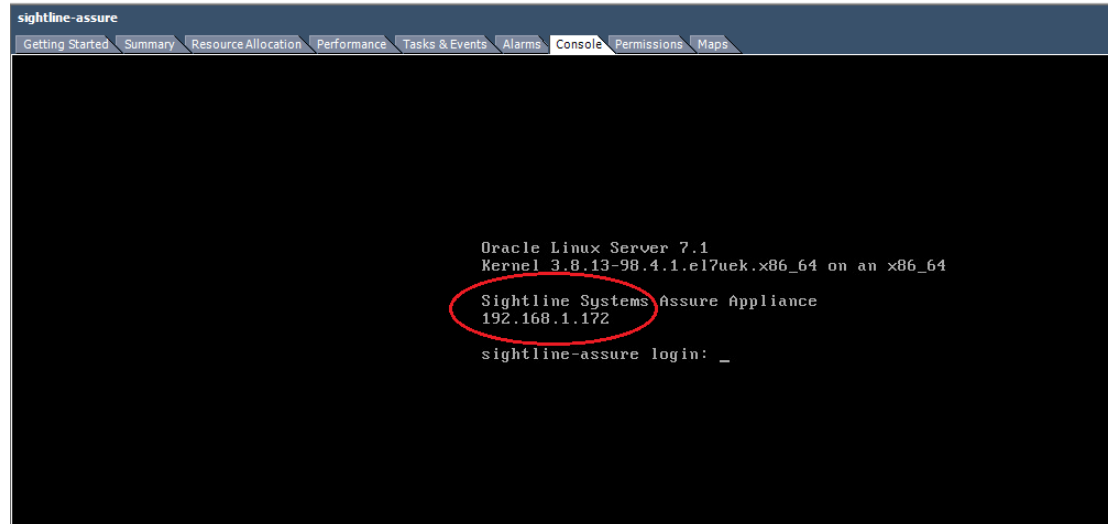


Figure 2-31. Static IP Address Verification.

Once network services are back up, the assigned static IP address or the hostname **sightline-assure** (if DNS is configured) can be used to access Assure via your web browser, using the following URLs:

`http://<static-IP-address>:8080/edm`

OR

<http://sightline-assure:8080/edm> <-- if DNS is configured.

2.3.3.2 Changing Time Zones

The Default Time Zone is set to EDT for the system clock. To change the time zone, copy the appropriate file from `/usr/share/zoneinfo` to `/etc/localtime`. For example:

```

#cd /usr/share/zoneinfo
#ls

Africa      Asia      Canada   Cuba     EST
America    Atlantic CET       EET     EST5EDT
Antarctica Australia Chile    Egypt   Etc
Arctic     Brazil   CST6CDT Eire     Europe ...

#cp /usr/share/zoneinfo/Europe/Riga /etc/localtime

```

2.3.4 Configuring the Sightline Power Agent

The appliance's Power Agent requires an AccessKey; use the AccessKey from your Assure implementation. There are three places you might refer to for the AccessKey string. Even if the strings are different, they should all be valid.

- If you received an email with the Assure AccessKey, then it will include the AccessKey string for the Power Agent.
- If you are running Assure in trial mode, then the AccessKey string will be shown in the **Additional Monitoring** dialog box; simply copy this string and use it during the Power Agent installation.



Figure 2-32. Additional Monitoring Dialog Box

- If you have entered an AccessKey string into your Assure implementation, the **Monitored Servers** section of the AccessKey string should be used for the Power Agent. Select **Settings | Update AccessKey** and make a note of the AccessKey string to the right of the **Monitored Servers** entry.

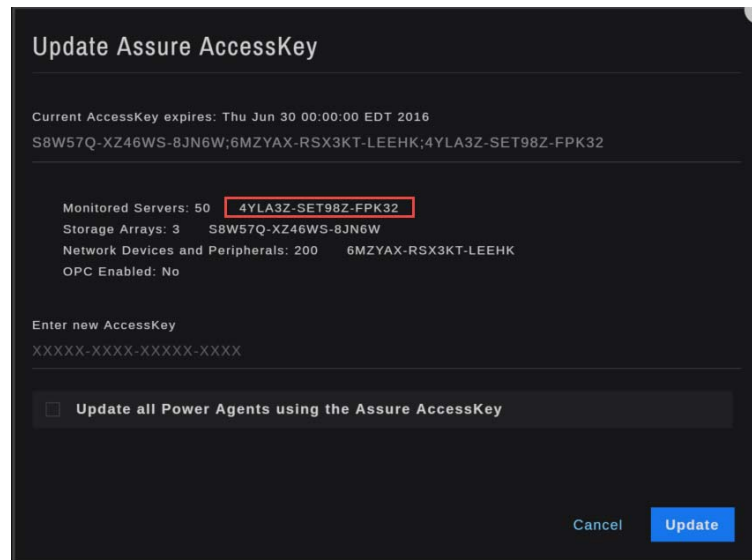


Figure 2-33. Update Assure AccessKey Dialog Box

Follow these instructions to apply the AccessKey to the appliance.

1. Log into the Assure server with the provided credentials above.
2. Navigate to the directory containing the Power Agent configuration file:

```
#cd /usr/local/sightline/SightlinePA/etc
#ls -l
```

3. Open the `agent.xml` configuration file:

```
#vi agent.xml
```

4. Locate the `<ACCESS_KEY>` tag, and update the AccessKey string:

```
<ACCESS_KEY>insert_access_key_here</ACCESS_KEY>
```

5. Save changes and exit the configuration file: press the **Esc** key, then type:

```
:wq
```

6. Start the Power Agent:

```
#!/etc/init.d/slagent start
uid=0(root) gid=0(root) groups=0(root),105(sfcb)
FRTLHOME is /usr/sightlinePA
Warning: TimeZone is not set in /etc/timezone
Removed agentmgr.log file
Removed datamgr.log file
Removed servd.log file
Removed protomgr.log file
Removed protomgr.LOGFILEEIA.log log file
Removed datamgr.LOGFILEEIA.log log file
Removed datamgr.Local.log log file
Removed slaaListener.log file
SightLine Agent Manager system started.
SightLine Service Daemon started.
SightLine Data Manager started.
SightLine Agent Administrator started.
```

7. Logout of the server console, and you're done:

```
#logout
```

2.4 Assure Communication Ports

The Assure installation process should open all of the ports required for its internal communication and communication to monitored objects. However, if a port cannot be opened, or if your Firewall/Antivirus software is installed or updated after the Sightline install, you may need to open ports manually. Table 2.1 lists Assure's required communication ports.

Table 2.1. Assure's required communication ports

Sightline Process/Purpose	Port/Program	Protocol	Notes
Servd	1645	TCP/UDP	
SLAA	30000	TCP	
Sightline callback port range	50000-51000	TCP	
HTTP	8080	TCP	
Assure Java	c:\Program Files\Assure \jre8\bin\java	N/A	Windows only

2.5 Uninstalling Assure

2.5.1 Uninstalling Assure on a Windows System

Uninstalling Assure can be performed by simply executing one command. The Uninstall will remove every component that was installed for use by Assure, including the PostgreSQL database, Java, the Sightline Power Agent, and Assure itself.



Do not use the Windows Control Panel UI option to uninstall the Assure software; not all of the Assure components will be completely removed from the system if this method is used.

Open a command prompt as Administrator and navigate to the directory where the Assure install directory resides:

```

Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd %userprofile%\Downloads
C:\Users\Administrator\Downloads>dir
Volume in drive C has no label.
Volume Serial Number is F81-2194

Directory of C:\Users\Administrator\Downloads
06/27/2016 11:00 AM <DIR> .
06/27/2016 11:00 AM <DIR> ..
06/27/2016 11:06 AM <DIR> assure_windows_2.0
06/27/2016 10:11 AM 537,681,722 assure_windows_2.0.zip
01/01/2016 11:07 AM 195,911,256 jdk-8u73-windows-x64.exe
04/06/2016 10:37 AM 4,283,848 npp-6.7.1_installer.exe
06/21/2016 10:25 AM 1,056 test.bat
4 File(s) 737,799,874 bytes
3 Dir(s) 143,254,269,952 bytes free
C:\Users\Administrator\Downloads>_

```

Figure 2-34. Navigate to Assure Installer Directory

Type following command to dive into the Assure install directory, and view the directory contents:

1. C:\>cd <path to Assure installer>\assure_windows_2.0
2. dir

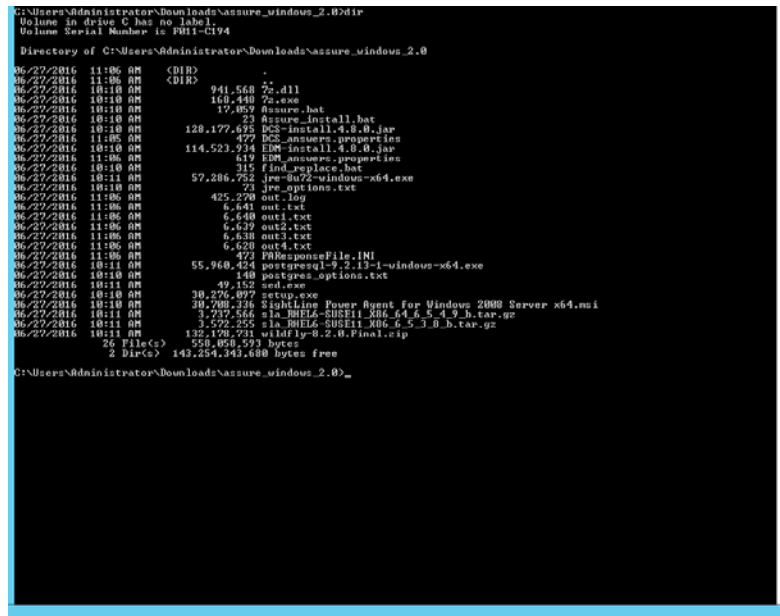


Figure 2-35. Contents of Assure Installer Directory.

Next, execute the following command to uninstall Assure:

```
C:\assure_windows_2.0>Assure.bat uninstall
```

This command will start the uninstall process, and progress can be viewed from the command prompt. The uninstall process should take approximately 1-2 minutes. An “operation completed” message at the end of the command prompt indicates that the uninstall was successfully completed.

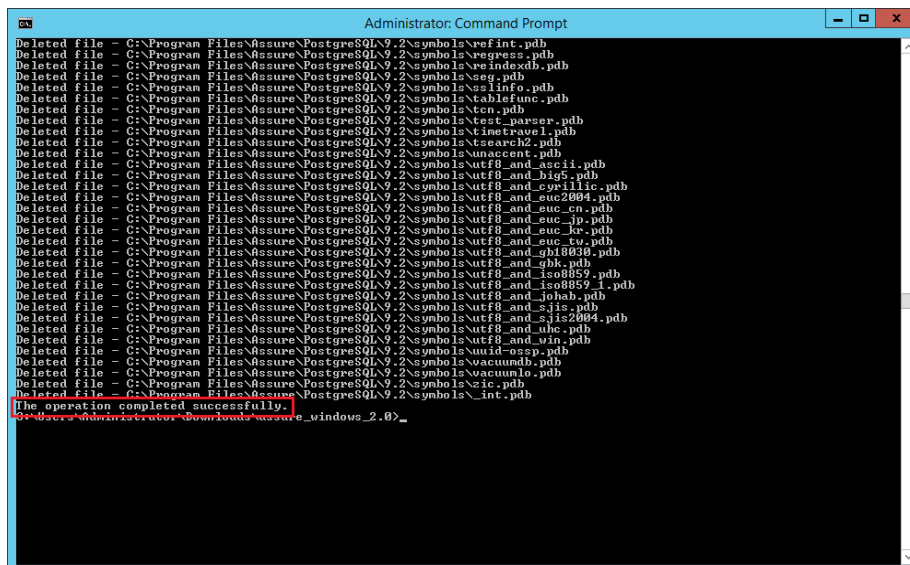


Figure 2-36. Successful Assure Windows Uninstall Message.

The Assure install has now complete, and the command prompt can be closed.

2.5.2 Uninstalling Assure on a Linux System

Uninstalling Assure can be performed by simply executing one command. The Uninstall will remove every component that was installed for use by Assure. The components include the PostgreSQL database, Java, the Sightline Power Agent, and Assure itself.

Open a command prompt to the Assure server, and navigate to the Assure install directory.

```
#cd /usr/local/assure_linux_2.0
```

From this directory, execute the following command to start the install:

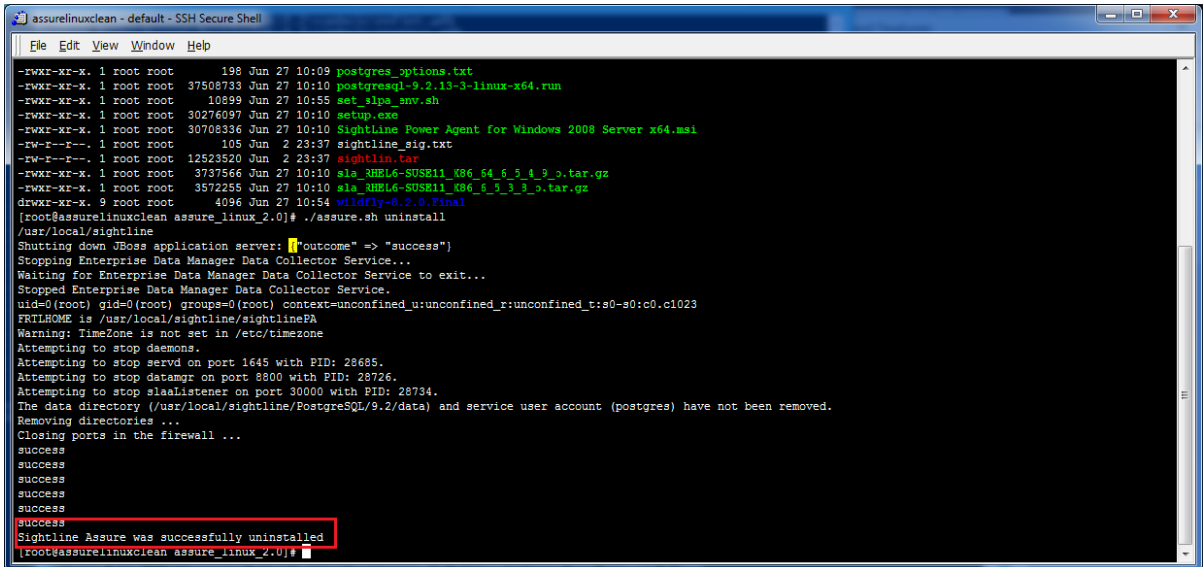
```
#!/./assure.sh uninstall
```

***Non-root users** can use the command below:

```
#sudo sh assure.sh uninstall
```

The above command will start the uninstall process, and progress can be viewed from the command prompt. The uninstall process should take approximately 1-2 minutes.

A message at the end of the command prompt will indicate that the uninstall was successfully completed.



```

assurelinuxclean - default - SSH Secure Shell
File Edit View Window Help
-rwxr-xr-x. 1 root root      198 Jun 27 10:09 postgres_options.txt
-rwxr-xr-x. 1 root root    37508733 Jun 27 10:10 postgresql-9.2.13-3-linux-x64.run
-rwxr-xr-x. 1 root root      10899 Jun 27 10:55 set_slpa_srv.sh
-rwxr-xr-x. 1 root root    30276097 Jun 27 10:10 setup.exe
-rwxr-xr-x. 1 root root    30708336 Jun 27 10:10 Sightline Power Agent for Windows 2008 Server x64.asi
-rw-r--r--. 1 root root      105 Jun 2 23:37 sightline_sig.txt
-rw-r--r--. 1 root root    12523520 Jun 2 23:37 sightlin.tar
-rwxr-xr-x. 1 root root     3737566 Jun 27 10:10 sla_RHEL6-SUSE11_486_64_6_3_3_3.tar.gz
-rwxr-xr-x. 1 root root     3572255 Jun 27 10:10 sla_RHEL6-SUSE11_486_6_3_3_3.tar.gz
-rwxr-xr-x. 9 root root      4096 Jun 27 10:54 wildfly-8.2.0.Final
[root@assurelinuxclean assure_linux_2.0]# ./assure.sh uninstall
/usr/local/sightline
Shutting down JBoss application server: [outcome] => "success"
Stopping Enterprise Data Manager Data Collector Service...
Waiting for Enterprise Data Manager Data Collector Service to exit...
Stopped Enterprise Data Manager Data Collector Service.
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
FRILHOME is /usr/local/sightline/sightlineFA
Warning: TimeZone is not set in /etc/timezone
Attempting to stop daemons.
Attempting to stop servd on port 1645 with PID: 28685.
Attempting to stop datamgr on port 8800 with PID: 28726.
Attempting to stop slaalister on port 30000 with PID: 28734.
The data directory (/usr/local/sightline/PostgreSQL/9.2/data) and service user account (postgres) have not been removed.
Removing directories ...
Closing ports in the firewall ...
success
success
success
success
success
Sightline Assure was successfully uninstalled
[root@assurelinuxclean assure_linux_2.0]#

```

Figure 2-37. Successful Assure Linux Uninstall Message

2.6 Assure Memory Allocation

The initial memory allocated to Assure during the installation process is based on an Assure implementation with fewer than five or six monitored objects (servers, devices, storage arrays, etc.). If you are monitoring more objects, or if Assure's UI response seems sluggish, you may need to allocate more memory to Assure.

There are two Assure processes that will need to be updated. The Data Collector Service (DCS), which performs data collection and storage, and EDM, which presents the Assure UI. After updating the configuration files, DCS and EDM will need to be restarted (see below for details).

2.6.1 Increasing Memory on Windows Systems

2.6.1.1 Update Memory for DCS

1. Log into the Windows system where Assure is installed as a user with administrator privileges.
2. Navigate to `c:\Program Files\Assure\dcs\conf`
3. Open the `wrapper.conf` file with any editor.
4. Locate the line (at about line 115) containing `wrapper.java.maxmemory`; it will look something like this:

```
# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=512
Increase the memory allocation by increasing the maxmemory setting:
```

```
# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=2048
```

5. Save the file and exit the editor.

2.6.1.2 Update Memory for EDM

1. Navigate to `c:\Program Files\Assure\Wildfly-8.2.0.Final\bin\`
2. Open the `standalone.conf.bat` file with any editor.
3. Locate the `set JAVA_OPTS` entry the `Xmx` parameter (at about line 50); it should look like this:

```
rem # JVM memory allocation pool parameters - modify as appropriate.
set JAVA_OPTS=%JAVA_OPTS% -DEDM -Xms256m -Xmx512m
                                -XX:+CMSClassUnloadingEnabled -XX:MaxPermSize=256m
```

4. Increase the memory allocation by increasing the **Xmx** setting:

```
rem # JVM memory allocation pool parameters - modify as appropriate.
set JAVA_OPTS=%JAVA_OPTS% -DEDM -Xms256m -Xmx2048m
                                -XX:+CMSClassUnloadingEnabled -XX:MaxPermSize=256m
```

5. Save the file and exit the editor.

2.6.1.3 Restart the Sightline Services

There are two services to be restarted: **Sightline DCS** and **Sightline EDM**.

1. Open the Services window (**Start | Administrative Tools | Services**).
2. Locate the **Sightline DCS** service. Click on the name to highlight it; the **Stop** and **Restart** links will appear. Click **Restart**.
3. . Click on the **Sightline EDM** service to highlight it; the **Stop** and **Restart** links will appear. Click **Restart**.
4. The Sightline EDM service may take a few minutes to restart. During this time, you may see a 404 error or the Wildfly page when you try to access Assure in your browser. Wait a few minute and try again.

2.6.2 Increasing Memory on Linux Systems

2.6.2.1 Update Memory for DCS

1. Log into the Linux system where Assure is installed as a user with administrator privileges.
2. Navigate to `/usr/local/sightline/dcs/conf`
3. Open the `wrapper.conf` file with any editor.
4. Locate the line (at about line 115) containing `wrapper.java.maxmemory`; it will look something like this:

```
# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=512
```

5. Increase the memory allocation by increasing the **maxmemory** setting:

```
# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=2048
```

6. Save the file and exit the editor.

2.6.2.2 Update Memory for EDM

1. Navigate to `/usr/local/sightline/wildfly-8.2.0.Final/bin/`
2. Open the `standalone.conf` file with any editor.
3. Locate the `set JAVA_OPTS` entry the `Xmx` parameter (at about line 50); it should look like this:

```
JAVA_OPTS="-DEDM -Xms256m -Xmx512m -XX:MaxPermSize=256m  
-Djava.net.preferIPv4Stack=true
```

4. Increase the memory allocation by increasing the `Xmx` setting:

```
JAVA_OPTS="-DEDM -Xms256m -Xmx2048m -XX:MaxPermSize=256m  
-Djava.net.preferIPv4Stack=true
```

5. Save the file and exit the editor.

2.6.2.3 Restart the Sightline daemons

There are two daemons to be restarted: **Sightline DCS** and **Sightline EDM**.

1. To restart DCS, enter:

```
/etc/init.d/DCS stop
```

followed by:

```
/etc/init.d/DCS start
```

2. To stop EDM, enter:

```
/etc/init.d/EDM stop
```

Wait until the results of `ps -ef | grep EDM` no longer show a process. It can take a few seconds for the Wildfly application server to shutdown fully.

3. To start EDM, enter:

```
/etc/init.d/EDM start
```

4. The Sightline EDM service may take a few minutes to restart. During this time, you may see a 404 error or the Wildfly page when you try to access Assure in your browser. Wait a few minute and try again.

Chapter 3

Getting Started with Sightline Assure

3.1 Accessing Assure through your Browser

Access to Sightline Assure is through a browser window. The URL takes the following format:

```
http://<hostname>:<port>/edm
```

By default, port 8080 is used for access to Assure. You can use either the hostname or IP address of the system running Assure.

```
http://sightline-assure:8080/edm  
http://10.10.1.100:8080/edm
```

3.2 Logging into Assure

The default **User Name / Password** combination when Assure is installed is `admin/admin`. You can update the password using the **Manage Users** settings, or create new users.

Supported Language options include English, Japanese and Spanish.

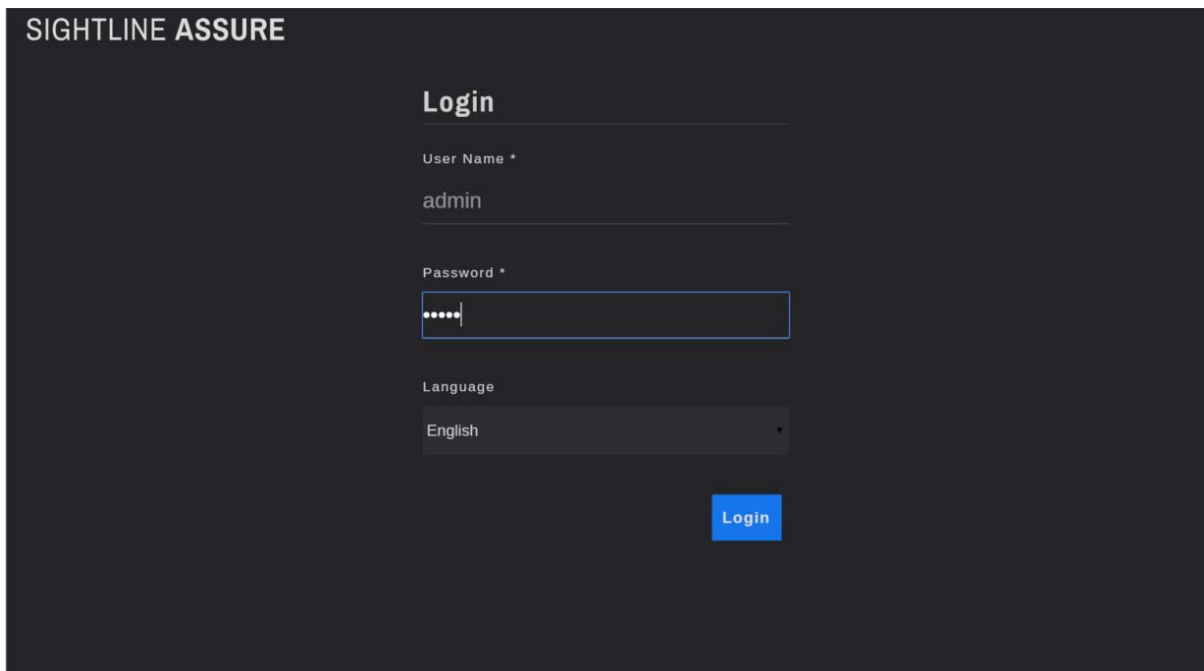


Figure 3-1. Assure Login Screen

3.3 Entering the AccessKey

The first time you start the Assure application, you'll be executing Assure in trial mode. Trial mode extends for 45 days from the first time that you log into Assure. You'll see the green Trial mode indicator at the top of the screen.

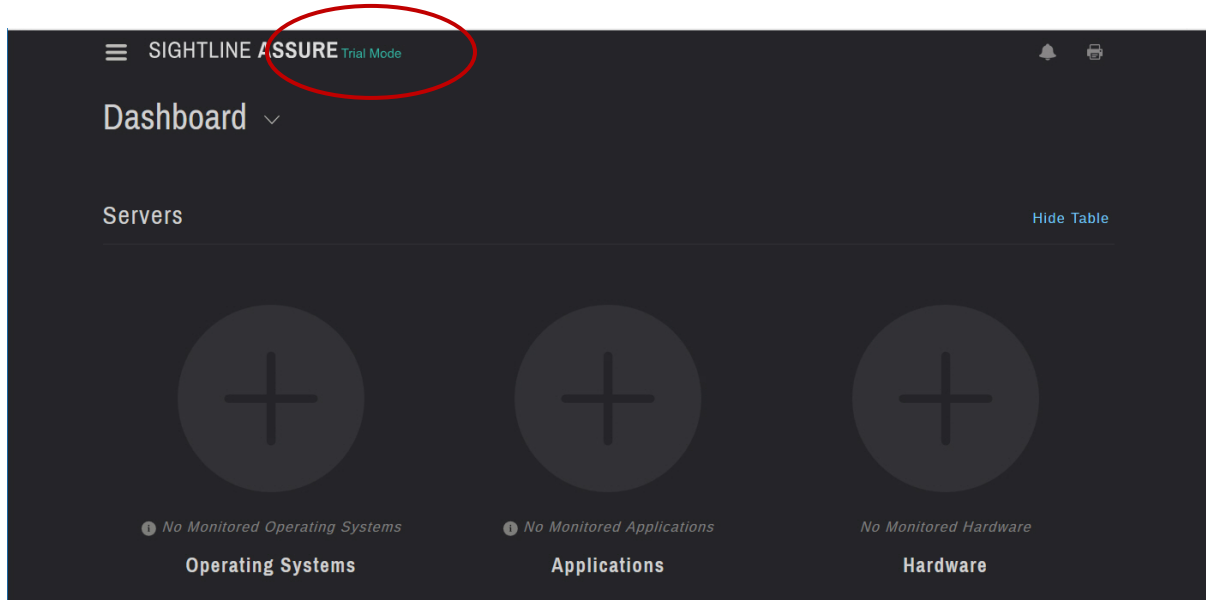


Figure 3-2. Assure running in Trial mode

At any time during the trial period, you can apply an AccessKey to license Assure (contact your Assure distributor to obtain the appropriate AccessKey string).

Click the menu icon at the top left of the window (the “hamburger” icon) to display the **Settings** menu, and select **Update AccessKey**. Enter your AccessKey string and click **Save**. You can cut-and-paste the AccessKey, but if you must enter it manually then type it exactly as it was provided to you, including capitalization and dashes. See also Section 5.6, *Update AccessKey*.

3.4 The Assure Setup Wizard

The first time that Sightline Assure is accessed via the browser, the **Setup Wizard** is run. The **Setup Wizard** has five screens, which solicit basic information for the Assure system. You can skip any screen and use the **Settings** menu to supply (or edit) the information at a later time.

If you don't complete the **Setup Wizard**, it will be opened the next time you access Assure.

The **Setup Wizard** begins with the **Welcome to Assure** screen.

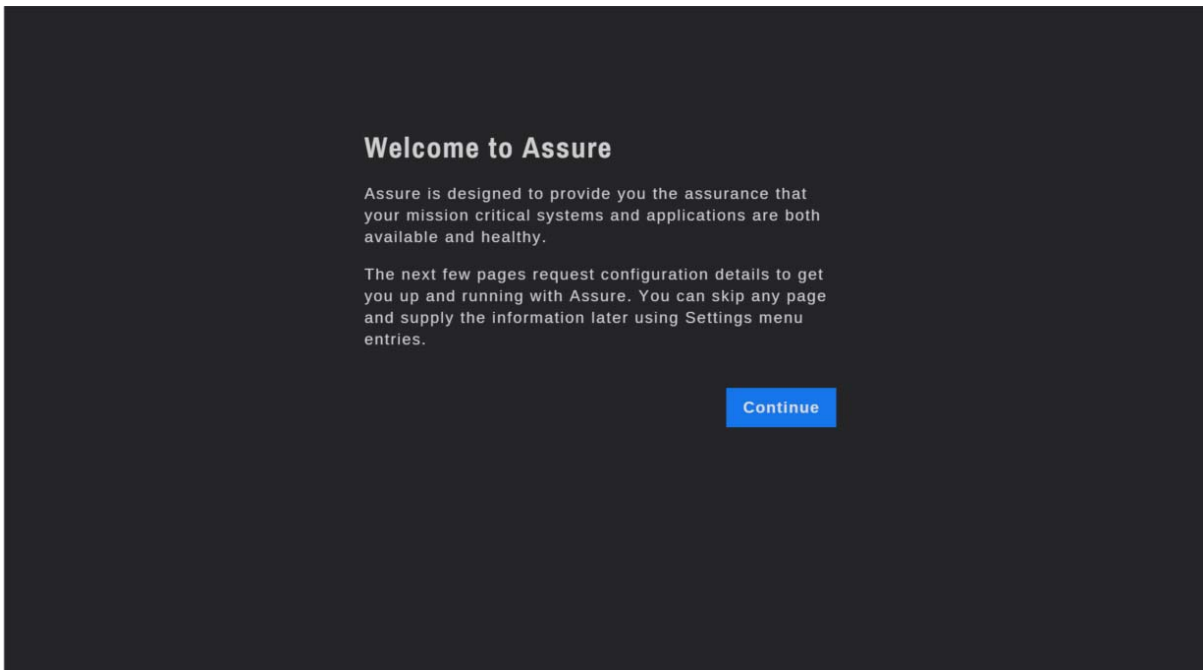


Figure 3-3. Welcome to Assure Screen

Click **Continue** to move to the **Add Server** screen.

The **Add Server** screen lets you provide the DNS name or IP address of a server to be monitored. This must be a physical system running a Windows or Linux operating system (also called bare-metal). For VMware systems, the root user and password will also be requested.

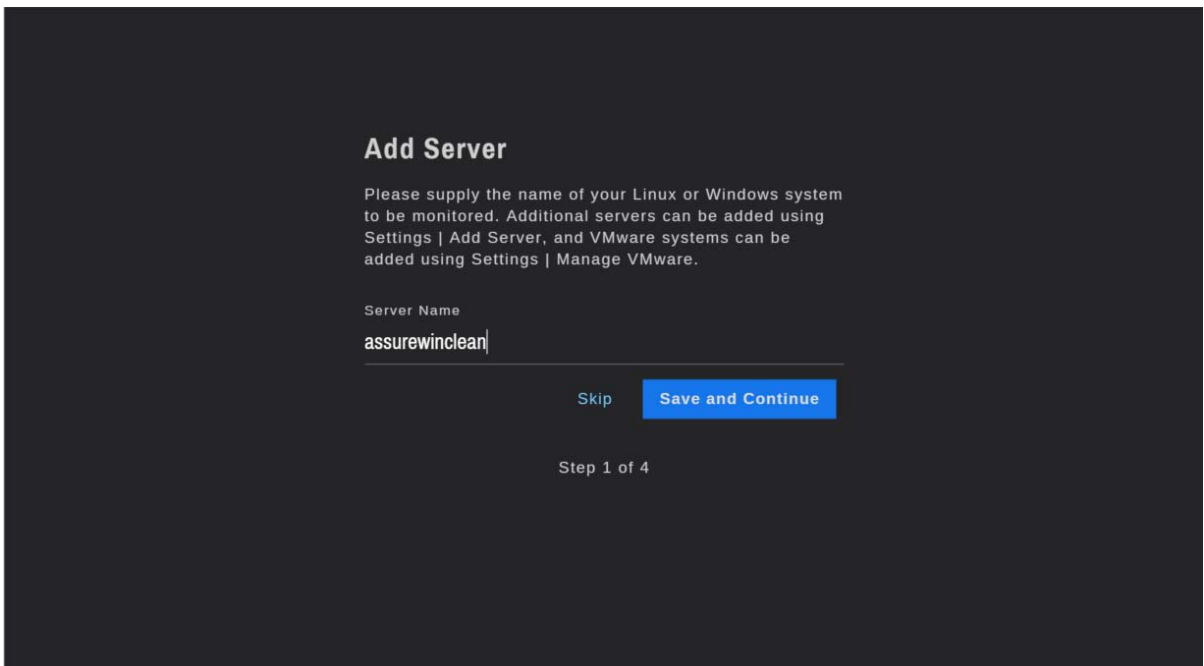


Figure 3-4. Add Server Screen

Click **Skip** to bypass this screen without providing the requested information. You can use **Settings | Add Server** to add the server to Assure at a later date.

To add the server to Assure at this time, enter the server name and then click **Save and Continue**. The **Email Server Settings** screen will be displayed (Figure 3-5).

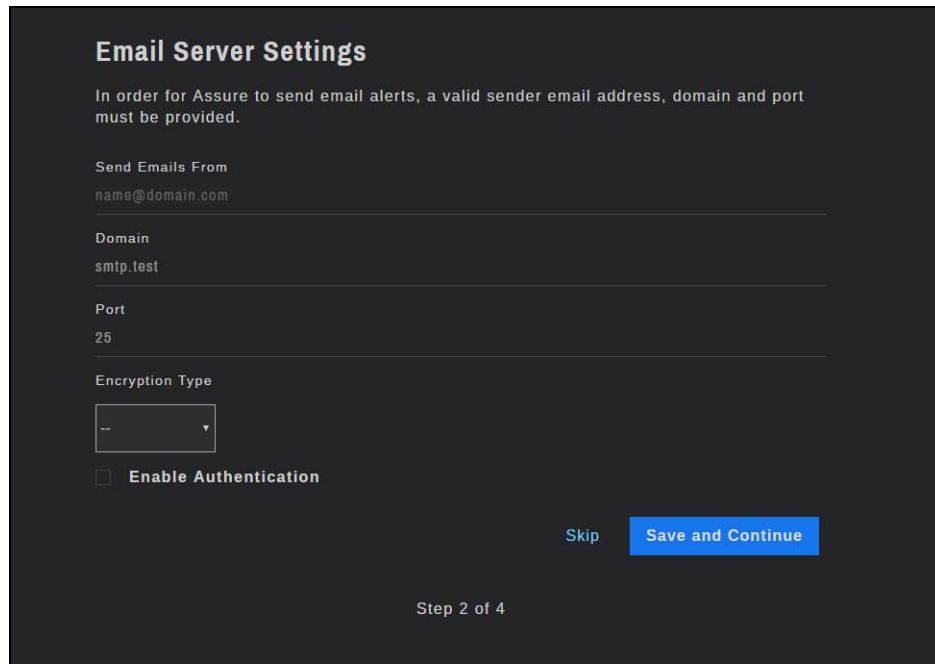


Figure 3-5. Email Server Settings Screen

As part of Assure’s alerting feature, emails can be sent to notify users when alerts or utilization thresholds violations occur. To send emails, an email server must be identified and a “sent from” email address must be provided.

In the **Send Emails From** entry, type the Assure sender email address. Depending on your email server, this address may not need to be a valid user, but it must appear in valid email format.

In the **Domain** entry, enter the name of the email server or domain.

Confirm the **Port** used for email.

Select an **Encryption Type** drop-down between **SSL**, **TLS** or **none**.

If your email system requires authentication, check **Enable Authentication** and then provide the requested username and password (Figure 3-6).

Email Server Settings

In order for Assure to send email alerts, a valid sender email address, domain and port must be provided.

Send Emails From
name@domain.com

Domain
smtp.test

Port
25

Encryption Type
SSL

Enable Authentication

User Name
User Name

Password

Re-enter Password

Skip **Save and Continue**

Figure 3-6. Email Settings – Enable Authentication Screen

You can click **Skip** to bypass this screen without providing the requested information. Use **Settings | Email Settings** to supply or update the email server information a later time.

Click **Save and Continue** if you have entered the information for your email server. The **Emails for Alerts** screen will be displayed (Figure 3-7).

As previously mentioned, Assure can send emails to configured users when alerts or utilization thresholds violations occur. There are four types of alerts: Assure system alerts, which occur when issues or errors happen on the Assure System; application alerts, which occur when a configured application (or a component of the application) is not active; operating system alerts, which reflect resource utilization issues in an operating system instance; and hardware alerts, which indicate problems with individual hardware components.

For each alert type, Assure will send an email to the email address(es) provided. Multiple emails can be entered, separated by commas. It is not necessary to provide email addresses for each alert type; if no email address is provided then Assure will not attempt to send an email. The alert, however, will be shown in the **Active Alerts** display for the system where it occurred.

Click **Skip** to bypass this screen without providing any email addresses. Use **Settings | Email Settings** to supply or update email addresses a later time. Click **Save and Continue** if you have entered an email address for one or more alert types.

The **Configure Scheduled Reports** screen will be displayed (Figure 3-8).

Emails for Alerts

For each alert type, provide email addresses to receive alert notifications.

Assure System Alerts
Any issues or errors that occur on the Assure System.
john.park@sightlinesystems.com

Application Alerts
Occur when specified processes or applications are not active.
inesystems.com, john.park@sightlinesystems.com

Operating System Alerts
Reflect resource utilization issues on individual OS instances.
debi.ray@sightlinesystems.com

Hardware Alerts
Include problems with individual hardware components.
name@domain.com

Skip **Save and Continue**

Step 3 of 4

Figure 3-7. Emails for Alerts Screen

Configure Scheduled Reports

Assure can send automated IT overview reports on a daily or weekly basis; overview reports provide a summary of any issues that occurred during the time period.

Daily Reports

Weekly Reports

Email Addresses (use commas to separate multiple email addresses)
name@domain.com, name@domain.com...

Skip **Save and Finish**

Step 4 of 4

Figure 3-8. Configure Scheduled Reports Screen

Assure also provides the option to deliver daily or weekly reports, which are summaries of the triggered alerts for the time period. Daily and weekly reports include a summary of all alerts for each system, for all three alert categories. Enter the email addresses for the scheduled reports;

You can click **Skip** to bypass this screen without providing the requested information, or click **Save and Finish** to complete the wizard even if this screen is blank. Use **Settings | Report Settings** to update the report selection and/or email addresses at a later time.

Chapter 4

Using Assure

This section describes the basic concepts behind using Assure and the Sightline Assure display. It outlines what information is provided by Assure and how the displays are related.

4.1 The Assure Dashboard

The **Assure Dashboard** is Assure's main page, and the first page that appears on the screen when you log into Assure. The Dashboard provides an at-a-glance overview of the status of your monitored systems. The top three circles represent the availability of your monitored operating system instances, applications and hardware. The three lower circles represent the availability of your monitored network devices, storage arrays and peripherals. To display more of the device details, you can use the **Hide Table** link to suppress the server table.

The intuitive Assure interface clearly conveys system status with three basic colors: **grey** (good), **yellow** (warning) and **red** (critical). The status of all systems is rolled up into the Dashboard, so that any issue can be investigated by clicking the links to the affected system. When an event does occur, the circle representing that component is updated, and the message describing the alert is listed in the Active Alerts table.

As an example, in Figure 4-1 there are 15 operating system instances being monitored. Although only five are listed, there actually more guest VMs on the **ftassure** VMware system and the **everRun** system. Between the 15 OS instances, there are 8 configured applications and for two of the systems hardware is being actively monitored.

When an alert is triggered, it's rolled up to the main dashboard for display; in this case you can see an application alert on a server called **jefferson**. You can see that there is one active Application alert; the alert details and system name are shown in the **Active Alerts** table. Click **View Details** to switch to the **Server Overview** page for that server, where you can see more details about the activity on the system.

At the top right of the screen, the bell icon is used to access notifications from the Assure system. Notifications may be generated when AccessKeys are expired or approaching their expiration date, or a new version of Assure is available. Expiration dates are checked at midnight for Assure and Power Agents on monitored systems.

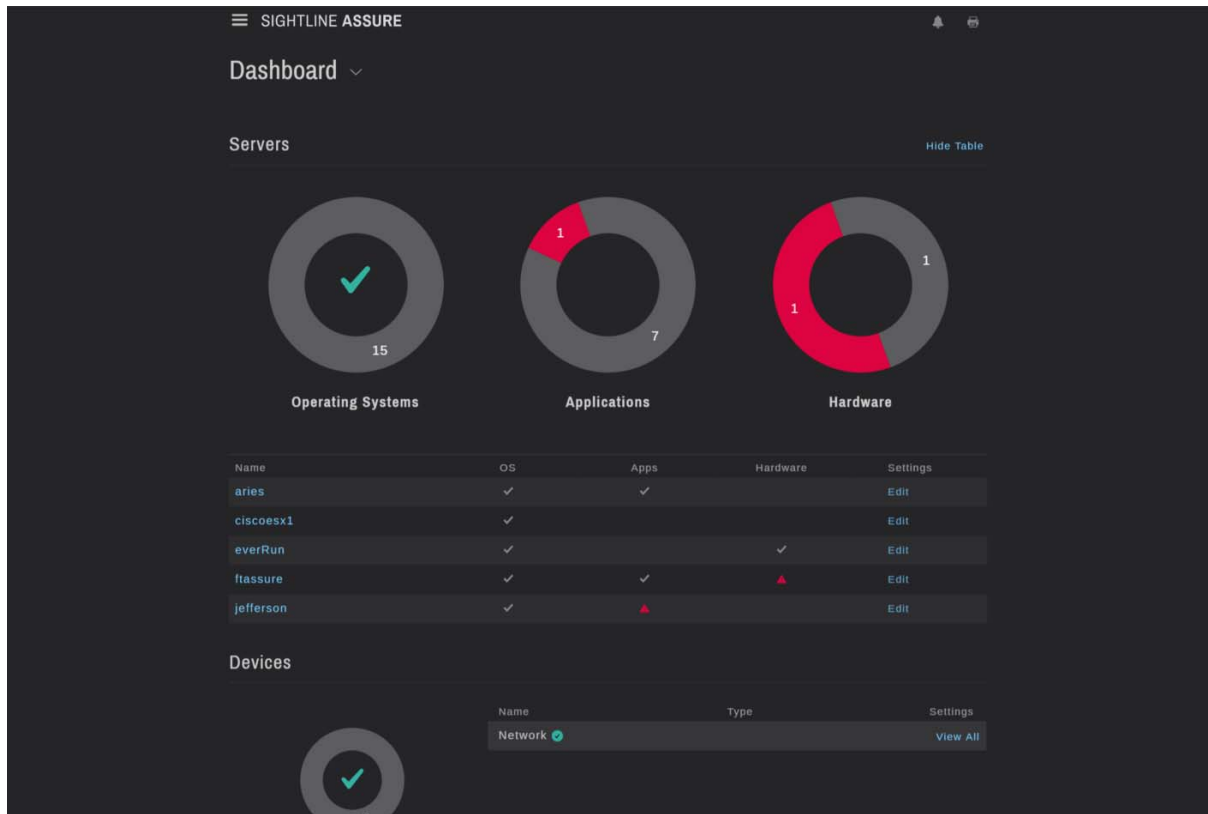


Figure 4-1. Assure Dashboard

4.2 Assure Server Overview Page

Assure provides an overview of the activity on any monitored system. The Main Dashboard includes a list of all monitored servers, both VMware servers and bare metal servers running Linux or Microsoft Windows. The server name is a link to the **System Overview** page for the server. To see the **System Overview** page for a VMware guest, navigate first to the **VMware Server Overview** page (see Section 4.1.2), and then to the **VMware Guest Overview** page.

At the top of any Assure display you'll see the Sightline Assure logo; click on the logo to return to the main Dashboard page. To the left of the logo is the menu icon; click here to display the Assure **Settings** menu.



To view icons when printing you may need to update your browser settings to print background images.

For Chrome, in the print preview window select the -> **More settings** -> **Options** -> **Background graphics** checkbox.

For IE 11, select the **Settings** -> **Print** -> **Page setup** -> **Print Background Colors and Images** checkbox.

For Firefox, select **File -> Page Setup -> Format & Options Tab -> Print Background** (colors & images).

There are four parts to the **System Overview** page: system health checks, monitored applications, alerts and charts.

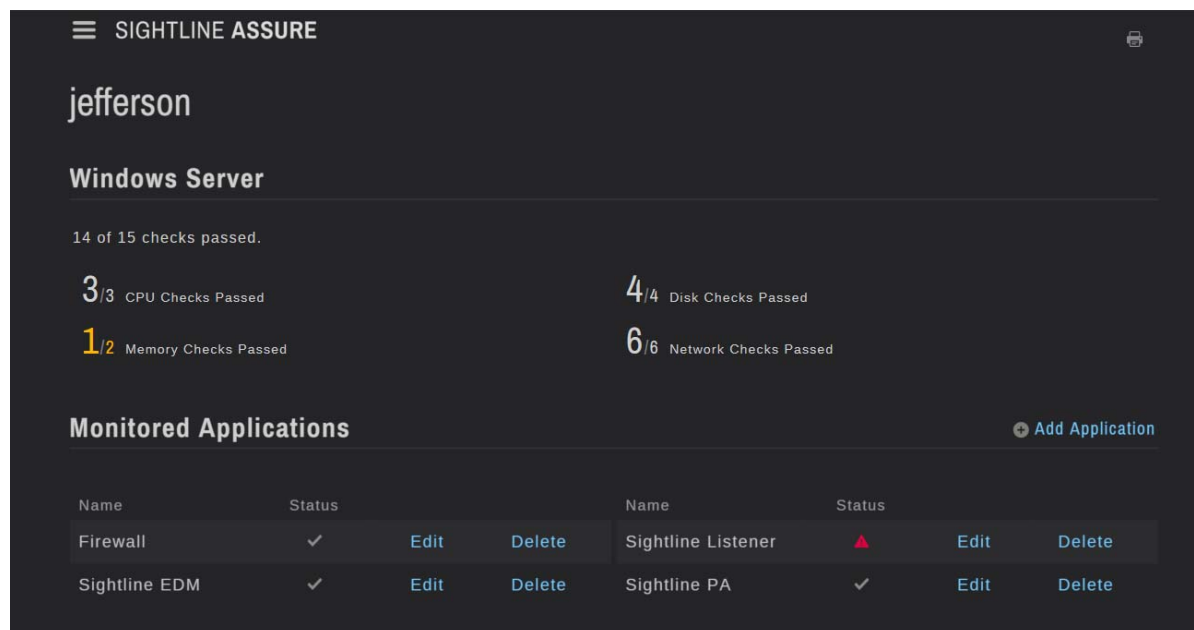


Figure 4-2. Monitored System Overview Page

4.2.1 System Health Checks

Health checks provide a summary of the health of the operating system instance. The section title indicates the operating system running on the server: Windows, Linux or VMware. Assure checks the four basic system resources: cpu, memory, disk and network. There are two or more checks for each resource, monitored every 20 or 30 seconds. If any utilization value exceeds its configured threshold level it will be noted in this section. Note that there may be both a caution threshold and a critical threshold for the same resource, where the caution alert is displayed in yellow and the critical alert is shown in red.

On **jefferson**, for example, the caution threshold for a disk check returned a utilization value that exceed the threshold, so only 1 of the 2 checks passed for the interval. The number 1 is shown in yellow, but would be red if a critical threshold was exceeded. In the event that multiple thresholds are exceeded, then the color of the more serious alert will be shown.

Note that the color of each section changes to blue when hovering. This is a link to the associated charts at the bottom of the page (see Section 4.2.4). For example, click on the **Disk** link to jump to the charts for disk utilization; this will provide more details about the disk usage and threshold settings.

4.2.2 Monitored Applications

Beneath the health checks for the system is the list of **Monitored Applications**. Applications on Windows systems can be either processes or ports; applications on Linux systems are based on ports. See Section 4.6 for a discussion on configuring applications.

You can see that **jefferson** has four applications configured and one of them, **Sightline Listener**, was not performing as expected. An application alert is always a critical alert, and you can see the red triangle beside the application name. In addition, you will see details about the alert in the **Active Alerts** section of the page.

4.2.3 Active Alerts and Alert History

Assure's powerful alerting capability includes customizable threshold settings for resource utilization on the monitored system as well as the ability to track applications and hardware availability. There are two sections on the **System Overview** page for tracking alerts: the **Active Alerts** table and the **Alert History** display (Figure 4-3).

The **Active Alerts** table includes an entry for any active alert on the monitored system. In Figure 4-3, you can see that there are two active alerts on **jefferson** – an OS alert (low disk space) and an application alert (a monitored process is not active). When OS alerts are reported, there will be a short description of the alert, but if you click the **Show More** link you'll see a more detailed explanation and potential remediation steps. You'll also see the duration of the alert, which would be the length of time that the utilization has been abnormal or the monitored application has been in active.

When the alert is no longer active, it will be removed from the **Active Alerts** table. For instance, when the Sightline Agent Administrator Listener service is restarted, the application will no longer be listed with an active alert.

The **Alert History** table shows alert history for the system. The four OS resources are listed first, followed by a line for each monitored application. By default, the last day (24 hours) is shown, but you can update to display to show the last week or month. In addition, you can limit the number of lines shown by selecting only the Windows OS alerts (because **jefferson** is a Windows system) or only the Application alerts.

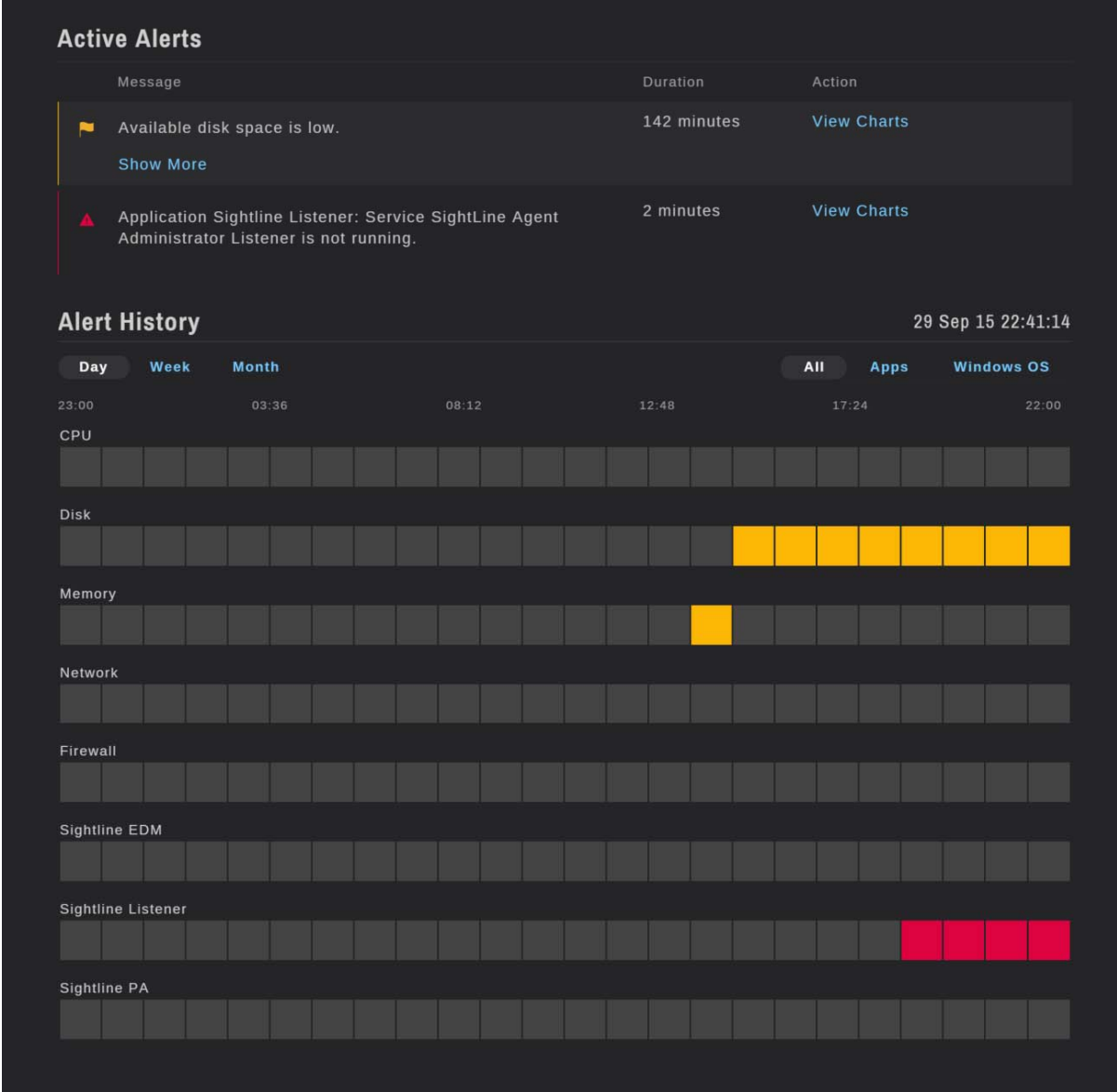


Figure 4-3. Active Alerts and Alert History

4.2.4 Utilization Charts

Several charts are provided in the **System Overview** to provide more information about the OS resource utilization on the system. You'll see at least one chart for each of the four resource areas (cpu, disk, memory and network).

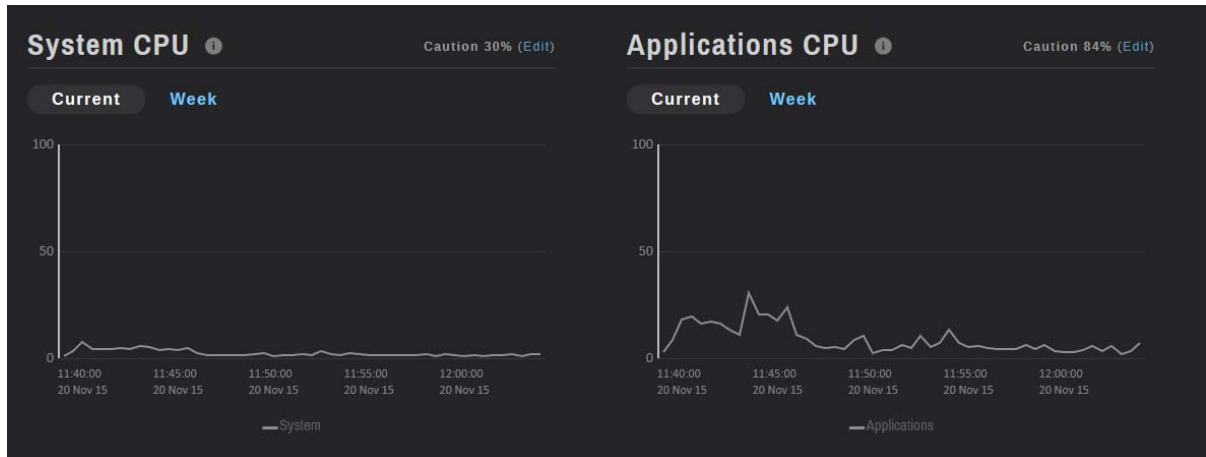


Figure 4-4. CPU Charts

By default, the current resource utilization is shown. In Figure 4-4, line charts show cpu utilization for the last several minutes. Click **Week** to change the display to a line or area chart of the last week's utilization. If there is not a week of data already collected, the chart will be populated as far back as the available data allows.

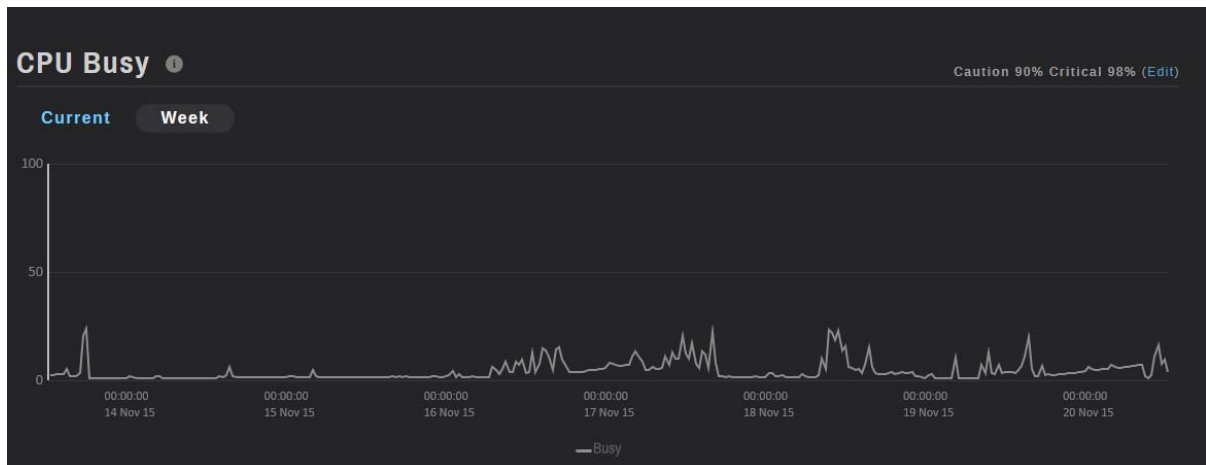


Figure 4-5. CPU Busy for the Last Week



You may occasionally see a yellow or red alert indicator on a chart, but no alert email has been generated. This is because some alerts are based on more active metrics, and wait for a slightly longer period before generating the email.

In all charts you will the current setting of any caution (yellow) or critical (red) thresholds in the top right corner of the chart. In the **Disk Space Used** chart, notice that the indicator for C is yellow, and crosses the threshold line at 90%. This matches the active alert for disk space in the **Active Alerts** table.

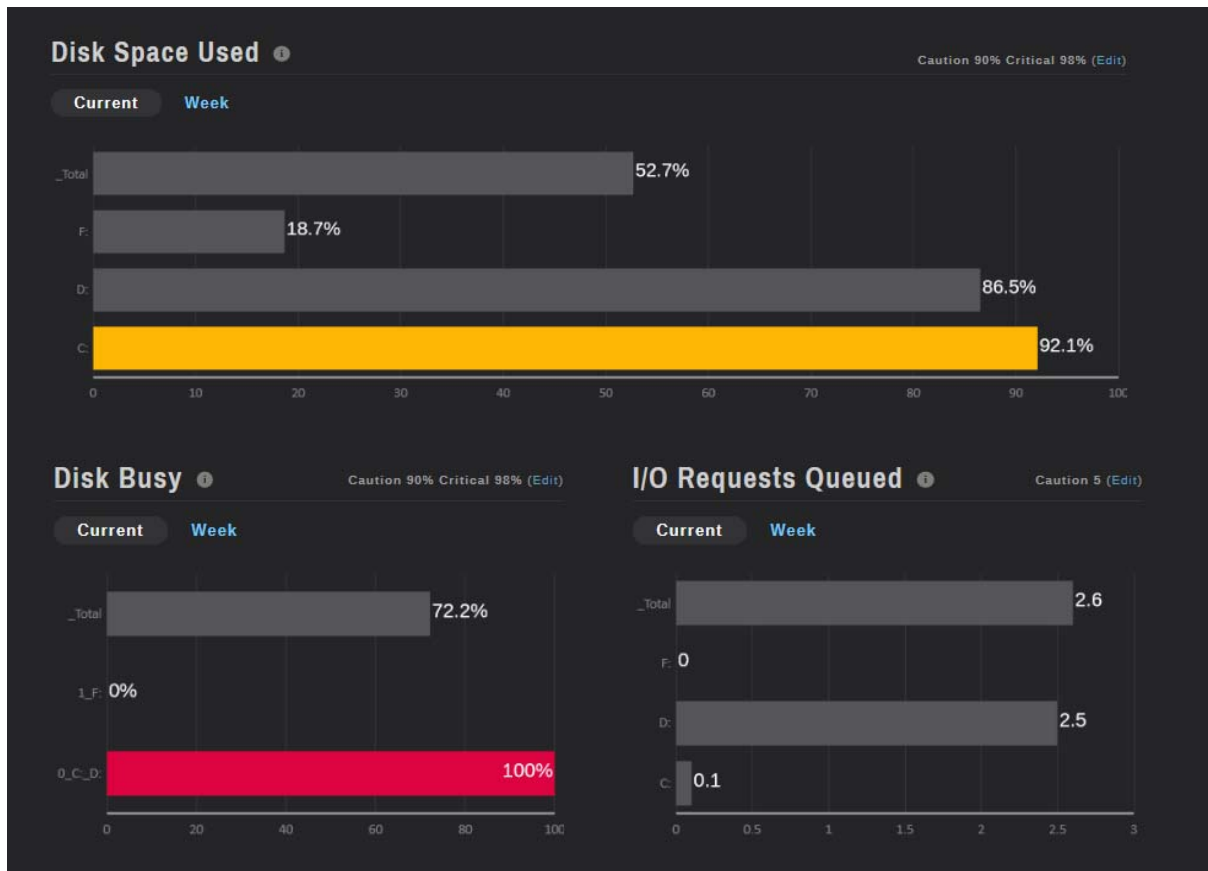


Figure 4-6. Disk Utilization Charts



In Assure, **Bar** charts display up to 10 metrics from a particular resource.

You'll also see an **Edit** link on each chart. **Edit** is used to change the value of the thresholds indicated in the chart. Click **Edit** to display the **Threshold Details** dialog for the chart. As an example, the current threshold values for **Disk Space Used** are 98% for critical and 90% for caution. These are indicated by the red triangle and yellow flag icons in the **Threshold Details** dialog (Figure 4-7).

To change a threshold value, click on the number itself and then update it with the new number. Click **Save**. Threshold values are applied to all servers in the environment, and a reminder will be shown. To save the updated value, click **Yes**, otherwise click **No**. The new threshold setting will take effect immediately.

Refresh can be found in the top right corner of the header. It is used to refresh the chart display; the chart is not automatically updated because this often interferes with analysis efforts. Rather, the data values shown in the chart are not updated unless you specifically refresh the chart.

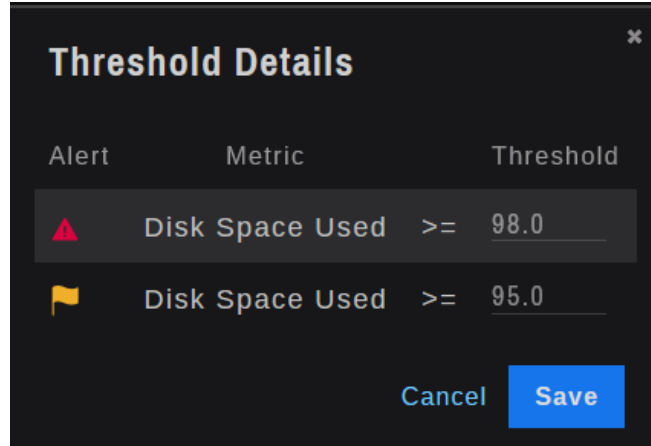


Figure 4-7. Threshold Details Dialog

In some instances values are represented by text charts, as you see in the memory and network charts. Text values are used when values for a specific resource vary widely or remain at zero.

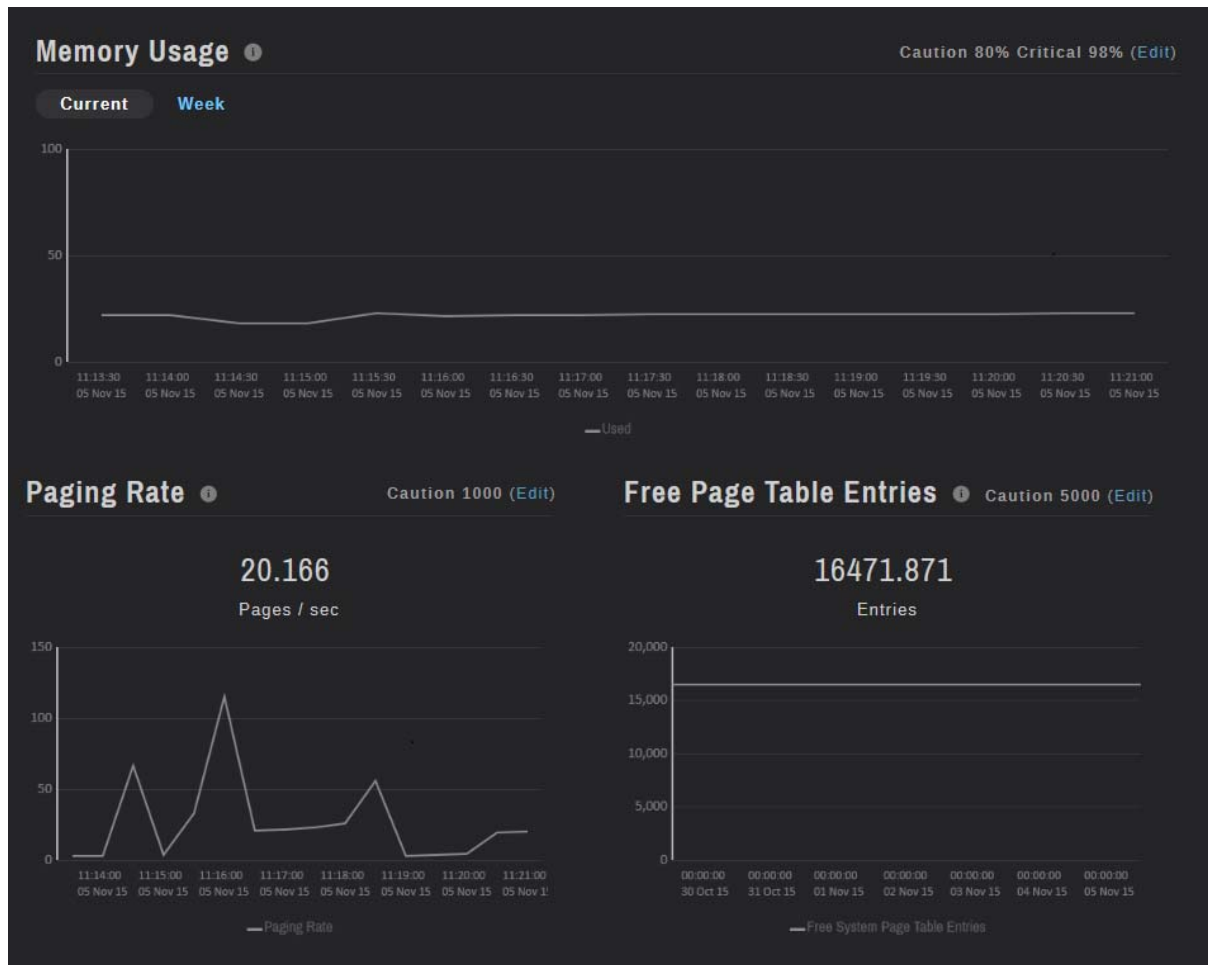


Figure 4-8. Memory Utilization Charts

In the memory paging charts, one metric is represented. The current value is shown in text, and values for the previous day or week are shown in the line chart below it. Another good example of zero values is the **Network Errors** chart for Windows systems. Because these counters are expected to be zero or very low, they would not be well represented in a graphical display.

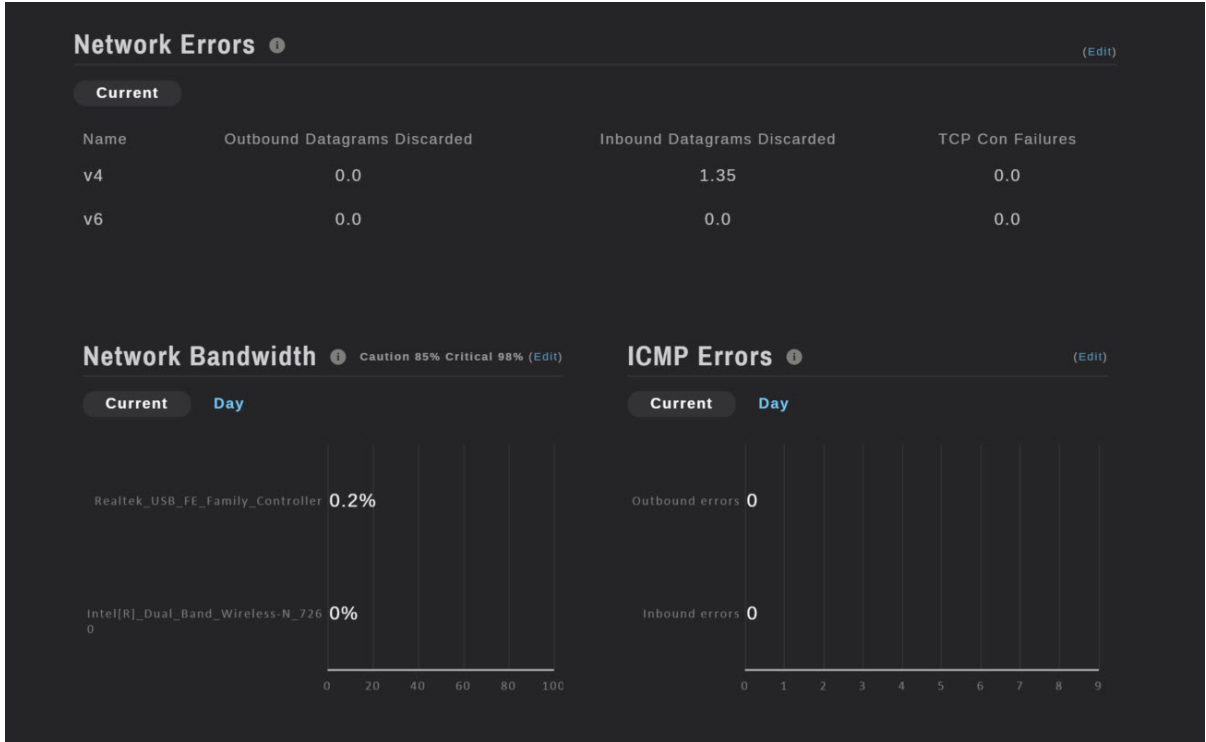


Figure 4-9. Network Utilization Charts

Because there are multiple metrics in the chart, switching to the Weekly view expands the chart to a table showing a summary of alerts for each day, where the icon represents the most critical alert that occurred on that day. A day with no alerts has a gray check mark, caution errors on a day result in a yellow flag, and any day when a critical alert occurred will have a red triangle.

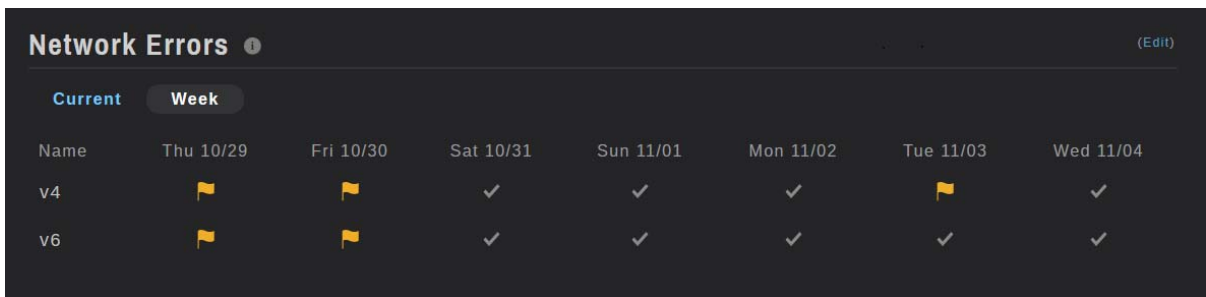


Figure 4-10. Weekly View of Network Errors Chart

4.3 VMware Host Overview Page

The **VMware Host Overview** page is similar to the **Server Overview** page. The page includes all of the same information for System Health Checks, Active Alerts and Alert History, and Charts. However, note that VMware hosts do not have applications; rather, they have guest VMs, or virtual machines.

The **VMware Host Overview** page also includes a section representing its guest VMs, shown in Figure 4-11. For each **Guest** there is an indicator representing the health of the VM's applications and operating system instance. The Guest name is also a link to the **System Overview** for that guest's OS instance.

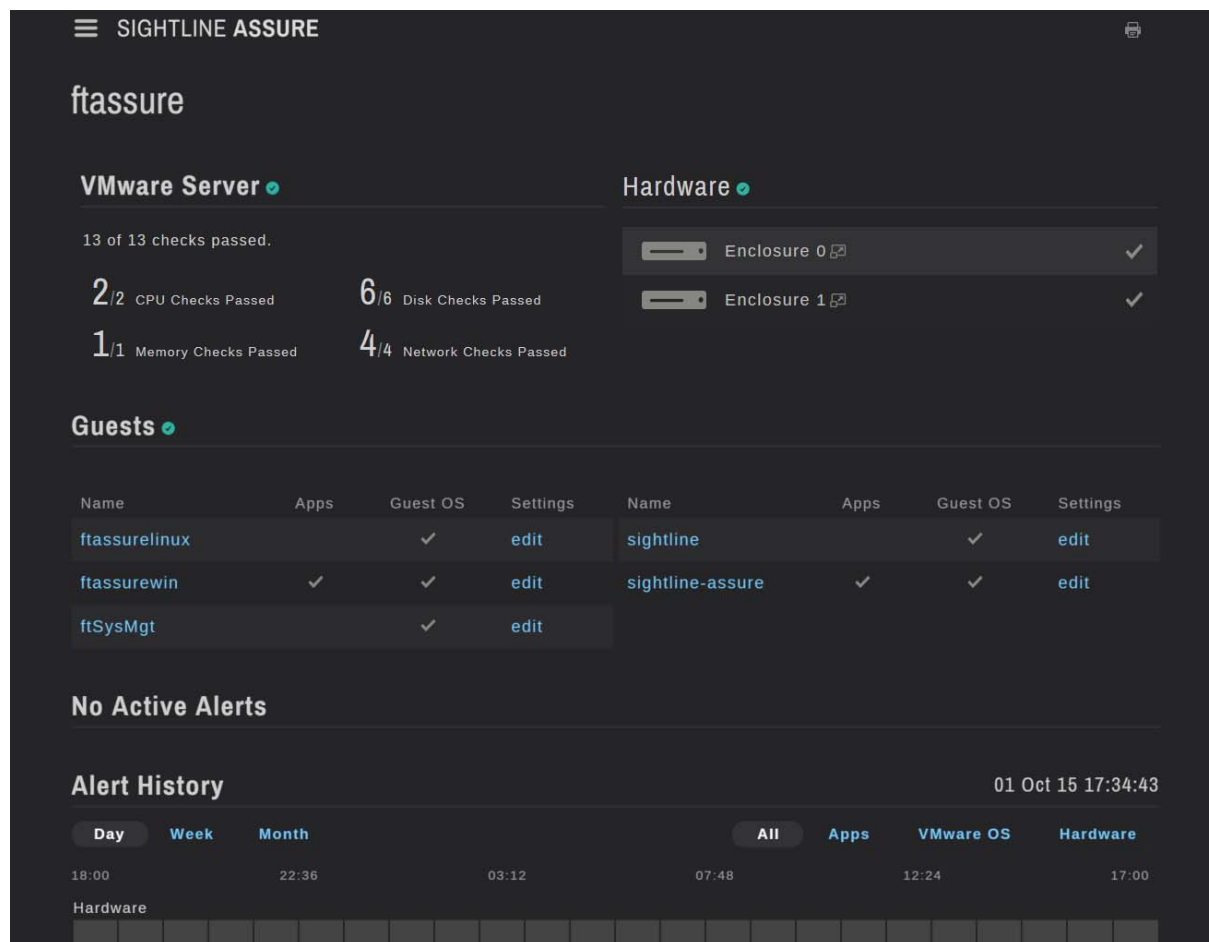


Figure 4-11. Network Utilization Charts

Note that the **System Health Checks, Alerts** and **Charts** represent the activity on the VMware host itself, not its guests.

Another section on the VMware page is the **Hardware** health. This section represents the two enclosures on the ftServer system and will turn either yellow or red if any hardware alerts are reported such as a network card not available.

4.4 System Overview Page for a VMware Guest

The **System Overview** page for a VMware guest is very similar to the **System Overview** page for a Windows or Linux operating system instance on a bare metal server. The main difference is the identification of the server at the top of the screen – you’ll see the system name, but also the name of the VMware server where it resides.

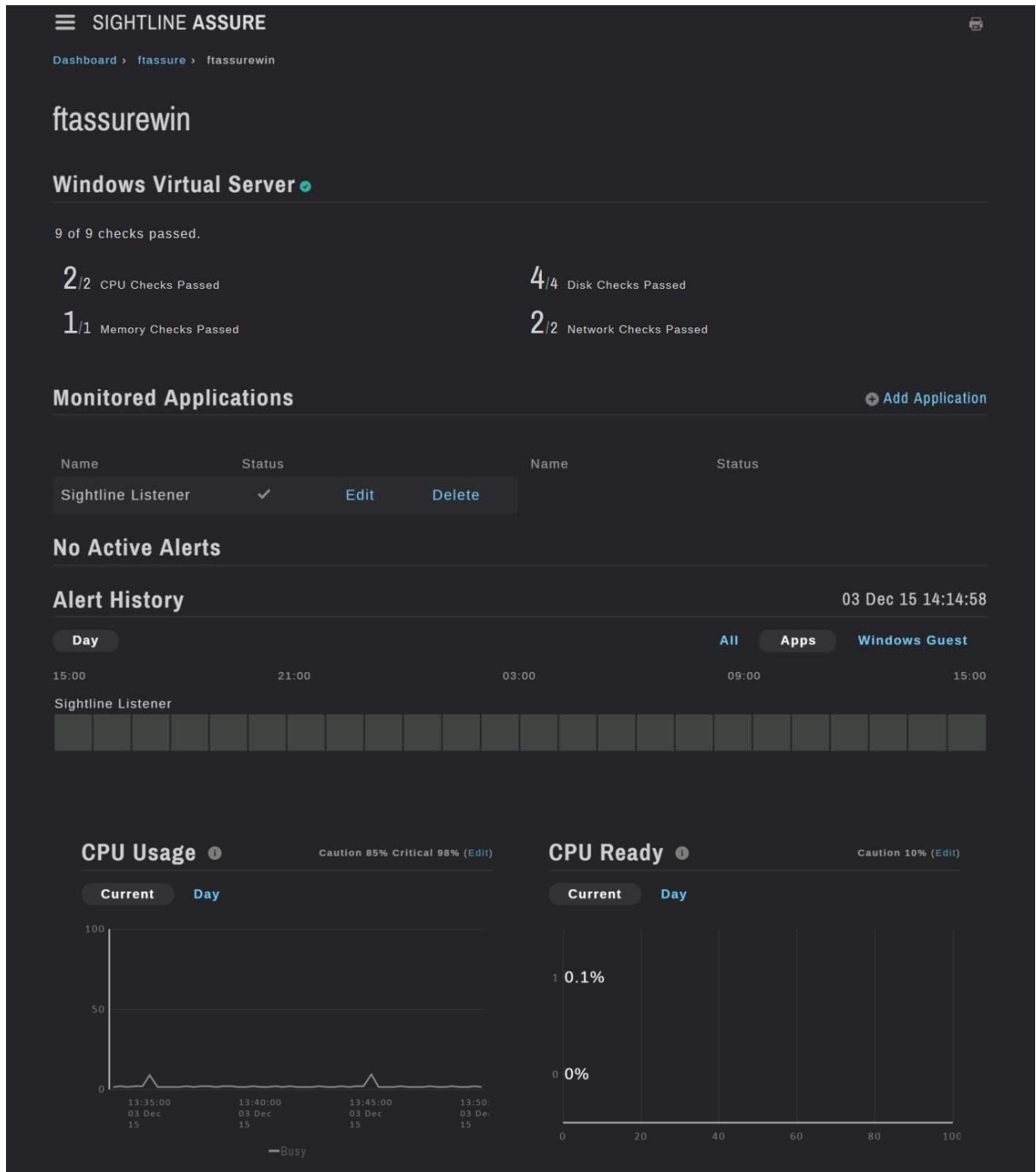


Figure 4-12. VMware Guest Overview Page

In Figure 4-12, the server **ftassurewin** is a Windows Virtual Server that resides on the VMware server called **ftassure**. As you scroll down the page, you'll see that the same sections are included: the health checks, monitored applications, alerts and charts. Notice that the charts may be slightly different between a physical Windows system and guest Windows instance, because the data is retrieved differently from VMware guests systems.

4.5 Monitoring Options for VMware Guests

Due to the unique nature of VMware, there are several options available for monitoring VMware guests. Notice that there is an **Edit** link for each VMware guest in the **VMware System Overview** page (see Figure 4-11). Click **Edit** to display the **Edit Guest** dialog box (Figure 4-13).

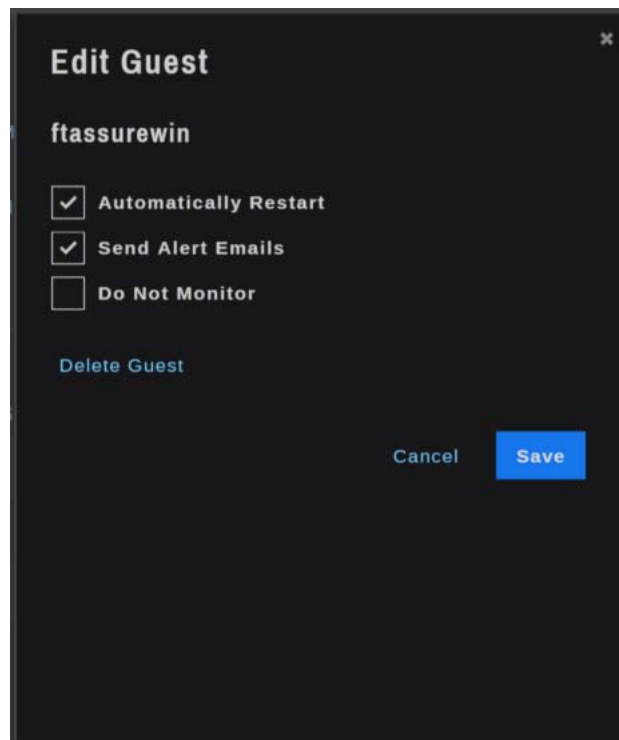


Figure 4-13. Edit Guest Dialog Box

Assure receives an update from the VMware system every 20 seconds. If the update indicates that a VMware guest is not active, you can opt to have Assure attempt to restart the guest. Check **Automatically Restart** to select this option. Assure will attempt to restart the guest once and notify you (as a VMware OS alert) that the guest was inactive and the restart was attempted.

You may also decide to turn off email notifications for a particular guest, perhaps if you know that the guest may be going on and off. Uncheck **Send Alert Emails** for the guest; this is checked by default for all VMware guests. Alerts will still be tracked in the **Active Alerts** and **Alert History** tables.

Do Not Monitor is used to ignore a VMware guest. In some instances, guests may be created on the system but are not active. Rather than continually reporting the guest as inactive, **Do Not Monitor** is used to suppress any alerts from being triggered for the guest. Should the guest become active, simply uncheck **Do Not Monitor** and Assure will actively monitor the guest.

Delete Guest is used to remove the guest instance from the **VMware Guest** table. When a guest is physically removed from the VMware guest system, you must tell Assure that it no longer exists by deleting it.



If you delete a guest from Assure but it still exists on the VMware system, it will be rediscovered in the next monitoring interval and added back into the VMware system's guest list. If the guest still exists, then **Do Not Monitor** may be a better option.

Click **Delete Guest**; a confirmation dialog box will be displayed. Click **Yes** to delete the guest or **No** to cancel.

4.6 System Overview Page for everRun Systems

The **everRun Overview** page (Figure 4-14) is similar to the **VMware Overview** page, in that it has sections for everRun, hardware and guests. However, everRun Overview page has hardware information, health checks and charts for each of the everRun nodes.

Note that the **System Health Checks** for **everRun Server** apply to the complete everRun instance. The hardware and node information shows Node0 on the left of the page and Node1 on the right. **Alert History** can be shown for everRun, Node0, Node1 or all categories. **Charts** are provided for everRun and also the individual nodes.

everRun guests are monitored and shown on the everRun Overview page. You may decide to turn off email notifications for a particular guest, perhaps if you know that the guest may be going on and off. Uncheck **Send Alert Emails** for the guest; this is checked by default for all guests. Alerts will still be tracked in the **Active Alerts** and **Alert History** tables.

Do Not Monitor is used to ignore a guest. In some instances, guests may be created on the system but are not active. Should the guest become active, simply uncheck **Do Not Monitor** and Assure will actively monitor the guest.



We recommend that you install a Sightline Power Agent on any everRun guest, particularly those that are considered mission-critical. The depth of monitoring is enhanced when the Power Agent is present on the guest.

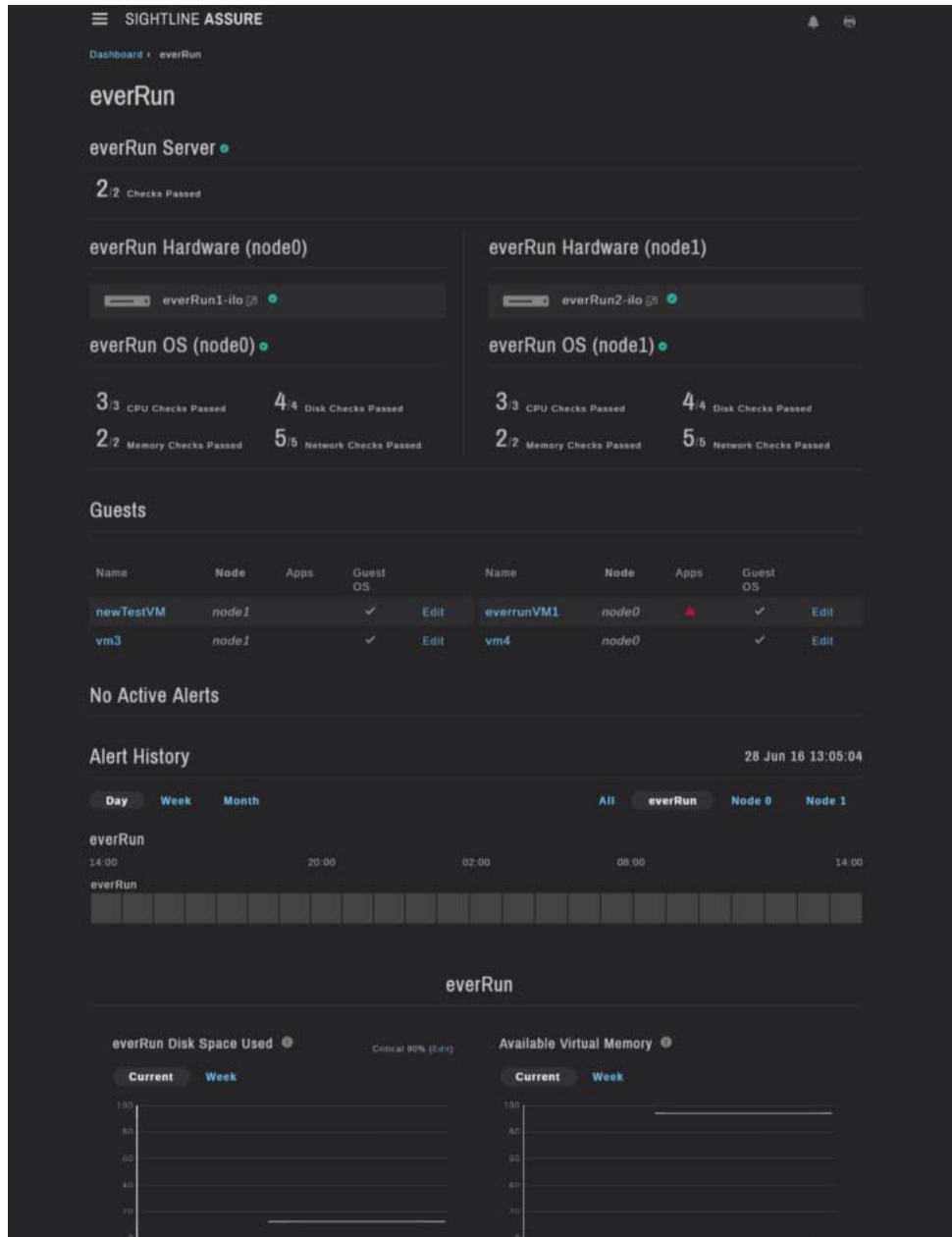


Figure 4-14. everRun Overview Page

4.7 Creating and Monitoring Applications

Applications can be created and monitored on any Windows or Linux OS instance. On Windows systems, applications can be based on services or ports; for Linux systems applications are based on ports.

4.7.1 Creating Applications

To create an application, use the **Add Application** link on the server overview page.

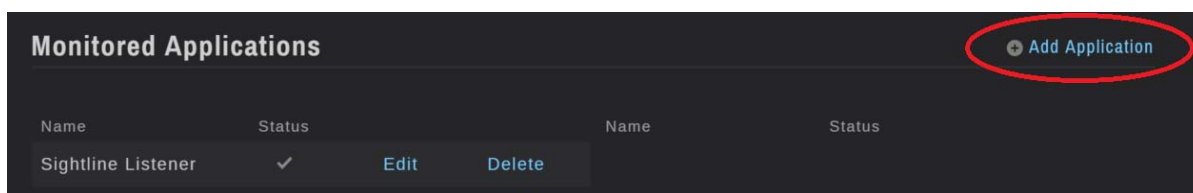


Figure 4-15. Add Application Link

This will display the **Create an Application to Monitor** dialog box (Figure 4-16). Supply the application name, and then indicate if you want to **Monitor Windows Services** (Windows systems only) and / or TCP ports (Windows and Linux systems).

If you check **Monitor Windows Services**, Assure will retrieve the list of services from the Windows system and display it so that you can create the application based on the presented list (Figure 4-17).



When creating applications to monitor Windows services, the firewall rules on the monitored server may need to be updated. Specifically, the **File and Printer Sharing (NB-Session-In)** rule must be enabled for Assure to retrieve the services list and then monitor the services.

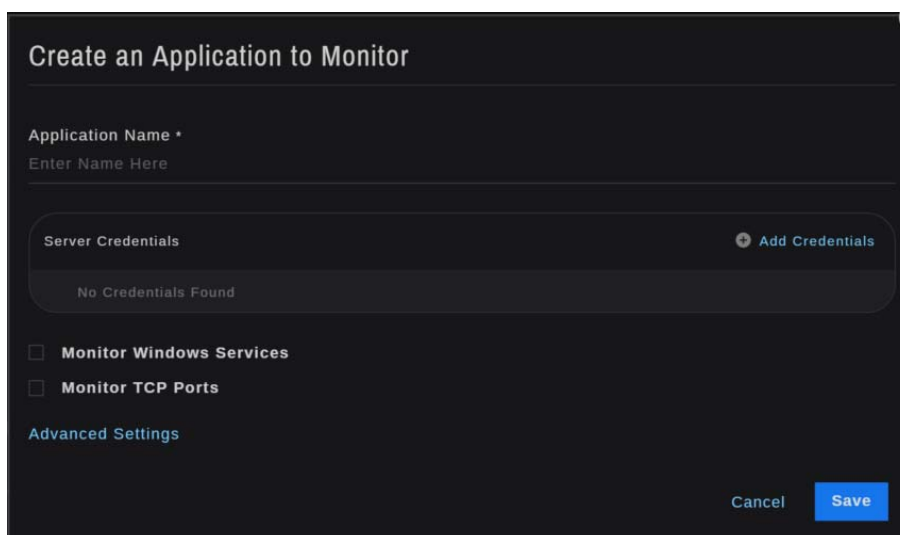
A screenshot of the 'Create an Application to Monitor' dialog box. It features a text input field for 'Application Name' with a placeholder 'Enter Name Here'. Below this is a section for 'Server Credentials' with an 'Add Credentials' button and the text 'No Credentials Found'. There are two checkboxes: 'Monitor Windows Services' and 'Monitor TCP Ports', both currently unchecked. At the bottom, there is an 'Advanced Settings' link, a 'Cancel' button, and a blue 'Save' button.

Figure 4-16. Create an Application to Monitor Dialog Box



If this is the first application you are creating for a server, you will need to provide windows credentials in order to retrieve the list of services. See Section 4.6.2, *Managing Credentials*.

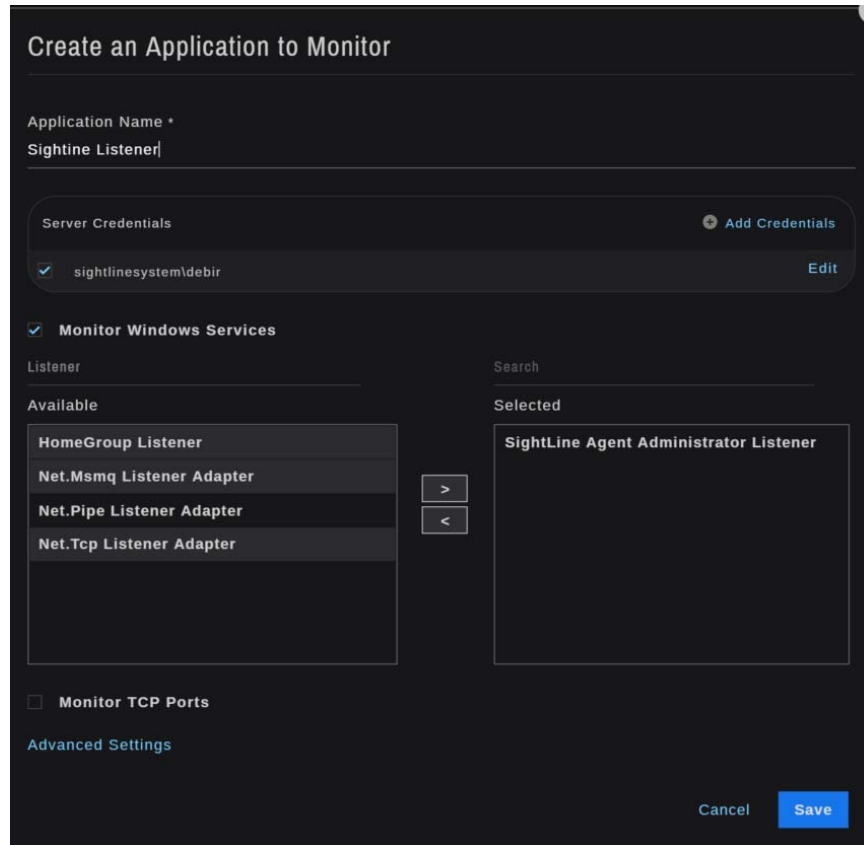
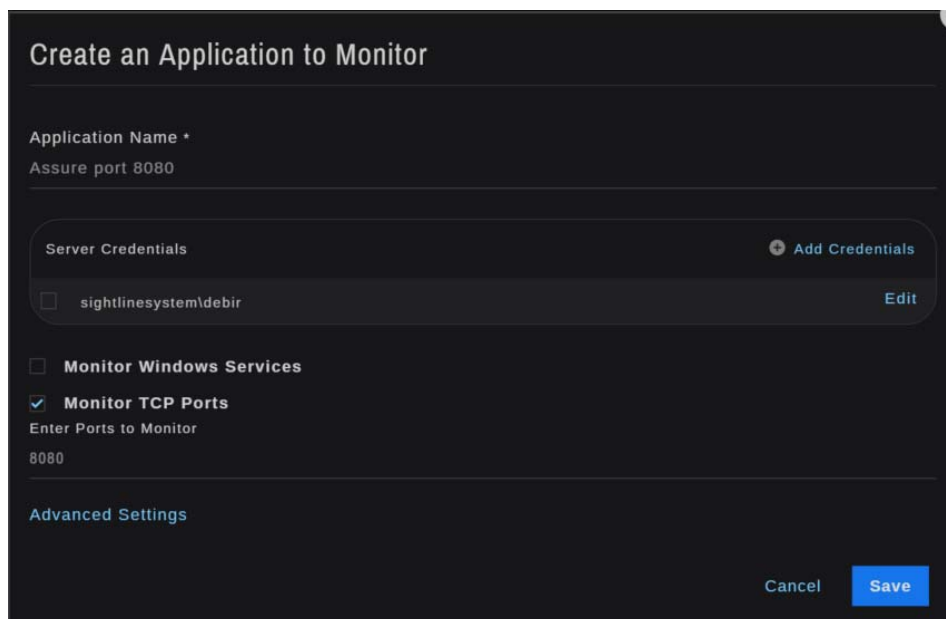


Figure 4-17. Monitor Windows Services

The list of **Available** services will be shown on the left. Select one or more services and add them to the **Selected** box on the right. This list will be presented in alphabetical order, but a search capability is also provided. You can include the same service in one or more applications.

Check the **Monitor TCP Ports** option to monitor one or more ports. Multiple ports should be separated by commas. Assure will test the ports every minute and generate an Application Alert if one or more of the ports does not respond. Note that an application on a Windows system can have a combination of services and ports.

For applications on Windows systems, you can optionally configure a **Corrective Action**. That is, provide the path to a script for Assure to execute if an application generates an alert. Provide the entire path to the script. Assure will execute the script one time. Remember that you must have assigned credentials for the system in order to implement corrective actions. In addition, on Windows systems you must have an ssh server installed on the monitored system.



Create an Application to Monitor

Application Name +
Assure port 8080

Server Credentials ➕ Add Credentials

sightlinesystem\debir Edit

Monitor Windows Services

Monitor TCP Ports

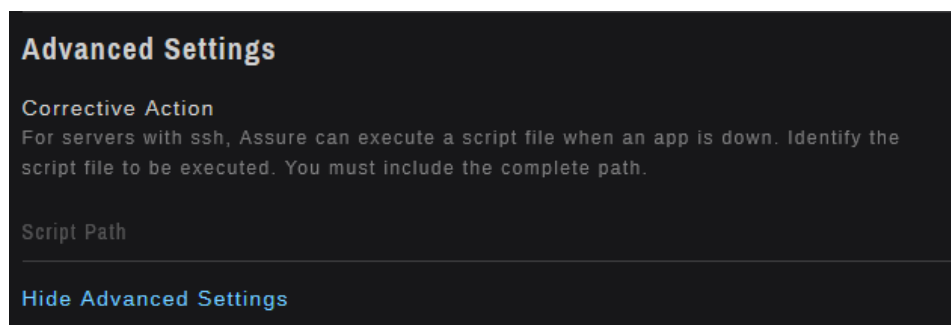
Enter Ports to Monitor
8080

Advanced Settings

Cancel Save

Figure 4-18. Monitor TCP Ports

Click **Advanced Settings** to expand the section.



Advanced Settings

Corrective Action
For servers with ssh, Assure can execute a script file when an app is down. Identify the script file to be executed. You must include the complete path.

Script Path

[Hide Advanced Settings](#)

Figure 4-19. Advanced Settings

For applications on Linux systems, you can optionally configure a **Corrective Action**. That is, provide the path to a script for Assure to execute if an application generates an alert. Provide the entire path to the script. Assure will execute the script one time. Note that you must have assigned credentials for the system in order to implement corrective actions.

When you have filled in all options click **Save**. The newly created application will be added to the list of **Monitored Application** on the **Server Overview** page.

Initially, the application's status will be represented by a red "disconnect" icon, but will be updated after the next monitoring interval. At each monitoring interval, Assure will check all services that have been included in an application. An application alert will be generated for any application where one of its included services is not active.

4.7.2 Managing Credentials

In order to access a Windows system to retrieve the services list, you must provide login credentials so that Assure can obtain the information required to monitor the processes. Applications on Windows systems can also be based on ports, but these applications do not require credentials in order for Assure to monitor them.

Credentials are also required for using the **Corrective Action** feature under **Advanced Settings** on Linux systems.

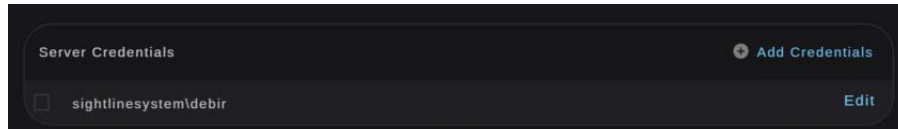


Figure 4-20. Monitor TCP Ports

Select existing credentials by checking the box to the left of the credentials. To show the entire list of credentials click on the **Show More** Link.

Use the **Add Credentials** link to create new credentials, or the **Edit** link to update existing credentials.

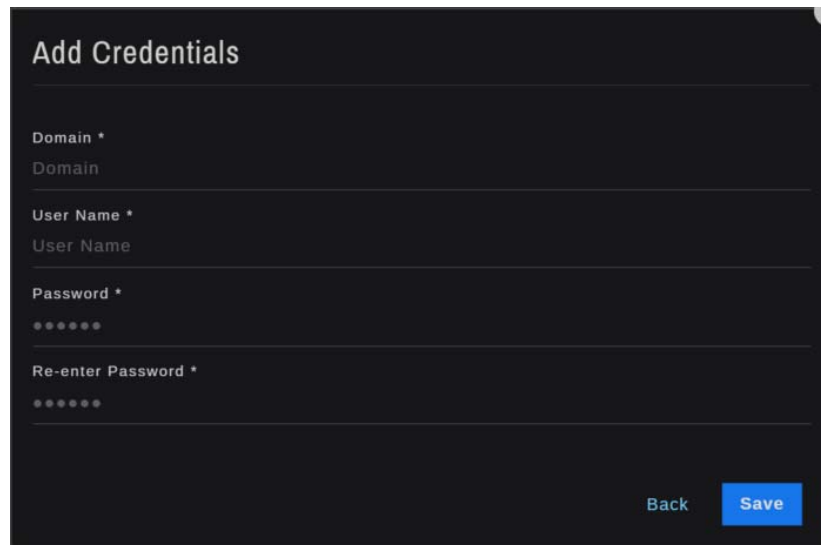
A screenshot of a web form titled "Add Credentials". The form has four input fields: "Domain *" with a placeholder "Domain", "User Name *" with a placeholder "User Name", "Password *" with a masked password "*****", and "Re-enter Password *" with a masked password "*****". At the bottom right, there are two buttons: "Back" and "Save".

Figure 4-21. Monitor TCP Ports

Credentials consist of a **Domain**, **User Name** and **Password**. After clicking **Save** the new credentials will be added to the list of existing credentials and can be selected.

Once the correct credentials have been selected, you can choose to monitor one or more Windows services, or specify the correction action path. Note that once credentials are validated on a system, you will not be able to edit them.

4.8 Alert Notification Emails

As part of Assure's alerting feature, emails can be sent to notify users when alerts or utilization thresholds violations occur. Three email settings can be configured: operating system alerts (alerts generated based on resource utilization thresholds), application alerts, and hardware alerts. Email addresses are entered or modified in the **Settings | Email Settings** dialog.



Figure 4-22. Alert Emails

Emails are generated for critical alerts and sent to the email address(es) identified for that alert type. If no emails were supplied, the alert is still shown in the Active Alert table. If multiple alerts are active, they will be combined into a single email.

4.9 Scheduled Reports

Daily and/or weekly reports can be requested from Assure, using the **Settings | Scheduled Reports** dialog. Scheduled reports provide a summary of all alerts that were generated for all systems in the Assure monitored environment.

Daily reports are generated at 30 minutes past midnight, and include all alerts generated during the previous day. Weekly reports are generated at 12:30 am on Monday mornings and include all alerts that were generated during the previous Monday through Sunday. All systems are included in the report.

4.10 Assure Mobile

Assure is easily accessed using your mobile device. Simply access your corporate VPN or network, and then use the browser to access Assure the same as you would on your desktop.

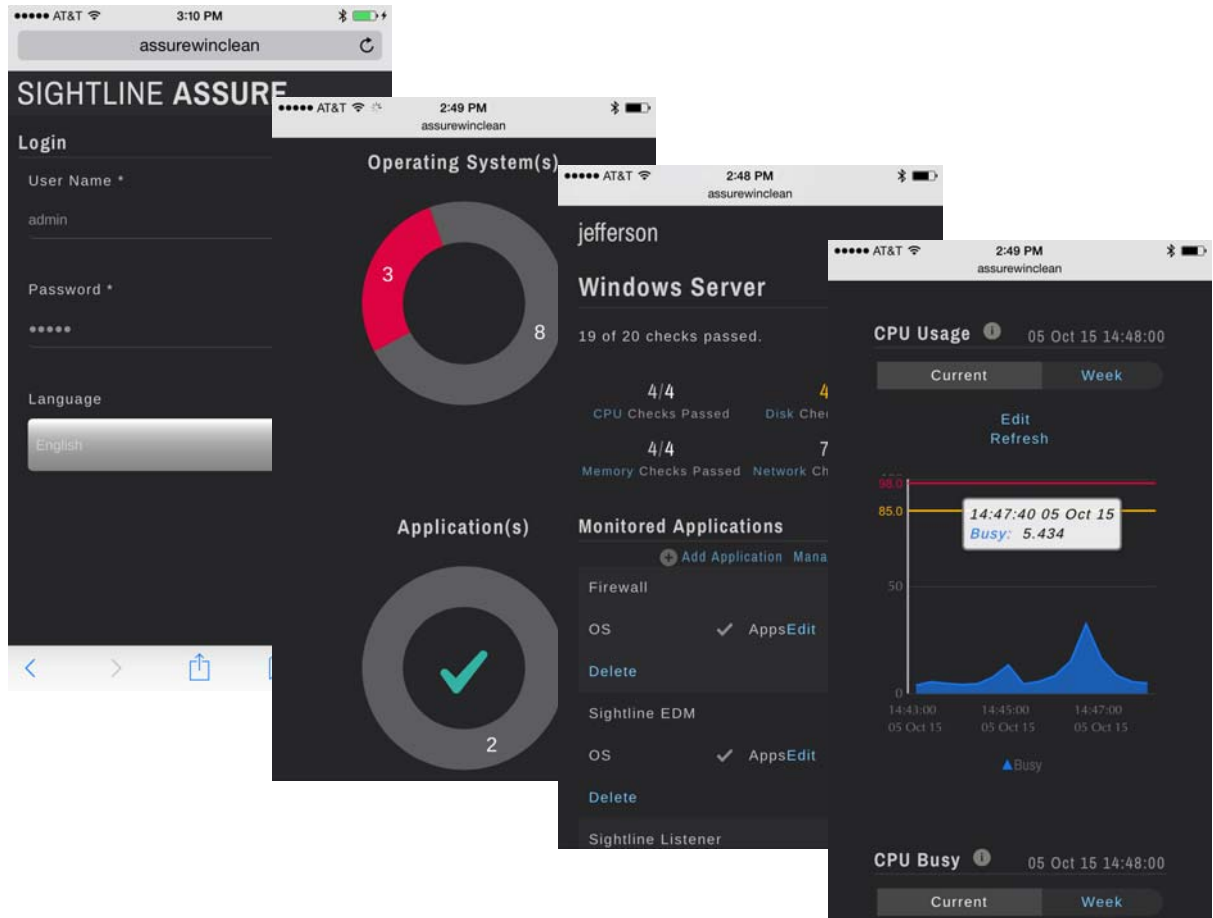


Figure 4-23. Assure Mobile

Chapter 5

Assure Settings Menu

The entries in Assure's **Settings** menu are used to configure many of the behaviors of Assure. This section contains a description of each item in the **Settings** menu.

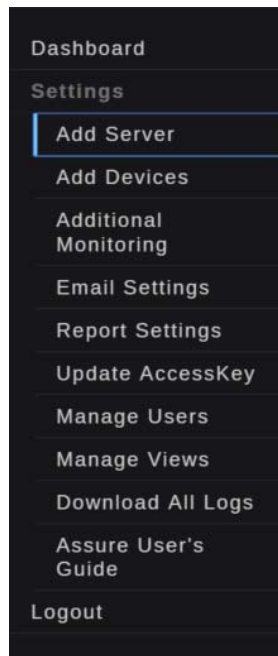


Figure 5-1. Assure Settings Menu

To display the **Settings** menu, click the “hamburger” icon at the top left of the Assure window.

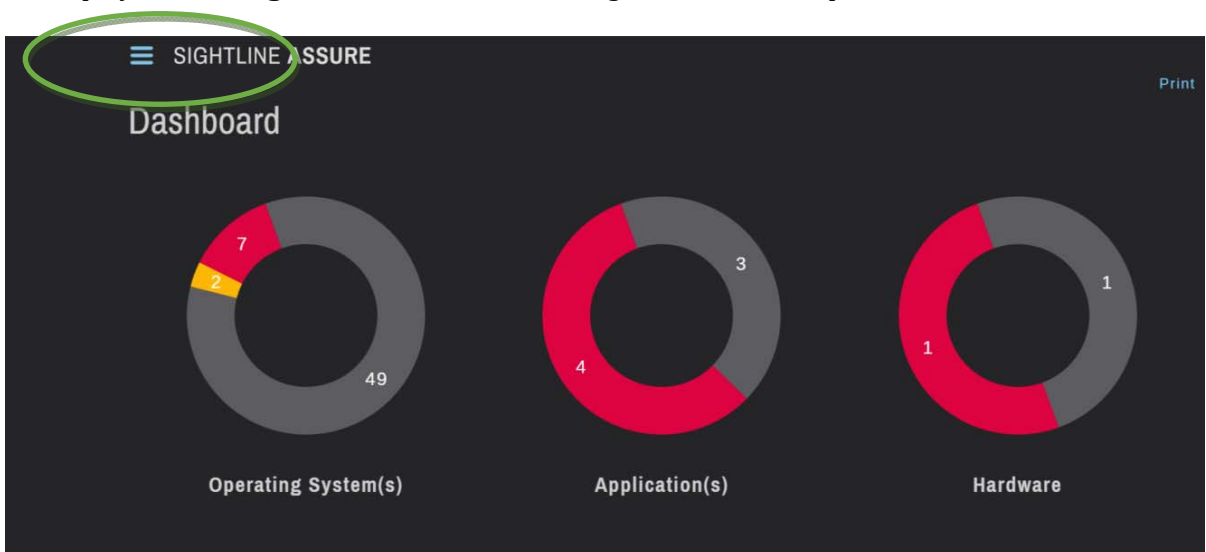


Figure 5-2. Accessing the Assure Settings Menu

5.1 Dashboard

The entry above the **Settings** menu provides a short-cut to the main Assure dashboard. From any page in the Assure display, you can click the **Dashboard** link here to return to the main Assure dashboard.

Clicking on the Sightline Assure logo will also return you to the main Assure dashboard display.

5.2 Add Server

The first item under **Settings** is **Add Server**. Use **Add Server** to identify a server to be monitored and add it to the list of monitored servers. You can add any VMware ESX server or a physical server that's running a supported Sightline Power Agent: Linux, Windows or OpenVMS. See Appendix B, *Monitoring Stratus everRun Systems*, for details about adding an everRun® instance to Assure.

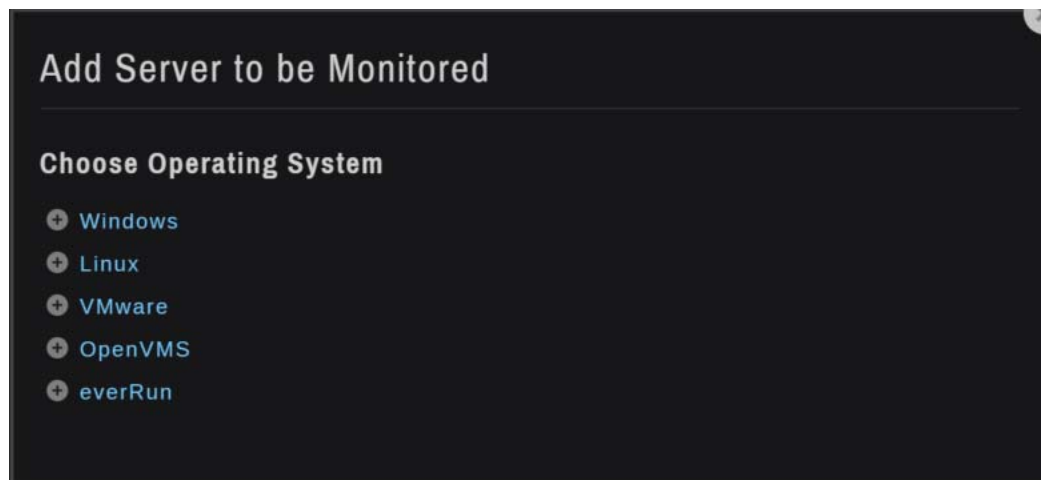


Figure 5-3. *Add Server to be Monitored* Dialog

Select the operating system of the monitored system. The **Add Server** dialog will be updated to request information specific to the system being added: the system name, display name and, optionally, hardware details when hardware monitoring is desired (Figure 5-4).

Enter the server name or its IP address or DNS name so that the server can be discovered and populated in Assure's server list in the main Dashboard.

Host Display Name is useful when the servers in the environment must be identified by IP address or DNS name to be discovered by Assure and added as monitored objects. Rather than a list of IP addresses or long DNS names, use the display name option to make server names more easily understood.

Add Windows Server

Before adding the server to Assure, please confirm that a Sightline Power Agent is installed and running on the system to be monitored.

Enter DNS Name or IP Address *

DNS Name or IP Address

Host Display Name (optional)

Enter Host Name to be displayed

Hardware Monitoring

Assure can provide hardware monitoring for certain servers. To enable hardware monitoring, select your server type here.

Select Type

ftServer

Cisco UCS
Cisco Integrated Management Controller (CIMC) Hostname or IP *

HP

Dell

IBM

SNMP Community String (optional)

public

Hide Options

Cancel Save

Figure 5-4. Expanded **Add Windows Server** Dialog

Expand the **Hardware Monitoring** section of the dialog to identify the server hardware type. Assure can monitor ftServer, Cisco, HP, Dell and IBM server hardware. Additional information may be required so that the hardware information can be retrieved via an SNMP connection:

- ◆ For Cisco hardware monitoring, the CIMC (Cisco Integrated Management Controller) hostname or IP address
- ◆ For HP hardware, the iLo (HP Integrity Integrated Lights-Out) hostname or IP address
- ◆ For IBM hardware, the IBM hostname or IP address

In addition, you may need to specify the **Community String** for SNMP connections made to obtain the hardware details; the default is *public* if the community string is not supplied.

When the server is first added to the server list in Assure, you might see a red “disconnected” icon in the OS column. It may take a few minutes for the connection to be established and the first performance data to be processed.

For Windows, Linux and OpenVMS servers, there must be a Sightline Power Agent installed and running or the server will not be discovered (see Section 5.4, *Additional Monitoring*, for more information about Power Agents). Confirm also that there are no firewall issues between the Assure system and server to be monitored.



As a general rule, VMware guests should not be added to Assure individually using **Add Server**. VMware guests are monitored as part of the host VMware system.

In Figure 5-5, a server with hostname **win2012r2** has been discovered and added to the Assure display. Note that the health of the host's OS and Application components is displayed; if no hardware is specified then that column will remain empty.

Server	Operating System(s)	Application(s)	Hardware	Settings
angkor	OS	Apps	Hardware	Edit
argos	OS			Edit
asgard	OS			Edit
avaris	OS			Edit
ftassure	OS	Apps	Hardware	Edit
win2012r2	OS	Apps		Edit

Message	Server	Duration	Action
Disk utilization is high and disk queue write latency is also high.	angkor	113 minutes	Server Details

Figure 5-5. Adding a Server running a Power Agent

When adding VMware hosts, **Add VMware System** will be displayed, prompting you for the VMware server's hostname or IP address, along with proper VMware username and password credentials.

When adding everRun systems, the **Add everRun Server** dialog will be displayed, prompting you for the IP addresses or DNS names of both node0 and node1, as well as both hardware IP Addresses.



See Appendix B, *Monitoring Stratus everRun Systems*, for more information about configuring Sightline Power Agents on the everRun nodes and adding the everRun system to Assure.

Once all fields have been completed, click **Save**. The dialog will warn you if there is a password mismatch. The specified monitored system will be discovered and populated in Assure's server list on the main Dashboard display.

5.3 Add Devices

Use **Add Devices** to add devices to the Assure instance. Network devices include SNMP-enabled network devices such as switches and routers. Assure supports EMC VNXe storage devices and ONVIF-compliant cameras as peripherals.

Figure 5-6. Add Devices Dialog

Select a category of devices and supply the range of IP Addresses to be checked. To specify an individual IP Address, enter the same value in the **From** and **To** sections of the range (for example, 192.168.1.50-50).

If you select **Network** devices, an **SNMP Community String** will be requested. The default is *public* if the community string is not supplied. If you have multiple community strings in your environment, separate discoveries for each community string will be required to add all of the devices to Assure.



As a general rule, the larger the range of IP addresses you supply, the longer the discovery will take. A status bar will be presented during the discovery process.

Assure will discover any **Network** devices that match the RFC1213 standard MIB or the Cisco Catalyst 3750X MIB. Assure will discover EMC VNXe **Storage** devices, and ONVIF-compliant cameras as **Peripherals**.



Storage devices are monitored using the Sightline SMI-S Interface Agent, which is associated with a Windows Power Agent (see *Installing the Sightline Power Agent for Windows Systems* under **Additional Monitoring** for details). The IP address of the VNXe storage device will be the IP address of the Windows system where the Power Agent is installed.



If your camera requires credentials to be accessed, then the credentials must be provided for Assure to monitor it. The camera will be discovered and shown under **Peripherals** but will be disconnected. In addition, an alert will be generated notifying you that credentials are required. Use the **Edit** link for the camera to provide the **User Name** and **Password**.

Once discovered, Assure will present a list of the devices that were found on the network. Select the items that you want to add to the Assure dashboard.

The screenshot shows the 'Devices' dialog with three sections:

- Network (7 devices):**

Name	Type	Settings
Network		View Less
192.168.1.27	RFC1213	Edit
192.168.1.3	RFC1213	Edit
192.168.1.5	Cisco 3750-X	Edit
192.168.1.9	RFC1213	Edit
- Storage (1 device):**

Name	Type	Settings
Storage		View Less
192.168.103.11	EMC VNXe	Edit
- Peripherals (1 device):**

Name	Type	Settings
Peripherals		View Less
192.168.1.188	ONVIF Compliant Camera	Edit

Figure 5-7. Add Devices Dialog

5.4 Additional Monitoring

Assure provides an option to download a Sightline Power Agent for deeper system data collection. Power Agents are available directly from Assure for Microsoft Windows 2008 or Windows 2012 systems, Linux servers or OpenVMS servers. Once installed, Assure can discover the server with the running Power Agent, and can start monitoring Power Agent metrics for the system.

To download the Power Agent installation kit, select **Settings | Additional Server Monitoring**, and then select the **Windows Power Agent**, **Linux Power Agent**, or **OpenVMS Power Agent** link. Then download the installation instructions.



Figure 5-8. Downloading a Sightline Power Agent

The downloaded installer can then be transferred to the target server for installation. Retrieve the Power Agent installation instructions for further information.



Power Agents should not be installed on VMware guests. Guest information is included with the VMware host monitoring.

5.5 Email Settings

As part of Assure’s alerting feature, emails can be sent to notify users when alerts or utilization thresholds violations occur. To send emails, an email server must be identified and a “sent from” email address must be provided.

Email settings may be provided through the Assure Setup Wizard, or through the **Email Settings** dialog. Settings can also be editing using **Email Settings**.

Send Emails From is the “sent from” email address for all emails initiated by Assure. Depending on your email server, this address may not need to be a valid user, but it must appear in valid email format.

Domain is the email server’s domain name, and **Port** is the email server’s port number.

If encryption is enabled on your email system, select **SSL** or **TLS** under **Encryption Type**. The default setting is **none** (--).

If your email system requires credentials for authentication, check **Enable Authentication** and then provide the requested username and password.

The screenshot shows the 'Email Settings' dialog box. It has a title bar 'Email Settings'. Below the title bar, there are several sections with input fields:

- Send Emails From ***: assure@sightline.com
- Domain**: aspmx.l.google.com
- Port**: 25
- Encryption Type**: A dropdown menu with a downward arrow.
- Enable Authentication**: An unchecked checkbox.
- Email Addresses (use commas to separate multiple email addresses)**:
 - Assure System Alerts**: admin@sightline.com
 - Application Alerts**: name@domain.com
 - Operating System Alerts**: name@domain.com
 - Hardware Alerts**: tadmin@sightline.com

At the bottom right, there are two buttons: 'Cancel' and 'Save'.

Figure 5-9. Email Alert Settings Dialog

Assure System alerts occur when something is wrong with the overall Assure system. For example, an Assure component goes down and Assure is unable to collect performance data. This will trigger a system alert email to be sent.

Application alerts occur when a configured application (or a component of the application) is not active. Enter the email addresses of the recipients of application alert emails. Multiple email addresses should be comma-separated. You can leave this entry blank if application alert emails will not be sent by Assure.

Operating system alerts reflect resource utilization issues in an operating system instance. Enter the email addresses of the recipients of operating system alert emails. Multiple email addresses should be comma-separated. You can leave this entry blank if operating system alert emails will not be sent by Assure.

Hardware alerts indicate problems with individual hardware components. Enter the email addresses for the recipients of hardware alert emails. Multiple email addresses should be comma-separated. Leave this entry blank if hardware alert emails will not be sent by Assure.

For each alert type, Assure will send an email to the email address(es) provided. If no email address is provided then Assure will not attempt to send an email. The alert, however, will be shown in the **Active Alerts** display for the system where it occurred.

If there are multiple emails in a specific alert category, they will be combined into a single email by Assure, to avoid multiple emails being sent.

5.5 Report Settings

Assure provides the option to deliver daily or weekly reports, which are summaries of the triggered alerts for the time period.

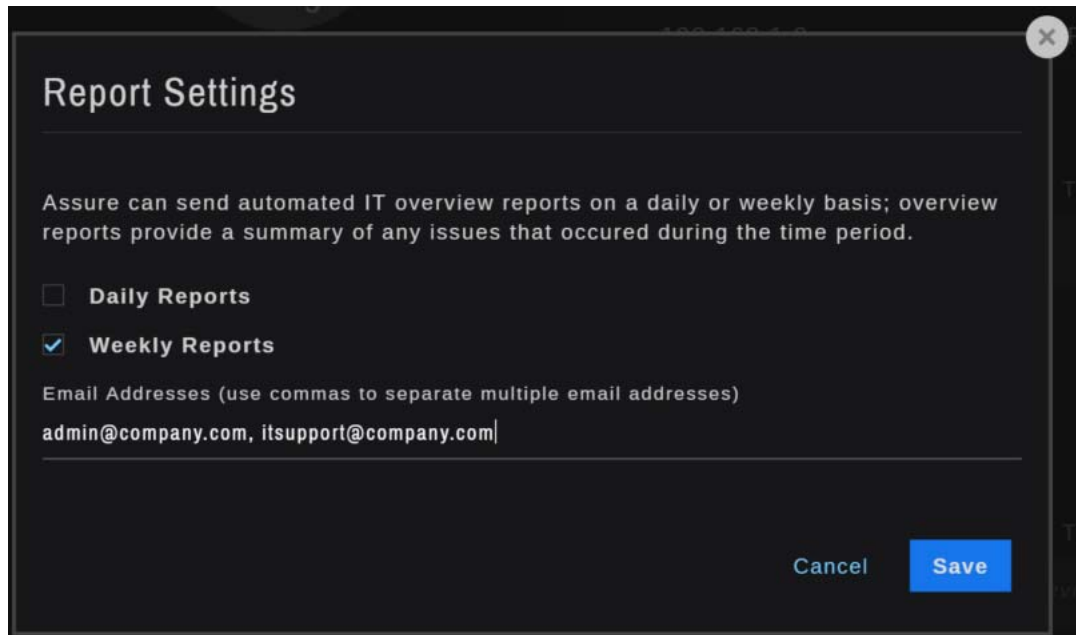


Figure 5-10. Report Settings Dialog

Daily and weekly reports include an alert summary for each system, for all three alert categories. Select either **Daily Reports**, **Weekly Reports** or both, and then provide the email addresses for the scheduled report recipients. Multiple email addresses are separated by commas.

5.6 Update AccessKey

Use **Update AccessKey** to enter an Assure AccessKey or to update your existing AccessKey. This may be required to update the types and numbers of servers and devices to be monitored by the Assure implementation, or to extend the license expiration.



The first time that Assure is started after installation, it will be running in *Trial mode* for 45 days. Trial mode enables up to five monitored systems and five network devices and peripherals. You will not see an AccessKey string but you will see the expiration date. You must enter a valid AccessKey string before the expiration date to ensure uninterrupted use of Assure, or to enable additional monitored objects.

In the **Update Assure AccessKey** dialog box, simply enter your new AccessKey string and click **Save**. AccessKey updates take place immediately, without having to restart Assure. Be sure to copy the entire string, including dashes and semi-colons.

Update Assure AccessKey

Current AccessKey expires: Fri Jun 30 00:00:00 EDT 2017
 FB9B92N-3E686PA-6Y4RDM;AD4D462-5X6FEL-8X46BX;2JZJZXE-4MXTSN-ZEA3ZQ

Monitored Servers: 25 FB9B92N-3E686PA-6Y4RDM
 Storage Arrays: 5 AD4D462-5X6FEL-8X46BX
 Network Devices and Peripherals: 200 2JZJZXE-4MXTSN-ZEA3ZQ
 OPC Enabled: Yes

Enter new AccessKey
 XXXXX-XXXX-XXXX-XXXX

Update all Power Agents using the Assure AccessKey

Cancel Update

Figure 5-11. Updating Assure AccessKey

The **Update all Power Agents using the Assure AccessKey** check box tells Assure to contact the Sightline Power Agents that are being monitored by Assure and update them using the Assure AccessKey. This is useful when extending your Assure license. Check the notification list to see if any Power Agent AccessKeys were not updated; they will have to be updated manually using the Edit Server dialog or by logging into the system and updating the Power Agent's configuration file.

5.7 Manage Users

Manage Users provides the ability to add new users to Assure, or to edit the settings for existing users. When you first install Assure, there is one user configured; this user has username *admin* with the default password *admin*.

When you first select **Manage Users**, the **Manage Users** dialog box will be displayed, showing a list of all current Assure users and the last time they logged into Assure. Click **Edit** to update the settings for an existing user, or **Add User** to configure a new user for Assure.

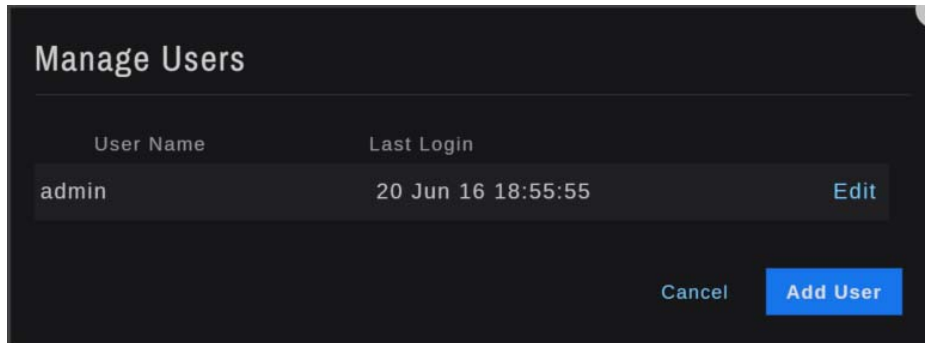


Figure 5-12. Manage Users Dialog

The dialog will be expanded so that you can add or edit the user's settings.

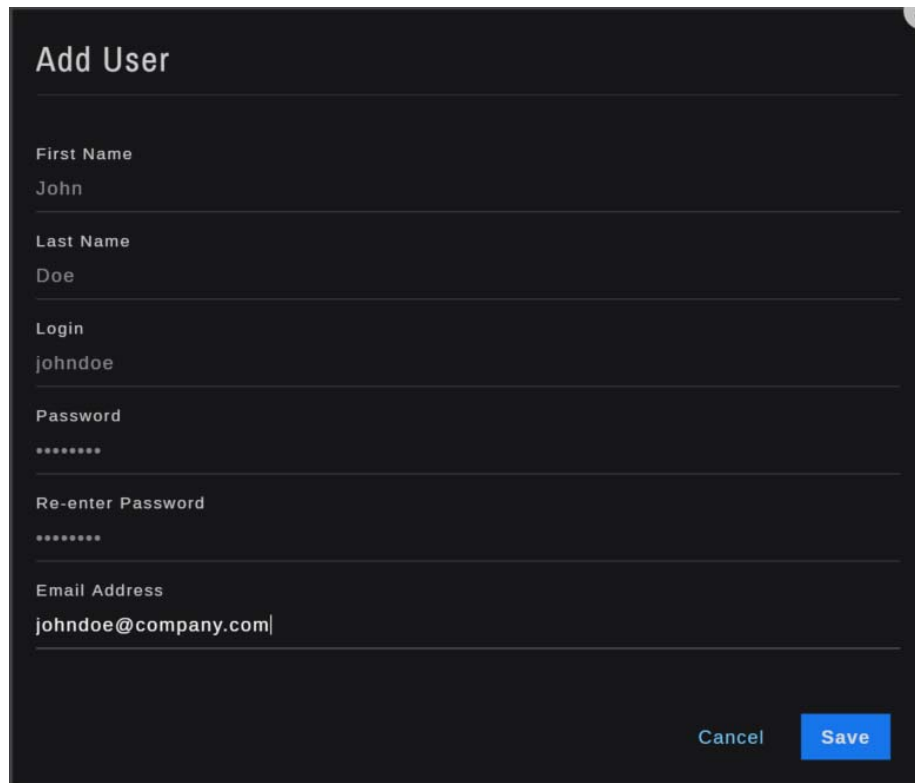
The screenshot shows a dark-themed dialog box titled "Add User". It contains several input fields: "First Name" (John), "Last Name" (Doe), "Login" (johndoe), "Password" (masked with asterisks), "Re-enter Password" (masked with asterisks), and "Email Address" (johndoe@company.com). At the bottom right, there are two buttons: "Cancel" and "Save".

Figure 5-13. Manage Users Dialog

To add a new user, provide the **First Name**, **Last Name**, **Login** (username), **Password** and their **Email Address**. All of these fields are required.

The **Login** can contain letters, numbers and underscore characters. Note that the **Login** is case-sensitive. The **Password** must have at least six characters, letters and numbers only. The **Password** is also case-sensitive.

When updating a user's login information, changes will take effect immediately after they are applied. Note that the **Login** cannot be changed once the user entry has been created.

Click **Save** to store your updates, or **Cancel** to close the dialog without making any changes.

5.8 Manage Views

A *View* is a subset of the monitored systems and devices in Assure. Use **Manage Views** to add views to your Assure implementation or to edit or delete existing views. The list of available views is accessed by clicking the down arrow to the right of the Dashboard title on the Assure Dashboard.

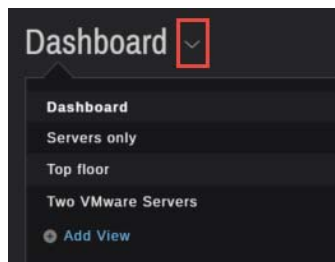


Figure 5-14. Displaying a View

This down arrow also appears to the right of the title on any System Overview page or View on display in the Assure UI.

When you select **Manage Views**, the **Add View** dialog will be displayed. Enter the view name and click **Add Servers and Devices**. A list of all monitored objects will be displayed.

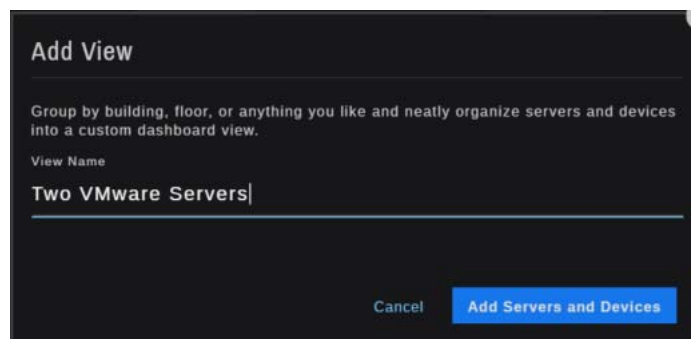


Figure 5-15. Adding a View

Select the objects to be included in your view. In Figure 5-16, only two servers are selected; notice that when the view is shown (Figure 5-17), only information for the selected servers is included in the display.

Likewise, in the **Top Floor** view in Figure 5-18 only the selected devices are shown.

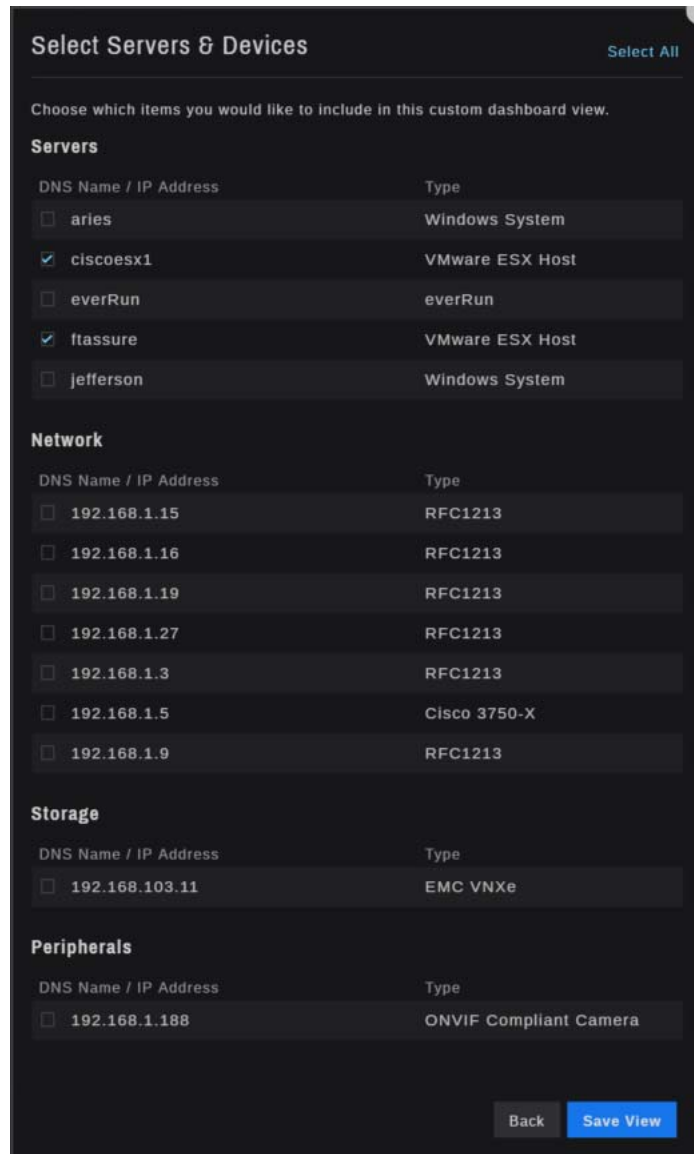


Figure 5-16. Select Servers and Devices

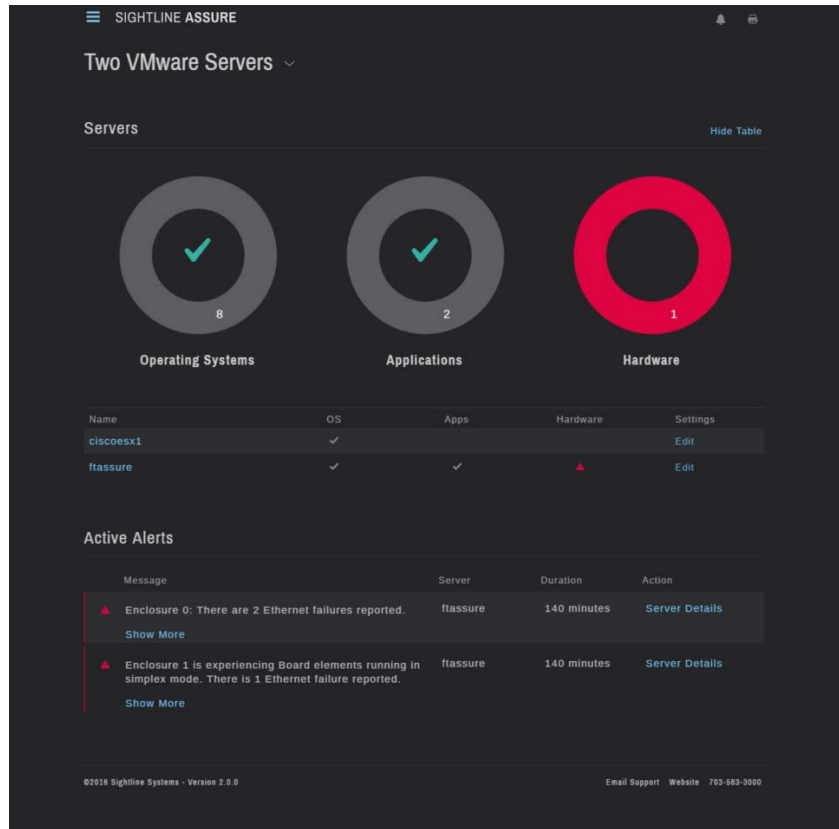


Figure 5-17. Adding a View

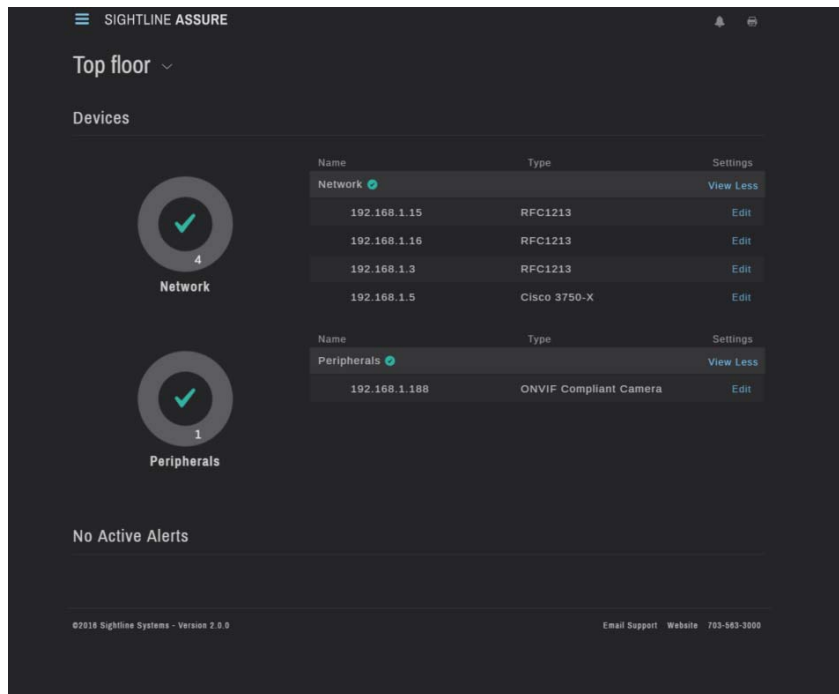


Figure 5-18. Adding a View

To edit a view, use **Manage Views** and click **Edit** for the view to be updated.

To delete a view, use **Manage Views** to display the list of all views, click **Edit** for the view to be deleted, and then click **Delete View** from the **Edit View** dialog box.

5.9 Download All Logs

Download All Logs is provided for trouble-shooting purposes. Rather than logging in to the Assure system, your Assure support representative may ask you to use Download All Logs to send the Assure log files to be reviewed.

When you select **Download All Logs**, Assure retrieves the log files, zips them together, and stores them on your local system. You will be asked where to save the files. Generally the zip file is small enough to be attached to an email to your support representative.

5.10 Assure User's Guide

Use the **Assure User's Guide** link to display this User's Guide, in PDF format, in the Assure web browser. This can be helpful when you have questions about how to perform an operation in the Assure UI, or to review Assure's rich feature set.

Appendix A

Sightline OPC Server

Open Platform Communications (OPC) is a set of standards and specifications for industrial telecommunication. It was designed to provide a common bridge for software applications and process control hardware from different manufacturers to communicate.

Sightline Assure includes an OPC Server to make status information from the Assure dashboard available to your OPC client. Enabling the Sightline OPC server capability requires two steps:

1. Ensure that your Assure AccessKey enables the OPC functionality. If you are not certain, contact your Sightline Assure distributor.
2. Point your OPC client to the Assure OPC server using the following connection URL:

```
opc.tcp://<ip address>:52520/OPCUA/SightlineOPCServer
```

Select **none** as the security mode.

Table A.1 below lists the data items that are delivered from Assure to the OPC client.

Table A.1. OPC data items

Counter	Description
edmOSStatus	The color of the most critical server represented in the Operating Systems ring chart on the Assure dashboard. Possible values are other (0), green (1), yellow (2), red (3).
edmOSGreen	The number of elements in the Operating System ring chart that are in green (good) status.
edmOSYellow	The number of elements in the Operating System ring chart that are in yellow (caution) status.
edmOSRed	The number of elements in the Operating System ring chart that are in red (critical) status.
edmHardwareStatus	The color of the most critical server represented in the Hardware ring chart on the Assure dashboard. Possible values are other (0), green (1), yellow (2), red (3).
edmHardwareGreen	The number of elements in the Hardware ring chart that are in green (good) status.
edmHardwareYellow	The number of elements in the Hardware System ring chart that are in yellow (caution) status.
edmHardwareRed	The number of elements in the Hardware System ring chart that are in red (critical) status.

Counter	Description
edmApplicationStatus	The color of the most critical server represented in the Applications ring chart on the Assure dashboard. Possible values are other (0), green (1), yellow (2), red (3).
edmApplicationGreen	The number of elements in the Applications ring chart that are in green (good) status.
edmApplicationYellow	The number of elements in the Applications System ring chart that are in yellow (caution) status.
edmApplicationRed	The number of elements in the Applications System ring chart that are in red (critical) status.
edmNetworkDeviceStatus	The color of the most critical server represented in the Network Devices ring chart on the Assure dashboard. Possible values are other (0), green (1), yellow (2), red (3).
edmNetworkDeviceGreen	The number of elements in the Network Devices ring chart that are in green (good) status.
edmNetworkDeviceYellow	The number of elements in the Network Devices System ring chart that are in yellow (caution) status.
edmNetworkDeviceRed	The number of elements in the Network Devices System ring chart that are in red (critical) status.
edmStorageDeviceStatus	The color of the most critical server represented in the Storage Devices ring chart on the Assure dashboard. Possible values are other (0), green (1), yellow (2), red (3).
edmStorageDeviceGreen	The number of elements in the Storage Devices ring chart that are in green (good) status.
edmStorageDeviceYellow	The number of elements in the Storage Devices System ring chart that are in yellow (caution) status.
edmStorageDeviceRed	The number of elements in the Storage Devices System ring chart that are in red (critical) status.
edmPeripheralDeviceStatus	The color of the most critical server represented in the Peripheral Devices ring chart on the Assure dashboard. Possible values are other (0), green (1), yellow (2), red (3).
edmPeripheralDeviceGreen	The number of elements in the Peripheral Devices ring chart that are in green (good) status.
edmPeripheralDeviceYellow	The number of elements in the Peripheral Devices System ring chart that are in yellow (caution) status.
edmPeripheralDeviceRed	The number of elements in the Peripheral Devices System ring chart that are in red (critical) status.

Appendix B

Monitoring Stratus everRun Systems

Assure includes *everRun* as an option in the **Add Server** dialog when adding a server to the Assure dashboard. There are several items being monitored, and you will need to supply the appropriate details when adding an everRun system to Assure. In addition, you must install a Sightline Power Agent on both nodes of the everRun system being monitored in order to receive accurate performance information about the system.



SNMP must be configured on the everRun nodes for Sightline to remotely monitor the system. See Section B.3, *Configuring SNMP Settings*, for details.



When creating everRun guests, the guest name must be a valid DNS name that resolves to a valid IP address. If not, applications configured on the guest will not be correctly monitored by Assure. Sightline also recommends that a Power Agent be installed on all monitored everRun guests (see Section B.2, *Monitoring KVM guests on everRun Systems*).

B.1 Installing the Sightline Power Agent for Linux Systems on everRun nodes

The performance data for monitored everRun nodes is supplied by the Sightline Power Agent on each node. Some information about each KVM guest is included, but we recommend that a Power Agent be installed in any guest being monitored.

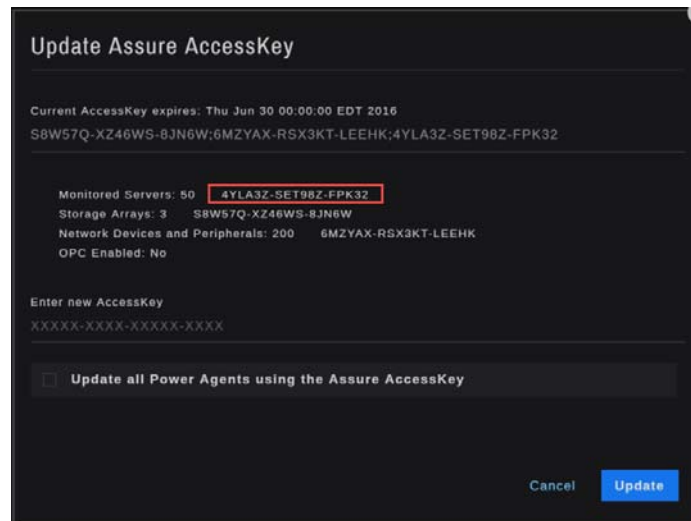
B.1.1 Retrieve your AccessKey string

During the installation of the Power Agent, an AccessKey will be requested. There are three places you might refer to for the AccessKey string.

- If you received an email with the Assure AccessKey, then it will include the AccessKey string for the Power Agent.
- If you are running Assure in trial mode, then the AccessKey string will be shown in the **Additional Monitoring** dialog box; simply copy this string and use it during the Power Agent installation.



- If you have entered an AccessKey string into your Assure implementation, the **Monitored Servers** section of the AccessKey string should be used for the Power Agent. Select **Settings | Update AccessKey** and make a note of the AccessKey string to the right of the **Monitored Servers** entry.



B.1.2 Download the Power Agent Installation Kit

From **Settings | Additional Monitoring** in the Assure interface, download the Linux Power Agent installation kit. This will be a file called `LinuxPA.tar.gz`.

B.1.3 Transfer the Power Agent Installation Kit to the target system

Copy the `LinuxPA.tar.gz` file from the download directory to the `/usr` directory on the Linux system to be monitored.

B.1.4 Unzip the install file

From the target Linux host, navigate to the `/usr` directory, and unzip:

```
#gunzip LinuxPA.tar.gz
```

Unzipping the installer will extract the `LinuxPA.tar` file to the directory.

B.1.5 Untar the install file

From the `/usr` directory, untar the installer:

```
#tar -xvf LinuxPA.tar
```

Untarring `LinuxPA.tar` will create another tar file named `sightlin.tar` and a `sightline_sig.txt` file. The `.txt` file contains information regarding the Power Agent, and is not necessary to complete the installation.

Untar `sightlin.tar`:

```
#tar -xvf sightlin.tar
```

Untarring will generate a `sightlinePA` directory.

B.1.6 Execute the install script

Navigate into `sightlinePA/bin` directory to execute the install script:

```
#cd sightlinePA/bin  
#./config-agents
```

B.1.7 Supply the requested information

The installation script will walk you through a few prompts where user input will be requested. Accept the default settings with the exception of these three items:

- ◆ For the hostname, enter the DNS name for the system being monitored.
- ◆ When the AccessKey is requested, supply the AccessKey that you copied from Assure. If you type the AccessKey string, type it exactly as it appears, including capitalization and dashes.
- ◆ For the collection interval, enter 20 seconds (instead of the default value of 30 seconds).
- ◆ **Important!** When the prompt for the **KVM Interface Agent** is presented, respond **[Y]es**.

If the option to **Start the power agent now** was selected as **Y**, you will see the Power Agent being started up from the command prompt after completing the install. Below is an example of the expected console output:

```
uid=0(root) gid=0(root) groups=0(root),105(sfcb)
FRTLHOME is /usr/sightlinePA
Warning: TimeZone is not set in /etc/timezone
Removed agentmgr.log file
Removed datamgr.log file
Removed servd.log file
Removed protomgr.log file
Removed protomgr.LOGFILEEIA.log log file
Removed datamgr.LOGFILEEIA.log log file
Removed datamgr.Local.log log file
Removed slaaListener.log file
SightLine Agent Manager system started.
SightLine Service Daemon started.
SightLine Data Manager started.
SightLine Agent Administrator started.
```

B.1.8 Add the system to Assure

In Assure, select **Settings | Add System** and supply the name of the everRun system, including names or IP addresses for everRun, both nodes and, optionally, both hardware instances. It will be added to the Assure dashboard as a single monitored system.



SNMP must be configured on the everRun nodes for Sightline to remotely monitor the system. See Section B.3, *Configuring SNMP Settings*, for details.

B.2 Monitoring KVM guests on everRun Systems

We recommend that you install a Sightline Power Agent on each guest of the monitored everRun system. This provides additional information about the performance of the guest.

everRun guests can be created as either Windows or Linux systems. Use the Power Agent installation kits and installation instructions located under the **Settings | Additional Monitoring** menu in Assure to obtain the necessary software.



When creating the everRun guest, note that the guest name must be a valid DNS name that resolves to a valid IP address. If not, the Power Agent on the guest will not be discovered. In addition, applications configured on the guest will not be correctly monitored by Assure (with or without a Power Agent on the guest).

B.3 Configure SNMP Settings

Simple Network Management Protocol (SNMP) must be enabled on each everRun node for Assure to monitor the everRun hardware. You can enable SNMP requests and SNMP traps:

- **SNMP request**—a request sent to the everRun system to retrieve the values of objects listed in the Management Information Bases (MIBs) supported by the everRun software. These MIBs include an everRun-specific MIB that is a collection of objects describing the everRun system.
- **SNMP trap**—a message initiated by the everRun system after an event such as an alert that is then sent to an identified list of recipients, typically a network management station (NMS).

To specify the desired security parameters, you must edit the standard `/etc/snmp/snmpd.conf` file on both nodes. For example, to allow SNMP requests by any user using the default `public` community, comment out or delete the following lines from that file on each node:

```
com2sec notConfigUser default public

group notConfigGroup v1 notConfigUser
group notConfigGroup v2c notConfigUser

view systemview included .1.3.6.1.2.1.1
view systemview included .1.3.6.1.2.1.25.1.1

access notConfigGroup "" any noauth exact systemview none none
```

After you save the edited files, you must restart the `snmpd` process on each node by entering the following command:

```
service snmpd restart
```

To enable SNMP requests:

1. Click **Preferences** in the left-hand navigation panel, to open the **Preference** page.
2. Under **Notification**, click **SNMP Configuration**.
3. Activate the check box next to **Enable SNMP Requests**.
4. Click **Save** (or click **Reset** to restore the previously-saved values).

To enable SNMP traps:

1. Click **Preferences** in the left-hand navigation panel, to open the **Preference** page.
2. Under **Notification**, click **SNMP Configuration**.

3. Activate the check box next to **Enable SNMP Traps**.
4. Type the name of the SNMP Community, or keep the default (public).
5. Next to **List of Recipients for SNMP traps**, type the IP address or host name for each recipient, one per line.
6. Click **Save** (or click **Reset** to restore the previously saved values).
7. Configure your organization's firewall to allow SNMP operations, as described below.
8. Generate a test alert, as described below.



Note: When you enable or modify the SNMP trap settings, generate a test alert to confirm that traps are received.

To configure your firewall to allow SNMP operations

To enable SNMP management systems to receive alerts from and send traps to the everRun system, configure your organization's firewall to open the following ports:

Message Type: SNMP

Protocol: SNMP

Port: 161 (Get/Walk) 162 (Traps)

To generate a test alert

Click **Generate Test Alert**. A test alert gets generated that triggers the delivery of SNMP traps. Watch the Alerts History log for delivery status. A sample SNMP trap is sent to all the recipients.

Appendix C

Prerequisites for Hardware Monitoring

Assure uses SNMP to retrieve hardware on monitored servers. You may need to enable SNMP on your system. In addition, you may need to configure a community string for your monitored systems.

C.1 Cisco

To monitor Cisco hardware, the firmware must be upgraded to at least version 2.0.

Use the CIMC portal to enable SNMP, as follows:

- ◆ Login to the CIMC portal of the server you want to monitor.
- ◆ Choose the **Admin** tab in the left navigation pane, and then select **Communication Services**.
- ◆ In the **Communication Services** window on the right, select the **SNMP** tab.
- ◆ Ensure that SNMP is enabled and has an **Access Community String**.
- ◆ Limited **SNMP Community Access** is acceptable for Assure.
- ◆ Save and exit.



Figure C-1. Cisco CIMC portal

C.2 Dell iDRAC 6

To enable SNMP on Dell iDRAC 6 system, open the iDRAC web page and follow these steps.

- ◆ Select **iDRAC Settings** in the left navigation pane.
- ◆ Select the **Network /Security** tab.
- ◆ Under the **Services** submenu, scroll down to **SNMP Agent**.
- ◆ Check the box to enable SNMP and provide a community string if you do not want to use public (default).

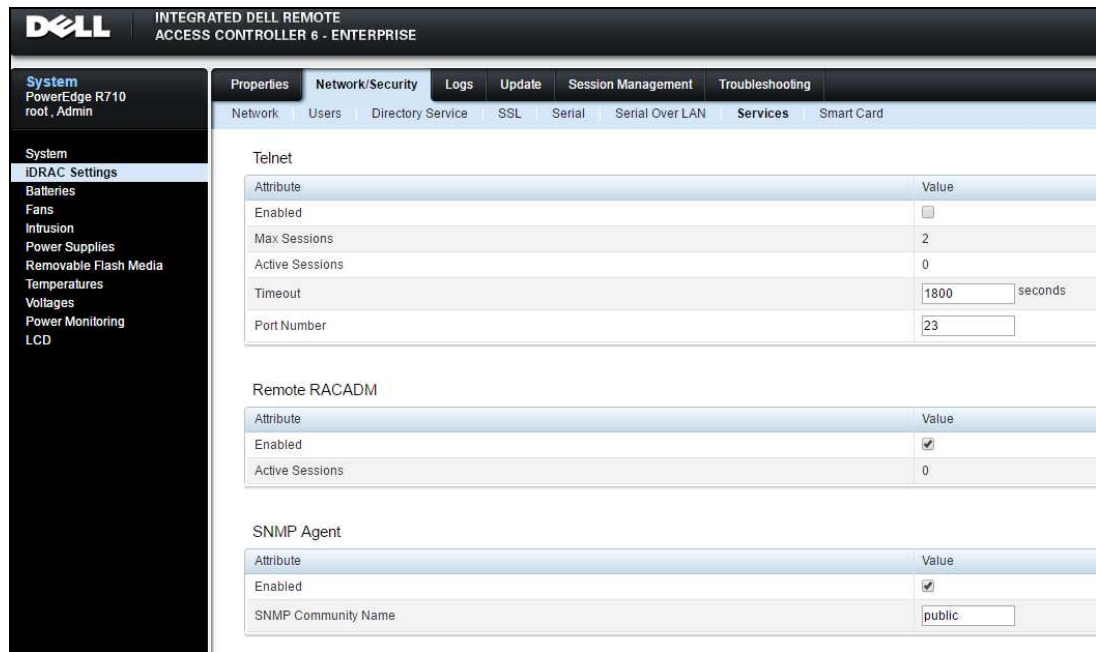


Figure C-2. Dell iDRAC portal

C.3 HP ilo

To enable SNMP on your HP system:

- ◆ Log into the ilo web interface.
- ◆ Select **Administration** in the left pane, and then the **Management** sub entry.
- ◆ Ensure that a community name exists in the **Read Community** field.
- ◆ Apply your settings.

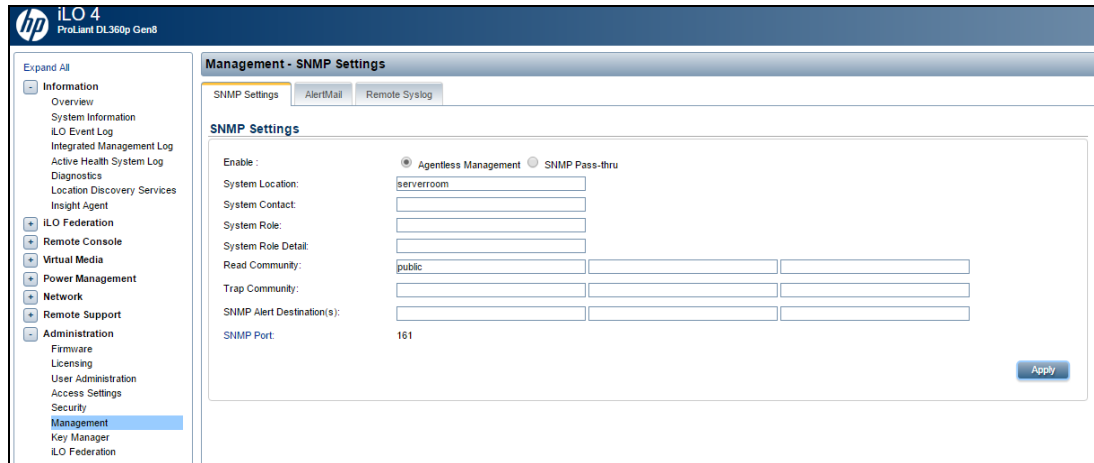


Figure C-3. HP ilo portal

C.4 Windows 2012 Systems

To configure an SNMP agent and community string on Windows 2012 systems:

- ◆ Log into your Windows 2012 server using Remote Desktop.
- ◆ Select **Windows Key > Administrative Tools > Server Manager**.
- ◆ Click **Manage > Add Roles and Features**.
- ◆ Click **Next > Next > Next > Next**.
- ◆ Verify that SNMP Services are installed and then click **Cancel**. (If SNMP is not installed, contact your systems administrator.)

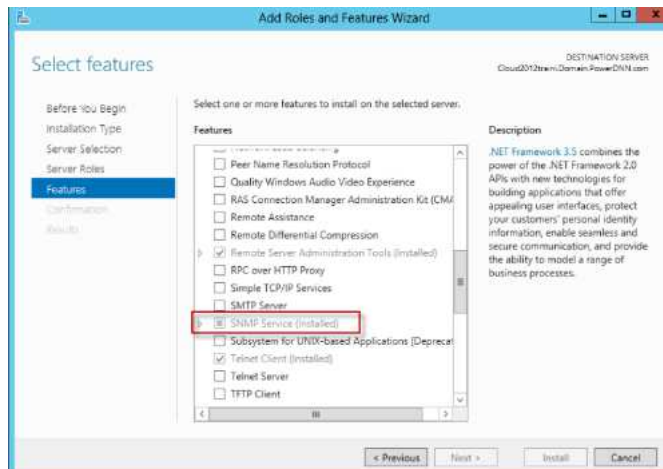


Figure C-4. Confirm SNMP Services on Windows 2012 Server

- ◆ Click **Windows Key > Administrative Tools > Services**.
- ◆ Right-click on **SNMP Service** and then click on **Properties**.
- ◆ Click on the **Security** tab.
- ◆ Enter your 8-10 character community string and set it to **READ ONLY**.

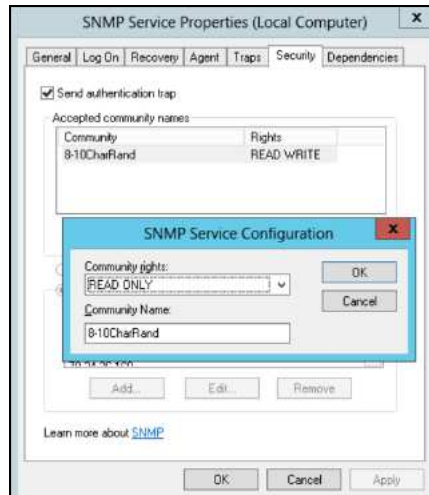


Figure C-5. Setting the Community String

- ◆ Click **OK** and **OK** again to exit all dialog boxes.

C.5 Windows 2008 R2 Systems

To configure an SNMP agent and community string on Windows 2008 R2 systems:

- ◆ Log into your Windows 2012 server using Remote Desktop.
- ◆ Select **Start > Administrative Tools > Server Manager**.
- ◆ Click **Features > Add Features**.
- ◆ Verify SNMP Services are installed.
- ◆ Click **Configuration > Services**.
- ◆ Right-click on **SNMP Service** and then click on **Properties**.
- ◆ Click on the **Security** tab.
- ◆ Enter your community string and set it to **READ ONLY**.
- ◆ Click **Add** and then exit all dialog boxes.

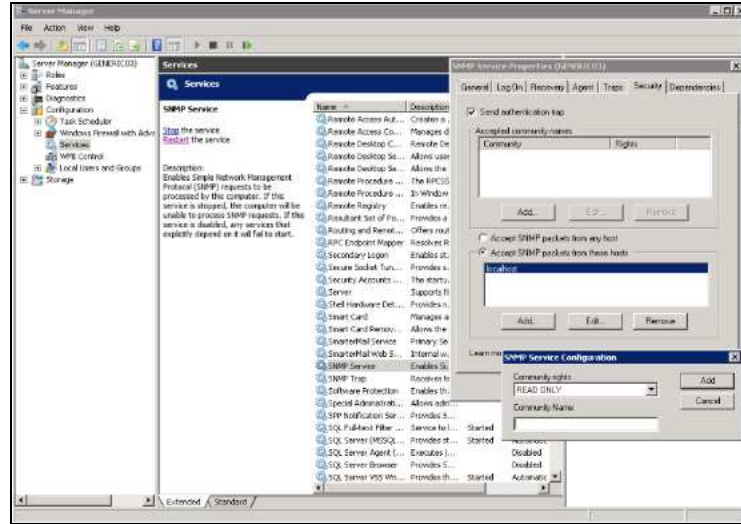


Figure C-6. Configure Community String on Windows 2008 R2 Server

